Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Network Event Correlation Using Unsupervised Machine Learning Algorithms

Maxwell Dondo, Peter Mason, Nathalie Japkowicz
and Reuben Smith

Defence R&D Canada – Ottawa
TECHNICAL MEMORANDUM
DRDC Ottawa TM 2006-193
November 2006

Canada

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Network Event Correlation Using Unsupervised Machine Learning Algorithms	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defence R&D Canada - Ottawa Technical Memorandum DRDC Ottawa TM 2006-193 Canada**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**108**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Network Event Correlation Using Unsupervised Machine Learning Algorithms

Maxwell Dondo
Peter Mason
DRDC Ottawa

Nathalie Japkowicz
Reuben Smith
University of Ottawa

Defence R&D Canada – Ottawa
Technical Memorandum
DRDC Ottawa TM 2006-193
November 2006

Principal Author

Original signed by Maxwell Dondo

Maxwell Dondo

Approved by

Original signed by J. Lefebvre

J. Lefebvre
Head/NIO Section

Approved for release by

Original signed by C. Boulet

C. Boulet
Head/Document Review Panel

© Her Majesty the Queen in Right of Canada as represented by the Minister of National Defence, 2006

© Sa Majesté la Reine (en droit du Canada), telle que représentée par le ministre de la Défense nationale, 2006

Abstract

We have successfully implemented a two-stage event correlation model for intrusion detection system (IDS) alerts. The model is designed to automate alert and incidents management and reduce the workload on an IDS analyst. We achieve this correlation by clustering similar alerts together, thus allowing the analyst to only look at a few clusters instead of hundreds or thousands of alerts. The first stage of this model uses an artificial neural network (ANN)-based autoassociator. The autoassociator is trained to reproduce each alert at its output, and it uses the error metric between its input and output to cluster similar alerts together. The accuracy of the system is improved by adding another machine-learning stage which attempts to combine closely related clusters produced by the first stage into super-clusters. The second stage uses the Expectation–Maximisation (EM) clustering algorithm. The model and performance of this model are tested with intrusion alerts generated by a Snort IDS on DARPA's 1999 IDS evaluation data as well as `incidents.org` alerts.

Résumé

Nous avons réussi l'implantation d'un modèle de corrélation d'événements à deux étapes pour les alertes IDS (système de détection d'intrusion). Ce modèle a été étudié afin d'automatiser la gestion des alertes et des incidents et réduire la charge de travail de l'analyste IDS. Nous réalisons cette corrélation en groupant les alertes semblables, ce qui permet à l'analyste d'examiner des groupes au lieu de centaines, voire de milliers d'alertes. La première étape de ce modèle a recours à un auto-associateur basé sur ANN. Cet auto-associateur subit un apprentissage pour reproduire chaque alerte en sortie, et exploite une mesure d'erreur entre l'entrée et la sortie pour grouper les alertes semblables. La précision du système est rehaussée grce à l'ajout d'une autre étape d'apprentissage machine dans laquelle on essaie de combiner les groupes étroitement reliés, obtenus dans la première étape, et former de supergroupes. La seconde étape fonctionne avec l'algorithme de groupage EM. Le modèle et sa performance sont testés au moyen d'alertes d'intrusion générées par un Snort IDS exploitant des données d'évaluation IDS 1999 du DARPA.

This page intentionally left blank.

Executive summary

Network Event Correlation Using Unsupervised Machine Learning Algorithms

Maxwell Dondo, Peter Mason, Nathalie Japkowicz, Reuben Smith; DRDC Ottawa
TM 2006-193; Defence R&D Canada – Ottawa; November 2006.

Background: This work is a follow-up of our earlier work, Autocorrel I [1], in which we attempted to make an intrusion detection system (IDS) analyst's job easier by clustering similar alerts together, thereby reducing the number of alerts that an analyst has to deal with. In this work we tried to address the shortcomings of Autocorrel I, in particular the accuracy of the results.

In our conclusions to the Autocorrel I model, we noted that the results could be improved. We also noted that the most likely source of our errors was in the collapsing of a 42-tuple input pattern into a single threshold value which was used to perform the clustering. Therefore, in this work we added a second stage to provide a second layer of clustering. This second stage combines the threshold heuristic of the first stage (Autocorrel I) with raw attributes from Snort alerts.

We propose to use a neural network-based novelty detection approach and a machine-learning clustering algorithm to identify and cluster alerts into smaller attack categories. In this way, the analyst's job is made significantly easier.

Principal results: We applied our approach to labelled DARPA alerts obtained from the 1999 DARPA IDS evaluation data set as well as to unlabelled `incidents.org` alerts. We successfully clustered sets of 500 alerts in each case with an accuracy of over 86%. The data was clustered into 21 and 18 clusters respectively. Thus, instead of sifting through 500 alerts, the analyst would only go through a maximum of 21 clusters for these particular data sets. This was a significant improvement from the results of Autocorrel I which produced an accuracy of 59% (76% with manual human intervention).

Significance of results: The accuracy of our results show that our original objectives were met. We were able to reduce the number of alerts that an analyst has to deal with on a daily basis, and we were able to significantly improve the accuracy of our results from the previous model. If developed further, this approach could produce a product that would be useful to IDS analysts like the Canadian Forces (CF) Computer Incident Response Team (CIRT) at the Canadian Forces Network Operations Centre (CFNOC). However, since the results were not perfect, more experimentation with different algorithms could improve the accuracy even more.

Future work: Although no future work is planned at this time, future work could focus on improving the accuracy of the system by using other clustering algorithms. An approach may also be required to help the analyst identify and manage the few instances of erroneous clustering.

Sommaire

Network Event Correlation Using Unsupervised Machine Learning Algorithms

Maxwell Dondo, Peter Mason, Nathalie Japkowicz, Reuben Smith; DRDC Ottawa TM 2006-193; R & D pour la défense Canada – Ottawa; novembre 2006.

Contexte: Ce travail est la poursuite d'un travail précédent, Autocorrel I [1], dans lequel on a essayé de faciliter le travail d'un analyste IDS en groupant des alertes similaires, afin de réduire le nombre d'alertes qu'un analyste devait examiner. Dans le travail actuel, nous avons essayé de corriger les lacunes de Autocorrel, tout particulièrement d'améliorer l'exactitude des résultats.

Dans nos conclusions sur le modèle Autocorrel I, nous avions souligné le fait que les résultats pouvaient tre améliorés. Nous avions aussi mentionné que la source la plus probable des erreurs découle de la réduction d'un modèle d'entrée à 42-tuples en un modèle à un seuil unique, nécessaire pour effectuer le groupage. C'est pourquoi, dans la recherche actuelle, nous avons ajouté une deuxième étape afin d'obtenir une seconde couche de groupage. Cette deuxième étape combine la solution d'une valeur seuil, celle de la première étape de Autocorrel I, aux attributs bruts des alertes Snort.

Nous proposons d'utiliser un réseau neuronal fonctionnant d'après une nouvelle approche de détection et un algorithme de groupage par apprentissage machine servant à l'identification et au groupage des alertes en petites attaques. Ainsi, le travail de l'analyste se trouve considérablement simplifier.

Principaux résultats: Nous avons mis en pratique notre approche sur des alertes DARPA étiquettées provenant des données d'évaluation IDS 1999 de DARPA, de mme que sur des alertes non étiquettées `incidents.org`. Nous avons réussi à grouper des ensembles de 500 alertes dans chaque cas, avec une précision supérieure à 86%. Les données ont été réunies en groupes de 21 et 18 alertes respectivement. Ainsi, l'analyste au lieu de parcourir 500 alertes n'a plus à examiner que 21 groupes pour cet ensembleparticulier de données. Il s'agit là d'une amélioration importante par rapport aux résultats de Autocorrel I, qui avait rendu une précision de 59% (76% dans le cas de l'intervention humaine).

Interprétation des résultats: L'exactitude de nos résultats démontre l'atteinte de nos objectifs de départ. Nous avons été en mesure de réduire le nombre d'alertes qu'un analyste doit traiter chaque jour, et nous sommes parvenus à améliorer sensiblement l'exactitude de nos résultats, par rapport au modèle précédent. Si nous poursuivons

cette recherche, nous allons pouvoir construire un produit utile aux analystes IDS, comme le CF CIRT est utile pour le CFNOC. Comme nos résultats ne sont pas parfaits, un surplus d'expérimentation avec des algorithmes différents devrait rehausser encore plus l'exactitude des résultats.

Travaux à venir: Bien que rien ne soit prévu pour le moment, les travaux à venir devront se concentrer sur l'exactitude du système via l'utilisation d'autres algorithmes de groupage. Une approche devrait aussi tre aussi envisagée afin d'aider l'analyste à déceler et à gérer les quelques cas de groupages erronés.

Table of contents

List of figures

This page intentionally left blank.

1 Introduction

In our earlier work, Autocorrel I [1,2], we implemented an event correlation approach using an artificial neural network (ANN). The purpose of that work was to correlate network events in an effort to assist an intrusion detection system (IDS) analyst. In this work, we build on the success of Autocorrel I, and attempt to address its shortcomings. We also hope to be able to address the research recommendations made in Autocorrel I.

1.1 Background

Intrusion detection analysts can be overwhelmed by the multitude of alerts that they receive on a daily basis. The majority of these alerts are not new, but the analyst must go through each one of them to determine the threat they each pose. It would be beneficial to the IDS analyst if similar alerts were clustered together. In some cases, analysts use multiple IDS rules to classify alerts or use some of the generic correlation tools that come bundled together with IDSs.

There are a number of IDSs that can perform correlation using different correlation techniques. However, most of the correlation tools use only limited attributes within the alert to perform the correlation, and are often unable to produce accurate results. As a result, there have been significant research efforts to design correlation tools that can improve on these existing approaches. In this work, we explore a machine-learning approach to network event correlation that builds and improves on our previous model, Autocorrel I.

In this section, we review existing approaches to event correlation. We then present our approach and show how it is related to the existing approaches.

1.1.1 Previous Work

The majority of the existing correlation tools use elementary approaches to correlate attacks. For example, Shadow [3] and ACID [4] use the internet protocol (IP) addresses to correlate attacks. However, it is known that IP addresses may be spoofed, therefore using IP addresses alone may not be sufficient to identify correlated alerts.

Recent work reported by Haines *et al.* [5] details some of the common correlation tools and approaches. The majority of these approaches take one alert attribute at a time to correlate with other possible attacks. More sophisticated approaches use statistical methods on multiple alert attributes [6]. Statistical approaches usually make assumptions about the underlying statistical distributions of alert attributes. ANNs, on the other hand, do not make prior assumptions about the data they handle [7,8].

In their recent work, Hätälä *et al.* [9] also analyse various alert correlation efforts by different groups. They give the details of a number of correlation systems, most of which are not based on machine learning. They also discuss the Intrusion Detection Message Exchange Format (IDMEF) standard proposed by the Intrusion Detection Working Group (IDWG) [10] which hopes to encourage the development and interoperability of alert correlation in deployed intrusion detection systems.

Ning and Cui [8] recognise that many existing IDSs tend to detect low-level events without being able to relate these events to the broader plan of the attacker. Their goal was to create hierarchies of alerts using prerequisites and consequences for each type of alert. They attained this goal using a rule-based system (rather than a machine-learning system) that assigned prerequisites and consequences to each type of alert, which in turn allowed the analyst to see the possible consequences of the most mundane of alerts. Their system ran on the output of existing IDS systems. They demonstrated the usefulness of their system by showing how their system could significantly reduce the number of false alarms reported by an IDS while negligibly reducing the valid alarms. Their tool is most logically used as an off-line forensic tool for mining old stored alerts after a new vulnerability is found.

Debar and Wespi [11] presented an aggregation and correlation component (ACC) for an IDS. They used this correlation component to flag alerts as an original, a consequence, or a double alert. In this research, they presented rule-based methods for attaining this goal. They concerned themselves with implementation issues such as integrating their ACC with existing IDSs – namely, the Tivoli Enterprise Console – and they adopted the use of the IDWG [10] format for their work. They discussed other issues such as raising or lowering the priority of IDS alerts to reflect the inferences of their ACC.

Julisch *et al.* used a conceptual clustering algorithm in their model [12]. They resolved the problem of training their system by relying on conceptual clustering algorithms rather than classification algorithms which require training. However, they require to train the system as to which alerts can be handled automatically. They advocated having the administrator hand-modify the correlation system once per month to reflect the changes in the network environment. Their system also required that the correlation system have information specific to the local network before initial operation of the system. The approach requires a seasoned analyst to perform this initial configuration.

Dain and Cunningham [13] also presented another machine-learning-based correlation system. In their paper, they trained machine learning algorithms such as neural networks and decision trees to recognise attack scenarios based on a novel list of features. Hätälä *et al.* [9] criticise this work for its use of a simplistic data set. The Dain *et al.* research was only tested with a Defence Conference (DEFCON) data

set [14]. The use of this data set simplified the problem of alert correlation because attackers were motivated by points in the competition and no points were awarded for stealthy attacks. As such, many of the attacks originated from a single IP address (Dain *et al.* [13]).

Other traditional correlation techniques involve the storage of historical data for future correlations. Due to the huge amounts of data that needs to be stored, a format called the *TCP Quad format* [15] is usually used to store reduced data content. It only stores six event attributes, namely `date, time, Source IP, Source Port, Dest IP, Dest Port, Protocol`. However, by reducing the data, there is less information available with which to correlate.

Our previous work, Autocorrel I [1], attempted to address many of these shortcomings. We implemented an ANN-based event correlation engine that took most alert attributes into account. However, the results produced by the Novelty Detection algorithm [16] used in this work produced systematic errors. The main source of this error was attributed to mapping a 42-dimensional alert attribute space into a 1-dimensional clustering metric. It required manual human intervention to improve its alert clustering accuracy to 76%.

1.2 Our Approach

The objective of this work was to build on the success we achieved in Autocorrel I [1] and improve the performance of the model while trying to achieve our original correlation goal. We implemented a two-stage alert correlation approach involving an ANN autoassociator and another machine-learning model, the Expectation–Maximisation (EM) algorithm.

The first step takes a set of alerts, constructs the first step alert attributes, trains an autoassociator, and outputs alert clusters. Based on the reconstruction error determined by the autoassociator, closely matched alerts are grouped together to form this first set of clusters. The reconstruction error from the first stage and attributes from raw alerts in the first stage clusters are processed by the second stage using the EM algorithm. The result is a new set of clusters which include clusters from the first stage.

Adding a second stage of clustering effectively mimics Valdes and Skinner's approach [6] of finding attack step correlations after the threading and multi-sensor correlations have been done. However, unlike approaches by Dain *et al.* [13] and Julisch *et al* [12], which used supervised data mining approaches, we used an unsupervised machine-learning approach.

There are several advantages to using an ANN based approach. First, ANNs acquire

knowledge straight from the data without the need for a human expert to build sets of domain rules and facts. Second, once trained, ANNs are known to be fast and quite good for near real-time applications. Finally, while learning, ANNs perform a type of dimensionality reduction allowing a user to input large amounts of information without fearing an efficiency bottleneck. Thus, rather than storing the data in transmission control protocol (TCP) Quad format [17] and performing a multi-stage query on insufficient information, the user can input all the relevant information available and allow the neural network to organise and reduce this knowledge in an adaptive and goal-oriented fashion. We also explored a number of clustering algorithms to determine the best algorithm for the second stage. We concluded, through experimentation, that the EM algorithm would be the best for this work.

We demonstrate this approach by applying the system to the labelled 1999 DARPA IDS evaluation data set [18] as well as unlabelled `www.incidents.org` alerts. We use Snort [19] to extract alerts from the supplied raw TCPDump [20] format data.

The layout of our report starts with an overview of ANNs and clustering algorithms in Section 2. In Section 3, we present the complete model used, and the data modelling process. The experimentation and results are presented in Section 4. We follow this with our conclusions and discussions in Section 5.

2 Artificial Neural Networks (ANN)s and Clustering Algorithms

In this section we review the theory of ANNs. We also look at clustering algorithms, and explain how they were used in this work.

2.1 Artificial Neural Networks

ANN models attempt to emulate the human brain through the dense interconnection of simple computational elements called neurons [21]. Each neuron is linked to some of its neighbours through synaptic connections of varying strengths. Learning is accomplished by continuously adjusting these connection strengths (weights) until the overall network outputs the desired results. These weight adjustments are based on nonlinear optimisation algorithms.

2.1.1 The Neuron

Similar to the biological nervous system, the basic computational element of an ANN is called the neuron or processing node. The neuron model is a highly simplified model of the biological neuron. A simple node is shown in Figure 1, where N inputs are summed at the node. Each input u_i is connected to the processing node through the

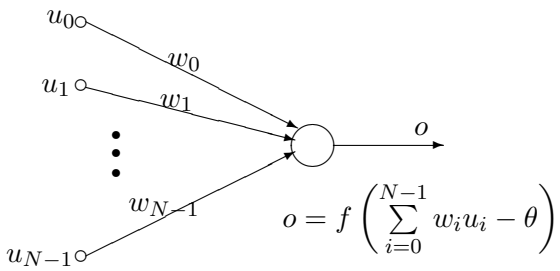


Figure 1: *The basic neuron*

synaptic connections, which are represented by connection strengths called weights w_i. A bias term θ is also used at each node. The sum is fed through a transfer function f, called the activation function, to generate the output o. The signal flow is considered unidirectional, as indicated by the arrows.

Although ANNs are constructed using this fundamental building block, there are significant differences in the architectures and driving fundamentals behind each ANN model.

2.1.2 The Activation Function

The activation function f plays a pivotal role in the functioning of the neuron. It determines the node output. As in Figure 1, the neuron output signal is given by:

$$o = f\left(\mathbf{w}^T\mathbf{u}\right) \tag{1}$$

where $\mathbf{w}$ is the weight vector defined as

$$\mathbf{w} \equiv \left[\begin{array}{cccc} w_1 & w_2 & \cdots & w_N \end{array}\right]^T$$

and the input vector $\mathbf{u}$ is defined as

$$\mathbf{u} \equiv \left[\begin{array}{cccc} u_1 & u_2 & \cdots & u_N \end{array}\right]^T$$

It should be noted that in ANN implementations, $u_N = -1$ and $\theta = w_N$.

There are many different types of activation functions f to choose from, depending on the application [21, 22, 23]. Some of the commonly used activation functions are shown in Figure 2. These activation functions are the *hard-limiter*, the *threshold logic*, and the *sigmoid*. Since real applications are usually modeled as continuous functions, the most commonly used smooth continuous activation function is the sigmoid.

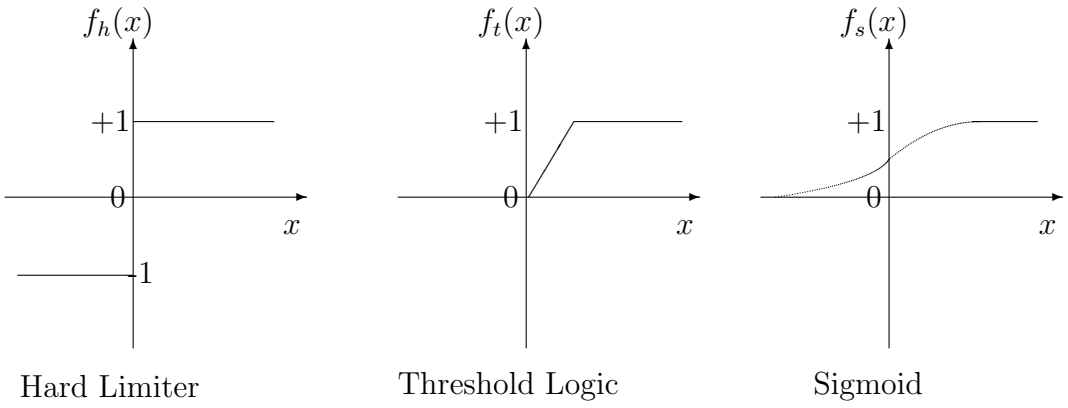


Figure 2: *Activation functions*

Activation functions may be either unipolar, for positive output, or bipolar for output that may be positive or negative. For example, the bipolar sigmoidal activation function is defined as:

$$f(x) \equiv \frac{2}{1 + \exp^{-\lambda x}} - 1 \tag{2}$$

and the unipolar sigmoidal activation function is defined as

$$f(x) \equiv \frac{1}{1 + \exp^{-\lambda x}} \tag{3}$$

where λ is a constant.

The basic building block of an ANN is a single node based on the neuron model shown in Figure 1. It is called a *perceptron* after the work of Rosenblatt [21]. A perceptron can consist of one or more neurons in one layer. If a continuous activation function is used, the neuron model is known as a *continuous perceptron*. A continuous perceptron is capable of classifying *linearly separable* classes of data of the form $f(x) = ax + b$.

2.1.3 Multi-Layer ANNs

To emulate massively interconnected biological systems, ANNs have to be similarly interconnected. ANNs are the simple clustering of primitive artificial neurons. This clustering occurs by creating layers of neurons which are connected to one another. Figure 3 shows a multi-layer perceptron (MLP). An input layer interfaces with the outside world to receive inputs and an output layer provides the outside world with the network's outputs. The rest of the neurons are hidden from view, and are called *hidden layers*.

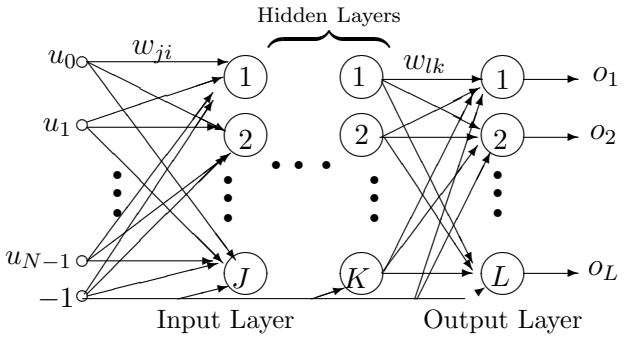


Figure 3: *Multi-layer perceptron.*

The objective of using an MLP is to be able to classify patterns that linear classifiers (single layer ANNs) are incapable of classifying. The most important attribute of multi-layer ANNs is that they can learn to classify a problem of any complexity. The biggest challenge is usually in deciding the number of hidden layers in an ANN.

Zurada [23] gives an extensive discussion on the design of the number and size of hidden layers in a given architecture; nevertheless, trial and error methods have been widely used. If the number of hidden layers is too large, the ANN architecture will

have problems generalizing; it will simply memorize the training set, making it useless for use with new data sets.

Inter-layer connections within an ANN architecture can take the following forms [23]:

- In a *fully-connected* ANN, each neuron on one layer is connected to every neuron on the next layer.
- In a *partially-connected* ANN, a neuron on one layer does not have to be connected to all neurons on the next layer.

If signal flow direction is taken into consideration, these two architectures can be further refined:

- In a *feedforward* ANN, the neurons on one layer send their output to the neurons in the next layer (uni-directional), but they do not receive any input back from the neurons in the next layer.
- In a *bi-directional* ANN, the neurons on one layer may send their output to the next layer or the preceding layer, and the subsequent layers may also do the same.
- In a *hierarchical* ANN connection, the neurons of a lower layer may only communicate with neurons on the next level of layers. The problem is divided and solved in more than one step.
- In a *resonance-connected* ANN, the layers have bi-directional connections, and they can continue sending messages across the connections a number of times until previously defined conditions are achieved.

In more sophisticated ANN structures the neurons communicate among themselves within a layer; this is known as intra-layer connection. These take the following two forms:

- In fully- or partially-connected *recurrent* networks, neurons within a layer communicate their outputs to neurons within the same layer. This is done a number of times before they are allowed to send their outputs to another layer.
- In *on-center/off-surround* ANNs, a neuron in one layer has an excitatory connection to itself and its neighbors, and has inhibitory connections to other neurons in the same layer.

The overall architecture of an ANN depends on the input–output mappings required, the type of input patterns, and the learning rules to be used.

