Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Reported By

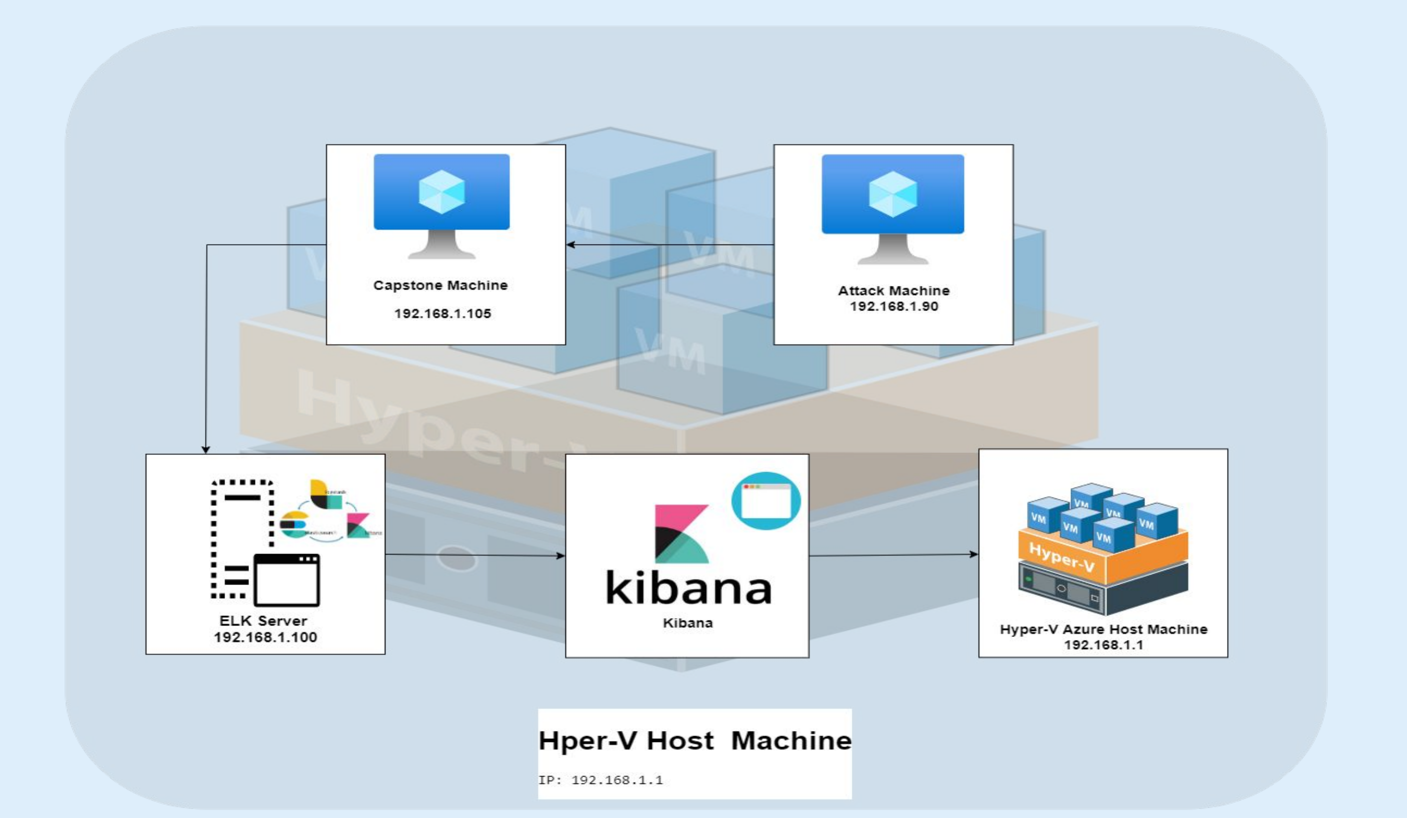
Marcus Cooper

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: 10.0.0.76

Machines
IPv4:1 192.168.1.1
OS: Windows 10
Hostname: Azure
Hyper-V
ML-RefVm-684427

