

Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Group 4

Table of Contents

This document contains the following sections:

01

Network Topology

02

Red Team: Security Assessment

03

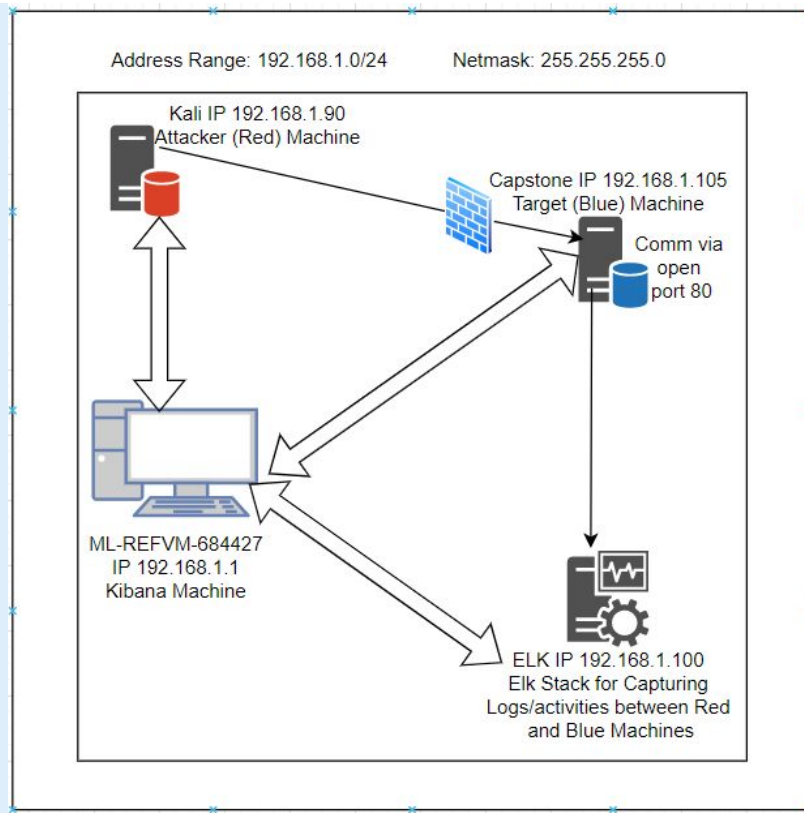
Blue Team: Log Analysis and Attack Characterization

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: 0.0.0.0

Machines

IPv4:192.168.1.90
OS: Linux
Hostname:Kali

IPv4:192.168.1.105
OS:Linux
Hostname:Capstone

IPv4:192.168.1.100
OS:Linux
Hostname:Elk

IPv4:192.168.1.1
OS:Windows
Hostname: Hyper-V
Manager

The background of the slide is a dark red, almost black, geometric pattern composed of numerous triangles and polygons of varying shades of red and maroon, creating a complex, low-poly aesthetic.

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 for the Machine Cloud, using the Hyper-V application to handle Kali, Elk, and Capstone.
Kali	192.168.1.90	The Attacker Machine was used to break into the Capstone machine.
Elk	192.168.1.100	Logs from Capstone Machine's Filebeat, Metricbeat, and Packetbeat are collected and shown in Kibana.
Capstone	192.168.1.105	ELK receives log data from Apache Server and Target Machine.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80	An open port allows attackers to try a variety of infiltration techniques.	With access to users and passwords, attackers can utilize C2 attacks to cause even more damage.
Brute Force Attack	To get access, a systematic entering of several credentials from a file is used.	Attacks can be carried out until the proper credentials are discovered if there are no preventative settings in place to stop many failed attempts.
Apache 2.4.29 CVE-2018-1312	The nonce delivered to avoid reply attacks when constructing an HTTP Digest authentication challenge was not appropriately produced using pseudo-random seed. Using a common Digest authentication setting across a cluster of servers	Attacks can be carried out until the proper credentials are discovered if there are no preventative settings in place to stop many failed attempts.

