

```
# Nmap 7.95 scan initiated Wed Feb 19 22:17:30 2025 as: /usr/lib/nmap/nmap
--privileged -A -sC -sV -O -T4 -Pn -iL domains.txt -oN script_os_all_results.txt
Nmap scan report for xytify.net (89.233.104.66)
Host is up.
rDNS record for 89.233.104.66: 89-233-104-66.static.hvvc.us
All 1000 scanned ports on xytify.net (89.233.104.66) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details
```

```
TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
-   Hops 1-9 are the same as for 66.96.84.22
10  ...
11  157.35 ms 193.82.22.198
12  ... 30
```

```
=====
=====

Nmap scan report for au.xytify.net (45.32.241.230)
Host is up (0.23s latency).
Other addresses for au.xytify.net (not scanned):
2001:19f0:5800:8bf9:5400:ff:fe24:b8cb
rDNS record for 45.32.241.230: au.trez.space
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 34:44:b6:28:e1:c5:70:13:cb:6e:fc:fa:e4:3f:b8:4a (RSA)
|   256 2c:10:50:3a:4b:b2:2c:8b:ab:8f:dd:40:ec:2b:c2:8f (ECDSA)
|_  256 bb:cb:0c:f9:48:7e:3f:ab:e5:fe:a9:1d:3b:19:e8:70 (ED25519)
25/tcp    closed smtp
80/tcp    closed http
443/tcp   closed https
465/tcp   closed smtps
587/tcp   closed submission
993/tcp   closed imaps
1723/tcp  open  pptp         linux (Firmware: 1)
Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 5.1 - 5.15 (96%), Linux 3.2 -
4.14 (94%), Linux 3.13 - 4.4 (94%), Linux 4.10 (94%), Linux 3.10 (93%), Linux 4.4
(93%), Linux 3.16 - 4.6 (92%), OpenWrt 19.07 (Linux 4.14) (92%), Linux 2.6.32 -
3.13 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 25 hops
Service Info: Host: local
```

```
TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
```

```

- Hops 1-6 are the same as for 66.96.84.22
7 21.63 ms lag-414-10.dllstx976iw-bcr00.netops.charter.com (66.109.6.52)
8 16.85 ms lag-0.pr3.dfw10.netops.charter.com (66.109.5.121)
9 ...
10 50.76 ms ae3.cs2.dfw2.us.zip.zayo.com (64.125.26.204)
11 48.09 ms ae12.cs2.lax112.us.zip.zayo.com (64.125.26.183)
12 ...
13 50.56 ms 64.124.151.5.IPYX-284545-900-ZY0.zip.zayo.com (64.124.151.5)
14 49.23 ms i-95.1wlt-core02.telstraglobal.net (202.84.143.29)
15 181.90 ms i-95.1wlt-core02.telstraglobal.net (202.84.143.29)
16 190.05 ms i-10406.sydo-core04.telstraglobal.net (202.84.141.226)
17 191.21 ms bundle-ether4.oxf-gw30.sydney.telstra.net (203.50.13.93)
18 217.00 ms bundle-ether1.oxf-gw31.sydney.telstra.net (203.50.6.101)
19 233.85 ms bundle-ether5.stl-core30.sydney.telstra.net (203.50.6.117)
20 190.82 ms ae0.alx-edge421.sydney.telstra.net (203.50.12.133)
21 238.02 ms twi4278618.lnk.telstra.net (138.217.181.66)
22 ... 24
25 229.88 ms au.trez.space (45.32.241.230)

```

```

=====
=====

```

```

Nmap scan report for jp.xytify.net (66.96.84.22)
Host is up (0.16s latency).
Other addresses for jp.xytify.net (not scanned): 2602:ff16:8:0:1:d1:0:1
rDNS record for 66.96.84.22: 66-96-84-22.static.hvvc.us
Not shown: 990 closed tcp ports (reset)
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 62:d9:f7:f5:fd:22:74:57:7c:d2:ba:6a:49:d0:80:1a (RSA)
|   256 6e:df:6d:7a:8a:02:a1:5f:82:f8:a5:a8:8f:3e:5f:26 (ECDSA)
|_  256 d0:fa:c3:02:4e:04:2d:d1:d2:1e:e5:8f:f6:8d:a8:fd (ED25519)
25/tcp    open      smtp         Postfix smtpd
|_smtp-commands: jp.xytify.net, PIPELINING, SIZE 10240000, VRFY, ETRN,
ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp    open      http         Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
|_http-title: Did not follow redirect to https://jp.xytify.net/
111/tcp   open      rpcbind      2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000   2,3,4        111/tcp     rpcbind
|   100000   2,3,4        111/udp     rpcbind
|   100000   3,4          111/tcp6    rpcbind
|_  100000   3,4          111/udp6    rpcbind
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn

```

```
443/tcp open      ssl/http      Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
|_ssl-cert: Subject: commonName=jp.xytify.net
|_Subject Alternative Name: DNS:jp.xytify.net
|_Not valid before: 2024-08-21T14:43:19
|_Not valid after: 2024-11-19T14:43:18
|_http-methods:
|_Potentially risky methods: TRACE
445/tcp filtered microsoft-ds
593/tcp filtered http-rpc-epmap
3306/tcp open      mysql        MariaDB 10.3.23 or earlier (unauthorized)
Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 5.1 - 5.15 (96%), Linux 3.2 -
4.14 (94%), Linux 3.13 - 4.4 (94%), Linux 4.10 (94%), Linux 3.10 (93%), Linux 4.4
(93%), Linux 3.16 - 4.6 (92%), OpenWrt 19.07 (Linux 4.14) (92%), Linux 2.6.32 -
3.13 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 12 hops
Service Info: Host:  jp.xytify.net
```

TRACEROUTE (using port 5900/tcp)

HOP	RTT	ADDRESS
1	1.91 ms	192.168.1.1
2	7.27 ms	syn-070-120-064-001.res.spectrum.com (70.120.64.1)
3	...	
4	16.33 ms	lag-64.snantxvy02r.netops.charter.com (24.175.33.244)
5	26.06 ms	lag-11.mcr11snantxvy.netops.charter.com (24.175.32.210)
6	34.68 ms	lag-23.rcr01dllatx37.netops.charter.com (24.175.32.146)
7	22.25 ms	lag-24-10.dllstx976iw-bcr00.netops.charter.com (66.109.1.216)
8	30.77 ms	lag-302.pr3.dfw10.netops.charter.com (209.18.43.77)
9	25.07 ms	8220-da6-ix.equinix.com (206.223.118.241)
10	...	11
12	154.55 ms	66-96-84-22.static.hvvc.us (66.96.84.22)

```
=====
=====
```

Nmap scan report for za.xytify.net (102.214.11.124)

Host is up.  
rDNS record for 102.214.11.124: 102-214-11-124.zadns.co.za  
All 1000 scanned ports on za.xytify.net (102.214.11.124) are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)

HOP	RTT	ADDRESS
-		Hops 1-8 are the same as for 186.64.123.161
9	138.24 ms	ae1.3505.edge4.mrs1.neo.colt.net (171.75.8.243)

```
10 139.10 ms SEACOM.edge4.Marseille1.Level3.net (212.133.4.70)
11 325.49 ms ae-0.cr-01-mrs.fr.seacomnet.com (105.16.32.1)
12 292.80 ms ce-0-1-7.cr-01-cpt.za.seacomnet.com (105.16.9.201)
13 306.27 ms et-0-1-4-cr-01-jnb.za.seacomnet.com (105.25.161.113)
14 288.86 ms xe-2-0-1.er-06-jnb.za.seacomnet.com (105.16.13.246)
15 271.01 ms 105.25.136.70
16 ... 30
```

```
=====
=====
```

Nmap scan report for cl.xytify.net (186.64.123.161)

Host is up (0.16s latency).

Not shown: 990 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 7.4 (protocol 2.0)
--------	------	-----	----------------------------

| ssh-hostkey:

| 2048 1b:9d:57:eb:0a:05:b7:d5:c6:f7:ac:55:45:ab:62:65 (RSA)

| 256 b4:00:89:8c:cd:7a:fd:be:a0:1e:9a:cc:1a:58:55:47 (ECDSA)

|\_ 256 99:22:4e:08:75:0c:36:7b:46:22:53:e7:b1:ca:a1:80 (ED25519)

25/tcp	open	smtp	Postfix smtpd
--------	------	------	---------------

|\_smtp-commands: cl.xytify.net, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN

80/tcp	open	http	Apache httpd 2.4.6 ((CentOS))
--------	------	------	-------------------------------

|\_http-server-header: Apache/2.4.6 (CentOS)

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-title: Site doesn't have a title (text/html; charset=UTF-8).

