



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

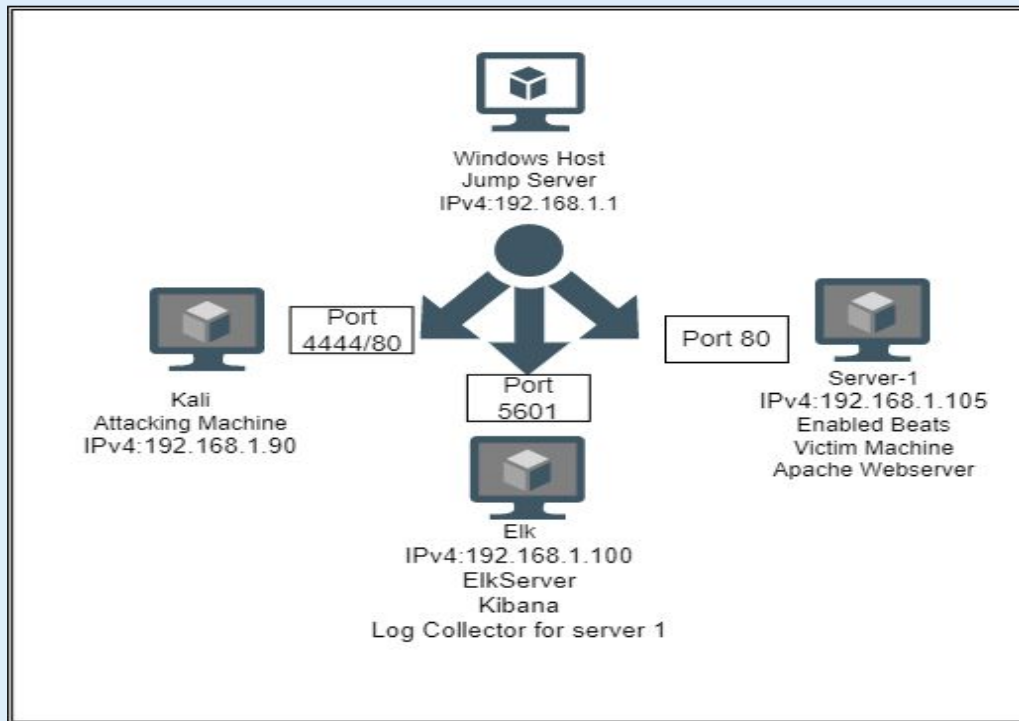
04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology

Capstone Engagement
Network
IP Range 192.168.1.0/24
Netmask 255.255.255.0



Network

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

Machines

IPv4:192.168.1.90
OS:kali
Hostname:Kali

IPv4:192.168.1.105
OS:Ubuntu 18.04.1 LTS
Hostname:server1

IPv4:192.168.1.100
OS:Linux
Hostname:Elk

IPv4:192.168.1.1
OS:Windows
Hostname:
ML-RefVm-684427

The background of the slide is a dark red, almost black, field filled with a complex, repeating geometric pattern of triangles and polygons in various shades of red and maroon, creating a textured, crystalline effect.

Red Team Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Machines Kali	IPv4:192.168.1.90	Attacking Machine
Server1	IPv4:192.168.1.105	Enabled beats to Elk server Apache Webserver (capstone) Victim machine
Elk	IPv4:192.168.1.100	Elk Server(Kibana) -Log Collector for server1
Windows Host	IPv4:192.168.1.1	Jump Server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Reverse Shell TCP	<i>Allows attacker to gain access to shell on victim's machine with equal privileges, lets attacker establish a meterpreter session.</i>	<i>You can access files, traverse directories, download content (screenshot, read/write, remote delete files, execute scripts, stop server).</i>
Weak Passwords	Easily found using password dictionary.	Puts computer and network at risk of being compromised.
Brute Force Login	Login to a password protected directory, by providing a variety of combination	Identity theft, install malware, loss of data, downtime
Port Scan	Used NMAP to scan open ports on the network.	This allowed me to find vulnerable ports so that I could further exploit.

