# Capstone Engagement

## Assessment, Analysis, and Hardening of a Vulnerable System

# Table of Contents

This document contains the following sections:


01 **Network Topology**

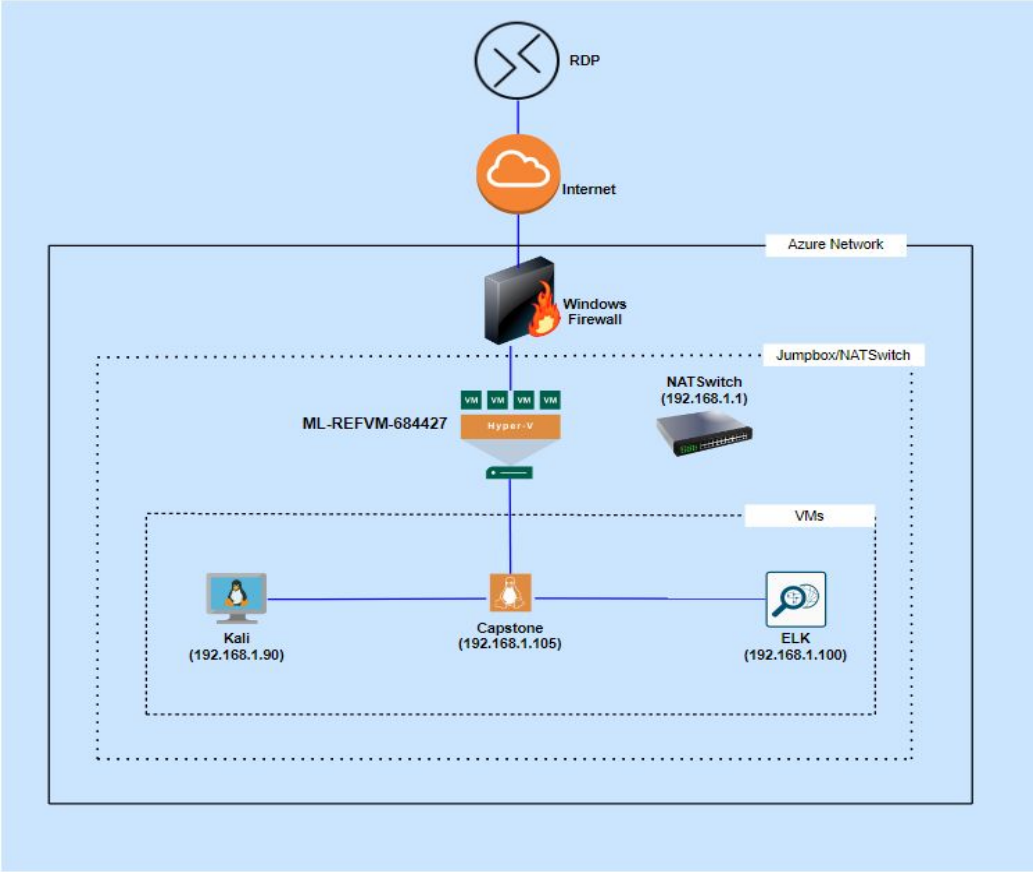
02 **Red Team**: Security Assessment

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: 192.168.1.1

**Machines**
IPv4: 192.168.1.1
OS: Windows
Hostname: ML-REFVM-684427

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

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 |
|---|---|---|
| Kali | 192.168.1.90 | Red Team attacking machine |
| Capstone | 192.168.1.105 | Blue team target Machine |
| ELK | 192.168.1.100 | SIEM network |
| ML-REFVM-684427 | 192.168.1.1 | NAT switch |

# Vulnerability Assessment

## The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| **CVE 2003-1138** | Web browser was used to read the contents of directories within the Apache server via GET request containing double slash (//). | The exploit revealed Ashton was the administrator for the company's restricted directory *(/company_folders/secret_folder)*. |
| **Weak Password** | A weak password allowed access to restricted directories via brute force attack. | The exploit allowed the attacking team access to the */secret_folder/*, in addition to providing access to *dav://192.168.1.105/webdav*. |
| **Reverse Shell Backdoor** | A reverse shell payload was deployed on the web server as a result of poorly configured firewall settings, which allowed the exploit to go undetected on outbound ports. | Remote backdoor shell access was established on the Apache web server. |
| | | |
| | | |

# Exploitation: CVE 2003-1138 Directory Listing Enabled

01

**Tools & Processes**

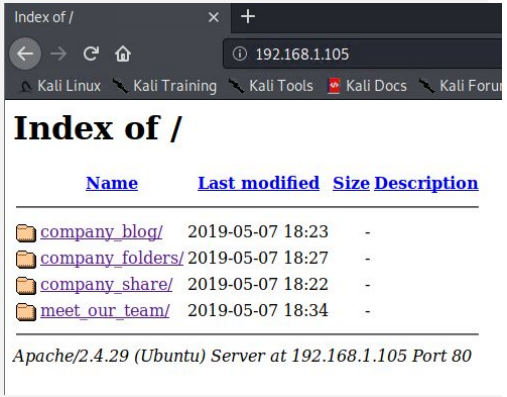
Found the IP address of the vulnerable server using nmap. Navigated to the company page 192.168.1.105 using web browser.

