Capstone Project

Conducting a brute force attack and data breach on a target server and analyzing its footprint using Kibana SIEM

By Glen Abalayan

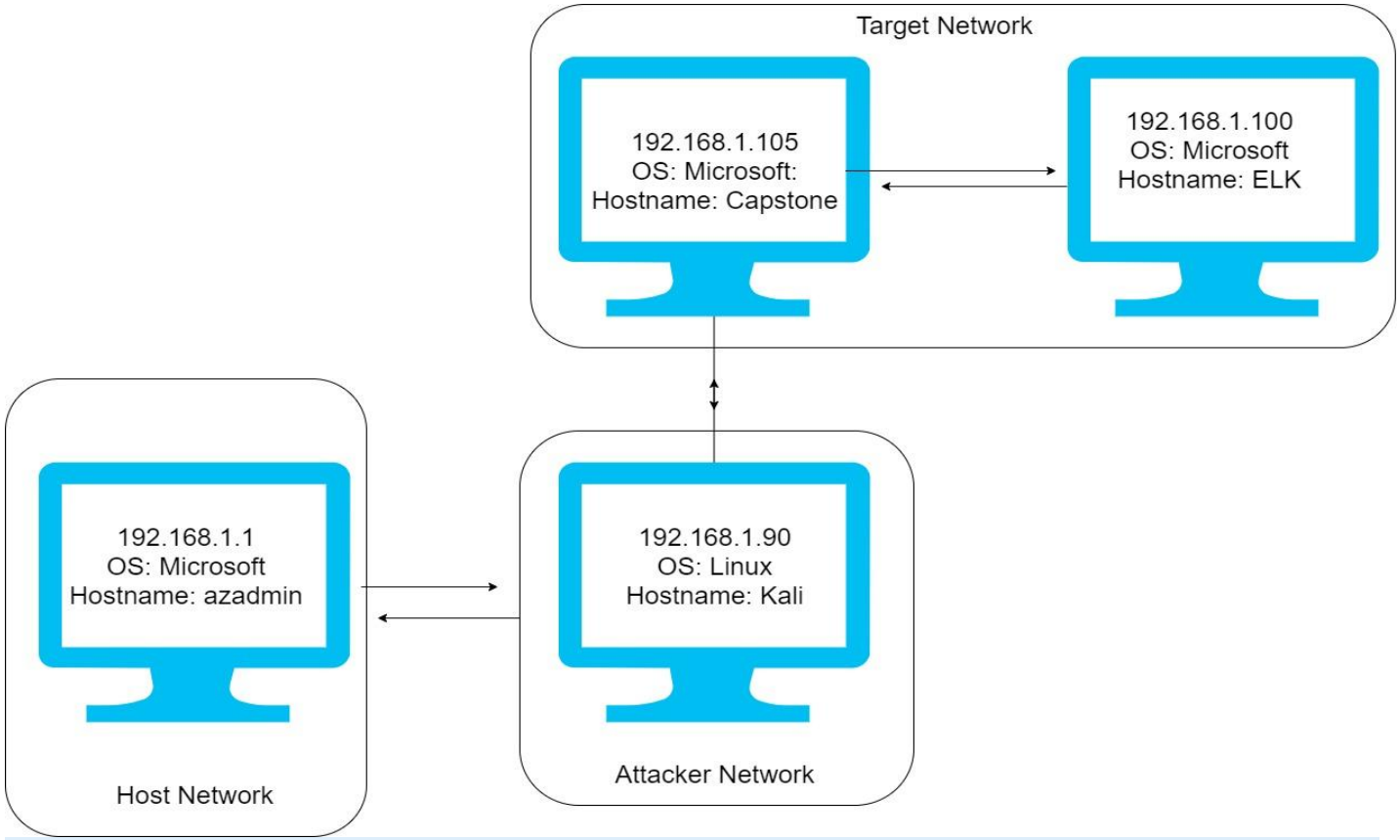
April 7, 2021

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.1-254
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.100
OS: Microsoft
Hostname: ELK

IPv4: 192.168.1.105
OS: Microsoft
Hostname: Capstone

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.1
OS: Microsoft
Hostname: azadmin

Network map of the project environment, including the attacker and target networks.

