Hack The Box Pentesting Machine Writeup: Nibbles (Linux)

By Khedron

It is assumed that the user is working in Kali Linux, or another VM/OS with the necessary tools installed, and that the user's machine is configured with the proper openVPN configuration to use Hackthebox machines.

1. Given the IP of 10.10.10.75, first run an nmap scan: `nmap -A 10.10.10.75 -vv` Option –A will scan for some additional details, such as the OS and version running, and option –vv will increase verbosity of the scan.
2. Running this scan shows that port 80 is open, which is the port that HTTP runs over. Entering `10.10.10.75` into a web browser shows a mostly blank page with only the words "hello world" shown (indicating that we are on the right track). Use the browser's element inspector, page source viewer, or similar feature to see a commented line in the HTML file which reads `<!-- /nibbleblog/ directory. Nothing interesting here! -->`. Quite to the contrary, this is very interesting indeed.
3. Now entering `10.10.10.75/nibbleblog/` into the browser to navigate to the page hinted at in the HTML comment, and a blog page is discovered. Modifying this address to `10.10.10.75/nibbleblog/admin/` will allow you to navigate through a file directory.
4. Enter `10.10.10.75/nibbleblog/admin.php` to find a login page, with a prompt for username and password. Seeing as Nibbles is one of the easiest boxes in the HTB network, these credentials can be guessed with ease; there is no need for any type of brute forcing or more complicated enumeration tools. Use the username `admin` and password `nibbles` to get access to an administrator control panel for the blog.
5. Leaving the web browser, open a terminal and enter `mfsconsole` to launch the Metasploit framework.
6. Enter `search nibble` to look for exploits to use against the nibbleblog hosted on 10.10.10.75. One of the found exploits is `exploit/multi/http/nibbleblog_file_upload`.
7. Enter `use exploit/multi/http/nibbleblog_file_upload` to load this exploit. Enter `options` to see what settings are needed to configure the exploit. A reverse shell is the default payload, which we will leave as it is. To configure, enter the following commands: `set USERNAME admin`, `set PASSWORD nibbles`, `set RHOST 10.10.10.75`, and `set TARGETURI /nibbleblog`.
8. Enter `exploit` to launch the exploit. Note: Any errors that occur are a result of other Hackthebox users changing configurations within the machine. If the exploit doesn't execute successfully, wait just a minute or two and the box will likely be reset, or reset the box yourself from the HTB website and enter `exploit` again.
9. When the exploit finishes running, the reverse shell will be running on the nibbles PC. The first thing to do in this new command prompt is to enter `cd /` to back out of the nibbleblog directory of the machine. Enter `cd /home/nibbler` to navigate to the user folder. Entering `ls` will show a text file called `user.txt`. Enter `cat user.txt` to get the first flag!
10. The root flag is in `/root/root.txt`. In order to open this file, some method of privilege escalation is required, as the root folder is not readable/writable by the user "nibbler". Entering `ls` in the `/home/nibbler` folder shows a file called `personal.zip`. If there also exists a directory called `personal`, there is no need to unzip it; otherwise, enter `shell` to, guess what, enter a shell. Enter `unzip personal.zip` to, right again, unzip the personal.zip file. Now enter `cd /personal/stuff` to move into this new directory.
11. Inside this directory is a file called `monitor.sh`. We will use this file to get the root flag. Notice that this file will run with the privilege of the file's owner, which is root, but is editable by user nibbler. This means that we can treat the `monitor.sh` file as a sort of black box to execute

commands with a higher privilege.

12. Still in a shell, enter `echo cat /root/root.txt > monitor.sh`. This will overwrite the `monitor.sh` file's original code (which displayed some system usage statistics) with `cat /root/root.txt`, which when executed, will print the contents of `root.txt` into the terminal.
13. To ensure the last step worked correctly, enter `cat monitor.sh`. You should see `cat /root/root.txt` in the terminal, being the contents of `monitor.sh`. At this point, enter `sudo ./monitor.sh` to run the file, and the root flag will be printed in the terminal.