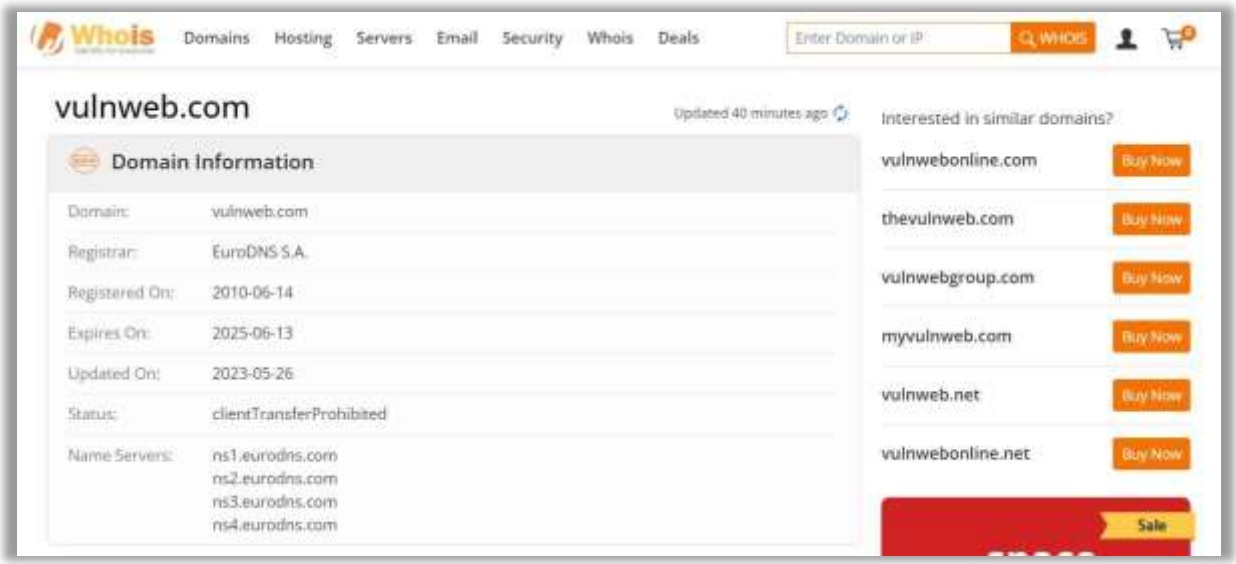
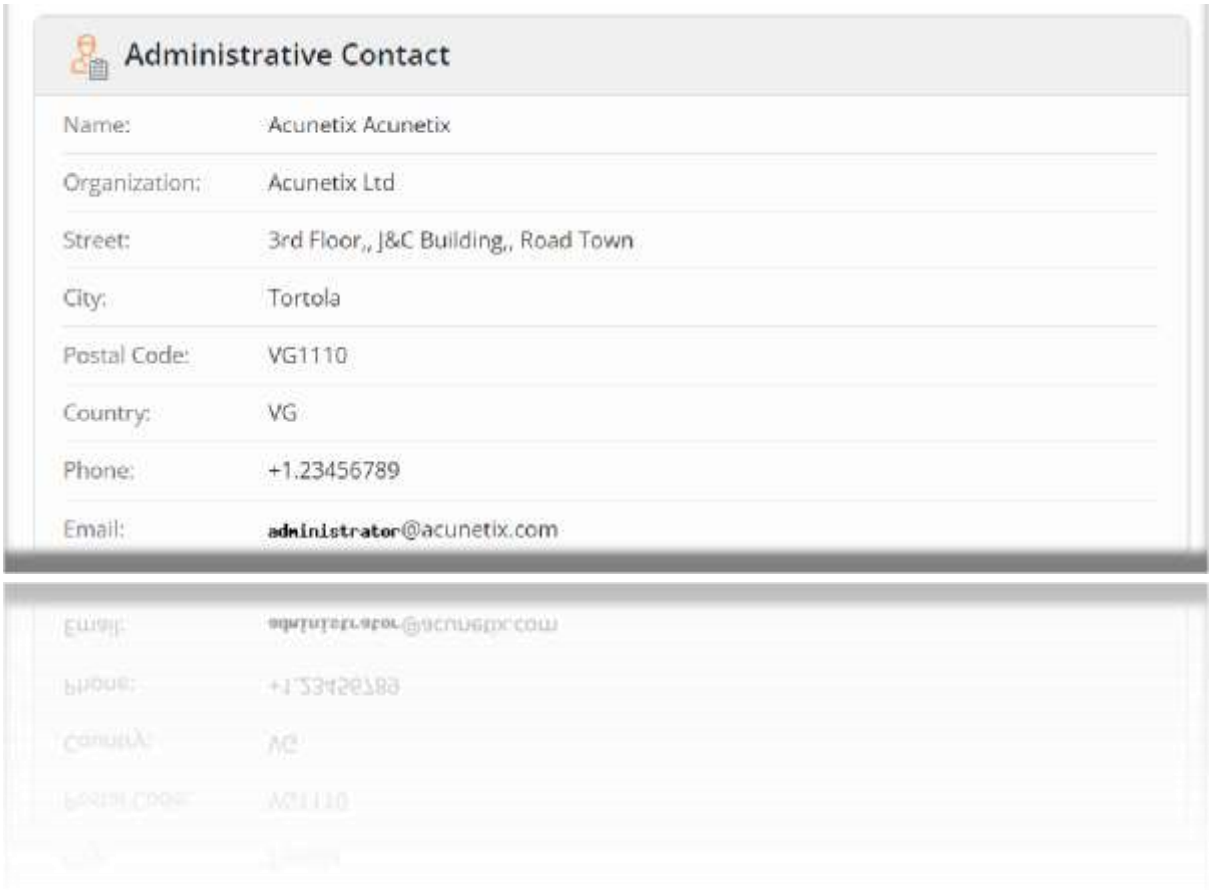
Information gathering in WHOIS

