

Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Jaseong Koo

Table of Contents

This document contains the following sections:

01

Network Topology

02

Red Team: Security Assessment

03

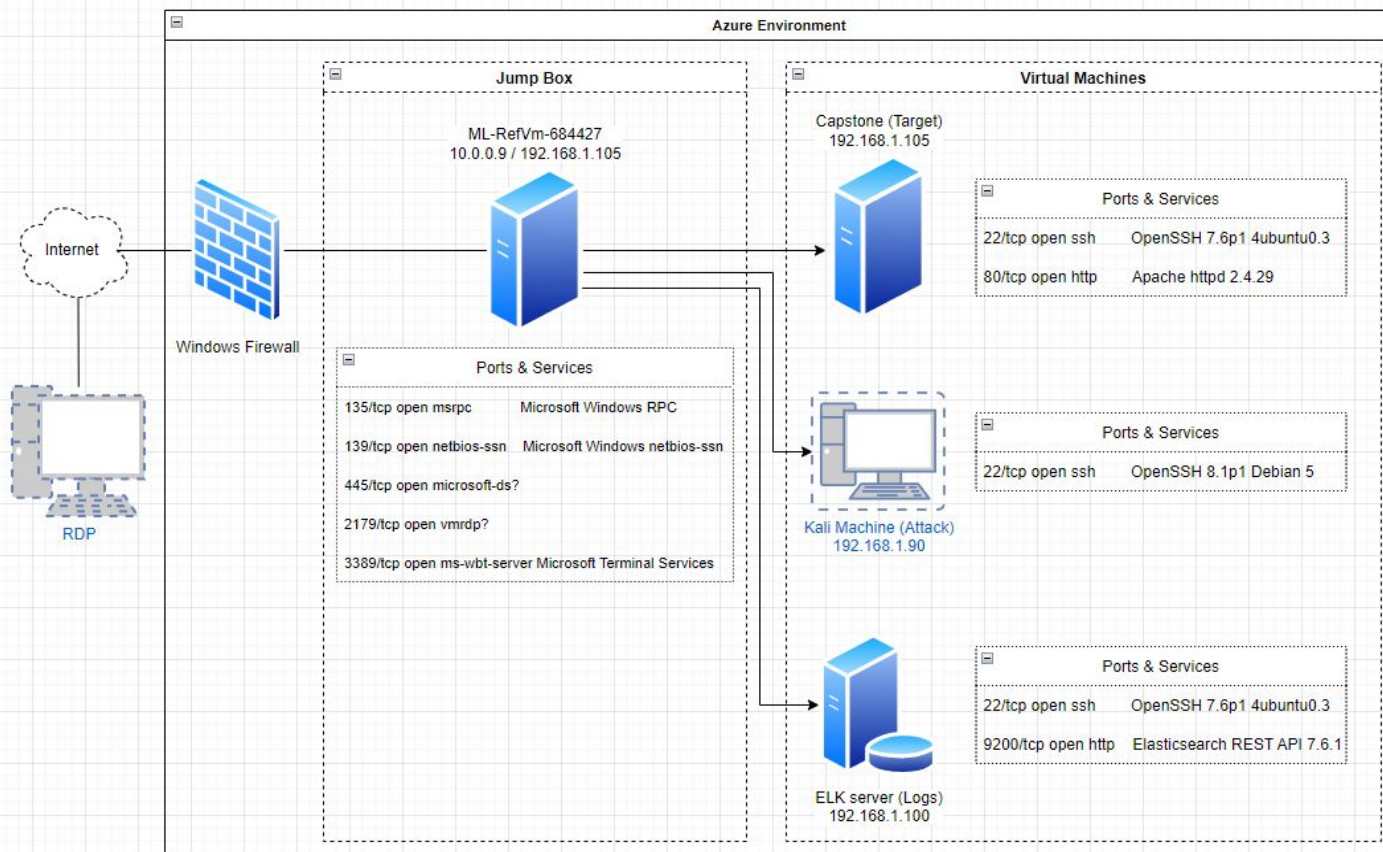
Blue Team: Log Analysis and Attack Characterization

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:192.168.1.1

Machines

IPv4: 192.168.1.1
OS: Windows
Hostname: Hyper Visor

IPv4: 192.168.1.90
OS: Linux 2.6.32
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux 3.2 - 4.9
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux 3.2 - 4.9
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
Hyper Visor	192.168.1.1	Host Machine of the virtual environment
Kali	192.168.1.90	Kali Machine (Attacking)
ELK	192.168.1.100	ELK server (Logging)
Capstone	192.168.1.105	Capstone Machine (Target)

