Capstone Engagement

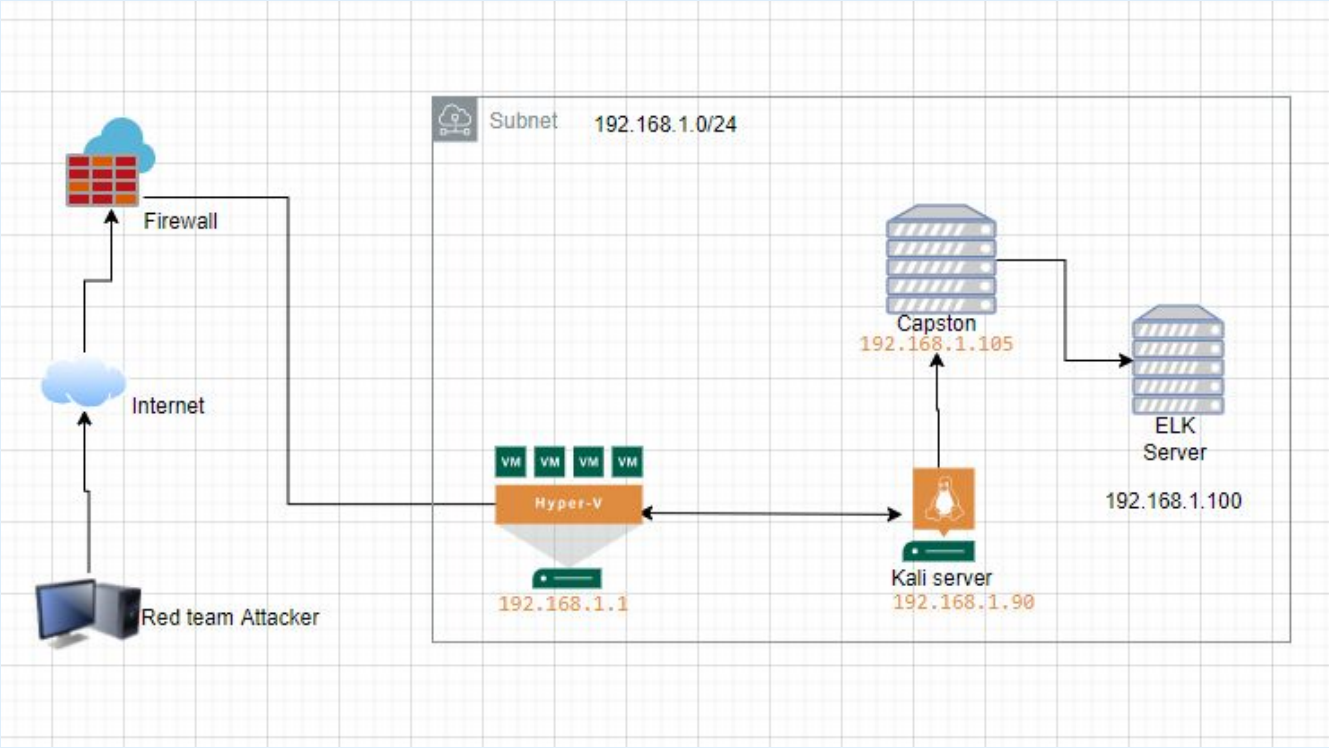
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address
Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway:192.168.1.1

Machines
IPv4: 192.168.1.100
OS: Linux
Hostname: **ELK**

IPv4: 192.168.1.90
OS: Linux
Hostname: **Kali**

IPv4: 192.168.1.105
OS: Linux
Hostname: **Capstone**

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`	Attacking Machine
Capstone	`192.168.1.10`	Target /Victim Machine
ELK	`192.168.1.100`	Collect Logs 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 are open in Victim Machine*	*TCP 80 allowed Red team attacker and explore HTML web page on Server*
Open Directory	Presence of secret folder which allows attacker to attack on web server	- Potential entities presence such as Personal dealing with secret folder
Data	Sensitive info in plain text file	Data could be understood well and simple English Laugage
Credentials (weak)	Easy password subjected to attack	Leopoldo, linux4u - easy password as brute force.

