

ASSIGNMENT-1

CHITTALA SWATHI

B. TECH

20ME1A4612

RCEE

Information gathering in WHOIS

The image shows two screenshots of the Whois website interface. The top screenshot shows the 'Whois Domain Lookup' page with the IP address 44.228.249.3 entered in the search bar. The bottom screenshot shows the results for the domain vulnweb.com, which was updated 4 days ago. The domain information is as follows:

Domain Information	
Domain:	vulnweb.com
Registrar:	EuroDNS S.A.
Registered On:	2010-06-14
Expires On:	2025-06-13
Updated On:	2023-05-26
Status:	clientTransferProhibited
Name Servers:	ns1.eurodns.com ns2.eurodns.com ns3.eurodns.com ns4.eurodns.com

Interested in similar domains?

vulnwebonline.com	Buy Now
thevulnweb.com	Buy Now
vulnwebgroup.com	Buy Now
myvulnweb.com	Buy Now
vulnweb.net	Buy Now
vulnwebonline.net	Buy Now

There is also a red banner with the word 'Sale' at the bottom right of the results section.

Whois vulnweb.com

whois.com/whois/vulnweb.com

GmailYouTubeMapsAircrack-ng - Downl...Server World - ネット...edyodaInstagramACXEthical Hacking - ...SkillsBuild

.COM @ \$9.98Register a .COM domain for only \$9.98! While stocks last!BUY NOW

WhoisIdentity for everyone

DomainsHostingServersEmailSecurityWhoisDeals

Enter Domain or IPWHOIS

Registrant Contact

Name:Acunetix Acunetix

Organization:Acunetix Ltd

Street:3rd Floor,, J&C Building,, Road Town

City:Tortola

Postal Code:VG1110

Country:VG

Phone:+1.23456789

Email:administrator@acunetix.com

Administrative Contact

.space

~~\$29.88~~ \$1.88

BUY NOW

*while stocks last

On Sale!

.LIFE

.LIFE @ \$2.48 \$35.88

Whois vulnweb.com

whois.com/whois/vulnweb.com

GmailYouTubeMapsAircrack-ng - Downl...Server World - ネット...edyodaInstagramACXEthical Hacking - ...SkillsBuild

.COM @ \$9.98Register a .COM domain for only \$9.98! While stocks last!BUY NOW

WhoisIdentity for everyone

DomainsHostingServersEmailSecurityWhoisDeals

Enter Domain or IPWHOIS

Administrative Contact

Name:Acunetix Acunetix

Organization:Acunetix Ltd

Street:3rd Floor,, J&C Building,, Road Town

City:Tortola

Postal Code:VG1110

Country:VG

Phone:+1.23456789

Email:administrator@acunetix.com

Technical Contact

Introducing

WORDPRESSHOSTING

\$5.48/mo

VIEW MORE

Whois vulnweb.com

whois.com/whois/vulnweb.com

.COM @ \$9.98 Register a .COM domain for only \$9.98! While stocks last! BUY NOW

Whois Domains Hosting Servers Email Security Whois Deals Enter Domain or IP WHOIS

Technical Contact

Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	administrator@acunetix.com

Raw Whois Data

44.228.249.3 DNS Lookup Whois IP 44.228.249.3

whois.com/whois/44.228.249.3

.COM @ \$9.98 Register a .COM domain for only \$9.98! While stocks last! BUY NOW

Whois Domains Hosting Servers Email Security Whois Deals Enter Domain or IP WHOIS