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ELK	192.168.1.100	• The role of the ELK server is to **monitor network traffic** and visualize data travelling across the network
Capstone	192.168.1.105	• The role of the Capstone server is to act as the **target machine** to launch a reverse shell attack.
Kali	192.168.1.90	• The role of the Kali machine is to act as the **attacker machine**
Azadmin	192.168.1.1	• The Azadmin host acts as the **gateway** between the VMs and Internet

Vulnerability Assessment

Vulnerability	Description	Impact
Weak Passwords	A password is considered weak when it is less than 10 characters, is a word in the dictionary, and lacks any special characters.	Systems with weak passwords allow hackers to easily gain access by using password crackers that can run thousands of commonly used passwords within minutes.
Directory Transversal	Directory transversal is the ability for a client to navigate to other areas of the site by simply adjusting the HTML address.	Attackers can use this vulnerability to access secret parts of the website and input malicious code
Remote uploads	Users can upload files remotely from outside the host's network. This is increasing in popularity due to the rise of work from home.	Attackers can use this feature to upload malicious files into the network
No Account Lockout Policy	Account lockout locks users out after reaching a number of failed attempts.	Attackers can use this vulnerability to run brute force attacks and gain access.

Exploitation: Brute Force Attack

01

Tools & Processes

1. Used **nmap** to find target server IP address and noticed port 80
(HTTP) was open
2. Navigated to the target site and saw that Ashton is the system administrator.
3. Used **THC-Hydra** password cracker with Ashton's username and wordlist
4. THC-Hydra cracked Ashton's password and used it to log in.

02

Achievements

The brute force attack allowed attackers to successfully crack Ashton's password and later used these credentials to **grant continued access** to the site.

03

```
Nmap scan report for 192.168.1.105
Host is up (0.00071s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)
```


```
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105
http-get /company_folders/secret_folder/
```

```
[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 2021-04-03 15:52:47
root@Kali:~#
```

Exploitation: Remote connection to the WebDAV server

01

Tools & Processes

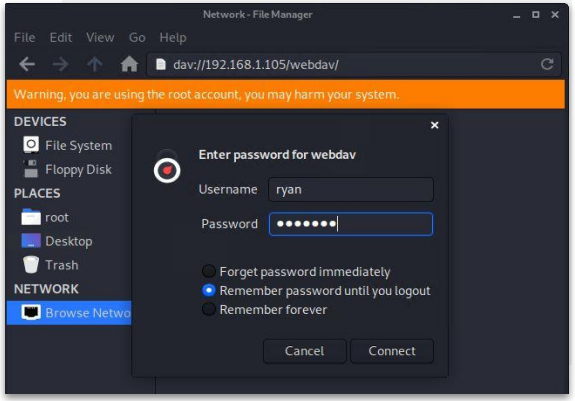
1. Used **Network File Manager** to connect to WebDAV server (dav://192.168.1.105/webdav/)
2. Determined that Ryan is the administrator of the server.
3. Used **MD5Online** to decrypt Ryan's password hash.
4. Gained authorized access to the server by inputting Ryan's credentials (**ryan : linux4u**)

02

Achievements

Once attackers gain access to the administrator's credentials to the WebDAV server, they can then **upload malware** disguised as small changes onto a server that clients believe is trustworthy. Depending on the malware, attackers can **steal files**, **destroy data**, and **paralyze entire networks**.

