Writeup for basic_pentesting_2

Method2(ProFTPD)

General:

This machine is an Ubuntu server that is basically a web server which is to be cracked and root privileges are to be gained. The machine cannot even be started by entering the root password. It stops at the login screen itself for us to work our way around.

Steps:

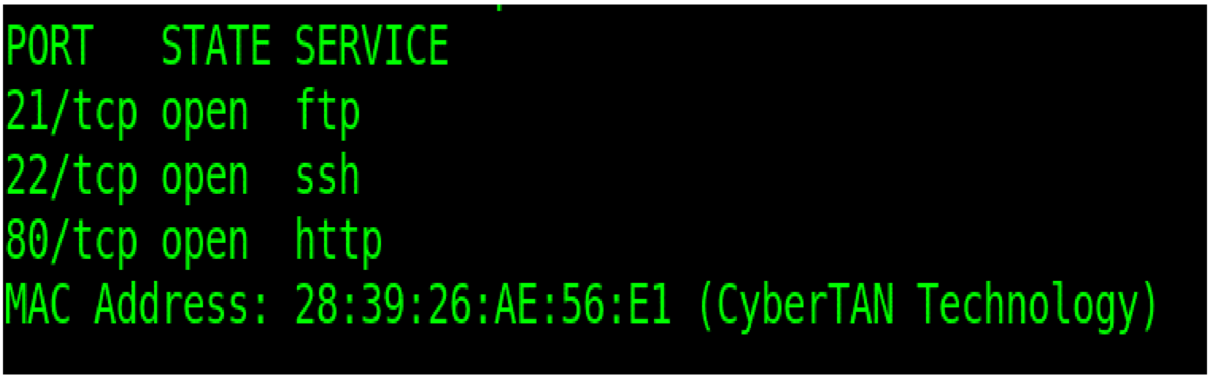
→Enumerating the machine

Tools used: NMAP

Other tools that can be used: netdiscover

We get to know that there are 3 posts open ie. 21, 22 and port 80

The corresponding services are as follows:



```
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 28:39:26:AE:56:E1 (CyberTAN Technology)
```

Upon doing a -A type (fast) scan on the machine ip we get to know that there is a ProFTPD 1.3.3.c service running on port 21.

→Searching for a suitable exploit

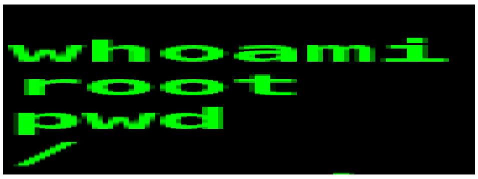
Upon searching ExploitDB for ProFTPD 1.3.3.c using searchsploit we get one for Backdoor Command Execution which is of our use.

Tools used: searchsploit

→exploitation using metasploit

Run metasploit and using the "search" command find the exploit for ProFTPD. We will be using "exploit/unix/ftp/proftpd_133c_backdoor". Set the required options for it and also use a payload "cmd/unix/reverse". This payload will be run on the vulnhub machine and will give us a Double Reverse TCP (telnet) connection between both the machines.

Tools used: msfconsole



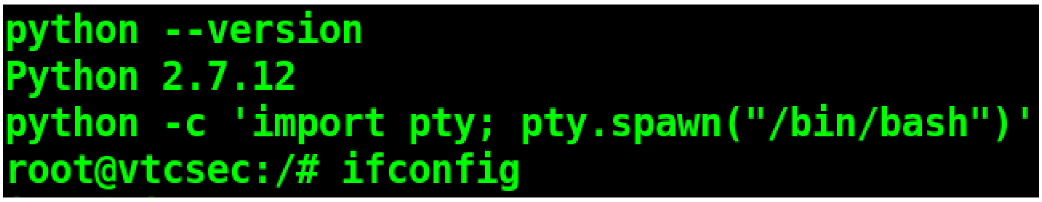
```
whoami
root
pwd
/
```

→SPAWNING AN INTERACTIVE SHELL USING PYTHON

As already known from the type 1 way of exploitation we can upgrade a simple reverse shell to a fully interactive tty (teletype) using python.

Note: The tty command of terminal basically prints the file name of the terminal connected to standard input. tty is short of teletype, but popularly known as a terminal it allows you to interact with the system by passing on the data (you input) to the system, and displaying the output produced by the system.

Tools used: Metasploit-framework, Python



```
python --version
Python 2.7.12
python -c 'import pty; pty.spawn("/bin/bash")'
root@vtcsec:/# ifconfig
```

→GETTING THE HASHED PASSWORD OF THE USER MARLINSPIKE

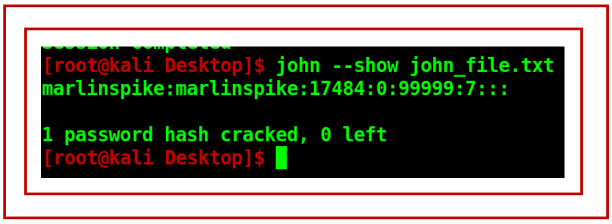
After properly using tty to spawn an interactive shell we can now copy the hashed password from the "/etc/shadow" file onto our kali machine and crack it using John The Ripper.

→CRACKING THE HASHED PASSWORD

Using John The Ripper we will now crack the hashed version and convert it to the simple text format. We first copy-paste the hashed version of the password to a file and pass the file to john. Then we use the "—show" command to display the cracked password which turns out to be marlinspike. ENJOY!!!

Tools used: John The Ripper

P*roof of me owning the machine:*



```
[root@kali Desktop]$ john --show john_file.txt
marlinspike:marlinspike:17484:0:99999:7:::

1 password hash cracked, 0 left
[root@kali Desktop]$ █
```