Lab 1 - Enumeration and Information Leakage

Updated: 2023-09-29.

Introduction to the lab

Learning outcomes

- Enumeration of servers using NMAP and other tools.
- Identify possible attack vectors.

Submission

This is an individual assignment. You may submit as you go but be sure to complete and submit all activities up to 48 hours after the class.
We strongly recommend submitting the work at the end of the class as it is, and then, improving it.

2.1 HTB Machines

In this assessment, you will enumerate as much information as possible from ALL the following HTB Machines:

- Format
- PC
- Jupiter
- Pilgrimage
- SAU
- Authority
- Gofer
- CozyHosting
- Clicker

You do not need to get into the machine. The goal is to enumerate information for future use. But if you want, feel free to hack them.

2.2 Machine: Format

This section presents a possible approach for machine Format. However, you may follow a different strategy. The following steps may help you to reveal some hiding information in this machine.

a) Use NMAP to identify possible ports and services available.

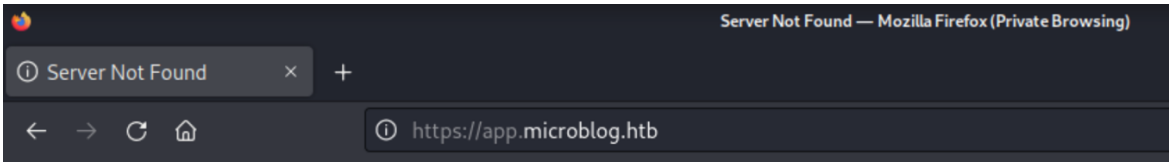
```
└─$ nmap -sV 10.10.11.213
Starting Nmap 7.91 ( https://nmap.org ) at 2023-09-29 00:57 BST
Nmap scan report for 10.10.11.213
Host is up (0.16s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp   open  http    nginx 1.18.0
3000/tcp open  http    nginx 1.18.0
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 32.83 seconds
```

b) Trying to reach the HTTP application existent in such ports.

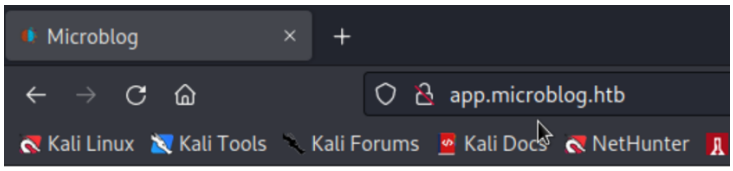
   a. 10.10.11.213:80

   b. 10.10.11.213:3000

If it does not work, you may need to configure the server IP hosting for a specific domain.




```
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali.kali       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.11.213    app.microblog.htb
```



Microblog
Don't complicate it,
keep it micro

Let Microblog bring your stories to life
completely **free of charge** in minutes

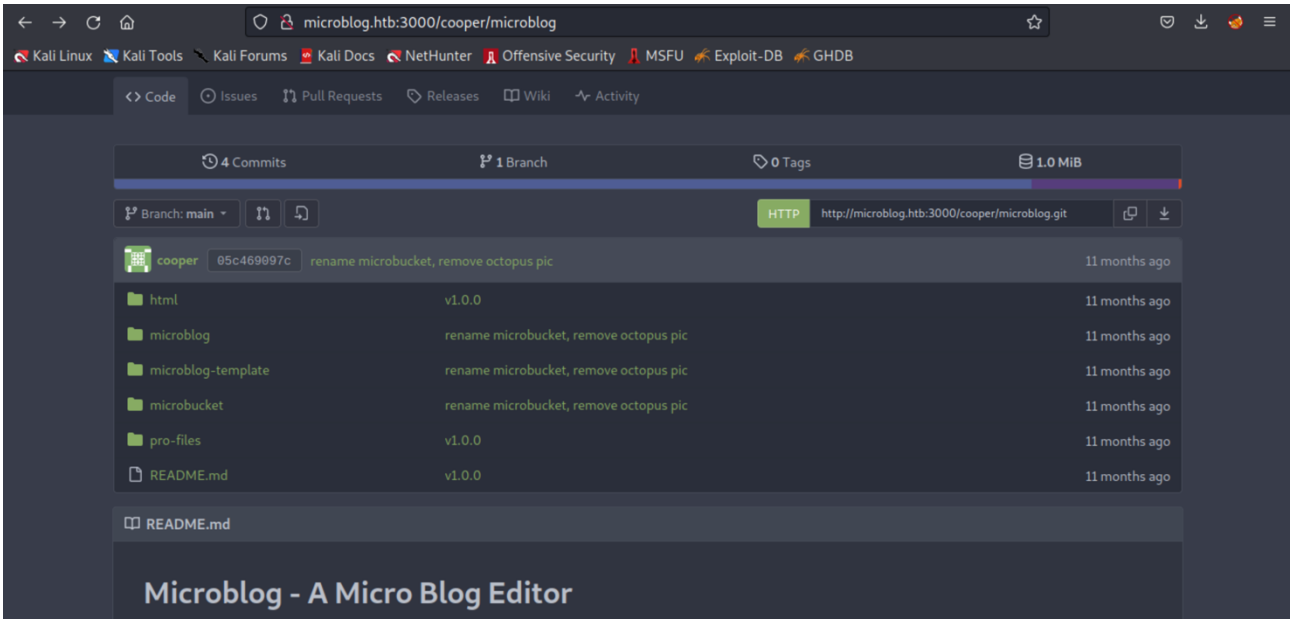
Get Blogging

c) Document these findings (for both ports).

d) Now use wfuzz to enumerate subdomains. This tool can also be used to enumerate paths using a domain as a base.

```
└─$ wfuzz -w /usr/share/wordlists/dirb/common.txt -u  http://microblog.htb -H "Host: FUZZ.microblog.htb" --sc 200
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz mi
 fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://microblog.htb/
Total requests: 4614

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        8 L      13 W       135 Ch      "http://microblog.htb/"
000000432:   200        83 L     306 W      3973 Ch     "app"

Total time: 0
Processed Requests: 4614
Filtered Requests: 4612
Requests/sec.: 0
```

e) By playing with the menus, we can find that there is an open repository for this application, that may help us to find possible issues.



f) Check some banners in the HTTP requests.