Domain Information

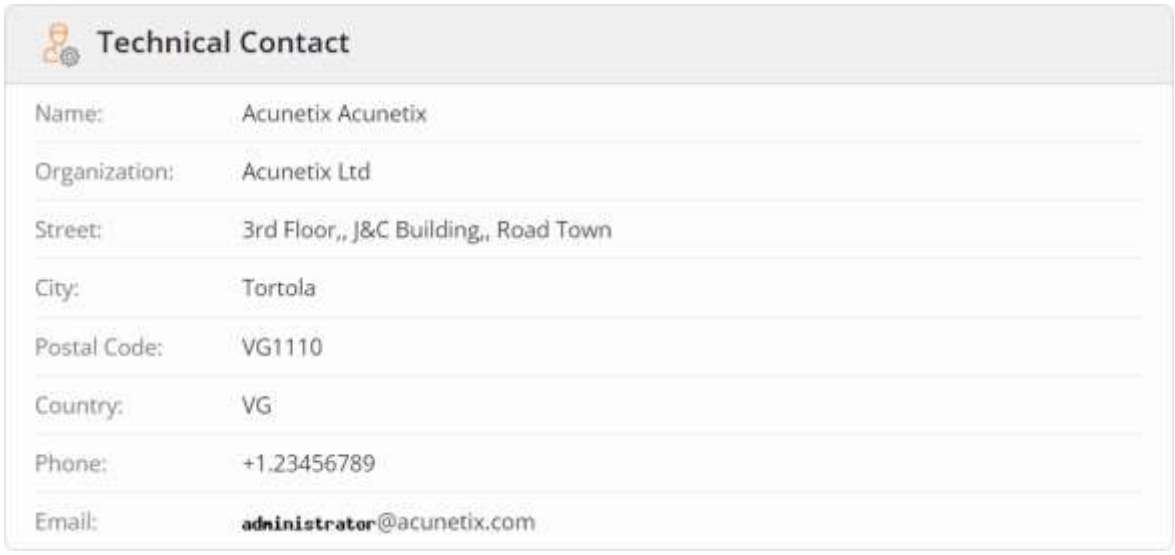


Registrant Contact

Administrative Contact



Technical Contact



Raw Whois Data

```
Domain Name: vulnweb.com

Registry Domain ID: D16000066-COM

Registrar WHOIS Server: whois.eurodns.com

Registrar URL: http://www.eurodns.com

Updated Date: 2023-05-26T10:04:20Z

Creation Date: 2010-06-14T00:00:00Z

Registrar Registration Expiration Date: 2025-06-
13T00:00:00Z
```

Registrar: Eurodns S.A.