Exploitation: Port Scan

01

Tools & Processes

In order to find IP address of the machine, I used Nmap to scan network.

02

Achievements

From Nmap we see that port 80 is open Apache Web Server. I typed IP address in web browser and located hidden directory.

03

```
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.83 seconds
root@kali:~# nmap -v 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-27 19:09 PST
Nmap scan report for 192.168.1.1
Host is up (0.0004s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp    open  rpcbind      2.x-4.x
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
2128/tcp   open  vnc?
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:15:5D:00:04:10 (Microsoft)
Service Info: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.0004s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Elasticsearch REST API 7.4.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address: 4C:18:42:02:10:07 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.0003s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache/2.4.29
MAC Address: 08:15:5D:00:04:10 (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.90
Host is up (0.000000s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.1p1 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 28.63 seconds
root@kali:~#
```


Exploitation: Brute Force

01

Tools & Processes

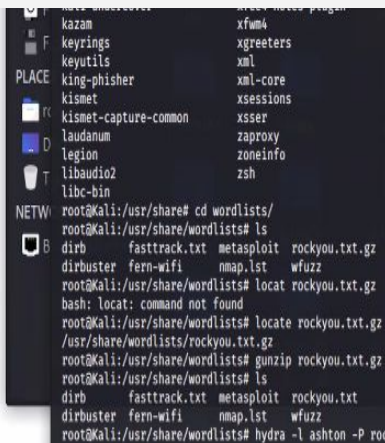
Used Hydra attack against directory.

02

Achievements

I was able to gain privileges through finding username "ashton" and password "leopoldo."

03



The screenshot shows a terminal window with the following content:

```
root@kali:~# cd /usr/share/wordlists/
root@kali:~# ls
dirb fasttrack.txt metasploit rockyou.txt.gz
dirbuster fern-wifi nmap.lst wfuzz
root@kali:~# locate rockyou.txt.gz
bash: locate: command not found
root@kali:~# locate rockyou.txt.gz
/usr/share/wordlists/rockyou.txt.gz
root@kali:~# gunzip rockyou.txt.gz
root@kali:~# ls
dirb fasttrack.txt metasploit rockyou.txt
dirbuster fern-wifi nmap.lst wfuzz
root@kali:~# hydra -l ashton -P rockyou.txt -s 80 -f -vV
```

- hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder

Exploitation: Reverse TCP

01

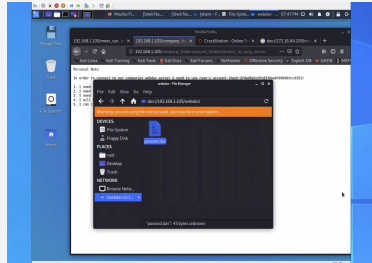
Tools & Processes

Using the newly acquired login credentials, I opened a file called "connecting_to_webdav." In that file I found username and a hashed password. Using CrackStation I solved the hash and gained the resulting password "linux4u." Next I connected to the VM's WebDAV directory and entered newly gained credentials.

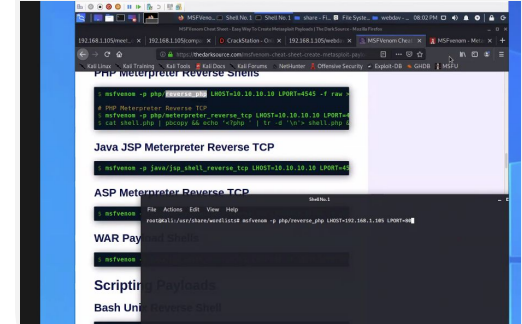
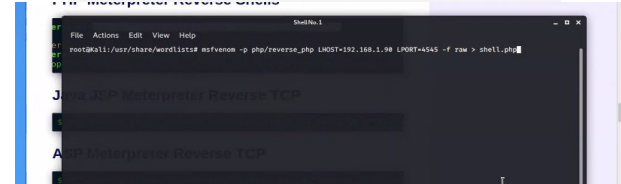
02

Achievements

Uploaded PHP reverse shell payload in order to set up a listener command on Meterpreter and uploaded PHP file to WebDAV directory.



