Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

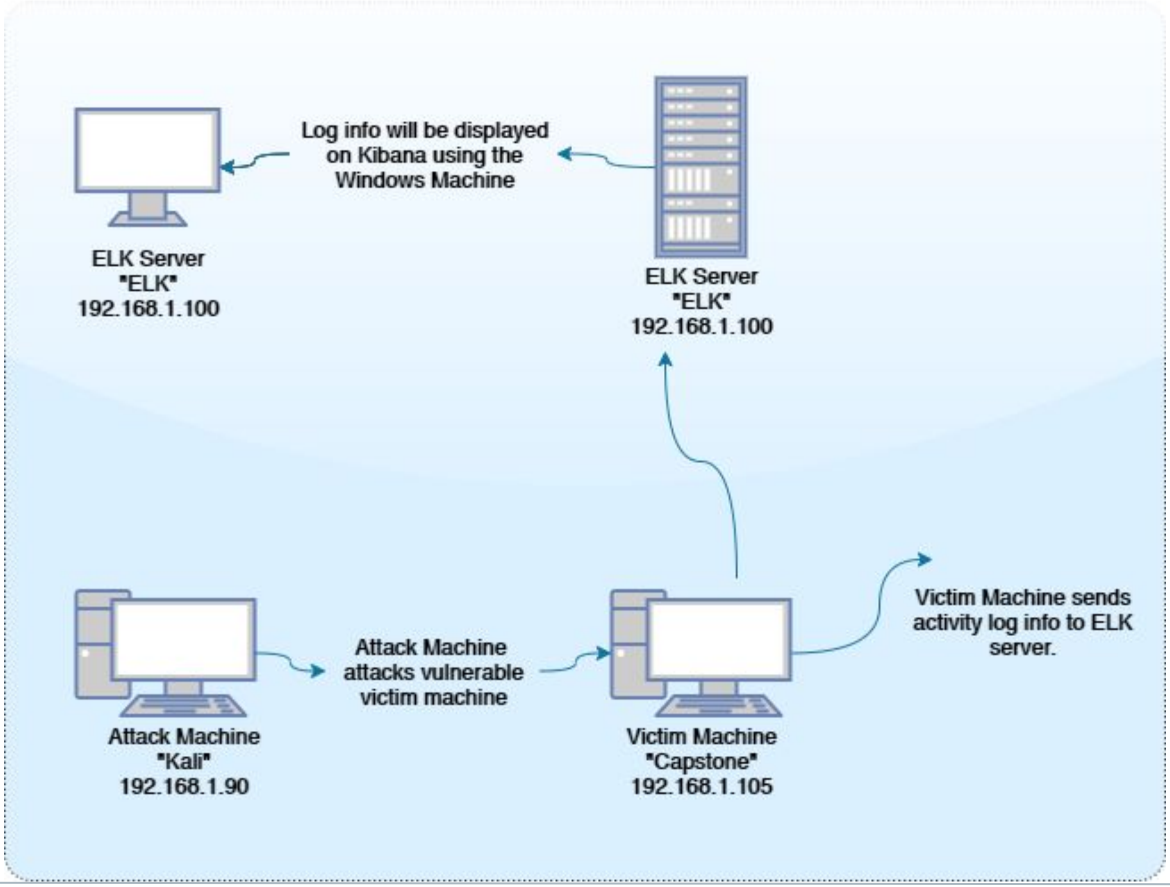
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Log info will be displayed on Kibana using the Windows Machine
ELK Server "ELK" 192.168.1.100
ELK Server "ELK" 192.168.1.100
Attack Machine "Kali" 192.168.1.90
Attack Machine attacks vulnerable victim machine
Victim Machine "Capstone" 192.168.1.105
Victim Machine sends activity log info to ELK server.

