

Capstone Engagement

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

Table of Contents

This document contains the following sections:

01

Network Topology

02

Red Team: Security Assessment

03

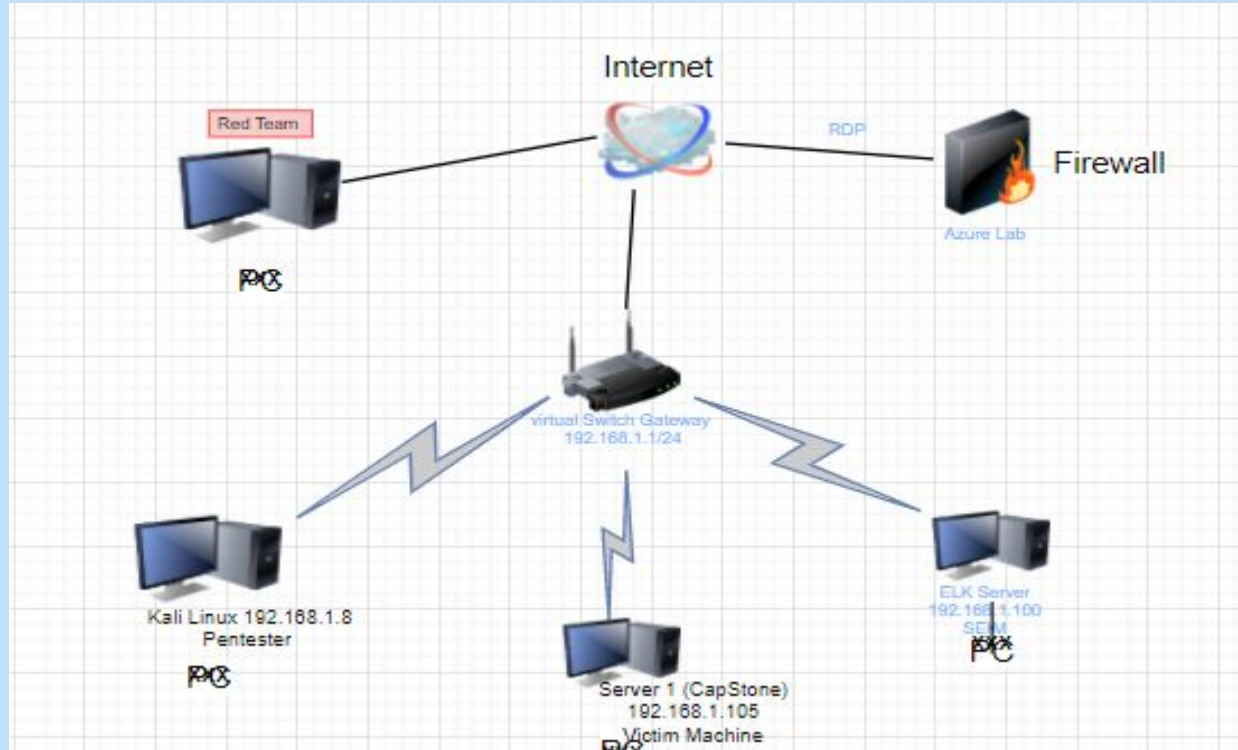
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

Address Range:

192.168.1.1

Netmask:

/24 255.255.255.0

Gateway:

192.168.1.1

Machines

IPv4: 192.168.1.8

OS: Debian Kali 5.4.0

Hostname: Kali

IPv4: 192.168.1.105

OS: Ubuntu 18.04

Hostname: Server 1 (Capstone)

IPv4: 192.168.1.100

OS: Ubuntu 18.04

Hostname: Elk

IPv4: 192.168.1.1

OS: Windows 10 Hyper-V

Hostname: Azure Host Machine



Red Team Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure Host Machine	192.168.1.1	Windows 10 Hyper-V gateway
Kali Linux	192.168.1.8	Penetration Tester
Capstone (Server 1)	192.168.1.105	Target running the vulnerable Apache web server.
Elk	192.168.1.100	SEIM the Elastic Search, Logstash, Kibana

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Web Server Directory List	Directory listing is a web server function that displays the directory content when there is no index file in a specific website directory or when the function is left on.	It is dangerous to leave this function turned on because it leads to information disclosure on the web server. Example - Exposed folder structures and files.
Vulnerable Password	Brute Force Attack in this case is when a wordlist is used against a user to guess/submit many passwords in order to find the password that belongs to a user.	The attacker used a Brute Force Attack which allowed them to crack and gain users password.
PHP Reverse TCP Shell Script	Executable file(payload) that can be uploaded to the web server.	The attacker was able to upload a PHP reverse shell script using WebDav to gain access to the web server to then execute it.

