Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

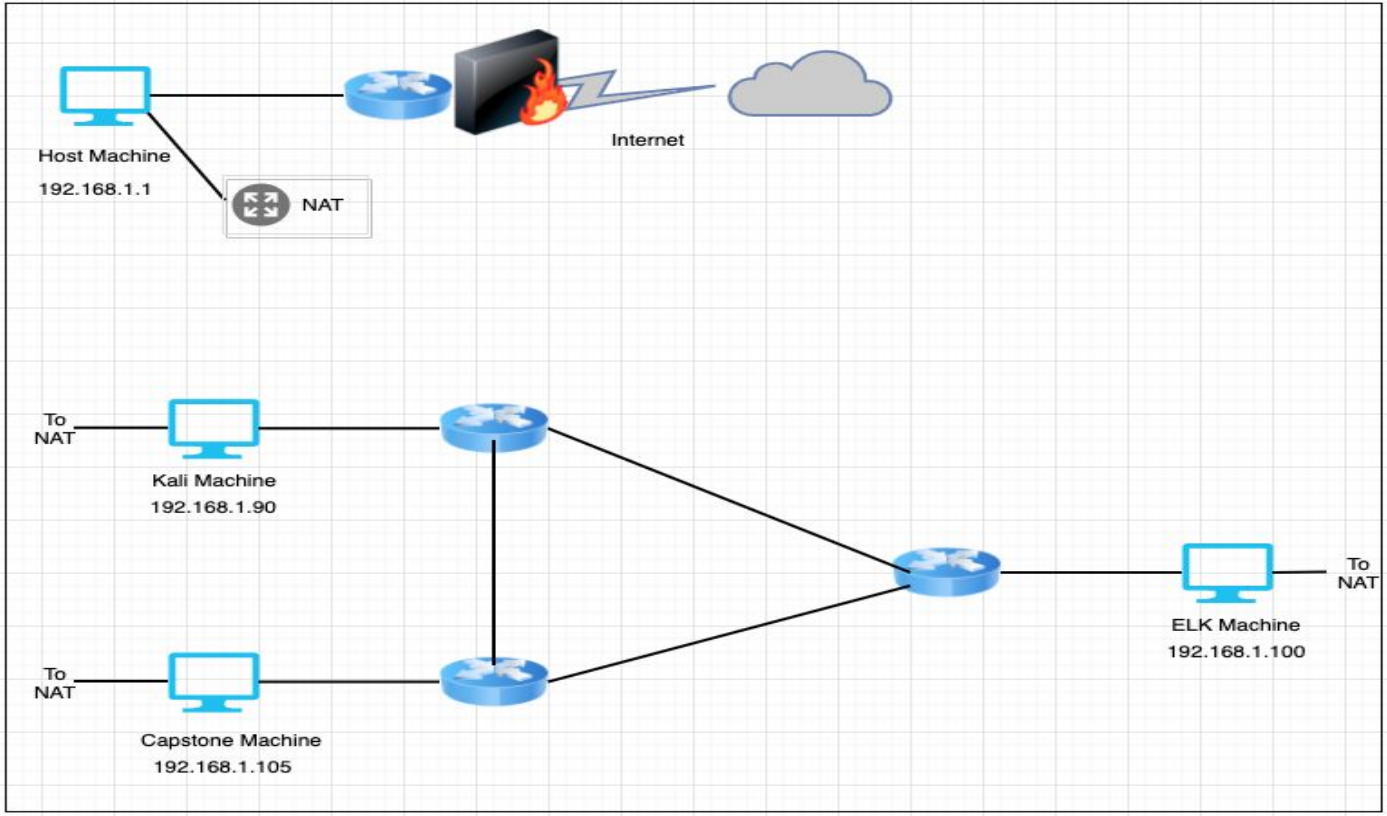
- Liquan (Q) Bai

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



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

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

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.90
OS: Linux 2.6.32
Hostname: Kali

```
root@Kali:~# nmap --iflist
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-28 08:43 PDT
************************INTERFACES************************
DEV  (SHORT) IP/MASK                     TYPE     UP MTU   MAC
lo   (lo)    127.0.0.1/8                 loopback up 65536
lo   (lo)    ::1/128                     loopback up 65536
eth0 (eth0)  192.168.1.90/24             ethernet up 1500  00:15:5D:00:04:12
eth0 (eth0)  fe80::215:5dff:fe00:412/64  ethernet up 1500  00:15:5D:00:04:12

**************************ROUTES**************************
DST/MASK                    DEV  METRIC GATEWAY
192.168.1.0/24              eth0 0
0.0.0.0/0                   eth0 0      192.168.1.1
::1/128                     lo   0
fe80::215:5dff:fe00:412/128 eth0 0
::1/128                     lo   256
fe80::/64                   eth0 256
ff00::/8                    eth0 256

root@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
ELK	192.168.1.100	ELK server
Capstone	192.168.1.105	Targeting machine
Kali	192.168.1.90	Attacking machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-1999-0661	A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1 f, (4) IRC client (IrcII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6	This vulnerability affects confidentiality, integrity, and availability
CVE-2012-2516	An ActiveX control in KeyHelp.ocx in KeyWorks KeyHelp Module (aka the HTML Help component), as used in GE Intelligent Platforms Proficy Historian 3.1, 3.5, 4.0, and 4.5; Proficy HMI/SCADA iFIX 5.0 and 5.1; Proficy Pulse 1.0; Proficy Batch Execution 5.6; SI7 I/O Driver 7.20 through 7.42; and other products	This vulnerability allows remote attackers to execute arbitrary commands via crafted input, related to a "command injection vulnerability.“