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: **Red vs Blue - ML-REFVM**

IPv4: **192.168.1.90**
OS: **Linux 2.6.32**
Hostname: **Kali**

IPv4: **192.168.1.100**
OS: **Linux**
Hostname: **ELK**

IPv4: **192.168.1.105**
OS: **Linux**
Hostname: **Capstone**

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	Base Machine hosting the 3 VMs below
Kali	192.168.1.90	Attack Machine used for penetration testing
ELK	192.168.1.100	Logs data from Capstone Machine. Hosting a Kibana server and capturing activity on 192.168.1.105
Capstone	192.168.1.105	Vulnerable machine, Box we are attempting to pop hosting an apache and ssh server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80/TCP	The more applications and services run using open port for internet communication, the higher the risk of one of them having a vulnerability that can be exploited	Open port 80 allow attackers to gain access to a network and to sensitive information as it’s often used for transmitting sensitive data.
Weak Authentication Management	Attackers can detect weak authentication using manual means and exploit them using automated tools with password lists and dictionary attacks	Attackers have to gain access to only a few accounts to compromise the system. This may allow money laundering, identity theft, or disclose legally protected highly sensitive information.
Remote Command Execution	When attempting to compromise a server, an attacker may try to exploit a command injection vulnerability on the server system. The injection code will often be a reverse shell script to provide a convenient command a shell for further malicious activities.	Once sufficiently compromised the attacker may be able to access any and all information on a server such as databases containing confidential information.

Exploitation: Open Port 80

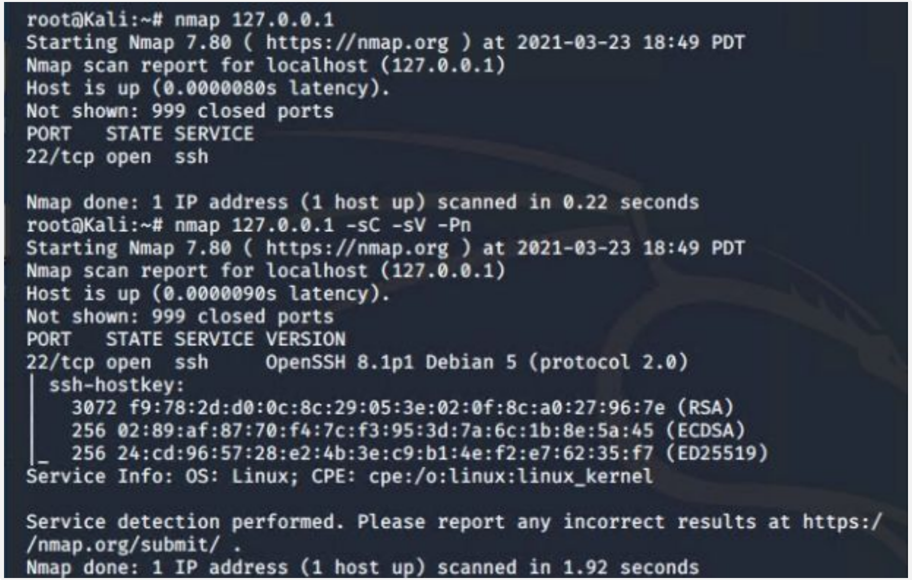
01

Tools & Processes
An Nmap scan showed that port 80 is open. By opening a web browser and typing the IP address of the machine into the address bar got access to the server with company’s directories.

02

Achievements
Identified the IP address and exposed services of the target VM. Got access to sensitive information on 192.168.1.105 has open ports 22 , 80. Discovered a path to secret folder

03



```
root@Kali:~# nmap 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-23 18:49 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
root@Kali:~# nmap 127.0.0.1 -sC -sV -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-23 18:49 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000090s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 f9:78:2d:d0:0c:8c:29:05:3e:02:0f:8c:a0:27:96:7e (RSA)
|   256 02:89:af:87:70:f4:7c:f3:95:3d:7a:6c:1b:8e:5a:45 (ECDSA)
|_  256 24:cd:96:57:28:e2:4b:3e:c9:b1:4e:f2:e7:62:35:f7 (ED25519)
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: 1 IP address (1 host up) scanned in 1.92 seconds
```

