# *David Cornish*
# *Cyber Security Professional Portfolio*

# *Capstone Engagement*

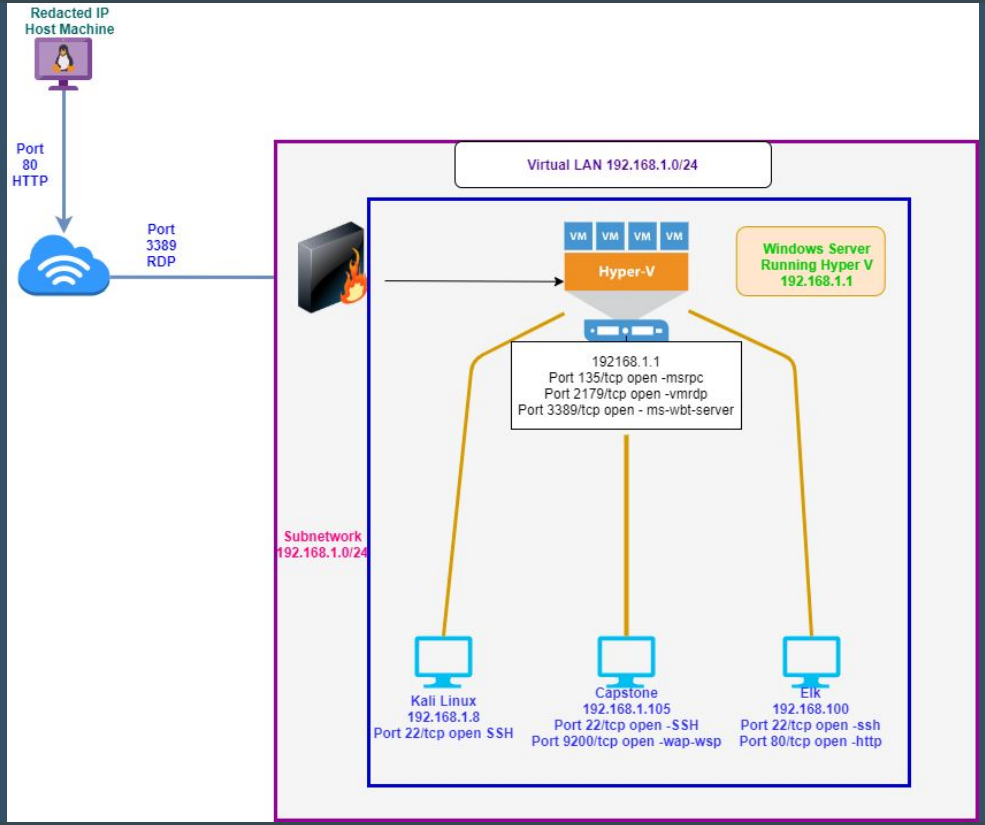
## *Assessment, Analysis, and Hardening of a Vulnerable System*

# Table of Contents

This document contains the following sections:

# Network Topology

# Network Topology




Network
Address Range:
Netmask:
Gateway:

Machines
IPv4:192.168.1.1
OS: Windows
Hostname: Hyper V

IPv4: 192.168.1.105
OS: Red vs Blue
Hostname: Capstone

IPv4: 192.168.1.8
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Red vs Blue
Hostname: Elk

