Incident Handling

35 Points–Partner Lab
Due Date: Lesson 24

1 Overview

In this practical exercise you will gain familiarity with the incident handling process by examining artifacts of a potential network security incident and making recommendations to network administrators to limit exposure to future incidents. You will draw on your experience in the other labs you've done so far to understand the operation of the servers you are trying to protect, the protocols they run, and content of the files you will analyze.

2 Lab Setup

You will only need a single VM for this lab. The packet captures and log files you will analyze in this exercise are listed below. You can move these files to your VM via thumb drive, share folders or Internet (i.e. DropBox, gmail, etc).

2.1 Files

firwewall rules.txt	Firewall rules on external network interface
partial DNS.log	Partial log file from DNS server at the time of the event
ftp server.log	Partial log file from FTP server
www-internal access.log	Partial access log file from internal web server
mysql query.log	Partial query log from SQL server running on internal web server

You may use any tools you would like to analyze these files. Remember that the logs will tell you what commands the various servers handled, but only the packet traces will show you whether the commands were successful and what data was transferred. Brushing up on Wireshark filters to help you narrow the set of packets you're examining for each task will be helpful:
`https://wiki.wireshark.org/DisplayFilters`

3 Scenerio

Your network consists of a DMZ hosting basic services such as DNS, HTTP, FTP, and SSH, along with a user subnet (see Figure 1, below). Network traffic is being captured on your router's DMZ interface doing full packet capture on the traffic going into and out of your DMZ subnet. There is a firewall on your network's inbound link and the firewall rules are included in your file set (*firewall rules.txt*).

You recently joined your organization's incident handling team. One of the network system administrators has noted anomalous traffic on the internal web server and has identified it as a "network event." You are on call and need to do an initial analysis of the data to determine whether the event should be classified as a

"network incident." Assuming an incident has occurred, you will also be asked to make recommendations to your organization for mitigating this incident and for improving the security of your network.

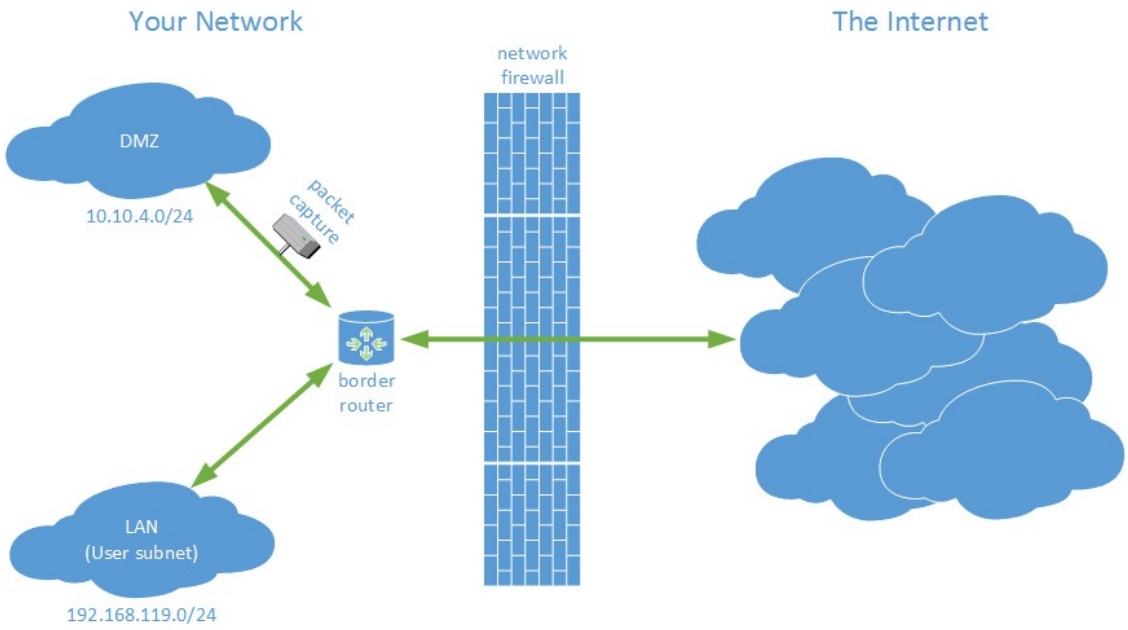

Figure 1: Organization Network Topology

Services that should be visible from the Internet are:

DMZ Server IP Address	Services
10.10.4.1	http, https
10.10.4.5	smtp
10.10.4.16	ssh, ftp
10.10.4.251	dns

Any other services listening on internal hosts are intended for use only on the internal networks (DMZ and LAN).

3.1 Phase 1: Preparation

Question 1: What tools will you use to analyze the network traffic and log files for this network event? List the tools (VMs and software) that you will use during your investigation and what each will be used for. You will likely update this list as you go through the lab.

3.2 Phase 2: Identification

Sysadmins inform you that the suspicious behavior on the web server came from an Internet host (external to our network) in the `172.16.2.0/24` subnet. Before we examine the web server traffic, we'll start with

an attacker's most likely initial target in our network, the DNS server.

In the *incident capture.pcap file*, inspect the initial few interactions between hosts in `172.16.2.0/24` network and our DNS server (at `10.10.4.251`).

Question 2:

1. What is the IP address of the host in the `172.16.2.0/24` subnet that accessed our DNS server?
2. What are the first three requests made from that host to our DNS server?
3. What information has the external host determined about our network that he/she might use during subsequent penetration attempts?
4. What is unusual about this interaction between an (external) Internet host and our DNS server?