03

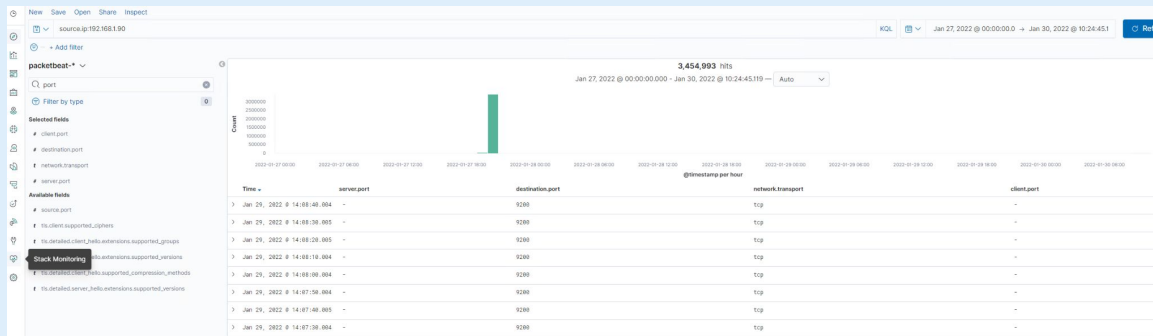




Blue Team

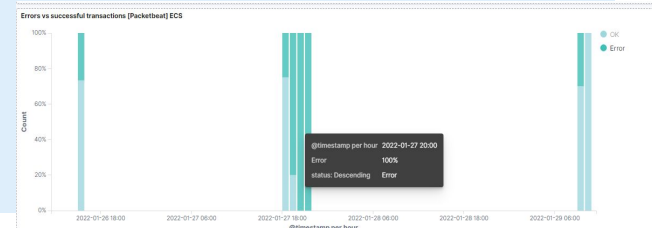
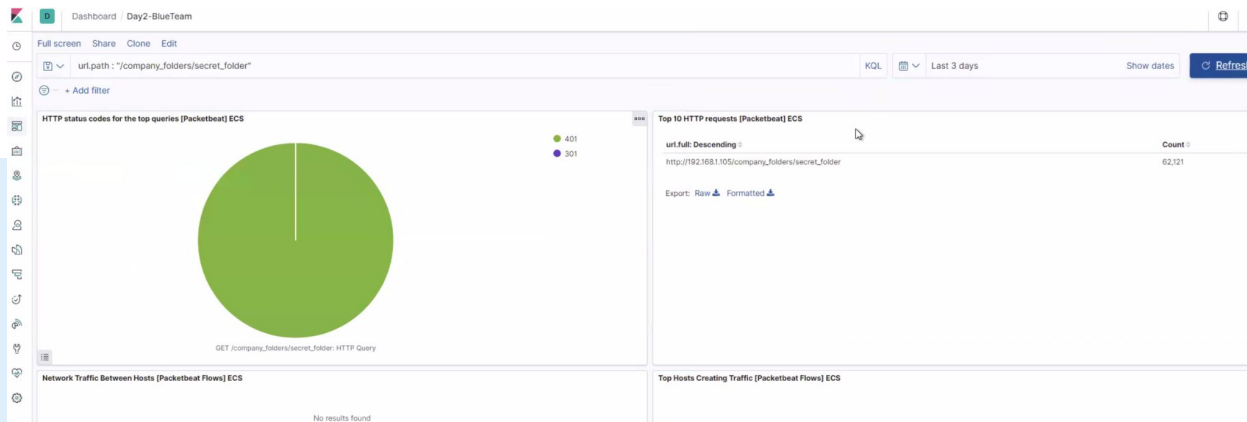
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- Port Scan occurred Jan 27, 2022
- Source IP 192.168.1.90
- The large quantity of scans in a short amount of time indicates an attack