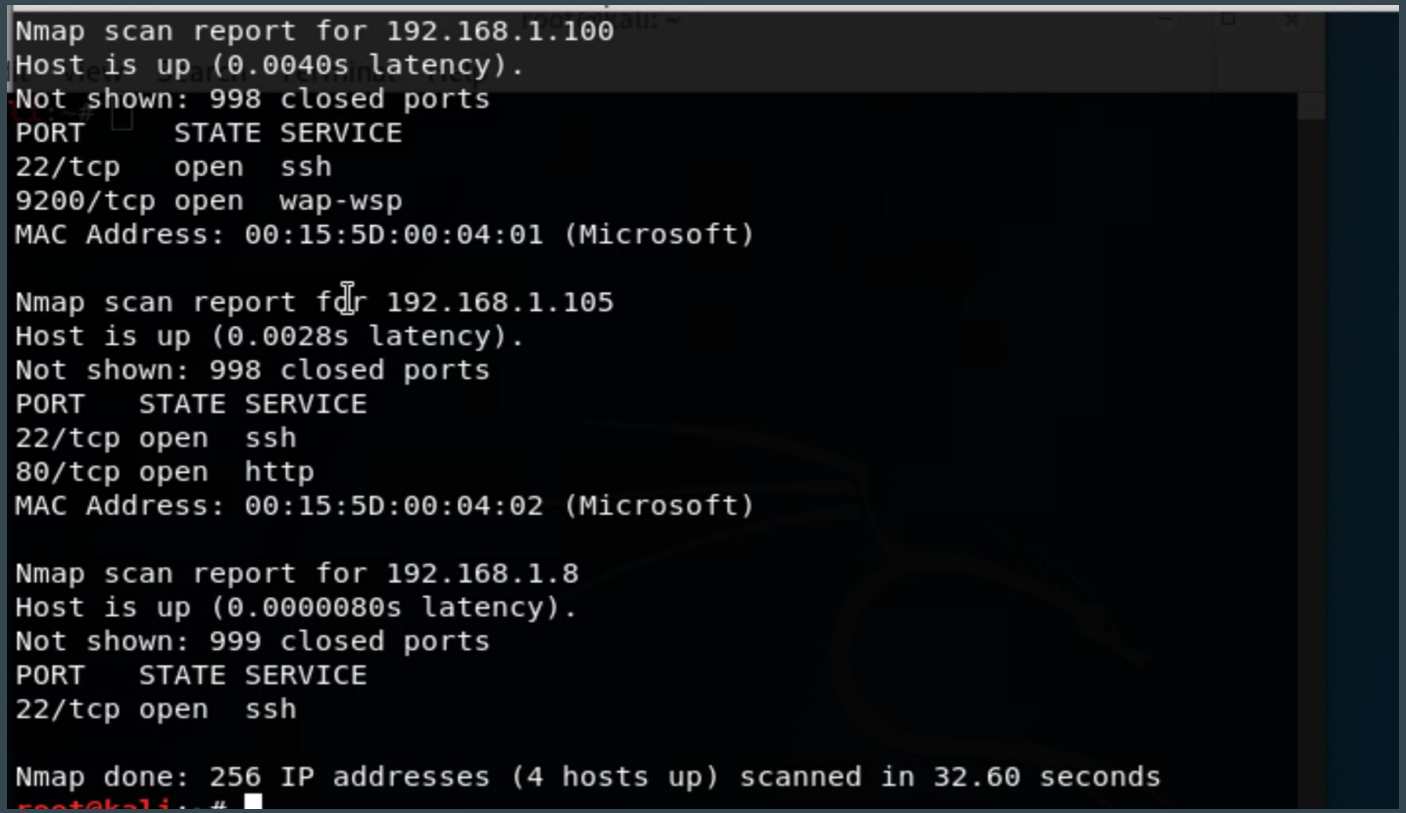
# **Red Team**
# Security Assessment

# Recon: Describing the Target

Nmap identified the following hosts on the network: ***nmap 192.168.1.0/24***

| Hostname | IP Address | Role on Network |
|---|---|---|
| **ELK Server** | **192.168.1.100** | **Blue Team Defensive Machine** |
| **Kali Linux** | **192.168.1.8** | **Attacker** |
| **Capstone VM** | **192.168.1.105** | **Target Machine** |
| **Hyper V** | **192.168.1.1** | **VM Host** |

# Nmap 192.168.1.0/24 Scan



# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| Credentials that are stored in a web file were discovered and used to gain access to the website | Credentials to accounts with administrative access were stored on the web server | Credentials were used to inject script and sensitive data was discovered |
| Brute-Force Attack | Passwords and usernames were obtained and the server was accessed | If usernames are available then access to sensitive information and control of a system are possible |
| Script injection | The server is vulnerable to script injection which was achieved | This leaves sensitive data vulnerable |

# Exploitation: Sensitive Data Exposure/Security Misconfiguration

01

**Tools & Processes**

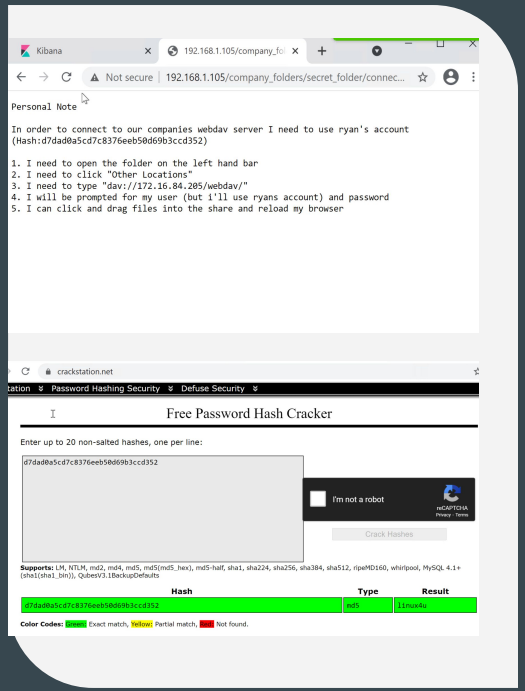
**Crackstation.net was used to crack the hash that was discovered on the web app resulting in the password linux4u and allowed us to log in using usernames discovered on the webapp. This allows us access to hidden files.**

