



# **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

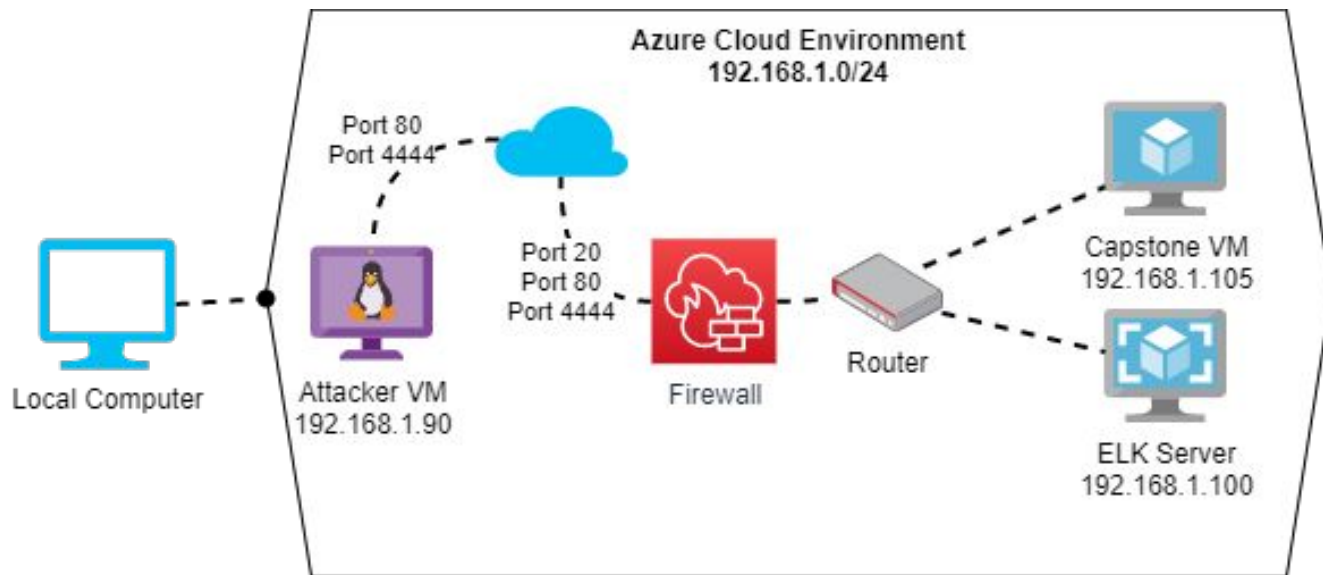
04

**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: Azure cloud

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

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	Role on Network
ML-REFVM-684427	192.168.1.1	Azure Cloud Environment
Kali Linux	192.168.1.90	Red Team : Offensive Machine
ELK Server	192.168.1.100	Blue Team : Defensive Machine
Capstone VM	192.168.1.105	Target Machine

---

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Brute-Force Attack	Force method using a list of possible passwords.	Attacker able to query the server if the username is available. Attacker able to access sensitive information and able to take control of a system.
Credential stored in web file	Credential to user's account with administrative privileges are stored on web server.	Easily achievable credentials on web server that able to exploit, inject script and loss of sensitive data.
Gain-privilege script injection	Open to script injection for user who shouldn't able to upload and execute files.	Vulnerable to data leak, stolen and loss of control.

# Exploitation: [Brute-Force Attack]

01

## Tools & Processes

Nmap and Hydra

02

## Achievements

Credential Access to sensitive information

03

```
[*] target 192.168.1.105 - login 'ashton' - pass 'montes' - 10122 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'memo123' - 10123 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'meandi' - 10124 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'marcho' - 10125 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'madonna' - 10126 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'lindinha' - 10127 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'leopoldo' - 10128 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'laruku' - 10129 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'lampshade' - 10130 of 14344399 [child 16] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'lanaelinda' - 10131 of 14344399 [child 17] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'lakota' - 10132 of 14344399 [child 18] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'lindie' - 10133 of 14344399 [child 19] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'krizia' - 10134 of 14344399 [child 20] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'kolokoy' - 10135 of 14344399 [child 21] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'kodiak' - 10136 of 14344399 [child 22] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'kittykitty' - 10137 of 14344399 [child 23] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'kiki123' - 10138 of 14344399 [child 24] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'kholish' - 10139 of 14344399 [child 25] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'kantot' - 10140 of 14344399 [child 26] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'jony' - 10141 of 14344399 [child 27] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'jeferson' - 10142 of 14344399 [child 28] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'jackassz' - 10143 of 14344399 [child 29] (0/0)
[0][*] 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 2021-07-08 03:58:48
root@kali:~#
```

192.168.1.105/company\_folders/secret\_folder/connect\_to\_corp\_server

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB

Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7da08a5cd7c8376eeb58d69b3ccd352)

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://172.16.94.205/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



# Exploitation: [Credential Web App]

01

## Tools & Processes

crackstation.net

Decode Ryan's password hash.

