Writeup for basic_pentesting_1

Method1(Wordpress)

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:

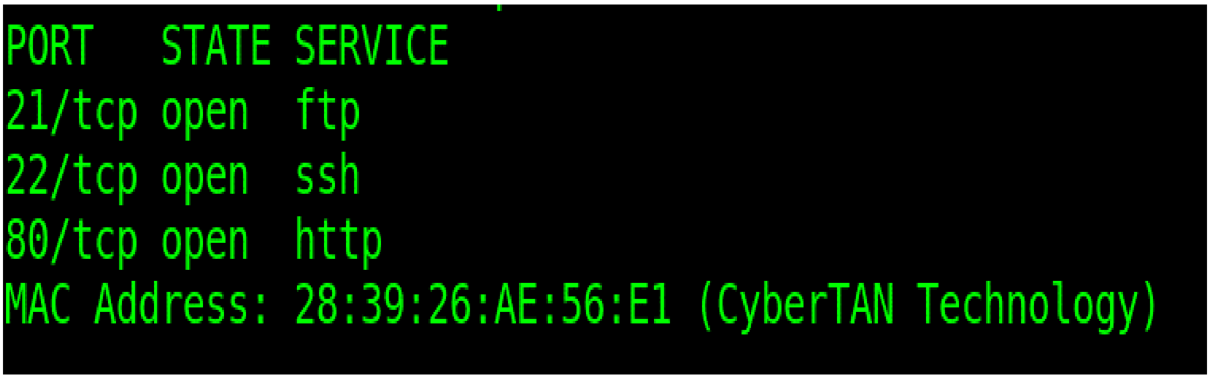
→Enumerating the machine

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 finding the ip address of the machine we navigate to that web address to find a basic dummy website.

→Finding hidden directories

This web address must have many other hidden directories and to find them we use dirb for enumerating about them.

Tools used: dirb

Other tools that can be used:

dirbuster, gobuster, Metasploit auxiliary/scanner/http/dir_scanner, wfuzz, dirsearch

The result of dirb tells us that the /secret directory exists on the web server. Upon navigating to the directory in a web browser we find out that it is a web blog using wordpress. Upon searching more on the blog page in the /secret directory we find that the domain “vtcsec” is used to host it.

Note: If the /secret directory of the web server is down or not fully loading then add an entry for the domain name “vtcsec” in your attacker machine’s host file for the domain vtcsec and the corresponding ip that the vulnhub machine has acquired from your network. In this way the attacker system knows that the vtcsec domain refers to which ip on the network, basically resolving vtcsec to an ip.

→Enumerating the blog

This blog is found to have a login option allowing us to login into the wordpress dashboard. Now we will use tools to find potential users and also ways to bruteforce the login for wordpress.

Tools used: wpscan

Other tools that can be used: Wpcracker, NMAP NSE Scripts, burpsuite_intruder, nikto scanner

Upon using the tools, we find out that the default user “admin” does exists upon the system. Now to get the password for it is the next task. The default username:password combination for wordpress is admin:admin. Luckily for this machine admin:admin works and we are into the wordpress dashboard.

→Uploading a Metasploit plugin to gain meterpreter access

Here we have used a plugin by the name “wp_admin_shell_upload” to open a meterpreter session on the target. A meterpreter session can then be used to upload a shell on the target. Meterpreter session is successfully created and now we start with the “getuid” command to know our identity of login in the meterpreter session. We are not root and will take some work to reach there.

Tools used: Metasploit-framework

→Privilege escalation

We will be using the “unix-privesc-check” script to look for potential misconfigurations that can lead to privilege escalation. The script is from the pentestmonkey authors and they advise to grep the “WARNING” that is returned after the script is run. The warning displays that the /etc/passwd file has global write set for it, which is exactly the misconfiguration we have been looking for.

→Modifying the /etc/passwd file and uploading it

Now that we know that the /etc/passwd file is loosely configured we can download it onto our attacker system for local use, modify it and also upload the modified copy onto the vulnhub system. What we are going to do is create a hashed version of the root password of our choice (own3d in this case) using openssl, add the hashed version in the locally downloaded /etc/passwd file, then upload this file onto the vulnhub machine.

Tools used: openssl

Note: There is a difference between gaining a meterpreter session and a shell on the vulnhub machine!! A meterpreter session is always gained by default, but a meterpreter session is more like a two-way communication medium between the attacker machine and the hacked machine. A shell on the other hand, is used to modify the hacked system itself. Tasks like downloading and uploading files between the two systems cannot be done using a shell but can be done using a meterpreter session. In order to alter the hacked system and to spawn a interactive /bin/bash terminal of the hacked system we can use a shell. A shell can run commands on the hacked machine as if it being run from the terminal after a successful login.

→Invoking an interactive terminal on the hacked machine

Using the shell we will now spawn an interactive terminal using the "pty" package/module from python. The command for the same is:

python -c 'import pty; pty.spawn("/bin/bash")'

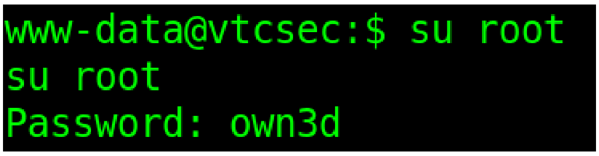
This will invoke /bin/bash and we get the interactive terminal.

→Logging in as root

The /etc/passwd file already has the hashed version of the "own3d" password and so when we switch user on the interactive terminal to root and enter the password as "own3d" we get a successful login.

We now Own the system…..ENJOY!!

Proof of me owning the machine:



```
www-data@vtcsec:$ su root
su root
Password: own3d
```