2.1.4 ANN Training

Similar to the brain, ANNs learn from experience. ANNs are trained by adjusting the connection weights $\mathbf{w}$ during each iteration until the desired output is produced at o (see Equation 1). The learning ability of an ANN is determined by its architecture and by the algorithm chosen for training. The training methods [21] fall into broad categories:

- In *unsupervised training*, hidden neurons find an optimum operating point by themselves, without external influence.
- *Supervised training* requires that the network be given sample input and output patterns to learn. It is guided through the learning process until a satisfactory optimum operating point or a predefined threshold is reached. The most common training termination criteria is by setting a training threshold.

Backpropagation training is a form of supervised learning that has proven highly successful in training multi-layered ANNs. Information about errors is filtered back through the system and is used to adjust the connections between the layers, thus improving performance.

ANNs can be trained *on-line* or *off-line*. In off-line training algorithms, weights do not change after the successful completion of the initial training. This is the most common training approach; especially in supervised training. In on-line or real time learning, weights continuously change when the system is in operation [23].

2.1.5 Training Rules

There is a wide variety of learning rules that are used with ANNs. In general, all ANN learning involves the iterative updating of the connection weights until the desired result is achieved. Most training algorithms start by initializing the weights to 0 or very small random numbers. This weight update is given by:

$$\mathbf{w}^{k+1} = \mathbf{w}^k - \Delta\mathbf{w}^k \tag{4}$$

Equation 4 is the ANN *general learning rule* [23]. The numerous learning rules, which are variations of this rule, only differ by the mathematical algorithms used to update the connection weights, or more specifically to calculate the value of $\Delta\mathbf{w}^k$ at each iteration k. Some of the common training rules are as follows:

- In the *Hebbian* rule [23, 22], the connection weight update $\Delta\mathbf{w}^k$ is proportional to the neuron's output. This was the first ANN learning rule [21, 24].
- The *perceptron* rule [21] updates the weights based on the difference between the desired output d and the actual neuron's response o.

- The *delta* learning rule [21,24] is based on the minimisation of the mean square error (MSE):

$$\mathbf{w}^{k+1} = \mathbf{w}^k - \eta \nabla E\left(\mathbf{w}^k\right) \tag{5}$$

where η is a learning constant, and ∇E is the gradient of the error function E, defined by:

$$E_k = \frac{1}{2}\left(d^k - o^k\right)^2 \tag{6}$$

The objective is to iterate Equation 5 until the error E approaches zero (or a preset threshold value).

- The *Widrow-Hoff* [22,23] learning rule (sometimes called the *Least Mean Square* learning rule) is considered a special case of the delta learning rule in that the neuron output o is independent of the activation function f.

- The most widely used supervised training approach, which is derived from the Widrow-Hoff algorithm, is the *error backpropagation training algorithm*. As the name implies, the error $\Delta\mathbf{w}^k$ is propagated back into the previous layers. This is done one layer at a time, until the first layer is reached.

  Consider an ANN with one hidden layer, K outputs, J hidden nodes, and I inputs. The output layer weights are adjusted as follows:

$$w_{kj} = w_{kj} + \eta\delta_{ok}y_j, \quad \text{for } k = 1,\cdots,K,\ j = 1,\cdots,J \tag{7}$$

where η is a learning constant and the output error δ_{ok} is given by

$$\delta_{ok} = \frac{1}{2}(d_k - o_k)(1 - o_k^2), \quad \text{for } k = 1,2,\cdots,K \tag{8}$$

The weight update for the hidden layer is as follows:

$$w_{ji} = w_{ji} + \eta\delta_{yj}u_i, \quad \text{for } k = 1,\cdots,K,\ i = 1,\cdots,I \tag{9}$$

where the output error δ_{yj} is given by

$$\delta_{yj} = \frac{1}{2}(1 - y_j^2)\sum_{k=1}^{K}\delta_{ok}w_{kj}, \quad \text{for } j = 1,2,\cdots,J \tag{10}$$

The process is iteratively repeated until a preset threshold of the mean square error (MSE).

For an ANN with P training patterns, and K outputs, the *root-mean square error* is defined as:

$$E_{rms} = \frac{1}{PK}\sqrt{\sum_{p=1}^{P}\sum_{k=1}^{K}(d_{pk} - o_{pk})^2} \tag{11}$$

In most ANN implementations, this value is usually used to terminate training when a satisfactory value is reached. Reaching the maximum number of training epochs can also be used to terminate training.

2.1.6 The Autoassociator

The autoassociator is a fully-connected, multi-layer, feedforward ANN. The principle of autoassociation is very simple: in an unsupervised ANN training, inputs are made the targets. An autoassociator ANN thus tries to learn the identity function.

The architecture is similar to that of a MLP shown in Figure 3. The potential of the autoassociator to internally represent data trends often lies in the number of hidden units and design of the hidden layer, so these parameters should be carefully tailored to the problem. The input and output layers are of equal size.

From Figure 3, the reconstruction error ϵ for a given autoassociator with M inputs is given by the Euclidian distance between input and output:

$$\epsilon = ||\mathbf{u} - \mathbf{o}|| = \sqrt{\sum_{i=1}^{M} [o_i - u_i]^2} \tag{12}$$

where $\mathbf{u}$ is the input vector and $\mathbf{o}$ is the output vector. In our work, this represents the reconstruction error (RE).

The autoassociator uses the reconstruction error ϵ to classify different inputs. The theory holds that data items from input data categories which did not have representative training examples will have higher reconstruction errors. Data items which are not similar are expected to have distinguishable reconstruction errors [25].

In this work, we use the autoassociator as an extension to the work by Japkowicz *et al.* [16,26] and other researchers such as Sungzoon *et al.* [27] on Novelty Detection. In these works, it was seen that the autoassociator was very good at grouping previously seen events together, discriminating them from novel events. That kind of clustering, however, was coarse-grained. Our purpose here is to use the autoassociator in a similar capacity, but as a finer-grained clustering system.

2.2 Clustering Algorithms

Like the autoassociator, clustering algorithms are machine-learning approaches used to categorise similar objects based on the objects' attributes. Since our work involves alert clustering, in this section, we review the theory of the two clustering algorithms used in our model; namely the Expectation–Maximisation (EM) algorithm (Section 2.2.1) and self-organising maps (SOM) (Section 2.2.2). We also use the autoassociator (Section 2.1.6) as will be explained later.

2.2.1 The Expectation–Maximisation (EM) Algorithm

The EM algorithm is one of the most well-known clustering algorithms [28, 29]. It helps to find maximum-likelihood estimators in problems with incomplete or missing data. Initially presented in Dempster *et al.* [30], it consists of two repeated steps: expectation and maximisation. The EM algorithm uses a statistical model called *finite mixtures* to achieve the goal of producing the most likely set of clusters given the number of clusters, k, and a set of data [31].

The model consists of a set of k probability distributions, one to represent the data of each cluster. There are parameters that define each of the k distributions. The EM algorithm begins by making initial guesses for these parameters based on the input data, then, for each data instance, determines the probability that it belongs to a particular cluster using these parameter guesses. Based on the results, the distribution parameters are revised again and this process is repeated until the resulting clusters satisfy some predefined conditions or until a maximum number of algorithm iterations is reached.

In this work, we utilise the EM algorithm as implemented in the Waikato Environment for Knowledge Analysis (Weka). Weka [32] is a tool developed at the University of Waikato in New Zealand.

2.2.2 Self-Organizing Maps (SOM)

The SOM is an ANN algorithm developed by Teuvo Kohonen [33, 34], though some prefer to refer to it as a specific type of clustering algorithm [28]. It is an unsupervised method of mapping a high-dimensional input to a two-dimensional output such that similar inputs are mapped to close locations in the two-dimensional map (grid or lattice) output as illustrated in Figure 4 [21]. (Actually, other dimensionalities are available for output as well, but two-dimensional output is the most common.) This mapping is primarily used for the visualisation of high-dimensional data, but it can also be used for clustering.

Like other ANNs, the SOM has training parameters and is trained iteratively. The first step is to initialise the weights from N inputs to the M output nodes to small random numbers, and define an initial neighborhood radius for each node. The neighborhood d is the set of nodes which are similar to a given node. As the training progresses, the number of nodes in the neighborhood shrinks until only nodes representing similar inputs are left in the neighborhood. Thus, $M > d(t_1) > d(t_2) \ldots$, where time $t_1 < t_2 \ldots$.

As illustrated in Figure 4, each input x_i is connected to every output node j through a weight w_{ij}. At each step, an input vector $\mathbf{x}$ is presented to the SOM. The distance

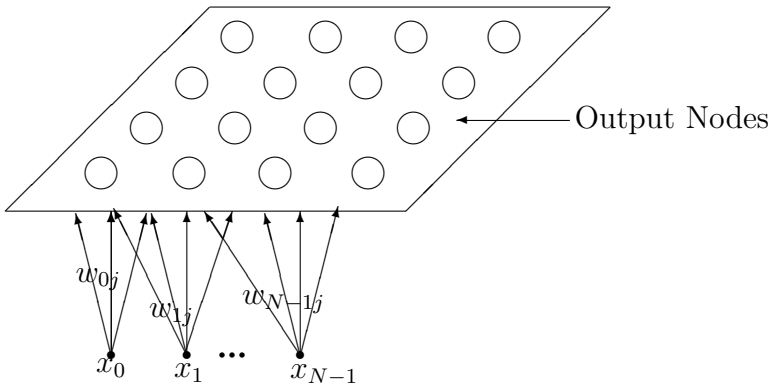


Figure 4: *Representation of an SOM.*

between $\mathbf{x}$ and the SOM weight vectors is calculated, and the neuron whose weight vector $\mathbf{w}_c$ is closest to the input vector $\mathbf{x}$ is called the best-matching unit (BMU) as defined by the following equation:

$$||\mathbf{x} - \mathbf{w}_c|| = \min_i ||\mathbf{x} - \mathbf{w}_i|| \quad \text{for} \quad i = 1, \ldots, d \tag{13}$$

where $||\cdot||$ is the Euclidian distance similar to Equation 12.

Whenever an example $\mathbf{x}$ is presented to the SOM, the closest representative weight vector $\mathbf{w}_j$ is found. The weight update at each iteration is as follows:

$$\mathbf{w}_i \leftarrow \mathbf{w}_i + \alpha[\mathbf{x} - \mathbf{w}_i] \quad \text{for all } i \text{ in the spatial neighbourhood of } j \tag{14}$$

The constant α and the neighbourhood are allowed to change. Vesanto *et al.* [35] also discuss other methods of clustering the SOM. In other related work, Vesanto *et al.* [36] developed the SOM Toolbox for use with MATLAB.

In our implementation the SOM is trained by initially giving the training data their approximate position on the grid and initialising the weights to small random numbers. Data is presented to the SOM and the corresponding output determined. For SOMs the output for an input data instance represents a point in the SOM. Similar outputs in the SOM should have similar representation in the higher dimensional input space. To cluster the SOM output we create one cluster for every point in the SOM output that has at least one data instance associated with it. In practice this produces acceptable clusters.

3 The Alert Correlation Model

Our model of finding correlations was implemented in two steps. The first step clustered input alerts. The second step was designed to take these clusters, and re-cluster them into super-clusters. The steps are summarised in Figure 5.

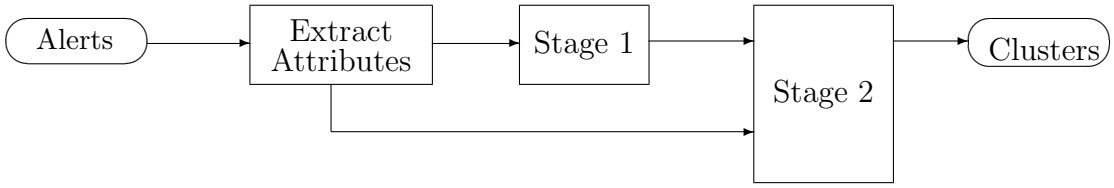


Figure 5: *AutoCorrel II model layout.*

The model takes alerts as input. Attributes are extracted from the alerts and fed into the first correlation step, Stage 1. This stage is very similar to Autocorrel I, in our previous work [1]. Stage 2 takes in the output from Stage 1 as well as original attributes extracted from the alerts. The processing in this stage produces the final alert clusters.

We will describe each of the stages in more detail. We will also give details of the data that was used in this work.

3.1 First Correlation Step (Stage 1)

In the first stage, our model collects alerts from input sensors. These sensors could be homogeneous or heterogeneous. However, we expect that all the sensors pass in their alerts as packets or sequences of packets that can be converted into Snort alerts. The alert packets are passed to Snort which then generates the relevant alerts. Using the same approach we used with Autocorrel I [1, 2], we extracted selected features from these alerts. This set of features was created to fully represent an IP packet flagged as an alert by an IDS, in our case by a Snort IDS. The feature set allows similar-looking IP packets to be clustered together by our algorithm.

In the first stage, we used the autoassociator for clustering. We used this ANN because we want to build on its performance from our previous work. We hope to improve the results of this model by adding a second stage.

As illustrated in Figure 6, we input the alerts data into an autoassociator. We then train it to reproduce the same alerts at the output. When training is complete, alerts are presented to the autoassociator. The reconstruction error (RE) between the input alert vector $\mathbf{x}_i$ and the autoassociator output alert vector $\mathbf{y}_i$ is determined for each

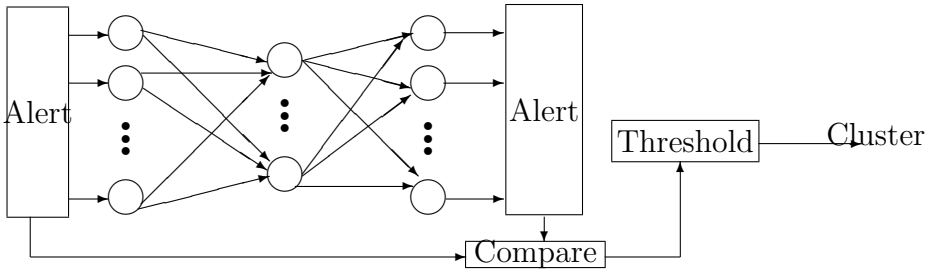


Figure 6: *AutoCorrel I model.*

alert as follows:

$$e_i = ||\mathbf{x}_i - \mathbf{y}_i|| \tag{15}$$

Using a predetermined threshold value, alerts with similar REs are grouped together as clusters. These clusters are the final result of stage 1, and they become an input to stage 2. Equation 15 essentially reduced a 42-dimensional vector into a 1-dimensional threshold metric e (RE) used for clustering (this was identified as the source of errors in Autocorrel I.). The result of the clustering was multiple alert groups that each have similar attributes.

Unlike other clustering algorithms like the *EM algorithm* [30] or SOMs [33], the autoassociator does not require knowledge of the number of output clusters in advance. It determines that through a self-optimisation process in the training algorithm. This is the main reason why we used the autoassociator in the first stage.

3.1.1 Feature Extraction

We extracted variables' information from the Snort alert. We did not use any information specific to Snort, so our selection of features can represent the alerts generated by any IDS. For instance, we did not use the Snort attack priority level or Snort's labelling of the attack because this information cannot be found in the raw IP packet.

The features extracted consist of the header information associated with the alert. To maximise correlation and to ensure that all the important factors of a possible attack are taken into consideration, as much information as possible is extracted from the alert content. In the end, we had 42 features that we passed to the autoassociator for classification. These features are listed in Table 1. Some attributes of the alerts were dropped for various reasons; for example, the source IP address was dropped because this may give some misleading clusters in cases where the IP address is spoofed; like in DoS attacks (for example). We also felt that the IP address attribute could dominate the alert clustering, when in fact we know that different alerts may originate from the same IP address. Early trials of our model also showed that the exclusion had no

Table 1: *Feature extraction for the first correlation step.*

Feature	Feature	Feature	Feature
portSrc	portDest	ipIsIcmpProtocol	ipIsIgmpProtocol
ipIsTcpProtocol	ipIsUdpProtocol	ipLen	ipDgmLen
ipId	ipTos	ipTtl	ipOptLsrr
ipPacketDefrag	ipReserveBit	ipMiniFrag	ipFragOffset
ipFragSize	icmpCode	icmpId	icmpSeq
icmpType	tcpFlag1	tcpFlag2	tcpFlagUrg
tcpFlagAck	tcpFlagPsh	tcpFlagRst	tcpFlagSyn
tcpFlagFin	tcpLen	tcpWinNum	tcpUrgPtr
tcpOptMss	tcpOptNopCount	tcpOptSackOk	tcpOptTs1
tcpOptTs2	tcpOptWs	tcpHeaderTrunc	udpLen

impact on the results and the remaining attributes were able to provide the required classification. In fact, the IP addresses were used to verify that the clustering was good. So it was our contention that the remaining variables should be able to identify and correlate any alert based on the remaining input variables. However, it should be noted that we did use IP source and destination addresses in the second correlation step.

3.1.2 Scaling Algorithms

ANN nodes perform nonlinear calculations which would result in loss of accuracy when the training data ranges are of significantly different magnitudes. It is therefore desirable to scale the input and output patterns to some smaller range [37]. The scaling described here is applicable to both stages of this work. We scaled the data using the common method of determining a linear map from the training data, then applying it to both the training data and the testing and evaluation data [38].

Specifically, for every feature in the data-set we determined the range of values for that set. For a given feature x_i, we called the highest value $high$ and the lowest value low. From these values we computed the linearly scaled value for x_i of a data item d_i as $(d_i - low)/(high - low)$, resulting in a linear scaling in the interval $[0, 1]$.

For IP addresses, for example, we know that the addresses are 32 bits by definition of the IPv4 header, so the values of the addresses are always in the range of encoded values $[0, 2^{32} - 1]$ [39]. We can assign $low = 0$ and $high = 2^{32} - 1$ and remove the step for determination of $high$ and low altogether when running the scaling algorithm, leaving the system with more predictable sets of values produced.

An alternative to this linear scaling is to do a Gaussian scaling of the data. To

compute the Gaussian scaling for a given feature x_i on a data item d_i, we first have to determine the mean μ and the standard deviation $\sqrt{\omega}$. We then used these values to compute the new value for d_i as $(d_i - \mu)/\sqrt{\omega}$, where the formula includes the unscaled values for d_i. This gives the training data a new mean of 0 and a new standard deviation of 1. The values of μ and $\sqrt{\omega}$ from the training set are used to scale the evaluation and testing sets.

3.1.3 Training the Autoassociator

An input vector $\mathbf{x}_i$, made up of alert TCP/IP information extracted as described in Section 3.1.1, is fed through an autoassociator through weights w_i. The objective is for the autoassociator to reproduce the vector $\mathbf{x}_i$. However, the reproduction is not perfect, and a reconstruction error is a measure of this imperfection. Similar attack scenarios have similar attributes, and we expect their reconstruction errors to be very close. Similar alerts are grouped together based on the reconstruction error. This idea is an extension of the work by Japkowicz *et al.* [16,26] on Novelty Detection. In that work, it was seen that the autoassociator was very good at grouping previously seen events together, discriminating them from novel events.

Based on the Novelty Detection approach by Japkowicz *et al* [25], a three layer, fully connected feedforward ANN with N input nodes, N output nodes and J hidden nodes was used. The output at node i of each layer is given by:

$$y_i = f(\sum_{k=1}^{K_i} w_{ik} y_k) \tag{16}$$

where y_i is the output of neuron i after receiving K_i signals from the neurons of the preceding layer, and $y_i = x_i$ for the input layer.

The network is trained using the error-backpropagation algorithm with the objective of reconstructing the input at the output. This algorithm has been successfully used in other intrusion detection research [40], and this is also the training algorithm used by Japkowicz *et al.* [25] in their Novelty Detection work. The training objective is to minimise the error function E, as given by:

$$E = \sum_{i=1}^{n} ||x_i - y_i||^2 \tag{17}$$

The ANN weights are iteratively updated until convergence is achieved. Once training has been completed, a threshold level is used to compare with the resultant RE e_i given by:

$$e_i = ||\mathbf{x}_i - \mathbf{y}_i|| \tag{18}$$

for each input vector $\mathbf{x}_i$ during ANN recall. This is illustrated in Fig. 6. Equation 18 essentially reduces a 42-dimensional vector into a 1-dimensional threshold metric e used for clustering. The result of the clustering is multiple alert groups that have similar attributes.

This heuristic is formally known as a *single-link clustering algorithm* [41] and it is applied to one-dimensional data — namely the reconstruction errors of the data. The clustering algorithm is known as a single-link algorithm because if the distance between any two data in a set is less than the threshold then those two data will appear in the same cluster.

3.2 Second Correlation Step

For this second correlation step shown in Figure 5, we took the output clusters of the previous stage and represented them each as new data items, each encoded using a new set of features. To facilitate the learning process, we constructed our features such that a cluster of alerts representing a single step of an attack would be similar to another cluster of alerts from the same attack.

By having a second step in our correlation system we hoped to be able to cluster each of the clusters produced by the first step to form *super-clusters*, or clusters of clusters of alerts–the first stage clusters are *sub-clusters* of the *super-clusters*. We did this because we hoped to link clusters from the previous step that are related, but that did not form one discrete cluster. Effectively, we hoped to be able to link different steps of an attack together by representing each step such that it can be correctly clustered with other steps from the same attack.

Our feature extraction and construction for this stage closely resembles work by other researchers in the area, in particular Dain and Cunningham [13]. We used these features in unsupervised training of clustering algorithms. The features are are as follows:

1. `ipSrcAddrCommonPart`: Attackers often perpetrate an attack from a single host, or from a single IP subnet. This feature indicates similarity between the source IP addresses of two alerts.

2. `ipDestAddrCommonPart`: Attackers often target a single host or subnet in their attacks [13]. Thus, we constructed a feature indicating the similarity of two destination IP addresses.

3. `ipSrcAddrCommonBits`: Similar to the work by Dain and Cunningham [13], we use a measure of closeness between two IP addresses as one of our attributes. This is applied to the source and destination IP addresses of alerts. The closeness was defined as the maximal number of most-significant bits shared between

two encoded IP addresses (called r). Thus, if the binary `and` operation is used on two IP addresses IP_1 and IP_2, and the result yields $b_1 b_1 \cdots b_{32}$, then

$$r = \sum_{i=1}^{32} b_i \tag{19}$$

According to Dain and Cunningham, "An attack scenario may contain components with spoofed source IP addresses while other components of the attack may use the attacker's real source IP."

4. `avgTimeSig` and `varTimeSig`: This features indicates the similarity in time between two alerts. In our model we have features to indicate the average time when a group of alerts was generated, and the standard deviation (named `varTimeSig`) for the times when a group of alerts were generated.

5. `avgReconsErr`: This feature indicates the average reconstruction error of a group of alerts. As we've established in the previous reports [1, 2], the reconstruction errors of alerts tend to correspond directly with their type. This value is drawn from the autoassociator in the first stage.

We also experimented with some other features that other researchers like Dain and Cunningham didn't consider. These are as follows:

1. `modePortSrc` and `modePortDest`: We found that using the TCP source and destination ports was a strong indicator in determining the grouping of a set of alerts. We also found that when the ports were the dominant variables, there was almost always a particular source or destination port that was more common than the rest. Therefore, we created two features: one to encode the most common TCP source port in a cluster of alerts, and one to encode the most common destination port.

2. `avgSeqNumDiff`: We also found that TCP sequence and acknowledgement numbers are sometimes good predictors of the use of a hacker tool. Often there are obvious patterns in a group of sequence or acknowledgement numbers, and this pattern can usually be identified by taking the difference of the two numbers.

3.3 The Data Sources

Our data was obtained in two ways. We downloaded Snort [19] alerts directly from `incidents.org` [42]. We also used labelled alerts from the 1999 Defense Advanced Research Projects Agency (DARPA) [18] IDS evaluation data. Since the labelled DARPA data was in packet form, we ran the data through Snort using the commonly used configuration filters. We developed some Perl [43] scripts to read the text-based Snort alerts into numeric data for use with our machine-learning algorithms.

In these data sets of alerts, we reserved 10 000 alerts for training and a separate set of 1 000 alerts for evaluation and testing. These data sets offer the IP traffic as seen by single or multiple homogeneous sensors. Alerts from heterogeneous sensors need to be handled slightly differently. We chose not to go into this at this time.