Exploitation: Open Port 80

01

Tools & Processes

Ran nmap scan

```
root@Kali:~# nmap -sV -sC 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-06 17:06 PDT
Nmap scan report for 192.168.1.105
```

02

Achievements

The scan revealed vulnerabilities and directs bad actors to a source to attack via http requests. Also noted: Servers is running an outdated version of Apache

03

```
Shell No.1
File Actions Edit View Help

9200/tcp open  http      Elasticsearch REST API 7.6.1 (name: elk; cluster: el
asticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
80/tcp    open  http      Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l

Nmap scan report for 192.168.1.90
Host is up (0.000011s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://
/nmap.org/submit/ .
Nmap done: 105 IP addresses (4 hosts up) scanned in 30.87 seconds
root@Kali:~#
```


Exploitation: Exposed Password Hash

01

Tools & Processes

Ryan's password hash was located in a folder on the webserver and cracked via crackstation.net

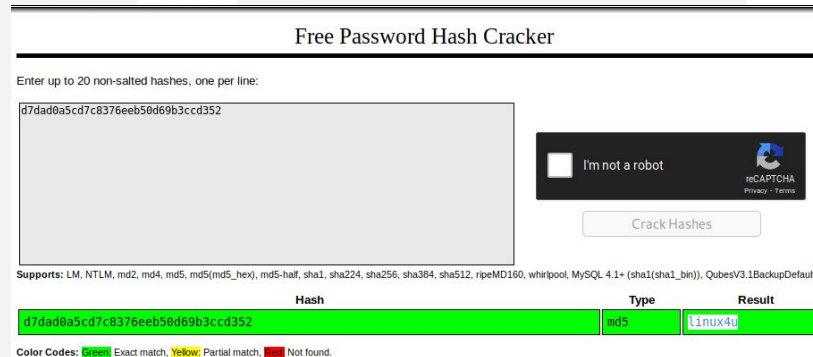
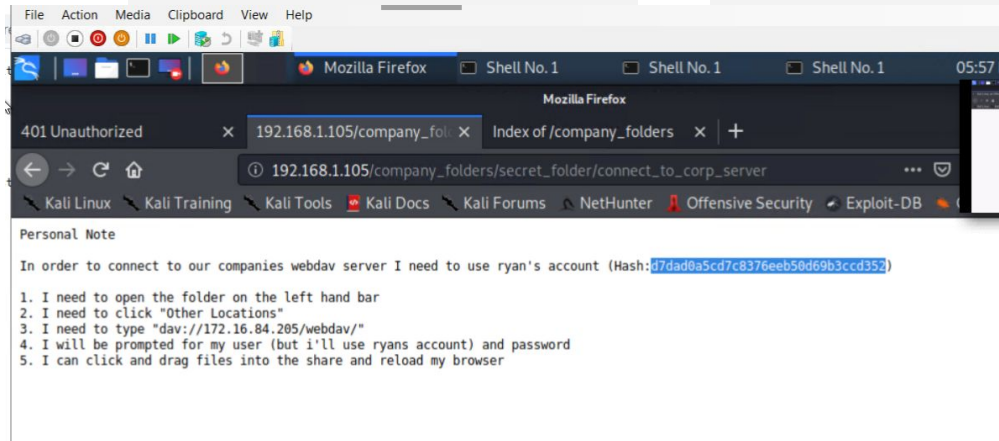
02

Achievements

The md5 hash found was cracked-Password "linux4u"

03

Screenshots



Exploitation: Weak Password Security/No MFA or 2FA

01

Tools & Processes

Used the tool hydra.

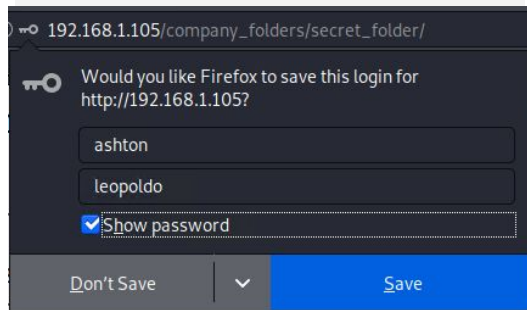
Executed the following command to try password list:

```
oot@Kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -f -vV 192.168.1.105 http-get /company_folders/secret_folder
```

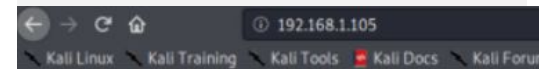
02

Achievements

Was able to crack simple password via brute force-MFA/2FA enabled would



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 18:22	-	
 meet_our_team/	2019-05-07 18:34	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Brute Force Attack

01

Tools & Processes

Used the tool hydra.