Whois IP 44.228.249.3

Updated 1 minute ago

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

# start

NetRange: 44.192.0.0 - 44.255.255.255
CIDR: 44.192.0.0/10
NetName: AMAZO-4
```

.space Sale

~~\$29.88~~ **\$1.88**

BUY NOW

*while stocks last

On Sale!

.blog

44.228.249.3 x DNS Lookup x Whois IP 44.228.249.3 x +

whois.com/whois/44.228.249.3

.COM @ \$9.98 Register a .COM domain for only \$9.98! While stocks last! BUY NOW

Whois Domains Hosting Servers Email Security Whois Deals Enter Domain or IP WHOIS

NetName: AMAZO-4
NetHandle: NET-44-192-0-0-1
Parent: NET44 (NET-44-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Amazon.com, Inc. (AMAZO-4)
RegDate: 2019-07-18
Updated: 2019-07-18
Ref: https://rdap.arin.net/registry/ip/44.192.0.0

OrgName: Amazon.com, Inc.
OrgId: AMAZO-4
Address: Amazon Web Services, Inc.
Address: P.O. Box 81226
City: Seattle
StateProv: WA
PostalCode: 98108-1226
Country: US
RegDate: 2005-09-29

.FUN @ \$1.98 ~~\$35.00~~

Introducing
WORDPRESS HOSTING
\$5.48/mo
VIEW MORE

44.228.249.3 x DNS Lookup x Whois IP 44.228.249.3 x +

whois.com/whois/44.228.249.3

.COM @ \$9.98 Register a .COM domain for only \$9.98! While stocks last! BUY NOW

Whois Domains Hosting Servers Email Security Whois Deals Enter Domain or IP WHOIS

OrgRoutingName: IP Routing
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-routing-poc@amazon.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/IPROU3-ARIN

OrgNOCHandle: AAN01-ARIN
OrgNOCName: Amazon AWS Network Operations
OrgNOCPhone: +1-206-555-0000
OrgNOCEmail: amazon-noc-contact@amazon.com
OrgNOCRef: https://rdap.arin.net/registry/entity/AAN01-ARIN

OrgTechHandle: ANO24-ARIN
OrgTechName: Amazon EC2 Network Operations
OrgTechPhone: +1-206-555-0000
OrgTechEmail: amazon-noc-contact@amazon.com
OrgTechRef: https://rdap.arin.net/registry/entity/ANO24-ARIN

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName: AWS RPKI Management POC
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-routing-poc@amazon.com

44.228.249.3 x DNS Lookup x Whois IP 44.228.249.3 x +

whois.com/whois/44.228.249.3

.COM @ \$9.98 Register a .COM domain for only \$9.98! While stocks last! BUY NOW

Whois Domains Hosting Servers Email Security Whois Deals Enter Domain or IP WHOIS

```
OrgAbuseHandle: AEAS-ARIN
OrgAbuseName: Amazon EC2 Abuse
OrgAbusePhone: +1-206-555-0000
OrgAbuseEmail: abuse@amazonaws.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/AEAS-ARIN

# end

# start

NetRange: 44.224.0.0 - 44.255.255.255
CIDR: 44.224.0.0/11
NetName: AMAZO-ZPDX
NetHandle: NET-44-224-0-0-1
Parent: AMAZO-4 (NET-44-192-0-0-1)
NetType: Reallocated
OriginAS:
Organization: Amazon.com, Inc. (AMAZO-47)
RegDate: 2019-08-01
```

44.228.249.3 x DNS Lookup x Whois IP 44.228.249.3 x +

whois.com/whois/44.228.249.3

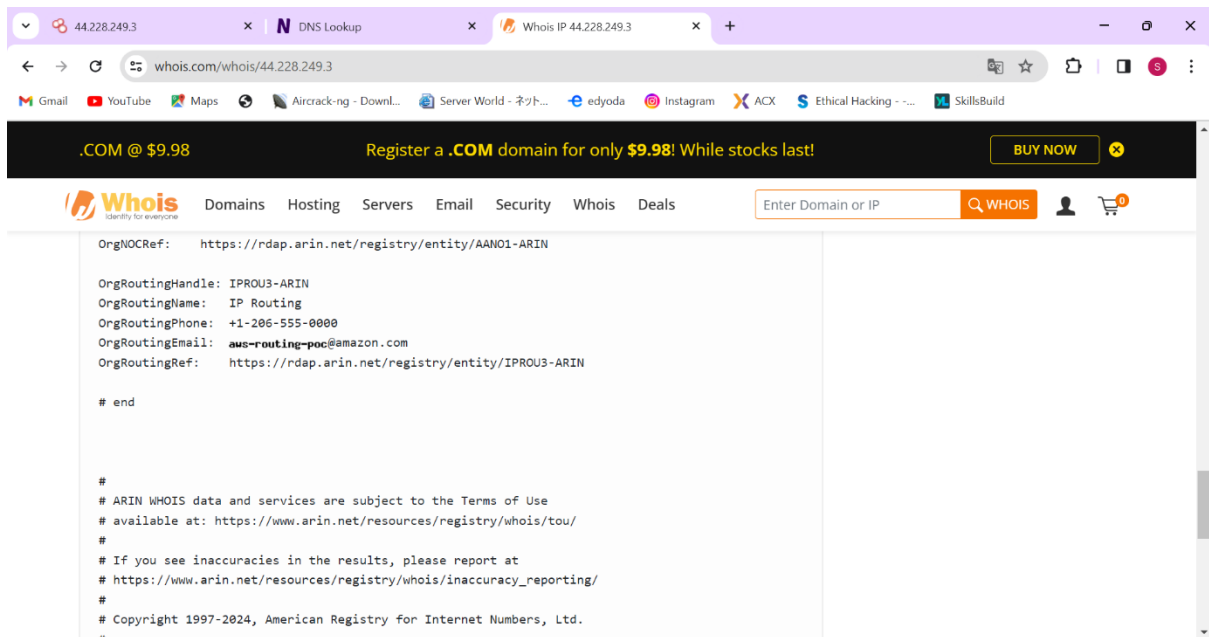
.COM @ \$9.98 Register a .COM domain for only \$9.98! While stocks last! BUY NOW

Whois Domains Hosting Servers Email Security Whois Deals Enter Domain or IP WHOIS