It should also be noted that in our work, we paid more attention to the accuracy of our results with the `incidents.org` data set because this represented a real alert data set. Alerts from `incidents.org` were found "in the wild" and represent real attack patterns as opposed to the DARPA data set which was obtained from a simulated network. As will be seen later, more interesting and meaningful correlations were achieved with the `incidents.org` data set.

4 Results Analysis

In this section, we present the implementation of our model. We start by presenting the performance evaluation metrics. This is followed by the experiments we carried out to select parameters and algorithms. Finally, we present sample results from the implementation of our approach on two data sets.

4.1 Performance Evaluation

In this work, we use a number of methods and metrics to evaluate the system's performance. Like in the work by Dain and Cunningham [13], we use a manually constructed data set, the *gold standard*, to evaluate our system. We also define experimentation effectiveness measures to show the performance of the system relative to the *gold standard*.

4.1.1 Gold Standard for Performance

We manually created a *gold standard* to dictate the type of results we want to see produced automatically by our system. When creating the gold standard, we tried to be consistent to the notion that one *super-cluster* – a cluster produced by the second correlation step of our system: a cluster of clusters – should represent one attack attempt against the network. The gold standard is only for testing system performance. It is not required for the system to work.

We draw the gold standard from the data sets described earlier, i.e. from the `incidents.org` and the 1999 DARPA data sets. The 500 alerts used in the gold standard are the first half of the subset of 1000 alerts reserved for evaluation and testing from the start of the data set. These 500 alerts are manually organised into clusters based on our knowledge and experience.

4.1.2 Experimentation Effectiveness Measures

Since this is an experiment, errors are inevitable. To understand and analyse the outcome of our experiments, we have used basic performance measures to characterise the effectiveness of the system.

We counted the number of errors we made by counting the number of alerts which were correctly clustered versus the number of alerts which were incorrectly clustered for a sample of test data. We use the gold standard from Section 4.1.1 to determine which alerts are errors. The performance measures we used in this work are as follows:

1. *separation errors (SE)* occur when a distinct group of alerts should belong to a larger group of related alerts, but isn't clustered with the larger group. For instance, if we have a cluster A of 10 `nmap scan` alerts and a separate cluster B of 3 `nmap scan` alerts that are related to cluster A, then we count 3 separation errors because the 3 alerts in B should have been grouped with the 10 alerts in A. This implies that the analyst will have more work to do.

2. *clustering errors (CE)* occur when two unrelated alerts are clustered together. For instance, if we have a mixed cluster of 10 `nmap` scans and 5 `Telnet Access` alerts where the alerts of the two types in the cluster are obviously not related, we count 5 clustering errors. This type of error indicates the problem of the system finding correlation where there is none.

3. *total number of errors (TE)* represent the total number of alerts erroneously placed into clusters where they do not belong.

$$TE = CE + SE \tag{20}$$

Obviously CEs are more serious errors than SEs because they may cause an IDS analyst to miss important events.

4.2 Experiments

In this section, we describe how we carried out experiments to determine the best attribute scaling model and cluster barrier size (the predetermined threshold described in Section 3.1) for the first stage as well as the best algorithm for the second stage. We also experimented on the parameters to most effectively train this model.

4.2.1 Data Scaling and Barrier Selection

In our previous work, with Autocorrel I [2], we used a linear scaling algorithm to scale features to the [0,1] range. Varying the cluster barriers produced different error levels. In Figure 7, we show the errors produced in the Autocorrel I system as we varied the cluster barrier. This shows that the best cluster barrier to use would be 0.0017. This is very close to the value of 0.025 used in the Autocorrel I system [2].

In this work, we experimented with different data scaling approaches. Our objective was to have a rough idea as to which scaling data approach to use. At the same time, we also determined the best cluster barrier to use in our model. Figure 8 shows a number of experiments conducted to determine the best cluster barrier to use with the autoassociator in the first stage for a given scaling range.

In the scaling process, we either used the training data set's lowest and highest values or we used predetermined attribute ranges. The predetermined attribute ranges were

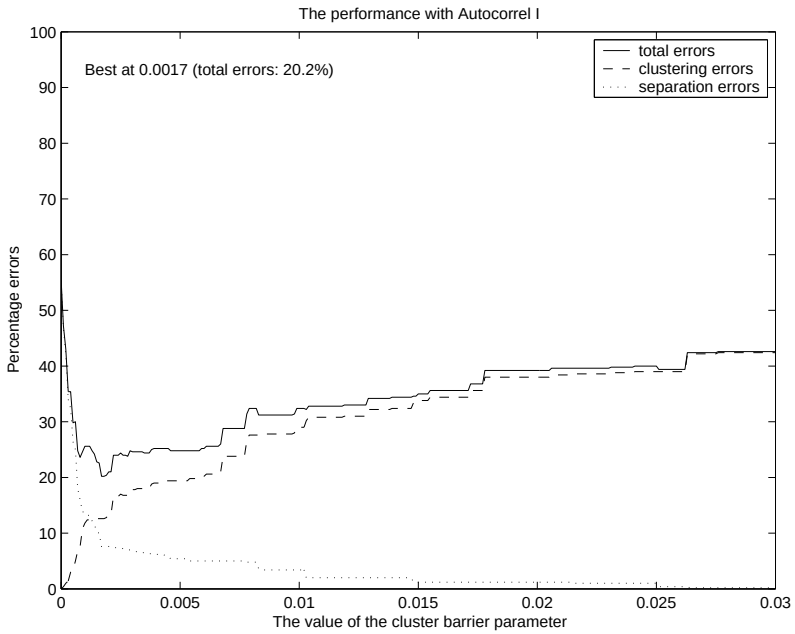


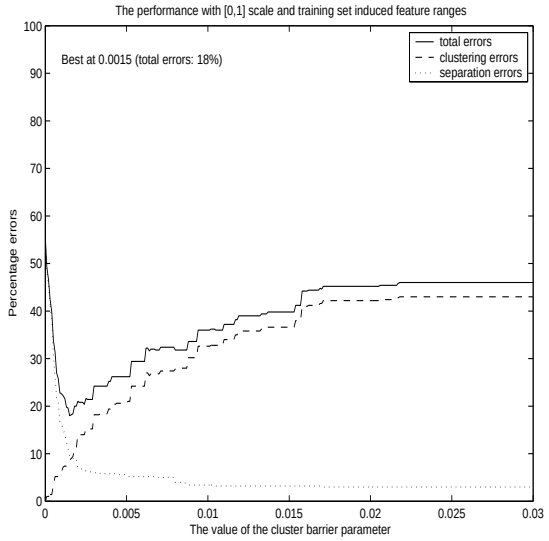
Figure 7: *The performance of Autocorrel I system [2], varying the cluster barrier parameter*

obtained from the theoretical knowledge of the possible ranges of the attribute values. For example, the TCP port numbers can only range from 0 to 65 535, so the input attribute range of $[0, 65\,535]$ was used to scale the data. In contrast, the training data set may only have values ranging from 20 to 22 000, for example. We set the output of the scaling to be either $[0, 1]$ or $[-1, 1]$.

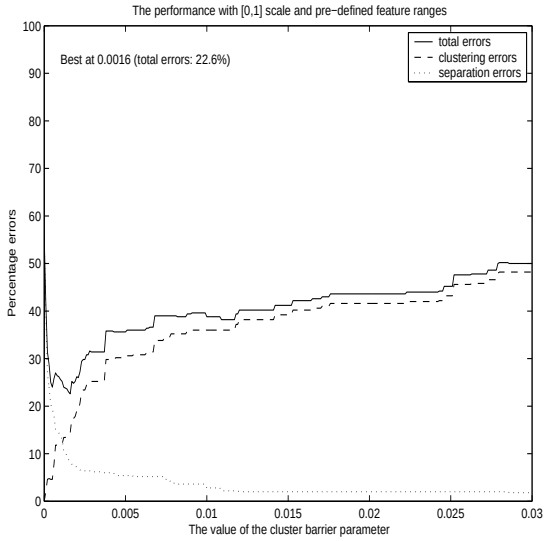
From the two scaling ranges, we chose $[-1, 1]$. Experiments shown in Figures 8(c) and 8(d) have lower error values than experiments shown in Figures 8(a) and 8(b). It is also important to note that the range $[-1, 1]$ gives the ANN more input option ranges than the $[0, 1]$ scale.

Between the scaling methods shown in Figures 8(c) and 8(d), we chose the predefined scaling range shown in Figure 8(d). Although experiments shown in figures 8(c) and 8(d) are nearly the same, the experiment shown on Figure 8(d) has the lowest error value. Figure 8(d) also shows the best clustering barrier of 0.0027–which is very close to what was recommended in Figure 8(c). Choosing experiments of Figure 8(d) over 8(c) also removes the possibility of handling input data lying outside the training data set boundaries. This would produce unpredictable errors.

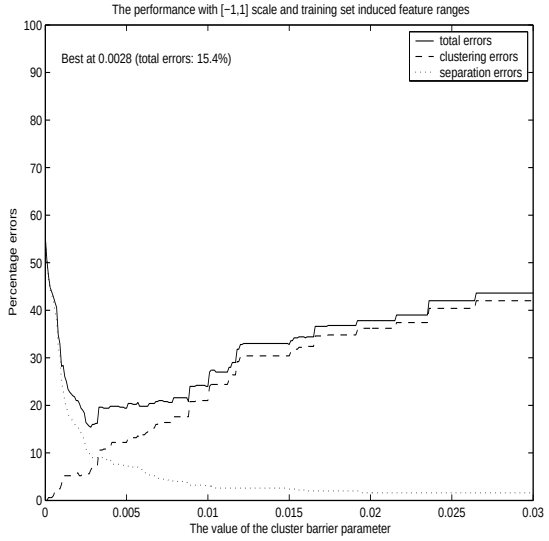
We also performed an additional experiment using the Gaussian scaling method. This is shown in Figure 9. The results are not as good as the ones from experiments reported in figures 8(c) and 8(d). The error level is worse than the other cases. It



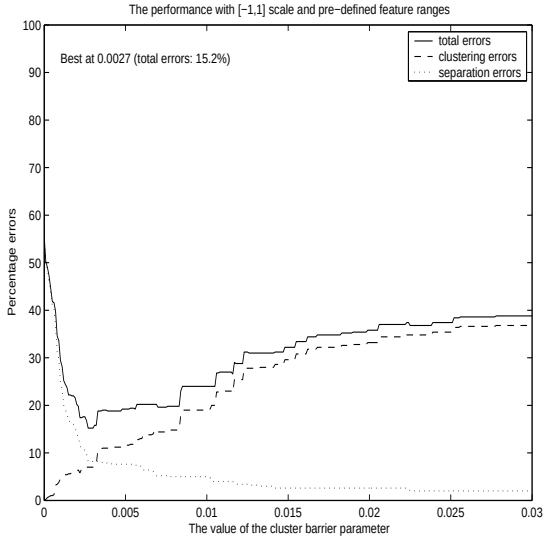
(a) Scale in $[0, 1]$ using training set to determine ranges.



(b) Scale in $[0, 1]$ using predefined attribute ranges.



(c) Scale in $[-1, 1]$ using training set to determine ranges.



(d) Scale in $[-1, 1]$ using predefined attribute ranges.

Figure 8: *Experiments to show how scaling method and clustering barriers were chosen.*

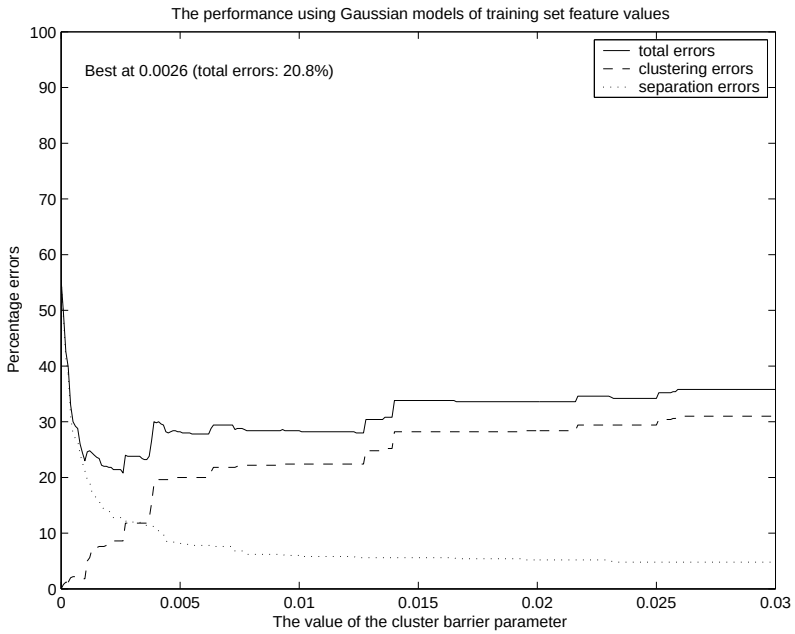


Figure 9: *Experiments to show how the Gaussian scaling method compares with the linear scaling methods.*

seems that the overall performance of the Gaussian scaling method is less affected by changes in cluster barrier sizes. However, in our model, we do not vary the cluster barrier after the initial selection. So, this approach has no advantages over the approach shown in Figure 8(d).

Since we were most concerned with the accuracy of our model, we decided to go with the method that produces the smallest error rate. We therefore chose the linear scaling in the interval $[-1, 1]$ with a cluster barrier of 0.0027.

4.2.2 Parameter and Algorithm Exploration

In this set of experiments, we show how we arrived at some of the training parameters that were used in this work. We varied two autoassociator parameters described in Section 3.1: training epochs and number of hidden nodes. We also examined three candidate clustering algorithms to determine which gave the best performance.

To compare the performance of the various modifications of our system, we took 100-consecutive alert windows from both the 1999 DARPA data set [18] and the `incidents.org` data set [42]. For easy error comparison, we took these 100 alerts from the gold standard that we created earlier.

This parameter exploration was intended to give guidance as to the parameters that

would give the best results in the given experimentation environment. As a result, we compared the output of our system against the gold standard for predetermined numbers of hidden nodes, namely 8, 16, 32, and 64. Other numbers tried but not reported include 20, 28, 40, 42 and 50. These were not reported because they did not produce significantly different results from the other four.

We also decided to predetermine the number of training epochs. As ANNs become more trained, they become more capable of recognising the particular data on which they are being trained. One notable pitfall of the training process is that if the neural network is trained for too many epochs, then *overfitting* may occur [38][1]. First, we trained an ANN until we achieved acceptable MSE values (initially set to the original cluster barrier value of 0.0025). Then, based on this successful training, we examined three candidate epoch values, namely 500, 2 500, and 5 000. In the SOM, we used a lattice (grid) map of 4×6.

We separately compared the results of clustering the evaluation data sets of 100 alerts each using a trained autoassociator and three different clustering algorithms: the single-link heuristic algorithm we developed for Autocorrel I, the EM algorithm, and self-organizing maps. In tables 2 to 4, we list the TE, CE, and SE.

Table 2: *Results of the autoassociator and the single-link algorithm*

Data Source	Hidden Nodes	Epochs=500			Epochs=2500			Epochs=5000		
		TE	CE	SE	TE	CE	SE	TE	CE	SE
incidents.org	8	29	8	21	37	3	34	37	3	34
	16	47	8	39	48	8	40	47	6	41
	32	42	2	40	43	1	42	38	0	38
	64	40	0	40	40	1	39	43	5	38
DARPA	8	52	6	46	52	0	52	52	4	48
	16	52	2	50	50	5	45	48	1	47
	32	51	4	47	50	2	48	51	0	51
	64	48	0	48	50	0	50	50	0	50

As previously noted, in our evaluation of this data, we were more concerned about good results for the incidents.org data than for the DARPA data. It will also be noticed in our results that the clustering accuracy for the DARPA data is lower. We attribute this to fact that this is simulated attack data which does not represent the same variability and correlations as with real attack data found "in the wild".

The results from tables 2 to 4 show that the lowest TE achieved was 28 from the SOM with 32 hidden nodes trained for 2 500 and 5 000 epochs. Since we regard CE as more

[1] An overfitted ANN is a neural network that has been trained for more epochs than it should have for optimal performance, and is unable to generalise.

Table 3: *Results of the autoassociator and the EM algorithm*

Data Source	Hidden Nodes	Epochs=500			Epochs=2500			Epochs=5000		
		TE	CE	SE	TE	CE	SE	TE	CE	SE
incidents.org	8	32	4	28	39	3	36	43	2	41
	16	44	0	44	44	0	44	44	0	44
	32	39	2	37	40	0	40	46	2	44
	64	39	2	37	43	1	42	38	1	37
DARPA	8	44	3	41	61	0	61	62	3	59
	16	63	4	59	43	3	40	43	3	40
	32	44	8	36	51	4	47	60	3	57
	64	65	3	62	45	3	42	64	3	61

Table 4: *Results of the autoassociator and the SOM*

Data Source	Hidden Nodes	Epochs=500			Epochs=2500			Epochs=5000		
		TE	CE	SE	TE	CE	SE	TE	CE	SE
incidents.org	8	34	6	28	33	4	29	31	3	28
	16	33	4	29	33	4	29	34	4	30
	32	29	4	25	28	2	26	28	5	23
	64	35	4	31	30	4	26	30	4	26
DARPA	8	62	4	58	61	4	57	57	7	50
	16	61	3	58	61	2	59	59	3	56
	32	58	6	52	60	9	51	59	2	57
	64	60	9	51	58	6	52	58	5	53

harmful than SE, we concluded that the best system performance in this experiment would be attained by the SOM maps with an autoassociator with 32 hidden nodes trained for 2 500 epochs.

Table 5: *Clustering algorithm average errors*

Data Source	Clustering Algorithm	Average Errors TE	CE	SE
incidents.org	Single-link	40.9 (*28.8*)	3.8	37.2
	EM	40.9 (*14.8*)	1.4	39.5
	SOM	31.5 (*6.1*)	4	27.5
DARPA	Single-link	50.5 (*2.1*)	2	48.5
	EM	53.8 (*89.3*)	3.3	50.4
	SOM	59.5 (*2.5*)	5	54.5

To further analyse the effectiveness of the three clustering algorithms, we considered the averages of TE and CE for tables 2, 3, and 4. These averages are shown in Table 5. The values in *italics* are the variance measures of the total errors. While the SOM has the lowest TE, the EM algorithm produces the lowest average CE. The single-link algorithm preformed much better for an autoassociator with 32 or 64 hidden units. Since the CE are more critical than SE, we therefore decided to use the single-link algorithm (which is the same model as AutoCorrel I) in the first stage and use the EM algorithm in the second stage[2].

4.3 Sample Results

The model was tested with unlabelled alerts from `www.incidents.org` as well as labeled alerts from the 1999 DARPA IDS evaluation set. In each case, 10 000 alerts were used for training.

For the first stage, an autoassociator with 42 inputs, 32 hidden layers and 42 outputs was trained, using the error backpropagation algorithm with a training constant η of 0.4. Training was initially fixed to 500 epochs, but could be changed if desired. The data was then passed onto the EM algorithm in the second stage, and clusters were produced.

We loaded 500 alerts from the `incidents.org` data set first. Using the EM algorithm implemented in Weka as the second stage clustering algorithm, we were able to cluster the data into 18 clusters. In Figure 10, we show a screen-shot of the Weka window that produced these clusters. The clusters can be distinguished by the different colours of

[2]It should be noted that the only evaluation done for the first stage was the cluster barrier, number of training epochs and scaling range (which is also applicable to the second stage).

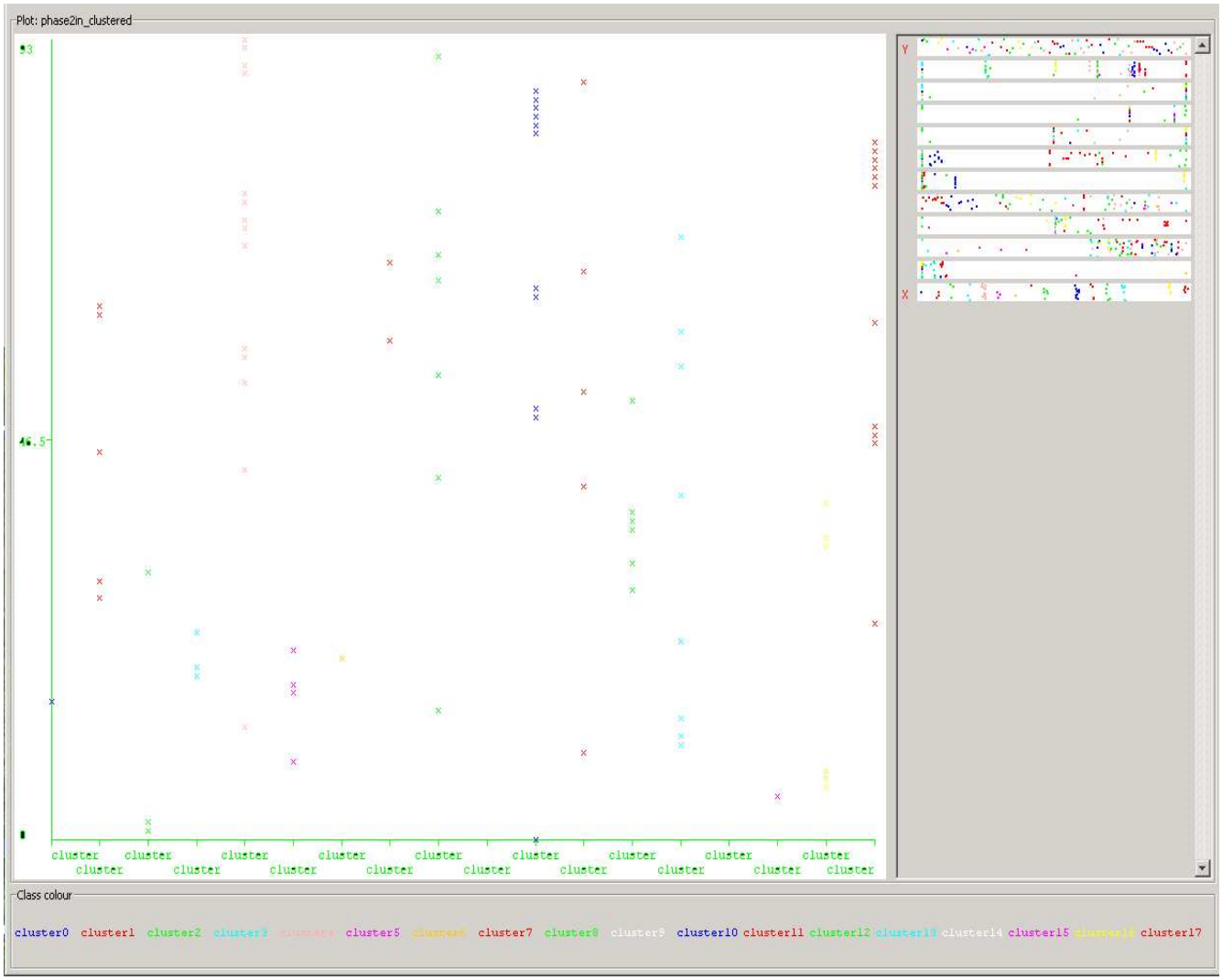


Figure 10: *A Weka screen shot showing the alert instance on the y-axis and the clusters on the x-axis.*

the individual alerts and the key at the bottom. Some of the colours are very similar, and therefore difficult to distinguish[3]. In addition, Weka seems to merge data points that are similar into one point. That explains why the number of alert instances seems to be less than the 500 alerts that were tested.