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2013-2249	mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID	unspecified impact and remote attack vectors
CVE-2012-2379	Apache CXF 2.4.x before 2.4.8, 2.5.x before 2.5.4, and 2.6.x before 2.6.1, when a Supporting Token specifies a child WS-SecurityPolicy 1.1 or 1.2 policy, does not properly ensure that an XML element is signed or encrypted	unspecified impact and attack vectors

Exploitation: web server files are accessible

01

Tools & Processes
Used nmap to scan open ports and potential vulnerabilities of target machine.

02

Achievements
Target machine port 80 and port 22 are open. Some important information, files, folders, such as the share_folders and other folders on the target machine (web server) was able to be accessed via web browser.

Exploitation: web server files are accessible

Index of /

192.168.1.105

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

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

Exploitation: secret hidden file is accessible

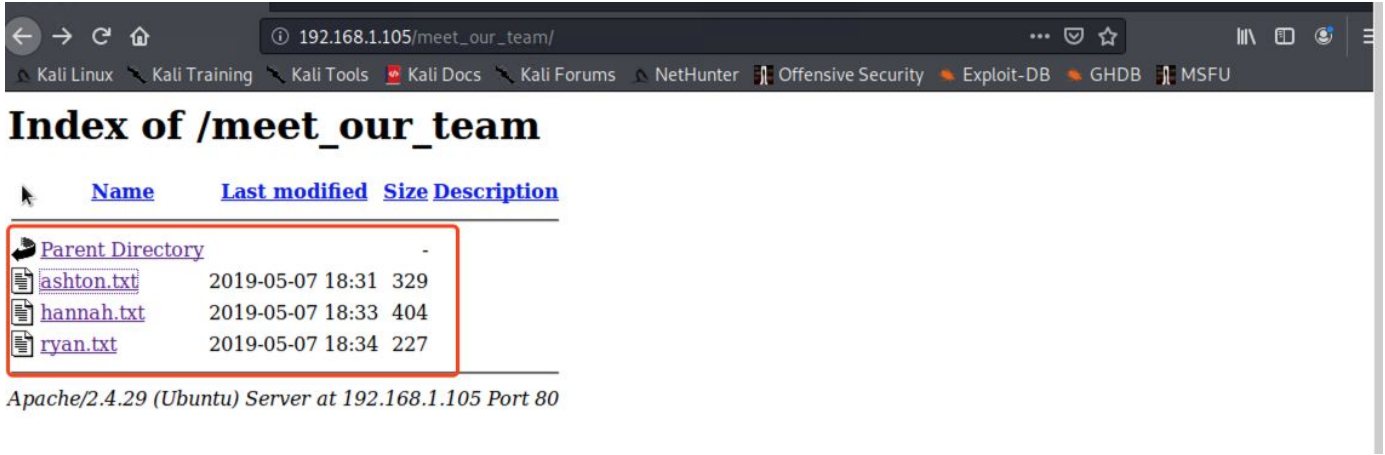
01

Tools & Processes
Used Hydra to crack employee's (ashton) login password

02

Achievements
Successfully cracked employee ashton's login credentials for accessing the secret hidden file to gather more information from target machine

Exploitation: secret hidden file is accessible




```
root@Kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -s 80 -f 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 2020-07-22 0
8:13:57
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l
:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.1.105:80/company_folders/secret_folder