IPv4: 192.168.1.90
OS: Linux 2.6.32
Hostname: Kali

IPv4:192.168.1.100
OS: Linux
Hostname: ELK-Stack

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
Hyper-V Azure Machine ML-RefVm-684427	192.168.1.1	Host Machine Cloud Based
Kali	192.168.1.90	Attacking Machine
ELK Stack	192.168.1.100	Network Monitoring Machine Running Kibana
Capstone	192.168.1.105	Target Machine Replicating A Vulnerable Server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 open with public access *CVE-2019-6579*	An attacker with network access to the web server on port 80/TCP or 443/TCP could execute system commands with administrative privileges.	*Files and Folders are accessible that describes users roles and access.*
CWE-307: Improper Restriction of Excessive Authentication Attempts	Hydra is a fast and flexible login cracker which supports protocols like AFP, HTTP-FORM-GET, HTTP-GET, HTTP-FORM-POST, HTTP-HEAD, HTTP-PROXY, and many more.	By using Hydra to Brute force into Ashton's secret folder I found that he had another users username and password hash stored.
CWE-916: Use of Password Hash With Insufficient Computational Effort	The software generates a hash for a password, but it uses a scheme that does not provide a sufficient level of computational effort that would make password cracking attacks infeasible or expensive.	The amount of time and money it takes to crack passwords that are not salted is low so your data is under constant threat.
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.	With weak password requirements you are opening yourself up to more brute force attacks.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-522: Insufficiently Protected Credentials	The product transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval.	Not only is this a threat when an attacker gets ahold of passwords saved in plain text files but anyone with malicious intent.
HTTP request smuggling vulnerability in Apache HTTP Server 2.4.52 and earlier (CVE-2022-22720)	Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling	If an attacker is able to intercept legitimate end-user queries, they can append the end-user's query to their own malicious query and present it to a front-end proxy using the same connection.
Oracle Solaris 11: CVE-2019-6111: Vulnerability in Openssh, RCP	An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented).	A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory.

Exploitation: NMAP Scan For Open Ports

01

Tools & Processes

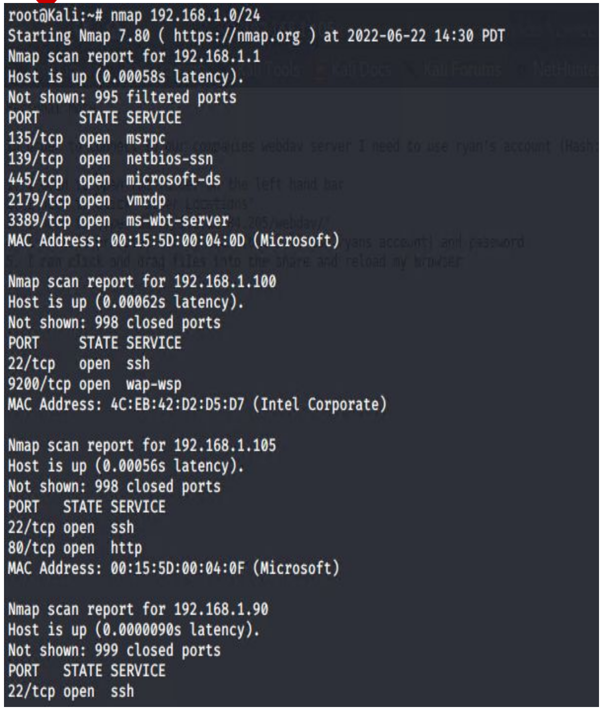
I used NMap to scan for any open ports on the target machine.

02

Achievements

Nmap scanned 256
IP addresses and found that port 22 and 80 are open on the Capstone machine.

03



```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-22 14:30 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00058s 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  vmrdp
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 (0.00062s 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 (0.00056s 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 (0.0000090s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
```

Exploitation: Brute Force Attack

01

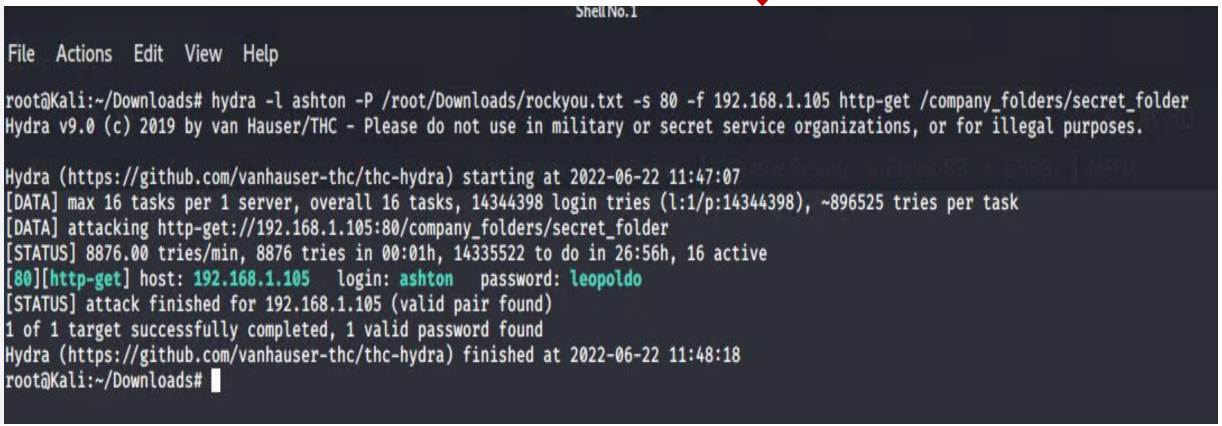
Tools & Processes
I used a preinstalled linux tool called Hydra to gain access to the secret folder on the Capstone machine using port 80 http.

