Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

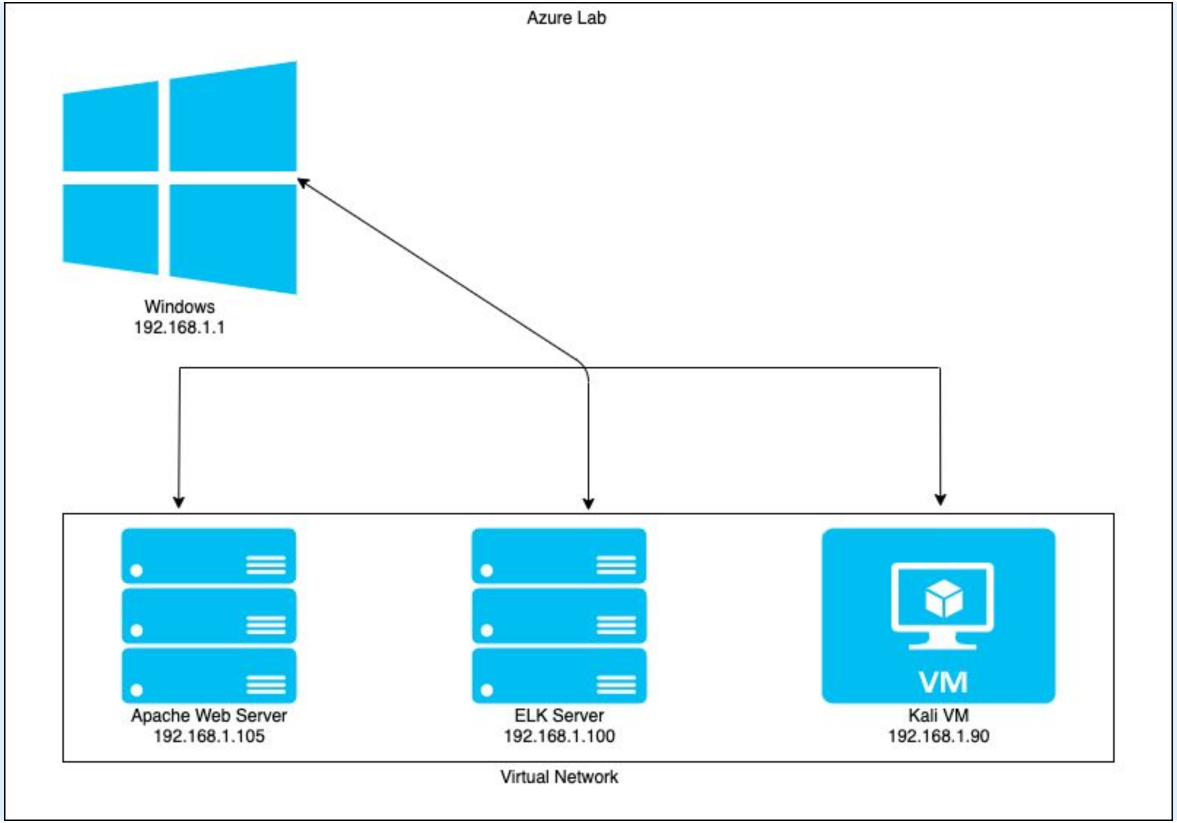
02 **Red Team**: Security Assessment

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: 192.168.1.1
OS: Windows 2008 Server
Hostname: Microsoft

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK Server

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone
(Apache Web Server)

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Windows 2008 Server	192.168.1.1	Remote Desktop
ELK	192.168.1.100	Search and analytics engine
Capstone	192.168.1.105	Linux Server
Kali	192.168.1.90	Attack Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2014-9278	*Open SSH*	*which might bypass intended authorization requirements that would force a local login*
CVE-2018-1312	Authentication Challenge	When generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated. HTTP Requests could be replayed across servers
CVE-2019-0211	Privilege Escalation	*Code executing in less-privileged child processes or threads could execute arbitrary code with the privileges of the parent process by manipulating the scoreboard*
Ashton’s Blog	Unsecured data	Confidentiality breach

Exploitation: Ashton’s Blog

01

Tools & Processes

Tools used:

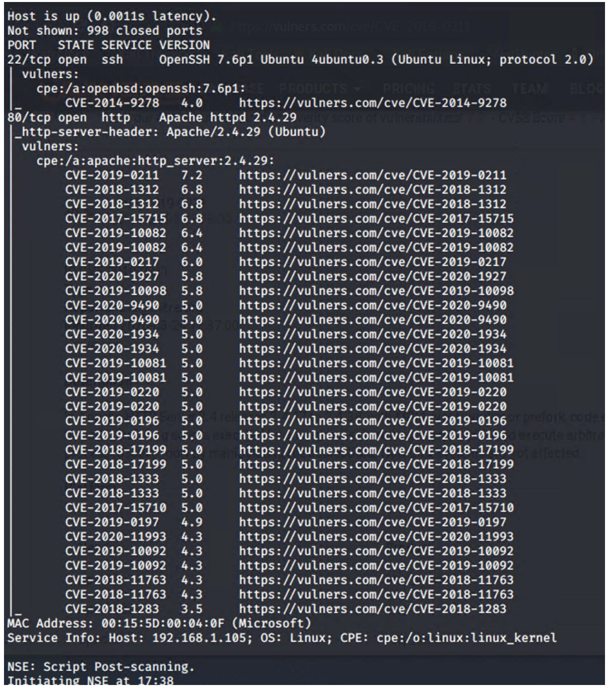
NMAP

02

Achievements

An NMAP scan found there were to ports open: 22, and 80. Without an SSH key, port 22 would not be accessible. Port 80 reveals that there is access through a website available.