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Exposed Critical Data	Sensitive data was present in the secret_folder accessible to public	The information inside the secret_folder contained how to access the company's web server which allows attackers to manipulate the data
Brute Force Attack Vulnerability	Able to gain access to the specific web application server by brute force attack	Attackers may gain access to vulnerable machine for critical data
Unrestricted File Upload	Insufficient access controls on critical points of the server which allows the uploads on the server	Unauthorized users can access and upload malicious files which can allow disclosure, alteration, and destruction
Insufficient Monitoring	No baseline/threshold were set to trigger alerts to be sent	Without any alerts, security personnel will have no time to react nor attackers can penetrate further

Exploitation: Exposed Critical Data

01

Tools & Processes

- Searched through the indexed pages using web browser

02

Achievements

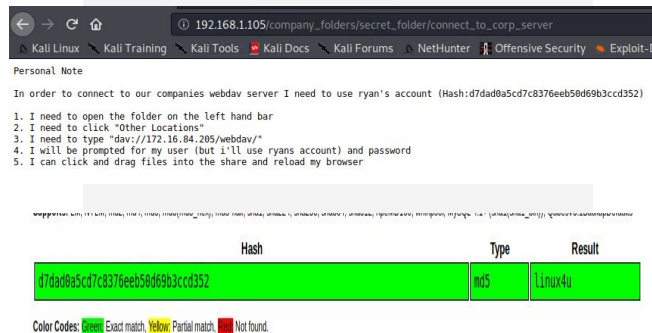
- Discovered secret_folder which contained several sensitive data

03

Index of /company_folders/secret_folder

[Name](#) [Last modified](#) [Size](#) [Description](#)

[Parent Directory](#) -
[connect_to_corp_server](#) 2019-05-07 18:28 414



Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad9a5cd7c8376eeb50d69b3ccd352)

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

Hash	Type	Result
d7dad9a5cd7c8376eeb50d69b3ccd352	md5	Linux4u

Color Codes: Exact match, Partial match, Not found.

Exploitation: Brute-force Attack Vulnerability

01

Tools & Processes

- Username was found on the web page of the company
- Used Hydra with a wordlist "rockyou.txt" and successfully cracked a hashed password

02

Achievements

- Gained access to the /secret_folder under /company_folders
- Inside the secret_folder, there was an instruction how to login to the server with valid credential

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 2022-01-28
```

Exploitation: Unrestricted File Upload

01

Tools & Processes

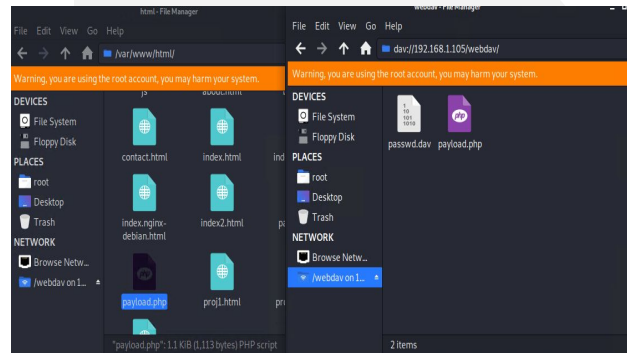
- After gaining access to the Webdav server, utilized msfvenom to upload and insert a reverse shell to the server
- After successful exploitation, Meterpreter was initiated with session via reverse shell

02

Achievements

- Achieved the use of shell
- Later penetration could gain access to root

03