02

## Achievements

Username and password to webdav.

Lateral movement.

03



# Exploitation: [Name of Third Vulnerability]

01

## Tools & Processes

Metasploit

- MSFvenom

Payload generator.

- Meterpreter

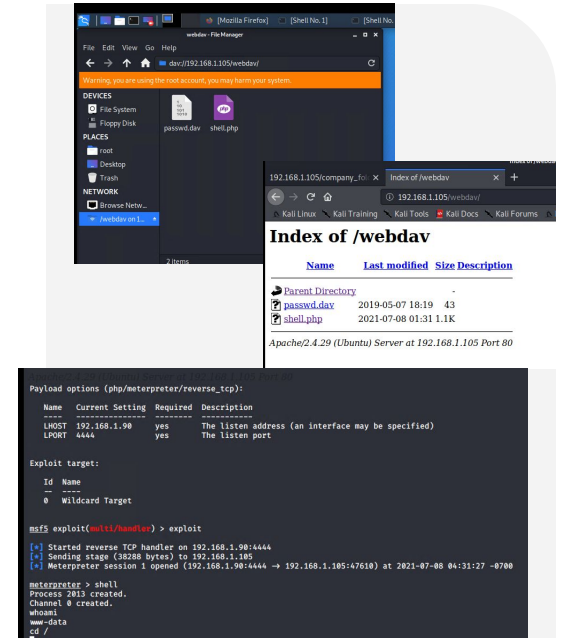
The payload that provides a reverse shell.

02

## Achievements

Execution and remote control the target's machine.

03



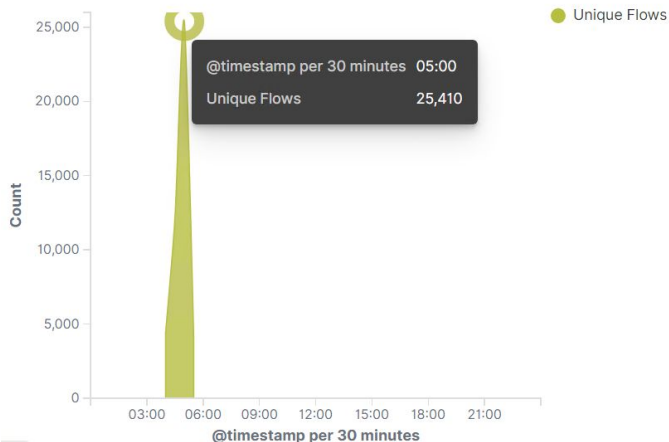


# **Blue Team**

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

Connections over time [Packetbeat Flows] ECS



Network Traffic Between Hosts [Packetbeat Flows] ECS

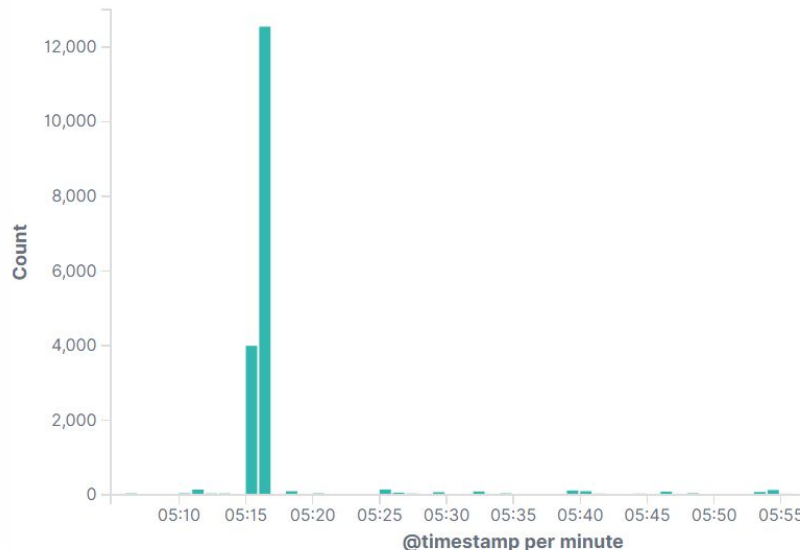
192.168.1.90	192.168.1.105	52.7MB	94MB
192.168.1.90	192.168.1.1	587.5KB	2.3KB
192.168.1.90	192.168.1.90	586.5KB	546.9KB
192.168.1.90	172.217.2.106	87.5KB	26.7MB
192.168.1.105	192.168.1.100	21.6GB	917.6MB
192.168.1.105	91.189.88.142	170.9KB	44.9MB
192.168.1.105	169.254.169.254	30.6KB	75.2KB
192.168.1.105	91.189.92.41	28.4KB	14.7KB
192.168.1.105	91.189.92.38	25.1KB	4.8MB

