```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-28 09:15 UTC
NSE: Loaded 296 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:15
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.a
NSE: [mtrace] A source IP must be provided through fromip argument.
Completed NSE at 09:15, 11.53s elapsed
Initiating NSE at 09:15
Completed NSE at 09:15, 0.00s elapsed
Initiating NSE at 09:15
Completed NSE at 09:15, 0.00s elapsed
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API.
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See htt
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Initiating ARP Ping Scan at 09:15
Scanning 10.0.2.11 [1 port]
Completed ARP Ping Scan at 09:15, 0.31s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 09:15
Scanning potato (10.0.2.11) [65535 ports]
Discovered open port 80/tcp on 10.0.2.11
Discovered open port 22/tcp on 10.0.2.11
Discovered open port 2112/tcp on 10.0.2.11
Completed SYN Stealth Scan at 09:15, 5.09s elapsed (65535 total ports)
Initiating Service scan at 09:15
Scanning 3 services on potato (10.0.2.11)
Completed Service scan at 09:15, 11.03s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against potato (10.0.2.11)
NSE: Script scanning 10.0.2.11.
Initiating NSE at 09:15
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command
Completed NSE at 09:15, 17.98s elapsed
Initiating NSE at 09:15
Completed NSE at 09:15, 0.24s elapsed
Initiating NSE at 09:15
Completed NSE at 09:15, 0.01s elapsed
Nmap scan report for potato (10.0.2.11)
Host is up (0.00050s latency).
Not shown: 65532 closed tcp ports (reset)
Bug in http-security-headers: no string output.
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2
| ssh2-enum-algos:
|   kex_algorithms: (9)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|   server_host_key_algorithms: (5)
|       rsa-sha2-512
```

```
|       rsa-sha2-256
|       ssh-rsa
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
|_banner: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
| ssh-hostkey:
|   3072 ef:24:0e:ab:d2:b3:16:b4:4b:2e:27:c0:5f:48:79:8b (RSA)
|   256 f2:d8:35:3f:49:59:85:85:07:e6:a2:0e:65:7a:8c:4b (ECDSA)
|_  256 0b:23:89:c3:c0:26:d5:64:5e:93:b7:ba:f5:14:7f:3e (ED25519)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-headers:
|   Date: Fri, 28 Jun 2024 09:15:43 GMT
|   Server: Apache/2.4.41 (Ubuntu)
|   Connection: close
|   Content-Type: text/html; charset=UTF-8
|
|_  (Request type: HEAD)
| http-traceroute:
|_  Possible reverse proxy detected.
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-date: Fri, 28 Jun 2024 09:15:44 GMT; 0s from local time.
| http-xssed:
|
|     UNFIXED XSS vuln.
|
|       http://de.forum.gpotato.eu/Common/Aspx/ImageUpload/ImageUploadType1.asp?
|
|       http://de.flyff.gpotato.eu/Forum/Common/Aspx/ErrMsg.aspx?STYPE=DB&amp;ER
|
|       http://register.gpotato.com/?m=Register&amp;a=Registration
|
|_
|_http-title: Potato company
```

```
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-comments-displayer: Couldn't find any comments.
|_http-mobileversion-checker: No mobile version detected.
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
2112/tcp open  ftp     ProFTPD
|_banner: 220 ProFTPD Server (Debian) [::ffff:10.0.2.11]
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--   1 ftp      ftp           901 Aug  2  2020 index.php.bak
|_-rw-r--r--   1 ftp      ftp            54 Aug  2  2020 welcome.msg
MAC Address: 08:00:27:9B:68:59 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 6.679 days (since Fri Jun 21 16:57:50 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| qscan:
| PORT  FAMILY  MEAN (us)  STDDEV  LOSS (%)
| 1     0       531.90     50.60   0.0%
| 22    0       614.70     259.99  0.0%
| 80    0       499.20     93.63   0.0%
|_2112  0       618.40     244.91  0.0%
|_ipidseq: ERROR: Script execution failed (use -d to debug)
| traceroute-geolocation:
|   HOP  RTT   ADDRESS             GEOLOCATION
|_  1    0.50  potato (10.0.2.11)  - ,-
|_path-mtu: PMTU == 1500
|_fcrdns: FAIL (No PTR record)

TRACEROUTE
HOP RTT     ADDRESS
1   0.50 ms potato (10.0.2.11)
```

```
NSE: Script Post-scanning.
Initiating NSE at 09:16
Completed NSE at 09:16, 0.00s elapsed
Initiating NSE at 09:16
Completed NSE at 09:16, 0.00s elapsed
Initiating NSE at 09:16
Completed NSE at 09:16, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https
Nmap done: 1 IP address (1 host up) scanned in 50.88 seconds
           Raw packets sent: 65600 (2.889MB) | Rcvd: 65551 (2.623MB)
```