To carry out the analysis in more detail, we list a sample of the `incidents.org` clustered alerts in Table 6. The rest of the clustered alerts are listed in Annex C. The sample is from the first of the 18 clusters produced. Within this cluster there are three sub-clusters, each of which was output from stage 1. The printout from our

Table 6: *A sample of cluster 1 alerts produced by this model.*

```
Supercluster1/18
------------------

Cluster1/3 (sc:  1)
-------------------

[**][1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
AttemptedInformation Leak] [Priority:  2] 11/16-18:16:20.416507
206.48.61.152:2359-> 170.129.108.46:8080 TCP TTL:113 TOS:0x0
ID:31456IpLen:20 DgmLen:48 DF
******S*Seq:  0x1439203 Ack:  0x0 Win:  0x2000 TcpLen:  28
TCPOptions (4) => MSS: 536 NOP NOP SackOK

[**][1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
AttemptedInformation Leak] [Priority:  2] 11/16-18:16:23.436507
206.48.61.152:2359-> 170.129.108.46:8080 TCP TTL:113 TOS:0x0
ID:33248IpLen:20 DgmLen:48 DF
******S*Seq:  0x1439203 Ack:  0x0 Win:  0x2000 TcpLen:  28
TCPOptions (4) => MSS: 536 NOP NOP SackOK

[**][1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
AttemptedInformation Leak] [Priority:  2] 11/16-13:34:38.646507
206.48.61.152:2234-> 170.129.89.189:8080 TCP TTL:113 TOS:0x0
ID:29481IpLen:20 DgmLen:48 DF
******S*Seq:  0x419789 Ack:  0x0 Win:  0x2000 TcpLen:  28
TCPOptions (4) => MSS: 536 NOP NOP SackOK

....

Cluster2/3 (sc:  1)
-------------------

[**][1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
AttemptedInformation Leak] [Priority:  2] 11/15-18:54:31.966507
204.188.170.90:4175-> 170.129.152.15:8080 TCP TTL:113 TOS:0x0
ID:52708IpLen:20 DgmLen:48 DF
******S*Seq:  0x1CF3682 Ack:  0x0 Win:  0x2000 TcpLen:  28
TCPOptions (4) => MSS: 536 NOP NOP SackOK

Cluster3/3 (sc:  1)
-------------------

[**][1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
AttemptedInformation Leak] [Priority:  2] 11/16-12:59:08.856507
206.48.61.152:3109-> 170.129.132.70:8080 TCP TTL:113 TOS:0x0
ID:63760IpLen:20 DgmLen:48 DF
******S*Seq:  0x211675 Ack:  0x0 Win:  0x2000 TcpLen:  28
TCPOptions (4) => MSS: 536 NOP NOP SackOK
```

model shows `Supercluster 1/18`, meaning that this is cluster 1 of 18 super-clusters. The next line shows `Cluster 1/3 (sc:1)`, meaning that within this super-cluster this is cluster 1 of 3; `sc:1` reminds us that we are still in super-cluster 1.

The results on Table 6 are an example of the `Proxy Port Scan`. A comparison with the gold standard shows that all these alerts belong to the same cluster. In this

[3]Unfortunately, Weka does not have the option to reconfigure these screen shots.

cluster, there are no alerts that do not belong to the `Proxy Port Scan` group; thus $CE = 0\%$.

A summary of the results is shown in Table 7. Detailed results of all the alert clusters summarised here are listed in Annex C. We compared the output of our system with

Table 7: *System-produced clusters for the* `incidents.org` *data set.*

System-Produced Clusters	Cluster Description	Gold Standard Clusters												
		Proxy Port Scan	HTTP Attack	Backdoor Q Access	Malformed Packets	Shellcode x86/x90	TCP Port 0	Tiny Fragments	TCP nmap SCAN	IP Reserved bit	P2P Gnutella	Low Source Port	Land Attack	Error *CE*
1	Scan Proxy Port	[12]	0	0	0	0	0	0	0	0	0	0	0	0%
2	HTTP Attack	0	**8**	0	0	0	0	0	0	0	0	0	0	0%
3	Backdoor Q Access	0	0	**81**	0	0	0	0	0	0	0	0	0	0%
4	Malformed Packet	0	0	0	**7**	0	0	0	1	0	0	0	0	12.5%
5	Scan Proxy Port	[2]	0	0	0	0	0	0	0	0	0	0	0	0%
6	Shell code x86	0	3	0	0	8	0	0	0	0	0	0	0	27.3%
7	Shell code x86	0	0	0	0	0	[2]	0	0	0	0	0	0	0%
8	TCP Port 0	[5]	4	0	0	5	**157**	0	0	0	0	0	0	6%
9	Malformed Packets	0	0	0	[2]	0	0	[1]	0	0	0	0	0	33.3%
10	Shell code x86	0	0	0	0	**34**	0	0	0	0	2	0	0	5.6%
11	TCP nmap Scan	0	0	0	0	0	0	0	**99**	0	0	0	0	0%
12	Low Source Port	0	0	0	1	0	0	0	0	0	0	1	0	50%
13	Shell code x86	0	0	0	0	[1]	0	0	0	0	0	0	0	0%
14	Malformed Packet	0	0	0	[1]	0	0	0	0	0	0	0	0	0%
15	Scan Proxy Port	[2]	0	0	0	0	0	0	0	0	0	0	0	0%
16	IP Reserved Bit	0	0	0	0	0	0	0	0	**11**	0	0	0	0%
	Land Attack	0	0	0	0	0	0	0	0	0	0	0	**34**	0%
17	Scan Proxy Port	**13**	0	0	0	0	0	0	0	0	0	0	0	0%
18	Malformed Packets	0	0	0	[2]	0	0	0	0	0	0	0	0	0%
Error(SE)		61.7%	46.7%	0%	46.1%	29.1%	1.3%	0%	0%	0%	0%	0%	0%	

the gold standard clusters. It should be noted that the clusters produced by our system are not in the same order as the gold standard clusters.

In Figure 7, the numbers in boldface represent the number of machine produced alerts which correspond to the gold standard. The boxed numbers represent the alerts that have been erroneously separated from the main clusters, but they individually occupy sub-clusters of their own.

Although some clusters do not match the gold standard, they constituted clusters of their own. So, if there were no dissimilar alerts in these clusters, we associated a CE

of 0% to the clusters. However, the errors associated with these clusters are reflected in the corresponding SE, since they are clearly separated from the main clusters of their type. Examples of these are clusters 1, 5, 8, and 15 as shown in Table 7.

In all cases, whenever there were two or more clusters representing the same gold standard attack type, we chose the cluster with the highest number of alerts to represent that cluster group. Thus, we chose cluster 17 to represent the `Proxy Port Scan` cluster over cluster 1. We also "separated" some clusters which had two or more significant alert groupings in sub-clusters of their own. For example cluster 16 was split up into two as shown in Table 7. A sample of these alerts is shown in Table 8. The cluster contains two sub-clusters of two distinct attack types. Although

Table 8: *Sample of cluster 16 alerts.*

```
...
Cluster1/2 (sc:  16)
-------------------

[**][1:523:4] BAD-TRAFFIC ip reserved bit set [**]
[Classification:Misc activity] [Priority:  3] 11/14-23:28:20.656507
200.200.200.1-> 170.129.53.47 TCP TTL:241 TOS:0x0 ID:0 IpLen:20
DgmLen:40RB Frag Offset:  0x0864 Frag Size:  0x0014

[**][1:523:4] BAD-TRAFFIC ip reserved bit set [**] [Classification:
Miscactivity] [Priority:  3] 11/15-01:09:54.346507 200.200.200.1 ->
170.129.217.111TCP TTL:241 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB Frag
Offset:0x0864 Frag Size:  0x0014

[**][1:523:4] BAD-TRAFFIC ip reserved bit set [**] [Classification:
Miscactivity] [Priority:  3] 11/15-01:21:09.846507 200.200.200.1 ->
170.129.127.227TCP TTL:241 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB Frag
Offset:0x0864 Frag Size:  0x0014
...
Cluster2/2 (sc:  16)
-------------------

[**][1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
PotentiallyBad Traffic] [Priority:  2] 11/14-22:36:45.306507
170.129.215.99-> 170.129.215.99 IGMP TTL:47 TOS:0x0 ID:0 IpLen:20
DgmLen:28

[**][1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
PotentiallyBad Traffic] [Priority:  2] 11/14-22:36:45.306507
170.129.215.104-> 170.129.215.104 IGMP TTL:47 TOS:0x0 ID:0 IpLen:20
DgmLen:28
...
```

they are clearly related (they are all targeting the same `170.129.x.y` addresses), they represent two different modes of attacks and separating them this way would be beneficial to the analyst. On the other hand, the sub-cluster `1/2` could be the first stages of a denial of service (DoS) *land attack* represented by sub-cluster `2/2`, in which case, separating them would provide the analyst with less information. In cases like these, it would be best to leave such decisions to the analyst.

We therefore concluded that from the 18 system-produced clusters, 9 matched the gold standard. However, the system failed to classify `Tiny Fragments`, `P2P Gnutella`,

and `Low source port` alerts into their own individual clusters. Although the failure proportion is low (25%), this is the type of error that an analyst would want to avoid. The alerts themselves are hidden inside other clusters, and an analyst can easily miss them as a result.

We can see that the CEs for the system-produced clusters range from $0 - 50\%$. The 50% in cluster 12 is not necessarily statistically significant since there are only two alerts in this cluster. Only 18 (3.6%) alerts were placed completely erroneously. However, if we consider all the alerts that did not fall into any of the 9 matched clusters, we have a total of 56 erroneously placed alerts. This corresponds to a TE of 11.2%.

Similarly, the separation errors produced for this data set range from $0 - 61.7\%$. The worst case is `Proxy Port Scan` cluster. However, in each one of the separated clusters, our system was able to distinguish the alerts as unique and put them into their own cluster (as in cluster 15 and 17) or sub-cluster (as in clusters 5 and 8). This can easily be fixed manually.

We also carried out a similar simulation with DARPA data. The results of this simulation are summarised in Table 9. In this case the CE varied from $0 - 33\%$. In this data set, the system managed to produce 11 clusters out of a possible 12. The only exception was that it also produced as a sub-cluster of cluster 16. This is the only case of a complete CE in this data set. However, most of the errors are SEs. There were a total of 66 SEs. This corresponds to a TE of 13.2%; this is the same TE error range as for the `incidents.org` data set. It should also be noted that all the SEs in this data set were also individual sub-clusters. Although these sub-clusters were small, their existence as sub-clusters or clusters is an aid to any human intervention that may be required.

In comparison, our system performed better on the labelled DARPA alerts than it did on the `incidents.org` alerts. It is also important to note that absence of significant CEs in the DARPA data set results is a major achievement of this approach which we would like to emphasise. Our algorithm was able to achieve its goals with an SE percentage of less than 14%.

Clearly our system performs better than our earlier model, AutoCorrel I. The improvements came from expanding the model to two stages. Our new system also found a way around the 42-1 mapping limitation of AutoCorrel I by using the reconstruction error and other original alert attributes in the final stage of the correlation. However, separation errors are still significant. The only immediate solution to that at the moment is to have human intervention associate these "lost" clusters with one another.

Table 9: *System-produced clusters for the DARPA data set.*

System-Produced Clusters	Cluster Description	Gold Standard Clusters												
		Apache dir. disclosure	SNMP access	Tiny Fragments	telnet login incorrect	telnet access 2	CGI redirect	CGI calendar	Web /doc access	IIS register.asp	CGI count.cgi	Web 403 forbidden	Web search.dll	Error *CE*
1	telnet access	0	0	0	0	[1]	0	0	0	0	0	0	0	0%
2	Apache dir.disclosure	**74**	0	0	0	0	0	0	0	0	0	0	0	0%
3	telnet access	0	0	0	0	0	[1]	0	0	0	0	0	0	0%
4	telnet login incorrect	0	0	0	**2**	0	0	0	0	0	0	0	0	0%
5	telnet access	0	0	0	0	[1]	0	0	0	0	0	0	0	0%
6	telnet access	0	0	0	0	[2]	0	0	0	0	0	0	0	0%
7	SNMP access	0	[6]	0	0	0	0	0	0	0	0	0	0	0%
8	Web 403 forbidden	0	0	0	0	0	[1]	0	0	0	0	0	0	0%
9	telnet access	0	0	0	0	[1]	0	0	0	0	0	0	0	0%
10	Tiny Fragments	0	0	**225**	0	0	0	0	0	0	0	0	0	0%
11	SNMP access	0	**124**	0	0	0	0	0	0	0	0	0	0	0%
12	SNMP access	0	[22]	0	0	0	0	0	0	0	0	0	0	0%
13	SNMP access	0	[24]	0	0	0	0	0	0	0	0	0	0	0%
14	Web search.dll	0	0	0	0	0	0	0	0	0	0	0	**2**	0%
15	Web /doc access	0	0	0	0	0	0	0	**1**	0	0	0	0	0%
16	IIS register.asp	0	0	0	0	0	0	0	0	**2**	[1]	0	0	33%
17	Web 403 forbidden	0	0	0	0	0	0	0	0	0	0	**1**	0	0%
18	CGI calendar	0	0	0	0	0	0	**1**	0	0	0	0	0	0%
19	Web 403 forbidden	0	0	0	0	0	[1]	0	0	0	0	0	0	0%
20	CGI redirect	0	0	0	0	0	**1**	0	0	0	0	0	0	0%
21	telnet access	0	0	0	0	**6**	0	0	0	0	0	0	0	0%
Error (*SE*)		0%	29.5%	0%	0%	45.4%	75%	0%	0%	0%	100%	0%	0%	10%

5 Discussion and Conclusions

In this work, we successfully designed and implemented a two-stage alert correlation model using an autoassociator and the Expectation–Maximisation (EM) algorithm. We demonstrated how our model was able to cluster similar alerts with better accuracy than what we achieved with our earlier model, Autocorrel I. With this model, the number of alerts that an analyst has to deal with is significantly reduced.

Like Autocorrel I, our approach capitalises on the ability of artificial neural network (ANN)s to learn through self-optimisation based on given training examples. To improve the performance and errors encountered with Autocorrel I, we added a stage that implements another machine learning clustering algorithm. We reported our investigations into the use of different clustering techniques. We showed that for this type of work, the EM algorithm performs better than the self-organising maps (SOM) and the single-link clustering algorithms. Our results show that this new model architecture achieved much better performance than Autocorrel I–with a clustering accuracy of over 86%.

We successfully tested this approach on unlabelled alerts from `incidents.org`. With an accuracy of over 86%, we were able to cluster 500 alerts into 18 clusters. We also successfully tested the approach with a labelled data-set from the 1999 DARPA IDS evaluation data-set. In this case, we were able to accurately cluster 500 alerts into 21 clusters. The accuracy of the results was impressive in both cases. We achieved an accuracy of over 86% in each case. Although the number of clustering errors (CE)s is very low (less than 5% in each of the tested case), these are errors which can result in important missed calls by an analyst, so it would be good to find a way to reduce these errors even further. The number of separation errors (SE)s is very small as well, and very manageable through human intervention to ensure that the straying clusters and sub-clusters are associated with the right clusters.

5.1 Future Work

While no future work is currently planned in this area, there are a few things that could be worked on to improve what we have achieved here.

The results show that the addition of the second correlation stage significantly reduced the number of CEs. However, the same cannot be said about SEs. Although the total number of errors have significantly gone down, some additional thought needs to be put in to further reduce the SEs. It may be worthwhile to investigate using this approach with other non-machine learning methods. Perhaps adding a supervised machine training algorithm could also improve the performance.

The number of SEs, though small, means that human intervention is required to

ensure completely accurate clustering. Future work in this area should also investigate the possibility of reading the output from this approach and reorganising it into error-free clusters that could be used in day-to-day intrusion detection system (IDS) analyses. Further work may also include the coupling of Autocorrel II with good visualisation techniques to provide an easy-to-use tool for clustering alerts.

The current design of this model is such that it can only directly handle Snort-based alerts. Alerts generated by other sensors have to be transformed to be compatible with this model. In fact, if the other sensor does not present all the attributes used by our model, the results are unpredictable, if not outright wrong. For sensors that log the actual offending packets, but don't provide enough attribute data in their logs, this approach would still be applicable by running the packets through Snort first. Future work could expand AutoCorrel II to directly handle inputs from multiple heterogeneous sensors.

References

[1] Dondo, Maxwell, Japkowicz, Nathalie, and Smith, Reuben (2005), Autocorrel I: A Neural Network Based Network Event Correlation Approach, (DRDC Ottawa TM 2005-193) Defence R&D Canada-Ottawa.

[2] Japkowicz, Nathalie and Smith, Reuben (2005), Autocorrel I: A Neural Network Based Network Event Correlation Approach, (DRDC Ottawa CR 2005-030) Defence R&D Canada-Ottawa.

[3] SANS Institute (2001), Shadow, *SANS Institute*. Available on-line at http://www.nswc.navy.mil/ISSEC/CID/.

[4] Southcott Patrick (2002), Snort & Acid, *Online*.

[5] Haines, Joshua, Ryder, Dorene K., Tinnel, Laura, and Taylor, Stephen (2003), Intrusion Alert Correlation: Validation of Sensor alert Correlations, *IEEE Security & Privacy*, pp. 46–56.

[6] Valdes, Alfonso and Skinner, Keith (2001), Probabilistic Alert Correlation, In *RAID 2001, LNCS 2212*, pp. 54–68, Springer-Verlag.

[7] Lunt, T. F. (1993), A survey of intrusion detection techniques, *Computers & Security*, 4(12), 405–418.

[8] Ning, Peng and Cui, Yun (2002), An Intrusion Alert Correlator Based on Prerequisites of Intrusions, *Department of Computer Science, North Carolina State University*.

[9] Antti Hätälä, Camillo Särs, Addams-Moring, Ronja, and Virtanen, Teemupekka (2004), Event Data Exchange and Intrusion Alert Correlation in Heterogeneous Networks, In *Proceedings of the 8th Colloquium for Information Systems Security Education (CISSE)*, pp. 84–92, Westpoint, NY: CISSE.

[10] Debar, H., Curry, D., and Feinstein, B. (2004), The Intrusion Detection Message Exchange Format, *IETF Working Group*.

[11] Debar, Hervé and Wespi, Andreas (2001), Aggregation and Correlation of Intrusion-Detection Alerts, In *RAID '00: Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection*, pp. 85–103, Springer-Verlag.

[12] Julisch, Klaus and Dacier, Marc (2002), Mining Intrusion Detection Alarms for Actionable Knowledge, In *Proceedings of SIGKDD '02, the 8th International Conference on Knowledge Discovery and Data Mining*, pp. 366–375, Edmonton, Alberta, Canada: ACM.

[13] Dain, Oliver and Cunningham, Robert K. (2001), Fusing a Heterogeneous Alert Stream into Scenarios, In *Proceedings of the 2001 ACM Workshop on Data Mining for Security Applications*, pp. 1–13, Philadelphia, PA.

[14] The DEFCON Data Set (online), defcon.org, http://www.defcon.org/ (Access Date: Mar. 14, 2004).

[15] Northcutt, Stephen and Novak, Judy (2000), Network Intrusion Detection : An Analyst's Handbook, 2 ed, Indianapolis, Indiana: New Riders.

[16] Japkowicz, N. (2001), Supervised versus Unsupervised Binary-Learning by Feedforward Neural Networks, *Machine Learning*, 42(1/2), 97–122.

[17] Northcutt, Stephen (1999), Network Intrusion Detection: An Analyst's Handbook, Indianapolis, IN: New Riders Publishing.

[18] Lippmann, Robert, Haines, Joshua W., Fried, David J., Korba, Jonathan, and Das, Kumar (2000), The 1999 DARPA Off-Line Intrusion Detection Evaluation, *Computer Networks*, 34(4), 579–595.

[19] Roesch, Martin (1999), Snort—Lightweight Intrusion Detection for Networks, In *Proceedings of LISA '99: 13th Systems Administration Conference*, pp. 229–238, Seattle, Washington: The USENIX Association.

[20] The TCPDump Program (online), tcpdump.org, http://www.tcpdump.org/ (Access Date: Jan. 20, 2004).

[21] Lippman, R.P. (1987), An Introduction to Computing with Neural Nets, In *IEEE ASSP Magazine*, pp. 4–22.

[22] Demuth, Howard and Beale, Mark (2001), Neural Network Toolbox, MathWorks Version 4.

[23] Zurada, J. M. (1992), Introduction to Artificial Neural Systems, New York NY: West Publishing Company.

[24] Widrow, B. and Lehr, M.A. (1990), 30 Years of Adaptive Neural Networks: Perceptron, Madaline, and Backpropagation, In *IEEE Proceedings*, Vol. 78, pp. 1415–1442.

[25] Japkowicz, Nathalie (2001), Supervised Versus Unsupervised Binary-Learning by Feedforward Neural Networks, *Mach. Learn.*, 42(1-2), 97–122.

[26] Japkowicz, N., Myers, C., and Gluck, M (1995), A Novelty Detection Approach to Classification, In *The Fourteenth International Joint Conference on Artificial Intelligence (IJCAI-95)*, pp. 518–523.

[27] Cho, Sungzoon, Han, Chingeun, Han, DAe Hee, and Kim, Hyung-Il (2000), Web based Keystroke Dynamics Identity Verification using Neural Network, *Journal of Organizational Computing and Electronic Commerce*, 10(4), 295–307.

[28] Ripley, B.D. (1996), Pattern Recognition and Neural Networks, 1 ed, Cambridge: Cambridge University Press.

[29] Bilmes, J. (1997), A Gentle Tutorial on the EM Algorithm and its Application to Parameter Estimation for Gaussian Mixture and Hidden Markov Models, (Technical Report ICSI-TR-97-021) University of Berkeley.

[30] Dempster, A.P., Laird, N.M., and Rubin, D.B. (1977), Maximum Likelihood from Incoming Data via the EM Algorithm, *J. Royal Stat. Soc., Series B*, 39(1), 1–36.

[31] Witten, Ian H. and Frank, Eibe (2000), Data Mining: Practical Machine Learning Tools and Techniques with Java Implementations, The Morgan Kaufmann Series in Data Management Systems, San Francisco, CA: Morgan Kaufmann Publishers.

[32] Weka 3: Data Mining Software in Java (online), http://www.cs.waikato.ac.nz/ml/weka/ (Access Date: 19 Jan 2006).

[33] Kohonen, Teuvo (1995), Self-Organizing Maps, Vol. 30 of *Springer Series in Information Sciences*, Berlin, Heidelberg: Springer-Verlag. (Second Extended Edition 1997).

[34] Kohonen, Teuvo, Hynninen, Jussi, Kangas, Jari, and Laaksonen, Jorma (1996), SOM_PAK: The Self-Organizing Map Program Package, (Report A31) Helsinki University of Technology, Laboratory of Computer and Information Science.

[35] Vesanto, Juha and Alhoniemi, Esa (2000), Clustering of the Self-Organizing Map, *IEEE Transactions on Neural Networks*, 11(3), 586–600.

[36] Vesanto, Juha, Himberg, Johan, Alhoniemi, Esa, and Parhankangas, Juha (2000), SOM Toolbox for Matlab 5, (Technical Report Report A57) Helsinki University of Technology, Espoo,Finland.

[37] Hsu, Chih-Wei, Chang, Chih-Chung, and Lin, Chih-Jen (2003), A Practical Guide to Support Vector Classification, *National Taiwan University*.

[38] Duda, Richard O., Hart, Peter E., and Stork, David G. (2001), Pattern Classification, New York, NY: John Wiley and Sons. (Second Edition).

[39] Stevens, W. Richard (1994), TCP/IP Illustrated : The Protocols, Vol. 1, Addison-Wesley.

[40] Ghosh, Anup K. and Schwartzbard, Aaron (1999), A Study in Using Neural Networks for Anomaly and Misuse Detection, In *Proceedings of the Eighth USENIX Security Symposium.*

[41] Jain, A.K., Murty, M.N., and Flynn, P.J. (1999), Data Clustering: A Review, *ACM Comput. Surv.*, 31(3), 264–323.

[42] The incidents.org Data Set (online), incidents.org, http://www.incidents.org/logs/ (Access Date: Mar. 14, 2004).

[43] Wall, Larry, The Perl programming language (online), www.perl.com, http://www.perl.com/ (Access Date: Sept. 1, 2004).

Annex A: Acronyms and Abbreviations

ACC aggregation and correlation component

BMU best-matching unit

ANN artificial neural network

CE clustering errors

CF Canadian Forces

CFNOC Canadian Forces Network Operations Centre

CIRT Computer Incident Response Team

DARPA Defense Advanced Research Projects Agency

DEFCON Defence Conference

DoS denial of service

EM Expectation–Maximisation

IDMEF Intrusion Detection Message Exchange Format

IDS intrusion detection system

IDWG Intrusion Detection Working Group

IP internet protocol

MSE mean square error

MLP multi-layer perceptron

RE reconstruction error

SE separation errors

SOM self-organising maps

TE total number of errors

TCP transmission control protocol

Weka Waikato Environment for Knowledge Analysis

This page intentionally left blank.

