Step by step commands and tools used in this CTF

CTF: Mr Robot

Difficulty: Easy

Goal: have root access to the machine remotely.

Tools used:

- nmap (network scanning/enumeration)
- nikto (website host scanning)
- Metasploit (exploitation tool)
- Hydra (brute force username and password)

What I have done in this CTF is:

Information gathering: collecting info for exploitation

Exploitation: to have control over the machine.

Post Exploitation: to determine the value of the machine exploited and to maintain control of the machine for later use.

Vulnerabilities Found:

- Sensitive information disclosure (robots.txt exposure, Password hashes and usernames)
- Unprotected Wordpress admin portal (no brute force protection, allowed dictionary attack using hydra)

- Wordpress plugin upload vulnerability (used Metasploit module `wp_admin_shell_upload`. This exploit uploads a PHP reverse shell as a plugin through the wordpress dashboard)
- Weak credentials
- Misconfigured File permissions (SUID bit exploit)

Scan the network and find the ip of the vulnerable machine. Use nmap or netdiscover for scanning.

Now scan the host. The enumeration should include versions and ports details. I suggest using -A flag (aggressive scanning) for such enumeration.

Port 80 and 443 was open. So use the ip and put it into the browser. This will open the web service.

U won't see much insights initially. So always check the robots.txt page. What I found there was a flag and a list of words file.

I used the file for cracking passwords and username. But I don't know where should I put the credentials in the web.

`sort wordfile.dic | uniq >> new_wordfile.dic` ; this will sort and remove duplicate value from the list and store into new file. We can use this file later. First we need to find the login portal.

Use Nikto web scanner for scanning our web portal. It returned a lot of pages, most of them which I seemed

useful, but was not. I manually navigated to each and found that the portal is using wordpress service. Also got the login page in /wp-admin-login… Lezz go.

Now I can brute force username and password from the list I got from the robots.txt page.

I used hydra for cracking the credentials.
`hydra -vV -L new_wordfile.dic -p wedontcare 192.168.43.12 http-post-form '/wplogin.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'

`

- ***-vV** : Verbose*
- ***-L new_wordfile.dic** : Try all the usernames from the file fsocity.dic.uniq*
- ***-p wedontcare** : Use an unique password, it doesn't matter (we're only interested in the username for now)*
- ***192.168.43.12** : The IP of the machine we're attacking*
- ***http-post-form** : What we're trying to brute force, here a HTTP POST form*
- ***'/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'***
    - ***/wp-login.php** : The path to where the form is located*
    - ***log=^USER^&pwd=^PASS^&wp-submit=Log+In** : The POST parameters to send.*

^USER^ and ^PASS^ are placeholders that wiil be replaced with the actual values.

- ***F=Invalid username** : Consider an attempt as a failure (F) if the response contains the text Invalid username*

We will get username ‘Elliot’. Now password:

`hydra -vV -l elliot -P new_wordfile.dic 192.168.43.12 http-post-form '/wplogin.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=incorrect password'

And we got the password as well. Now login with these credentials to break into the word press dashboard.

Perfect. Now we have login and password, we need to inject plugin into the wordpress with admin shell payload. URL on exploit details: https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_admin_shell_upload/

Use Metasploit for exploitation. Search for ‘wp_admin_shell’ keyword and use it. Provide required options like password, username, target host (rhost). Note: it may get interrupted saying that the host is not using wordpress. So go to the exploit code and comment out the warning.

‘vim /usr/share/metasploit-framework/modules/exploits/unix/webapp/wp_admin_shell_upload.rb’

Now it will run without interruption. We would get a meterpreter session.

Analyse the directories. U may get a key there. Also username for shell login. I got one;

Now open shell session using ‘shell’ and then **`python -c ‘import pty; pty.spawn(“/bin/bash”)’`**

U will get a fully interactive shell. Now login as username u got using `su`. Enter the password (crack the hash first).

Again, go through the file system. U will get another hash.

POST EXPLOITATON

What our main goal is to get root access. But we don’t have now. So, let’s go and find commands with SUID bit set.

SUID (set userID) is a special permission that allows programs/commands to execute with the permission of the file’s owner rather than normal user executing it.

Use `find` command to find programs having SUID bit enabled.

`find / -perm -u=s -type f 2>/dev/null`

From my list, nmap is one of them. Go and check the nmap version and find if there is something to utilize.
Nmap version : 3.81
Option : --interactive (this opens an interactive session)

Use the interactive mode and open shell using `!sh` command. Check `id`. Now try navigation to /root folder.
Done…