03



```
Host is up (0.0011s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.6p1:
|_      CVE-2014-9278   4.0     https://vulners.com/cve/CVE-2014-9278
80/tcp open  http    Apache httpd 2.4.29
|_http-server-header: Apache/2.4.29 (Ubuntu)
| vulners:
|   cpe:/a:apache:http_server:2.4.29:
|       CVE-2019-0211   7.2     https://vulners.com/cve/CVE-2019-0211
|       CVE-2018-1312   6.8     https://vulners.com/cve/CVE-2018-1312
|       CVE-2018-1312   6.8     https://vulners.com/cve/CVE-2018-1312
|       CVE-2017-15715  6.8     https://vulners.com/cve/CVE-2017-15715
|       CVE-2019-10082  6.4     https://vulners.com/cve/CVE-2019-10082
|       CVE-2019-10082  6.4     https://vulners.com/cve/CVE-2019-10082
|       CVE-2019-0217   6.0     https://vulners.com/cve/CVE-2019-0217
|       CVE-2020-1927   5.8     https://vulners.com/cve/CVE-2020-1927
|       CVE-2019-10098  5.8     https://vulners.com/cve/CVE-2019-10098
|       CVE-2020-9490   5.0     https://vulners.com/cve/CVE-2020-9490
|       CVE-2020-9490   5.0     https://vulners.com/cve/CVE-2020-9490
|       CVE-2020-1934   5.0     https://vulners.com/cve/CVE-2020-1934
|       CVE-2020-1934   5.0     https://vulners.com/cve/CVE-2020-1934
|       CVE-2019-10081  5.0     https://vulners.com/cve/CVE-2019-10081
|       CVE-2019-10081  5.0     https://vulners.com/cve/CVE-2019-10081
|       CVE-2019-0220   5.0     https://vulners.com/cve/CVE-2019-0220
|       CVE-2019-0220   5.0     https://vulners.com/cve/CVE-2019-0220
|       CVE-2019-0196   5.0     https://vulners.com/cve/CVE-2019-0196
|       CVE-2019-0196   5.0     https://vulners.com/cve/CVE-2019-0196
|       CVE-2018-17199  5.0     https://vulners.com/cve/CVE-2018-17199
|       CVE-2018-17199  5.0     https://vulners.com/cve/CVE-2018-17199
|       CVE-2018-1333   5.0     https://vulners.com/cve/CVE-2018-1333
|       CVE-2018-1333   5.0     https://vulners.com/cve/CVE-2018-1333
|       CVE-2017-15710  5.0     https://vulners.com/cve/CVE-2017-15710
|       CVE-2019-0197   4.9     https://vulners.com/cve/CVE-2019-0197
|       CVE-2020-11993  4.3     https://vulners.com/cve/CVE-2020-11993
|       CVE-2019-10092  4.3     https://vulners.com/cve/CVE-2019-10092
|       CVE-2019-10092  4.3     https://vulners.com/cve/CVE-2019-10092
|       CVE-2018-11763  4.3     https://vulners.com/cve/CVE-2018-11763
|       CVE-2018-11763  4.3     https://vulners.com/cve/CVE-2018-11763
|_      CVE-2018-1283   3.5     https://vulners.com/cve/CVE-2018-1283
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 17:38
```

Exploitation: /webdav/ password crack

01

Tools & Processes

THC Hydra

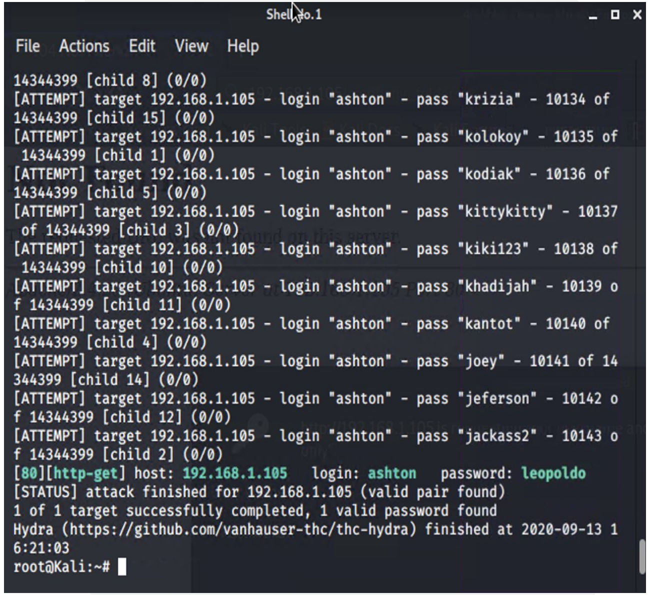
02

Achievements

Hydra was used to bruteforce the username and password for authentication into the /company_folders/secret_folder directory. After running Hydra, we were able to access the hidden directory and found the username:password was: Ashton:leopoldo

Inside were inscructions to access the /webdav/ server

03



```
14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 12] (0/0)
[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 2020-09-13 1
6:21:03
root@Kali:~# █
```

Exploitation:

01

Tools & Processes

Kali File System

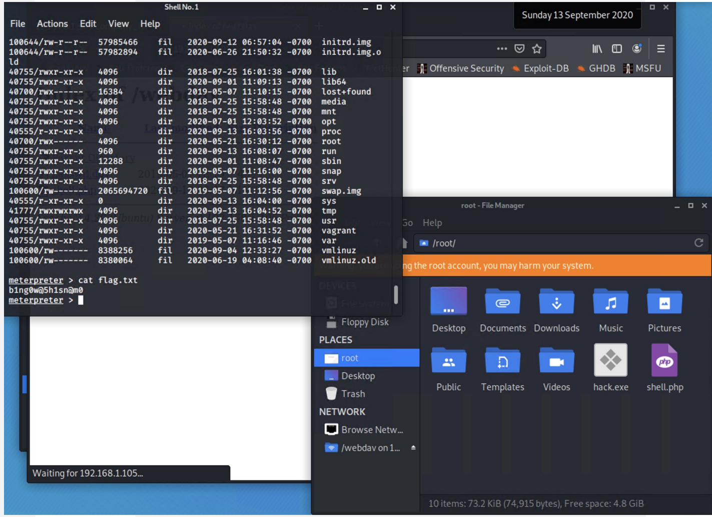
Metasploit: msfvenom PHP reverse shell payload

02

Achievements

After achieving connecting to the /webdav server through Kali File System Network, we created a PHP reverse shell payload using Metasploit msfvenom. We then dropped the payload into the /webdav directory through the file system. We logged back into the /webdav server through the browser and opened the shell and gained full access to the root directory using Metasploit meterpreter.

03



Sunday 13 September 2020

```
100644/rw-r--r--  57985466    fil   2020-09-12 06:57:04 -0700  initrd.img
100644/rw-r--r--  57982894    fil   2020-06-26 21:50:32 -0700  initrd.img.o
ld
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096        dir   2020-09-01 11:09:13 -0700  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   2020-09-13 16:03:56 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   960         dir   2020-09-13 16:08:07 -0700  run
40755/rwxr-xr-x   12288       dir   2020-09-01 11:08:47 -0700  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   2020-09-13 16:04:00 -0700  sys
41777/rwxrwxrwx   4096        dir   2020-09-13 16:04:52 -0700  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   2020-09-04 12:33:27 -0700  vmlinuz
100600/rw-------  8380064     fil   2020-06-19 04:08:40 -0700  vmlinuz.old

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

ng the root account, you may harm your system.

10 items: 73.2 KiB (74,915 bytes), Free space: 4.8 GiB

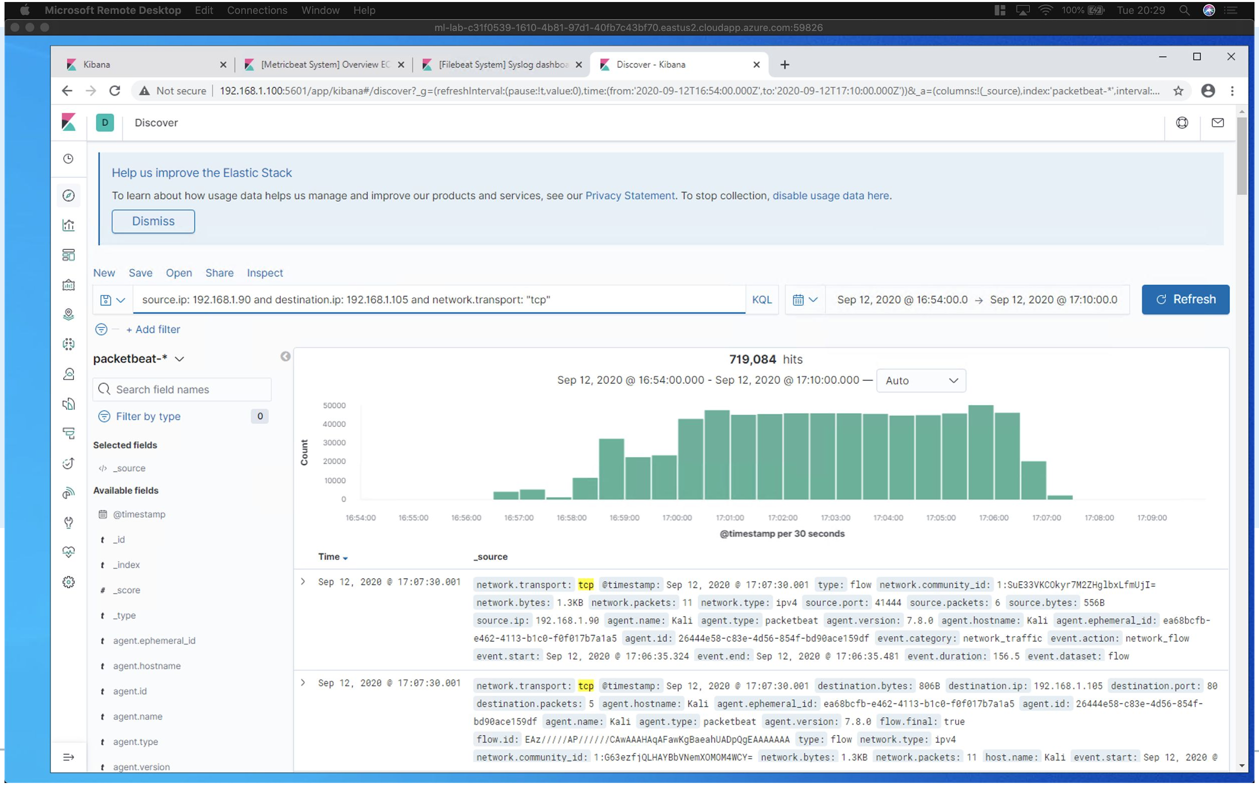
Waiting for 192.168.1.105...

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scans were between 2020-09-12 16:58:00-17:07:00
- This was likely an NMAP scan from the unusually high spike of TCP requests



192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2020-09-12T16:54:00.000Z',to:'2020-09-12T17:10:00.000Z'))&_a=(columns:!(_source),index:'packetbeat-*',interval:...

Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Dismiss

source.ip: 192.168.1.90 and destination.ip: 192.168.1.105 and network.transport: "tcp"

Sep 12, 2020 @ 16:54:00.0 → Sep 12, 2020 @ 17:10:00.0

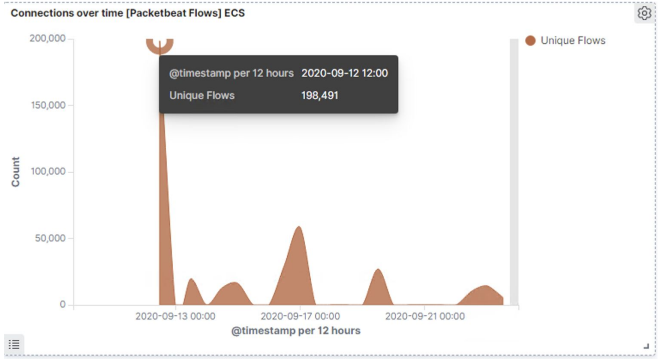
719,084 hits

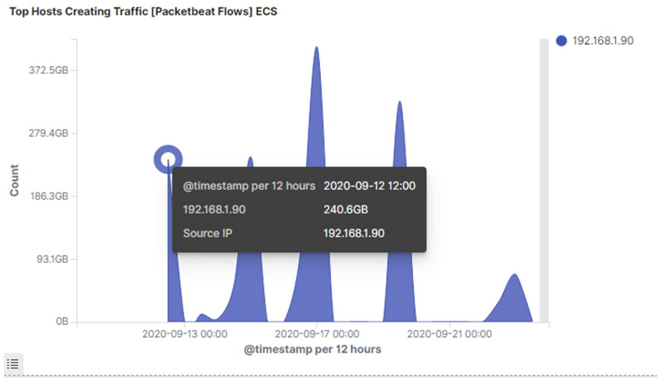
Sep 12, 2020 @ 16:54:00.000 - Sep 12, 2020 @ 17:10:00.000 —