```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -

meterpreter > |
```



Blue Team

Log Analysis and Attack Characterization

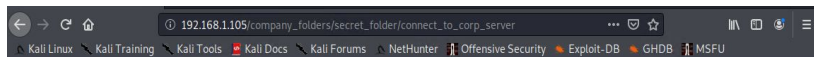
Analysis: Identifying the Port Scan

- Port scan occurred at 13:21.40.001
- 1,019 packets were sent from 192.168.1.90
- It showed that multiple ports were requested from the same IP address at the same time.



Analysis: Finding the Request for the Hidden Directory

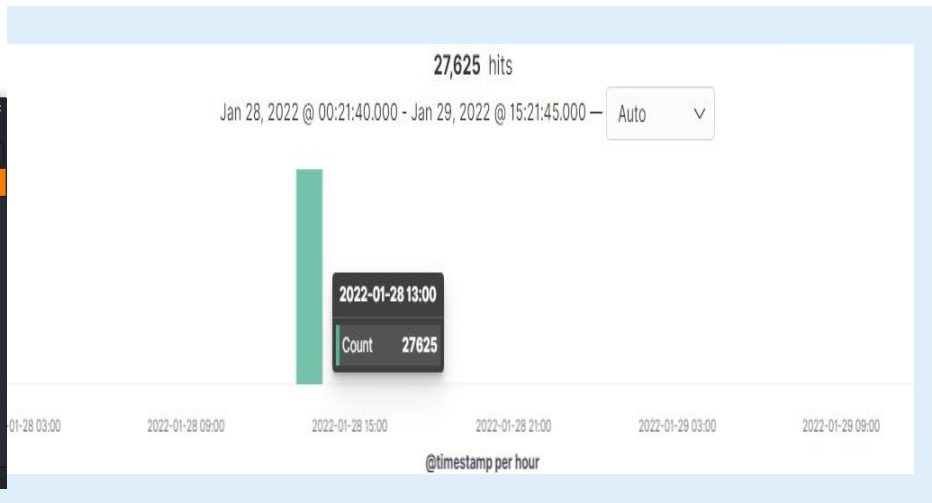
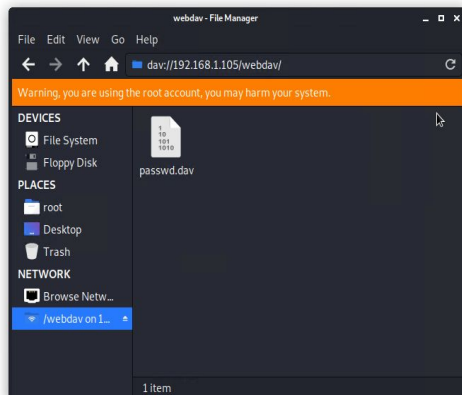
- Request for the hidden directory occurred between 13:28 and 13:31
- There were 27,624 requests made to http://192.168.1.105/company_folders/secret_folder
- The “**connect_to_corp_server**” file was requested, which had an instruction of **WebDav** connection



Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad8a5cd7c8376eeb5d69b3ccd352)

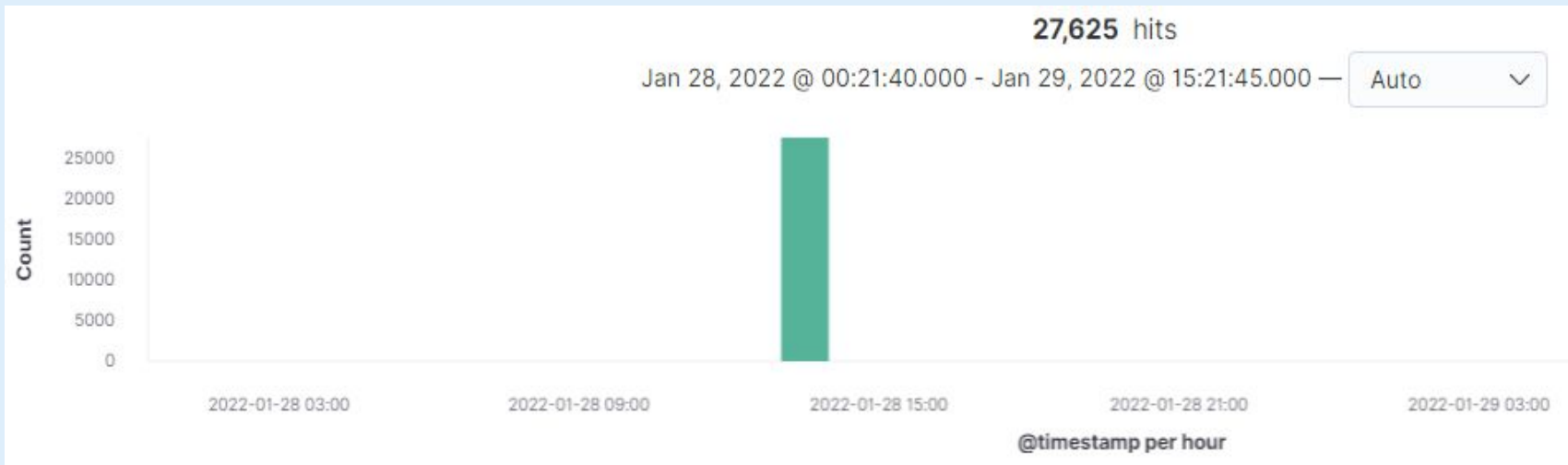
1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser



Analysis: Uncovering the Brute Force Attack

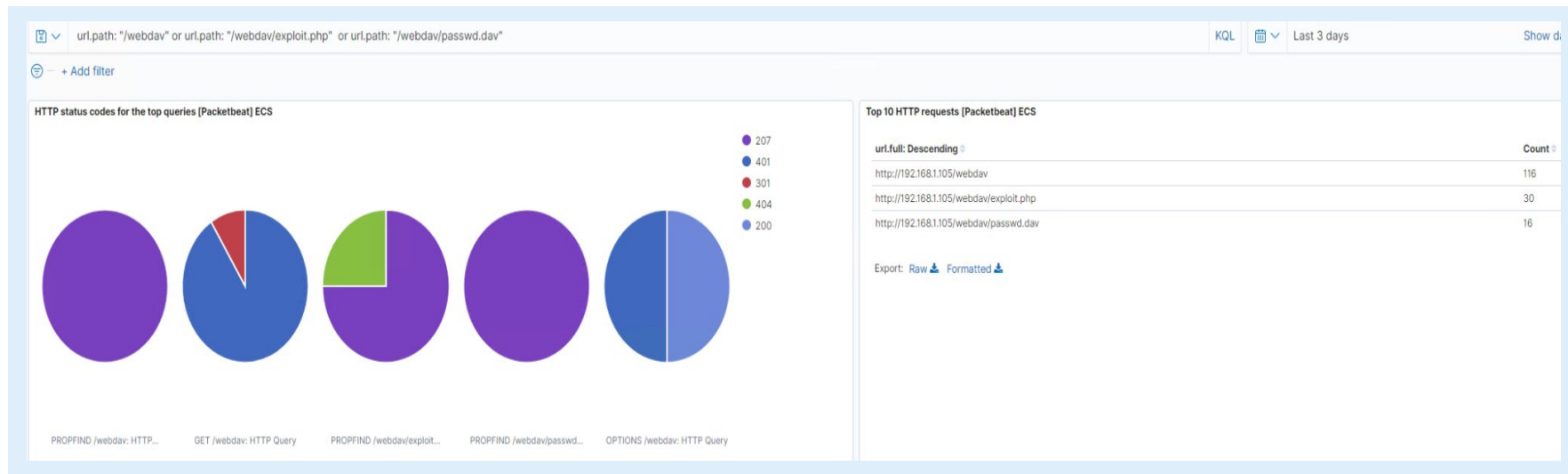
- 27,625 requests were made in the Brute Force Attack
- 27,624 requests were made before the attacker discovered the password

source.ip: 192.168.1.90 AND destination.ip: 192.168.1.105 AND user_agent.original: "Mozilla/4.0 (Hydra)"



Analysis: Finding the WebDAV Connection

- 116 requests were made to /WebDav directory
- /passwd.dav was requested and /exploit.php was uploaded





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?

- Alarm with threshold to detect the number of ports accessed per each source IP every second.

What threshold would you set to activate this alarm?

- An alarm that will be triggered to send out an email and log when a certain IP address sends more than 5 port scans in one second.

System Hardening

What configurations can be set on the host to mitigate port scans?

- Block every other port (incoming/outgoing) except for the required ports (80, 443)
- Techniques such as scan-delays or port-blocking via firewall will be an effective port scan mitigation.
- Whitelist specific IP addresses which needs access to the server