Exploitation: [Name of First Vulnerability]

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

02

Achievements

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

01

```
root@Kali:~# nmap -sT 192.168.1.100
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-04 16:44 PDT
Nmap scan report for 192.168.1.100
Host is up (0.00037s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
root@Kali:~# nmap sV 192.168.1.100
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-04 16:45 PDT
Failed to resolve "sV".
Nmap scan report for 192.168.1.100
Host is up (0.00058s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
root@Kali:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group d
efault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
```

02

```
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00053s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: el
asticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00051s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.52 seconds
root@Kali:~# ~~
```

Exploitation: [Name of Second Vulnerability]

01

Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

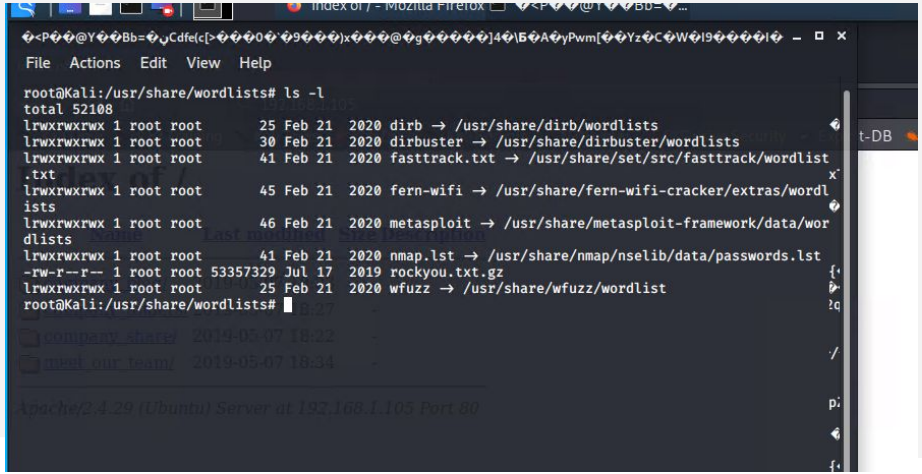
02

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

03

[INSERT: screenshot or command output illustrating the exploit.]

03



Exploitation: [Name of Third Vulnerability]

01

Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

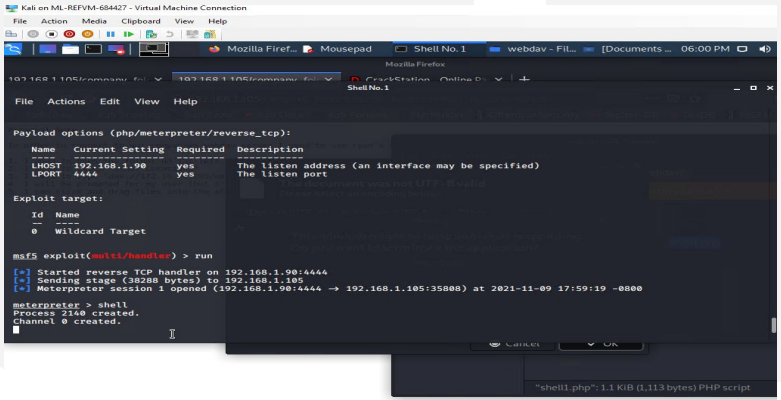
02

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

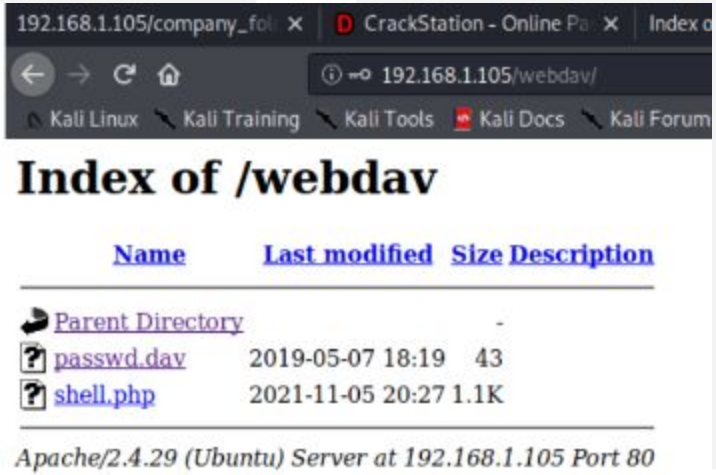
03

[INSERT: screenshot or command output illustrating the exploit.]