Exploitation: Brute Force Password

01

Tools & Processes

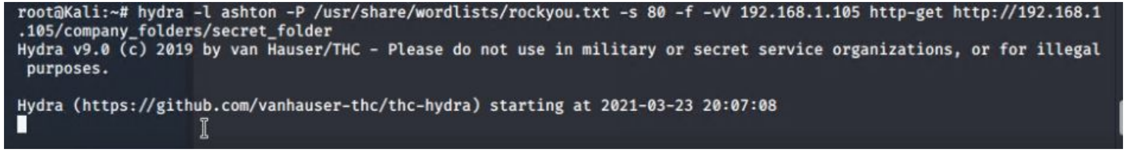
Used Brute Force attack on the password for the hidden directory using Hydra. Used Ashton's name, ran the Hydra attack against the directory.

02

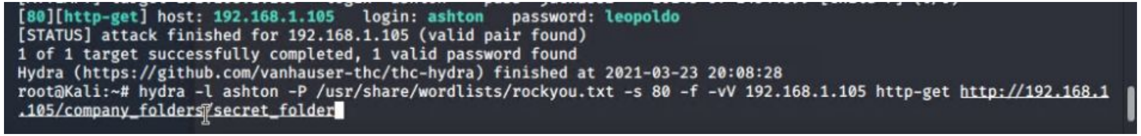
Achievements

Found the username "ashton" and the password "leopold". Used credentials to log into the hidden folder. Located inside of the WebDAV file instructions on how to connect to the WebDAV directory, as well the user's username and hashed password.

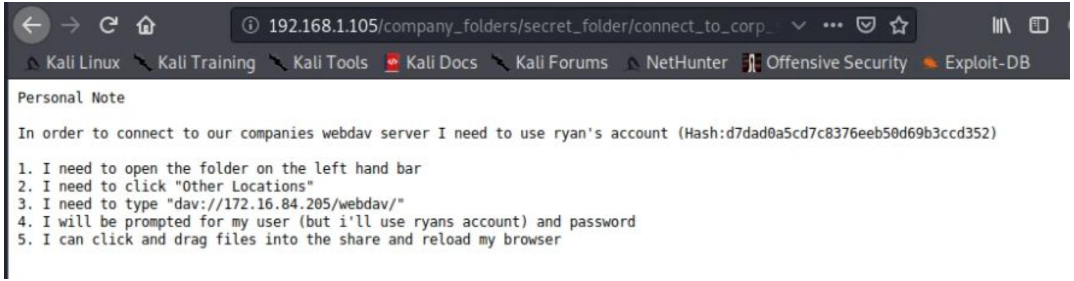
03



```
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get http://192.168.1
.105/company_folders/secret_folder
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal
 purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-23 20:07:08
```



```
[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 2021-03-23 20:08:28
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get http://192.168.1
.105/company_folders/secret_folder
```



```
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
```

