AFRL-RI-RS-TR-2013-070

WIRELESS ACCESS POINT TREASURE HUNT ORGANIZATIONAL METHODOLOGY

MARCH 2013

INTERIM TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2013-070 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/ S /

E. PAUL RATAZZI
Work Unit Manager

/ S /

WARREN H. DEBANY, JR.
Technical Advisor, Information
Exploitation & Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
MARCH 2013	INTERIM TECHNICAL REPORT	JAN 2010 – AUG 2010

4. TITLE AND SUBTITLE

WIRELESS ACCESS POINT TREASURE HUNT ORGANIZATIONAL METHODOLOGY

5a. CONTRACT NUMBER
IN-HOUSE

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
62788F

6. AUTHOR(S)
Sonja Glumich

5d. PROJECT NUMBER
GAIH

5e. TASK NUMBER
CY

5f. WORK UNIT NUMBER
BR

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site/RIGA
525 Brooks Road
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site/RIGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TR-2013-070

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. PA# 88ABW-2011-3665
Date Cleared: 27 JUN 2011

13. SUPPLEMENTARY NOTES

14. ABSTRACT

During the Wireless Access Point (WAP) Treasure Hunt, student teams of three engaged in wardriving across a small city to locate a series of time-constrained challenges. Wardriving entails utilizing a vehicle and a portable computing device to search a geographic area for a wireless network. Students used network detector software such as NetStumbler and Kismet to locate exercise WAPs and challenges temporarily dispersed by instructors. The Treasure Hunt challenges included completing a cryptography problem and circuit worksheet, discovering a WAP password vulnerability, conducting a forensics analysis on a thumb drive, exploring authentication on a website, identifying file, database, and mail server misconfigurations, and testing a WEP key. The exercise culminated with a final challenge at a bowling alley where students found the "treasure", a cellophane package of silver and gold chocolate candies and a surprise pizza and bowling party.

15. SUBJECT TERMS
Wireless access point hunt, wardriving, cyber education, cyber training

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**PAUL RATAZZI**
U	U	U	UU	13	19b. TELEPHONE NUMBER (*Include area code*) **N/A**

1. Introduction

1.1 Document Purpose

The purpose of this document is to describe the Wireless Access Point (WAP) Treasure Hunt organizational methodology developed and tested over three years by instructors from the Air Force Research Laboratory. This document focuses on the organizational aspects of exercise as opposed to the technical challenges completed by the students. The WAP Treasure Hunt held in 2009 serves as the example for this document, where eight student teams named Alpha, Bravo, Charlie, Delta, Echo, Foxtrot, Golf, and Hotel and 15 staff members worked together to achieve a successful exercise.

1.2 WAP Treasure Hunt Description

During the Wireless Access Point (WAP) Treasure Hunt, student teams of three engaged in wardriving across a small city to locate a series of time-constrained challenges. Wardriving entails utilizing a vehicle and a portable computing device to search a geographic area for a wireless network. Students used network detector software such as NetStumbler and Kismet to locate exercise WAPs and challenges temporarily dispersed by instructors. The Treasure Hunt challenges included completing a cryptography problem and circuit worksheet, discovering a WAP password vulnerability, conducting a forensics analysis on a thumb drive, exploring authentication on a website, identifying file, database, and mail server misconfigurations, and testing a WEP key. The exercise culminated with a final challenge at a bowling alley where students found the "treasure", a cellophane package of silver and gold chocolate candies and a surprise pizza and bowling party. For additional details regarding the technical challenges held at each site, please see [1].

The WAP Treasure Hunt exercise lasted approximately five hours and required 15 staff members to drive eight teams and manage seven challenge sites. Instructors selected challenge site locations based on the availability of power for the WAPs. Site locations should also be far enough apart so their associated WAP signals don't overlap. The challenge sites included the following:

1. **Initial 448 Site (4)**: Instructors introduced students to the exercise. Students completed a cryptography and circuit diagram challenge. (No WAP)
2. **Yard Site (Y)**: The 'Davy Jones' Locker' site for teams choosing the wrong map at the initial 448 site. Students answered a set of penalty questions. (No WAP)
3. **Larry Site (L):** Students completed the file, database, and mail server misconfiguration challenge. (WAP)
4. **Sonja Site (S):** Students accomplished the website authentication challenge. (WAP)
5. **TJ Site (T):** Students engaged in the WAP authentication challenge. (WAP)
6. **GI Site (G):** Students completed the forensics challenge. (WAP)
7. **Final Bowling Alley Site (B):** Students engaged in the WEP key test challenge. (No WAP)

2. Site Path

As shown in Table 1 below, teams Alpha through Hotel all started at challenge site 4 (448) and ended at challenge site B (Bowling Alley). Instructors generated a unique path of intermediary challenge site visits for each team (Larry, Sonja, TJ, and GI). Although a unique ordering is desirable, it may not always be possible depending on the number of teams and stops. Instructors also assigned each team a ribbon color. For example, instructors assigned the ribbon color black to team Alpha and blue to team Bravo.

