Nibbles

Related Academy Modules

- Network Enumeration with Nmap
- Using the Metasploit Framework
- Linux Privilege Escalation
- Attacking Web Applications with Ffuf
- Login Brute Forcing
- Broken Authentication
- Password Attacks
- Introduction to Networking
- Web Requests
- Introduction to Web Applications
- Getting Started
- Linux Fundamentals
- Introduction to Bash Scripting

Nmap Scan

```
nmap -sC -sV -O  -T5 10.10.10.75
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-25 15:49 EDT
Nmap scan report for 10.10.10.75
Host is up (0.032s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.13 - 4.4
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
```

```
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.61 seconds
```

> **Note**
>
> Won't really matter much what we found here. You may be able to get a more reliable connection to the machine with the SSH than me with my reverse shell. That's about it

Ffuf Scan

Navigating to the website, I feel the need to fuzz its files.

```
└─$ ffuf -u http://10.10.10.75/nibbleblog/FUZZ -w
/usr/share/seclists/Discovery/Web-Content/big.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.75/nibbleblog/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-
Content/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

README                  [Status: 200, Size: 4628, Words: 589, Lines: 64,
Duration: 31ms]
.htaccess               [Status: 403, Size: 306, Words: 22, Lines: 12,
Duration: 3257ms]
.htpasswd               [Status: 403, Size: 306, Words: 22, Lines: 12,
Duration: 3257ms]
admin                   [Status: 301, Size: 321, Words: 20, Lines: 10,
Duration: 30ms]
content                 [Status: 301, Size: 323, Words: 20, Lines: 10,
Duration: 40ms]
```

```
languages               [Status: 301, Size: 325, Words: 20, Lines: 10,
Duration: 38ms]
plugins                 [Status: 301, Size: 323, Words: 20, Lines: 10,
Duration: 31ms]
themes                  [Status: 301, Size: 322, Words: 20, Lines: 10,
Duration: 34ms]
:: Progress: [20478/20478] :: Job [1/1] :: 913 req/sec :: Duration:
[0:00:22] :: Errors: 0 ::
```

Pretty interesting traversable directories here. Not much to find, some guessing got me the admin password on `admin.php`.

CVE-2015-6967

There's of course a well-known exploit also available in metasploit. We got a shell from CVE-2015-6967 and the known credentials, so we can easily find the user flag now, before beating our head with escalating privileges.

Root Flag

Turns out, the most important thing I learned from this machine is if that a user can run */home/nibbler/personal/stuff/monitor.sh* as root without supplying a password that doesn't mean that he can run from the *stuff* directory just *monitor.sh* without a password.

Here I was messing up for some time from a not upgraded shell making typos every second command because I just couldn't figure out why do I still have to supply a password to run *monitor.sh* if I can run */home/nibbler/personal/stuff/monitor.sh*. It's because I need to run the whole path to the file...

Anyway, after figuring out stuff like this, I feel both a sense of achievement and some defeat, but I still learned! So I just wrote `echo "cat /root/root.txt"` in the *monitor.sh* file and ran it as sudo.

Goodbye!