Nmap Aggressive Scan Report

Scan Initiated By: **sample**

Timestamp: 2025-04-22 14:41:29

Target: zonetransfer.me

```
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-22 14:40 IST
Nmap scan report for zonetransfer.me (5.196.105.14)
Host is up (0.16s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE VERSION
25/tcp open smtp
| fingerprint-strings:
| GenericLines:
| 220 eig-obgw-6006a.ext.cloudfilter.net cmsmtp ESMTP server ready
| command unrecognized
| command unrecognized
| GetRequest:
| 220 eig-obgw-6007a.ext.cloudfilter.net cmsmtp ESMTP server ready
| command unrecognized
| command unrecognized
| Hello:
| 220 eig-obgw-6009a.ext.cloudfilter.net cmsmtp ESMTP server ready
| EHLO requires valid address
```

| Help:

| 220 eig-obgw-6002a.ext.cloudfilter.net cmsmtp ESMTP server ready

| command unrecognized

| NULL:

|_ 220 eig-obgw-6009a.ext.cloudfilter.net cmsmtp ESMTP server ready

|_smtp-commands: eig-obgw-6002a.ext.cloudfilter.net hello [216.10.242.35], pleased to meet you, AUTH LOGIN PLAIN, SIZE 30000000, 8BITMIME, STARTTLS, OK

|_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=*.smtp.a.cloudfilter.net/organizationName=Proofpoint, Inc./stateOrProvinceName=California/countryName=US

| Subject Alternative Name: DNS:*.smtp.a.cloudfilter.net

| Not valid before: 2024-07-24T00:00:00

|_Not valid after: 2025-07-24T23:59:59

80/tcp open http Apache httpd (Sparkles)

|_http-title: Did not follow redirect to https://zonetransfer.me/

|_http-server-header: Apache

81/tcp open http Apache httpd

|_http-title: 404 Not Found

|_http-server-header: Apache

443/tcp open ssl/http Apache httpd (Rainbows and XSSalert(1))

|_http-title: Did not follow redirect to https://digi.ninja/projects/zonetransferme.php

|_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=alertlab.digi.ninja

| Subject Alternative Name: DNS:alertlab.digi.ninja, DNS:authlab.digi.ninja, DNS:cors-client.digi.ninja, DNS:cors-server.digi.ninja, DNS:crackedflask.digi.ninja, DNS:digi.ninja, DNS:digininja.org, DNS:frontme.vuln-demo.com,

DNS:frontmecf.vuln-demo.com, DNS:graphqlab.digi.ninja, DNS:html5.digi.ninja, DNS:html5server.digi.ninja, DNS:iot-cert.space, DNS:ip.digi.ninja, DNS:secret.digi.ninja, DNS:splitxsslab.digi.ninja, DNS:svg.digi.ninja, DNS:vuln-demo.com, DNS:vulndap.digi.ninja, DNS:ws.digi.ninja, DNS:www.digi.ninja, DNS:www.digininja.org, DNS:www.iot-cert.space, DNS:www.vuln-demo.com, DNS:www.zonetransfer.me, DNS:zonetransfer.me

| Not valid before: 2025-03-28T03:30:16

|_Not valid after: 2025-06-26T03:30:15

|_http-server-header: Apache

4000/tcp open http Node.js (Express middleware)

|_http-title: GraphQLab

8080/tcp open http-proxy?

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port25-TCP:V=7.92%I=7%D=4/22%Time=68075D17%P=x86_64-redhat-linux-gnu%r(

SF:NULL,42,"220\x20eig-obgw-6009a\.ext\.cloudfilter\.net\x20cmsmtp\x20ESMT

SF:P\x20server\x20ready\r\n")%r(Hello,63,"220\x20eig-obgw-6009a\.ext\.clou

SF:dfilter\.net\x20cmsmtp\x20ESMTP\x20server\x20ready\r\n501\x20EHLO\x20re

SF:quires\x20valid\x20address\r\n")%r(Help,5C,"220\x20eig-obgw-6002a\.ext\

SF:.cloudfilter\.net\x20cmsmtp\x20ESMTP\x20server\x20ready\r\n500\x20comma

SF:nd\x20unrecognized\r\n")%r(GenericLines,76,"220\x20eig-obgw-6006a\.ext\

SF:.cloudfilter\.net\x20cmsmtp\x20ESMTP\x20server\x20ready\r\n500\x20comma

SF:nd\x20unrecognized\r\n500\x20command\x20unrecognized\r\n")%r(GetRequest

SF:,76,"220\x20eig-obgw-6007a\.ext\.cloudfilter\.net\x20cmsmtp\x20ESMTP\x2

SF:0server\x20ready\r\n500\x20command\x20unrecognized\r\n500\x20command\x2

SF:0unrecognized\r\n");

Device type: WAP|general purpose|VoIP phone|phone|specialized

Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (91%), Linksys embedded (91%), Cisco embedded (88%), Google Android 4.0.X (88%), Suga embedded (87%)

OS CPE: cpe:/o:linux:linux_kernel cpe:/h:linksys:ea3500 cpe:/o:linux:linux_kernel:3.16 cpe:/o:linux:linux_kernel:4.4 cpe:/h:cisco:cp-dx80 cpe:/o:google:android cpe:/o:linux:linux_kernel:2.6 cpe:/o:google:android:4.0.4

Aggressive OS guesses: Linksys EA3500 WAP (91%), Linux 3.16 (90%), Linux 4.4 (90%), Cisco CP-DX80 collaboration endpoint (Android) (88%), Linux 3.6 - 3.10 (88%), Linux 2.6.18 - 2.6.32 (87%), Android 4.0.4 (Linux 2.6) (87%), Suga embedded WiFi module (87%), Axis M3006-V network camera (87%), Android 4.4.0 (87%)

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

Network Distance: 13 hops

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 ...

2 0.32 ms 172.31.0.3

3 0.66 ms 125.19.200.161

4 126.59 ms 116.119.68.58

5 136.04 ms lon-thw-pb3-nc5.uk.eu (91.121.131.34)

6 ... 8

9 127.96 ms be101.rbx-g3-nc5.fr.eu (54.36.50.241)

10 ... 12

13 128.29 ms 5.196.105.14

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 52.94 seconds