[STATUS] 8751.00 tries/min, 8751 tries in 00:01h, 14335648 to do in 27:19h, 16 active
[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 2020-07-22 08:15:12
root@Kali:/usr/share/wordlists#
```

Exploitation: secret hidden file is accessible

192.168.1.105/company_folders/secret_folder/

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

Index of /company_folders/secret_folder

Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

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 | GHDB | MSFU

```
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: web server configuration folder is accessible

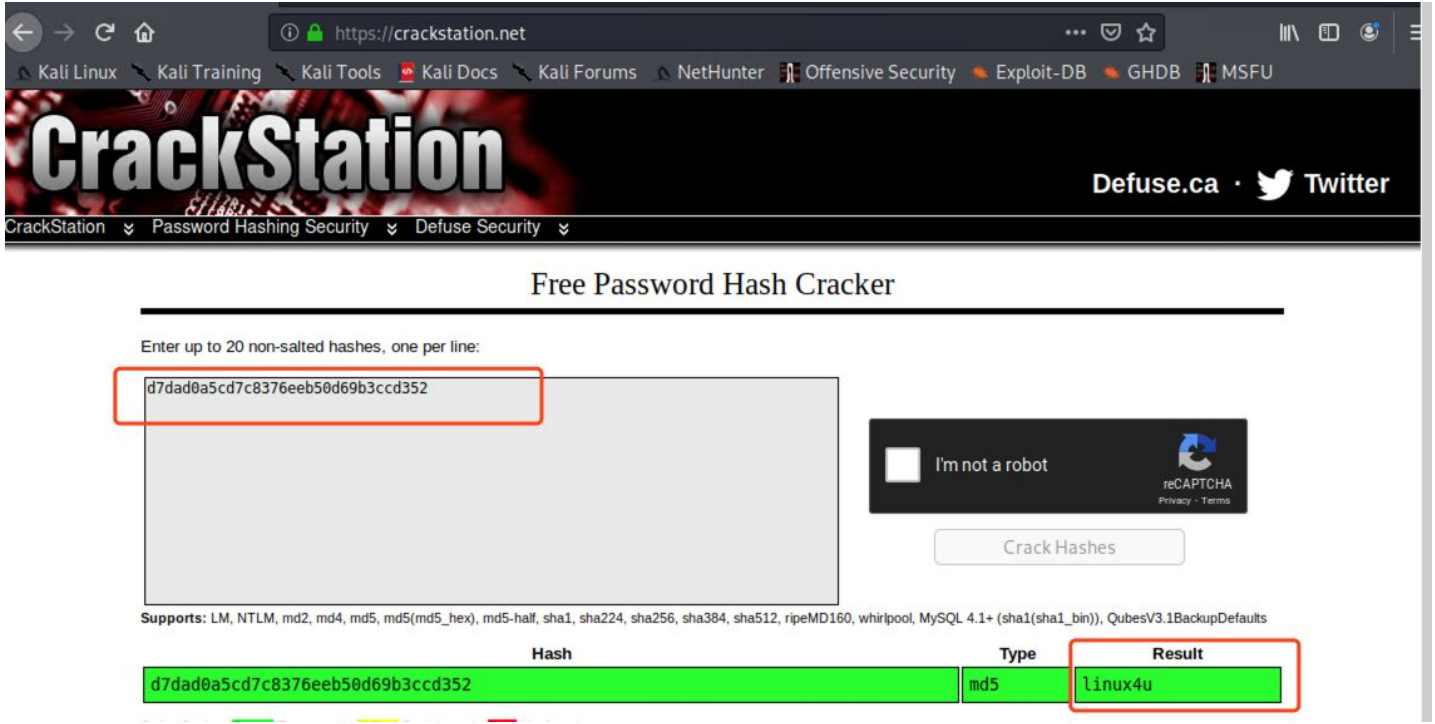
01

Tools & Processes
Used CrackStation online tool to decode ryan's password hash value which encoded with md5.

