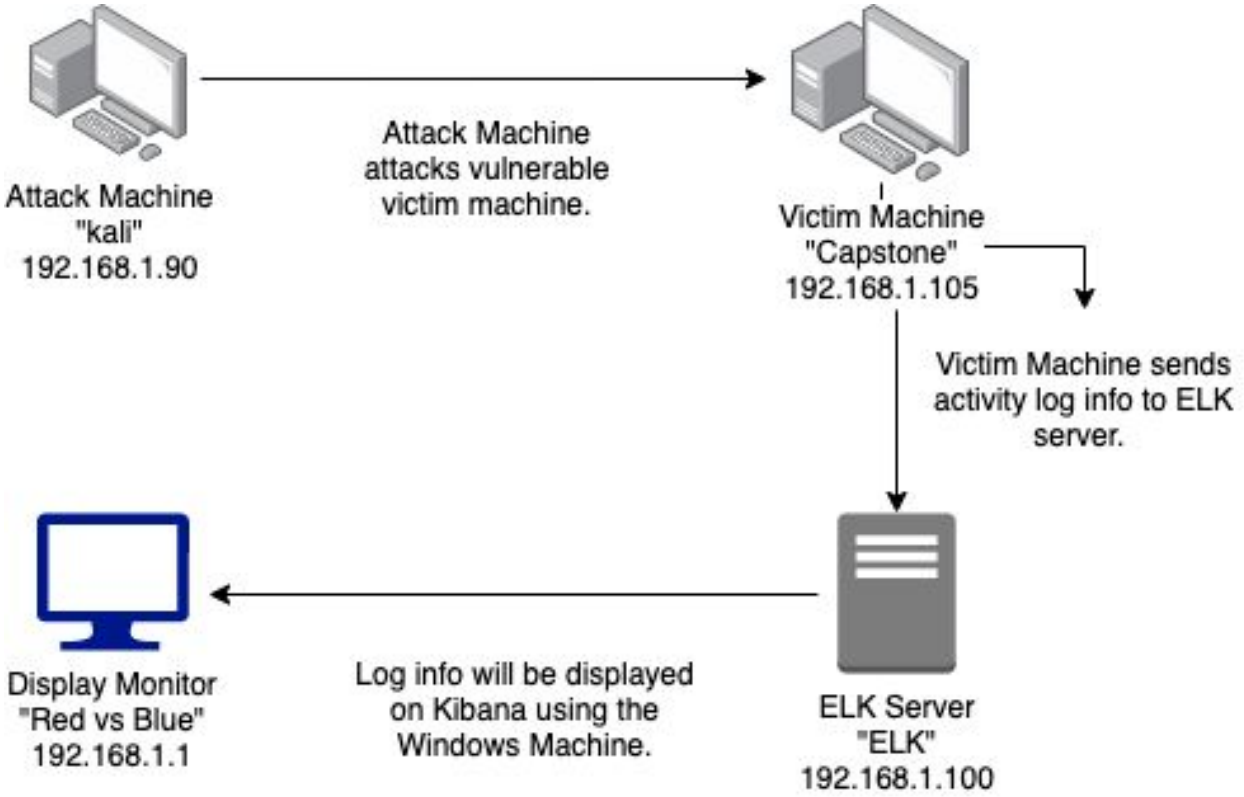
Table of Contents

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: 192.168.1.90
OS: Linux 2.6.32
Hostname: kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.0.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.1
OS: Windows
Hostname: Red vs Blue - ML-REFVM

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Red vs Blue ML-REFVM	192.168.1.1	Virtual Host Machine, we will view log data from here
Kali	192.168.1.90	Attack machine
ELK	192.168.1.100	Logs activity data from Capstone machine
Capstone	192.168.1.105	Vulnerable machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80	Open ports can allow attackers to access private information and increase the risk of a data breach.	This allowed the red team to find private directory with accessible files.
Accessible Files	Web servers, FTP servers, and similar servers may store a set of files underneath a "root" directory that is accessible to the server's users.	This allowed the red team to view the files after accessing the IP on port 80 on Firefox. From there, the red team obtained the server's users and secret file information.
Brute Force Password	When the password is easy to guess, it can be found in a brute force tool wordlist to be hacked.	This allowed the red team to brute force Ashton's password, which was Leopoldo, and access the secret files in the system.
Hashed Password	A hashed password can be cracked through different tools like John the Ripper, hashcat, and other online tools. It can take only minutes to crack if the password is not salted.	This allowed the red team to use md5cracker to identify the password for John, which was linux4u.