```
> Sep 12, 2020 @ 17:07:30.001  network.transport: tcp @timestamp: Sep 12, 2020 @ 17:07:30.001 type: flow network.community_id: 1:SuE33VKCOkyr7M2ZHglbxLfmUjI=
                               network.bytes: 1.3KB network.packets: 11 network.type: ipv4 source.port: 41444 source.packets: 6 source.bytes: 556B
                               source.ip: 192.168.1.90 agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: ea68bcfb-
                               e462-4113-b1c0-f0f017b7a1a5 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df event.category: network_traffic event.action: network_flow
                               event.start: Sep 12, 2020 @ 17:06:35.324 event.end: Sep 12, 2020 @ 17:06:35.481 event.duration: 156.5 event.dataset: flow

> Sep 12, 2020 @ 17:07:30.001  network.transport: tcp @timestamp: Sep 12, 2020 @ 17:07:30.001 destination.bytes: 806B destination.ip: 192.168.1.105 destination.port: 80
                               destination.packets: 5 agent.hostname: Kali agent.ephemeral_id: ea68bcfb-e462-4113-b1c0-f0f017b7a1a5 agent.id: 26444e58-c83e-4d56-854f-
                               bd90ace159df agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 flow.final: true
                               flow.id: EAz/////AP//////CAwAAAHAqAFawKgBaeahUADpQgEAAAAAAA type: flow network.type: ipv4