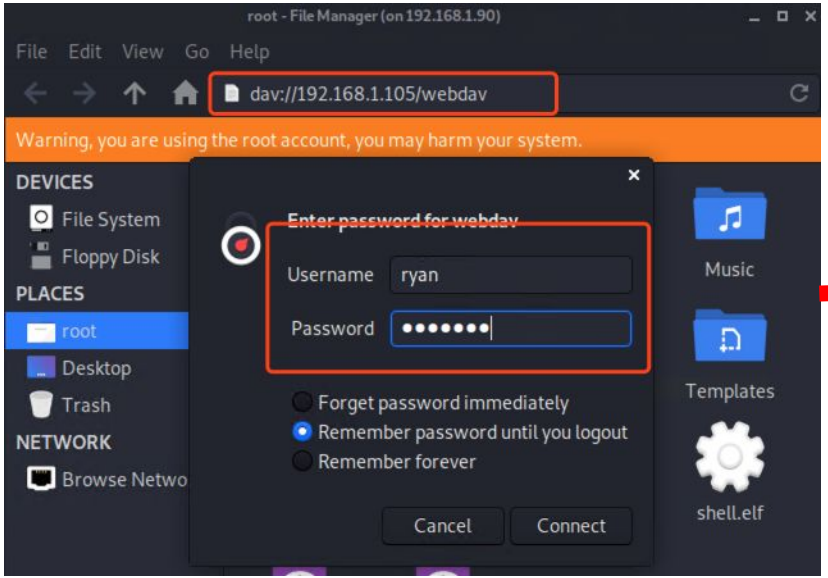
02

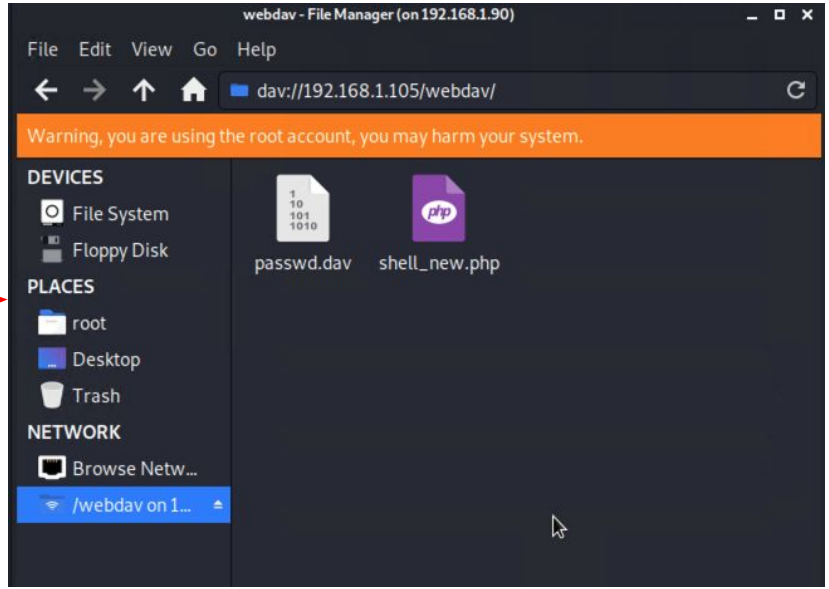
Achievements
Successfully decoded ryan's password hash value and retrieved ryan's password.