Exploitation: [Name of First Vulnerability]

01

Tools & Processes

Ifconfig:

Used to discover the Kali Linux machine IP to then discover the subnet.

Nmap:

Used to scan all IPs on the network (knowing the subnet from ifconfig) to return machines and services running.

02

Achievements

Uncovered:

Apache server located at 192.168.1.105

The list of directories on the Apache server in the Nmap result.

The open ports of 22 and 80.

03

```
root@kali:~# nmap -sn 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2021-12-07 19:58 EST
Nmap scan report for 192.168.1.1
Host is up (0.00066s latency).
MAC Address: 00:15:5D:00:04:03 (Microsoft)
Nmap scan report for 192.168.1.100
Host is up (0.00080s latency).
MAC Address: 00:15:5D:00:04:01 (Microsoft)
Nmap scan report for 192.168.1.105
Host is up (0.00087s latency).
MAC Address: 00:15:5D:00:04:02 (Microsoft)
```


Exploitation: [Name of Second Vulnerability]

01

Tools & Processes

Hydra:

Used to run a list of common passwords against user Ashton.

Wordlist:

In this case rockyou.txt was used to brute force attack user Ashton's password with Hydra.

02

Achievements

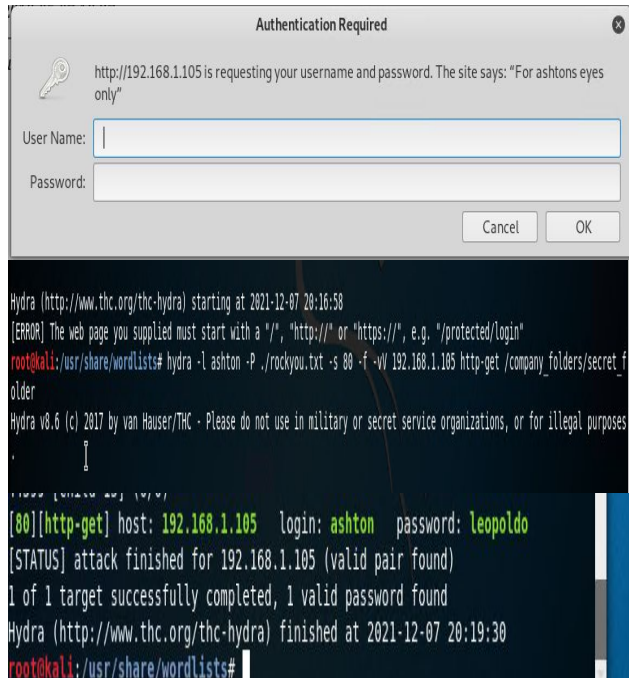
Hydra cracked user Ashton's password with the wordlist

Authentication into secret_folder that user Ashton had to access to.

Uncovered:

A "Personal Note" was then found with Ryan's credentials to the server.

03



Exploitation: [Name of Third Vulnerability]

01

Tools & Processes

Metasploit/ MSFvenom:

Used MSFvenom (in Metasploit) to find a PHP reverse TCP shell script, create a shell.php payload and Meterpreter session.

02

Achievements

Successfully added the PHP reverse TCP payload script (shell.php) to the server.


Created a Meterpreter session to the server.

Uncovered:

Root access, more directories on the server and a flag.txt

03

```
msf exploit(multi/handler) > exploit file Size Description
[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.8:4444 -> 192.168.1.105:54586) at 2021-12-08 02:32:30
meterpreter > cd /
meterpreter > ls /
Listing: /
=====
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80
Mode      Size      Type Last modified      Name
----      -
40755/rwxr-xr-x 4096    dir  2019-05-07 14:10:19 -0400 bin
40755/rwxr-xr-x 4096    dir  2020-09-03 12:07:41 -0400 boot
40755/rwxr-xr-x 3840    dir  2021-12-07 19:02:07 -0500 dev
40755/rwxr-xr-x 4096    dir  2021-01-28 10:25:41 -0500 etc
100644/rw-r--r-- 16      fil  2019-05-07 15:15:12 -0400 flag.txt
```



Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Summary of Analysis



- The port scan occurred on Dec. 8th 01:04 AM.
- 4 Packets were sent to IP 192.168.1.8 (attacker)
- Based on port scan User Agent was a NMAP Scripting Engine.