Exploitation: Weak Authentication Management

01

Tools & Processes

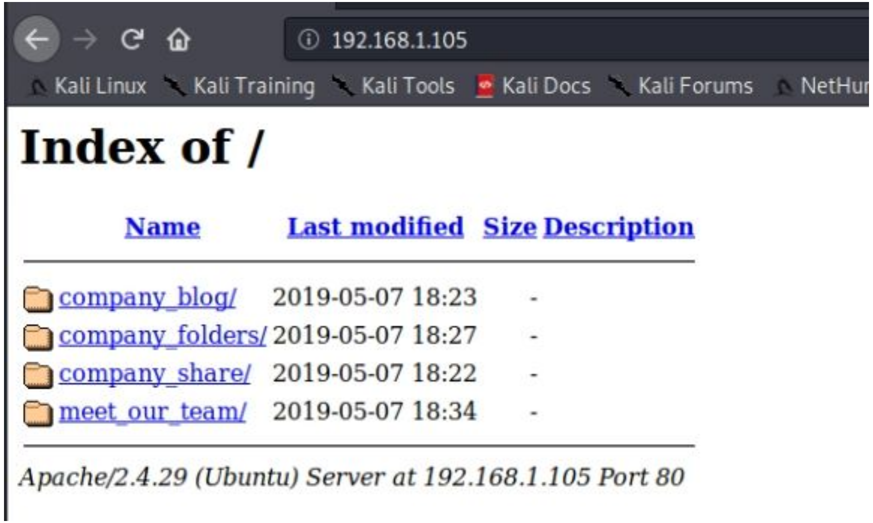
Using the open port 80, I opened a web browser to see if there is anything important to see

02

Achievements

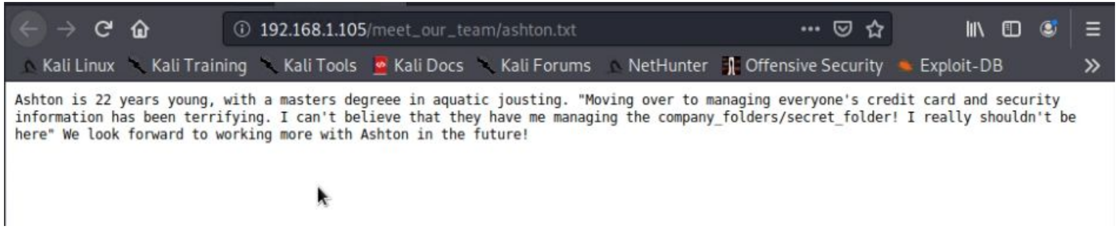
Accessing the files gave us intel on which users had access to what and that where their secret files were located

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
```



```
Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and security
information 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!
```

Exploitation: Hashed Password

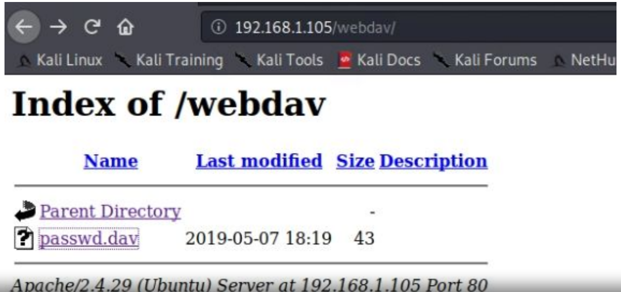
01

Tools & Processes
I used the website calls md5cracker to translate the hashed password for ryan’s account

02

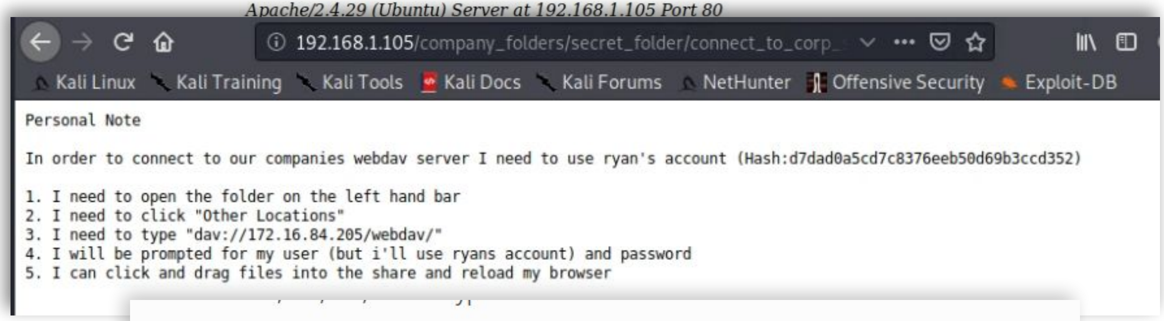
Achievements
This password granted us to access to 192.168.1.105/WebDav page, which later we will us to upload a shell scripts to attack

03

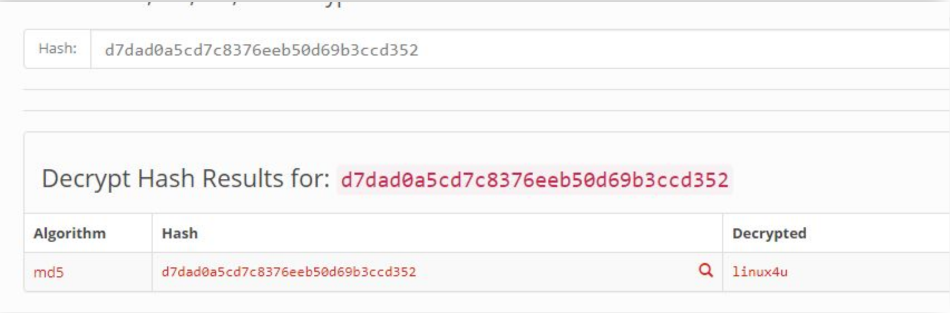


Index of /webdav