Exploitation: web server configuration folder is accessible



Exploitation: web server configuration folder is accessible



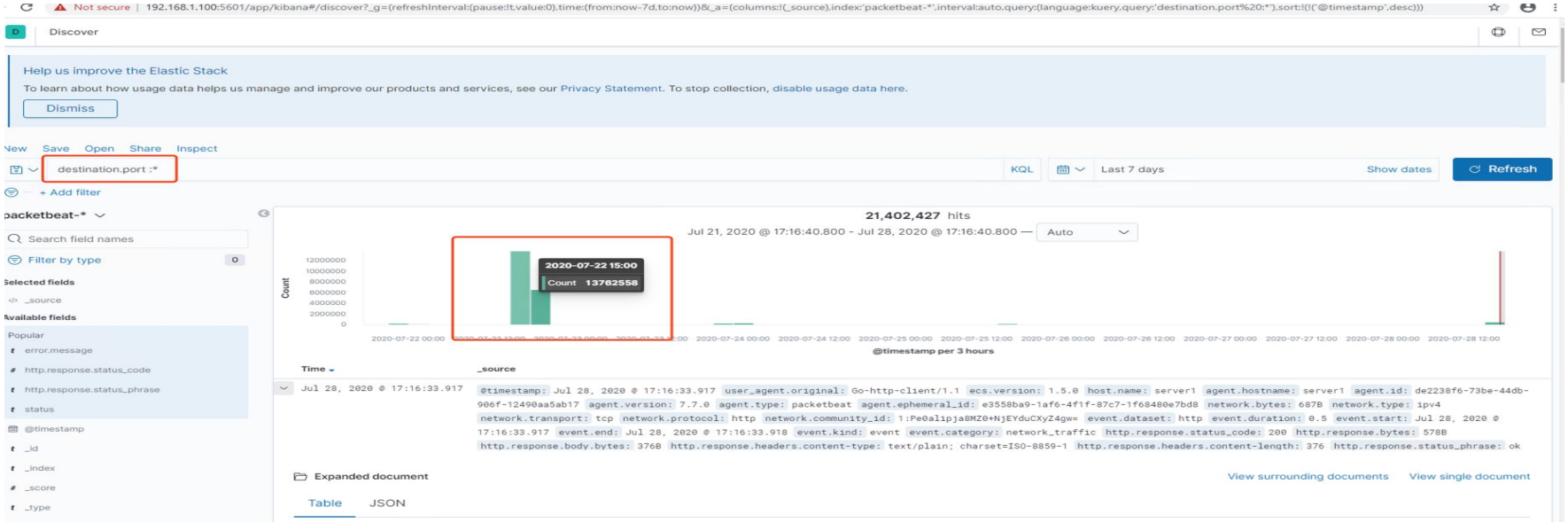


Blue Team

Log Analysis and Attack Characterization

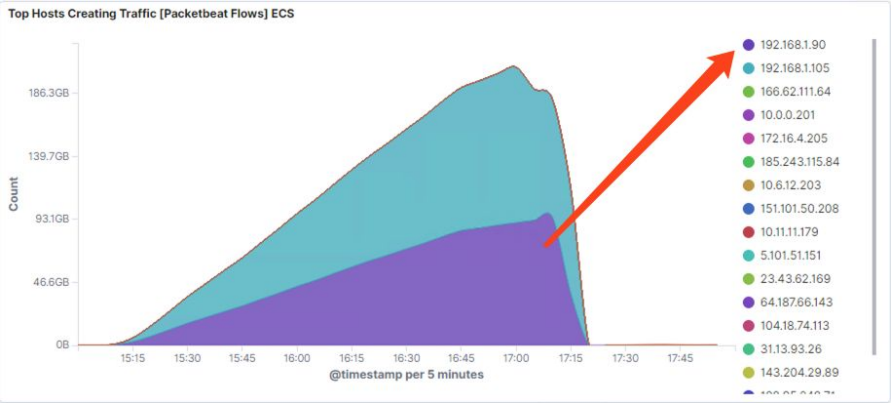
Analysis: Identifying the Port Scan

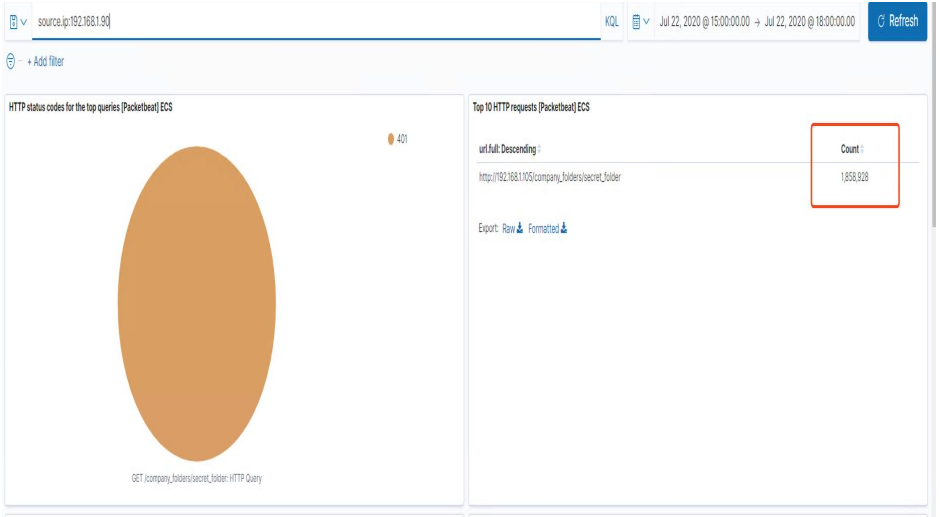
- Port scan occurred on 7/22/2020 between 15:00 - 18:00 (UTC)