Command:
$ hydra -l ashton -P /root/Downloads/rockyou.txt -s 80 -f 192.16.8.1.105 http-get /company_folders/secret_folder

02

Achievements
Using this exploit I was able to obtain user Ashton password “**leopoldo**”.

03



```
root@Kali:~/Downloads# hydra -l ashton -P /root/Downloads/rockyou.txt -s 80 -f 192.168.1.105 http-get /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 2022-06-22 11:47:07
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-get://192.168.1.105:80/company_folders/secret_folder
[STATUS] 8876.00 tries/min, 8876 tries in 00:01h, 14335522 to do in 26:56h, 16 active
[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 2022-06-22 11:48:18
root@Kali:~/Downloads# 
```

Exploitation: Weak Password Hash and Passwords Saved in Plain Text File

01

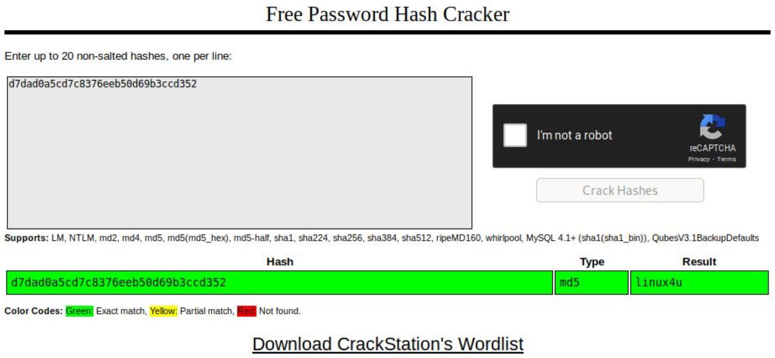
Tools & Processes:

After Brute forcing into the “/secret_folder” I found it contained a file with a password hash for the account of another user “Ryan”. I used a free hash cracker to get the password.

02

I am now able to gain access to another user's account to further infiltrate the system.