Exploitation: Open Port 80

01

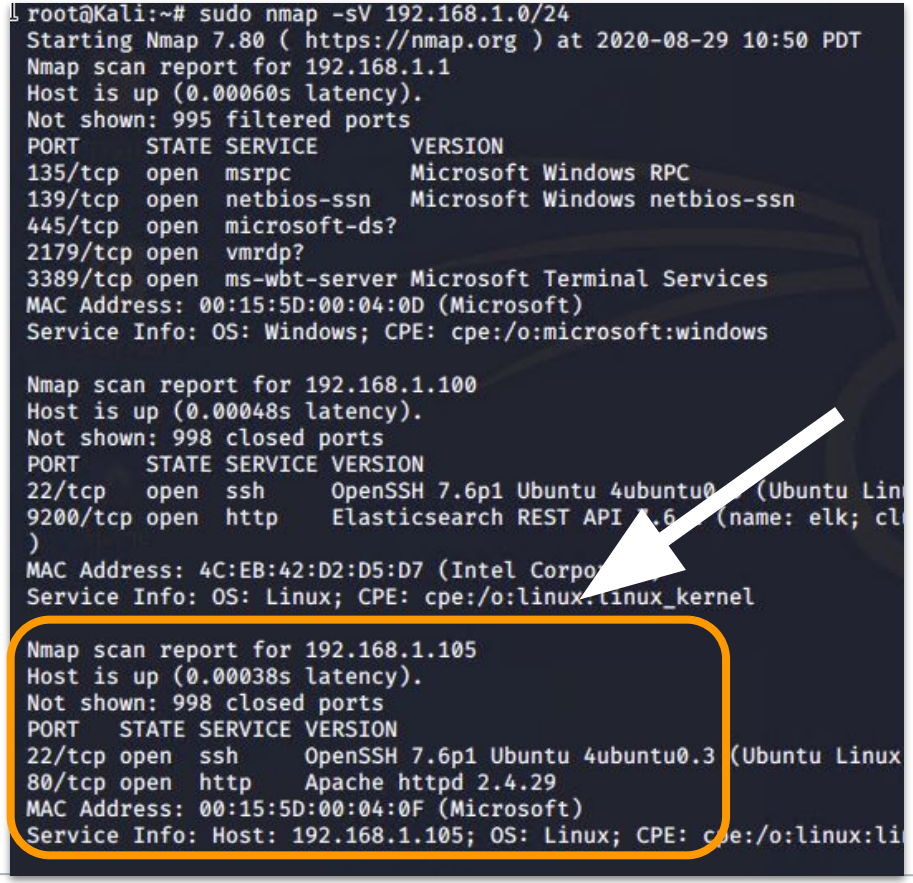
Tools & Processes

We used **nmap** to scan for any open ports and services in our network.

02

Achievements

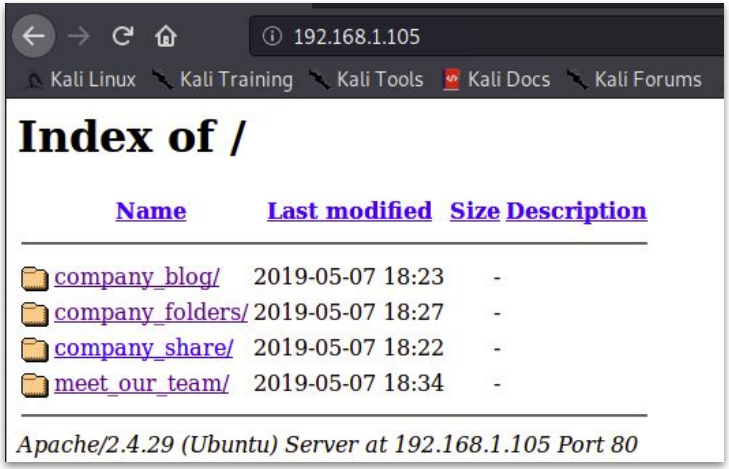
We found that IP address 192.168.1.105 had an open port 80, through which we were able to access a directory with important files.