                               network.community_id: 1:G63ezfjQLHAYBbVNemXOMOM4WCY= network.bytes: 1.3KB network.packets: 11 host.name: Kali event.start: Sep 12, 2020 @
```

Analysis: Identifying the Port Scan (cont.)

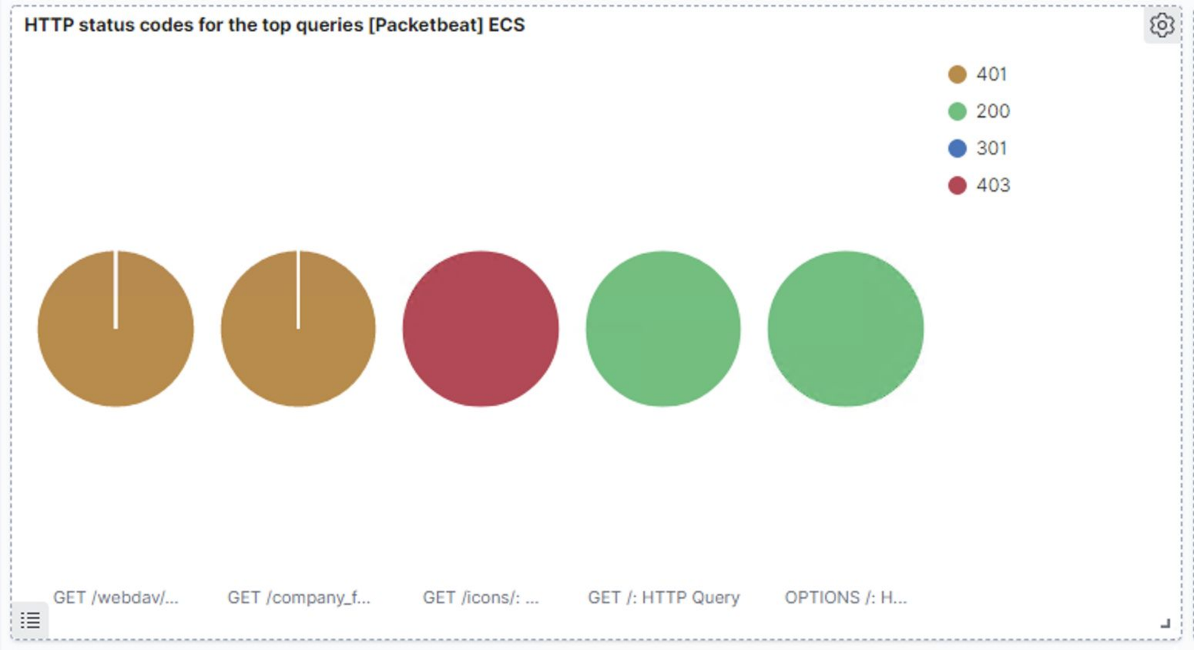

Connections over time [Packetbeat Flows] ECS


Top Hosts Creating Traffic [Packetbeat Flows] ECS

- There were 198,491 packets sent from the IP address: 192.168.1.90

Analysis: Identifying the Port Scan (cont.)

The victim's response:

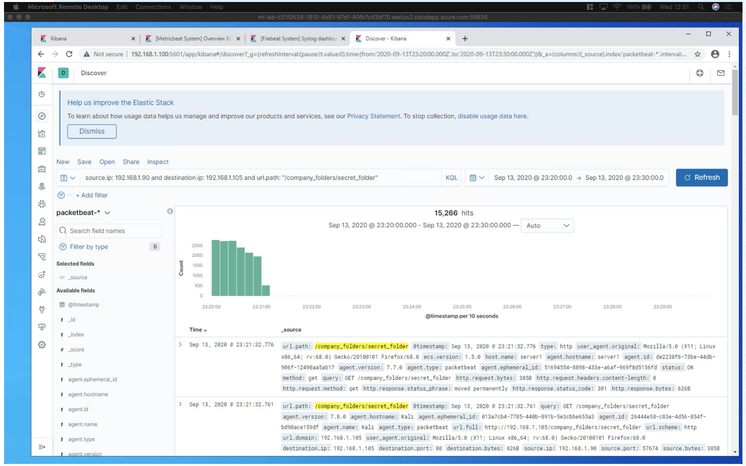


The victim responded back with the following HTTP status codes:

- 401 (unauthorized client error)
- 200 (ok)
- 301 (moved permanently redirect)
- 403 (Forbidden client error)

Analysis: Finding the Request for the Hidden Directory

- Access to the url path /company_folders/secret_folder that contained information to login to the server



Not secure | 192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2020-09-13T23:20:00.000Z',to:'2020-09-13T23:30:00.000Z'))&_a=(columns:!(_source),index:'packetbeat-*',interval:...

Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Dismiss

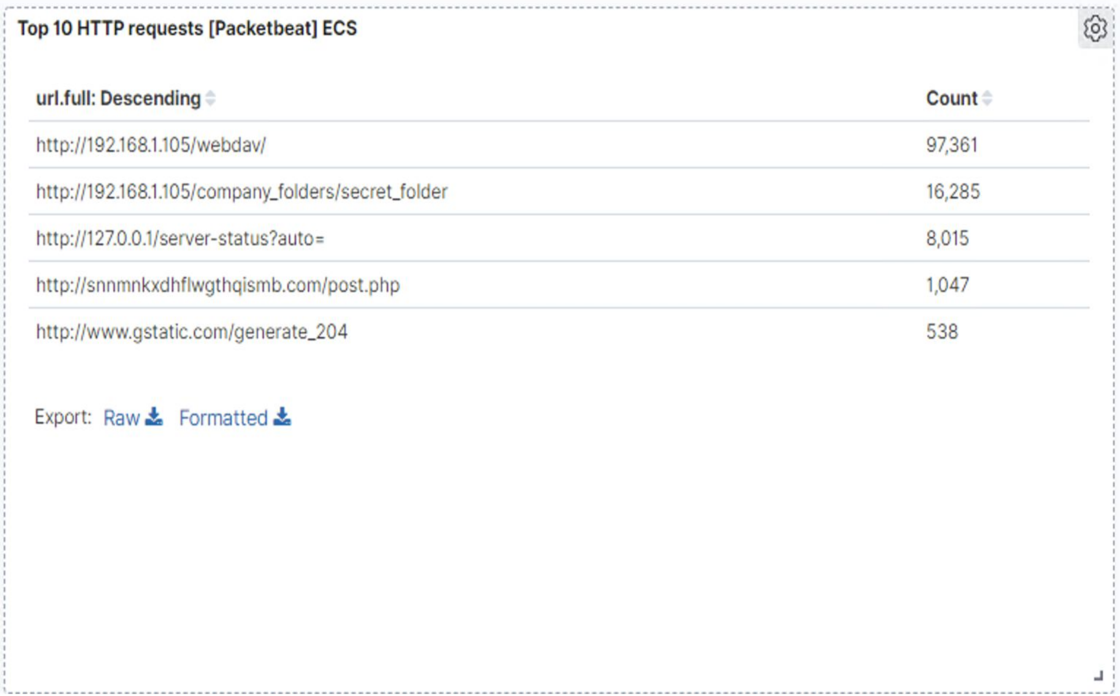
source.ip: 192.168.1.90 and destination.ip: 192.168.1.105 and url.path: "/company_folders/secret_folder"

Sep 13, 2020 @ 23:20:00.0 → Sep 13, 2020 @ 23:30:00.0

15,266 hits

Sep 13, 2020 @ 23:20:00.000 - Sep 13, 2020 @ 23:30:00.000