Registrar IANA ID: 1052

Registrar Abuse Contact Email: legalservices@eurodns.com

Registrar Abuse Contact Phone: +352.27220150

Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Registry Registrant ID:

Registrant Name: Acunetix Acunetix

Registrant Organization: Acunetix Ltd

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

Registrant City: Tortola

Registrant State/Province:

Registrant Postal Code: VG1110

Registrant Country: VG

Registrant Phone: +1.23456789

Registrant Fax:

Registrant Email: administrator@acunetix.com

Registry Admin ID:

Admin Name: Acunetix Acunetix

Admin Organization: Acunetix Ltd

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

Admin City: Tortola

Admin State/Province:

Admin Postal Code: VG1110

Admin Country: VG

Admin Phone: +1.23456789

Admin Fax:

Admin Email: administrator@acunetix.com

Registry Tech ID:

Tech Name: Acunetix Acunetix

Tech Organization: Acunetix Ltd

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

Tech City: Tortola

Tech State/Province:

Tech Postal Code: VG1110

Tech Country: VG

Tech Phone: +1.23456789

Tech Fax:

Tech Email: administrator@acunetix.com

Name Server: ns1.eurodns.com

Name Server: ns2.eurodns.com

Name Server: ns3.eurodns.com

Name Server: ns4.eurodns.com

DNSSEC: unsigned

Background

Site title	Home of Acunetix Art	Date first seen	April 2017
Site rank	2339	Primary language	English
Description	Not Present		

Network

Site	http://testphp.vulnweb.com/	Domain	vulnweb.com
Netblock Owner	Amazon.com, Inc.	Nameserver	ns1.eurodns.com
Hosting company	Amazon - US West (Oregon) datacenter	Domain registrar	eurodns.com
Hosting country	us	Nameserver organisation	whois.eurodns.com
IPv4 address	44.228.249.3 (VirusTotal)	Organisation	Acunetix Ltd, 3rd Floor, J&C Building, Road Town, Tortola, VG1110, Virgin Islands (British)
IPv4 autonomous systems	AS16509	DNS admin	hostmaster@eurodns.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)

IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Unknown
Reverse DNS	ec2-44-228-249-3.us-west-2.compute.amazonaws.com		

IP delegation

IPv4 address (44.228.249.3)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
44.0.0.0-44.255.255.255	United States	NET44	American Registry for Internet Numbers
44.192.0.0-44.255.255.255	United States	AMAZO-4	Amazon.com, Inc.
44.224.0.0-44.255.255.255	United States	AMAZO-ZPDX	Amazon.com, Inc.
44.228.249.3	United States	AMAZO-ZPDX	Amazon.com, Inc.

IP delegation

IPv4 address (44.228.249.3)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
44.0.0.0-44.255.255.255	United States	NET44	American Registry for Internet Numbers
44.192.0.0-44.255.255.255	United States	AMAZO-4	Amazon.com, Inc.
44.224.0.0-44.255.255.255	United States	AMAZO-ZPDX	Amazon.com, Inc.
44.228.249.3	United States	AMAZO-ZPDX	Amazon.com, Inc.