Annex B: Gold Standard Output

This section contains an editted version of the gold standard super-clusters for the incidents.org dataset [42]. This section is editted because it was too long (about 50 pages) to include here otherwise. It has been editted to give an overview of how the gold standard was created.

```
Supercluster 1/25
------------------
Cluster 1/6 (sc:1)
------------------
[**][116:46:1] (snort_decoder) TCP Data Offset is less than 5!  [**]
11/09-20:51:11.676507 62.13.27.29:0->207.166.33.145:0
TCP TTL:234 TOS:0x0 ID:0 IpLen:20 DgmLen:40
*****R** Seq:0x81F9750 Ack:0x81F9750 Win:0x0 TcpLen:0


[**][116:46:1] (snort_decoder) TCP Data Offset is less than 5!  [**]
11/10-01:12:17.866507 172.20.10.199:0->207.166.119.62:0
TCP TTL:235 TOS:0x0 ID:0 IpLen:20 DgmLen:40
*****R** Seq:0xBDD2D468 Ack:0xBDD2D468 Win:0x0 TcpLen:16


[**][116:46:1] (snort_decoder) TCP Data Offset is less than 5!  [**]
11/10-01:28:34.556507 62.13.27.29:0->207.166.78.44:0
TCP TTL:234 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
*****R** Seq:0x91D8C02 Ack:0x91D8C02 Win:0x0 TcpLen:12


Cluster 2/6 (sc:1)
------------------
[**][116:46:1] (snort_decoder) TCP Data Offset is less than 5!  [**]
11/12-18:38:17.846507 203.80.239.162:0->207.166.182.137:0
TCP TTL:107 TOS:0x0 ID:35119 IpLen:20 DgmLen:48 DF
1*UA**** Seq:0x7930005 Ack:0xD80A04D1 Win:0x64BA TcpLen:0 UrgPtr:0x800
...

Supercluster 2/25
------------------
Cluster 1/6 (sc:2)
------------------
[**][119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
11/14-09:54:38.316507 170.129.50.120:63362->159.153.199.24:80
TCP TTL:125 TOS:0x0 ID:38908 IpLen:20 DgmLen:436 DF
***AP*** Seq:0x99AD8FC7 Ack:0x732FBFCD Win:0x4230 TcpLen:20

[**][119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
11/14-09:54:47.286507 170.129.50.120:63387->159.153.199.24:80
TCP TTL:125 TOS:0x0 ID:38984 IpLen:20 DgmLen:436 DF
***AP*** Seq:0x99C8B003 Ack:0x733D8EE2 Win:0x4230 TcpLen:20


Cluster 2/6 (sc:2)
------------------
[**][119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
11/14-13:03:42.666507 170.129.50.120:63598->64.4.22.250:80
TCP TTL:124 TOS:0x0 ID:56064 IpLen:20 DgmLen:932 DF
***AP*** Seq:0x94851318 Ack:0x9AB18054 Win:0x43E1 TcpLen:20


Cluster 3/6 (sc:2)
------------------
[**][119:12:1] (http_inspect) APACHE WHITESPACE (TAB) [**]
11/15-02:46:28.446507 170.129.50.120:64749->216.130.211.11:80
TCP TTL:124 TOS:0x0 ID:40697 IpLen:20 DgmLen:1332 DF
***AP*** Seq:0x1601F507 Ack:0xF2FBCCD5 Win:0x2058 TcpLen:20


[**][119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
11/15-02:48:02.606507 170.129.50.120:64868->216.130.211.11:80
TCP TTL:124 TOS:0x0 ID:29178 IpLen:20 DgmLen:1332 DF
***AP*** Seq:0x1772D6D5 Ack:0x4E05CFF6 Win:0x2058 TcpLen:20


Cluster 1/5 (sc:3)
------------------
[**][1:184:4] BACKDOOR Q access [**]
11/14-09:29:14.826507 255.255.255.255:31337->170.129.172.186:515
TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq:0x0 Ack:0x0 Win:0x0 TcpLen:20
```

```
[**][1:184:4] BACKDOOR Q access [**]
11/14-09:32:53.016507 255.255.255.255:31337->170.129.132.79:515
TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq:0x0 Ack:0x0 Win:0x0 TcpLen:20

[**][1:184:4] BACKDOOR Q access [**]
11/14-09:49:26.156507 255.255.255.255:31337->170.129.129.188:515
TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq:0x0 Ack:0x0 Win:0x0 TcpLen:20
...

Cluster 2/5 (sc:3)
-------------------
[**][1:184:4] BACKDOOR Q access [**]
11/14-23:47:53.416507 255.255.255.255:31337->170.129.19.28:515
TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq:0x0 Ack:0x0 Win:0x0 TcpLen:20

[**][1:184:4] BACKDOOR Q access [**]
11/14-23:55:50.456507 255.255.255.255:31337->170.129.161.133:515
TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq:0x0 Ack:0x0 Win:0x0 TcpLen:20
...

Supercluster 4/25
------------------
Cluster 1/6 (sc:4)
-------------------
[**][1:628:3] SCAN nmap TCP [**]
11/14-10:10:03.816507 61.218.161.202:80->170.129.19.170:80
TCP TTL:48 TOS:0x0 ID:30084 IpLen:20 DgmLen:40
***A**** Seq:0x134 Ack:0x0 Win:0x578 TcpLen:20

[**][1:628:3] SCAN nmap TCP [**]
11/14-10:10:08.786507 61.218.161.202:80->170.129.19.170:80
TCP TTL:48 TOS:0x0 ID:30366 IpLen:20 DgmLen:40
***A**** Seq:0x198 Ack:0x0 Win:0x578 TcpLen:20

[**][1:628:3] SCAN nmap TCP [**]
11/14-10:10:13.826507 61.218.161.210:80->170.129.19.170:80
TCP TTL:48 TOS:0x0 ID:30662 IpLen:20 DgmLen:40
***A**** Seq:0x20A Ack:0x0 Win:0x578 TcpLen:20
...

Cluster 2/6 (sc:4)
-------------------
[**][1:628:3] SCAN nmap TCP [**]
11/14-12:51:49.906507 61.218.161.202:80->170.129.14.62:80
TCP TTL:48 TOS:0x0 ID:28299 IpLen:20 DgmLen:40
***A**** Seq:0x11B Ack:0x0 Win:0x578 TcpLen:20

[**][1:628:3] SCAN nmap TCP [**]
11/14-12:51:54.916507 61.218.161.202:80->170.129.14.62:80
TCP TTL:48 TOS:0x0 ID:28601 IpLen:20 DgmLen:40
***A**** Seq:0x18D Ack:0x0 Win:0x578 TcpLen:20

[**][1:628:3] SCAN nmap TCP [**]
11/14-12:51:59.916507 61.218.161.210:80->170.129.14.62:80
TCP TTL:48 TOS:0x0 ID:28911 IpLen:20 DgmLen:40
***A**** Seq:0x209 Ack:0x0 Win:0x578 TcpLen:20
...

Supercluster 8/25
------------------
Cluster 1/4 (sc:8)
-------------------
[**][1:628:3] SCAN nmap TCP [**]
11/14-20:33:44.536507 61.218.15.126:80->170.129.69.49:80
TCP TTL:50 TOS:0x0 ID:9312 IpLen:20 DgmLen:40
***A**** Seq:0x1BF Ack:0x0 Win:0x578 TcpLen:20

[**][1:628:3] SCAN nmap TCP [**]
11/14-20:33:54.676507 61.221.88.198:80->170.129.69.49:80
TCP TTL:50 TOS:0x0 ID:10358 IpLen:20 DgmLen:40
***A**** Seq:0x286 Ack:0x0 Win:0x578 TcpLen:20

[**][1:628:3] SCAN nmap TCP [**]
11/14-20:34:00.056507 192.192.171.251:80->170.129.69.49:80
TCP TTL:44 TOS:0x0 ID:10868 IpLen:20 DgmLen:40
```

```
***A**** Seq:0x2EA Ack:0x0 Win:0x578 TcpLen:20
...

Cluster 2/4 (sc:8)
-------------------
[**][1:628:3] SCAN nmap TCP [**]
11/15-15:36:25.236507 192.192.171.251:80->170.129.105.7:80
TCP TTL:43 TOS:0x0 ID:10388 IpLen:20 DgmLen:40
***A**** Seq:0x260 Ack:0x0 Win:0x578 TcpLen:20


[**][1:628:3] SCAN nmap TCP [**]
11/15-15:36:17.916507 61.221.88.198:80->170.129.105.7:80
TCP TTL:49 TOS:0x0 ID:9868 IpLen:20 DgmLen:40
***A**** Seq:0x1FC Ack:0x0 Win:0x578 TcpLen:20


[**][1:628:3] SCAN nmap TCP [**]
11/15-15:36:07.886507 61.218.15.126:80->170.129.105.7:80
TCP TTL:49 TOS:0x0 ID:8842 IpLen:20 DgmLen:40
***A**** Seq:0x134 Ack:0x0 Win:0x578 TcpLen:20
...

Cluster 1/1 (sc:15)
-------------------
[**][1:556:5] P2P Outbound GNUTella client request [**]
11/14-15:43:37.096507 170.129.50.120:61121->24.65.114.32:6003
TCP TTL:123 TOS:0x0 ID:22720 IpLen:20 DgmLen:158 DF
***AP*** Seq:0x5A0CA92C Ack:0x53A65413 Win:0x4038 TcpLen:20


[**][1:556:5] P2P Outbound GNUTella client request [**]
11/14-15:43:37.316507 170.129.50.120:61122->24.65.114.32:6003
TCP TTL:123 TOS:0x0 ID:22766 IpLen:20 DgmLen:62 DF
***AP*** Seq:0x5A129557 Ack:0x53A7A3BA Win:0x4038 TcpLen:20

Supercluster 16/25
------------------
Cluster 1/2 (sc:16)
-------------------
[**][1:620:6] SCAN Proxy Port 8080 attempt [**]
11/14-16:00:56.996507 66.159.18.66:43517->170.129.50.120:8080
TCP TTL:53 TOS:0x0 ID:59575 IpLen:20 DgmLen:60 DF
******S* Seq:0xBED8745 Ack:0x0 Win:0x16D0 TcpLen:40
TCP Options (5) => MSS:1460 SackOK TS:48656370 0 NOP WS:0

[**][1:618:5] SCAN Squid Proxy attempt [**]
11/14-16:00:56.996507 66.159.18.66:43518->170.129.50.120:3128
TCP TTL:53 TOS:0x0 ID:50174 IpLen:20 DgmLen:60 DF
******S* Seq:0xBF3AC0C Ack:0x0 Win:0x16D0 TcpLen:40
TCP Options (5) => MSS:1460 SackOK TS:48656370 0 NOP WS:0
...

Cluster 2/2 (sc:16)
-------------------
[**][1:618:5] SCAN Squid Proxy attempt [**]
11/14-23:32:20.916507 66.159.18.49:55991->170.129.50.120:3128
TCP TTL:52 TOS:0x0 ID:16353 IpLen:20 DgmLen:60 DF
******S* Seq:0xB4E1FC5B Ack:0x0 Win:0x16D0 TcpLen:40
TCP Options (5) => MSS:1460 SackOK TS:51364794 0 NOP WS:0
...

Supercluster 21/25
------------------
Cluster 1/2 (sc:21)
-------------------
[**][1:1390:4] SHELLCODE x86 inc ebx NOOP [**]
11/14-16:10:30.806507 129.118.2.10:57425->170.129.50.120:63414
TCP TTL:51 TOS:0xA0 ID:56986 IpLen:20 DgmLen:1420 DF
***A**** Seq:0x8217BFFC Ack:0x90CF9E29 Win:0x16D0 TcpLen:20


[**][1:648:6] SHELLCODE x86 NOOP [**]
11/14-21:55:36.566507 129.118.2.10:57425->170.129.50.120:63414
TCP TTL:51 TOS:0xA0 ID:46490 IpLen:20 DgmLen:1420 DF
***A**** Seq:0xA074E240 Ack:0x90CF9E29 Win:0x16D0 TcpLen:20


[**][1:648:6] SHELLCODE x86 NOOP [**]
11/14-21:55:36.576507 129.118.2.10:57425->170.129.50.120:63414
TCP TTL:51 TOS:0xA0 ID:46491 IpLen:20 DgmLen:1420 DF
***A**** Seq:0xA074E7A4 Ack:0x90CF9E29 Win:0x16D0 TcpLen:20
...

Cluster 2/2 (sc:21)
-------------------
```

```
[**][1:1390:4] SHELLCODE x86 inc ebx NOOP [**]
11/14-21:56:03.856507 129.118.2.10:57425->170.129.50.120:63414
TCP TTL:51 TOS:0x0 ID:48298 IpLen:20 DgmLen:1420 DF
***AP*** Seq:0xA09AF480 Ack:0x90CF9E29 Win:0x16D0 TcpLen:20


[**][1:1390:4] SHELLCODE x86 inc ebx NOOP [**]
11/14-21:56:03.906507 129.118.2.10:57425->170.129.50.120:63414
TCP TTL:51 TOS:0xA0 ID:48302 IpLen:20 DgmLen:1420 DF
***AP*** Seq:0xA09B0A10 Ack:0x90CF9E29 Win:0x16D0 TcpLen:20
...

Supercluster 22/25
------------------
Cluster 1/13 (sc:22)
-------------------
[**][1:524:7] BAD-TRAFFIC tcp port 0 traffic [**]
11/15-07:36:26.406507 211.47.255.24:41866->170.129.195.40:0
TCP TTL:46 TOS:0x0 ID:0 IpLen:20 DgmLen:52 DF
******S* Seq:0xD8010CF5 Ack:0x0 Win:0x16D0 TcpLen:32
TCP Options (6) => MSS:1460 NOP NOP SackOK NOP WS:0


[**][1:524:7] BAD-TRAFFIC tcp port 0 traffic [**]
11/15-07:36:29.296507 211.47.255.24:41866->170.129.195.40:0
TCP TTL:46 TOS:0x0 ID:0 IpLen:20 DgmLen:52 DF
******S* Seq:0xD8010CF5 Ack:0x0 Win:0x16D0 TcpLen:32
TCP Options (6) => MSS:1460 NOP NOP SackOK NOP WS:0
...

Cluster 2/13 (sc:22)
-------------------
[**][1:524:7] BAD-TRAFFIC tcp port 0 traffic [**]
11/15-15:09:56.016507 211.47.255.23:47620->170.129.23.96:0
TCP TTL:46 TOS:0x0 ID:0 IpLen:20 DgmLen:52 DF
******S* Seq:0x88C07AEB Ack:0x0 Win:0x16D0 TcpLen:32
TCP Options (6) => MSS:1460 NOP NOP SackOK NOP WS:0


[**][1:524:7] BAD-TRAFFIC tcp port 0 traffic [**]
11/15-15:10:02.006507 211.47.255.23:47620->170.129.23.96:0
TCP TTL:46 TOS:0x0 ID:0 IpLen:20 DgmLen:52 DF
******S* Seq:0x88C07AEB Ack:0x0 Win:0x16D0 TcpLen:32
TCP Options (6) => MSS:1460 NOP NOP SackOK NOP WS:0 ...

Supercluster 23/25
------------------
Cluster 1/3 (sc:23)
-------------------
[**][1:527:4] BAD-TRAFFIC same SRC/DST [**]
11/14-22:36:45.306507 170.129.215.99->170.129.215.99
IGMP TTL:47 TOS:0x0 ID:0 IpLen:20 DgmLen:28


[**][1:527:4] BAD-TRAFFIC same SRC/DST [**]
11/14-22:36:45.306507 170.129.215.104->170.129.215.104
IGMP TTL:47 TOS:0x0 ID:0 IpLen:20 DgmLen:28
...

Cluster 2/3 (sc:23)
-------------------
[**][1:527:4] BAD-TRAFFIC same SRC/DST [**]
11/16-03:26:16.456507 170.129.71.37->170.129.71.37
IGMP TTL:46 TOS:0x0 ID:0 IpLen:20 DgmLen:28


[**][1:527:4] BAD-TRAFFIC same SRC/DST [**]
11/16-03:26:16.456507 170.129.71.42->170.129.71.42
IGMP TTL:46 TOS:0x0 ID:0 IpLen:20 DgmLen:28
...

Supercluster 24/25
------------------
Cluster 1/3 (sc:24)
-------------------
[**][1:523:4] BAD-TRAFFIC ip reserved bit set [**]
11/14-11:21:09.916507 200.200.200.1->170.129.211.200
TCP TTL:242 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB
Frag Offset:0x0864 Frag Size:0x0014


[**][1:523:4] BAD-TRAFFIC ip reserved bit set [**]

11/14-14:37:18.296507 200.200.200.1->170.129.2.16

TCP TTL:242 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB
```

```
Frag Offset:0x0864 Frag Size:0x0014

...
```

This page intentionally left blank.

