Unfolding an Investigation using Forensic Tools and Techniques

Leena Arora

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-1172

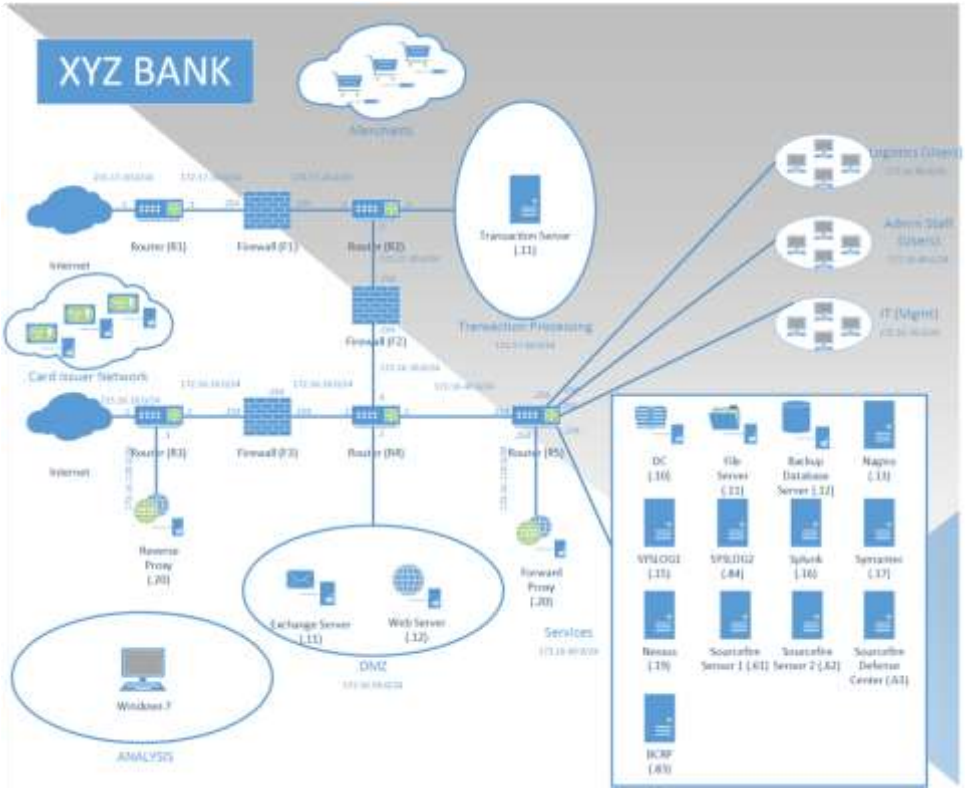
Objectives

- Conduct memory and hard drive analysis
- Familiarize with forensic analysis tools and techniques

Scenario

You are a group of Forensic Analysts called at XYZ Bank. You're tasked to conduct forensic analysis of the systems involved in the incident.

XYZ Bank Topology



Tools Available

- Autopsy
- Volatility
- Registry Explorer
- Strings
- Others..