03



Free Password Hash Cracker

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

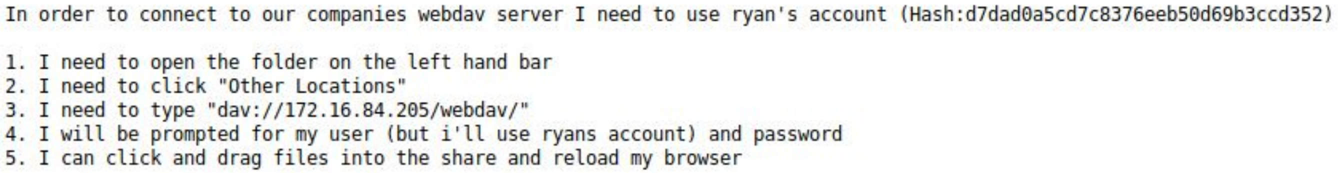
```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, 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.

Download CrackStation's Wordlist



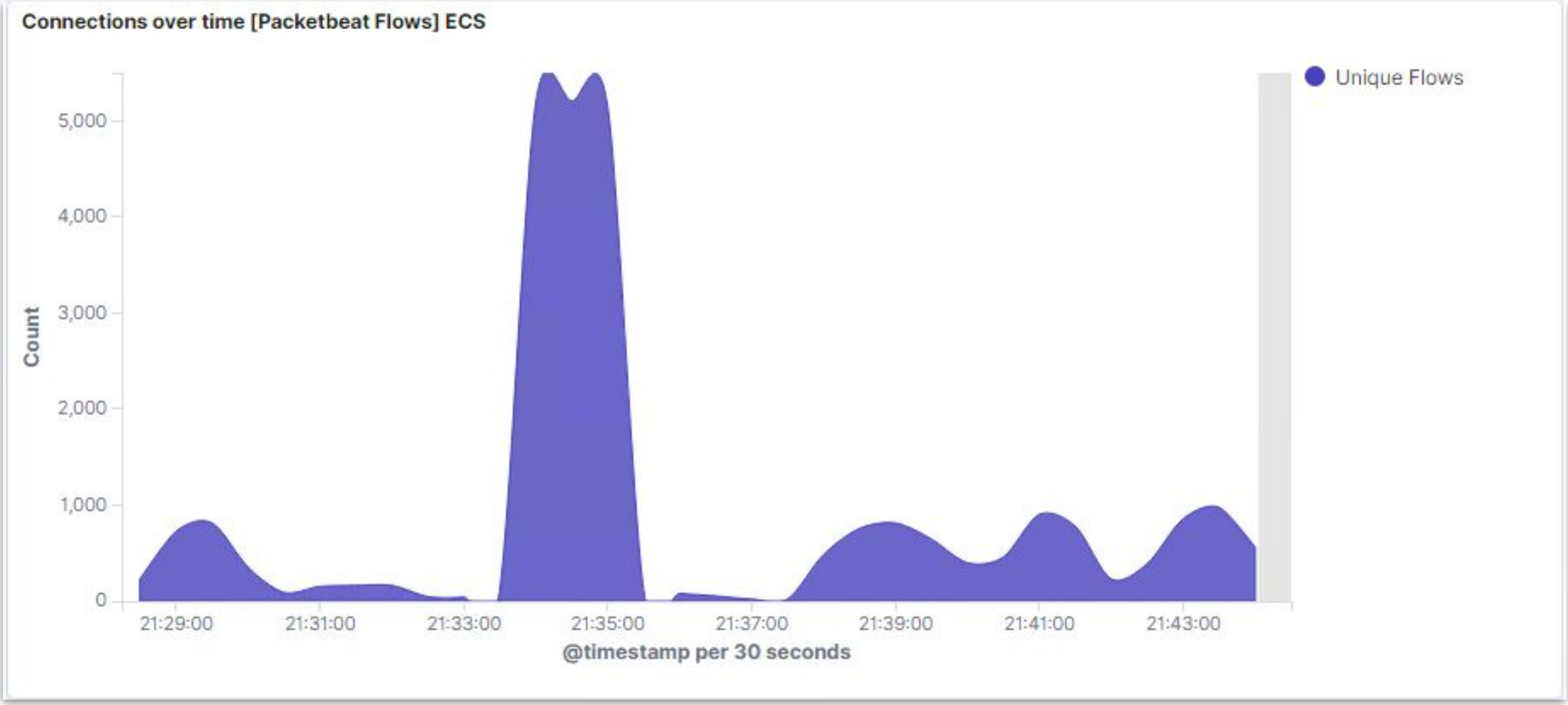
```
In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