Exploitation: Accessible Files

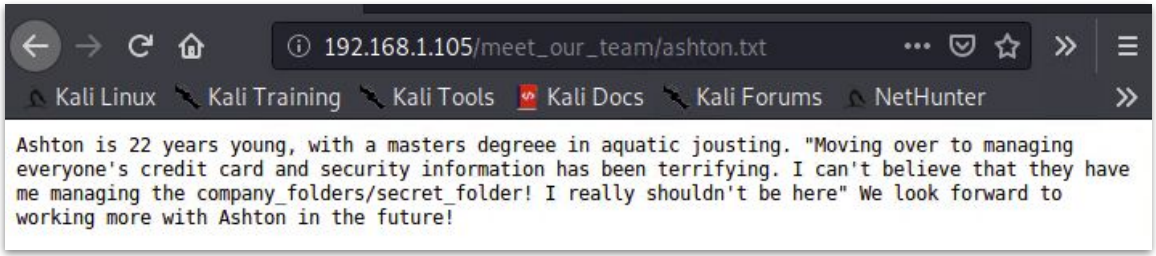
01

Tools & Processes
Using the open port 80, we opened a web browser to see if there was anything important to view.



02

Achievements
Accessing the files gave us intel on which users had access to what and that where their secret files were located.



Exploitation: Brute Force Password

01

Tools & Processes

We used the tool **Hydra** to brute force Ashton's password using the username: ashton.

02

Achievements

The exploit granted us user shell access into the victim machine so we could navigate to the secret files.