Table 1: Team Paths and Ribbon Colors

Team	Path	Scroll Ribbon Color
Alpha	4LGTSB	Alpha = Black
Bravo	4GLSTB	Bravo = Blue
Charlie	4LTGSB	Charlie = Green
Delta	4TLSGB	Delta = Purple
Echo	4STGLB	Echo = Orange
Foxtrot	4TSLGB	Foxtrot = Red
Golf	4SGTLB	Golf = Yellow
Hotel	4GSLTB	Hotel = White

3. Map Scrolls

Instructors created two types of maps (see examples in section 5), rolled them into scrolls, and secured them with colored ribbon. To mimic an aged color, instructors soaked the maps in black chai tea, crumpled them, let them dry, and then rubbed them with vegetable oil. The map for WAP sites denoted the search area with a red box and included the SSID of the WAP of interest. The intermediary sites Sonja, Larry, TJ, and GI required this map type. The map for non-WAP sites directly marked the location of a specific site ('X' marks the spot). The initial site 448 and the final Bowling site necessitated this type of map. For seven sites and eight teams, instructors created a total of 88 map scrolls.

To guide scroll creation, instructors created a comprehensive list of scrolls indicating the total number of maps needed of each site and their associated ribbon colors. For example, instructors created a total of 40 map scrolls leading to the Yard penalty site and tied five with black ribbons, five with blue ribbons, etc. See below Table 2 listing all scrolls required for the exercise.

Table 2: Comprehensive List of Map Scrolls and Ribbon Colors

Site	Total Scrolls Needed at the Site and Their Ribbon Colors
Yard	5 each Black, Blue, Green, Purple, Orange, Red, Yellow, White
Larry	2 Black, 2 Green, 1 each Blue, Purple, Orange, Red, Yellow, White
Sonja	2 Orange, 2 Yellow, 1 each Black, Blue, Green, Purple, Red, White
TJ	2 Red, 2 Purple, 1 each Black, Blue, Green, Orange, Yellow, White
GI	2 Blue, 2 White, 1 each Black, Green, Purple, Orange, Red, Yellow
Bowling	1 each Black, Blue, Green, Purple, Orange, Red, Yellow, White

After creating the scrolls and tying them with ribbon, instructors divided the scrolls into bags according to challenge site. The scrolls required at the initial 448 site were further subdivided by team as displayed in Table 3 below:

Table 3: Map Scrolls and Ribbon Colors Required at Initial Site 448

Team	Scrolls Needed	
Alpha	Larry Black	Yard Blue, Green, Purple, Orange, Red
Bravo	GI Blue	Yard Green, Purple, Orange, Red, Yellow
Charlie	Larry Green	Yard Purple, Orange, Red, Yellow, White
Delta	TJ Purple	Yard Orange, Red, Yellow, White, Black
Echo	Sonja Orange	Yard Red, Yellow, White, Black, Blue
Foxtrot	TJ Red	Yard Yellow, White, Black, Blue, Green
Golf	Sonja Yellow	Yard White, Black, Blue, Green, Purple
Hotel	GI White	Yard Black, Blue, Green, Purple Orange

For team Alpha, the scroll tied with the black ribbon was the correct scroll leading to the next challenge at site Larry. All other scrolls (blue, green, purple, orange, and red) led teams to the penalty Yard site. For team Bravo, the blue scroll was correct and led to the next challenge at site GI. The green, purple, orange, red, and yellow scrolls all led to the penalty site. Specifying different colored correct scrolls for different teams reduced the risk of students being influenced by the color choices of other teams.

Intermediary sites such as Larry required one scroll per team which directed each team to the next challenge site (see Table 4). For instance, team Alpha required a map to the GI challenge site tied with a black ribbon and team Bravo required a map to the Sonja challenge site tied with a blue ribbon. Instructors created similar tables for intermediary sites Sonja, TJ, and GI. Site Bowling required no scrolls since it was the final stop.