```
Name                Last modified     Size Description
Parent Directory                        -
passwd.dav          2019-05-07 18:19   43
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
```



Hash: d7dad0a5cd7c8376eeb50d69b3ccd352

Decrypt Hash Results for: d7dad0a5cd7c8376eeb50d69b3ccd352

Algorithm	Hash	Decrypted
md5	d7dad0a5cd7c8376eeb50d69b3ccd352	linux4u

Blue Team

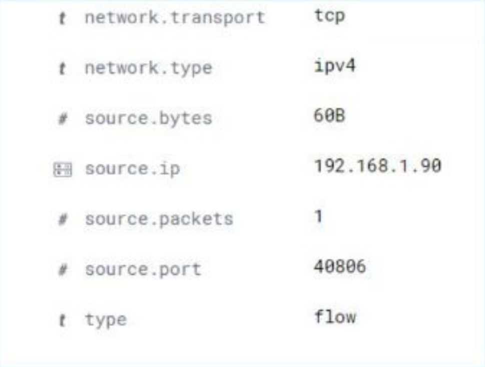
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan occurred on March 24, 2021
- 19,373 packet were sent from 192.168.1.90
- Multiple clues indicated this was a port scan. Details below

After manual digging through the packetbeat logs, a pattern started to develop. I noticed several things:

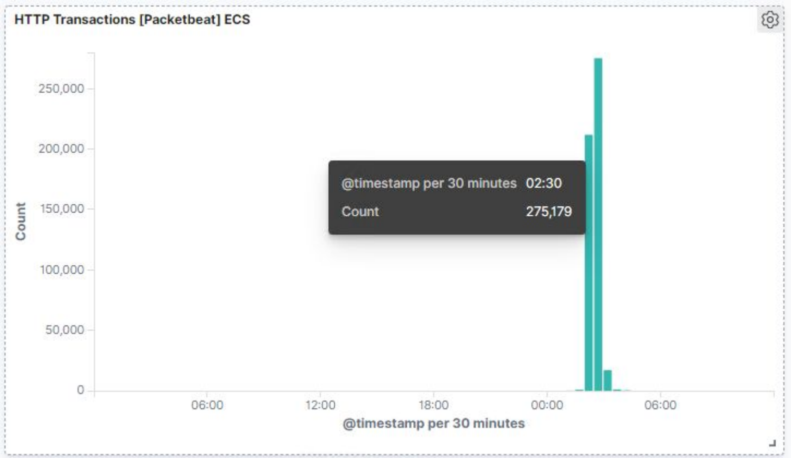
1) A large number of packets on the same timestamp from the same machine (192.168.1.90)
2) All the source traffic was coming from the same port: 40806