03



Exploitation: Uploading malware onto the WebDAV server

01

Tools & Processes

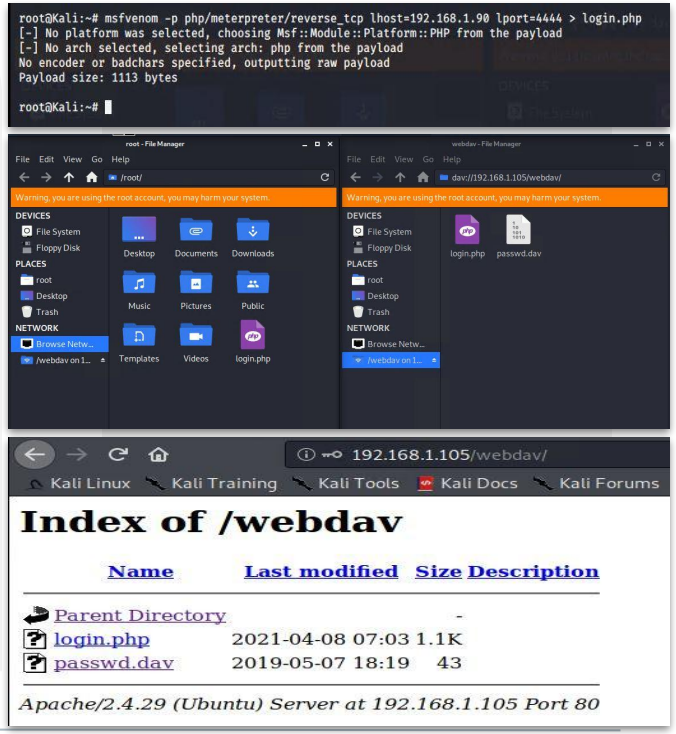
1. Used **msfvenom** to create a reverse shell payload.
2. Created a **meterpreter** listener session using **msfconsole**.
3. Uploaded the reverse shell payload (**login.php**) onto the WebDAV server.
4. The meterpreter session is activated once the link is clicked
5. While on the listener, dropped into a bash shell and located the root directory and **flag.txt**.

02

Achievements

Attackers can use reverse shell payloads to **access secret files** in the network by making the target communicate with the attacker via. a listener. Attackers can also exploit access to the WebDAV server by uploading **more dangerous forms of malware**.