```
OrgId: AMAZO-47
Address: EC2, EC2 1200 12th Ave South
City: Seattle
StateProv: WA
PostalCode: 98144
Country: US
RegDate: 2011-05-10
Updated: 2021-07-22
Ref: https://rdap.arin.net/registry/entity/AMAZO-47

OrgAbuseHandle: AEAS-ARIN
OrgAbuseName: Amazon EC2 Abuse
OrgAbusePhone: +1-206-555-0000
OrgAbuseEmail: abuse@amazonaws.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/AEAS-ARIN

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName: AWS RPKI Management POC
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-rpki-routing-poc@amazon.com
```



#

ARIN WHOIS data and services are subject to the Terms of Use

available at: <https://www.arin.net/resources/registry/whois/tou/>

#

If you see inaccuracies in the results, please report at

https://www.arin.net/resources/registry/whois/inaccuracy_reporting/

#

Copyright 1997-2024, American Registry for Internet Numbers, Ltd.

#

start

NetRange: 44.192.0.0 - 44.255.255.255

CIDR: 44.192.0.0/10

NetName: AMAZO-4

NetHandle: NET-44-192-0-0-1

Parent: NET44 (NET-44-0-0-0-0)

NetType: Direct Allocation
OriginAS:
Organization: Amazon.com, Inc. (AMAZO-4)
RegDate: 2019-07-18
Updated: 2019-07-18
Ref: <https://rdap.arin.net/registry/ip/44.192.0.0>

OrgName: Amazon.com, Inc.
OrgId: AMAZO-4
Address: Amazon Web Services, Inc.
Address: P.O. Box 81226
City: Seattle
StateProv: WA
PostalCode: 98108-1226
Country: US
RegDate: 2005-09-29
Updated: 2022-09-30
Comment: For details of this service please see
Comment: <http://ec2.amazonaws.com>
Ref: <https://rdap.arin.net/registry/entity/AMAZO-4>

OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName: IP Routing
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: **aws-routing-poc**@amazon.com
OrgRoutingRef: <https://rdap.arin.net/registry/entity/IPROU3-ARIN>

OrgNOCHandle: AANO1-ARIN

OrgNOCName: Amazon AWS Network Operations
OrgNOCPhone: +1-206-555-0000
OrgNOCEmail: **anzn-noc-contact**@amazon.com
OrgNOCRef: <https://rdap.arin.net/registry/entity/AANO1-ARIN>

OrgTechHandle: ANO24-ARIN
OrgTechName: Amazon EC2 Network Operations
OrgTechPhone: +1-206-555-0000
OrgTechEmail: **anzn-noc-contact**@amazon.com
OrgTechRef: <https://rdap.arin.net/registry/entity/ANO24-ARIN>

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName: AWS RPKI Management POC
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: **aws-rpki-routing-poc**@amazon.com
OrgRoutingRef: <https://rdap.arin.net/registry/entity/ARMP-ARIN>

OrgAbuseHandle: AEA8-ARIN
OrgAbuseName: Amazon EC2 Abuse
OrgAbusePhone: +1-206-555-0000
OrgAbuseEmail: **abuse**@amazonaws.com
OrgAbuseRef: <https://rdap.arin.net/registry/entity/AEA8-ARIN>

end

start

NetRange: 44.224.0.0 - 44.255.255.255
CIDR: 44.224.0.0/11
NetName: AMAZO-ZPDX

NetHandle: NET-44-224-0-0-1
Parent: AMAZO-4 (NET-44-192-0-0-1)
NetType: Reallocated
OriginAS:
Organization: Amazon.com, Inc. (AMAZO-47)
RegDate: 2019-08-01
Updated: 2019-08-01
Ref: <https://rdap.arin.net/registry/ip/44.224.0.0>

OrgName: Amazon.com, Inc.
OrgId: AMAZO-47
Address: EC2, EC2 1200 12th Ave South
City: Seattle
StateProv: WA
PostalCode: 98144
Country: US
RegDate: 2011-05-10
Updated: 2021-07-22
Ref: <https://rdap.arin.net/registry/entity/AMAZO-47>