3) The size of each record was a single packet.
4) The destination port was different each time.
5) I was able to filter for each host on the network and see the same pattern for each destination IP.
6) source.ip : 192.168.1.90 and source.packets: 1 and source.port: 40806 and destination.ip: 192.168.1.105
7) All of this added up to suggest a port scan.

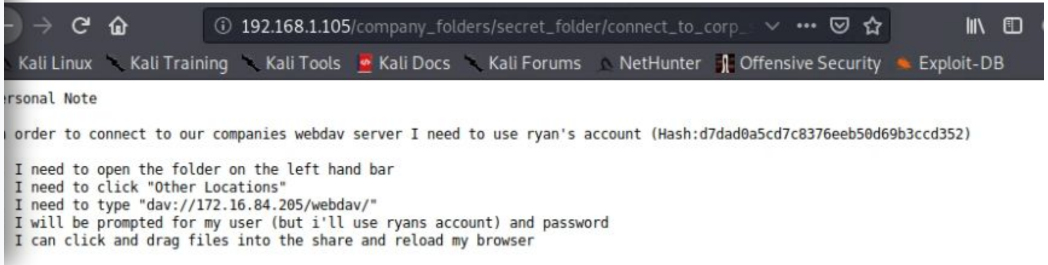


t	network.transport	tcp
t	network.type	ipv4
#	source.bytes	60B
▦	source.ip	192.168.1.90
#	source.packets	1
#	source.port	40806
t	type	flow

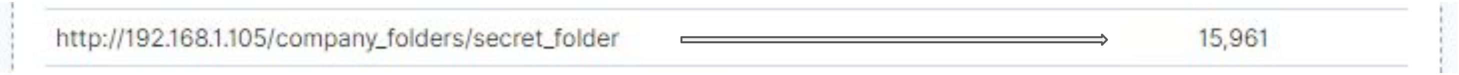
Analysis: Finding the Request for the Hidden Directory

- There are 15,961 request for the hidden directory between 00:00 am and 4:00 am.
- The secret folder contains instructions on how you can access the webdav server using Ryan’s account. It also included a hashed password





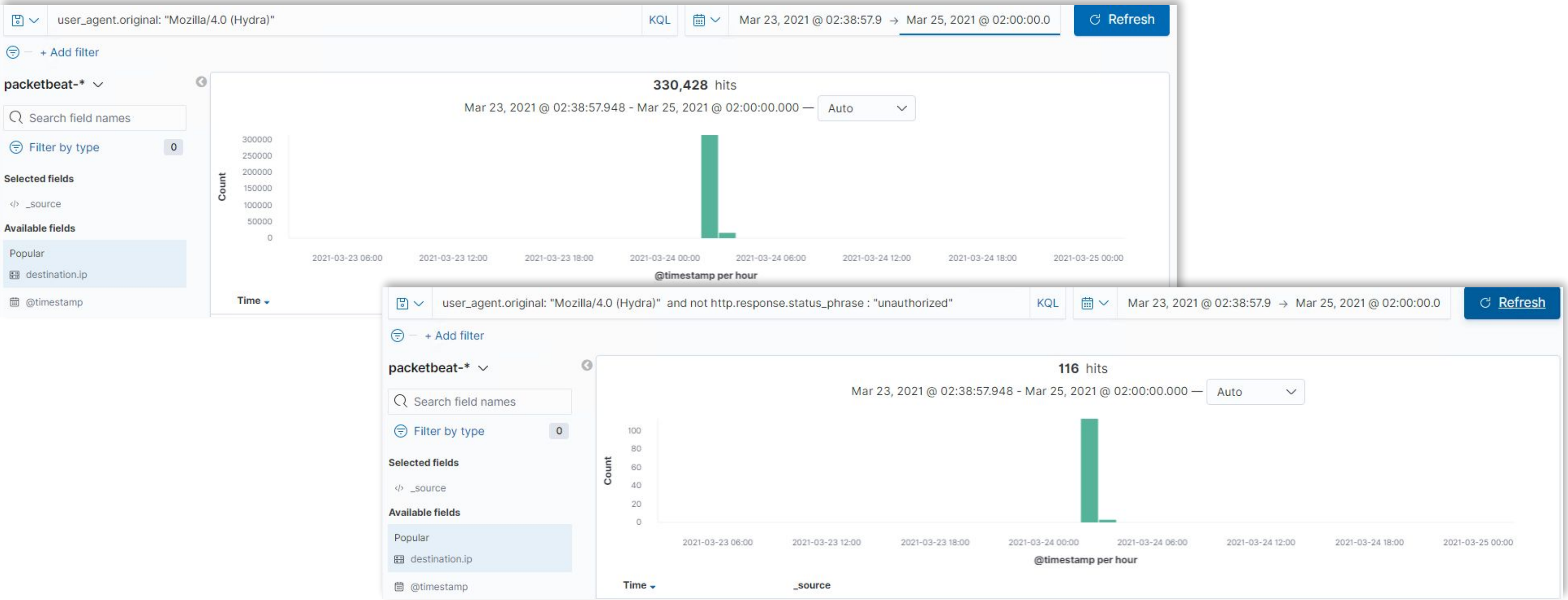
```
rsonal Note