Evidence Available

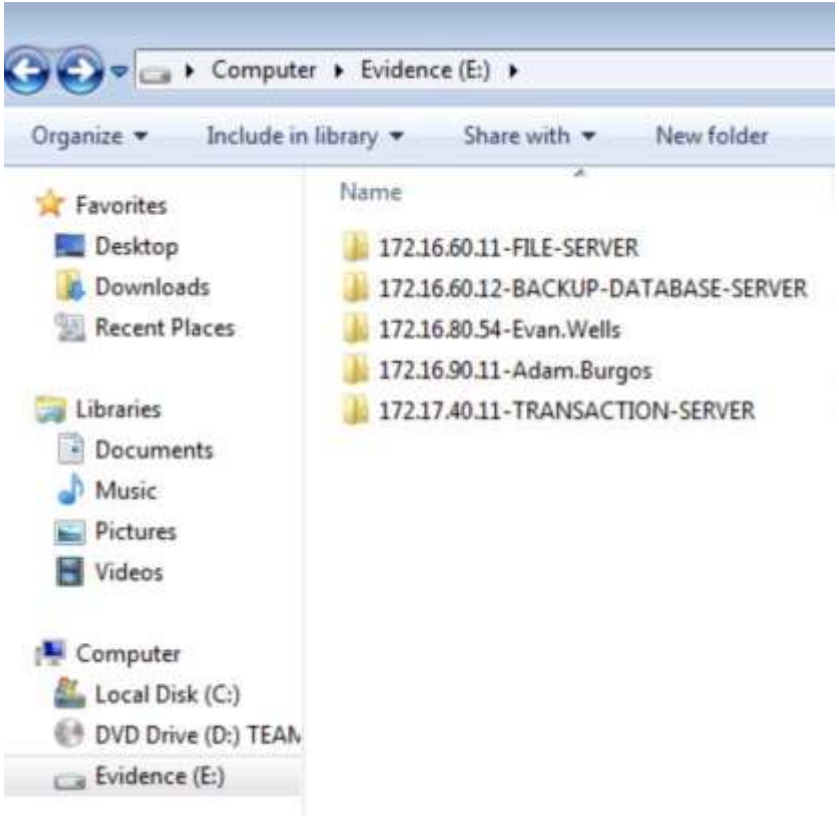
Adam.Burgos user system
- Memory image – Adam-Burgos.mem
- Hard Drive image – Adam-Burgos.001

Evan.Wells user system
- Memory image – Evan-Wells.mem
- Hard Drive image – Evan-Wells.001

File Server
- Memory image – file-server.mem
- Hard Drive image – file-server.001

