```
Target:
natas2.natas.labs.overthewire.org

Running Nmap scan...
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-11 02:36 UTC
NSE: Loaded 49 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:36
Completed NSE at 02:36, 0.00s elapsed
Initiating NSE at 02:36
Completed NSE at 02:36, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 02:36
Completed Parallel DNS resolution of 1 host. at 02:36, 0.12s elapsed
Initiating SYN Stealth Scan at 02:36
Scanning natas2.natas.labs.overthewire.org (16.170.58.40) [1000 ports]
Discovered open port 8080/tcp on 16.170.58.40
Discovered open port 443/tcp on 16.170.58.40
Discovered open port 80/tcp on 16.170.58.40
Discovered open port 22/tcp on 16.170.58.40
Discovered open port 5060/tcp on 16.170.58.40
Completed SYN Stealth Scan at 02:36, 5.32s elapsed (1000 total ports)
Initiating Service scan at 02:36
Scanning 5 services on natas2.natas.labs.overthewire.org (16.170.58.40)
Service scan Timing: About 60.00% done; ETC: 02:41 (0:01:44 remaining)
Completed Service scan at 02:39, 166.58s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against natas2.natas.labs.overthewire.org (16.170.58.40)
Retrying OS detection (try #2) against natas2.natas.labs.overthewire.org (16.170.58.40)
Initiating Traceroute at 02:39
Completed Traceroute at 02:39, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 02:39
Completed Parallel DNS resolution of 2 hosts. at 02:39, 0.00s elapsed
NSE: Script scanning 16.170.58.40.
Initiating NSE at 02:39
Completed NSE at 02:40, 69.25s elapsed
Initiating NSE at 02:40
Completed NSE at 02:41, 8.12s elapsed
Nmap scan report for natas2.natas.labs.overthewire.org (16.170.58.40)
Host is up (0.0043s latency).
rDNS record for 16.170.58.40: ec2-16-170-58-40.eu-north-1.compute.amazonaws.com
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 8.9p1 (protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
| vulners:
|   cpe:/a:apache:http_server:2.4.52:
|       CVE-2022-31813  7.5     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  7.5     https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  7.5     https://vulners.com/cve/CVE-2022-22720
|       CNVD-2022-73123 7.5     https://vulners.com/cnvd/CNVD-2022-73123
|       CVE-2022-28615  6.4     https://vulners.com/cve/CVE-2022-28615
|       CVE-2021-44224  6.4     https://vulners.com/cve/CVE-2021-44224
|       CVE-2022-22721  5.8     https://vulners.com/cve/CVE-2022-22721
|       CVE-2022-30556  5.0     https://vulners.com/cve/CVE-2022-30556
|       CVE-2022-29404  5.0     https://vulners.com/cve/CVE-2022-29404
|       CVE-2022-28614  5.0     https://vulners.com/cve/CVE-2022-28614
|       CVE-2022-26377  5.0     https://vulners.com/cve/CVE-2022-26377
|       CVE-2022-22719  5.0     https://vulners.com/cve/CVE-2022-22719
|       CNVD-2022-73122 5.0     https://vulners.com/cnvd/CNVD-2022-73122
|       CNVD-2022-53584 5.0     https://vulners.com/cnvd/CNVD-2022-53584
|       CNVD-2022-53582 5.0     https://vulners.com/cnvd/CNVD-2022-53582
|       CVE-2023-27522  0.0     https://vulners.com/cve/CVE-2023-27522
|       CVE-2023-25690  0.0     https://vulners.com/cve/CVE-2023-25690
|       CVE-2022-37436  0.0     https://vulners.com/cve/CVE-2022-37436
|       CVE-2022-36760  0.0     https://vulners.com/cve/CVE-2022-36760
```

```
|_      CVE-2006-20001  0.0     https://vulners.com/cve/CVE-2006-20001
443/tcp  open  https?
5060/tcp open  sip?
8080/tcp open  http-proxy?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 3.10 (93%), Linux 3.10 - 4.11 (93%), Linux 3.2
- 4.9 (93%), Linux 3.4 - 3.10 (93%), Linux 4.15 - 5.6 (93%), Linux 5.1 (93%), Linux 2.6.32 -
3.10 (92%), Linux 2.6.32 - 3.13 (92%), Linux 5.0 - 5.4 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 28.929 days (since Mon Mar 13 04:23:56 2023)
Network Distance: 3 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 8080/tcp)
HOP RTT     ADDRESS
1   0.13 ms 10.11.0.1
2   0.21 ms 172.20.0.254
3   0.72 ms ec2-16-170-58-40.eu-north-1.compute.amazonaws.com (16.170.58.40)

NSE: Script Post-scanning.
Initiating NSE at 02:41
Completed NSE at 02:41, 0.00s elapsed
Initiating NSE at 02:41
Completed NSE at 02:41, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 255.91 seconds
           Raw packets sent: 2108 (98.032KB) | Rcvd: 56 (2.848KB)

Running Nikto scan...
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          16.170.58.40
+ Target Hostname:    natas2.natas.labs.overthewire.org
+ Target Port:        80
+ Start Time:         2023-04-11 02:41:03 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.52 (Ubuntu)
+ 239 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time:           2023-04-11 02:41:37 (GMT0) (34 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

Running Wig scan...

wig - WebApp Information Gatherer


Scanning http://natas2.natas.labs.overthewire.org...
Loaded cache from: http..natas2.natas.labs.overthewire.org_-_1681180539.cache
Getting title ...
Error page detection ...
Determining CMS type ...
Detecting platform ...
Detecting interesting files ...
Detecting links ...
Detecting Javascript ...
Matching urlless fingerprints...
Checking for cookies ...
Detecting OS ...
Searching for sub domains ...
Searching for tools ...
Searching for vulnerabilities ...
```

```
Saved cache to: ./cache/http..natas2.natas.labs.overthewire.org_-_1681180539.cache
_________________ SITE INFO _________________
IP             Title
16.170.58.40   401 Unauthorized

_________________ VERSION _________________
Name           Versions   Type
Apache         2.4.52     Platform


_____________________________________________
Time: 2.6 sec  Urls: 599  Fingerprints: 39241

Running WhatWeb scan...
WhatWeb report for http://natas2.natas.labs.overthewire.org
Status    : 401 Unauthorized
Title     : 401 Unauthorized
IP        : 16.170.58.40
Country   : UNITED STATES, US

Summary   : Apache[2.4.52], HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], WWW-
Authenticate[Authentication required][Basic]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.4.52 (from HTTP Server Header)
        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Ubuntu Linux
        String       : Apache/2.4.52 (Ubuntu) (from server string)

[ WWW-Authenticate ]
        This plugin identifies the WWW-Authenticate HTTP header and
        extracts the authentication method and realm.

        Module       : Basic
        String       : Authentication required

HTTP Headers:
        HTTP/1.1 401 Unauthorized
        Date: Tue, 11 Apr 2023 02:41:51 GMT
        Server: Apache/2.4.52 (Ubuntu)
        WWW-Authenticate: Basic realm="Authentication required"
        Content-Length: 480
        Connection: close
        Content-Type: text/html; charset=iso-8859-1

DONE
```