135/tcp	filtered	msrpc	
---------	----------	-------	--

139/tcp	filtered	netbios-ssn	
---------	----------	-------------	--

143/tcp	open	imap	Dovecot imapd
---------	------	------	---------------

|\_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=imap.example.com

| Not valid before: 2023-02-28T17:53:35

|\_Not valid after: 2024-02-28T17:53:35

|\_imap-capabilities: ENABLE LOGIN-REFERRALS Pre-login OK have IMAP4rev1 LITERAL+ LOGINDISABLEDA0001 ID SASL-IR IDLE listed capabilities STARTTLS more post-login

445/tcp	filtered	microsoft-ds	
---------	----------	--------------	--

587/tcp	open	smtp	Postfix smtpd
---------	------	------	---------------

|\_smtp-commands: cl.xytify.net, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

593/tcp	filtered	http-rpc-epmap	
---------	----------	----------------	--

993/tcp	open	ssl/imap	Dovecot imapd
---------	------	----------	---------------

| ssl-cert: Subject: commonName=imap.example.com

| Not valid before: 2023-02-28T17:53:35

|\_Not valid after: 2024-02-28T17:53:35

|\_imap-capabilities: ENABLE LOGIN-REFERRALS Pre-login more IMAP4rev1 LITERAL+ have ID SASL-IR IDLE listed capabilities OK AUTH=PLAINA0001 post-login

|\_ssl-date: TLS randomness does not represent time  
Aggressive OS guesses: Linux 3.10 - 4.11 (98%), Linux 5.1 - 5.15 (96%), Linux 3.2 - 4.14 (94%), Linux 3.13 - 4.4 (94%), Linux 4.10 (94%), Linux 4.4 (94%), Linux 3.10 (92%), Linux 3.16 - 4.6 (92%), OpenWrt 19.07 (Linux 4.14) (92%), Linux 2.6.32 - 3.13 (91%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 13 hops  
Service Info: Host: cl.xytify.net

TRACEROUTE (using port 5900/tcp)

HOP	RTT	ADDRESS
-		Hops 1-7 are the same as for 66.96.84.22
8	19.35 ms	ae19.edge1.dal2.sp.lumen.tech (4.68.38.57)
9	147.29 ms	ae2.3601.edge1.sgo1.ciriontechnologies.net (200.189.207.6)
10	154.54 ms	8.243.191.134
11	...	12
13	160.24 ms	186.64.123.161

=====

Nmap scan report for uk.xytify.net (37.220.0.40)

Host is up (0.13s latency).

rDNS record for 37.220.0.40: toms-reward.leapplex.com

Not shown: 994 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.4 (protocol 2.0)

| ssh-hostkey:

| 2048 e5:c2:0a:77:df:43:bb:78:04:bb:64:2e:7d:cf:cf:40 (RSA)

| 256 e2:d8:52:19:62:cc:26:fa:23:20:9d:7a:39:45:bc:a9 (ECDSA)

|\_ 256 6c:93:76:c6:b1:25:96:07:a9:e1:1f:d1:4f:eb:50:ac (ED25519)

80/tcp	open	http	Apache httpd 2.4.6 ((CentOS))
--------	------	------	-------------------------------

|\_http-title: HomeSecure Pro 360

|\_http-server-header: Apache/2.4.6 (CentOS)

| http-methods:

|\_ Potentially risky methods: TRACE

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

445/tcp filtered microsoft-ds

593/tcp filtered http-rpc-epmap

Aggressive OS guesses: Linux 3.2 - 4.14 (94%), Linux 3.10 - 4.11 (93%), Linux 3.10 (92%), Linux 2.6.32 - 3.13 (91%), Linux 5.1 - 5.15 (91%), OpenWrt 19.07 (Linux 4.14) (90%), Linux 3.13 - 4.4 (89%), Linux 4.10 (89%), Linux 4.5 (89%), Linux 5.10 - 5.13 (89%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 22 hops

TRACEROUTE (using port 5900/tcp)

HOP	RTT	ADDRESS
-	Hops 1-8 are the same as for 66.96.84.22	
9	...	11
12	121.65 ms	ae13.cr1.atl10.us.zip.zayo.com (64.125.23.251)
13	124.22 ms	ae10.cr1.iad21.us.zip.zayo.com (64.125.25.132)
14	...	15
16	128.80 ms	ae5.cr1.lhr11.uk.eth.zayo.com (64.125.29.127)
17	123.32 ms	ae9.mpr1.lhr23.uk.zip.zayo.com (64.125.28.3)
18	132.04 ms	94.31.48.82.IPYX-107159-900-ZY0.zip.zayo.com (94.31.48.82)
19	131.39 ms	po200.dc9core2.as20860.net (62.128.205.130)
20	138.66 ms	1046.zone.6.r.dc10.redstation.co.uk (185.20.96.174)
21	127.11 ms	190-61-84-80.rackcentre.redstation.net.uk (80.84.61.190)
22	120.48 ms	toms-reward.leapplex.com (37.220.0.40)

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

# Nmap done at Wed Feb 19 22:19:41 2025 -- 6 IP addresses (6 hosts up) scanned in 131.39 seconds