02

**Achievements**

**We discovered a password that can be used to give us further access and expose more vulnerabilities**

03



# Exploitation: Brute Force Attack

01

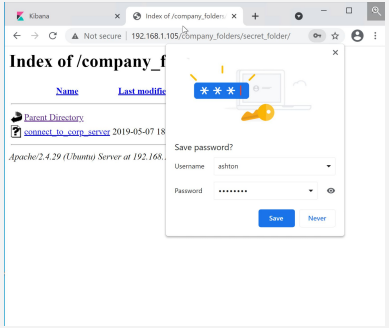
## Tools & Processes

**Hydra was used to crack user's password using a list of potential passwords and applying to associated user names**

02

## Achievements

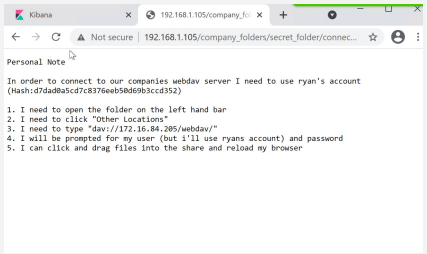
**Obtained credential access**




03

**hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get http://192.168.1.105:80/company_folders/secret_folder**

```
44399 [child 7] (0/0)
[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 (http://www.thc.org/thc-hydra) finished at 2021-04-15 19:47:30
root@kali:~#
```



# Exploitation: Script Injection

01

**Tools & Processes**

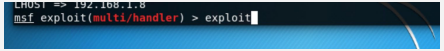
**DIRB, msfvenom, metasploit, and meterpreter will all used to exploit the vulnerabilities**

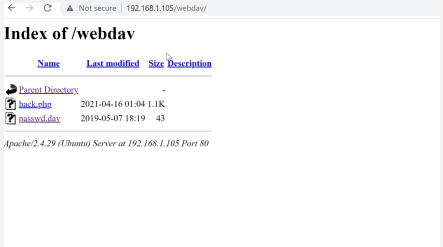
02

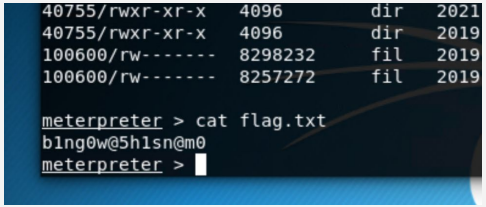
**Achievements**

**I was able to log in using a user's credentials, access privileged information, run an exploit, upload a php file (hack.php), and discover a flagged text file.**

03



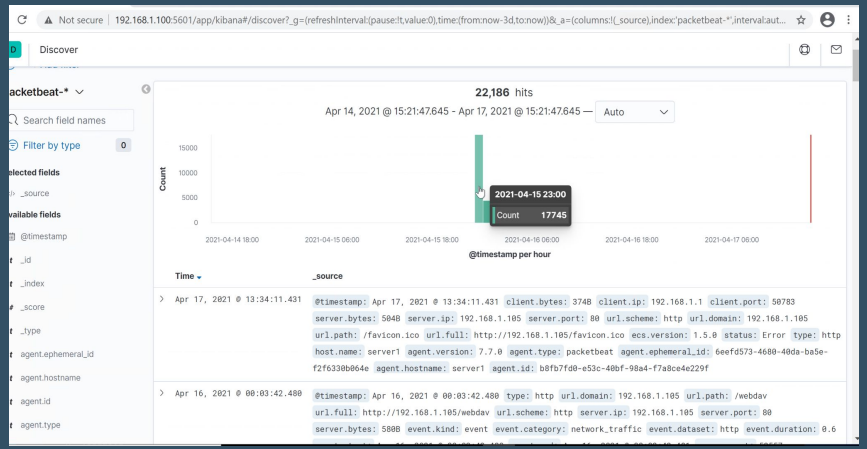



# **Blue Team**
# Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

| | | | |
|---|---|---|---|
| 192.168.1.8 | 255.255.255.255 | 840B | 0B |




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

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/webdav | 7,586 |
| http://192.168.1.105/company_folders/secret_folder | 5,827 |
| http://127.0.0.1/server-status?auto= | 1,803 |
| http://192.168.1.105/company_folder/secret_folder | 16 |
| http://192.168.1.105/company_folders/ | 8 |