Analysis: Finding the Request for the Hidden Directory



- 62,121 requests made at 13:20:13
- Secret_folder requested containing WebDAV access instructions

@timestamp

_id

_id.v

_score

_type

agent.ephemeral_id

agent.hostname

agent.id

agent.name

2022-01-28 12:00

2022-01-27 00:00

2022-01-27 06:00

2022-01-27 12:00

2022-01-27 18:00

2022-01-28 00:00

2022-01-28 06:00

2022-01-28 12:00

2022-01-28 18:00

2022-01-29 00:00

Time

Source

> Jan 29, 2022 @ 18:59:40.884

ecs.version: 1.5.8 event.category: network.traffic event.action: network_flow event.start: Jan 29, 2022 @ 08:32:56.111 event.end: Jan 29, 2022 @ 18:59:21.535 event.duration: 5185424.8 event.dataset: flow event.kind: event flow.family: false flow.id: CAT/1/AD/1/CPASAAaapfaagJyAaCM Types: flow network.bytes: 1.3MB network.packets: 2.1k network.type: ipv4 network.transport: tcp network.community_id: 1A817VhuqDQaP57Kx/UMWuHw agent.hostname: kali agent.ephemeral_id: a772c7b9-fc3b-4c3a-b914-c04d2495ac agent.id: 2444a6-c3b-40b-93af-bd9a-w350af agent.name: kali agent.type: packetbeat agent.version: 7.8.8 host.name: kali source.bytes: 1.1MB source.id: 192.168.1.190 source.port: 41772 source.packets: 1.1k destination.packets: 877 destination.bytes: 23.1MB destination.id: 192.168.1.190 destination.port: 8080 _id: nat3489agqg7y7v+_ _type: _doc _index: packetbeat-7.8.8-2022.01.28-000000 _source: -

> Jan 29, 2022 @ 18:59:30.085

timestamp: Jan 29, 2022 @ 18:59:30.085 network.type: ipv4 network.transport: tcp network.community_id: 1A817VhuqDQaP57Kx/UMWuHw network.bytes: 1.3MB network.packets: 2.1k destination.port: 8080 destination.bytes: 234.76k destination.id: 192.168.1.190 event.action: network_flow event.start: Jan 29, 2022 @ 08:32:56.111 event.end: Jan 29, 2022 @ 18:59:21.295 event.duration: 518163.8 event.dataset: flow event.kind: event event.category: network.traffic flow.id: CAT/1/AD/1/CPASAAaapfaagJyAaCM flow.family: false ecs.version: 1.5.8 host.name: kali agent.hostname: kali agent.ephemeral_id: a772c7b9-fc3b-4c3a-b914-c04d2495ac agent.id: 2444a6-c3b-40b-93af-bd9a-w350af agent.name: kali agent.type: packetbeat agent.version: 7.8.8 type: flow source.port: 41772 source.packets: 1.1k source.bytes: 1.1MB source.id: 192.168.1.190 _id: nat3489agqg7y7v+_ _type: _doc _index: packetbeat-7.8.8-2022.01.28-000000 _source: -

KQL

Jan 27, 2022 @ 00:00:00.0 -> Jan 27, 2022 @ 23:59:59

Refresh

HTTP status codes for the top queries [Packetbeat] ECS

field

value

401

469,523 (100%)

HTTP Status Code

401

301

200

204

GET /company/folders/secret_...