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Amazon.com, Inc. EC2, EC2 1200 12th Ave South Seattle WA US 98144	44.228.249.3	Linux	nginx/1.19.0	17-Feb-2024
Amazon.com, Inc. EC2, EC2 1200 12th Ave South Seattle WA US 98144	44.228.249.3	Linux	unknown	1-May-2023
Amazon.com, Inc. EC2, EC2 1200 12th Ave South Seattle WA US 98144	44.228.249.3	Linux	nginx/1.19.0	30-Apr-2023
Amazon.com, Inc. EC2, EC2 1200 12th Ave South Seattle WA US 98144	44.228.249.3	Linux	unknown	11-Apr-2023
Amazon.com, Inc. EC2, EC2 1200 12th Ave South Seattle WA US 98144	44.228.249.3	Linux	nginx/1.19.0	10-Apr-2023
Amazon.com, Inc. EC2, EC2 1200 12th Ave South Seattle WA US 98144	44.228.249.3	unknown	nginx/1.19.0	5-Feb-2023
Amazon.com, Inc. EC2, EC2 1200 12th Ave South Seattle WA US 98144	44.228.249.3	unknown	unknown	29-Dec-2022
Amazon.com, Inc. EC2, EC2 1200 12th Ave South Seattle WA US 98144	44.228.249.3	unknown	nginx/1.19.0	28-Dec-2022
Amazon.com, Inc. EC2, EC2 1200 12th Ave South Seattle WA US 98144	44.228.249.3	Linux	nginx/1.19.0	24-Sep-2022
Amazon.com, Inc. EC2, EC2 1200 12th Ave South Seattle WA US 98144	44.228.249.3	unknown	nginx/1.19.0	23-Sep-2022

Site Technology (fetched 14 days ago)

Cloud & PaaS

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Platform as a service (PaaS) is a category of cloud computing services that provide a computing platform and a solution stack as a service.

Technology	Description	Popular sites using this technology
Amazon Web Services - EC2	Cloud computing service (Elastic Compute Cloud)	www.makeuseof.com, www.duolingo.com, onlyfans.com

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

Technology	Description	Popular sites using this technology
Deliver	No description	www.emtpcorp.com, www.vincihoteles.com, www.24prensa.com

Using Nmap Tool

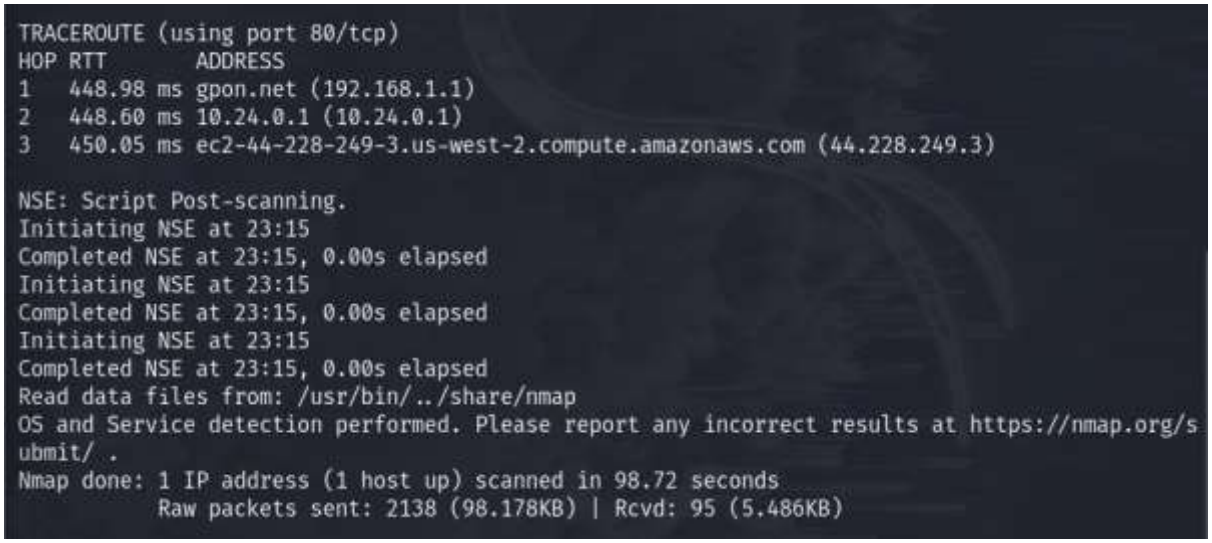
Intense Scan

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 (44.2
28.249.3)
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 clo
sed 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)