



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

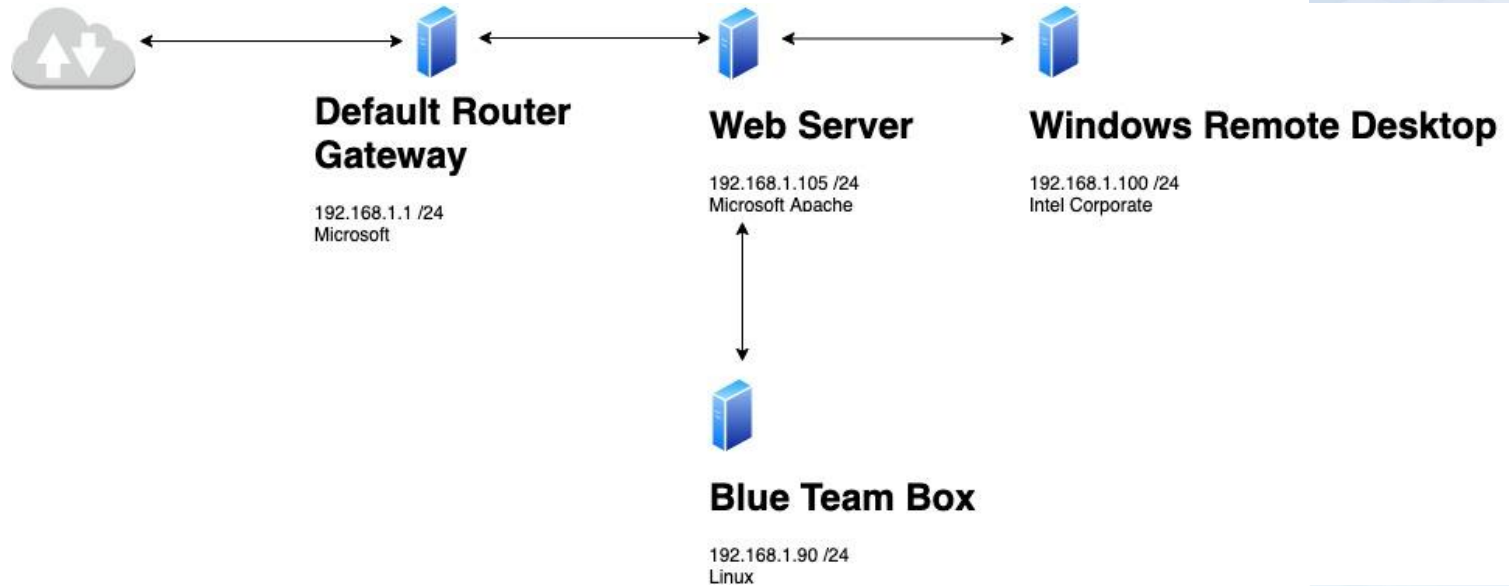
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



The background of the slide is a dark red, almost black, field filled with a complex, repeating geometric pattern of triangles and polygons in various shades of red and maroon, creating a textured, mosaic-like effect.

Red Team Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Microsoft vendor	192.168.1.1	Default gateway
Intel Corporate vendor	192.168.1.100	Windows Remote Desktop
unknown	192.168.1.90	Red Team box
Microsoft vendor	192.168.1.105	Blue Team box

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open port 22	Port 22 which supports SSH secure logins/file transfers/port forwarding is in OPEN state.	An attacker who has the password of this port can gain remote access and upload files, escalate privilege & take over system.
Open port 80	Port 80 which supports unencrypted web browsing is in OPEN state.	An attacker is able to gain access to back end via web facing server and upload files, escalate privilege & take over system.

Exploitation #1: [Open port 22]

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

Nmap was used to find the IP address of the box. By inputting the IP in a web browser, the site's web facing pages were found, users' IDs found and passwords cracked with Hydra. Using these login credentials, we could then SSH in to that box as said user.

02

Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

The exploit gave me a user shell access and see that many other user's folder also have write access, and also navigate to the /etc folder where critical information such as SSH, sudoers and shadow files are located.