```
Time                        _source
> Sep 13, 2020 @ 23:21:32.776   url.path: /company_folders/secret_folder @timestamp: Sep 13, 2020 @ 23:21:32.776 type: http user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 ecs.version: 1.5.0 host.name: server1 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 51694554-8898-433e-a6af-969f8d5156fd status: OK method: get query: GET /company_folders/secret_folder http.request.bytes: 385B http.request.headers.content-length: 0 http.request.method: get http.response.status_phrase: moved permanently http.response.status_code: 301 http.response.bytes: 626B
> Sep 13, 2020 @ 23:21:32.761   url.path: /company_folders/secret_folder @timestamp: Sep 13, 2020 @ 23:21:32.761 query: GET /company_folders/secret_folder agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: 013a7cb4-7785-440b-891b-5e3cbbe655a3 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 626B source.ip: 192.168.1.90 source.port: 57674 source.bytes: 385B
```

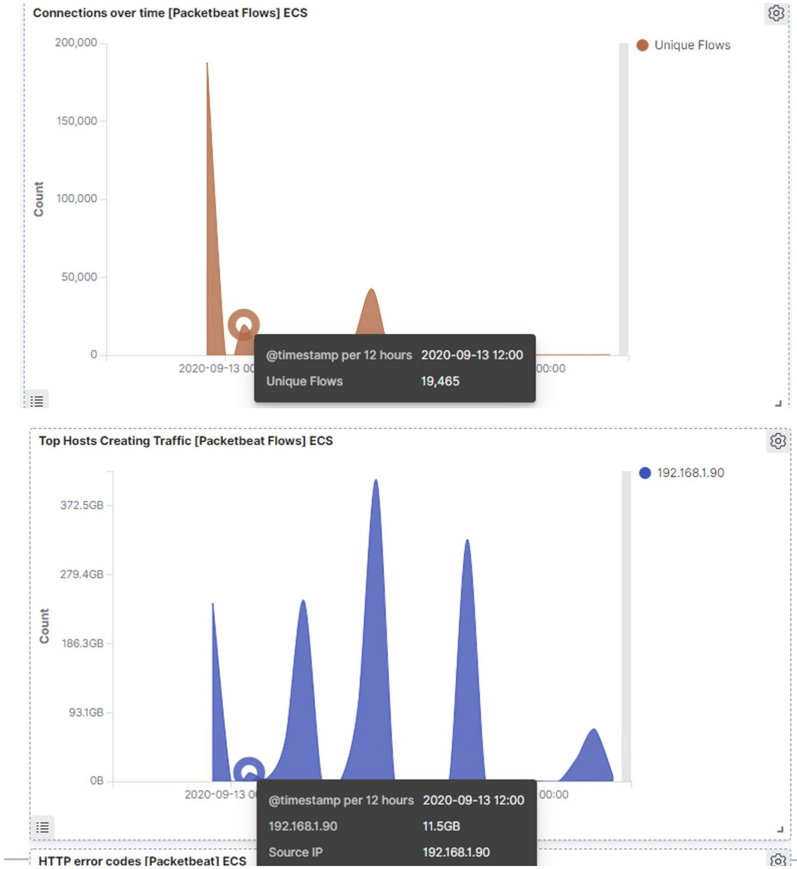


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/	97,361
http://192.168.1.105/company_folders/secret_folder	16,285
http://127.0.0.1/server-status?auto=	8,015