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
```

Blue Team

Log Analysis and Attack Characterization

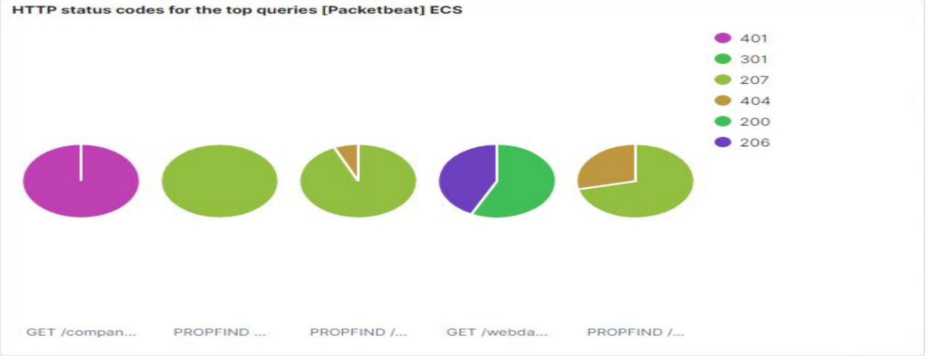
Analysis: Identifying the Port Scan

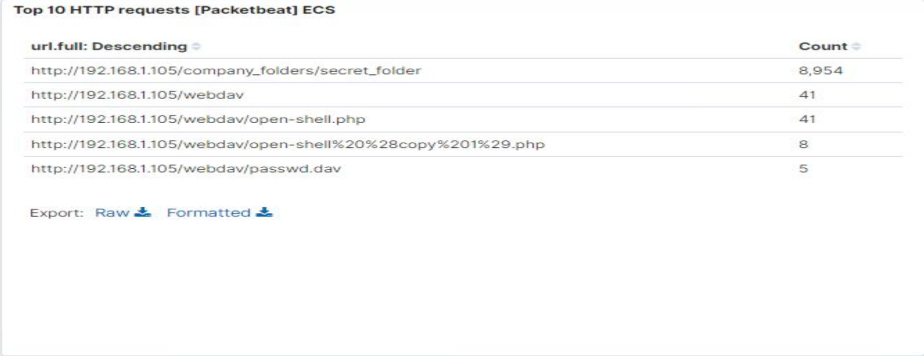
- On 07/05/2022 At approximately 2133 hours (6:33 pm est time) a nmap port scan was detected.
- Around 5000 packages were sent from source IP 192.168.1.90.
- This was identified as a port scan by the amount of packets that were sent.



Analysis: Finding the Request for the Hidden Directory

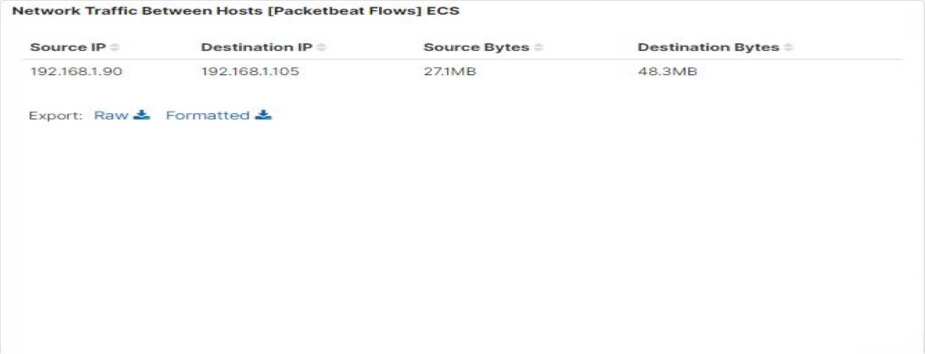
- This incident started around 2130 to 0130 (9:30pm-1:30pm) on 07/05/2022.
- Over 8,000 request were made to access all hidden folders.
- The first folder accessed was /secret_folder. This folder contains login credentials for Ryan's /webdav account.
- Once the credentials were captured this allowed me to move into the /webdav folder and upload a payload to further exploit the system.


HTTP status codes for the top queries [Packetbeat] ECS


Top 10 HTTP requests [Packetbeat] ECS

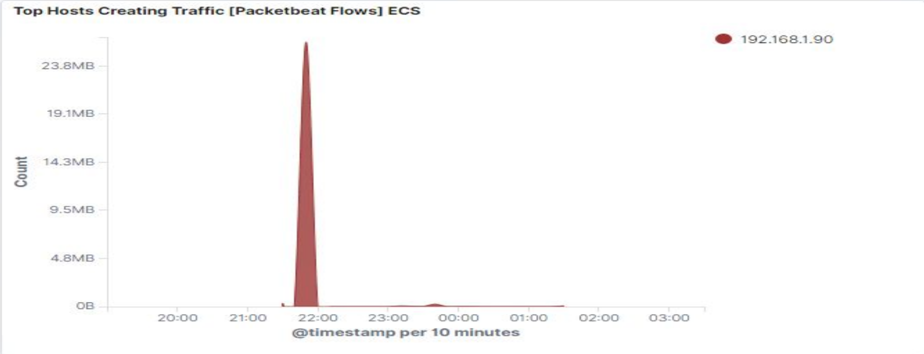
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	8,954
http://192.168.1.105/webdav	41
http://192.168.1.105/webdav/open-shell.php	41
http://192.168.1.105/webdav/open-shell%20%28copy%201%29.php	8
http://192.168.1.105/webdav/passwd.dav	5

Export: Raw Formatted


Network Traffic Between Hosts [Packetbeat Flows] ECS

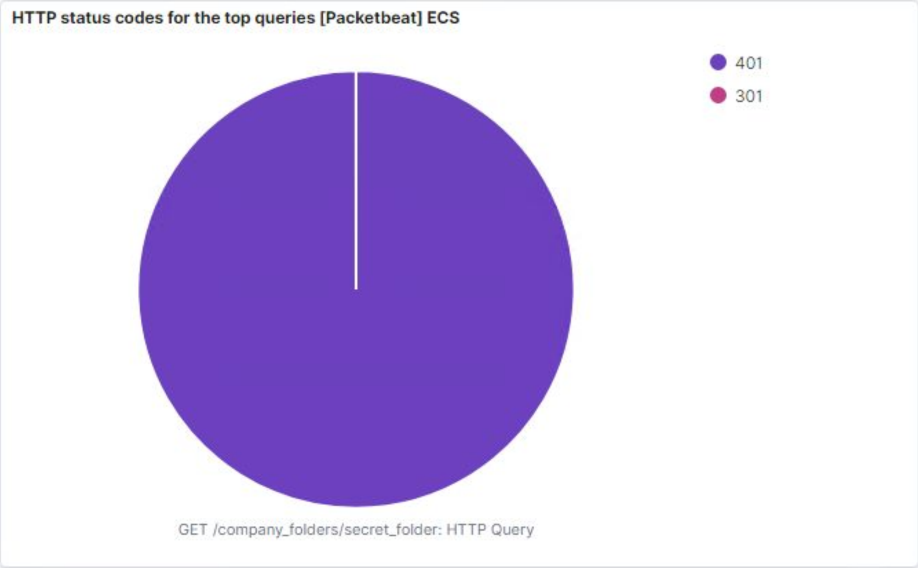
Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.105	27.1MB	48.3MB

Export: Raw Formatted

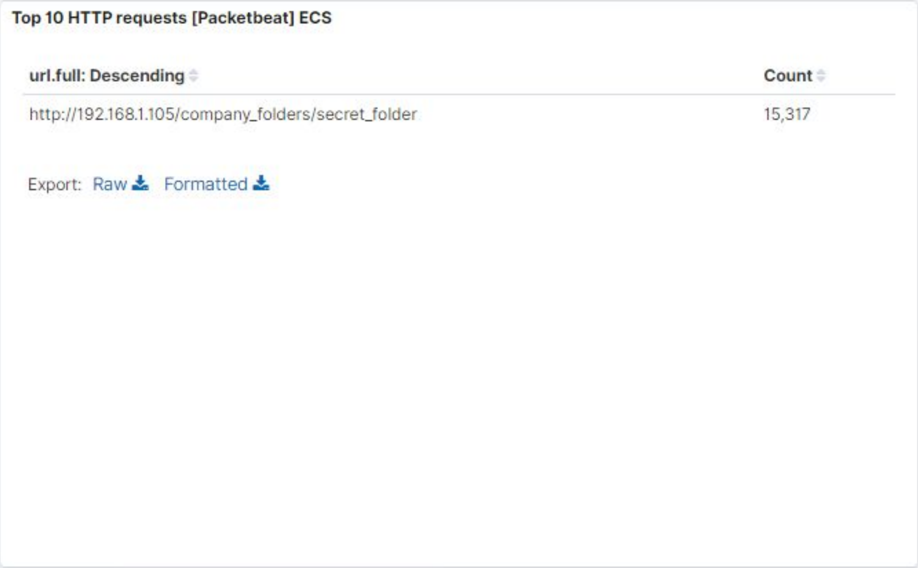

Top Hosts Creating Traffic [Packetbeat Flows] ECS