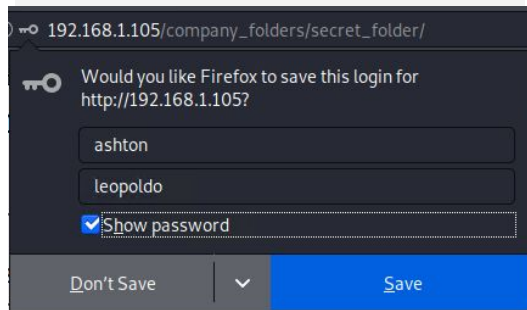
Executed the following command to try password list:

```
oot@Kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -f -vV 192.168.1.105 http-get /company_folders/secret_folder
```

02

Achievements


Was able to crack simple password via brute force-MFA/2FA enabled would



03

Screenshot

```
[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 2022-04-05 18:50:
root@Kali:/#
```

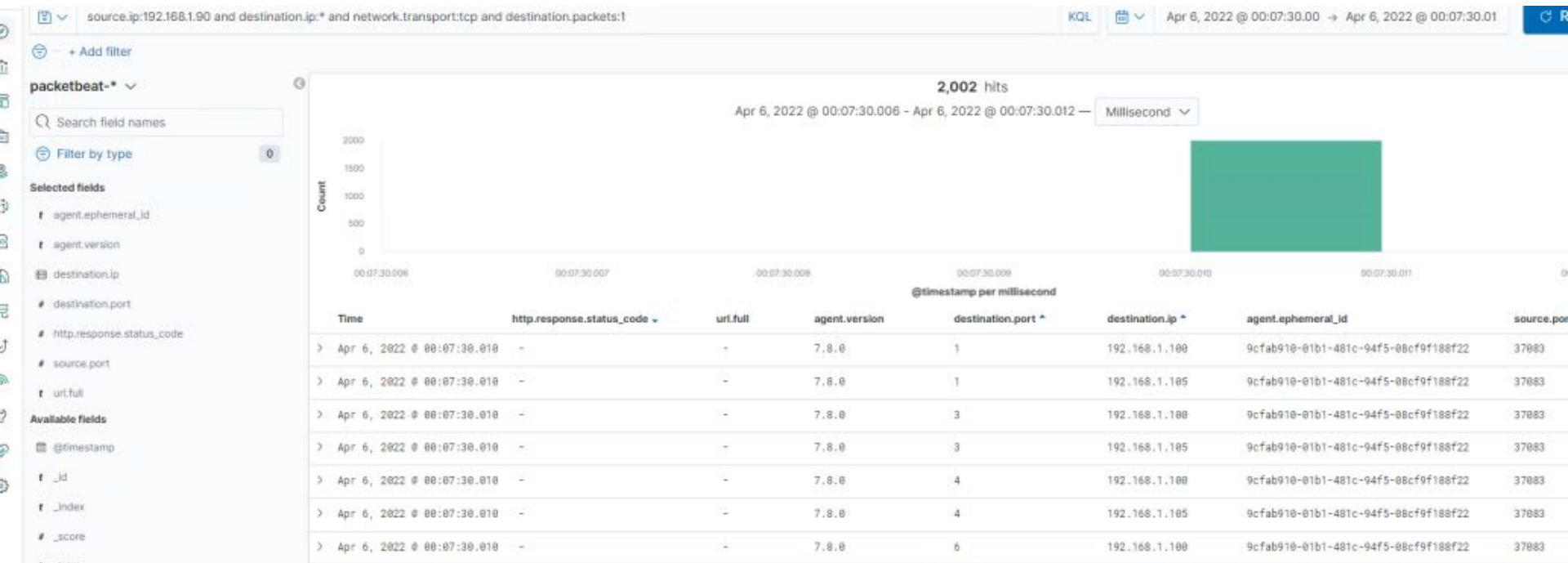


Blue Team