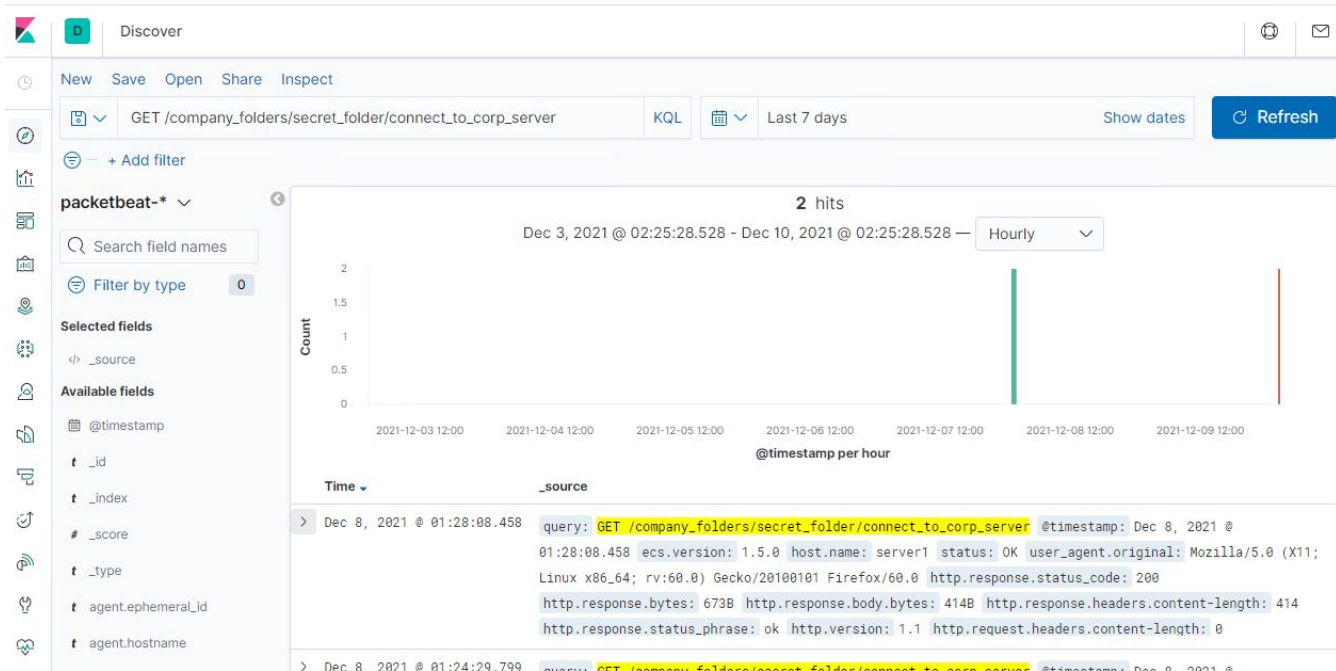


Analysis: Finding the Request for the Hidden Directory

Summary of Analysis



- Requested occurred @ 01:28 AM.
- 2 request were made to secret_folder/connect_to_corp_server
- The file requested was access.log and this secret_folder contained a “Personal Note” with user Ryan’s credentials and how to get to the server.