Analysis: Uncovering the Brute Force Attack

- On 07/05/2022 at approximately 2100 hours there were (15,316) 401 request and (1) 301 request made from source IP 192.168.1.90 to http://192.168.1.105/company _folder/secret_folder.
- I’ve identified this as a successful brute force attack judging by the amount of requests made in such little time and the status response codes.
  - 401 Unauthorized response status code indicates that the client request has not been completed because it lacks valid authentication credentials for the requested resource.
  - 301 Moved Permanently redirect status response code indicates that the requested resource has been definitively moved to the URL given by the Location headers.



HTTP status codes for the top queries [Packetbeat] ECS



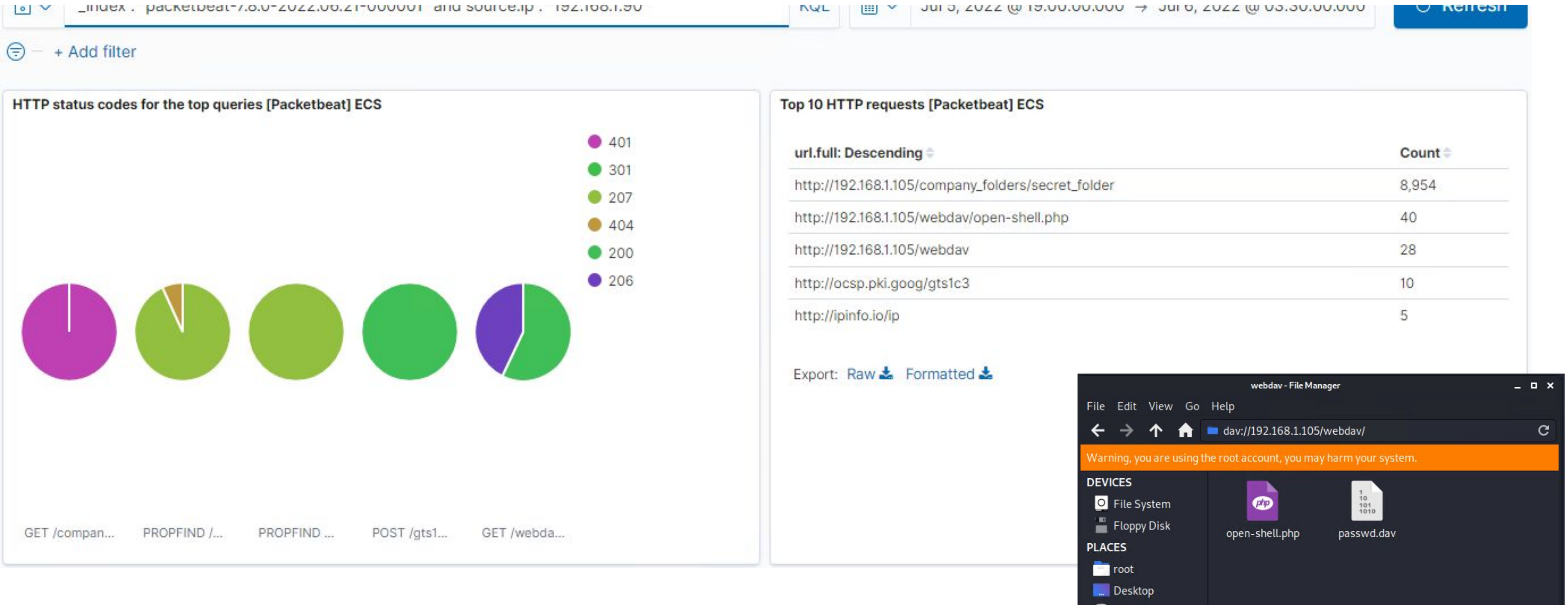
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,317

Export: Raw Formatted

Analysis: Finding the WebDAV Connection

- 68 request were made to the /WebDav directory.
- The primary request was for open-shell.php file.
  - _index:"packetbeat-7.8.0-2022.6.21-000001" and source.ip: "192.168.1.90"
  - **207: Multi-Status:** The 207 Multi-Status status code provides status for multiple independent processes and used by WebDAV servers.



_index : packetbeat-7.8.0-2022.06.21-000001 and source.ip : 192.168.1.90

KQL
Jul 5, 2022 @ 19:00:00.000 → Jul 6, 2022 @ 03:30:00.000
Refresh
+ Add filter
HTTP status codes for the top queries [Packetbeat] ECS
401
301
207
404
200
206
GET /compan...
PROPFIND /...
PROPFIND ...
POST /gts1...
GET /webda...

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	8,954
http://192.168.1.105/webdav/open-shell.php	40