01



03



Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Traffic b/w Hosts

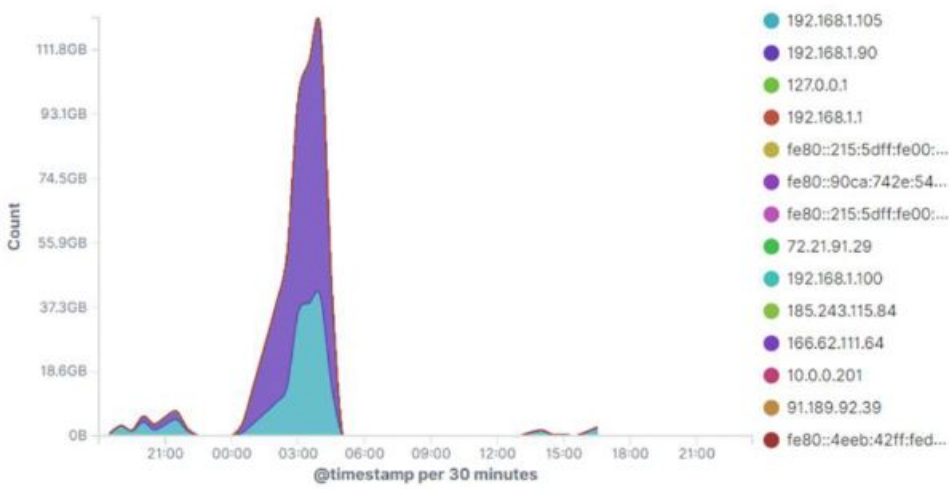
Network Traffic Between Hosts [Packetbeat Flows] ECS

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

Top Hosts Creating Traffic [Packetbeat Flows] ECS



- Port scan occurred at 7AM 2021-11-04
- 154.2 MB packets were sent from 192.168.1.90

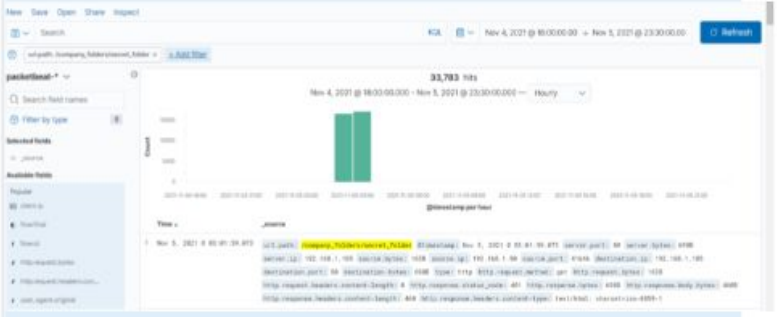
Analysis: Finding the Request for the Hidden Directory