Log Analysis and Attack Characterization

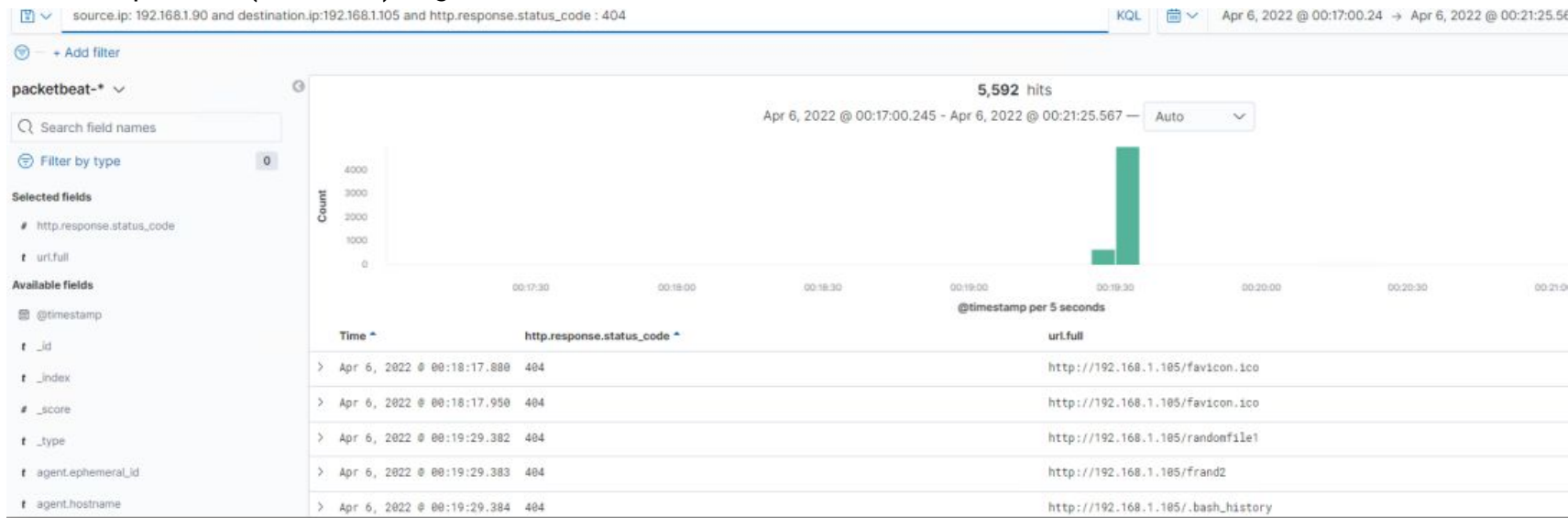
Analysis: Identifying the Port Scan

- The scan took place on April 5th, 2022 at 7:07 CST.
- From 192.168.1.90, around 3000 packets were transmitted.
- Variable ports, 1000 per ip address, and a single source ip, incremental ports with host The name kali is a red flag for a malicious nmap scanner.



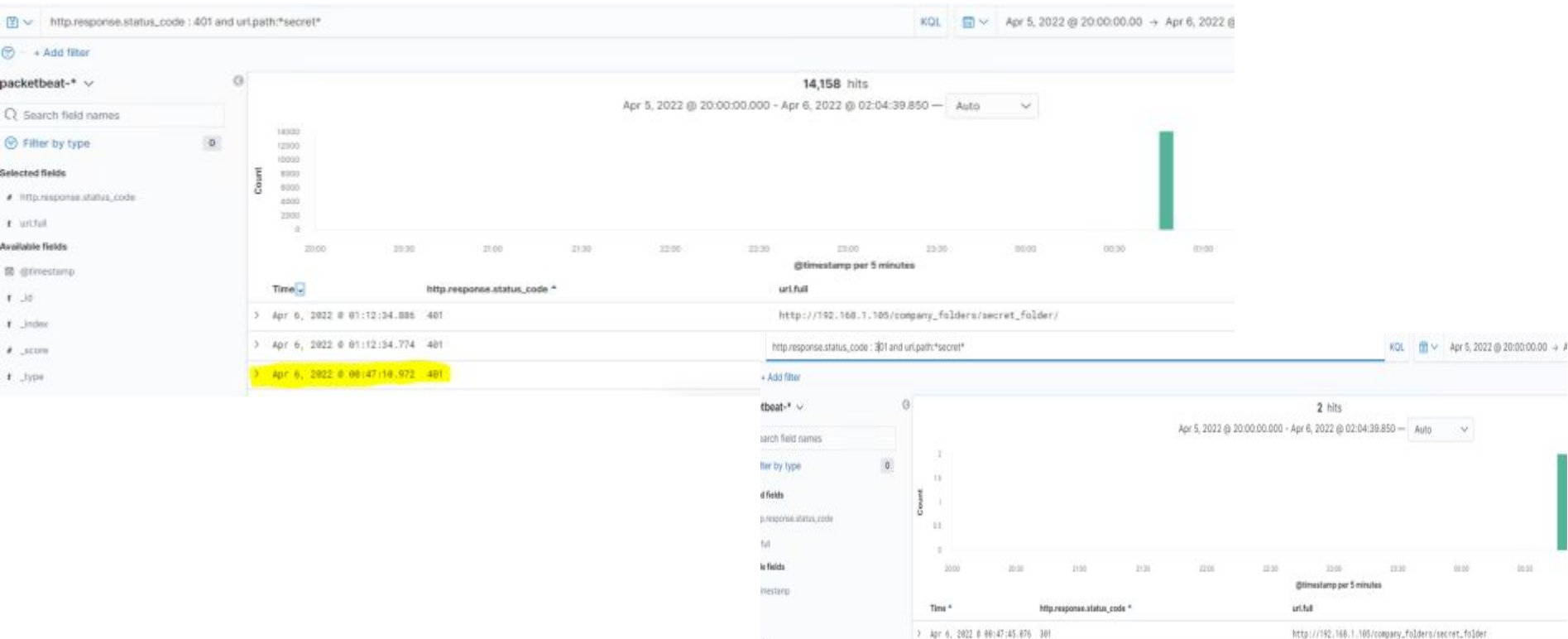
Analysis: Finding the Request for the Hidden Directory