 order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

 I need to open the folder on the left hand bar
 I need to click "Other Locations"
 I need to type "dav://172.16.84.205/webdav/"
 I will be prompted for my user (but i'll use ryans account) and password
 I can click and drag files into the share and reload my browser
```



http://192.168.1.105/company_folders/secret_folder ⟹ 15,961

Analysis: Uncovering the Brute Force Attack

330,428 request were made in the direct Brute Force Attack.



user_agent.original: "Mozilla/4.0 (Hydra)"

Mar 23, 2021 @ 02:38:57.9 → Mar 25, 2021 @ 02:00:00.0

packetbeat-*

330,428 hits

Mar 23, 2021 @ 02:38:57.948 - Mar 25, 2021 @ 02:00:00.000 — Auto

user_agent.original: "Mozilla/4.0 (Hydra)" and not http.response.status_phrase : "unauthorized"

Mar 23, 2021 @ 02:38:57.9 → Mar 25, 2021 @ 02:00:00.0

packetbeat-*

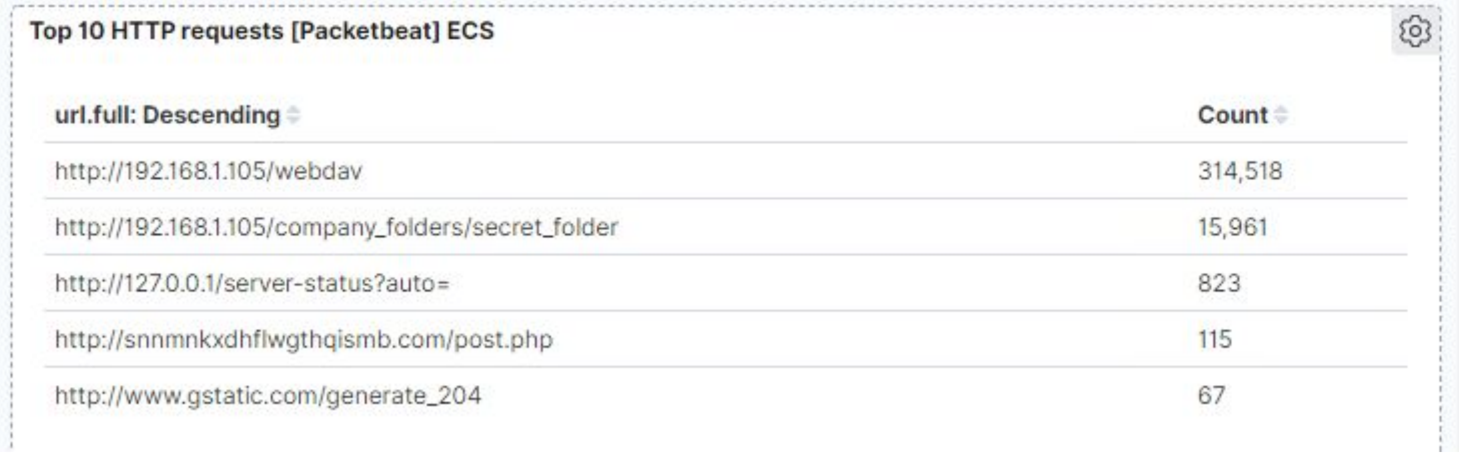
116 hits

Mar 23, 2021 @ 02:38:57.948 - Mar 25, 2021 @ 02:00:00.000 — Auto

There are 116 hits , Out of 330,428 request were successfully in the attacker discovering the password

Analysis: Finding the WebDAV Connection

- In the Top 10 HTTPS request [Packedbeat] ECS - we are able to see requests for webdav folder was connected and files were accessed.
- The files requested were the password.dav and additional file named “shell.php”.
- 15.961 request were made to the WebDav directory



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	314,518
http://192.168.1.105/company_folders/secret_folder	15,961
http://127.0.0.1/server-status?auto=	823
http://snnmnkxdhflwgthqismb.com/post.php	115
http://www.gstatic.com/generate_204	67

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?

- The scan and sweep filters track the number of port scan and host sweep attempt from a single source IP address. Host scan and port sweeps are blocked through the Quarantine feature. Scan and sweep filters only look at connections from traffic that undergoes Ips inspection.
-

What threshold would you set to activate this alarm?

- These filters have threshold values that can be configured per Security Profile and per filter. The filter becomes active when the number of connection attempts from a source IP address exceeds the threshold

System Hardening

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

- In order to block port scans, you need to enable filters 7000 to 7004 and 7016. Please ensure that you read the filter descriptions as some of them have warnings attached.

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

- 7000: TCP - Port Scan
- 7001: UDP - Port Scan