Table 4: Map Scrolls and Ribbon Colors Required at Site Larry

Location	Team	Scrolls Needed
Larry	Alpha (Black)	GI
	Bravo (Blue)	Sonja
	Charlie (Green)	TJ
	Delta (Purple)	GI
	Echo (Orange)	TJ
	Foxtrot (Red)	Larry
	Golf (Yellow)	GI
	Hotel (White)	Larry

4. Handouts

4.1 Student Instructions

Treasure Hunt Instructions

Your team possesses six scrolls, each secured with a different colored ribbon. Solve the logic problem to identify the ribbon color of the true treasure map. Do not touch any of the scrolls until you double check your math, for touching one means you have selected it as your treasure map and the others will "disappear". Fyodor help you if you pick the wrong one and go to the wrong location!

There are two types of maps. The first directly marks the next point (X marks the spot). In this case, please proceed directly to the location to receive additional instructions. The second type has a red box indicating a subarea of the city containing the wireless access point (WAP) and the SSID of the WAP. When you locate the WAP with the appropriate SSID, ask your driver for authorization to connect. After your driver grants you permission, examine the wireless network to find the passphrase. Upon retrieval, speak the passphrase to the site attendant at the WAP. If the passphrase is correct, the attendant will hand you the next map. Continue this process until you reach the treasure.

To stay on schedule, there exists a time deadline for each stage. Your team earns 100 points for each passphrase recovered before the deadline. If the deadline passes, your team discontinues the current challenge, losing any associated points, receives the next map from the site attendant, and immediately proceeds to the next stage. For instance, at the initial site your team must finish by 1415 or lose the points associated with the logic problem. After your team leaves the initial site, you have until 1500 to find the second site, examine the wireless network to find the passphrase, and provide the passphrase to the WAP guardian.

The team who earns the most points wins the exercise. In the event that two or more teams complete all challenge sites within the time limits, instructors will determine the winner based on overall order of finish.

Please remember to download any online software tools (e.g. wireless, forensics) or references you need before leaving the initial site.

4.2 Code of Conduct

- Students may not drive their own cars. Please do not distract your assigned driver. We value our pieces of eight and refuse to equip you with a peg leg or an eye patch.
- Students must complete the challenges without the assistance of their driver.
- Receive permission from your driver before connecting to the WAPs associated with the exercise.
- Be mindful of the people and property you encounter during the hunt.
- You may only use Internet access at the initial site. Download any required software tools and reference materials at that time.
- GPS receivers or other equipment other than your laptop are prohibited.
- Leave values on systems at the challenge sites unchanged.
- Be discreet - don't help the other teams by loudly discussing where you have been or where you are headed at the challenge sites.

4.3 Sample Driver Instructions

Addresses:
4=448
Y=Rome City Yard, 132 Race St (no SSID)
L=Larry, <address>, SSID 7337parrot
S=Sonja, <address>, SSID mehearty
T=TJ, <address>, SSID landlubberly
G=GI, 725 Daedalian Drive, SSID Squiffy
B=Bowling Alley, 7157 East Dominick St (no SSID)

Correct Location Order (Math problem correct):
4LGTSB

Alternative Location Order (Math problem incorrect):
4YLGTSB

Ken Check-in?	Completed in Time?	
	☐	**Location A: 448** **1300-1330 Introduction, Code of Conduct, Questions** **1330-1415 Cadets work to solve problem and select correct map** **1415 Deadline for initial map selection**
☐	☐	**Location B** **1500 Deadline, proceed directly to AP, passphrase revealed and points lost**
☐	☐	**Location C** **1545 Deadline, proceed directly to AP, passphrase revealed and points lost**
☐	☐	**Location D** **1630 Deadline, proceed directly to AP, passphrase revealed and points lost**
☐	☐	**Location E** **1715 Deadline, proceed directly to AP, passphrase revealed and points lost**
☐	☐	**Location F: Bowling Alley** **1800 Deadline**

Please check off the boxes for the locations where the team solved the problem and issued the password in time.

Please return this form to Sonja at the bowling alley.