http://192.168.1.105/webdav	28
http://ocsp.pki.goog/gts1c3	10
http://ipinfo.io/ip	5

Export: Raw Formatted

webdav - File Manager

dav://192.168.1.105/webdav/

Warning, you are using the root account, you may harm your system.

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

I recommend an alarm be set to alert the SOC team in the event of a port scan. This can be set to trigger an alert after the lowest possible detection rate (10 packets in a period of 1,000,000 microseconds).

System Hardening

- Port scans should first be ran to identify what is visible to an attacker during a port scan and any vulnerabilities should be addressed.
- To mitigating reconnaissance an IPS firewall should be installed which will automatically block traffic that is deemed malicious in real time.
- Threat hunting teams should be monitoring these IP addresses checking OSINT tools like looking glass to see if they are deemed malicious, and if so they should be putting DNS sinkhole request to have these attackers blocked.
- SOC team should be working 24 hours monitoring these alerts with a set time to respond so data collection could be minimal if any.

Mitigation: Finding the Request for the Hidden Directory

Alarm

To detect any unauthorized access to the companies hidden folders I would recommend a 5 attempt threshold be set. I will also recommend access to these folders be restricted to only allow access on the companies network/vpn.

System Hardening

- These folders should not be accessible to the public. Create a text file:

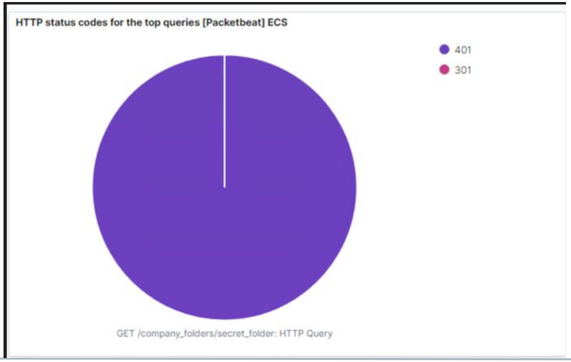
  -
    ```
    # Simple File List Access Restrictor