- 7002 TCP - Host Sweep
- 7003: UDP - Host Sweep
- 7004: ICMP - Host Sweep
- 7016: ICMPv6 - Host Weep

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

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

What threshold would you set to activate this alarm?

- The threshold would be just for any machine accessing it.

System Hardening

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

- This directory and file should be removed from the server all together.

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

- rmdir -R / deletes directory
- rm -R / deletes file

Mitigation: Preventing Brute Force Attacks

Alarm

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

- We could set an alert if 401 Unauthorized is returned from any server over a certain threshold that would weed out forgotten passwords.

What threshold would you set to activate this alarm?

- Start with 10 in one hour and refine from there

System Hardening

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

- Limit failed login attempts
- Make the root user inaccessible via SSH by editing the sshd_config file
- Limit logins to a specified IP address or range

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

- For failed login attempts on Windows:
  - Double click Account Policies
  - See Account lockout threshold
  - Double click and change the number of failed login attempts

Mitigation: Detecting the WebDAV Connection

Alarm

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

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

What threshold would you set to activate this alarm?

- Setting a range of acceptable IPs that are allowed access.
- Any IP outside of the acceptable range will trigger an alarm.

System Hardening

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

- 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

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

- Blocking port 80 and 443
  - HTTP and HTTPS

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

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

What threshold would you set to activate this alarm?

- Since we are setting an alert for ANY traffic moving over 4444, the threshold would be for any.

System Hardening

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

- Removing the ability to upload files to this directory over the web interface would take care of this issue
  - The required firewall rules for blocking the UPD port 4444 should be added

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

- For Ubuntu:
  - Sudo ufw deny 4444/udp

The End