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

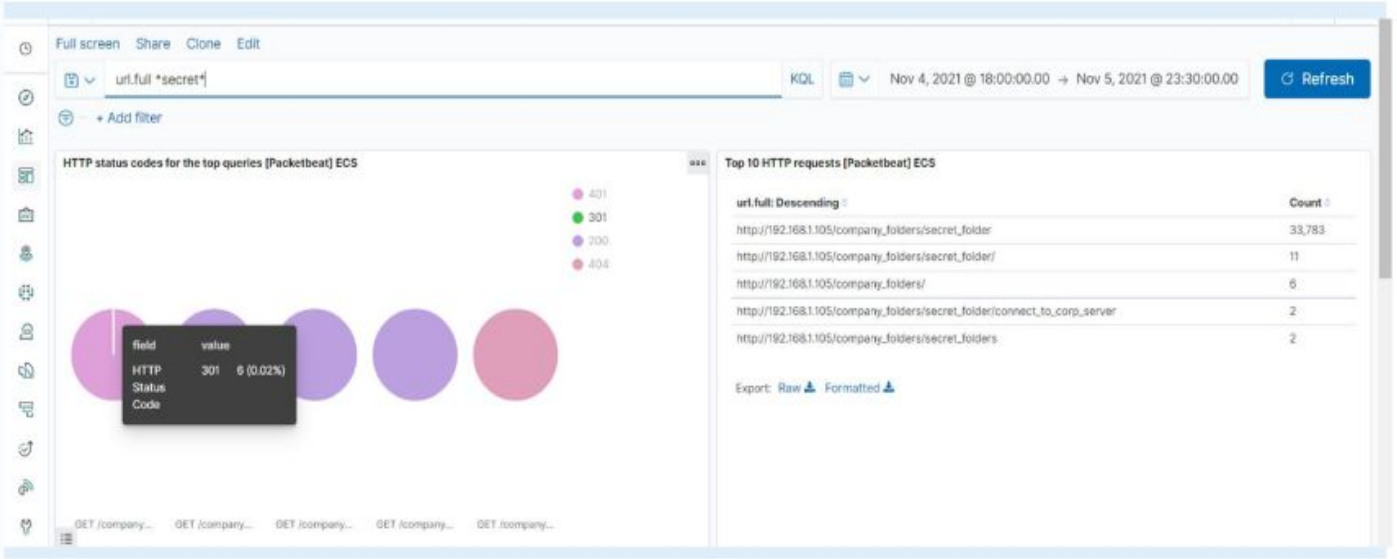
Export: Raw Formatted



- 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

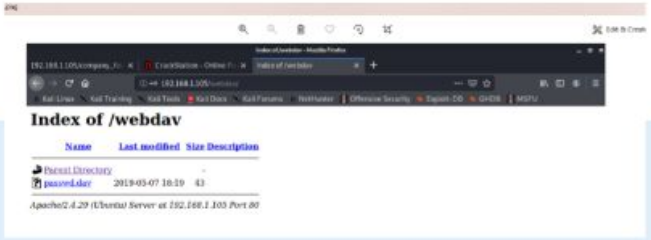
Full screen Share Clone Edit

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://bafildardavies.com/docs/article.php?c=123080&m=6491edf38d1a8b498bbca9cd7bd6bbaa&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-Vhq2RF82P9lr&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

Observation: No. of requested ports for each Source IP

Low thresh hold of 10-15 to maximum of 100+ set

System Hardening

- Firewall restricted to unauthorized access
- Inhouse scan should run periodically to find behavior of network, intrusion security detections
- Ports should stay closed, If not in use, so they should refrain from listening and responding to malicious traffic.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Set alarm for any machine that is attempted to access the directory which is hidden.

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

System Hardening

To block the unwanted access

- Files should be encrypted
- Directories should be encrypted
- Files/Directories not access to the public
- Thus should be removed from the server

Mitigation: Preventing Brute Force Attacks

Alarm

Alarms for the following:

- Multiple login attempts
- Hydra alarm should be set For use_agent_original

A threshold 3+ attempts

System Hardening

- Strong and complex passwords
- Regularly change passwords
- Avoid directory passwords
- For incorrect password attempts 3 times should be locked the account
- Multiple fail attempts could be block the IP and proxy IP
- Adding security questions
- Use Captcha

Mitigation: Detecting the WebDAV Connection

Alarm

Alarm for attempt unauthorized machine for any directory access.

Threshold should be set 1

System Hardening

- No access for shared folders should exit on web server
- Setup firewall rules to restrict the access,
- Monitor on regular basis to update

Mitigation: Identifying Reverse Shell Uploads

Alarm

Alarm for .php file whenever loaded on server

Alarm for incoming traffic on 4444 port

System Hardening

- Set up limitation for uploading files for particular extensions
- List of only permitted file extension on server
- Directories can be handled and removed if they are unauthorized and remove from server.
- Regular updates should be run on firewalls

the End