- The Dirb requests for the concealed directories began at 00:17 UTC on April 6th, 2022, or 7:17 UTC on April 5th, 2022. There were 5,592 hits that returned a 404 (not found) error, with a total of 5,653 hits.
- The attack made GET requests to the Dirb word lists attached to the url `http://192.168.1.105/*` and got two responses: webdav with a 401 (unauthorized) error and server-status with a 403 (not authorized) problem (forbidden) Regardless of access, these errors are existential confirmation.



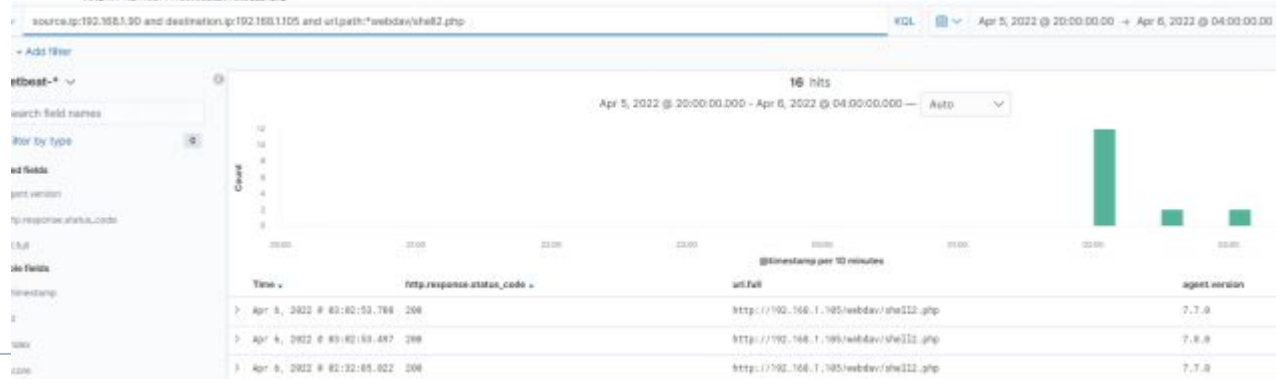
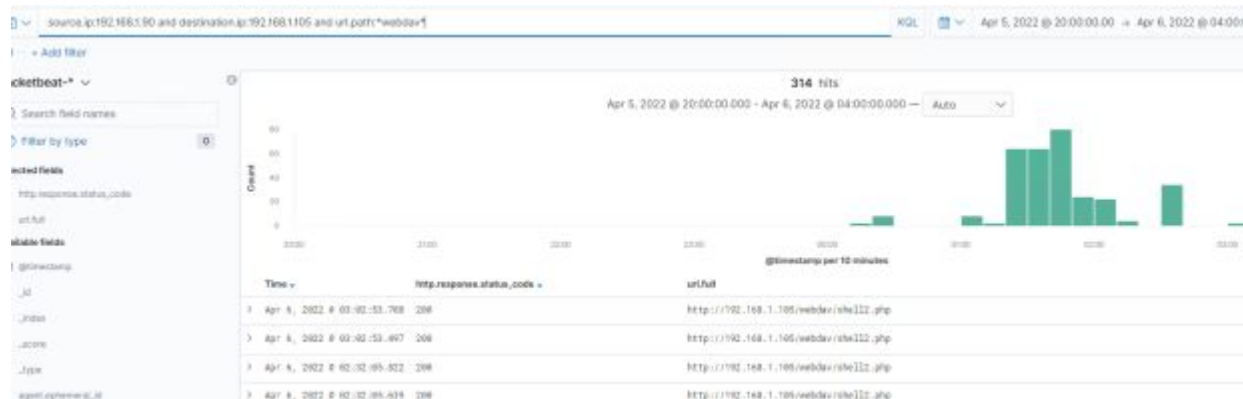
Analysis: Uncovering the Brute Force Attack