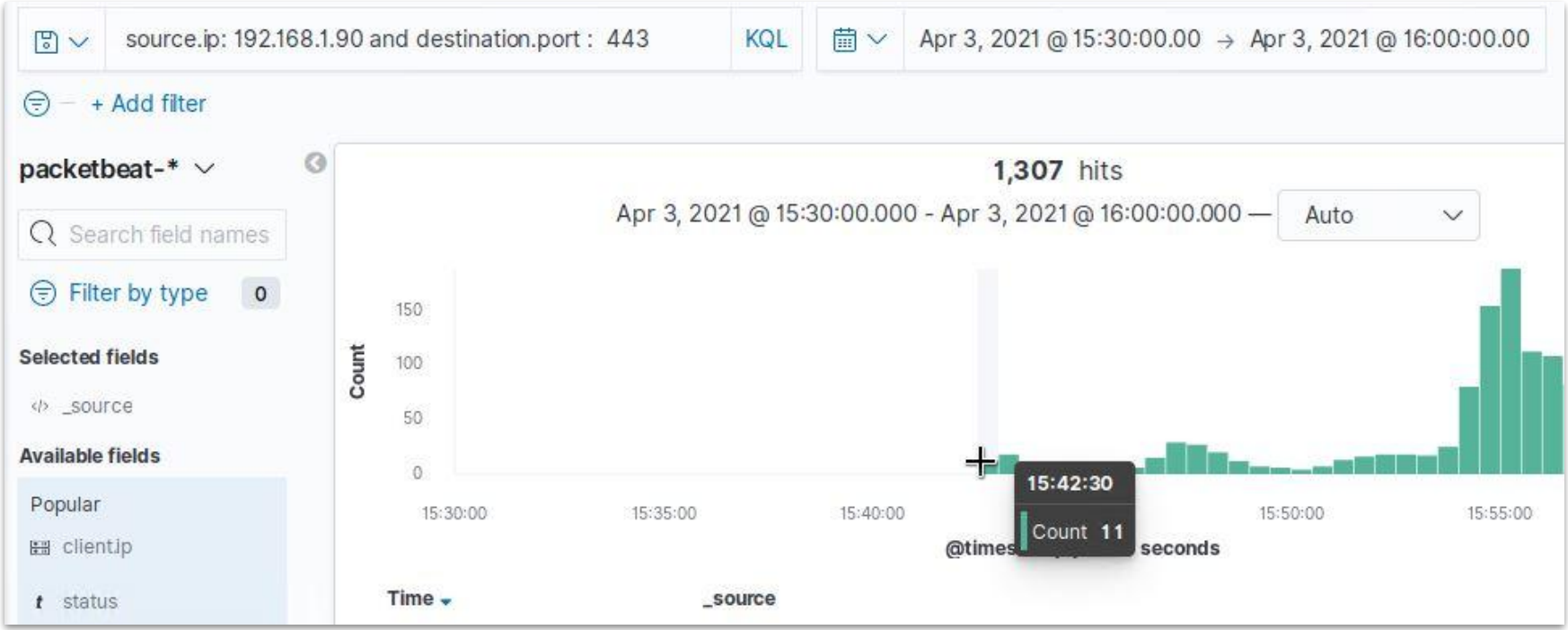
03



Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

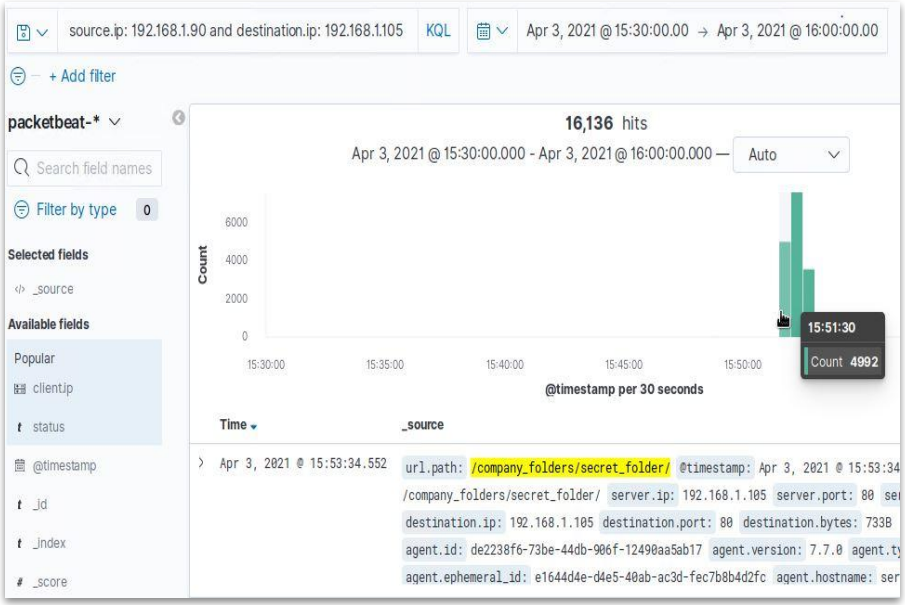
- The **nmap** port scan occurred at **15:42:30 HRS** on April 3, 2021
- At the start of the scan, 11 packets were sent from **192.168.1.90**, the attacker machine.
- We were able to identify the port scan by filtering for traffic on **port 443**, the port nmap uses by default.