http://snnmnkxdhflwgthqismb.com/post.php	1,047
http://www.gstatic.com/generate_204	538

Export: Raw Formatted

Analysis: Finding the Request for the Hidden Directory (cont.)



Connections over time [Packetbeat Flows] ECS

@timestamp per 12 hours 2020-09-13 12:00
Unique Flows 19,465

Top Hosts Creating Traffic [Packetbeat Flows] ECS

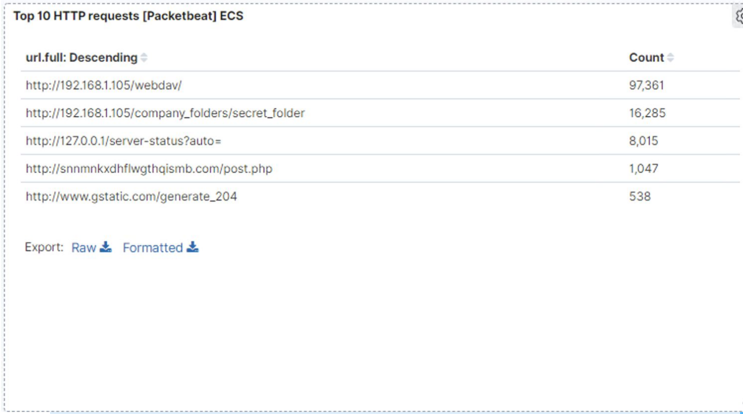
@timestamp per 12 hours 2020-09-13 12:00
192.168.1.90 11.5GB
Source IP 192.168.1.90

HTTP error codes [Packetbeat] ECS

- The Hidden Directory requests were started at 2020-09-13 23:20:00
- There were 19,465 requests

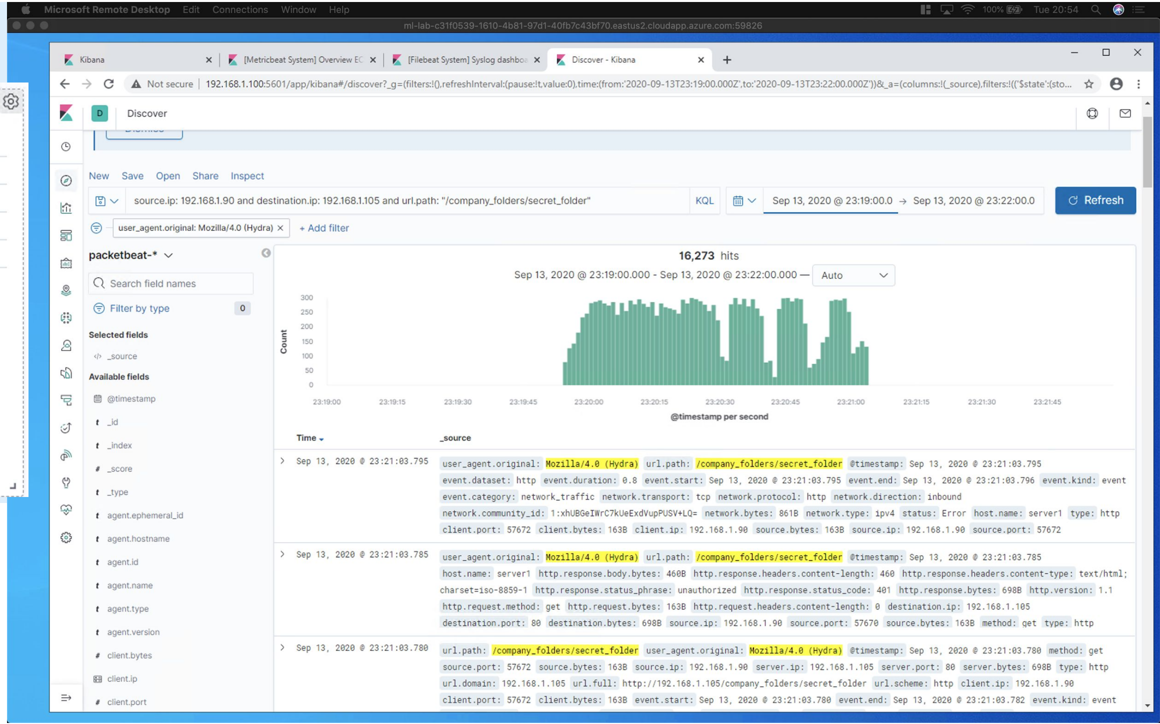
Analysis: Uncovering the Brute Force Attack

- The /secret_folder directory was requested 16,285 times
- There is not sufficient data from this particular data to show how many times the attacker discovered the password. However we do know the attacker got access due to the amount of requests for the /webdav/ directory



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/	97,361
http://192.168.1.105/company_folders/secret_folder	16,285
http://127.0.0.1/server-status?auto=	8,015
http://snnmnkxdhflwgthqismb.com/post.php	1,047
http://www.gstatic.com/generate_204	538