OrgAbuseHandle: AEA8-ARIN
OrgAbuseName: Amazon EC2 Abuse
OrgAbusePhone: +1-206-555-0000
OrgAbuseEmail: **abuse**@amazonaws.com
OrgAbuseRef: <https://rdap.arin.net/registry/entity/AEA8-ARIN>

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName: AWS RPKI Management POC

OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: **aws-rpki-routing-poc**@amazon.com
OrgRoutingRef: <https://rdap.arin.net/registry/entity/ARMP-ARIN>

OrgTechHandle: ANO24-ARIN
OrgTechName: Amazon EC2 Network Operations
OrgTechPhone: +1-206-555-0000
OrgTechEmail: **anzn-noc-contact**@amazon.com
OrgTechRef: <https://rdap.arin.net/registry/entity/ANO24-ARIN>

OrgNOCHandle: AANO1-ARIN
OrgNOCName: Amazon AWS Network Operations
OrgNOCPhone: +1-206-555-0000
OrgNOCEmail: **anzn-noc-contact**@amazon.com
OrgNOCRef: <https://rdap.arin.net/registry/entity/AANO1-ARIN>

OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName: IP Routing
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: **aws-routing-poc**@amazon.com
OrgRoutingRef: <https://rdap.arin.net/registry/entity/IPROU3-ARIN>

end

#

ARIN WHOIS data and services are subject to the Terms of Use

available at: <https://www.arin.net/resources/registry/whois/tou/>

#

If you see inaccuracies in the results, please report at

https://www.arin.net/resources/registry/whois/inaccuracy_reporting/

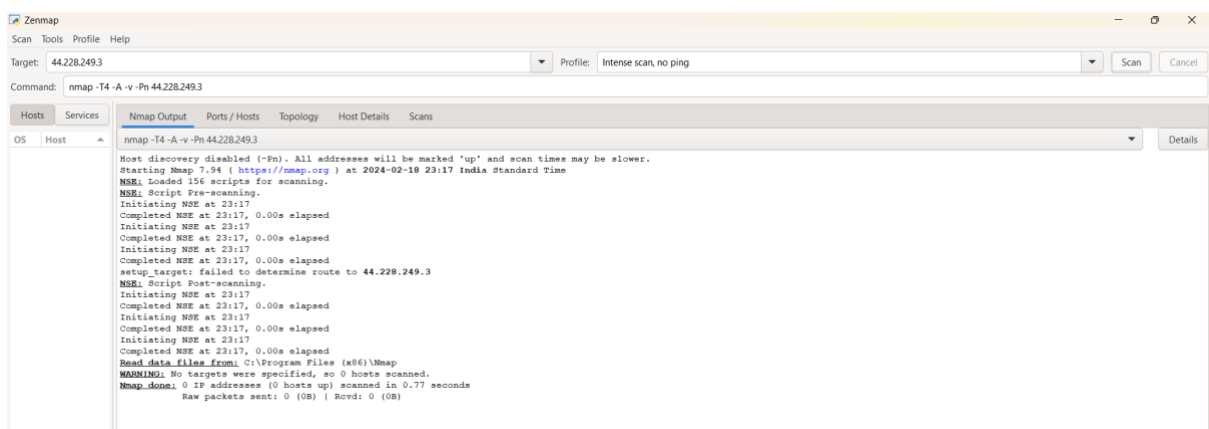
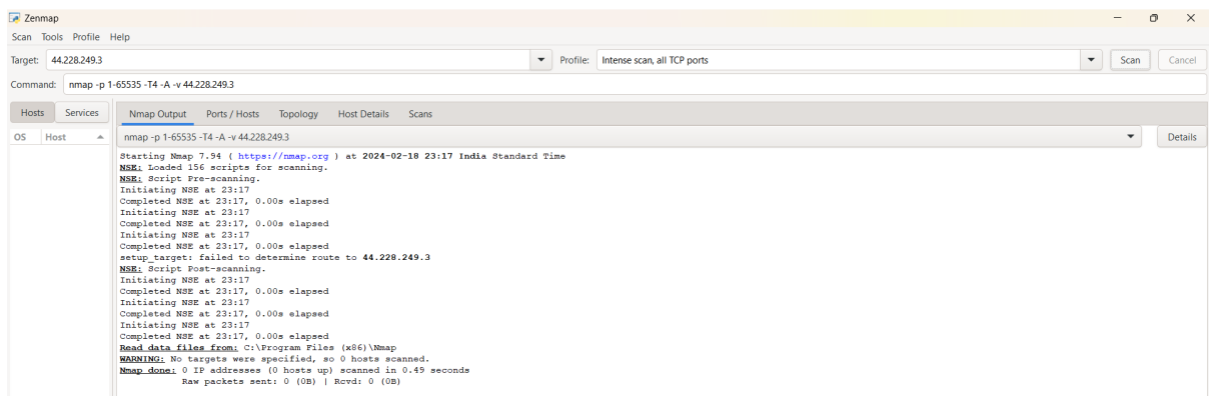
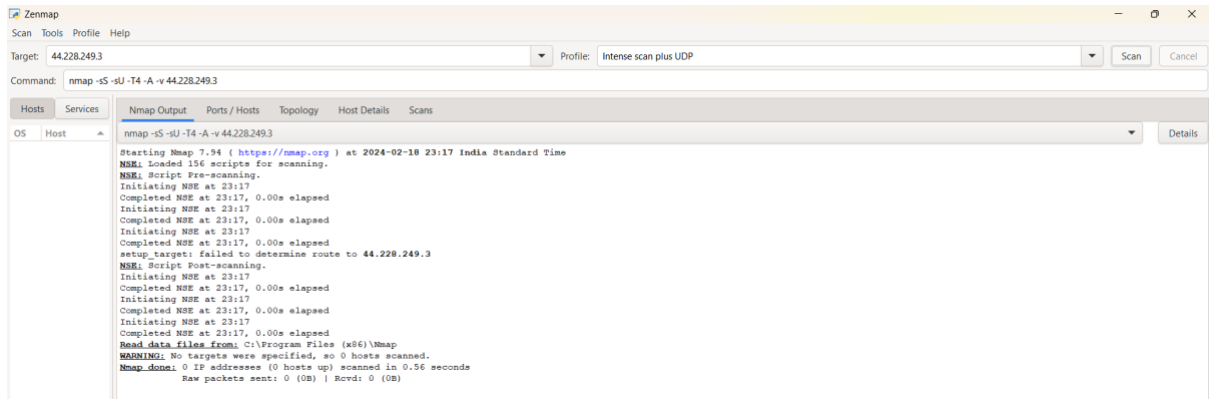
#

Copyright 1997-2024, American Registry for Internet Numbers, Ltd.

#

Using Nmap Tool

Intense Scan



In Kali linux Nmap