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Alarm that will notice the admin that shows the detected number of requests made per second

What threshold would you set to activate this alarm?

- Alert an admin when log shows >0 access to the "secret_folder" from IPs other than 192.168.1.105 or 192.168.1.1

System Hardening

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

- Whitelist specific IP addresses which are used for normal business operations
- Blacklist specific IP addresses which are trying to cross the threshold

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Alarm when IP addresses other than whitelisted IP addresses are detected will trigger an alarm of "Unauthorized IP"

What threshold would you set to activate this alarm?

- When the number of error (401) response is detected within 5 seconds the alarm should be activated
- When OK (200) response from unauthorized IP is detected at any time the alarm should be activated

System Hardening

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

- Create an admin/service account to manage the secret_folder
- Encrypt files and folders
- Implement a strong password policy
- Apply lock-out policy when multiple failed login attempts are made

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Whenever the WebDav directory gets access requests or access from unauthorized IPs, the alarm gets triggered

What threshold would you set to activate this alarm?

- If any requests are made from unauthorized IPs, alert email and log the event

System Hardening

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

- Whitelist specific IP addresses which needs to access WebDav directory

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- An alarm to detect any upload requests to the server from non-trusted source

What threshold would you set to activate this alarm?

- Alert an admin via email when any upload requests are made on protected folders/directories

System Hardening

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

- Whitelist certain credentials and IP addresses which have granted access
- Whitelist the specific ports that can access the critical machine
- Blacklist known malicious file type from uploads, such as, .php.

*The
End*