Packetbeat results identifying the attacker's nmap port scan over port 443

Analysis: Finding the Request for the Hidden Directory

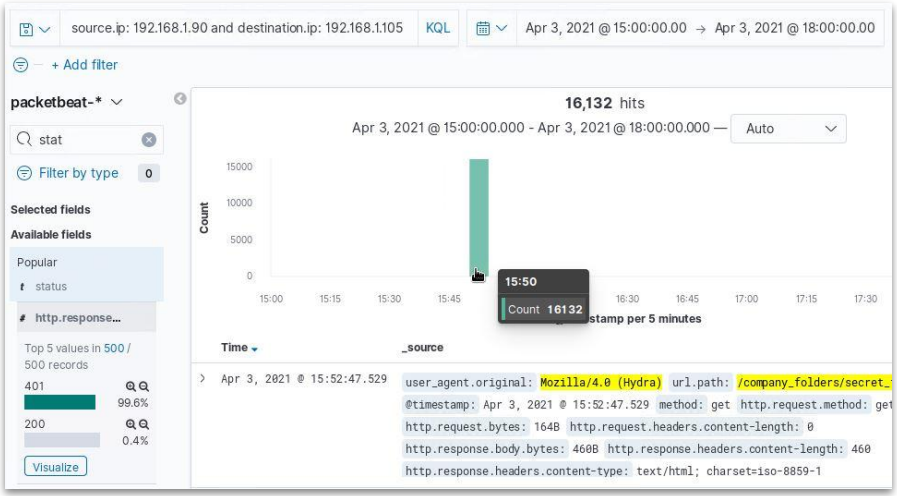
- The request for the hidden directory was initially made on **15:51:30 HRS on April 3, 2021**
- There were over **16,000 requests** for the secret folder, and **2 requests** for the connect_to_corp_server file inside.
- This behavior was identified by filtering for traffic between the attacker and target machine with the **url path** directed to the secret folder and its contents.



Packetbeat results for HTTP requests from the attacker machine for the secret directory and its contents.

Analysis: Uncovering the Brute Force Attack

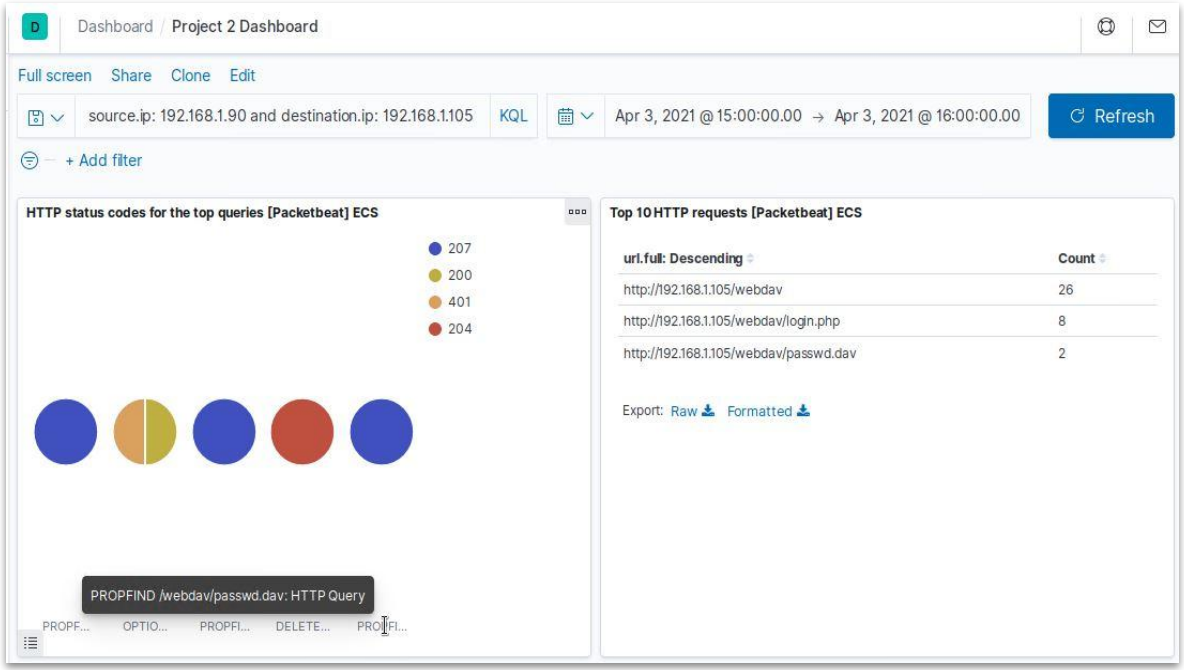
- The brute force attack occurred at **15:50 HRS** on April 3, 2021.
- During the attack, **16,132 unauthorized attempts** were made at cracking the password, with **2 successful attempts**.
- A brute force attack is assumed to have occurred due to the abnormally high number of failed requests made in a short amount of time.
- The brute force attack was detected by filtering for http response codes **401 (unauthorized)** and **200 (success)** between the attacker and target.