03

[INSERT: screenshot or command output illustrating the exploit.]

```
root@Kali:~# ssh ryan@192.168.1.105
ryan@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-108-generic x86_64)
```


Exploitation #2: [Reverse Shell]

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

Nmap was used to find the IP address of the box. By inputting the IP in a web browser, the server's web facing pages were found. Cyberchef was used to crack a MD5 hash. Hydra was used to brute force a 2nd user's password. MSF venom was used to create a payload and start a reverse shell on the victim.

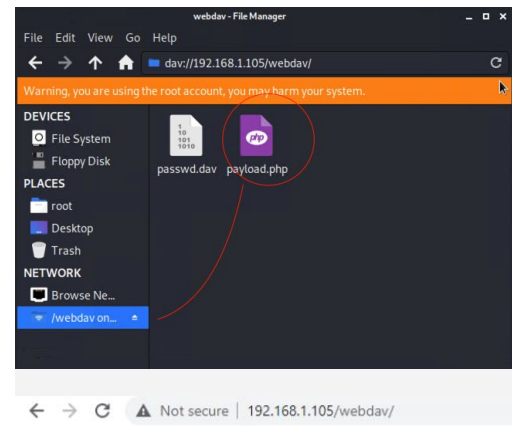
02

Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc

The exploit allowed me to login to the victim's file share via my Kali box's file manager, and upload a .php reverse shell script which i then went ran on the website. I could then listen in to all traffic happening on that server.


03



Index of /webdav

Name	Last modified	Size	Description
Parent Directory	-	-	-
passwd.dav	2019-05-07 18:19	43	
payload.php	2021-06-11 01:04	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



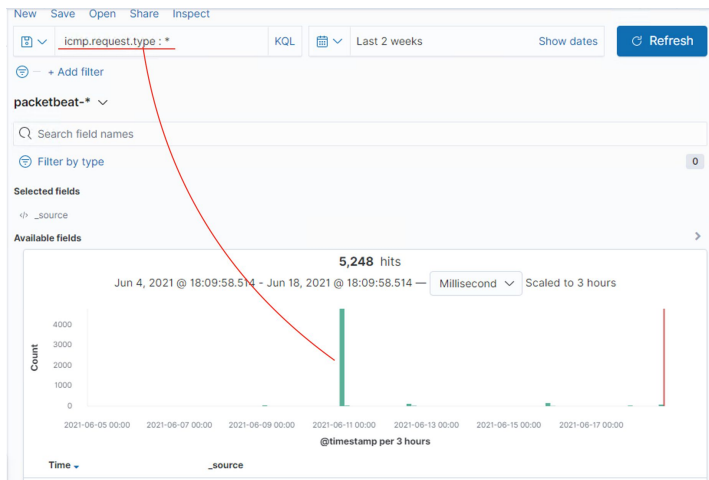
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?



The port scan started on 6/10 circa 11pm.

4777 packets were sent from IP 192.168.1.90.

The flood of ICMP packets indicate that a malicious machine may be using NMAP to send lots of SYN/ACK packets, to try and determine which port will respond thereby show itself to be open for penetration.

```
> Jun 10, 2021 @ 23:18:58.254 @timestamp: Jun 10, 2021 @ 23:18:58.254 network.bytes: 112B network.type: ipv4
network.transport: icmp network.direction: inbound
network.community_id: 1:8oSsNFpo3Mzjqss1QqWy+CTz5nA= type: icmp source.ip: 192.168.1.90
source.bytes: 56B client.ip: 192.168.1.90 client.bytes: 56B status: OK
destination.bytes: 56B destination.ip: 192.168.1.105 host.name: server1
```

Analysis: Finding the Request for the Hidden Directory



- What time did the request occur? How many requests were made?
- Which files were requested? What did they contain?