- The successful password was determined as leopoldo at 00:47:45.076 on April 6th, 2022 or 7:47:45 CST on April 5th, 2022 after 14,158 hits were made using Hydra in the attack.



Analysis: Finding the WebDAV Connection

- The webdav directory received 314 hits, with 16 of them accessing the shell2.php file.
- There appear to have been a few failed efforts to acquire remote access using various php scripts and files (phpmeterpreter-staged-reverse-tcp-443-php.rc, passwd.dav, and shell.php), but shell2.php was successful.





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 alert that detects port scans and sends an email to the SOC team to inform them to investigate once the threshold has been achieved.

What threshold would you set to activate this alarm?

Port scans from the same IP address in a row

System Hardening

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

Fortinet claims that "Unauthorized access to a company's private network can be prevented by using a firewall. It manages the visibility of ports and identifies when a port scan is in progress before shutting it down."

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

Install and maintain a firewall to block access to ports and deny traffic from IP addresses that are in violation.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- In the event of access, unknown ips that haven't been allowlisted should raise an alarm.
- Excessive request amounts should also be blocked if the IP address is attempting to connect.

What threshold would you set to activate this alarm?

- The alarm should go off in the event of any access from an unknown address and/or sends more than 5 requests/min

System Hardening

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

- This directory should not exist on the server in the first place, according to best standards.

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

- Command: `rmdir -r /company_folders/secret_folder`
- Place the folder on a secure internal network computer or in a cloud vault, but not on a C2 susceptible workstation.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- The alarm should be triggered if a single IP source sends more than 5 unauthorized messages in one minute. If the number of people is greater than 500, the alarm should be raised in intensity to get the attention of the SOC members.

What threshold would you set to activate this alarm?

- >5 for an email, >500 for text and email, >1000 for upper management notification

System Hardening

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

- For an hour, block incoming traffic from IP addresses that send more than 5 requests with unlawful status codes, then block permanently until an administrator reviews the IP addresses that have been in violation many times.

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

- Login attempts and lockout policies can be limited by user settings, while firewall settings can protect against unknown IP sources and bandwidth

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Allow only pre-approved IP addresses to connect, and notify you if any other source tries to join. Block traffic from outside the network as well.

What threshold would you set to activate this alarm?

- When any attempt is made, this alert should be delivered to layer 1 SOC members, and it should escalate to higher tiers if many attempts are made at the same time.

System Hardening

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

- Except for allow-listed ips, the host can be set to prohibit all access.
- Furthermore, ports such as 80 and 443 can be blocked for external ips attempting http connections, as they are primarily utilized by web dav.

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

- Implement allow-list/deny-list methods, and block all network-external communication on ports 80 and 443.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Monitor ports and set an alert for any communication coming from port 680 or any port with a successful authentication after that.
- When a new.php file is submitted from an unfamiliar IP address, you will receive an alert.

What threshold would you set to activate this alarm?

- Instant alert for traffic to port 680 (used in the assault) and/or any future ports that appear in use as a result of the.php reverse shell attack.

System Hardening

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

- Internal uploads are required, and external access privilege escalation is prohibited.
- External access to new.php files in protected directories is blocked, and public access requires administrator clearance.

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

- Remove access to previously used ports, such as 80 and 443, from known attackers.

*The
End*