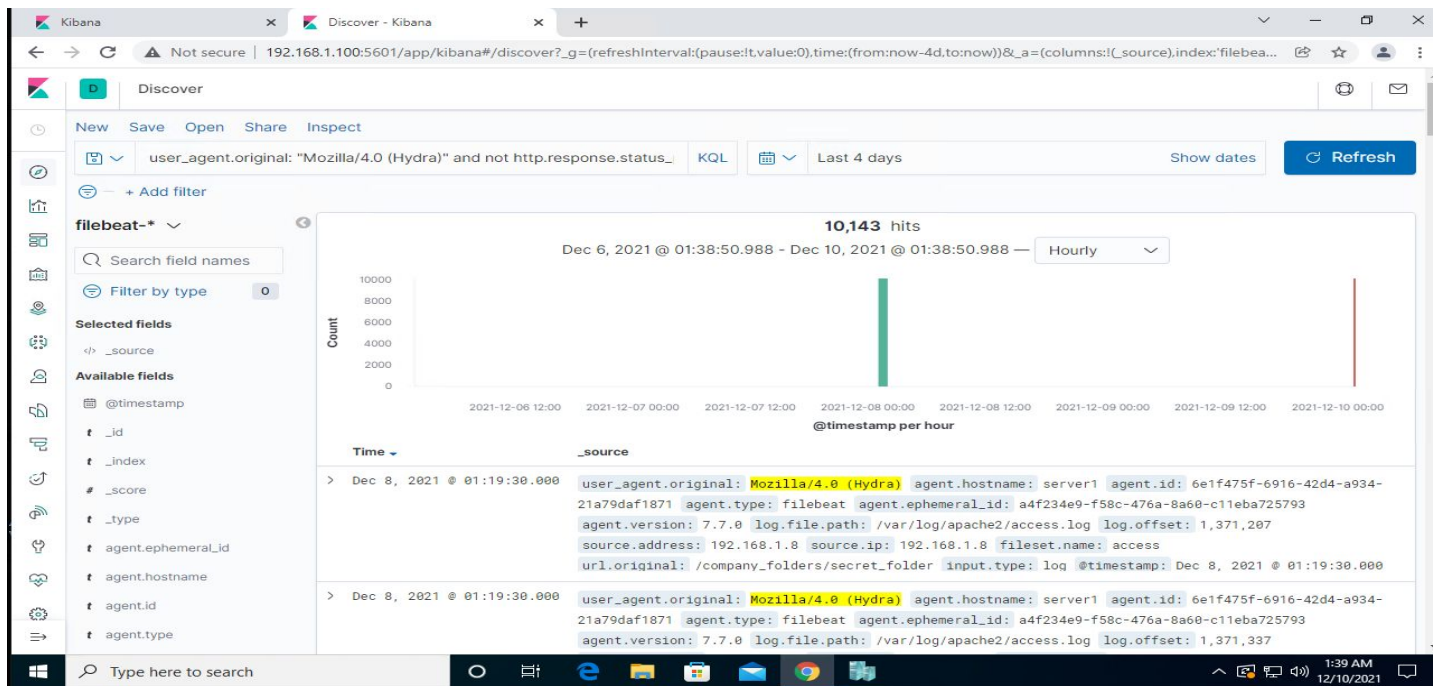


Analysis: Uncovering the Brute Force Attack

Summary of Analysis



- 10,143 request were made in the attack.
- 10,142 requests had been made before the attacked discovered the password.