- What time did the port scan occur?
  - Jul 18, 2021 @ 05:17:30.004
- How many packets were sent, and from which IP?
  - 25,410 from 192.168.1.90
- What indicates that this was a port scan?
  - Port scan is identified by the broadcast address 192.168.1.105

# Analysis: Finding the Request for the Hidden Directory

HTTP Transactions [Packetbeat] ECS

📅 Last 1 hour



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ↕

Count ↕

[http://192.168.1.105/company\\_folders/secret\\_folder](http://192.168.1.105/company_folders/secret_folder)

16,476

<http://127.0.0.1/server-status?auto=>

635

<http://snnmnkxdhflwqthqismb.com/post.php>

98

[http://www.gstatic.com/generate\\_204](http://www.gstatic.com/generate_204)

49

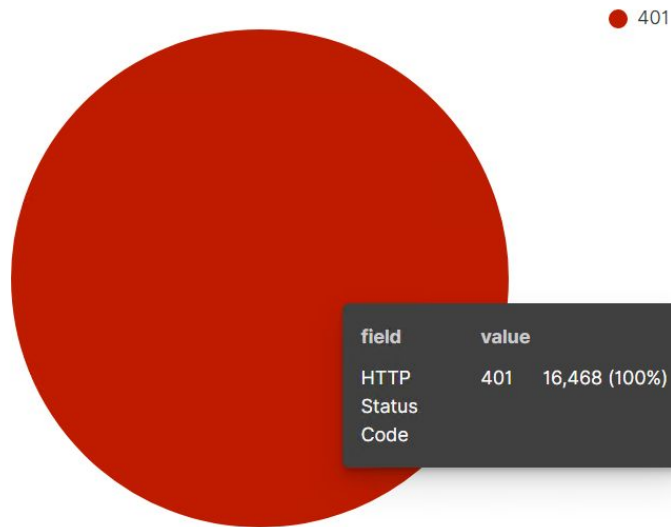
<http://ocsp.godaddy.com>

24

- What time did the request occur? How many requests were made?
  - 05:15
  - 16,475
- Which files were requested? What did they contain?
  - [http://192.168.1.105/company\\_folders/secret\\_folder](http://192.168.1.105/company_folders/secret_folder)
  - How to connect to company's server.

# Analysis: Uncovering the Brute Force Attack

HTTP status codes for the top queries [Packetbeat] ECS



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,468

Export: [Raw](#) [Formatted](#)

GET /company\_folders/secret\_folder: HTTP Query

- How many requests were made in the attack?
  - 16,468 requests were made during the attack
- How many requests had been made before the attacker discovered the password?
  - 16,465 request had been made before the attacker discover the password.

# Analysis: Finding the WebDAV Connection

---

## Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ↕	Count ↕
http://192.168.1.105/company_folders/secret_folder	16,476
http://127.0.0.1/server-status?auto=	990
http://snnmnkxdhflwgthqismb.com/post.php	140
http://www.gstatic.com/generate_204	76
http://192.168.1.105/webdav	38

- How many requests were made to this directory?
    - 38
  - Which files were requested?
    - http://192.168.1.105/webdav
-



# **Blue Team**

## Proposed Alarms and Mitigation Strategies



# Mitigation: Blocking the Port Scan

---

## Alarm

- An Intrusion Detection System can arranged to recognize a scan attempt.
- An Intrusion Prevention System can alert or block the suspicious IP address from the attacker.
- Setup an alarm when IPS request to attempts at TCP connections over various ports. Kibana able to detect and show there is a port scan occurring and then we able to block before any further steps are taken by an attacker.

## System Hardening

- Logging of TCP connection attempts
- Firewall configurations
- Deployment of IDS/IPS systems
  - Alerts for unusual port scans.
  - Block port scans

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

- Set alarm for any connection made to [http://192.169.1.105/company\\_folders/secret\\_folder](http://192.169.1.105/company_folders/secret_folder)

## System Hardening

- Creating a white-list to limit IPs that able to access into company's files and directories.
- Remove sensitive data (such as password, and how to get into company's webdav) from server.

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

- Set alarm to detect status code 401 when login requests are made more than four times.
- Detect any IP that notice Hydra in `<user_agent.original>`

## System Hardening

- Use Multi-factor authentications
- Send alert and lock account after fourth time failed to login.
- Block any IPs that `<user_agent.original>` noticed Hydra.

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

- Set alarm in any connection to `http://192.168.1.105/webdav`

## System Hardening

- Creating Whitelist of limited IPs that able to access to Webdav
  - Set two-factor authentication.
  - Don't allow storage of passwords and credentials for network authentication.
-

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

- Set alarm:
  - When there are traffic over port 4444 because it's Meterpreter's default port.
  - When there are files uploaded to server

## System Hardening

- Creating Whitelist for limited IPs that able to upload files and directories.
- Block all outgoing traffic by default on the WAN connection.
- Run chmod 700
  - This command allow only owner to read,write, and execute.

*The  
End*