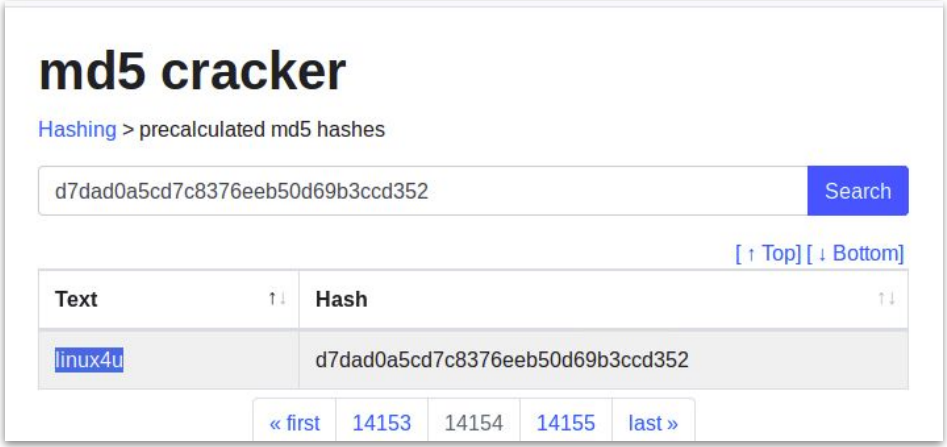
```
0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-08-29 11:04:02
root@Kali:~# ssh ashton@192.168.1.105 -p 80
kex_exchange_identification: Connection closed by remote host
root@Kali:~# ssh ashton@192.168.1.105 -p 22
The authenticity of host '192.168.1.105 (192.168.1.105)' can't be established.
ECDSA key fingerprint is SHA256:YbmWCN0wUP7c+L1Xrox2xN/2Ip5768J/sexE1EF+l04.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.105' (ECDSA) to the list of known hosts.
ashton@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-108-generic x86_64)
```

```
ashton@server1:~$ locate secret_folder
/var/www/html/company_folders/secret_folder
/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
ashton@server1:~$ cd /var/www/html/company_folders/secret_folder/
ashton@server1:/var/www/html/company_folders/secret_folder$ ls
connect_to_corp_server
ashton@server1:/var/www/html/company_folders/secret_folder$ cat connect_to_
corp_server
Personal Note

In order to connect to our companies webdav server I need to use ryan's acc