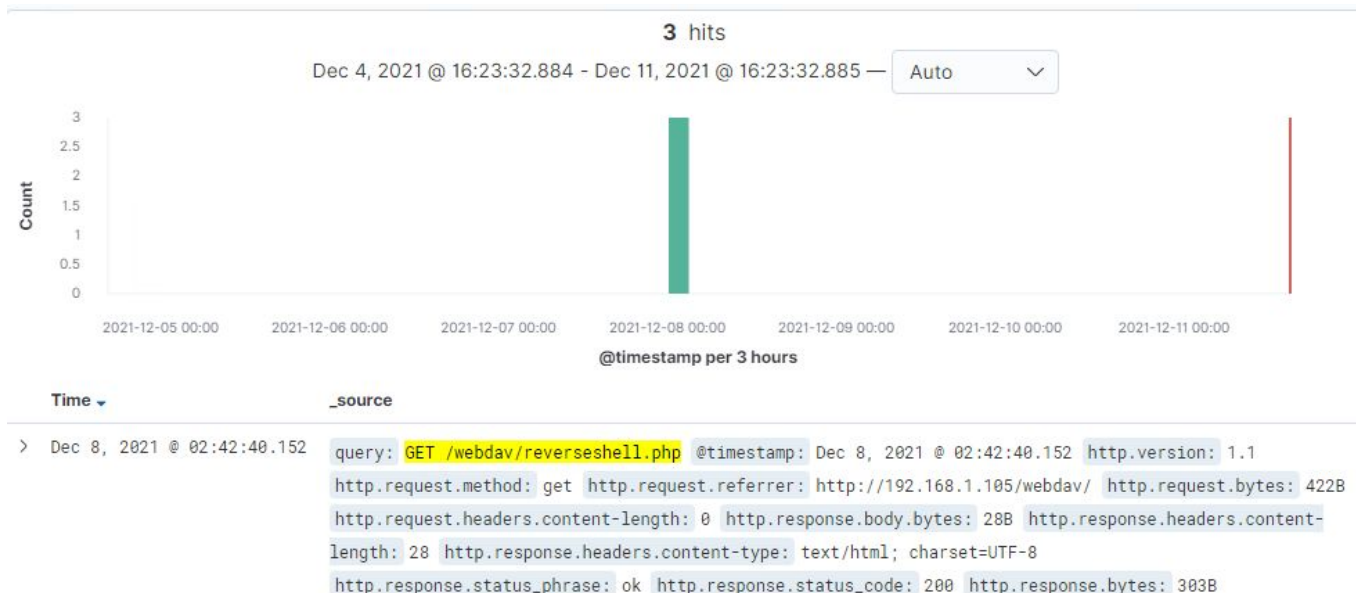


Analysis: Finding the WebDAV Connection

Summary of Analysis



- 3 request were made to the WebDav directory.
- The files requested were reverse shell.php and passwd.dav





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?

Alarms can be set off when:

- Any traffic to a port that contains Nmap as the User Agent or any other suspicious User Agents that run port scans.

What threshold would you set to activate this alarm?

Thresholds that activate the alarm:

- If a single IP address with a User Agent Nmap (for example) or any other suspicious User Agents attempts to access more than 3 ports.

System Hardening

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

- Create / add a rule in to a firewall or IDS to block any IP address that attempts to access more than 3 ports.
- Create / add a deny list of User Agents to be applied to firewall rules or an IDS.
- Close off any ports that are non essential to business.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Alarms can be set off when:

- There is an excessive or abnormal amount of traffic to the hidden directory.
- An unknown IP or device accesses the directory.

What threshold would you set to activate this alarm?

Thresholds that activate the alarm:

- If any unknown IP or device attempts to access the folder.
- If there is a sudden increase of requests and traffic to the hidden folder.

System Hardening

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

- Create / add a access list of known IPs and devices to be applied to firewall or IDS.
- Create a rule to block excessive amounts of traffic from unknown IPs and devices.
 - Create / add a deny list of IPs and devices (if needed) to firewall or IDS.

Mitigation: Preventing Brute Force Attacks

Alarm

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

Alarms can be set off when:

- There are an excessive amount of 401 (unauthorized) responses.
- There is an excess or abnormal amount of traffic from a single IP or device.

What threshold would you set to activate this alarm?

Thresholds that activate the alarm:

- If there are 3 or more unsuccessful logins.
- If there is a sudden increase of traffic from a single IP or device outside of the trusted list.

System Hardening

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

- Create / add a access list of known IPs and devices to a firewall or IDS.
- Create a rule to block any traffic returning an excess amount of 401 response codes.
- Lockout an account with an excess amount of bad logins.
- Add IPs or devices to a deny list if they are creating an excessive amount of traffic.

Mitigation: Detecting the WebDAV Connection

Alarm

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

Alarms can be set off when:

- Any new outbound traffic from the web server is detected.
- Any new machine is connected or establishes a connection to the web server.
- A user access the web server.

What threshold would you set to activate this alarm?

Thresholds that activate the alarm:

- If any outbound traffic is happening to a new machine.
- Anytime a user access the web server.

System Hardening

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

- Limit access to the WebDav server to those IPs or devices within the company's network.
 - Create / add a access list of known IPs, devices and users to a firewall or IDS.
 - Create / add a rule to block unknown IPs and devices to a firewall or IDS.
- Add restrictions and rules as to who can access or use the web server.
- Require strong passwords and regular password changes.
- State what information is allowed on the server. Ex. create a rule against storing credentials on the server.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Alarms can be set off when:

- A file is created or added to the server.
- A file extension like .php or any other server side scripting language extension is detected.
- A new outbound connection to a new port / machine is detected.

What threshold would you set to activate this alarm?

Thresholds that activate the alarm:

- Anytime a file or script file is created or added to the server.
- Anytime a new IP or device accesses the server.

System Hardening

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

- Configure a stateful firewall / IDS to detect when an original outbound connection to a new port and machine happens.
- Create / add a access list of known IPs, devices and users to a firewall or IDS.
- Close off any ports that are non essential to business.
- Add a rule to block traffic to any default ports tools such as Meterpreter use for connection.
 - Create / add a deny list of any IPs and devices trying to access port 4444 (Meterpreters default)

*The
End*