Export: Raw Formatted

**The port scan occurred on 4/15/2021 at 23:00**
**Of the 22,186 packets, the majority of requests came from 192.168.1.105**
**A port scan from 255.255.255.255 indicates this was a port scan**

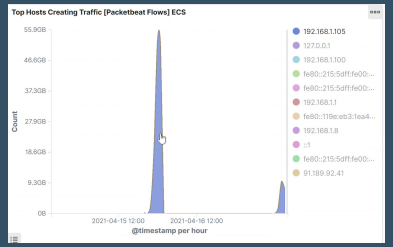
# Analysis: Finding the Request for the Hidden Directory

**Network Traffic Between Hosts [Packetbeat Flows] ECS**

| Source IP | Destination IP | Source Bytes | Destination Bytes |
|---|---|---|---|
| 192.168.1.105 | 192.168.1.100 | 145.9GB | 7.5GB |
| 192.168.1.105 | 91.189.88.178 | 485.9KB | 243.8MB |
| 192.168.1.105 | 169.254.169.254 | 78.9KB | 187.1KB |
| 192.168.1.105 | 91.189.92.39 | 56.7KB | 122.2KB |
| 192.168.1.105 | 192.168.1.8 | 32.8KB | 516.6KB |
| 192.168.1.8 | 192.168.1.105 | 52.5MB | 103.6MB |
| 192.168.1.8 | 192.168.1.255 | 1.4KB | 0B |
| 192.168.1.8 | 255.255.255.255 | 840B | 0B |
| 127.0.0.1 | 127.0.0.1 | 4.3MB | 8.8MB |
| 127.0.0.1 | 127.0.0.53 | 11.8KB | 19.2KB |

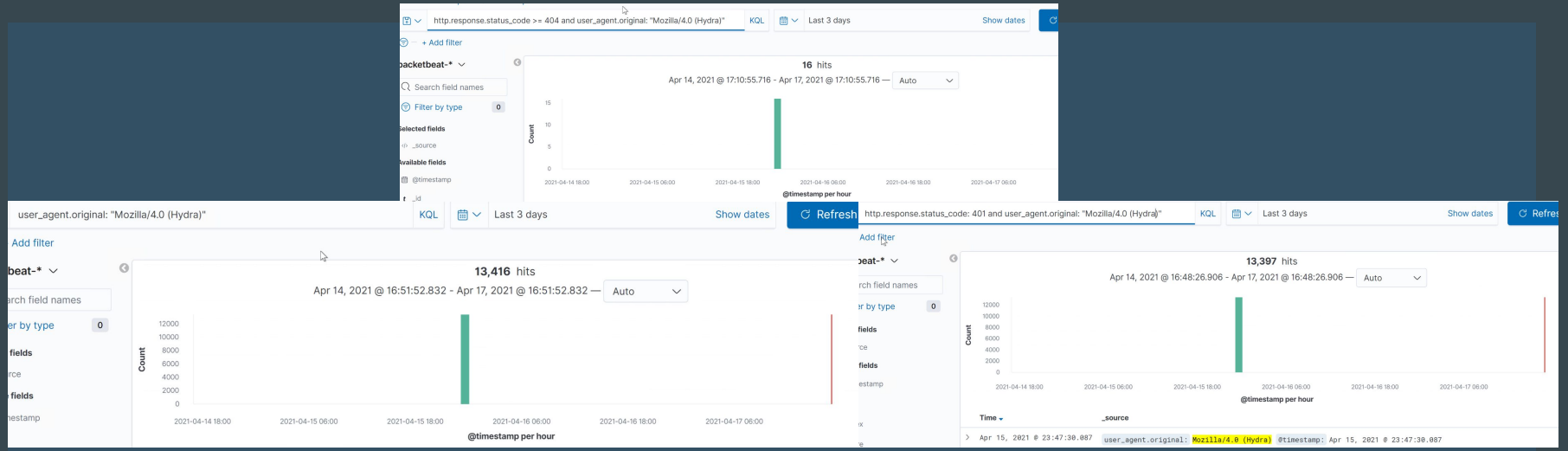
Export: Raw Formatted

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/webdav | 7,586 |
| http://192.168.1.105/company_folders/secret_folder | 5,827 |




**The requests occurred on 4/15/21**
**Attempts were made to access secret_folder and webdav**
**7,586 attempts were made to secret_folder and 5,827 attempts were made to webdav**
**The folders contain sensitive information including user names**