    RewriteEngine On

    # 1) If NOT the current host
    RewriteCond
    %{HTTP_HOST}@@%{HTTP_REFERER}
    !^([^@]*)@@https?://\1/.*

    # 2) Deny access to these types
    RewriteRule
    \.(gif|jpg|jpeg|png|tif|pdf|wav|wmv|wma|avi|mov|mp
    4|m4v|mp3|zip?)$ - [F]
    ```
- This should send a 403 forbidden response when trying to access. For more information visit site below:

https://simplefilelist.com/how-can-i-prevent-direct-url-access-to-my-files-from-outside-my-website/

Mitigation: Preventing Brute Force Attacks

Alarm

- The HyperText Transfer Protocol (HTTP) 401 Unauthorized response status code indicates that the client request has not been completed because it lacks valid authentication credentials for the requested resource.
- An Alert could be set to email the SOC team after multiple 401 errors occur.



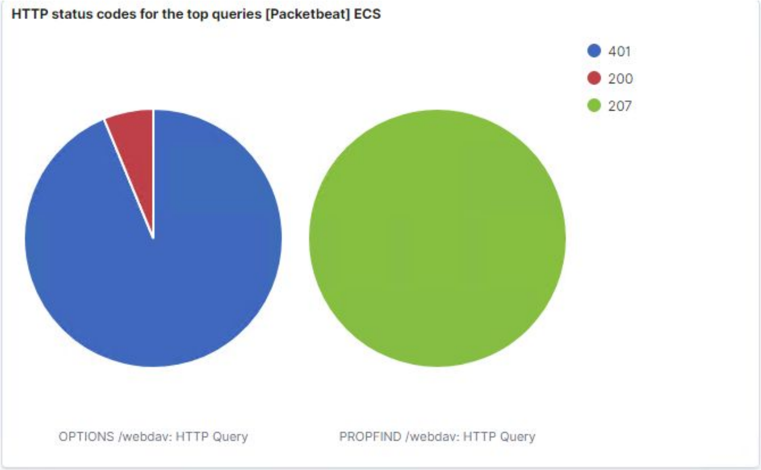
System Hardening

- A RSA token or any 2 factor authentication should be set to mitigate brute force attacks.
- Password policies should be strict 8 or more characters, letters, numbers, special characters, and no ascending or descending letters or numbers.
- Account lockout policy should be set to lock account after 3 to 5 failed attempts. Forcing the user to call the helpdesk to have the password unlocked.
- Limit login attempts to users with a certain IP address or IP range, limiting access to only users on the network or assigned to manage the folder.
- Login credentials shouldn't be shared.
- Passwords or hashes shouldn't be saved to plain text documents.

Mitigation: Detecting the WebDAV Connection

Alarm

- An Alert could be set to email the SOC team after multiple 401 errors occur. Alerts could also be set to alert the SOC team if a 200 status code is triggered from an outside IP address.



System Hardening

- If all other vulnerabilities are addressed then WebDAV connections will already be more secure.
- I recommend allowing only access to the WebDav from set IP address.
- Users credentials should not be shared.
- Of course passwords should be strengthen.
- RSA token could be setup for users accounts to insure users aren’t sharing accounts.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- An alert could be set to trigger an alert if specific types of files are uploaded.

System Hardening

- After changing the access to the WebDav to disable public access users shouldn't be able to login without access granted by IT.
- An SIEM like crowdstrike could be installed to quarantine files that are potentially malicious uploaded to servers. This will also scan the file in a case where the file extension is changed.

The End