ount (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: Hashed Password

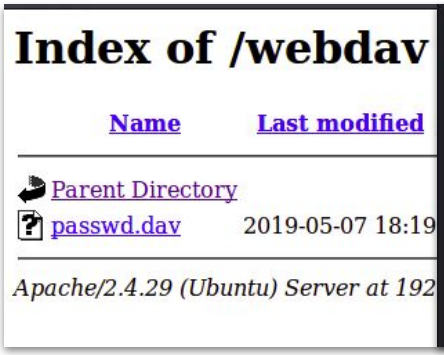
01

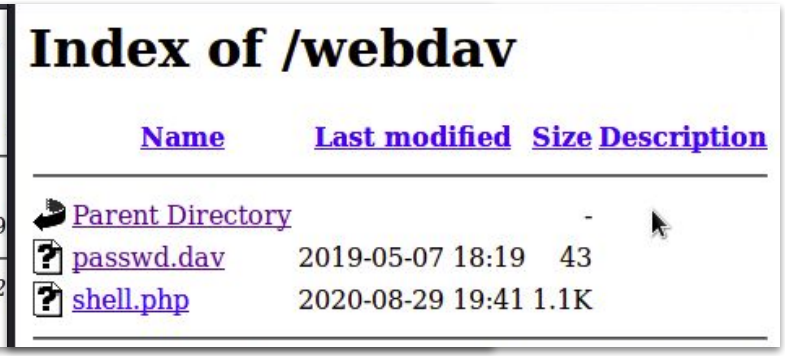
Tools & Processes
We used the website **md5cracker** to find the plaintext of the hashed password for john.



02

Achievements
This password granted us access to the system through the WebDav connection, which later allowed us to upload a shell script to attack.





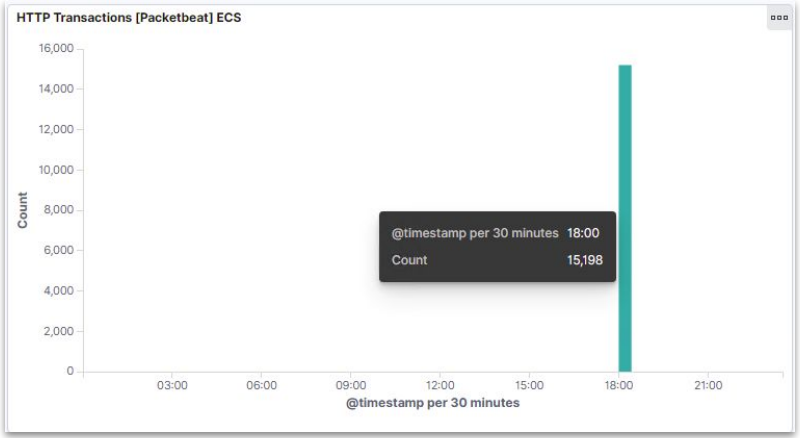
Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- **The port scan began at around 5:30pm**
- **2,486 hits were sent from 192.168.1.90**
- **The nmap ping scan sends requests to the 443 port, so filtering that, we saw the results below.**

Analysis: Finding the Request for the Hidden Directory

- **15,168 requests for the hidden directory occurred at 6pm.**
- **The file requested was a secret folder hidden within the company folders.**
- **The secret folder contained instructions on how to access the webdav server using Ryan's account. It also included a hashed password.**

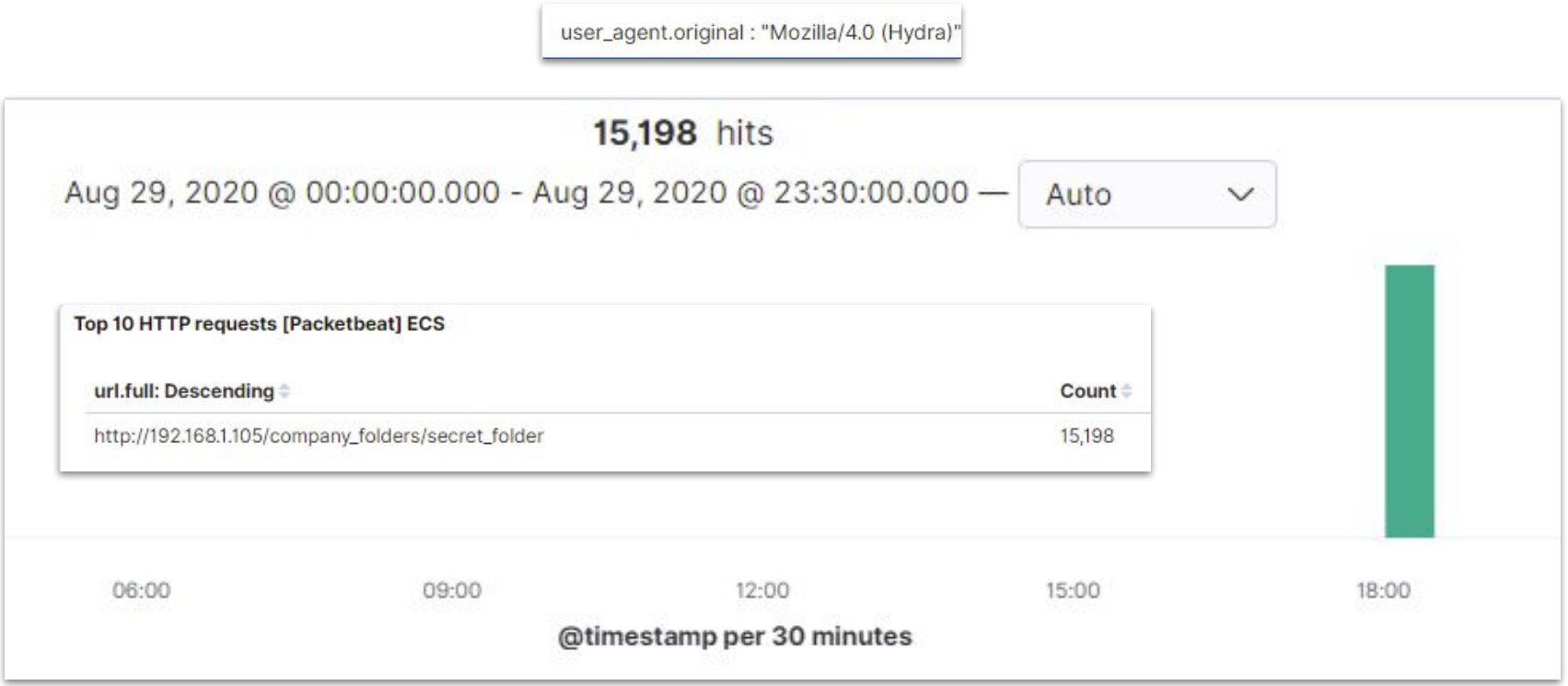