```
192.168.1.100:5601/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2020-09-13T23:19:00.000Z',to:'2020-09-13T23:22:00.000Z'))&_a=(columns:!(_source),filters:!(('$state':(sto...
```

```
source.ip: 192.168.1.90 and destination.ip: 192.168.1.105 and url.path: "/company_folders/secret_folder"
```

Sep 13, 2020 @ 23:19:00.0 → Sep 13, 2020 @ 23:22:00.0

user_agent.original: Mozilla/4.0 (Hydra)

16,273 hits

Sep 13, 2020 @ 23:19:00.000 - Sep 13, 2020 @ 23:22:00.000 —

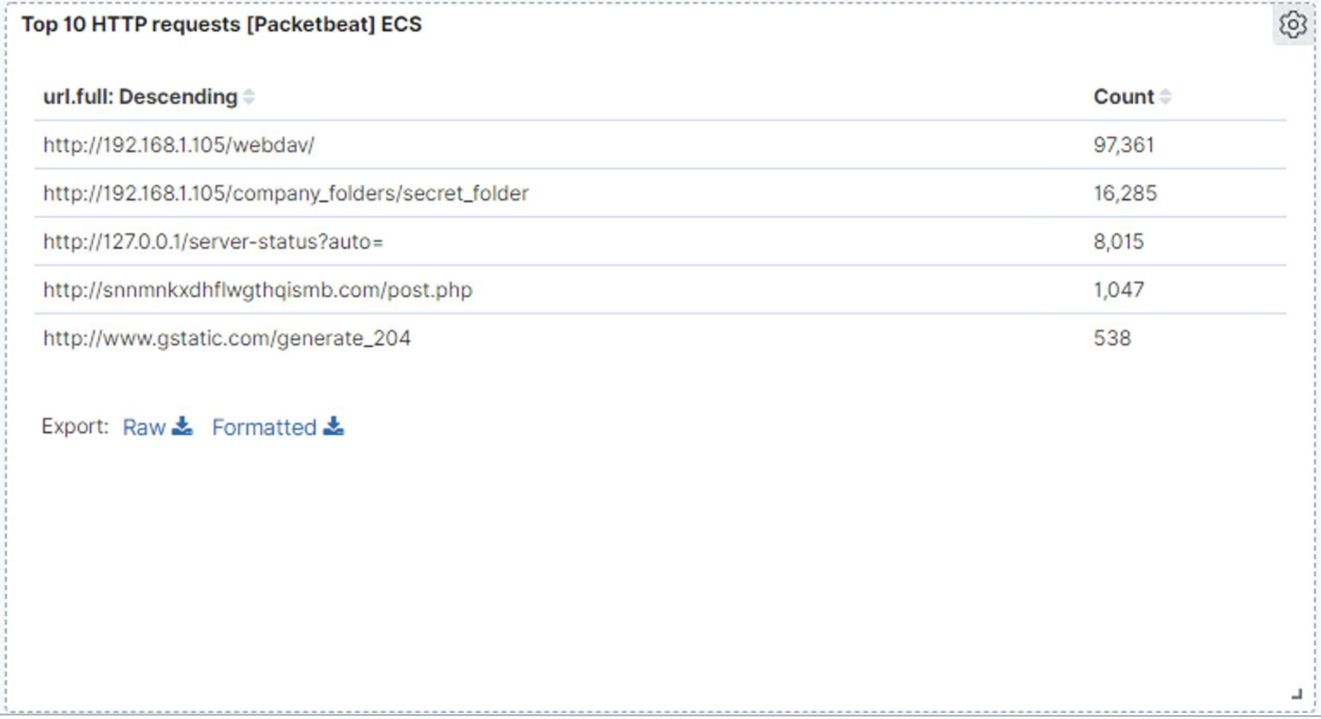
```
Sep 13, 2020 @ 23:21:03.795   user_agent.original: Mozilla/4.0 (Hydra) url.path: /company_folders/secret_folder @timestamp: Sep 13, 2020 @ 23:21:03.795
                              event.dataset: http event.duration: 0.8 event.start: Sep 13, 2020 @ 23:21:03.795 event.end: Sep 13, 2020 @ 23:21:03.796 event.kind: event
                              event.category: network_traffic network.transport: tcp network.protocol: http network.direction: inbound
                              network.community_id: 1:xhUBGeIWrC7kUeExdVupPUSV+LQ= network.bytes: 861B network.type: ipv4 status: Error host.name: server1 type: http
                              client.port: 57672 client.bytes: 163B client.ip: 192.168.1.90 source.bytes: 163B source.ip: 192.168.1.90 source.port: 57672

Sep 13, 2020 @ 23:21:03.785   user_agent.original: Mozilla/4.0 (Hydra) url.path: /company_folders/secret_folder @timestamp: Sep 13, 2020 @ 23:21:03.785
                              host.name: server1 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.response.bytes: 698B 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 source.ip: 192.168.1.90 source.port: 57670 source.bytes: 163B method: get type: http

Sep 13, 2020 @ 23:21:03.780   url.path: /company_folders/secret_folder user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Sep 13, 2020 @ 23:21:03.780 method: get
                              source.port: 57672 source.bytes: 163B source.ip: 192.168.1.90 server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B type: http
                              url.domain: 192.168.1.105 url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http client.ip: 192.168.1.90
                              client.port: 57672 client.bytes: 163B event.start: Sep 13, 2020 @ 23:21:03.780 event.end: Sep 13, 2020 @ 23:21:03.782 event.kind: event
```

Analysis: Finding the WebDAV Connection

- There were 97,361 requests to the /webdav/ directory
- The data provided do not reveal how many requests were made until the attacker requested the shell.php. However we do know a connection was established due to the shell.php found in the /webdav/ directory



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/	97,361
http://192.168.1.105/company_folders/secret_folder	16,285
http://127.0.0.1/server-status?auto=	8,015
http://snnmnkxdhflwgthqismb.com/post.php	1,047
http://www.gstatic.com/generate_204	538

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?

- The number of requests per second

What threshold would you set to activate this alarm?

- If a single IP address sends more than 10 reqests per second for more than 5 seconds

System Hardening

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

- A firewall can be used to throttle incoming connections
- An IP allowlist can be developed and enabled
- Filter ICMP traffic
- Use a firewall to redirect open ports to “honeypots” or open empty hosts

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Allowlist authorized IP addresses only
- If IP outside the allowlist attempts to connect to server it trips an alarm

What threshold would you set to activate this alarm?

- The threshold would be an IP outside of the allowlist trying to request access to the server

System Hardening

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

- The users should be required to change their password to something harder to crack and change them monthly.
- The sensitive files should have their own encryption in case they are acquired.
- Rename the directory name something less suspicious for attackers without any hints to help the user access the files

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Number of requests per second

What threshold would you set to activate this alarm?

- More than 100 requests per second for 5 seconds would be a good threshold
-

System Hardening

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

- Locking out accounts after a certain number of incorrect login attempts
- Make root user inaccessible via SSH by editing *sshd_config*
- Don't use a default port, change the port in *sshd_config*
- Two factor authentication
- Unique login URL's
- Limit logins to a specified IP address or range

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Monitor access to /webdav/ with Filebeat
- Set an alarm if any files within /webdav/ are accessed

What threshold would you set to activate this alarm?

- Anytime /webdav/ is accessed

System Hardening

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

- Admins have to install and configure Filebeat on the host

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Set an alarm if a POST request is detected containing a filetype such as .php

What threshold would you set to activate this alarm?

- Anytime a forbidden file is uploaded by anyone an alarm should be triggered

System Hardening

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

- Restrict write permissions
- Uploads can be isolated in a dedicated storage partition that can be monitored closely
- Enable and configure Filebeat
- Lock down outgoing connectivity to allow only specific IP addresses and ports

The End