Shortly after the DNS exchange, the attacker conducted a targeted port scan of DMZ hosts to try to find evidence of open ports that are not obvious from the DNS lookup.

Question 3: Which hosts were scanned?

Question 4: The attacker scanned the same group of ports on each server. Which ports did the attacker include in his/her scan of these hosts?

Question 5: Which ports did the attacker find open (which ports accepted connection attempts - Hint: look for evidence of a complete TCP 3-way handshake)?

Question 6: What is wrong with our firewall rules that allowed these scans to get to our DMZ network? (The firewall rules are provided in firewall rules.txt)

After the scan, the attacker's attention seems to have been focused on the FTP server and the web servers. The attacker was able to gain anonymous access to an FTP server. While anonymous login allows very limited access to the FTP server and does not allow file upload, the attacker was able to pull some useful information from the server that he/she might be able to use to facilitate intrusion into your network.

Question 7: What did the attacker do during his/her anonymous login? What information was the attacker able to get from the FTP server during the anonymous login (Hint: look at both the `ftp` and `ftp-data` traffic (tcp ports 20 and 21))?

The attacker didn't get much from the public facing web server at `www.iwar.itoc`; however, he/she seems to have been able to access to the internal web server at `www-internal.iwar.itoc`. Their activity there looks more interesting. This server contains a web page with backend database and the attacker spent some time on it. If you can correlate the data from the packet capture file, the web server access log, and the mysql query log, you can determine what the attacker was doing.

Question 8: What approach did the attacker take with the internal web server (what was he/she doing that could be considered malicious)? Give examples of the malicious behavior. (Hint: Don't forget the log files!)

Question 9: What information was the attacker able to gain from the internal web server that he/she could use in his/her continued attempts to compromise your network?

The attacker focuses their attention back on the FTP server and is able to log in with a valid user account.

Question 10: Which account does the attacker use to log in to the FTP server?

Question 11: what password does the attacker use to log on to the FTP server? Where did the attacker get that password?

Question 12: What files did the attacker attempt to GET from the FTP server? Which files did they successfully GET?

Question 13: The attacker placed some files on the FTP server. What are the names of the files the attacker tried to upload to the server? Which files did he/she successfully upload?

3.3 Phase 3: Containment

Your organization is using a stateless firewall on the inbound link to your company's network. The file `firewall rules.txt` contains your organization's current firewall configuration as implemented by one of the system administrators, Karl "lazyjoe" Moses-Hand.

Question 14: Should any rules be immediately applied to prevent further malicious activity from the suspected attacker? What should the new rule(s) be?

Action (ACCEPT/DROP)	**Transport Protocol**	**Source IP**	**Source port**	**Destination IP**	**Destination port**

Question 15: Are there any other actions that you would recommend to system administrators to contain the current event? (Your answer should be specific to the incident you are investigating.)

3.4 Phase 4: Eradication

Question 16: Is there evidence that the attacker put something on your system that will allow him or her to easily regain access? Explain. (Hint: What files did the attacker UPLOAD to your network and what might he/she be able to do with them?) What server would you check immediately to determine whether any unusual ports are open? Why?

Question 17: Assuming that you find evidence that one of your systems remains compromised after the attack, what actions do you recommend that system administrators take to remedy the compromise?

3.5 Phase 5: Recovery

In this phase we would put any systems taken off line for containment and eradication back on line, then confirm that they are available. You also want to monitor these systems for signs of subsequent compromise.

3.6 Phase 6: Lessons Learned and Recommendations

Question 18: What configuration changes must be made on our current DNS server to limit outsiders' access to detailed information about our network?

Question 19: The company is currently using a single DNS server to service both internal and external DNS requests. Assuming the company has sufficient resources to deploy a second DNS server, in what configuration should we deploy those servers to improve security? How is security improved by your rec- ommendation?

Question 20: What firewall rule changes do you recommend to provide better security to our DMZ? You need not provide a specific set of rules, but you should recommend a better approach for our firewall configuration (and provide enough guidance so your recommendations can be implemented).

Question 21: The only security-specific device in our network is a firewall. Are there any additional network devices that we could have placed in our network to alert systems administrators of potentially malicious activity on our network? How would such devices improve security?

Question 22: Are there any services on the network that should be turned off to better protect data in transit? What can those potentially insecure services be replaced with to provide better security?

Question 23: There seems to be a problem with the password policy on the network. You should have seen at least some passwords in the network traffic-what is wrong with them? What recommendations would you make with regard to password policy?

4 Submission requirements

4.1 Partner Submission

Provide one written lab report, answering each question properly labelled with the number and original question, per partner team. Be sure to include the time spent on the lab and document any external resources used. Again good documentation:

1. clearly enumerates tasks with a description of you did and evidence.
2. shows the progress you were able to achieve.
3. explains your troubleshooting attempts.
4. accurately describes an issue and the potential solution (if good, we will give near full credit).

4.2 Individual Submission

Each member needs to submit a detailed lab reflection. This includes

- approximately one half page that analyzes on the following statement:

  It is often asserted that in computer security the attacker has an easier mission than the defender. What are some of the advantages of the attacker and disadvantages of the defender that lend credibility to this statement?

- any challenging points or thoughts on what you found interesting during the lab
- time spent you personally spent and how much effort you put forth
- time your partner spent, and how much effort they put forth
- be sure document any external resources used.