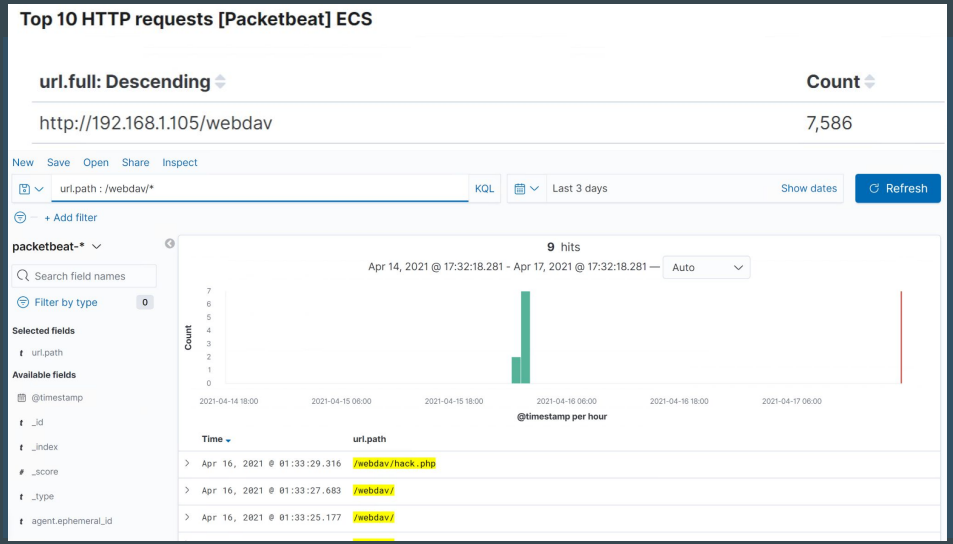
# Analysis: Uncovering the Brute Force Attack




**There were 13,416 requests**

**There were 13,397 requests before the attacker discovered the password**

# Analysis: Finding the WebDAV Connection




| Time | url.path |
|---|---|
| Apr 16, 2021 @ 01:33:29.316 | /webdav/hack.php |
| Apr 16, 2021 @ 01:33:27.683 | /webdav/ |
| Apr 16, 2021 @ 01:33:25.177 | /webdav/ |
| Apr 16, 2021 @ 01:33:19.607 | /webdav/ |
| Apr 16, 2021 @ 01:12:55.843 | /webdav/ |
| Apr 16, 2021 @ 01:04:52.314 | /webdav/hack.php |
| Apr 16, 2021 @ 01:02:21.975 | /webdav/hack.php |
| Apr 16, 2021 @ 00:03:55.059 | /webdav/passwd.dav |
| Apr 16, 2021 @ 00:03:42.485 | /webdav/ |

**7,586 requests were made to this directory /webdav/ and webdav/hack.php were requested**

# **Blue Team**
# Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

## Alarm

- Implement an IDS to recognize scan attempts
- Implement an IPS to alert or block offending IP address of attack
- Configure an IPA to alarm when multiple attempts at TCP connections over various ports to inform and block

## System Hardening

- Log TCP connection attempts
- Configure Firewall
- Deploy IDS/IPS systems
  - Alert for unusual scans
  - Block port scans

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

**A threshold should set and an alarm for 400 and greater http response codes so that when too many requests are made. IP whitelisting should be implemented.**

**An alarm should be set for any connection made to:**

**92.168.1.105/companyfolders/secret_folder**

## System Hardening

- **Remove sensitive directories, data, and files from the web server**
- **Create a white-list of IPs that have access to these files and directories**

# Mitigation: Preventing Brute Force Attacks

## Alarm

**Detection of status code 401 when login attempt are unsuccessfully made**

**What threshold would you set to activate this alarm?**

**When more than 3 unsuccessful login attempts**

## System Hardening

- **Multi-factor authentication**
- **Account locks and alerts after 3 three failed attempts**
- **Implement CAPTCHAs**

# Mitigation: Detecting the WebDAV Connection

## Alarm

**Set an alarm for any connection made to:**

**192.168.1.105/webdav**

## System Hardening

- **Implement policies that restrict credential storage on servers**
- **Create a whitelist of IPs that need access to webdav**
- **Two-factor authentication**

# Mitigation: Identifying Reverse Shell Uploads

## Alarm

- **Set alarms for:**
  - **Any traffic over port 444 (Meterpreter's port)**
  - **Any files uploaded to the server**
  - **Any time commands are executed**

## System Hardening

- **Restrict upload of files or directories to only whitelisted IP**
- **Remove remote web content for authoring operations**
- **Run the following command to set owner read, write, and execute permissions:**
  - **chmod 700**

*For additional screenshots and notes*
*click here*


The End