Backup Database Server
- Memory image – backup-database.mem

Transaction Server
- Hard Drive image – transaction-server.dd



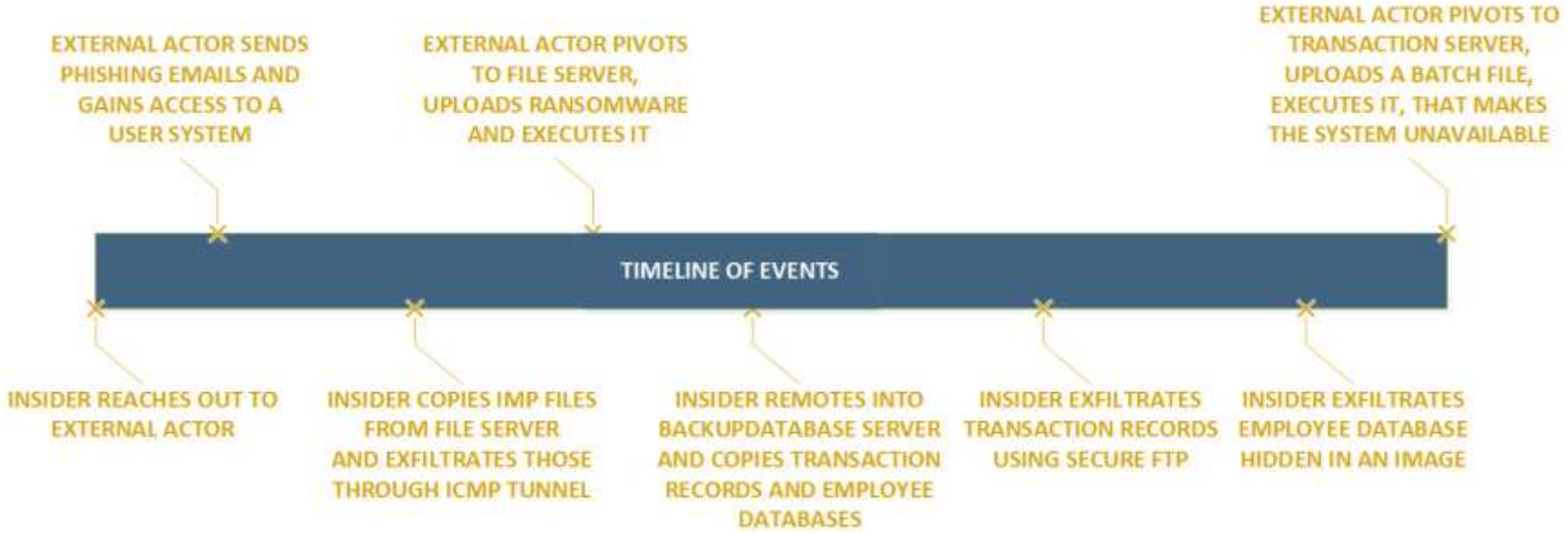
STEPfwd

URL - https://stepfwd.cert.org/lms

Username –

Password –

Timeline



Some more details

Insider

- Adam Burgos (172.16.90.11)

Victim of phishing email

- Evan Wells (172.16.80.54)

Other systems involved in the incident

- File Server (172.16.60.11)
- Backup Database Server (172.16.60.12)
- Transaction Server (172.17.40.11)

External IPs

46.236.64.10

- Had command line access to
  - Evan.Wells user system
  - File Server
  - Transaction server

46.236.64.15

- Used for chat between insider and external actor
- Used by insider to download hping and psexec.exe

External IPs

56.34.125.100

- Used by insider to upload transaction records

56.34.125.200

- Used by insider to upload
  - File server documents
  - Transaction records

Detailed Timeline -1

Chat	Actor	Event Description/Chat Message
	Insider	Uses netcat to connect to his friend's (External Actor) chat server at port 21
Insider -> External		Hey, what's up buddy?
External -> Insider		Hey man!
Insider -> External		Looks like I am gonna get fired soon! I want to bring this company down before I go down. Help me out…..
External -> Insider		On it buddy. Send a few email addresses.
Insider -> External		Here you go – Evan.Wells@xyz.com, Harry.Scanlon, Jeff.Smalls, Noah.Short, Ericka.Welch, Ingrid.Butts, Cayla.Lantz, Marlene.Dailey
External -> Insider		Got it
	External	Sends phishing emails. Victim (Evan Wells) clicks on the link and gets compromised
External -> Insider		Got a phish! Preparing ransomware
	External	Enumerates system info, migrates to svchost.exe, escalates privileges, dumps contents of SAM database
	Insider	Connects to File server, copies important company docs to his system
	Insider	Downloads hping
	Insider	Uses hping to exfiltrate important company docs in an ICMP tunnel
Insider -> External		Awesome!!!!!!! Run it on 172.16.60.11… That has all the imp company docs…
External-> Insider		On it!

Detailed Timeline -2

Chat	Actor	Event Description/Chat Message
Insider -> External		Its a win 2012r2 64 bit
	External	Pivots to file server using pass the hash technique, uploads ransomware and executes it
External-> Insider		That was a piece of cake… All sett!
	Insider	Using zenmap executes a portscan against services and transaction subnets searching for systems responding to port 1433 and 3500
Insider -> External		Thanks buddy! Can you bring 172.17.40.11 offline
		Its also win 2012r2 64 bit
	Insider	Downloads psexec tool
	Insider	Uses psexec to remotely access Backup Database server
	Insider	Uses bcp utility to export employee records and transaction records from the database server and copy those off to his system
	Insider	Uses Filezilla and FTPS protocol to exfiltrate transaction records
	Insider	Attaches a USB, copies Quick Stego tool, and installs it
	Insider	Uses stego tool to hide employee records in an image
	Insider	Uploads image to an external website
	External	Pivots to transaction server using pass the hash technique again
	External	Uploads a batch file to startup folder and executes it. Batch file shutdown the transaction server
External-> Insider		All set man!
Insider -> External		Thanks man! Our work is done here! Will see you in the evening!

Questions