nmap
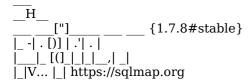
Starting Nmap 7.94 (https://nmap.org) at 2023-11-09 12:12 IST
Nmap scan report for 10.10.231.237
Host is up (0.15s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
80/tcp open http nginx 1.10.3 (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Welcome to nginx!
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 34.54 seconds

[{'port': '80', 'service': 'http', 'version': 'nginx 1.10.3 (Ubuntu)'}]

gobuster

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url: http://10.10.231.237/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/kali/Desktop/capstone-pentesting-tools/tools/wordlists/directory.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================

[2K/blood (Status: 301) [Size: 194] [--> http://10.10.231.237/blood/]
===============================================================
Finished
===============================================================
```

['http://10.10.231.237/blood']

gospider

[url] - [code-200] - http://10.10.231.237/blood/
[form] - http://10.10.231.237/blood/
[javascript] - http://10.10.231.237/blood/js/jquery.min.js
[javascript] - http://10.10.231.237/blood/js/bootstrap.min.js
[url] - [code-200] - http://10.10.231.237/blood/register.php
[form] - http://10.10.231.237/blood/register.php
[url] - [code-200] - http://10.10.231.237/
[url] - [code-200] - http://10.10.231.237/blood/login.php
[url] - [code-200] - http://10.10.231.237/blood/index.php
[form] - http://10.10.231.237/blood/index.php
[form] - http://10.10.231.237/blood/login.php
[url] - [code-200] - http://10.10.231.237/blood/tos.php
[linkfinder] - [from: http://10.10.231.237/blood/js/jquery.min.js] - text/xml
[linkfinder] - [from: http://10.10.231.237/blood/js/jquery.min.js] - text/plain
[linkfinder] - [from: http://10.10.231.237/blood/js/jquery.min.js] - text/html
[linkfinder] - [from: http://10.10.231.237/blood/js/jquery.min.js] - application/x-www-form-urlencoded
[linkfinder] - [from: http://10.10.231.237/blood/js/jquery.js] - text/xml
[linkfinder] - [from: http://10.10.231.237/blood/js/jquery.js] - text/plain
[linkfinder] - [from: http://10.10.231.237/blood/js/jquery.js] - text/html
[linkfinder] - [from: http://10.10.231.237/blood/js/jquery.js] - application/x-www-form-urlencoded

['http://10.10.231.237/blood/', 'http://10.10.231.237/blood/js/jquery.min.js',
'http://10.10.231.237/blood/js/bootstrap.min.js', 'http://10.10.231.237/blood/register.php', 'http://10.10.231.237/',
'http://10.10.231.237/blood/login.php', 'http://10.10.231.237/blood/index.php', 'http://10.10.231.237/blood/tos.php']

sqlmap

```
     ___
    __H__
 ___ ___["]_____ ___ ___  {1.7.8#stable}
|_ -| . [)]   | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...  |_|   https://sqlmap.org
```

[*] starting @ 12:14:00 /2023-11-09/

do you want to check for the existence of site's sitemap(.xml) [y/N] N
please enter number of threads? [Enter for 1 (current)] 1
please enter number of threads? [Enter for 1 (current)] 1

[*] ending @ 12:14:05 /2023-11-09/

{'dbms': '"[INFO] the back-end DBMS is \'MySQL\'"', 'database': [{'dbname': '[]', 'tables': []}]}