4.4 Sample Attendant Instructions

Sonja Access Point Attendant Instructions

Address:

Sonja Site	<address>
Bowling	7157 East Dominick St

Order of Visits:

Team	Path	Team	Path
Alpha	4LGTSB	Echo	4STGLB
Bravo	4GLSTB	Foxtrot	4TSLGB
Charlie	4LTGSB	Golf	4SGTLB
Delta	4TLSGB	Hotel	4GSLTB

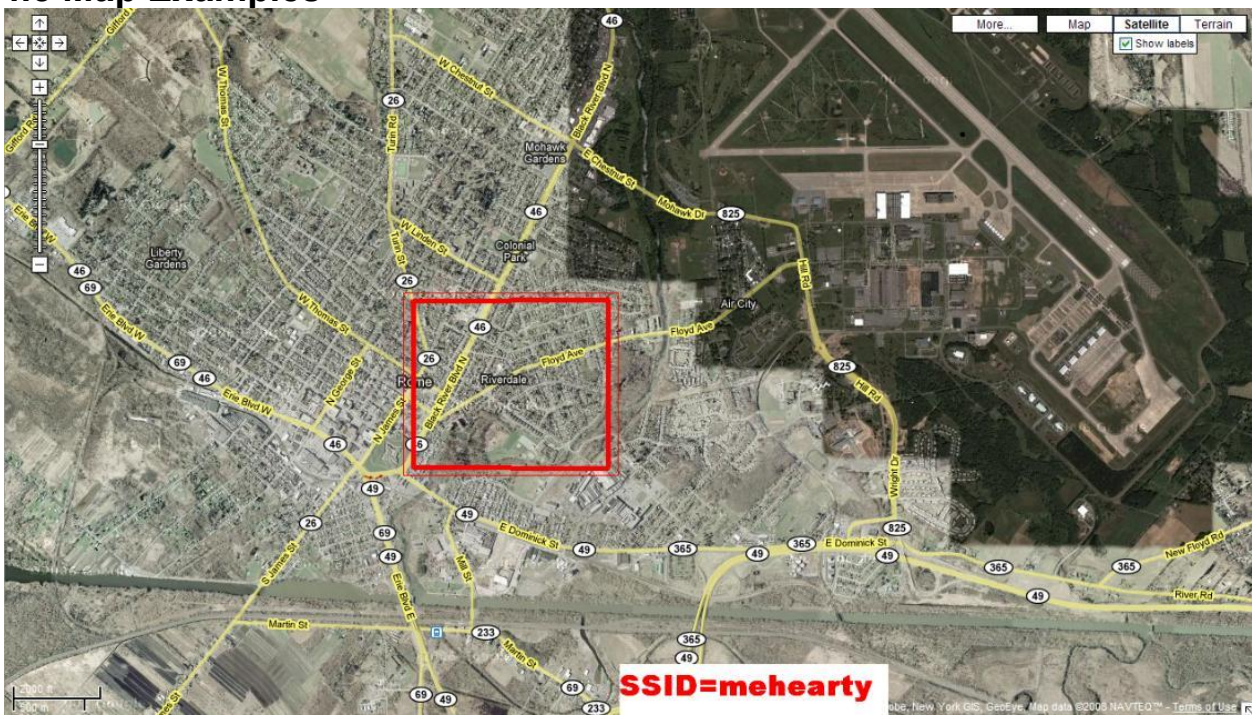
Ribbon Color: Alpha = Black, Bravo = Blue, Charlie = Green, Delta = Purple, Echo = Orange, Foxtrot = Red, Golf=Yellow, Hotel=White

Location A: 448
1300-1330 Introduction, Code of Conduct, Questions
1330-1415 Students work to solve problem and select correct map
1415 Deadline for initial map selection, passphrase revealed and points lost
Location B
1500 Deadline, proceed to next site, passphrase revealed and points lost
Location C
1545 Deadline, proceed to next site, passphrase revealed and points lost
Location D
1630 Deadline, proceed to next site, passphrase revealed and points lost
Location E
1715 Deadline, proceed to next site, passphrase revealed and points lost
Location F: Bowling Alley
1800 Deadline

Special Instructions:

SSID	mehearty
WAP address	192.168.0.30
Passphrase	“The crux of the biscuit is the apostrophe”

4.5 Map Examples



Google Maps Satellite Image of a Challenge Site [2]

Google Maps Satellite Image of "Davy Jones' Locker" Penalty Site [2]

5. References

[1] S. Glumich and B. Kropa, The 2011 World Congress in Computer Science Computer Engineering and Applied Computing. “DefEX: Hands-On Cyber Defense Exercises for Undergraduate Students”, Las Vegas, NV, 2011; ID: SAM5055.

[2] Google Maps Application. [Online]. Available: http://maps.google.com/