Analysis: Identifying the Port Scan

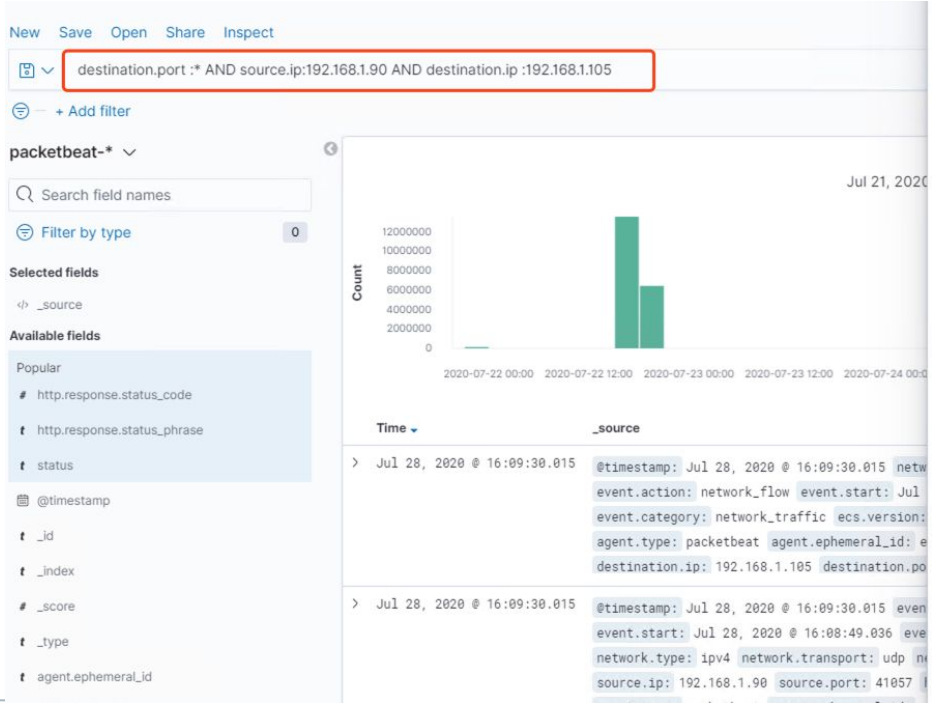
- There were 1,858,928 packets were sent from 192.168.1.90





Analysis: Identifying the Port Scan

- In very short period, there were many different ports of targeting machine were reached.




```
      "ephemeral_id": "e3558ba9-1af6-4f1f-87c7-1f68480e7bd8"
    },
    "type": "flow",
    "source": {
      "ip": "192.168.1.90",
      "port": 55497,
      "packets": 1,
      "bytes": 76
    },
    "destination": {
      "ip": "192.168.1.105",
      "port": 33435
    },
    "flow": {
      "id": "EAL/////AP////8I//8AAAHAqAFawKgBacnYm4I",
      "final": true
    }
  },
  "fields": {
    "event.end": [
      "2020-07-28T16:08:49.036Z"
    ],
    "@timestamp": [
      "2020-07-28T16:09:30.015Z"
    ],
    "event.start": [
      "2020-07-28T16:08:49.036Z"
    ]
  },
  "sort": [
    1595952570015
  ]
},
{
  "_index": "packetbeat-7.7.0-2020.07.16-000001",
  "_type": "_doc",
  "_id": "vBAvlnMBOb-c5_UUokyB",
```

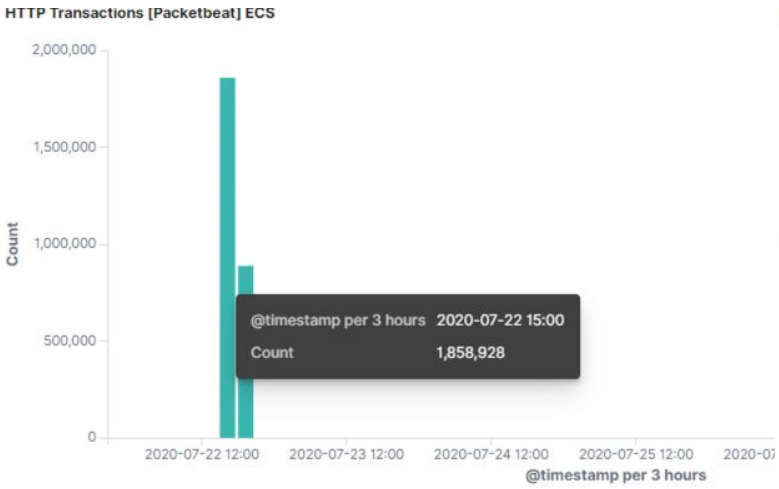
Analysis: Finding the Request for the Hidden Directory

