

EnumeRannden Report

Information Panel

IP: 1.1.1.1

Host's Operating System: Linux --> TTL=54

Open Ports: 53 80 443 8080

Main Directory: test

NMAP Results

File: test/enum/nmap_open_ports.txt

```
# Nmap 7.94SVN scan initiated Thu Jun 27 06:12:36 2024 as: nmap -p- --open --min-rate 5000 -Pn -oN test/enum/nmap_open_ports.txt 1.1.1.1
Nmap scan report for one.one.one.one (1.1.1.1)
Host is up (0.040s latency).
Not shown: 65385 filtered tcp ports (no-response), 146 filtered tcp ports (host-unreach)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy

# Nmap done at Thu Jun 27 06:13:03 2024 -- 1 IP address (1 host up) scanned in 26.48 seconds
```

WhatWeb Results

File: test/enum/whatweb_80.txt

```
[1m[34mhttp://1.1.1.1:80[0m [301 Moved Permanently] [1mCountry[0m[[0m[22mAUSTRALIA[0m][[1m[31mAU[0m], [1mHTTPServer[0m[[1m[36mcloudflare[0m], [1mIP[0m[[0m[22m1.1.1.1[0m], [1mRedirectLocation[0m[[0m[22mht
[1m[34mhttps://1.1.1.1/[0m [302 Found] [1mCountry[0m[[0m[22mAUSTRALIA[0m][[1m[31mAU[0m], [1mHTTPServer[0m[[1m[36mcloudflare[0m], [1mIP[0m[[0m[22m1.1.1.1[0m], [1mRedirectLocation[0m[[0m[22mhttps://one.one
[1m[34mhttps://one.one.one.one/[0m [200 OK] [1mCountry[0m[[0m[22mAUSTRALIA[0m][[1m[31mAU[0m], [1mHTML5[0m], [1mHTTPServer[0m[[1m[36mcloudflare[0m], [1mIP[0m[[0m[22m1.0.0.1[0m], [1mMeta-Author[0m[[0m[22m1.
```

Nikto Results

File: test/enum/nikto_80.txt

```
- Nikto v2.5.0
-----
+ Target IP:      1.1.1.1
+ Target Hostname: 1.1.1.1
+ Target Port:    80
+ Start Time:     2024-06-27 06:59:14 (GMT-4)
-----
+ Server: cloudflare
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerabi
+ Root page / redirects to: https://1.1.1.1/
```

Gobuster Results

File: test/enum/gobuster.txt

Hash Cracking Results

File: test/loot/cracked_hash1.txt

5ebe2294ecd0e0f08eab7690d2a6ee69:secret

Payloads Generated

File: test/exploits/pwned.elf

File: test/exploits/searchsploit_results_mouse.txt

File: test/exploits/shell.sh

OSINT Results

File: test/osint/theharvester_anubis_06-27-06:58.json

```
{"hosts":[],"shodan":[]}
```

File: test/osint/theharvester_anubis_06-27-06:58.xml