Top 10 HTTP requests [Packetbeat] ECS

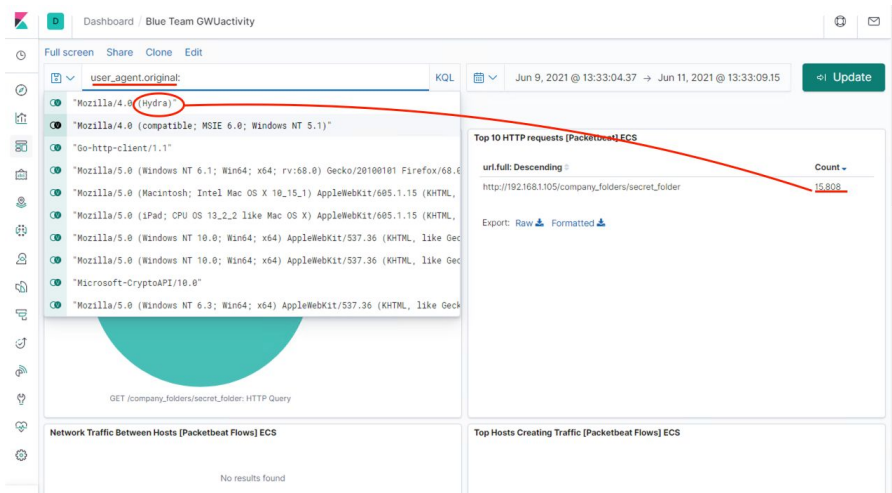
url.full: Descending ▾	Count ▾
http://192.168.1.105/company_folders/ <u>secret_folder</u>	15,816
http://127.0.0.1/server-status?auto=	4,213
http://snnmnkxdhflwghqismb.com/post.php	490
http://www.gstatic.com/generate_204	245
http://ocsp.godaddy.com	132

15,816 requests were made for the hidden directory '/secret folder' circa 6/10 at 11:30pm.

To see the files requested, the raw data was exported as a .csv file and we can grep information from anything that is associated with the machine being attacked (192.168.

Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack?
- How many requests had been made before the attacker discovered the password?



There were 15,808 requests made. This is discovered with the 'user_agent.original' filter on Kibana to check out suspicious user agent names. "Mozilla.4.0 (Hydra)" was found using this method and from there, could be determined that Hydra was used for the brute force attack.

Analysis: Finding the WebDAV Connection

Only 7 requests were made to the /webdav folder with majority of it being a client side 'lack of authorization' error. There appeared to be 2 successful HTTP transactions in one of those requests that was successful.



Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

A threshold alarm can be set to trigger an email to be sent to the SOC team should there be excessive SYNACK type connections over port 80 at non-traditional work hours.

System Hardening

To mitigate such attacks, there can be a firewall with IPS with rules to filter out packets that occur at abnormal rates, or close the port when the rules detect signatures of port scan attacks.

We can also create a firewall rule that silently drops all PING requests.

Mitigation: Finding the Request for the Hidden Directory

Alarm

To detect future motions on directories that contain sensitive files and information, an alert rule can be created to notify the SOC team should the folder incur any activity on a read/write/execute permission type.

System Hardening

We can harden such directories with sensitive information, by placing such directories on a different subnet than the one that contains vulnerable/public facing machines such as web servers etc.

Such directories with sensitive information may also be subject to tampering with. We should also hash the directories' content to ensure data integrity.

Mitigation: Preventing Brute Force Attacks

Alarm

An alarm can be set to prevent Brute Force Attacks, that gets triggered when authentication events occur more than a specific number of times possibly within a minute, and also a temporal lockdown of the authentication after specific number of unsuccessful attempts.

System Hardening

To mitigate such attacks on folders that are password protected, there can be a firewall with IPS with rules to filter out authentication-type packets that occur at abnormal rates, or close the port when the rules detect signatures of port scan attacks.

Mitigation: Detecting the WebDAV Connection

Alarm

To detect future motions on directories that contain sensitive files and information, an alert rule can be created to notify the SOC team should the folder incur any activity on a read/write/execute permission type.

System Hardening

The WebDAV folder seems to be a type of shared internal folders, but does not seem to have any relevance to the functionality of the company's public facing website. It should not sit on the same subnet as the webserver. It should ideally be on the company's intranet, accessible via VPN for remote workers if needed.

Mitigation: Identifying Reverse Shell Uploads

Alarm

An alert can be set up to send the SOC team an email, should any files with extensions that are uncommon to ordinary users such as .php or .exe or .sh.

Should there be users who are in the programming department and use such types of files daily, must sign an agreement to adhere to certain rules while using the system or risk penalties.

System Hardening

The folder can be set to read-only, and also further restricted read/write/execute for users of all lower policy groups.

*The
End*