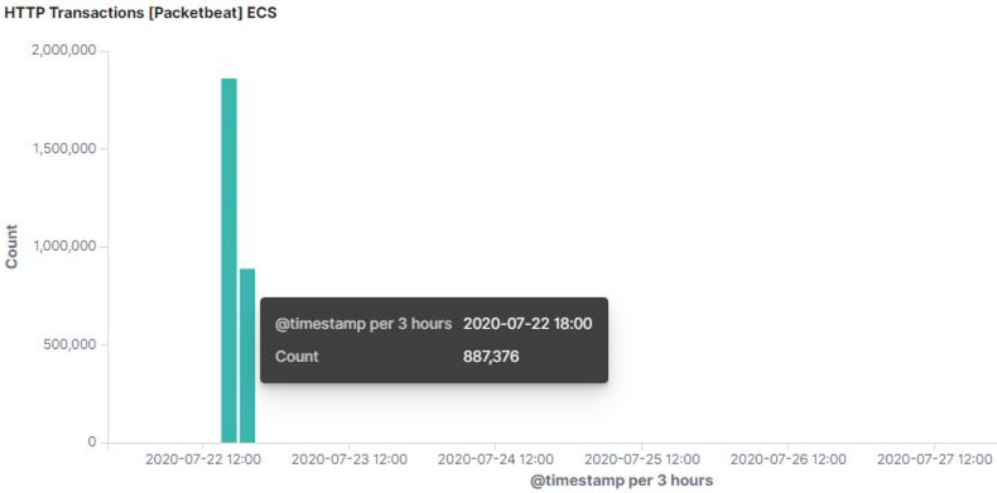
- The request occurred on 7/22/2022 between 15:00 to 18:00 (UTC)
- There were 2,746,308 requests made during this period

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	2,746,308

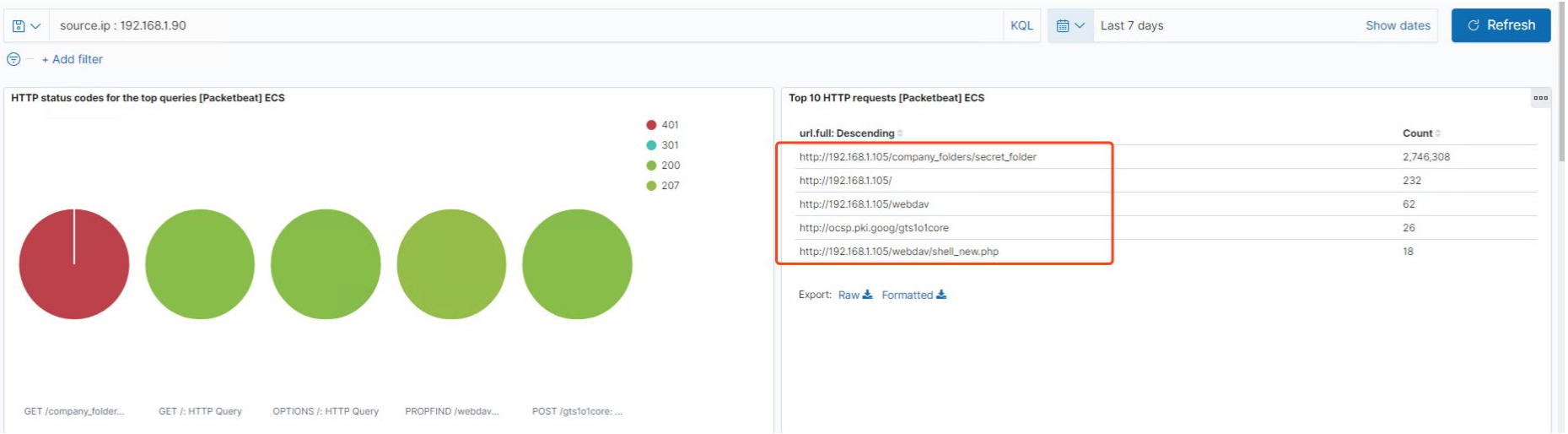
Export: Raw Formatted





Analysis: Finding the Request for the Hidden Directory

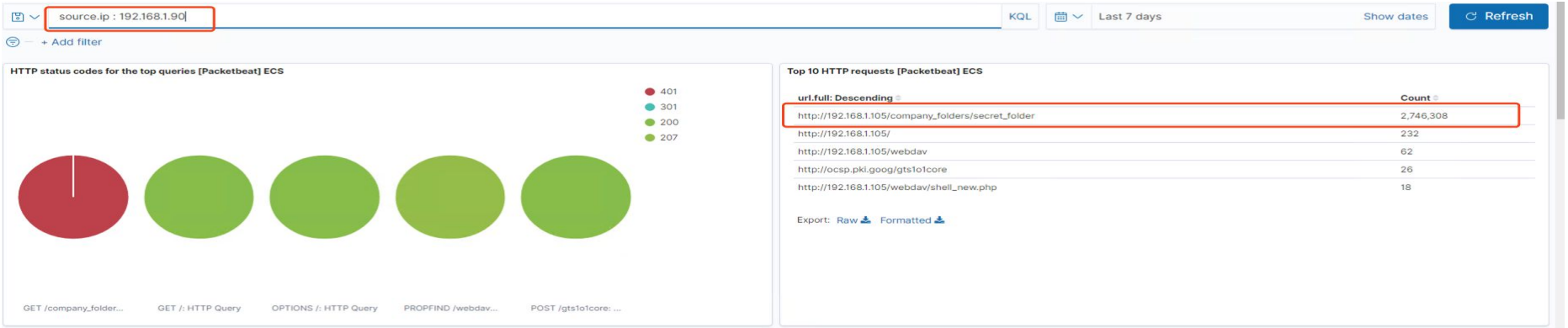
- There were other files were requested, such as /webdav, /webdav/shell_new.php, home directory (/)
- Based on the log, seems like attacker didn't go check other files in directory /company_folders, requested to access the /company_folders/secret_folder directly; /webdav contains shell_new.php file.