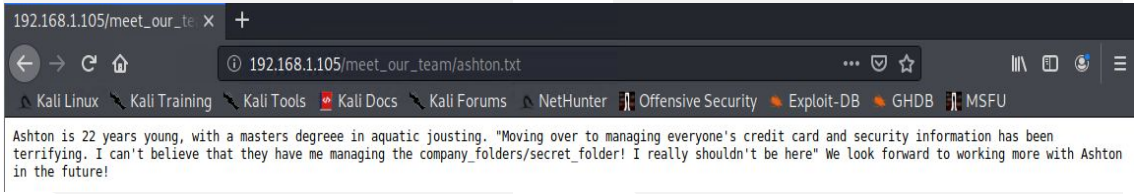
02

**Achievements**

After navigating through the various links, it was determined that Ashton was the admin for the desired target (*/company_folders/secret_folder*) What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

03



# Exploitation: Weak Password

01

**Tools & Processes**

A Hydra brute force attack was utilized to obtain Ashton's credentials and thereby access the contents of */company_folders/secret_folder/*.

02

**Achievements**

By obtaining the credentials for Ashton's account, access to restricted directories was achieved and their contents revealed to the attacker.

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 2021-04-02 1
8:20:27
root@Kali:~#
```

# Exploitation: Reverse Shell Payload

01

**Tools & Processes**

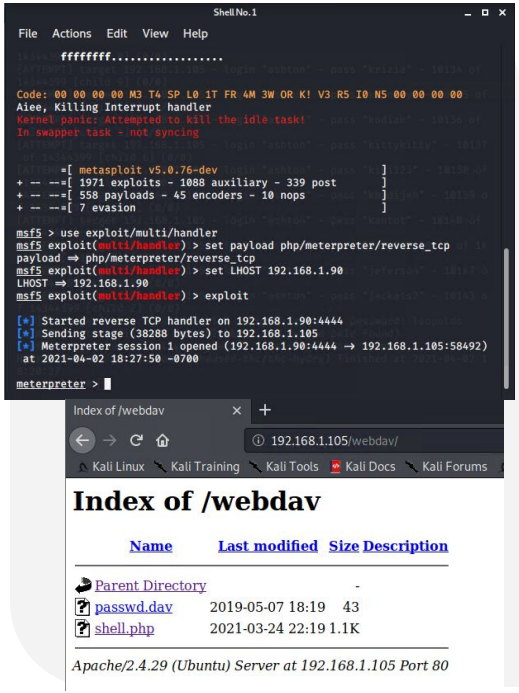
A file within the restricted directory contained instructions on how to obtain root privileges using the main admin's credentials. From here, a reverse payload shell could be placed anywhere on the web browser.

02

**Achievements**

By obtaining the credentials of the lead admin, a reverse shell payload, in the form of a .php file, was placed in the backend directories of the web browser. Once the file was launched, the attacker had full access to the vulnerable web server.

03



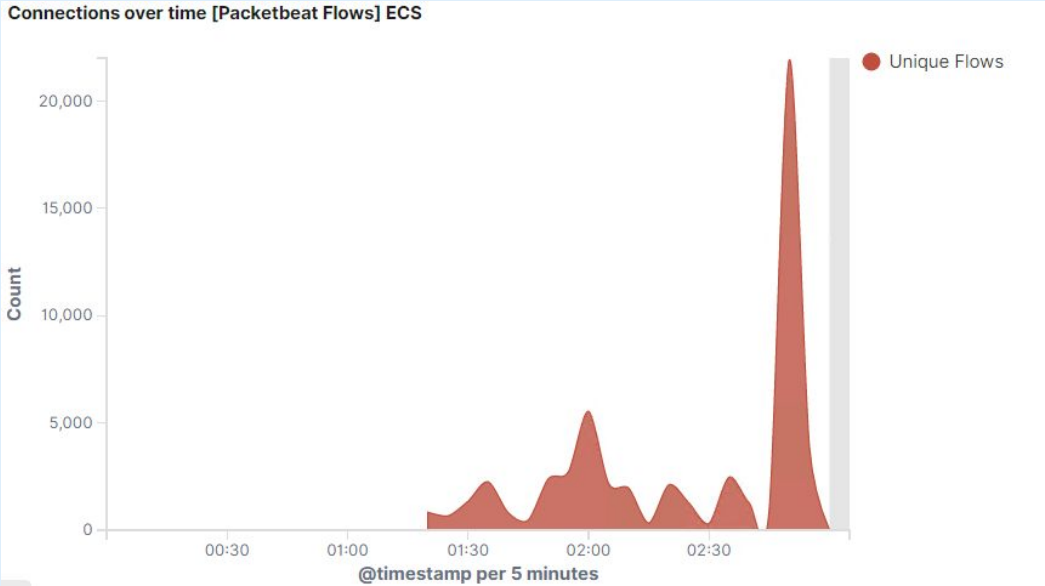
# Blue Team

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- The port scan occurred at approximately 2:45 UTC.
- Approximately 23,000 packets were sent from IP 192.168.1.90.
- The vast influx of network traffic over a short period indicates the IP range was being scanned for valid addresses.



# Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- The requests occurred between 2:50 and 3:00 UTC. In total, 15,856 requests were made.
- The requests were attempting to access the *secret_folder* directory and the contents inside.

**Top 10 HTTP requests [Packetbeat] ECS**

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/company_folders/secret_folder | 15,856 |
| http://127.0.0.1/server-status?auto= | 552 |
| http://snnmnkxdhflwgthqismb.com/post.php | 84 |
| http://www.gstatic.com/generate_204 | 42 |
| http://ocsp.godaddy.com | 23 |

# Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- During the attack 15,856 requests were made, attempting to access the *secret_folder*.
- There were 4 requests made before the attacker was able to access the password.


> Mar 24, 2021 @ 02:54:17.646

user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Mar 24, 2021 @ 02:54:17.646 method: get destination.port: 80
destination.bytes: 698B destination.ip: 192.168.1.105 server.port: 80 server.bytes: 698B server.ip: 192.168.1.105
network.direction: inbound network.community_id: 1:+kilzaHkaqv5oWK/BQbo7EBT5Gs= network.bytes: 857B network.type: ipv4
network.transport: tcp network.protocol: http host.name: server1 type: http query: GET /company_folders/secret_folder
http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html;

# Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- There were 54 requests made to  the webdav directory.
- The file that was requested was the .php shell which contained the reverse_tcp payload.

**Top 10 HTTP requests [Packetbeat] ECS**

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/company_folders/secret_folder | 31,863 |
| http://127.0.0.1/server-status?auto= | 982 |
| http://snnmnkxdhflwgthqismb.com/post.php | 154 |
| http://www.gstatic.com/generate_204 | 77 |
| http://192.168.1.105/webdav | 54 |

# Blue Team

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

## Alarm

In order to alert security teams of future port scans, it is recommended the following alarms and thresholds be put in place:

**Log and alert email when ports other than 80 and 443 are accessed multiple times from an unknown IP address.**

## System Hardening

It is recommended to strengthen host firewall settings in order to prevent network mapping and scanning of vulnerable ports.

Firewall settings should block all incoming and outgoing ports other than the necessary ones, in this case 80 and 443.

These firewall changes, in addition to a well configured IDS should provide solid security framework for the host network.

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

In order to alert host to intrusions, an alert and log should be created for certain directories. An alert and email should be set to trigger when an IP other than the host gains access to restricted directories, in this case *secret_folder*.

## System Hardening

The configuration file on the host network should block access to secret_folder from any IP other than approved ones. In order to do this:

-Navigate to etc/httpd/conf/httpd.conf
-Navigate to /var/www and set the following parameters:

```
<Directory /var/www/company_folders/secret_folder>
Allow from 192.168.1.1
Allow from 192.168.1.105
Deny from all
</Directory>
```

# Mitigation: Preventing Brute Force Attacks

## Alarm

In the future, an alert should be set in order to detect brute force attacks. The alert should be triggered when a surge in 401 errors occurs within a given time interval, ideally between 10-30 seconds. An email alert and log event should be triggered in this event.

## System Hardening

Stronger password configurations should be put in place, such as requiring lengthy and complex passwords for network users as well as lockouts due to failed login attempts.

# Mitigation: Detecting the WebDAV Connection

## Alarm

An alert should be created that sends an email and creates a log event when restricted files or directories are accessed by unknown IP's. It should detail the number of request attempts as well as logging information about the attacker's machine.

## System Hardening

The configuration file can be modified to prevent access by unknown IP addresses. The following configuration can be used:

As root user run
Nano etc/httpd/conf/httpd.conf
Navigate to /var/www section and set the following parameters:

```
<Directory /var/www/webdav>
Allow from 192.168.1.105
Allow from 192.168.1.1
Deny from all
</Directory>
```

# Mitigation: Identifying Reverse Shell Uploads

## Alarm

An alarm should be set that creates an email alert and log in the event that an unauthorized file begins transmitting data outside the network. The alert should log the http request method, url path and source IP.

## System Hardening

The configuration file can be modified to prevent access by unknown IP addresses. The following configuration can be used:

As root user run
Nano etc/httpd/conf/httpd.conf
Navigate to /var/www section and set the following parameters:

```
<Directory /var/www/webdav>
Allow from 192.168.1.105
Allow from 192.168.1.1
Deny from all
</Directory>
```

# the End