Annex C: Recall Results

```
Supercluster 1/18
------------------

Cluster 1/3 (sc: 1)
-------------------

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/16-18:16:20.416507
206.48.61.152:2359 -> 170.129.108.46:8080 TCP TTL:113 TOS:0x0
ID:31456 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1439203  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/16-18:16:23.436507
206.48.61.152:2359 -> 170.129.108.46:8080 TCP TTL:113 TOS:0x0
ID:33248 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1439203  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/16-13:34:38.646507
206.48.61.152:2234 -> 170.129.89.189:8080 TCP TTL:113 TOS:0x0
ID:29481 IpLen:20 DgmLen:48 DF
******S* Seq: 0x419789  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/16-13:34:35.646507
206.48.61.152:2234 -> 170.129.89.189:8080 TCP TTL:113 TOS:0x0
ID:26921 IpLen:20 DgmLen:48 DF
******S* Seq: 0x419789  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/16-13:18:20.076507
206.48.61.152:4786 -> 170.129.19.70:8080 TCP TTL:113 TOS:0x0
ID:16158 IpLen:20 DgmLen:48 DF
******S* Seq: 0x32A80E  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/16-13:22:53.866507
206.48.61.152:1215 -> 170.129.96.15:8080 TCP TTL:113 TOS:0x0
ID:26657 IpLen:20 DgmLen:48 DF
******S* Seq: 0x36D5DC  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/16-13:22:50.846507
206.48.61.152:1215 -> 170.129.96.15:8080 TCP TTL:113 TOS:0x0
ID:24097 IpLen:20 DgmLen:48 DF
******S* Seq: 0x36D5DC  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/16-13:18:17.046507
206.48.61.152:4786 -> 170.129.19.70:8080 TCP TTL:113 TOS:0x0
ID:13598 IpLen:20 DgmLen:48 DF
******S* Seq: 0x32A80E  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] [1:618:5] SCAN Squid Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/14-16:06:24.316507
206.48.61.139:4006 -> 170.129.23.239:3128 TCP TTL:114 TOS:0x0
ID:26758 IpLen:20 DgmLen:48 DF
******S* Seq: 0x13D84F7  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] [1:618:5] SCAN Squid Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/14-16:06:21.366507
206.48.61.139:4006 -> 170.129.23.239:3128 TCP TTL:114 TOS:0x0
ID:24710 IpLen:20 DgmLen:48 DF
******S* Seq: 0x13D84F7  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

Cluster 2/3 (sc: 1)
-------------------

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-18:54:31.966507
204.188.170.90:4175 -> 170.129.152.15:8080 TCP TTL:113 TOS:0x0
```

```
ID:52708 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1CF3682  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

Cluster 3/3 (sc: 1)
-------------------

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/16-12:59:08.856507
206.48.61.152:3109 -> 170.129.132.70:8080 TCP TTL:113 TOS:0x0
ID:63760 IpLen:20 DgmLen:48 DF
******S* Seq: 0x211675  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

Supercluster 2/18
-----------------

Cluster 1/3 (sc: 2)
-------------------

[**] [119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
11/14-09:54:38.316507 170.129.50.120:63362 -> 159.153.199.24:80 TCP
TTL:125 TOS:0x0 ID:38908 IpLen:20 DgmLen:436 DF
***AP*** Seq: 0x99AD8FC7  Ack: 0x732FBFCD  Win: 0x4230  TcpLen: 20

[**] [119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
11/14-09:54:47.286507 170.129.50.120:63387 -> 159.153.199.24:80 TCP
TTL:125 TOS:0x0 ID:38984 IpLen:20 DgmLen:436 DF
***AP*** Seq: 0x99C8B003  Ack: 0x733D8EE2  Win: 0x4230  TcpLen: 20

Cluster 2/3 (sc: 2)
-------------------

[**] [119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
11/15-10:00:30.986507 170.129.50.120:64645 -> 199.45.45.132:80 TCP
TTL:125 TOS:0x0 ID:1655 IpLen:20 DgmLen:829 DF
***AP*** Seq: 0x68E6FA3B  Ack: 0x43F74153  Win: 0x4470  TcpLen: 20

[**] [119:13:1] (http_inspect) NON-RFC HTTP DELIMITER [**]
11/15-10:00:30.986507 170.129.50.120:64645 -> 199.45.45.132:80 TCP
TTL:125 TOS:0x0 ID:1655 IpLen:20 DgmLen:829 DF
***AP*** Seq: 0x68E6FA3B  Ack: 0x43F74153  Win: 0x4470  TcpLen: 20

Cluster 3/3 (sc: 2)
-------------------

[**] [119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
11/15-05:01:26.376507 170.129.50.120:63188 -> 207.68.164.250:80 TCP
TTL:125 TOS:0x0 ID:5826 IpLen:20 DgmLen:932 DF
***AP*** Seq: 0xC9F1EEBB  Ack: 0xF019024A  Win: 0xFA61  TcpLen: 20

[**] [119:12:1] (http_inspect) APACHE WHITESPACE (TAB) [**]
11/15-05:01:25.396507 170.129.50.120:63188 -> 207.68.164.250:80 TCP
TTL:125 TOS:0x0 ID:5777 IpLen:20 DgmLen:932 DF
***AP*** Seq: 0xC9F10EBB  Ack: 0xF019024A  Win: 0xFA61  TcpLen: 20

[**] [119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
11/15-05:01:21.766507 170.129.50.120:63175 -> 207.68.164.250:80 TCP
TTL:125 TOS:0x0 ID:5651 IpLen:20 DgmLen:932 DF
***AP*** Seq: 0xC9E10861  Ack: 0x3015901B  Win: 0xFA61  TcpLen: 20

[**] [119:12:1] (http_inspect) APACHE WHITESPACE (TAB) [**]
11/15-05:01:20.766507 170.129.50.120:63175 -> 207.68.164.250:80 TCP
TTL:125 TOS:0x0 ID:5602 IpLen:20 DgmLen:932 DF
***AP*** Seq: 0xC9E02861  Ack: 0x3015901B  Win: 0xFA61  TcpLen: 20

Supercluster 3/18
-----------------

Cluster 1/1 (sc: 3)
-------------------

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-09:29:14.826507 255.255.255.255:31337
-> 170.129.172.186:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-09:32:53.016507 255.255.255.255:31337
-> 170.129.132.79:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-09:49:26.156507 255.255.255.255:31337
-> 170.129.129.188:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
```

```
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-10:10:22.596507 255.255.255.255:31337
-> 170.129.195.178:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-10:44:04.836507 255.255.255.255:31337
-> 170.129.30.34:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-11:44:56.156507 255.255.255.255:31337
-> 170.129.137.174:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-12:56:26.746507 255.255.255.255:31337
-> 170.129.89.87:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-14:01:20.986507 255.255.255.255:31337
-> 170.129.23.133:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-14:04:08.966507 255.255.255.255:31337
-> 170.129.190.188:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-16:14:32.966507 255.255.255.255:31337
-> 170.129.192.22:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-16:16:56.986507 255.255.255.255:31337
-> 170.129.134.5:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-16:17:12.036507 255.255.255.255:31337
-> 170.129.156.132:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-16:30:57.086507 255.255.255.255:31337
-> 170.129.146.62:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-16:47:18.156507 255.255.255.255:31337
-> 170.129.176.42:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-17:06:30.606507 255.255.255.255:31337
-> 170.129.80.5:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-17:11:03.616507 255.255.255.255:31337
-> 170.129.1.102:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-17:23:24.646507 255.255.255.255:31337
-> 170.129.41.171:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]
```

```
[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-19:34:10.596507 255.255.255.255:31337
-> 170.129.94.129:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-19:38:10.756507 255.255.255.255:31337
-> 170.129.181.145:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-20:56:56.236507 255.255.255.255:31337
-> 170.129.72.205:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-21:10:50.476507 255.255.255.255:31337
-> 170.129.156.91:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-21:29:40.696507 255.255.255.255:31337
-> 170.129.161.211:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-22:50:02.016507 255.255.255.255:31337
-> 170.129.103.3:515 TCP TTL:15 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-13:35:08.896507 255.255.255.255:31337
-> 170.129.200.84:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-23:47:53.416507 255.255.255.255:31337
-> 170.129.19.28:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/14-23:55:50.456507 255.255.255.255:31337
-> 170.129.161.133:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-00:38:36.896507 255.255.255.255:31337
-> 170.129.57.163:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-03:00:36.046507 255.255.255.255:31337
-> 170.129.193.103:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-04:16:09.186507 255.255.255.255:31337
-> 170.129.53.148:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-04:36:09.286507 255.255.255.255:31337
-> 170.129.178.16:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-04:52:48.246507 255.255.255.255:31337
-> 170.129.155.128:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-07:17:35.846507 255.255.255.255:31337
-> 170.129.153.135:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
```

```
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-07:22:02.826507 255.255.255.255:31337
-> 170.129.65.138:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-07:38:05.946507 255.255.255.255:31337
-> 170.129.190.224:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-09:21:00.436507 255.255.255.255:31337
-> 170.129.49.119:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-10:23:53.796507 255.255.255.255:31337
-> 170.129.38.133:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-10:25:17.826507 255.255.255.255:31337
-> 170.129.68.126:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-13:10:52.326507 255.255.255.255:31337
-> 170.129.40.192:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-13:20:22.396507 255.255.255.255:31337
-> 170.129.167.203:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-13:26:48.526507 255.255.255.255:31337
-> 170.129.69.141:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-13:58:21.556507 255.255.255.255:31337
-> 170.129.211.38:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-14:23:43.856507 255.255.255.255:31337
-> 170.129.142.93:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-14:28:15.856507 255.255.255.255:31337
-> 170.129.33.54:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-14:34:03.916507 255.255.255.255:31337
-> 170.129.33.72:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-15:01:15.966507 255.255.255.255:31337
-> 170.129.19.190:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-15:05:36.916507 255.255.255.255:31337
-> 170.129.115.50:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]
```

```
[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-15:39:36.996507 255.255.255.255:31337
-> 170.129.201.142:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-15:43:54.956507 255.255.255.255:31337
-> 170.129.72.94:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-16:10:01.256507 255.255.255.255:31337
-> 170.129.150.38:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-16:25:04.146507 255.255.255.255:31337
-> 170.129.222.145:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-19:26:47.606507 255.255.255.255:31337
-> 170.129.209.73:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-19:41:53.666507 255.255.255.255:31337
-> 170.129.146.14:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-20:38:06.496507 255.255.255.255:31337
-> 170.129.38.78:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-21:01:04.956507 255.255.255.255:31337
-> 170.129.227.19:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-21:59:46.406507 255.255.255.255:31337
-> 170.129.171.53:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-22:34:37.896507 255.255.255.255:31337
-> 170.129.197.57:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-23:35:17.646507 255.255.255.255:31337
-> 170.129.106.120:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/15-23:38:56.776507 255.255.255.255:31337
-> 170.129.159.157:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-00:14:44.586507 255.255.255.255:31337
-> 170.129.13.177:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-00:46:03.036507 255.255.255.255:31337
-> 170.129.129.128:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-01:50:26.406507 255.255.255.255:31337
-> 170.129.112.183:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
```

```
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-03:00:24.566507 255.255.255.255:31337
-> 170.129.153.108:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-03:32:33.276507 255.255.255.255:31337
-> 170.129.119.45:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-03:45:18.516507 255.255.255.255:31337
-> 170.129.203.58:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-04:50:19.176507 255.255.255.255:31337
-> 170.129.209.67:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-05:26:17.526507 255.255.255.255:31337
-> 170.129.89.164:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-05:44:56.686507 255.255.255.255:31337
-> 170.129.23.189:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-06:16:56.956507 255.255.255.255:31337
-> 170.129.207.122:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-07:52:33.616507 255.255.255.255:31337
-> 170.129.22.182:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-09:26:25.786507 255.255.255.255:31337
-> 170.129.56.82:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-10:16:39.326507 255.255.255.255:31337
-> 170.129.27.13:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-14:02:38.526507 255.255.255.255:31337
-> 170.129.119.210:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-16:07:42.286507 255.255.255.255:31337
-> 170.129.57.211:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-16:22:48.346507 255.255.255.255:31337
-> 170.129.157.148:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-16:55:37.766507 255.255.255.255:31337
-> 170.129.178.195:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]
```

```
[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-17:20:52.916507 255.255.255.255:31337
-> 170.129.24.44:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-18:23:11.826507 255.255.255.255:31337
-> 170.129.94.77:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-18:35:33.006507 255.255.255.255:31337
-> 170.129.165.132:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-18:49:56.076507 255.255.255.255:31337
-> 170.129.83.228:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-19:58:00.016507 255.255.255.255:31337
-> 170.129.214.158:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

[**] [1:184:4] BACKDOOR Q access [**] [Classification: Misc
activity] [Priority: 3] 11/16-21:49:41.436507 255.255.255.255:31337
-> 170.129.122.35:515 TCP TTL:14 TOS:0x0 ID:0 IpLen:20 DgmLen:43
***A*R** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS203]

Supercluster 4/18
------------------

Cluster 1/2 (sc: 4)
-------------------

[**] [116:46:1] (snort_decoder) WARNING: TCP Data Offset is less
than 5! [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] 11/11-09:08:23.926507 172.20.10.199:0 ->
207.166.207.98:0 TCP TTL:234 TOS:0x0 ID:0 IpLen:20 DgmLen:40
*****R** Seq: 0xC4AD19A6  Ack: 0xC4AD19A6  Win: 0x0  TcpLen: 16

[**] [116:46:1] (snort_decoder) WARNING: TCP Data Offset is less
than 5! [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] 11/10-01:12:17.866507 172.20.10.199:0 ->
207.166.119.62:0 TCP TTL:235 TOS:0x0 ID:0 IpLen:20 DgmLen:40
*****R** Seq: 0xBDD2D468  Ack: 0xBDD2D468  Win: 0x0  TcpLen: 16

[**] [116:46:1] (snort_decoder) WARNING: TCP Data Offset is less
than 5! [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] 11/10-01:28:34.556507 62.13.27.29:0 -> 207.166.78.44:0
TCP TTL:234 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x91D8C02  Ack: 0x91D8C02  Win: 0x0  TcpLen: 12

[**] [116:46:1] (snort_decoder) WARNING: TCP Data Offset is less
than 5! [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] 11/12-03:07:49.886507 210.243.145.141:0 ->
207.166.159.139:0 TCP TTL:237 TOS:0x0 ID:0 IpLen:20 DgmLen:40
*****R** Seq: 0x158662C0  Ack: 0x158662C0  Win: 0x0  TcpLen: 16

Cluster 2/2 (sc: 4)
-------------------

[**] [116:46:1] (snort_decoder) WARNING: TCP Data Offset is less
than 5! [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] 11/09-20:51:11.676507 62.13.27.29:0 ->
207.166.33.145:0 TCP TTL:234 TOS:0x0 ID:0 IpLen:20 DgmLen:40
*****R** Seq: 0x81F9750  Ack: 0x81F9750  Win: 0x0  TcpLen: 0

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-10:52:22.116507
63.211.17.228:80 -> 170.129.50.120:63874 TCP TTL:54 TOS:0x0 ID:563
IpLen:20 DgmLen:40
***A**** Seq: 0x3DC  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [116:46:1] (snort_decoder) WARNING: TCP Data Offset is less
than 5! [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] 11/10-07:20:11.976507 172.20.10.199:0 ->
207.166.168.10:0 TCP TTL:235 TOS:0x0 ID:0 IpLen:20 DgmLen:40
*****R** Seq: 0xBF23A8C4  Ack: 0xBF23A8C4  Win: 0x0  TcpLen: 0
```

```
[**] [116:46:1] (snort_decoder) WARNING: TCP Data Offset is less
than 5! [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] 11/12-20:25:11.826507 217.209.183.235:0 ->
207.166.252.249:0 TCP TTL:236 TOS:0x0 ID:0 IpLen:20 DgmLen:40
*****R** Seq: 0x24A1C4C  Ack: 0x24A1C4C  Win: 0x0  TcpLen: 0

Supercluster 5/18
------------------

Cluster 1/1 (sc: 5)
-------------------

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-18:54:34.916507
204.188.170.90:4175 -> 170.129.152.15:8080 TCP TTL:113 TOS:0x0
ID:54756 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1CF3682  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/14-23:32:20.806507
66.159.18.49:55990 -> 170.129.50.120:8080 TCP TTL:52 TOS:0x0
ID:52037 IpLen:20 DgmLen:60 DF
******S* Seq: 0xB4F108EA  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 51364783 0 NOP WS: 0

Supercluster 6/18
------------------

Cluster 1/1 (sc: 6)
-------------------

[**] [119:13:1] (http_inspect) NON-RFC HTTP DELIMITER [**]
11/15-04:45:24.366507 170.129.50.120:61044 -> 216.136.173.111:80 TCP
TTL:125 TOS:0x0 ID:10198 IpLen:20 DgmLen:932 DF
***AP*** Seq: 0xA014995  Ack: 0x6193010  Win: 0xFAF0  TcpLen: 20

[**] [119:12:1] (http_inspect) APACHE WHITESPACE (TAB) [**]
11/15-04:45:21.306507 170.129.50.120:61044 -> 216.136.173.111:80 TCP
TTL:125 TOS:0x0 ID:10054 IpLen:20 DgmLen:932 DF
***AP*** Seq: 0x9FEC995  Ack: 0x6193010  Win: 0xFAF0  TcpLen: 20

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:37.296507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46538 IpLen:20 DgmLen:1420 DF
***AP*** Seq: 0xA075E500  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:37.866507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46576 IpLen:20 DgmLen:1420 DF
***AP*** Seq: 0xA076B1D8  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:41.096507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46776 IpLen:20 DgmLen:1420 DF
***AP*** Seq: 0xA07AE7F8  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
11/15-04:45:11.546507 170.129.50.120:61044 -> 216.136.173.111:80 TCP
TTL:125 TOS:0x0 ID:9584 IpLen:20 DgmLen:932 DF
***AP*** Seq: 0x9F68995  Ack: 0x6193010  Win: 0xFAF0  TcpLen: 20

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:47.826507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:47206 IpLen:20 DgmLen:1420 DF
***AP*** Seq: 0xA083F5F0  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:48.306507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:47238 IpLen:20 DgmLen:1420 DF
***AP*** Seq: 0xA084A270  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:48.536507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:47252 IpLen:20 DgmLen:1420 DF
```

```
***AP*** Seq: 0xA084EDE8  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:48.476507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:47248 IpLen:20 DgmLen:1420 DF
***AP*** Seq: 0xA084D858  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
Executable code was detected] [Priority: 1] 11/14-21:56:03.906507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:48302 IpLen:20 DgmLen:1420 DF
***AP*** Seq: 0xA09B0A10  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

Supercluster 7/18
------------------

Cluster 1/1 (sc: 7)
-------------------

[**] [1:2314:1] SHELLCODE x86 0x90 NOOP unicode [**]
[Classification: Executable code was detected] [Priority: 1]
11/15-12:09:01.196507 216.183.64.22:43124 -> 170.129.50.3:20 TCP
TTL:235 TOS:0x0 ID:42286 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xAC0E29C3  Ack: 0x9ED7097C  Win: 0x65D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 208895632 6108063

[**] [1:2314:1] SHELLCODE x86 0x90 NOOP unicode [**]
[Classification: Executable code was detected] [Priority: 1]
11/15-12:09:01.256507 216.183.64.22:43124 -> 170.129.50.3:20 TCP
TTL:235 TOS:0x0 ID:42290 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0xAC0E4063  Ack: 0x9ED7097C  Win: 0x65D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 208895639 6108072

Supercluster 8/18
------------------

Cluster 1/2 (sc: 8)
-------------------

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/16-12:59:05.876507
206.48.61.152:3109 -> 170.129.132.70:8080 TCP TTL:113 TOS:0x0
ID:61200 IpLen:20 DgmLen:48 DF
******S* Seq: 0x211675  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] [1:615:5] SCAN SOCKS Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-06:59:47.096507
216.201.160.235:44398 -> 170.129.161.213:1080 TCP TTL:46 TOS:0x0
ID:52073 IpLen:20 DgmLen:60 DF
******S* Seq: 0x4E410469  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 17303918 0 NOP WS: 0 [Xref
=> http://help.undernet.org/proxyscan/]

[**] [1:615:5] SCAN SOCKS Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-06:59:50.116507
216.201.160.235:44398 -> 170.129.161.213:1080 TCP TTL:46 TOS:0x0
ID:52144 IpLen:20 DgmLen:60 DF
******S* Seq: 0x4E410469  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 17304218 0 NOP WS: 0 [Xref
=> http://help.undernet.org/proxyscan/]

[**] [1:615:5] SCAN SOCKS Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-06:59:56.086507
216.201.160.235:44398 -> 170.129.161.213:1080 TCP TTL:46 TOS:0x0
ID:52206 IpLen:20 DgmLen:60 DF
******S* Seq: 0x4E410469  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 17304818 0 NOP WS: 0 [Xref
=> http://help.undernet.org/proxyscan/]

[**] [1:615:5] SCAN SOCKS Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-07:00:08.076507
216.201.160.235:44398 -> 170.129.161.213:1080 TCP TTL:46 TOS:0x0
ID:52424 IpLen:20 DgmLen:60 DF
******S* Seq: 0x4E410469  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 17306018 0 NOP WS: 0 [Xref
=> http://help.undernet.org/proxyscan/]

Cluster 2/2 (sc: 8)
-------------------

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:09:56.016507
211.47.255.23:47620 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
```

```
IpLen:20 DgmLen:52 DF
******S* Seq: 0x88C07AEB  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:10:02.006507
211.47.255.23:47620 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x88C07AEB  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:10:14.016507
211.47.255.23:47620 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x88C07AEB  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:09:21.006507
211.47.255.23:47382 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x86DAFDF0  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:09:23.996507
211.47.255.23:47382 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x86DAFDF0  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:09:29.986507
211.47.255.23:47382 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x86DAFDF0  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:09:42.006507
211.47.255.23:47382 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x86DAFDF0  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:08:49.016507
211.47.255.23:47154 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x858405A9  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:08:52.016507
211.47.255.23:47154 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x858405A9  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:09:10.016507
211.47.255.23:47154 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x858405A9  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:08:17.016507
211.47.255.23:46919 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x83442FEE  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:08:19.996507
211.47.255.23:46919 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x83442FEE  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:08:25.996507
211.47.255.23:46919 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x83442FEE  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0
```

```
[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-15:08:37.996507
211.47.255.23:46919 -> 170.129.23.96:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x83442FEE  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:36:46.156507
211.47.255.20:47040 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x18C00FAD  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:36:49.176507
211.47.255.20:47040 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x18C00FAD  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:36:55.156507
211.47.255.20:47040 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x18C00FAD  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:37:08.116507
211.47.255.20:47040 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x18C00FAD  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:17:59.046507
211.47.255.21:50171 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB466ABD9  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:18:02.776507
211.47.255.21:50171 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB466ABD9  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:18:08.676507
211.47.255.21:50171 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB466ABD9  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:18:20.016507
211.47.255.21:50171 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB466ABD9  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:36:14.166507
211.47.255.20:46671 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x1661E114  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:36:17.166507
211.47.255.20:46671 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x1661E114  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:36:23.166507
211.47.255.20:46671 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x1661E114  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:36:35.146507
```

```
211.47.255.20:46671 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x1661E114  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:18:31.356507
211.47.255.21:50456 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB5E7FDB6  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:18:34.026507
211.47.255.21:50456 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB5E7FDB6  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:18:40.036507
211.47.255.21:50456 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB5E7FDB6  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:18:52.046507
211.47.255.21:50456 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB5E7FDB6  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:19:03.516507
211.47.255.21:50736 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB79B3E67  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:19:06.026507
211.47.255.21:50736 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB79B3E67  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:19:12.046507
211.47.255.21:50736 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB79B3E67  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:19:24.046507
211.47.255.21:50736 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB79B3E67  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:35:42.176507
211.47.255.20:46319 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x13A6B185  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:35:45.156507
211.47.255.20:46319 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x13A6B185  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:35:51.166507
211.47.255.20:46319 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x13A6B185  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:36:03.146507
211.47.255.20:46319 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x13A6B185  Ack: 0x0  Win: 0x16D0  TcpLen: 32
```

```
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:19:35.066507
211.47.255.21:51068 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB963B7C7  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:19:38.786507
211.47.255.21:51068 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB963B7C7  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:19:44.646507
211.47.255.21:51068 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB963B7C7  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:19:56.006507
211.47.255.21:51068 -> 170.129.48.125:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB963B7C7  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:35:10.156507
211.47.255.20:46000 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x121C24B1  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:35:13.156507
211.47.255.20:46000 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x121C24B1  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:35:19.166507
211.47.255.20:46000 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x121C24B1  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-07:35:31.146507
211.47.255.20:46000 -> 170.129.118.169:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x121C24B1  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:58:12.296507
211.47.255.24:43338 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB54600DF  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:58:15.286507
211.47.255.24:43338 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB54600DF  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:58:21.306507
211.47.255.24:43338 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB54600DF  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:58:33.276507
211.47.255.24:43338 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB54600DF  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
```

```
Misc activity] [Priority: 3] 11/15-11:57:40.276507
211.47.255.24:43155 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB3CCEB6A  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:57:49.426507
211.47.255.24:43155 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB3CCEB6A  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:58:01.296507
211.47.255.24:43155 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB3CCEB6A  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:57:08.306507
211.47.255.24:42950 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB108ED90  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:57:11.266507
211.47.255.24:42950 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB108ED90  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:57:17.306507
211.47.255.24:42950 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB108ED90  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:57:29.376507
211.47.255.24:42950 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB108ED90  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:56:36.296507
211.47.255.24:42742 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xAECA8CC2  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:56:39.336507
211.47.255.24:42742 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xAECA8CC2  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:56:45.296507
211.47.255.24:42742 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xAECA8CC2  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:56:57.656507
211.47.255.24:42742 -> 170.129.21.249:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xAECA8CC2  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:36:26.406507
211.47.255.24:41866 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD8010CF5  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:36:29.296507
211.47.255.24:41866 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
```

```
******S* Seq: 0xD8010CF5  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:36:35.286507
211.47.255.24:41866 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD8010CF5  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:36:47.306507
211.47.255.24:41866 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD8010CF5  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:48:34.676507
211.47.255.24:55235 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5950BEC6  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:48:40.676507
211.47.255.24:55235 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5950BEC6  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:48:52.676507
211.47.255.24:55235 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5950BEC6  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:35:54.326507
211.47.255.24:41611 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD60E9D41  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:35:57.316507
211.47.255.24:41611 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD60E9D41  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:36:03.286507
211.47.255.24:41611 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD60E9D41  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:36:15.296507
211.47.255.24:41611 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD60E9D41  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:53:41.296507
211.47.255.21:41618 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB978BA1D  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:53:44.296507
211.47.255.21:41618 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB978BA1D  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:53:50.316507
211.47.255.21:41618 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB978BA1D  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0
```

```
[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:54:02.296507
211.47.255.21:41618 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB978BA1D  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:49:03.686507
211.47.255.24:55518 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5B030D9A  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:49:06.666507
211.47.255.24:55518 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5B030D9A  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:49:12.676507
211.47.255.24:55518 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5B030D9A  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:49:24.676507
211.47.255.24:55518 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5B030D9A  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:35:22.326507
211.47.255.24:41358 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD4C4A857  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:35:25.406507
211.47.255.24:41358 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD4C4A857  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:35:31.326507
211.47.255.24:41358 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD4C4A857  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:49:35.676507
211.47.255.24:55769 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5D09DDB1  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:49:38.676507
211.47.255.24:55769 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5D09DDB1  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:49:44.676507
211.47.255.24:55769 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5D09DDB1  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:49:56.666507
211.47.255.24:55769 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5D09DDB1  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:34:50.446507
211.47.255.24:41104 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
```

```
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD30F0032  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:34:53.296507
211.47.255.24:41104 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD30F0032  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:34:59.466507
211.47.255.24:41104 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD30F0032  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-07:35:11.276507
211.47.255.24:41104 -> 170.129.195.40:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xD30F0032  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:53:09.286507
211.47.255.21:41067 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB794BBF4  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:53:12.286507
211.47.255.21:41067 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB794BBF4  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:53:19.176507
211.47.255.21:41067 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB794BBF4  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:53:30.286507
211.47.255.21:41067 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB794BBF4  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:50:07.696507
211.47.255.24:56011 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5F6DA539  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:50:10.676507
211.47.255.24:56011 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5F6DA539  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:50:16.676507
211.47.255.24:56011 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5F6DA539  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-15:50:28.686507
211.47.255.24:56011 -> 170.129.25.163:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x5F6DA539  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:52:37.296507
211.47.255.21:40582 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB5097658  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0
```

```
[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:52:40.296507
211.47.255.21:40582 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB5097658  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:52:46.296507
211.47.255.21:40582 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB5097658  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:52:58.316507
211.47.255.21:40582 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB5097658  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-21:55:13.716507
211.47.255.24:56519 -> 170.129.23.90:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xC1B34FCA  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-21:55:16.696507
211.47.255.24:56519 -> 170.129.23.90:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xC1B34FCA  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-21:55:22.706507
211.47.255.24:56519 -> 170.129.23.90:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xC1B34FCA  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-21:55:34.676507
211.47.255.24:56519 -> 170.129.23.90:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xC1B34FCA  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:52:05.286507
211.47.255.21:40037 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB34D8507  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:52:08.286507
211.47.255.21:40037 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB34D8507  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:52:14.276507
211.47.255.21:40037 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB34D8507  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/15-19:52:26.276507
211.47.255.21:40037 -> 170.129.156.144:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB34D8507  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-21:55:48.796507
211.47.255.24:57025 -> 170.129.23.90:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xC371A50B  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-21:56:06.836507
```

```
211.47.255.24:57025 -> 170.129.23.90:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xC371A50B  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:16:01.066507
211.47.255.22:39681 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x71C9D034  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:16:04.896507
211.47.255.22:39681 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x71C9D034  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:16:10.056507
211.47.255.22:39681 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x71C9D034  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:16:22.056507
211.47.255.22:39681 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x71C9D034  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:36.676507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0x0
ID:46498 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA0750D60  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
11/15-02:48:02.606507 170.129.50.120:64868 -> 216.130.211.11:80 TCP
TTL:124 TOS:0x0 ID:29178 IpLen:20 DgmLen:1332 DF
***AP*** Seq: 0x1772D6D5  Ack: 0x4E05CFF6  Win: 0x2058  TcpLen: 20

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:37.026507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0x0
ID:46521 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA075895C  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:15:29.056507
211.47.255.22:39442 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x6F8441E7  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:15:38.066507
211.47.255.22:39442 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x6F8441E7  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:15:50.066507
211.47.255.22:39442 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x6F8441E7  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:14:57.066507
211.47.255.22:39179 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x6CE8BFA0  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:15:00.056507
211.47.255.22:39179 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x6CE8BFA0  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0
```

```
[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:15:06.056507
211.47.255.22:39179 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x6CE8BFA0  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:15:18.076507
211.47.255.22:39179 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x6CE8BFA0  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:39.356507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0x0
ID:46669 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA078A72C  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:14:25.866507
211.47.255.22:38944 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x6B28A453  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:14:28.066507
211.47.255.22:38944 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x6B28A453  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:14:34.056507
211.47.255.22:38944 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x6B28A453  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-10:14:46.056507
211.47.255.22:38944 -> 170.129.228.55:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x6B28A453  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
11/15-02:46:26.726507 170.129.50.120:64749 -> 216.130.211.11:80 TCP
TTL:124 TOS:0x0 ID:26873 IpLen:20 DgmLen:1332 DF
***AP*** Seq: 0x1600D507  Ack: 0xF2FBCCD5  Win: 0x2058  TcpLen: 20

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:48.316507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0x0
ID:47239 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA084A7D4  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:48.506507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0x0
ID:47250 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA084E320  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:48.576507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0x0
ID:47255 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA084FE14  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:56:29.836507
211.47.255.20:36576 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x45FCB139  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:56:32.836507
211.47.255.20:36576 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x45FCB139  Ack: 0x0  Win: 0x16D0  TcpLen: 32
```

```
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:56:39.426507
211.47.255.20:36576 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x45FCB139  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:56:50.836507
211.47.255.20:36576 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x45FCB139  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:55:57.816507
211.47.255.20:36319 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x4304B38E  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:56:00.826507
211.47.255.20:36319 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x4304B38E  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:56:06.826507