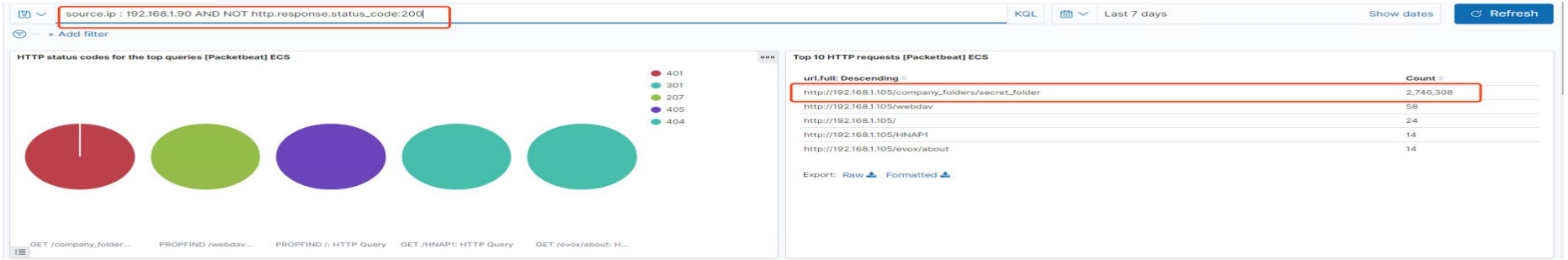


url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	2,746,308
http://192.168.1.105/	232
http://192.168.1.105/webdav	62
http://ocsp.pki.goog/gts1o1core	26
http://192.168.1.105/webdav/shell_new.php	18

Analysis: Uncovering the Brute Force Attack

- There were 2,746,308 requests made in the attack
- There were 2,746,308 requests had been made before the attacker discovered the password





Analysis: Finding the WebDAV Connection

- There were 62 requests made to this directory
- The file ‘shell_new.php’ was requested in this directory

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	2,746,308
http://192.168.1.105/	232
http://192.168.1.105/webdav	62
http://ocsp.pki.goog/gts1o1core	26
http://192.168.1.105/webdav/shell_new.php	18

Export: Raw Formatted

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 external IP send SYN to multiple internal IPs with one port
- An external IP send SYN to one internal IP with multiple ports

What threshold would you set to activate this alarm?

- One external IP send SYN to 25 internal IPs with one port in 1 min
- One external IP send SYN to one internal IP with more than 500 ports in 1 min

System Hardening

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

- Closed unused ports
- Monitoring opened ports

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Whenever the hidden directory is accessed or requested to access
- When the hidden directory is accessed from external network

System Hardening

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

- Multi-factor login
- Only allow authorized user to access the hidden directory with internal network (require using VPN)

Mitigation: Preventing Brute Force Attacks

Alarm

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

- A single user failed login multiple times in short period

What threshold would you set to activate this alarm?

- Attempts over 15 times in one minute

System Hardening

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

- Allow a single user to attempt login 3 times in 15 mins.
- Lock out the account if failed to login 3 times in 15 mins

Mitigation: Detecting the WebDAV Connection

Alarm

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

- When this directory is accessed from unauthorized user
- When this directory is accessed from external network

System Hardening

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

- Setup IDS to monitor
- Only allow authorized user access via the internal network or VPN

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Not allowed types of file uploaded occurred (ex. php)
- Un-authorized users try to upload files (especially from external network)

What threshold would you set to activate this alarm?

- Un-authorized upload attempts reach to 5 times in 10 mins
- Un-allowed type files try to be uploaded 3 times

System Hardening

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

- Require authentication to upload files
- Store uploaded files in a location not accessible from the web
- Filter certain types of file that are allowed to be uploaded

the End