```
ashton@server1:/var/www/html/company_folders/secret_folder$ cat connect_to_
corp_server
Personal Note

In order to connect to our companies webdav server I need to use ryan's acc
ount (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
```

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,198

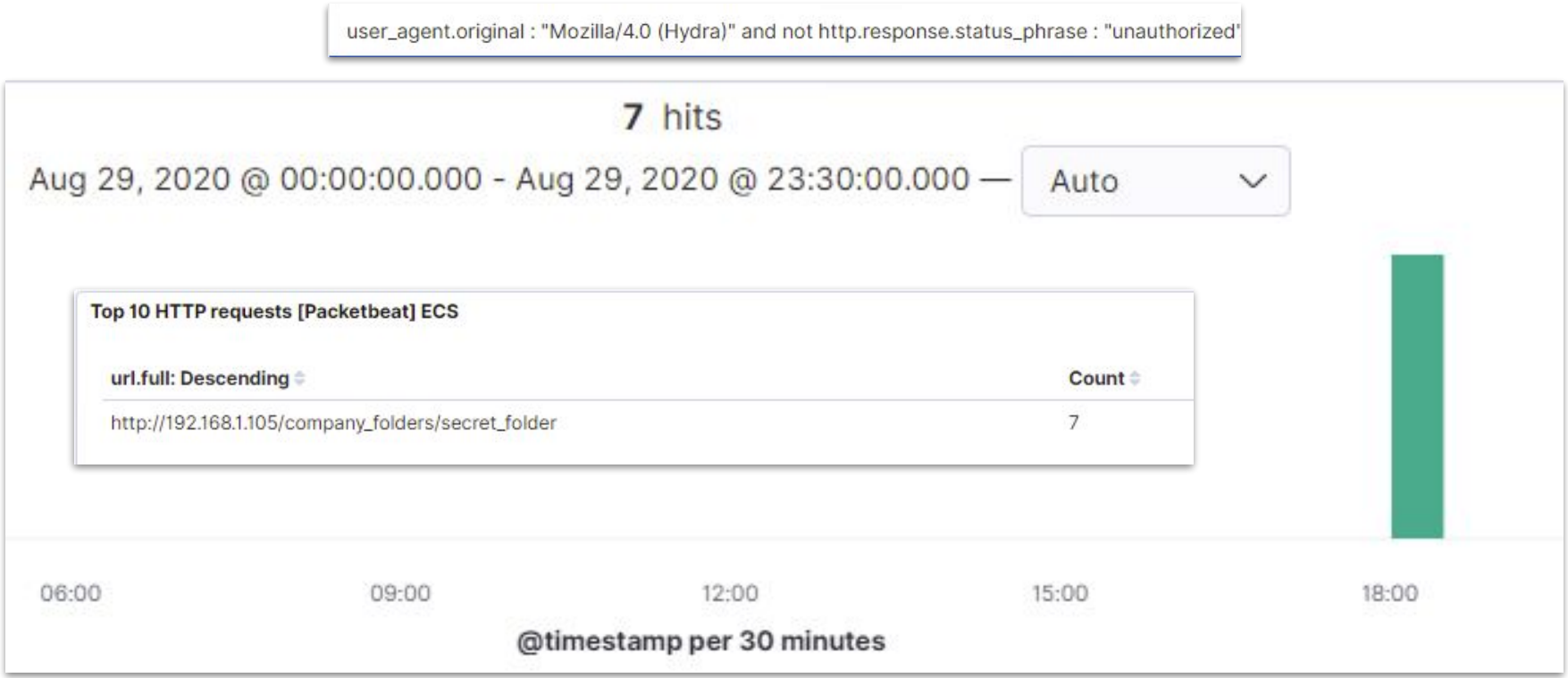
Analysis: Uncovering the Brute Force Attack

- **15,198 requests were made in the brute force attack.**



Analysis: Uncovering the Brute Force Attack

- **15,198 requests were made in the brute force attack.**
- **Out of 15,198 requests, only 7 were successful in the attacker discovering the password.**



Analysis: Finding the WebDAV Connection

- **38 requests were made to the WebDav directory.**
- **The shell.php file was requested. This was part of the red team's shell attack to start listening for activity on the victim machine.**

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,198
http://192.168.1.105/webdav	38
http://192.168.1.105/	16
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/favicon.ico	8

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

We will set up an alarm for when a firewall detects more than 10 port scans in a minute or 100 consecutive (ICMP) requests.

Most firewalls and IPSs can detect such scanning and cut it off in real time.

System Hardening

Enable only the traffic you need to access internal hosts and deny everything else.

This goes for standard ports, such as TCP 80 for HTTP and ICMP for ping requests.

Mitigation: Finding the Request for the Hidden Directory

Alarm

We will set an alert that goes off for any machine that attempts to access this directory or file.

The threshold will be more than 1 attempt.

System Hardening

Remove the directory and file from the server.

Terminal:
`rm -r ../company_files` → to remove directory

If needed, move the directory to a safer or offline location.

Mitigation: Preventing Brute Force Attacks

Alarm

We will set an alert if ‘401 Unauthorized’ is returned from any server to hat would weed out forgotten passwords. Start with 10 attempts in one hour and refine from there.

We will also create an alert if the `user_agent.original` value includes `Hydra` in the name.

System Hardening

After the limit of 10 ‘401 Unauthorized’ codes have been returned from a server, that server can automatically drop traffic from the offending IP address for a period of 1 hour.

We could also display a lockout message and lock the page from login for a temporary period of time from that user.

Mitigation: Detecting the WebDAV Connection

Alarm

We can create an alert anytime this directory is accessed by a machine _other_ than the machine that should have access.

The threshold will start off as more than 1 attempt.

System Hardening

Connections to this shared folder should not be accessible from the web interface.

Connections to this shared folder could be restricted by machine with a firewall rule.

Mitigation: Identifying Reverse Shell Uploads

Alarm

We can set an alert for any traffic moving over port `4444.`

We can set an alert for any `.php` file that is uploaded to a server.

The threshold will be more than 1 attempt.

System Hardening

Remove the ability to upload files to this directory over the web interface would take care of this issue.

Takeaways

Takeaways

As a company, it is important to think, not if a security breach will occur, but **when**.

RED TEAM:

- Opened Port 80
- Accessed Sensitive Files
- Brute-Forced to Gain Access
- Un-hashed Password to Gain Access and Inject a Shell Script

BLUE TEAM:

- Identified Port Scan
- Found Request for Hidden Directory
- Uncovered the Brute Force Attack
- Found the WebDav Connection

Continuous monitoring and communication between the security team and the employees will ensure swift response and prevention to attacks.