211.47.255.20:36319 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x4304B38E  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:56:18.826507
211.47.255.20:36319 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x4304B38E  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:55:28.826507
211.47.255.20:36015 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x40E17268  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:55:34.826507
211.47.255.20:36015 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x40E17268  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:55:46.826507
211.47.255.20:36015 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x40E17268  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:21:24.156507
211.47.255.20:35928 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB79B7F19  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:21:33.126507
211.47.255.20:35928 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB79B7F19  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:21:45.136507
211.47.255.20:35928 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB79B7F19  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
```

```
Misc activity] [Priority: 3] 11/16-08:54:53.826507
211.47.255.20:35752 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x3EAAD0C3  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:54:56.806507
211.47.255.20:35752 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x3EAAD0C3  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:55:02.826507
211.47.255.20:35752 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x3EAAD0C3  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-08:55:14.996507
211.47.255.20:35752 -> 170.129.44.181:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0x3EAAD0C3  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [119:12:1] (http_inspect) APACHE WHITESPACE (TAB) [**]
11/15-02:46:28.446507 170.129.50.120:64749 -> 216.130.211.11:80 TCP
TTL:124 TOS:0x0 ID:40697 IpLen:20 DgmLen:1332 DF
***AP*** Seq: 0x1601F507  Ack: 0xF2FBCCD5  Win: 0x2058  TcpLen: 20

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:20:52.146507
211.47.255.20:35382 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB5D0E140  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:20:55.136507
211.47.255.20:35382 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB5D0E140  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:21:01.156507
211.47.255.20:35382 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB5D0E140  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:21:13.126507
211.47.255.20:35382 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB5D0E140  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:20:20.136507
211.47.255.20:34851 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB3AFF15D  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:20:23.146507
211.47.255.20:34851 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB3AFF15D  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:20:29.146507
211.47.255.20:34851 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB3AFF15D  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:20:41.136507
211.47.255.20:34851 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB3AFF15D  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0
```

```
[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:19:51.146507
211.47.255.20:34339 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB1A713EE  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:19:57.136507
211.47.255.20:34339 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB1A713EE  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [1:524:7] BAD-TRAFFIC tcp port 0 traffic [**] [Classification:
Misc activity] [Priority: 3] 11/16-17:20:09.126507
211.47.255.20:34339 -> 170.129.210.216:0 TCP TTL:46 TOS:0x0 ID:0
IpLen:20 DgmLen:52 DF
******S* Seq: 0xB1A713EE  Ack: 0x0  Win: 0x16D0  TcpLen: 32
TCP Options (6) => MSS: 1460 NOP NOP SackOK NOP WS: 0

[**] [119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
11/14-13:03:42.666507 170.129.50.120:63598 -> 64.4.22.250:80 TCP
TTL:124 TOS:0x0 ID:56064 IpLen:20 DgmLen:932 DF
***AP*** Seq: 0x94851318  Ack: 0x9AB18054  Win: 0x43E1  TcpLen: 20

Supercluster 9/18
------------------

Cluster 1/2 (sc: 9)
-------------------

[**] [116:46:1] (snort_decoder) WARNING: TCP Data Offset is less
than 5! [**] 11/14-22:53:21.926507 68.41.28.138:0 ->
170.129.225.41:0 TCP TTL:107 TOS:0x0 ID:35590 IpLen:20 DgmLen:48 DF
******** Seq: 0x50989C  Ack: 0x2F470000  Win: 0x7002  TcpLen: 0

[**] [116:46:1] (snort_decoder) WARNING: TCP Data Offset is less
than 5! [**] 11/15-23:11:54.416507 68.41.28.138:0 -> 170.129.23.60:0
TCP TTL:106 TOS:0x0 ID:39864 IpLen:20 DgmLen:48 DF
******** Seq: 0x5B4F202C  Ack: 0x0  Win: 0x7002  TcpLen: 0

Cluster 2/2 (sc: 9)
-------------------

[**] [1:522:1] MISC Tiny Fragments [**] [Classification: Potentially
Bad Traffic] [Priority: 2] 11/16-06:42:06.146507 66.81.110.134 ->
170.129.139.231 TCP TTL:231 TOS:0x0 ID:0 IpLen:20 DgmLen:40 MF Frag
Offset: 0x0800   Frag Size: 0x0014

Supercluster 10/18
------------------

Cluster 1/1 (sc: 10)
--------------------

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:36.566507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46490 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA074E240  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:36.576507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46491 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA074E7A4  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:36.756507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46504 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA0752DB8  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:37.146507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46529 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA075B47C  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:37.216507
```

```
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46532 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA075C4A8  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:37.526507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46553 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA07635DC  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:37.626507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46560 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA0765B98  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:38.016507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46584 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA076DCF8  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:37.856507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46575 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA076AC74  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:37.876507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46577 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA076B73C  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:38.936507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46646 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA0782B30  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:39.306507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46667 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA0789C64  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:39.436507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46673 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA078BCBC  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:40.176507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:46719 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA079B4B4  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:615:5] SCAN SOCKS Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/14-23:32:20.686507
66.159.18.49:55989 -> 170.129.50.120:1080 TCP TTL:52 TOS:0x0
ID:59203 IpLen:20 DgmLen:60 DF
******S* Seq: 0xB4F124E7  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 51364772 0 NOP WS: 0 [Xref
=> http://help.undernet.org/proxyscan/]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:47.876507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:47208 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA08400B8  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:48.206507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:47231 IpLen:20 DgmLen:1420 DF
```

```
***A**** Seq: 0xA0847CB4  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:48.226507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:47233 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA084877C  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:48.456507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:47245 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA084C82C  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:48.466507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:47247 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA084D2F4  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:48.516507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:47251 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA084E884  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:648:6] SHELLCODE x86 NOOP [**] [Classification: Executable
code was detected] [Priority: 1] 11/14-21:55:48.596507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:47256 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA0850378  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS181]

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
Executable code was detected] [Priority: 1] 11/14-21:56:03.796507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:48293 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA09AD98C  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
Executable code was detected] [Priority: 1] 11/14-21:56:03.966507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:48306 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA09B1FA0  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
Executable code was detected] [Priority: 1] 11/14-21:56:03.806507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:48294 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA09ADEF0  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
Executable code was detected] [Priority: 1] 11/14-21:56:03.816507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:48295 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA09AE454  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
Executable code was detected] [Priority: 1] 11/14-21:56:03.836507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:48296 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA09AE9B8  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
Executable code was detected] [Priority: 1] 11/14-21:56:03.846507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:48297 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA09AEF1C  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
Executable code was detected] [Priority: 1] 11/14-21:56:03.856507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:48299 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA09AF9E4  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
Executable code was detected] [Priority: 1] 11/14-21:56:03.886507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:48300 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA09AFF48  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
```

```
Executable code was detected] [Priority: 1] 11/14-21:56:03.896507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:48301 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA09B04AC  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
Executable code was detected] [Priority: 1] 11/14-21:56:03.916507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:48303 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA09B0F74  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
Executable code was detected] [Priority: 1] 11/14-21:56:03.936507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:48304 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA09B14D8  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
Executable code was detected] [Priority: 1] 11/14-21:56:03.946507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:48305 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0xA09B1A3C  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

[**] [1:556:5] P2P Outbound GNUTella client request [**]
[Classification: Potential Corporate Privacy Violation] [Priority:
1] 11/14-15:43:37.096507 170.129.50.120:61121 -> 24.65.114.32:6003
TCP TTL:123 TOS:0x0 ID:22720 IpLen:20 DgmLen:158 DF
***AP*** Seq: 0x5A0CA92C  Ack: 0x53A65413  Win: 0x4038  TcpLen: 20

[**] [1:556:5] P2P Outbound GNUTella client request [**]
[Classification: Potential Corporate Privacy Violation] [Priority:
1] 11/14-15:43:37.316507 170.129.50.120:61122 -> 24.65.114.32:6003
TCP TTL:123 TOS:0x0 ID:22766 IpLen:20 DgmLen:62 DF
***AP*** Seq: 0x5A129557  Ack: 0x53A7A3BA  Win: 0x4038  TcpLen: 20

Supercluster 11/18
------------------

Cluster 1/3 (sc: 11)
--------------------

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-11:23:37.366507
64.152.70.68:80 -> 170.129.50.120:53 TCP TTL:53 TOS:0x0 ID:33050
IpLen:20 DgmLen:40
***A**** Seq: 0xC3  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-11:23:37.376507
64.152.70.68:53 -> 170.129.50.120:53 TCP TTL:53 TOS:0x0 ID:33051
IpLen:20 DgmLen:40
***A**** Seq: 0xC4  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-07:37:01.056507
12.111.47.194:80 -> 170.129.50.120:2564 TCP TTL:48 TOS:0x0 ID:24950
IpLen:20 DgmLen:40
***A**** Seq: 0xDC  Ack: 0x0  Win: 0x400  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-07:37:01.086507
141.155.200.194:80 -> 170.129.50.120:2564 TCP TTL:45 TOS:0x0
ID:24956 IpLen:20 DgmLen:40
***A**** Seq: 0xDE  Ack: 0x0  Win: 0x400  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-10:10:18.856507
61.218.161.210:80 -> 170.129.19.170:80 TCP TTL:48 TOS:0x0 ID:30943
IpLen:20 DgmLen:40
***A**** Seq: 0x278  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-10:10:13.826507
61.218.161.210:80 -> 170.129.19.170:80 TCP TTL:48 TOS:0x0 ID:30662
IpLen:20 DgmLen:40
***A**** Seq: 0x20A  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-10:10:08.786507
61.218.161.202:80 -> 170.129.19.170:80 TCP TTL:48 TOS:0x0 ID:30366
IpLen:20 DgmLen:40
```

```
***A**** Seq: 0x198  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-10:10:03.816507
61.218.161.202:80 -> 170.129.19.170:80 TCP TTL:48 TOS:0x0 ID:30084
IpLen:20 DgmLen:40
***A**** Seq: 0x134  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-12:52:04.916507
61.218.161.210:80 -> 170.129.14.62:80 TCP TTL:48 TOS:0x0 ID:29197
IpLen:20 DgmLen:40
***A**** Seq: 0x279  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-11:24:29.666507
208.155.15.101:80 -> 170.129.50.122:53 TCP TTL:54 TOS:0x0 ID:24273
IpLen:20 DgmLen:40
***A**** Seq: 0x365  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-11:24:29.636507
206.102.126.101:80 -> 170.129.50.122:53 TCP TTL:54 TOS:0x0 ID:24270
IpLen:20 DgmLen:40
***A**** Seq: 0x363  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-12:51:59.916507
61.218.161.210:80 -> 170.129.14.62:80 TCP TTL:48 TOS:0x0 ID:28911
IpLen:20 DgmLen:40
***A**** Seq: 0x209  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-12:51:54.916507
61.218.161.202:80 -> 170.129.14.62:80 TCP TTL:48 TOS:0x0 ID:28601
IpLen:20 DgmLen:40
***A**** Seq: 0x18D  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-12:51:49.906507
61.218.161.202:80 -> 170.129.14.62:80 TCP TTL:48 TOS:0x0 ID:28299
IpLen:20 DgmLen:40
***A**** Seq: 0x11B  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-11:47:58.956507
61.218.161.210:80 -> 170.129.152.4:80 TCP TTL:47 TOS:0x0 ID:28766
IpLen:20 DgmLen:40
***A**** Seq: 0x345  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-11:47:53.986507
61.218.161.210:80 -> 170.129.152.4:80 TCP TTL:47 TOS:0x0 ID:28502
IpLen:20 DgmLen:40
***A**** Seq: 0x2E3  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-11:47:48.986507
61.218.161.202:80 -> 170.129.152.4:80 TCP TTL:47 TOS:0x0 ID:28174
IpLen:20 DgmLen:40
***A**** Seq: 0x25F  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-11:47:44.106507
61.218.161.202:80 -> 170.129.152.4:80 TCP TTL:47 TOS:0x0 ID:27928
IpLen:20 DgmLen:40
***A**** Seq: 0x1FB  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-01:39:05.426507
61.218.161.210:80 -> 170.129.111.203:80 TCP TTL:47 TOS:0x0 ID:27640
IpLen:20 DgmLen:40
***A**** Seq: 0x25A  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]
```

```
[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-21:53:15.676507 202.29.28.1:80
-> 170.129.31.152:80 TCP TTL:44 TOS:0x0 ID:36247 IpLen:20 DgmLen:40
***A**** Seq: 0x1FE  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-21:53:25.666507 202.29.28.1:80
-> 170.129.31.152:80 TCP TTL:44 TOS:0x0 ID:36504 IpLen:20 DgmLen:40
***A**** Seq: 0x26C  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-21:53:35.666507 202.29.28.1:80
-> 170.129.31.152:80 TCP TTL:44 TOS:0x0 ID:36802 IpLen:20 DgmLen:40
***A**** Seq: 0x2EA  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-10:10:23.856507
163.23.238.9:80 -> 170.129.19.170:80 TCP TTL:44 TOS:0x0 ID:31290
IpLen:20 DgmLen:40
***A**** Seq: 0x300  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-21:53:45.706507 202.29.28.1:80
-> 170.129.31.152:80 TCP TTL:44 TOS:0x0 ID:37072 IpLen:20 DgmLen:40
***A**** Seq: 0x35F  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-01:39:00.386507
61.218.161.210:80 -> 170.129.111.203:80 TCP TTL:47 TOS:0x0 ID:27328
IpLen:20 DgmLen:40
***A**** Seq: 0x1D4  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-01:38:55.506507
61.218.161.202:80 -> 170.129.111.203:80 TCP TTL:47 TOS:0x0 ID:27067
IpLen:20 DgmLen:40
***A**** Seq: 0x170  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-01:38:50.396507
61.218.161.202:80 -> 170.129.111.203:80 TCP TTL:47 TOS:0x0 ID:26787
IpLen:20 DgmLen:40
***A**** Seq: 0x10A  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-12:52:09.906507
163.23.238.9:80 -> 170.129.14.62:80 TCP TTL:44 TOS:0x0 ID:29544
IpLen:20 DgmLen:40
***A**** Seq: 0x2FD  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-11:48:06.816507
163.23.238.9:80 -> 170.129.152.4:80 TCP TTL:43 TOS:0x0 ID:29034
IpLen:20 DgmLen:40
***A**** Seq: 0x39B  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-01:39:21.476507
163.23.238.9:80 -> 170.129.111.203:80 TCP TTL:43 TOS:0x0 ID:27949
IpLen:20 DgmLen:40
***A**** Seq: 0x2E2  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-23:18:23.756507
61.222.251.82:80 -> 170.129.50.3:80 TCP TTL:48 TOS:0x0 ID:44368
IpLen:20 DgmLen:40
***A**** Seq: 0x6D  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-14:29:34.136507 202.29.28.1:80
-> 170.129.238.112:80 TCP TTL:45 TOS:0x0 ID:23947 IpLen:20 DgmLen:40
***A**** Seq: 0x5D  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
```

```
Executable code was detected] [Priority: 1] 11/14-21:56:03.856507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0x0
ID:48298 IpLen:20 DgmLen:1420 DF
***AP*** Seq: 0xA09AF480  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-14:29:24.186507 202.29.28.1:80
-> 170.129.238.112:80 TCP TTL:45 TOS:0x0 ID:23770 IpLen:20 DgmLen:40
***A**** Seq: 0x0  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-14:29:14.306507 202.29.28.1:80
-> 170.129.238.112:80 TCP TTL:45 TOS:0x0 ID:23584 IpLen:20 DgmLen:40
***A**** Seq: 0x3A6  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-14:29:04.266507 202.29.28.1:80
-> 170.129.238.112:80 TCP TTL:45 TOS:0x0 ID:23404 IpLen:20 DgmLen:40
***A**** Seq: 0x348  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-14:28:54.256507 202.29.28.1:80
-> 170.129.238.112:80 TCP TTL:45 TOS:0x0 ID:23204 IpLen:20 DgmLen:40
***A**** Seq: 0x2E6  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-12:14:11.266507
61.222.14.98:80 -> 170.129.81.112:80 TCP TTL:49 TOS:0x0 ID:48192
IpLen:20 DgmLen:40
***A**** Seq: 0x144  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-12:14:16.266507
61.222.14.98:80 -> 170.129.81.112:80 TCP TTL:49 TOS:0x0 ID:48734
IpLen:20 DgmLen:40
***A**** Seq: 0x1A8  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-12:14:21.266507
61.222.192.98:80 -> 170.129.81.112:80 TCP TTL:49 TOS:0x0 ID:49258
IpLen:20 DgmLen:40
***A**** Seq: 0x20A  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-03:52:30.576507
61.221.99.242:80 -> 170.129.98.80:80 TCP TTL:47 TOS:0x0 ID:48912
IpLen:20 DgmLen:40
***A**** Seq: 0x4C  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-12:14:26.276507
61.222.192.98:80 -> 170.129.81.112:80 TCP TTL:49 TOS:0x0 ID:49820
IpLen:20 DgmLen:40
***A**** Seq: 0x271  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-03:52:35.556507
61.221.99.242:80 -> 170.129.98.80:80 TCP TTL:47 TOS:0x0 ID:49356
IpLen:20 DgmLen:40
***A**** Seq: 0xEE  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-12:12:33.956507 202.29.28.1:80
-> 170.129.127.161:80 TCP TTL:44 TOS:0x0 ID:19100 IpLen:20 DgmLen:40
***A**** Seq: 0x276  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-12:12:24.036507 202.29.28.1:80
-> 170.129.127.161:80 TCP TTL:44 TOS:0x0 ID:18859 IpLen:20 DgmLen:40
***A**** Seq: 0x202  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-03:52:41.016507
163.22.229.253:80 -> 170.129.98.80:80 TCP TTL:44 TOS:0x0 ID:49726
IpLen:20 DgmLen:40
```

```
***A**** Seq: 0x170  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-12:12:13.926507 202.29.28.1:80
-> 170.129.127.161:80 TCP TTL:44 TOS:0x0 ID:18595 IpLen:20 DgmLen:40
***A**** Seq: 0x18C  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-12:12:03.926507 202.29.28.1:80
-> 170.129.127.161:80 TCP TTL:44 TOS:0x0 ID:18328 IpLen:20 DgmLen:40
***A**** Seq: 0x11A  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-12:11:53.916507 202.29.28.1:80
-> 170.129.127.161:80 TCP TTL:44 TOS:0x0 ID:18054 IpLen:20 DgmLen:40
***A**** Seq: 0xA5  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-12:14:41.366507
210.66.117.5:80 -> 170.129.81.112:80 TCP TTL:47 TOS:0x0 ID:51450
IpLen:20 DgmLen:40
***A**** Seq: 0x39E  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-12:11:43.966507 202.29.28.1:80
-> 170.129.127.161:80 TCP TTL:44 TOS:0x0 ID:17803 IpLen:20 DgmLen:40
***A**** Seq: 0x33  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-12:14:46.366507
210.66.117.5:80 -> 170.129.81.112:80 TCP TTL:47 TOS:0x0 ID:51968
IpLen:20 DgmLen:40
***A**** Seq: 0x400  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

Cluster 2/3 (sc: 11)
--------------------

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-12:02:45.976507 167.79.91.3:80
-> 170.129.50.122:53 TCP TTL:49 TOS:0x0 ID:11661 IpLen:20 DgmLen:40
***A**** Seq: 0x2A5  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-12:02:46.046507 167.79.91.3:80
-> 170.129.50.122:53 TCP TTL:47 TOS:0x0 ID:11664 IpLen:20 DgmLen:40
***A**** Seq: 0x2A7  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-20:33:54.676507
61.221.88.198:80 -> 170.129.69.49:80 TCP TTL:50 TOS:0x0 ID:10358
IpLen:20 DgmLen:40
***A**** Seq: 0x286  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-19:39:06.696507 202.29.28.1:80
-> 170.129.185.21:80 TCP TTL:44 TOS:0x0 ID:56514 IpLen:20 DgmLen:40
***A**** Seq: 0xB2  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-19:39:16.696507 202.29.28.1:80
-> 170.129.185.21:80 TCP TTL:44 TOS:0x0 ID:56770 IpLen:20 DgmLen:40
***A**** Seq: 0x121  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-20:34:04.926507
192.192.171.251:80 -> 170.129.69.49:80 TCP TTL:44 TOS:0x0 ID:11428
IpLen:20 DgmLen:40
***A**** Seq: 0x353  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-19:39:26.706507 202.29.28.1:80
-> 170.129.185.21:80 TCP TTL:44 TOS:0x0 ID:57025 IpLen:20 DgmLen:40
***A**** Seq: 0x195  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]
```

```
[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-15:36:17.916507
61.221.88.198:80 -> 170.129.105.7:80 TCP TTL:49 TOS:0x0 ID:9868
IpLen:20 DgmLen:40
***A**** Seq: 0x1FC  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-19:39:36.706507 202.29.28.1:80
-> 170.129.185.21:80 TCP TTL:44 TOS:0x0 ID:57272 IpLen:20 DgmLen:40
***A**** Seq: 0x1FF  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-19:39:46.706507 202.29.28.1:80
-> 170.129.185.21:80 TCP TTL:44 TOS:0x0 ID:57504 IpLen:20 DgmLen:40
***A**** Seq: 0x263  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-20:33:44.536507
61.218.15.126:80 -> 170.129.69.49:80 TCP TTL:50 TOS:0x0 ID:9312
IpLen:20 DgmLen:40
***A**** Seq: 0x1BF  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-20:34:00.056507
192.192.171.251:80 -> 170.129.69.49:80 TCP TTL:44 TOS:0x0 ID:10868
IpLen:20 DgmLen:40
***A**** Seq: 0x2EA  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-15:36:12.906507
61.221.88.198:80 -> 170.129.105.7:80 TCP TTL:49 TOS:0x0 ID:9352
IpLen:20 DgmLen:40
***A**** Seq: 0x198  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-20:33:39.636507
61.218.15.126:80 -> 170.129.69.49:80 TCP TTL:50 TOS:0x0 ID:8768
IpLen:20 DgmLen:40
***A**** Seq: 0x158  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-15:36:07.886507
61.218.15.126:80 -> 170.129.105.7:80 TCP TTL:49 TOS:0x0 ID:8842
IpLen:20 DgmLen:40
***A**** Seq: 0x134  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-15:36:25.236507
192.192.171.251:80 -> 170.129.105.7:80 TCP TTL:43 TOS:0x0 ID:10388
IpLen:20 DgmLen:40
***A**** Seq: 0x260  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-20:33:34.876507
61.218.15.118:80 -> 170.129.69.49:80 TCP TTL:50 TOS:0x0 ID:8252
IpLen:20 DgmLen:40
***A**** Seq: 0xF4  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-01:06:03.086507
61.218.15.118:80 -> 170.129.29.7:80 TCP TTL:49 TOS:0x0 ID:59856
IpLen:20 DgmLen:40
***A**** Seq: 0x65  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-15:36:02.876507
61.218.15.126:80 -> 170.129.105.7:80 TCP TTL:49 TOS:0x0 ID:8314
IpLen:20 DgmLen:40
***A**** Seq: 0xD2  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-01:06:08.046507
61.218.15.118:80 -> 170.129.29.7:80 TCP TTL:49 TOS:0x0 ID:60354
IpLen:20 DgmLen:40
```

```
***A**** Seq: 0xC7  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-20:33:29.606507
61.218.15.118:80 -> 170.129.69.49:80 TCP TTL:50 TOS:0x0 ID:7722
IpLen:20 DgmLen:40
***A**** Seq: 0x92  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-15:35:57.876507
61.218.15.118:80 -> 170.129.105.7:80 TCP TTL:49 TOS:0x0 ID:7784
IpLen:20 DgmLen:40
***A**** Seq: 0x6B  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-01:06:13.056507
61.218.15.126:80 -> 170.129.29.7:80 TCP TTL:49 TOS:0x0 ID:60914
IpLen:20 DgmLen:40
***A**** Seq: 0x12D  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/15-15:35:52.886507
61.218.15.118:80 -> 170.129.105.7:80 TCP TTL:49 TOS:0x0 ID:7244
IpLen:20 DgmLen:40
***A**** Seq: 0x7  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-01:06:18.026507
61.218.15.126:80 -> 170.129.29.7:80 TCP TTL:49 TOS:0x0 ID:61428
IpLen:20 DgmLen:40
***A**** Seq: 0x18F  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-04:44:27.746507
61.218.15.118:80 -> 170.129.144.141:80 TCP TTL:49 TOS:0x0 ID:61812
IpLen:20 DgmLen:40
***A**** Seq: 0x34  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-01:06:23.066507
61.221.88.198:80 -> 170.129.29.7:80 TCP TTL:49 TOS:0x0 ID:61966
IpLen:20 DgmLen:40
***A**** Seq: 0x1F5  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-04:44:32.736507
61.218.15.118:80 -> 170.129.144.141:80 TCP TTL:49 TOS:0x0 ID:62382
IpLen:20 DgmLen:40
***A**** Seq: 0xA1  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-01:06:28.086507
61.221.88.198:80 -> 170.129.29.7:80 TCP TTL:49 TOS:0x0 ID:62482
IpLen:20 DgmLen:40
***A**** Seq: 0x258  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-04:44:37.796507
61.218.15.126:80 -> 170.129.144.141:80 TCP TTL:49 TOS:0x0 ID:62902
IpLen:20 DgmLen:40
***A**** Seq: 0x106  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-13:12:15.806507
61.218.161.202:80 -> 170.129.107.3:80 TCP TTL:47 TOS:0x0 ID:62695
IpLen:20 DgmLen:40
***A**** Seq: 0x186  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-13:12:20.816507
61.218.161.202:80 -> 170.129.107.3:80 TCP TTL:47 TOS:0x0 ID:62960
IpLen:20 DgmLen:40
***A**** Seq: 0x1F8  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]
```

```
[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-04:44:42.786507
61.218.15.126:80 -> 170.129.144.141:80 TCP TTL:49 TOS:0x0 ID:63460
IpLen:20 DgmLen:40
***A**** Seq: 0x170  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-13:12:25.806507
61.218.161.210:80 -> 170.129.107.3:80 TCP TTL:47 TOS:0x0 ID:63186
IpLen:20 DgmLen:40
***A**** Seq: 0x254  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-13:12:30.816507
61.218.161.210:80 -> 170.129.107.3:80 TCP TTL:47 TOS:0x0 ID:63520
IpLen:20 DgmLen:40
***A**** Seq: 0x2CE  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-04:44:47.756507
61.221.88.198:80 -> 170.129.144.141:80 TCP TTL:49 TOS:0x0 ID:63982
IpLen:20 DgmLen:40
***A**** Seq: 0x1D5  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-01:06:33.316507
192.192.171.251:80 -> 170.129.29.7:80 TCP TTL:43 TOS:0x0 ID:63010
IpLen:20 DgmLen:40
***A**** Seq: 0x2BD  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-04:44:52.776507
61.221.88.198:80 -> 170.129.144.141:80 TCP TTL:49 TOS:0x0 ID:64512
IpLen:20 DgmLen:40
***A**** Seq: 0x238  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-01:06:38.256507
192.192.171.251:80 -> 170.129.29.7:80 TCP TTL:43 TOS:0x0 ID:63530
IpLen:20 DgmLen:40
***A**** Seq: 0x322  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-14:50:18.166507
61.218.161.202:80 -> 170.129.151.28:80 TCP TTL:48 TOS:0x0 ID:64698
IpLen:20 DgmLen:40
***A**** Seq: 0x26  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-13:12:35.966507
163.23.238.9:80 -> 170.129.107.3:80 TCP TTL:43 TOS:0x0 ID:63792
IpLen:20 DgmLen:40
***A**** Seq: 0x334  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-14:50:23.136507
61.218.161.202:80 -> 170.129.151.28:80 TCP TTL:48 TOS:0x0 ID:64986
IpLen:20 DgmLen:40
***A**** Seq: 0x8C  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-14:50:28.126507
61.218.161.210:80 -> 170.129.151.28:80 TCP TTL:48 TOS:0x0 ID:65271
IpLen:20 DgmLen:40
***A**** Seq: 0x100  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-04:44:58.136507
192.192.171.251:80 -> 170.129.144.141:80 TCP TTL:43 TOS:0x0 ID:65068
IpLen:20 DgmLen:40
***A**** Seq: 0x29A  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

Cluster 3/3 (sc: 11)
--------------------
```

```
[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-14:50:33.266507
61.218.161.210:80 -> 170.129.151.28:80 TCP TTL:48 TOS:0x0 ID:32
IpLen:20 DgmLen:40
***A**** Seq: 0x17A  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/14-14:50:38.206507
163.23.238.9:80 -> 170.129.151.28:80 TCP TTL:44 TOS:0x0 ID:336
IpLen:20 DgmLen:40
***A**** Seq: 0x1EC  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

[**] [1:628:3] SCAN nmap TCP [**] [Classification: Attempted
Information Leak] [Priority: 2] 11/16-04:45:03.176507
192.192.171.251:80 -> 170.129.144.141:80 TCP TTL:43 TOS:0x0 ID:58
IpLen:20 DgmLen:40
***A**** Seq: 0x2FE  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS28]

Supercluster 12/18
------------------

Cluster 1/1 (sc: 12)
--------------------

[**] [1:504:4] MISC source port 53 to <1024 [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/15-11:24:29.636507
206.102.126.101:53 -> 170.129.50.122:53 TCP TTL:54 TOS:0x0 ID:24271
IpLen:20 DgmLen:40
******S* Seq: 0x4E80C2A7  Ack: 0x0  Win: 0x578  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS07]

[**] [116:46:1] (snort_decoder) WARNING: TCP Data Offset is less
than 5! [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] 11/12-18:38:17.846507 203.80.239.162:0 ->
207.166.182.137:0 TCP TTL:107 TOS:0x0 ID:35119 IpLen:20 DgmLen:48 DF
1*UA**** Seq: 0x7930005  Ack: 0xD80A04D1  Win: 0x64BA  TcpLen: 0
UrgPtr: 0x800

Supercluster 13/18
------------------

Cluster 1/1 (sc: 13)
--------------------

[**] [1:1390:4] SHELLCODE x86 inc ebx NOOP [**] [Classification:
Executable code was detected] [Priority: 1] 11/14-16:10:30.806507
129.118.2.10:57425 -> 170.129.50.120:63414 TCP TTL:51 TOS:0xA0
ID:56986 IpLen:20 DgmLen:1420 DF
***A**** Seq: 0x8217BFFC  Ack: 0x90CF9E29  Win: 0x16D0  TcpLen: 20

Supercluster 14/18
------------------

Cluster 1/1 (sc: 14)
--------------------

[**] [116:46:1] (snort_decoder) WARNING: TCP Data Offset is less
than 5! [**] 11/16-02:36:10.986507 210.243.145.141:0 ->
170.129.134.11:0 TCP TTL:236 TOS:0x0 ID:0 IpLen:20 DgmLen:40
*****R** Seq: 0x2A02EB38  Ack: 0x2A02EB38  Win: 0x0  TcpLen: 12

Supercluster 15/18
------------------

Cluster 1/2 (sc: 15)
--------------------

[**] [1:615:5] SCAN SOCKS Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/14-16:00:56.996507
66.159.18.66:43520 -> 170.129.50.120:1080 TCP TTL:53 TOS:0x0 ID:4253
IpLen:20 DgmLen:60 DF
******S* Seq: 0xB9A7F6F  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 48656370 0 NOP WS: 0 [Xref
=> http://help.undernet.org/proxyscan/]

Cluster 2/2 (sc: 15)
--------------------

[**] [1:615:5] SCAN SOCKS Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/14-16:00:56.996507
66.159.18.66:43521 -> 170.129.50.120:1080 TCP TTL:53 TOS:0x0 ID:2662
IpLen:20 DgmLen:60 DF
******S* Seq: 0xBF46594  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 48656370 0 NOP WS: 0 [Xref
```

```
=> http://help.undernet.org/proxyscan/]

Supercluster 16/18
------------------

Cluster 1/2 (sc: 16)
--------------------

[**] [1:523:4] BAD-TRAFFIC ip reserved bit set [**] [Classification:
Misc activity] [Priority: 3] 11/14-23:28:20.656507 200.200.200.1 ->
170.129.53.47 TCP TTL:241 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB Frag
Offset: 0x0864   Frag Size: 0x0014

[**] [1:523:4] BAD-TRAFFIC ip reserved bit set [**] [Classification:
Misc activity] [Priority: 3] 11/15-01:09:54.346507 200.200.200.1 ->
170.129.217.111 TCP TTL:241 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB Frag
Offset: 0x0864   Frag Size: 0x0014

[**] [1:523:4] BAD-TRAFFIC ip reserved bit set [**] [Classification:
Misc activity] [Priority: 3] 11/15-01:21:09.846507 200.200.200.1 ->
170.129.127.227 TCP TTL:241 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB Frag
Offset: 0x0864   Frag Size: 0x0014

[**] [1:523:4] BAD-TRAFFIC ip reserved bit set [**] [Classification:
Misc activity] [Priority: 3] 11/15-05:24:51.026507 200.200.200.1 ->
170.129.60.231 TCP TTL:241 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB Frag
Offset: 0x0864   Frag Size: 0x0014

[**] [1:523:4] BAD-TRAFFIC ip reserved bit set [**] [Classification:
Misc activity] [Priority: 3] 11/15-08:28:17.596507 200.200.200.1 ->
170.129.71.27 TCP TTL:241 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB Frag
Offset: 0x0864   Frag Size: 0x0014

[**] [1:523:4] BAD-TRAFFIC ip reserved bit set [**] [Classification:
Misc activity] [Priority: 3] 11/15-11:04:18.336507 200.200.200.1 ->
170.129.161.217 TCP TTL:241 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB Frag
Offset: 0x0864   Frag Size: 0x0014

[**] [1:523:4] BAD-TRAFFIC ip reserved bit set [**] [Classification:
Misc activity] [Priority: 3] 11/14-11:21:09.916507 200.200.200.1 ->
170.129.211.200 TCP TTL:242 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB Frag
Offset: 0x0864   Frag Size: 0x0014

[**] [1:523:4] BAD-TRAFFIC ip reserved bit set [**] [Classification:
Misc activity] [Priority: 3] 11/14-14:37:18.296507 200.200.200.1 ->
170.129.2.16 TCP TTL:242 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB Frag
Offset: 0x0864   Frag Size: 0x0014

[**] [1:523:4] BAD-TRAFFIC ip reserved bit set [**] [Classification:
Misc activity] [Priority: 3] 11/14-15:54:39.456507 200.200.200.1 ->
170.129.79.180 TCP TTL:242 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB Frag
Offset: 0x0864   Frag Size: 0x0014

[**] [1:523:4] BAD-TRAFFIC ip reserved bit set [**] [Classification:
Misc activity] [Priority: 3] 11/14-17:59:31.346507 200.200.200.1 ->
170.129.239.44 TCP TTL:242 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB Frag
Offset: 0x0864   Frag Size: 0x0014

[**] [1:523:4] BAD-TRAFFIC ip reserved bit set [**] [Classification:
Misc activity] [Priority: 3] 11/14-23:04:22.106507 200.200.200.1 ->
170.129.43.122 TCP TTL:242 TOS:0x0 ID:0 IpLen:20 DgmLen:40 RB Frag
Offset: 0x0864   Frag Size: 0x0014

Cluster 2/2 (sc: 16)
--------------------

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/14-22:36:45.306507
170.129.215.99 -> 170.129.215.99 IGMP TTL:47 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/14-22:36:45.306507
170.129.215.104 -> 170.129.215.104 IGMP TTL:47 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/14-22:36:45.306507
170.129.215.115 -> 170.129.215.115 IGMP TTL:47 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]
```

```
[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/14-22:36:45.306507
170.129.215.110 -> 170.129.215.110 IGMP TTL:47 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/14-22:36:45.306507
170.129.215.120 -> 170.129.215.120 IGMP TTL:47 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/14-22:36:45.306507
170.129.215.126 -> 170.129.215.126 IGMP TTL:47 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/14-22:36:45.306507
170.129.215.131 -> 170.129.215.131 IGMP TTL:47 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/14-22:36:45.306507
170.129.215.137 -> 170.129.215.137 IGMP TTL:47 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/14-22:36:45.306507
170.129.215.142 -> 170.129.215.142 IGMP TTL:47 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/14-22:36:45.306507
170.129.215.85 -> 170.129.215.85 IGMP TTL:47 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/14-22:36:45.306507
170.129.215.93 -> 170.129.215.93 IGMP TTL:47 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-03:26:16.456507
170.129.71.37 -> 170.129.71.37 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-03:26:16.456507
170.129.71.42 -> 170.129.71.42 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-03:26:16.456507
170.129.71.53 -> 170.129.71.53 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-03:26:16.456507
170.129.71.47 -> 170.129.71.47 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-03:26:16.456507
170.129.71.69 -> 170.129.71.69 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
```

```
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-03:26:16.456507
170.129.71.74 -> 170.129.71.74 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-03:26:16.456507
170.129.71.63 -> 170.129.71.63 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-03:26:16.456507
170.129.71.20 -> 170.129.71.20 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-03:26:16.456507
170.129.71.7 -> 170.129.71.7 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-03:26:16.456507
170.129.71.26 -> 170.129.71.26 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-03:26:16.456507
170.129.71.31 -> 170.129.71.31 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-03:26:16.456507
170.129.71.58 -> 170.129.71.58 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-11:33:01.856507
170.129.164.3 -> 170.129.164.3 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-11:33:01.856507
170.129.164.9 -> 170.129.164.9 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-11:33:01.856507
170.129.164.14 -> 170.129.164.14 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-11:33:01.856507
170.129.164.25 -> 170.129.164.25 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-11:33:01.856507
170.129.164.30 -> 170.129.164.30 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]
```

```
[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-11:33:01.856507
170.129.164.41 -> 170.129.164.41 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-11:33:01.856507
170.129.164.52 -> 170.129.164.52 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-11:33:01.856507
170.129.163.252 -> 170.129.163.252 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-11:33:01.856507
170.129.164.20 -> 170.129.164.20 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-11:33:01.856507
170.129.164.36 -> 170.129.164.36 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

[**] [1:527:4] BAD-TRAFFIC same SRC/DST [**] [Classification:
Potentially Bad Traffic] [Priority: 2] 11/16-11:33:01.856507
170.129.164.46 -> 170.129.164.46 IGMP TTL:46 TOS:0x0 ID:0 IpLen:20
DgmLen:28 [Xref =>
http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016]

Supercluster 17/18
------------------

Cluster 1/2 (sc: 17)
--------------------

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-06:59:47.096507
216.201.160.235:44389 -> 170.129.161.213:8080 TCP TTL:46 TOS:0x0
ID:52064 IpLen:20 DgmLen:60 DF
******S* Seq: 0x4E70998D  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 17303918 0 NOP WS: 0

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-06:59:50.116507
216.201.160.235:44389 -> 170.129.161.213:8080 TCP TTL:46 TOS:0x0
ID:52135 IpLen:20 DgmLen:60 DF
******S* Seq: 0x4E70998D  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 17304218 0 NOP WS: 0

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-06:59:56.086507
216.201.160.235:44389 -> 170.129.161.213:8080 TCP TTL:46 TOS:0x0
ID:52197 IpLen:20 DgmLen:60 DF
******S* Seq: 0x4E70998D  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 17304818 0 NOP WS: 0

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-07:00:08.076507
216.201.160.235:44389 -> 170.129.161.213:8080 TCP TTL:46 TOS:0x0
ID:52415 IpLen:20 DgmLen:60 DF
******S* Seq: 0x4E70998D  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 17306018 0 NOP WS: 0

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/16-00:41:48.616507
204.188.170.90:1921 -> 170.129.237.240:8080 TCP TTL:113 TOS:0x0
ID:54971 IpLen:20 DgmLen:48 DF
******S* Seq: 0x30D373E  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] [1:618:5] SCAN Squid Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/14-16:00:56.996507
66.159.18.66:43518 -> 170.129.50.120:3128 TCP TTL:53 TOS:0x0
```

```
ID:50174 IpLen:20 DgmLen:60 DF
******S* Seq: 0xBF3AC0C  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 48656370 0 NOP WS: 0

[**] [1:618:5] SCAN Squid Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/14-23:32:20.916507
66.159.18.49:55991 -> 170.129.50.120:3128 TCP TTL:52 TOS:0x0
ID:16353 IpLen:20 DgmLen:60 DF
******S* Seq: 0xB4E1FC5B  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 51364794 0 NOP WS: 0

Cluster 2/2 (sc: 17)
-------------------

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/16-00:41:51.536507
204.188.170.90:1921 -> 170.129.237.240:8080 TCP TTL:113 TOS:0x0
ID:57787 IpLen:20 DgmLen:48 DF
******S* Seq: 0x30D373E  Ack: 0x0  Win: 0x2000  TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

[**] [1:620:6] SCAN Proxy Port 8080 attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/14-16:00:56.996507
66.159.18.66:43517 -> 170.129.50.120:8080 TCP TTL:53 TOS:0x0
ID:59575 IpLen:20 DgmLen:60 DF
******S* Seq: 0xBED8745  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 48656370 0 NOP WS: 0

[**] [1:618:5] SCAN Squid Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-06:59:47.096507
216.201.160.235:44394 -> 170.129.161.213:3128 TCP TTL:46 TOS:0x0
ID:52069 IpLen:20 DgmLen:60 DF
******S* Seq: 0x4EE97664  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 17303918 0 NOP WS: 0

[**] [1:618:5] SCAN Squid Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-06:59:50.126507
216.201.160.235:44394 -> 170.129.161.213:3128 TCP TTL:46 TOS:0x0
ID:52140 IpLen:20 DgmLen:60 DF
******S* Seq: 0x4EE97664  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 17304218 0 NOP WS: 0

[**] [1:618:5] SCAN Squid Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-06:59:56.076507
216.201.160.235:44394 -> 170.129.161.213:3128 TCP TTL:46 TOS:0x0
ID:52202 IpLen:20 DgmLen:60 DF
******S* Seq: 0x4EE97664  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 17304818 0 NOP WS: 0

[**] [1:618:5] SCAN Squid Proxy attempt [**] [Classification:
Attempted Information Leak] [Priority: 2] 11/15-07:00:08.046507
216.201.160.235:44394 -> 170.129.161.213:3128 TCP TTL:46 TOS:0x0
ID:52420 IpLen:20 DgmLen:60 DF
******S* Seq: 0x4EE97664  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 17306018 0 NOP WS: 0

Supercluster 18/18
------------------

Cluster 1/2 (sc: 18)
-------------------

[**] [116:46:1] (snort_decoder) WARNING: TCP Data Offset is less
than 5! [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] 11/10-05:38:56.936507 62.13.27.29:0 -> 207.166.25.86:0
TCP TTL:234 TOS:0x0 ID:0 IpLen:20 DgmLen:40
*****R** Seq: 0xA02C678  Ack: 0xA02C678  Win: 0x0  TcpLen: 8

Cluster 2/2 (sc: 18)
-------------------

[**] [116:97:1] (snort_decoder): Short UDP packet, length field >
payload length [**] [Classification: Potential Corporate Privacy
Violation] [Priority: 1] 11/11-13:29:54.796507 211.194.68.39:0 ->
207.166.72.218:0 UDP TTL:109 TOS:0x0 ID:2062 IpLen:20 DgmLen:78 Len:
129
```