GET /server-status: HTTP Query

POST /post.php: HTTP Query

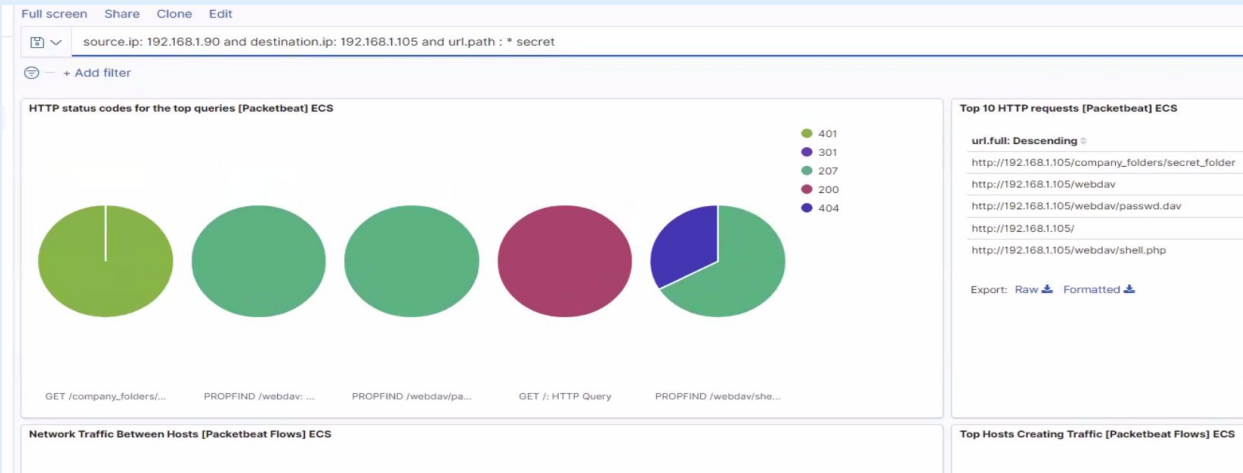
GET /p.media: HTTP Query

GET /generate_204: HTTP Query

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	469,523
http://192.168.1.105/webdav	2



- 2 WebDAV requests
- Shell.php and Passwd.dav requested



Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Create alarm when threshold of 500 ports scanned in 5 minutes occurs.

System Hardening

Set configurations on the host to mitigate port scans by blocking all ports not in use by configuring settings and setting up new rules. In Linux one option is run “sudo apt install firewalld”, “sudo service firewalld status, sudo firewall-cmd -
-remove-port=22/tcp
- -permanent”, “sudo firewall-cmd
- -remove-port=22/udp - -permanent,” for example. There are lots of ways to set firewalls and close ports.

Mitigation: Finding the Request for the Hidden Directory

Alarm

An alarm can be set to detect future unauthorized access when a non-Whitelist IP tries to access network. Set the threshold at 5 in an hour.

System Hardening

Set configuration on the host to block unwanted access by only allowing people from the Whitelist. In Linux you could run from root:

```
"# iptables -A INPUT -s <ip address> -j  
ACCEPT"
```

For all Whitelisted IPs.

Mitigation: Preventing Brute Force Attacks

Alarm

An alarm can be set to detect future brute force attacks by setting a threshold of 3 failed logins in a minute block. We could also add CAPTCHA and two-factor authentication.

System Hardening

We could add whitelisted IP's or use BotGaurd. Additionally we could do a lock out after too many failed attempts.
Ex: `auth required <account> deny=3
even_deny_root unlock_time=600 oner=fail
account required <account>`

Mitigation: Detecting the WebDAV Connection

Alarm

Alarm on non-Whitelisted IP on WebDAV (threshold 1) and make sure my firewall blocks all others.

System Hardening

In Ubuntu I would run the following command: \$
`iptables -A INPUT -s 192.168.1.0/24 -j DROP`

Mitigation: Identifying Reverse Shell Uploads

Alarm

Do not allow upload of code files including PHP (threshold 1). Also trigger alarm for all attempts on port 4444.

System Hardening

Set access to read only and have whitelisted IPs. Also insure that only necessary ports are open.

*The
End*