```
(root@kali)-[/home/kali]
```

```
# nmap -T4 -A -v 44.228.249.3
```

```
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-22 23:14 EST
```

```
NSE: Loaded 155 scripts for scanning.
```

```
NSE: Script Pre-scanning.
```

```
Initiating NSE at 23:14
```

```
Completed NSE at 23:14, 0.00s elapsed
```

```
Initiating NSE at 23:14
```

```
Completed NSE at 23:14, 0.00s elapsed
```

```
Initiating NSE at 23:14
```

```
Completed NSE at 23:14, 0.00s elapsed
```

```
Initiating Ping Scan at 23:14
```

```
Scanning 44.228.249.3 [4 ports]
```

```
Completed Ping Scan at 23:14, 0.37s elapsed (1 total hosts)
```

```
Initiating Parallel DNS resolution of 1 host. at 23:14
```

```
Completed Parallel DNS resolution of 1 host. at 23:14, 0.70s elapsed
```

```
Initiating SYN Stealth Scan at 23:14
```

```
Scanning ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3) [1000 ports]
```

```
Discovered open port 80/tcp on 44.228.249.3
```

```
Discovered open port 80/tcp on 44.228.249.3
```

```
Completed SYN Stealth Scan at 23:14, 26.47s elapsed (1000 total ports)
```

```
Initiating Service scan at 23:14
```

```
Scanning 1 service on ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
```

```
Completed Service scan at 23:15, 30.14s elapsed (1 service on 1 host)
```

```
Initiating OS detection (try #1) against ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
```

```
Retrying OS detection (try #2) against ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
```

```
Initiating Traceroute at 23:15
```

```
Completed Traceroute at 23:15, 1.49s elapsed
```

```
Initiating Parallel DNS resolution of 2 hosts. at 23:15
```

```
Completed Parallel DNS resolution of 2 hosts. at 23:15, 0.04s elapsed
```

```
NSE: Script scanning 44.228.249.3.
```

```
Initiating NSE at 23:15
```

```
Completed NSE at 23:15, 21.92s elapsed
```

```
Initiating NSE at 23:15
```

```
Completed NSE at 23:15, 3.00s elapsed
```

```
Initiating NSE at 23:15
```

```
Completed NSE at 23:15, 0.00s elapsed
```

```
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
```

```
Host is up (0.37s latency).
```

```
Not shown: 999 filtered tcp ports (no-response)
```

```
PORT      STATE SERVICE VERSION
```

```
80/tcp    open  http    nginx 1.19.0
```

```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

```
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
```

```
No OS matches for host
```

```
Uptime guess: 0.000 days (since Thu Feb 22 23:15:11 2024)
```

```
Network Distance: 3 hops
```

```
TCP Sequence Prediction: Difficulty=264 (Good luck!)
```

```
IP ID Sequence Generation: All zeros
```

```
TRACEROUTE (using port 80/tcp)
```

```
HOP RTT      ADDRESS
```

```
1 448.98 ms gpon.net (192.168.1.1)
```

```
2 448.60 ms 10.24.0.1 (10.24.0.1)
```

```
3 450.05 ms ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
```

TRACEROUTE (using port 80/tcp)

HOP	RTT	ADDRESS
1	448.98 ms	gpon.net (192.168.1.1)
2	448.60 ms	10.24.0.1 (10.24.0.1)
3	450.05 ms	ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)

NSE: Script Post-scanning.

Initiating NSE at 23:15

Completed NSE at 23:15, 0.00s elapsed

Initiating NSE at 23:15

Completed NSE at 23:15, 0.00s elapsed

Initiating NSE at 23:15

Completed NSE at 23:15, 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 98.72 seconds

Raw packets sent: 2138 (98.178KB) | Rcvd: 95 (5.486KB)