Distribution list

DRDC Ottawa TM 2006-193

Internal distribution

4 Author

1 Section Display

4 Library electronic

1 electronic Marc Grégoire

Total internal copies: 10

External distribution

1 Assistant Deputy Minister S&T (ADM S&T) (for distribution)

1 Director S&T for Command and Control Information Systems (DSTCCIS) electronic

1 electronic Director R&D Knowledge and Information Management (DRDKIM-2)

1 Maj. Kent Schramm (NO&SCFNOC), CFS Leitrim, 101 Colonel By Dr., Ottawa, ON K1A 0Z4

1 CFNOC CIRT Team Leader,CFS Leitrim, 101 Colonel By Dr., Ottawa, ON K1A 0Z4

1 Ted Bennett (CSE), Manager, Cyber Defence Futures, Edward Drake Building, 1500 Bronson Ave. Ottawa, ON K1G 3Z4

1 Luc Dandurand (CSE) Cyber Defence Futures, Edward Drake Building, 1500 Bronson Ave. Ottawa, ON K1G 3Z4

1 David Whyte (CSE)SIGINT, Sir Leonard Tilley Building, 719 Heron Road, Ottawa, ON K1A 0K2

1 Paul Van Oorschot, Canada Research Chair (Network and Software Security), Carleton University, 1125 Colonel By Drive Ottawa, ON K1S 5B6

1 Carlisle Adams, SITE, University of Ottawa, 800 King Edward Avenue Ottawa, ON K1N 6N5

2 Library and Archives Canada

1 CISTI

Total external copies: 13

Total copies: 23

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada – Ottawa
3701 Carling Avenue, Ottawa, Ontario, Canada
K1A 0Z4

2. SECURITY CLASSIFICATION (overall security classification of the document including special warning terms if applicable).

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C,R or U) in parentheses after the title).

Network Event Correlation Using Unsupervised Machine Learning Algorithms

4. AUTHORS (last name, first name, middle initial)

Dondo, M.; Mason, P.; Japkowicz, N.; Smith, R.

5. DATE OF PUBLICATION (month and year of publication of document)	6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc).	6b. NO. OF REFS (total cited in document)
November 2006	102	43

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered).

Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include address).

Defence R&D Canada – Ottawa
3701 Carling Avenue, Ottawa, Ontario, Canada K1A 0Z4

9a. PROJECT NO. (the applicable research and development project number under which the document was written. Specify whether project).	9b. GRANT OR CONTRACT NO. (if appropriate, the applicable number under which the document was written).
15BF29	

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique.)	10b. OTHER DOCUMENT NOs. (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC Ottawa TM 2006-193	

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
( ) Defence departments and defence contractors; further distribution only as approved
( ) Defence departments and Canadian defence contractors; further distribution only as approved
( ) Government departments and agencies; further distribution only as approved
( ) Defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution beyond the audience specified in (11) is possible, a wider announcement audience may be selected).

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

We have successfully implemented a two-stage event correlation model for IDS alerts. The model is designed to automate alert and incidents management and reduce the workload on an IDS analyst. We achieve this correlation by clustering similar alerts together, thus allowing the analyst to only look at a few clusters instead of hundreds or thousands of alerts. The first stage of this model uses an ANN-based autoassociator. The autoassociator is trained to reproduce each alert at its output, and it uses the error metric between its input and output to cluster similar alerts together. The accuracy of the system is improved by adding another machine-learning stage which attempts to combine closely related clusters produced by the first stage into super-clusters. The second stage uses the EM clustering algorithm. The model and performance of this model are tested with intrusion alerts generated by a Snort IDS on DARPA's 1999 IDS evaluation data as well as `incidents.org` alerts.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title).

Neural Network, Intrusion Detection System, Network Event Correlation, Alert Correlation, Autoassociator

Defence R&D Canada

Canada's leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

www.drdc-rddc.gc.ca