Packetbeat results for HTTP response code 401 (failure) and 200 (success)

Analysis: Finding the WebDAV Connection

- There were 26 requests made from the attacker machine to the WebDAV server.
- Attackers were also able to request **passwd.dav** (authentication) and **login.php** (malicious php shell)
- Securing the WebDAV connection is vital because it is a shared, collaborative server for the corporate network.



Dashboard results for requests to WebDAV and related assets

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- To prevent future port scans, it is recommended to set an alarm that notifies administrators **any time outside IP's send more than 10 packets a minute over port 443.**
- This alarm monitors traffic over port 443 because this is the default port used for port scans.

System Hardening

- To harden systems against port scans it is recommended to:
  - Block port 443 from outside traffic
  - Install a firewall to prevent unauthorized access and detect port scans
  - Close unnecessary ports

Mitigation: Finding the Request for the Hidden Directory

Alarm

- To prevent future breaches into the secret directory it is recommended to set an alarm **any time the secret folder is requested by any machine.**

System Hardening

- Measures to harden systems against unauthorized access to the secret directory include:
  - Moving the hidden directory outside of the public-facing network.
  - Requiring network administrators to use stronger, more complex passwords.

Mitigation: Preventing Brute Force Attacks

Alarm

- To prevent future brute force attacks it is recommended to set an alarm **any time the number of 401 (unauthorized) HTTP status codes exceeds 30 per hour.**
- To detect future attacks using Hydra, it is recommended to set a second alarm **any time the user_agent.original returns the value Hydra.**

System Hardening

- System hardening measures to prevent brute force attacks include:
  - Establishing an account lockout policy after 12 failed attempts.
  - Blocking traffic from IP addresses with a high rate of 401 status codes.
  - Disabling unnecessary services.
  - Closing unnecessary ports.
  - Blocking any traffic with Hydra as the user agent.

Mitigation: Detecting the WebDAV Connection

Alarm

- To prevent future unauthorized access to the WebDAV server, it is recommended to set an alarm that notifies administrators **any time the WebDAV server is accessed by machines outside of the access control list.**

System Hardening

- Recommendations to mitigate against unauthorized access to the WebDAV server include:
  - Moving the WebDAV server outside of the public-facing network.
  - Establishing a firewall rule that only allows machines with approved MAC addresses access to the server.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- To prevent future uploads of reverse shell payloads and other malware, it is recommended to set an alarm **any time a machine outside of the access control list uploads a .php or .exe file** to the WebDAV server.
- Another recommended alert would be to alert administrators **any time there is traffic on port 4444**. This is because port 4444 is meteterpreter's default port.

System Hardening

- Recommended hardening measures to prevent reverse shell uploads would be:
  - Set a firewall rule to only allow machines on the access control list to upload files to the server.
  - Close port 4444.
  - Restricting the ability to upload files directly to the WebDAV server from a web browser.
  - Test changes on shared repositories instead before allowing changes to the server.


Penetration Testing
Report Complete