Task-2

Footprinting (STEP1&2) website - vulnweb.com

Registrar name

Domain Name: VULNWEB.COM
Registry Domain ID: D16000066-COM
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

Registrar WHOIS Server: whois.eurodns.com

Registrar Status clientTransferProhibited

Dates   4,997 days old Created

on 2010-06-14 Expires

on 2025-06-13

Updated on 2023-05-26

IP Address	44.228.249.3 is hosted on a dedicated server
IP Location	- Oregon - Boardman - Amazon.com Inc.
ASN	AS16509 AMAZON-02, US (registered May 04, 2000)
Domain Status	Registered And No Website
IP History	4 changes on 4 unique IP addresses over 10 years
Registrar History	2 registrars

Name Servers   NS1.EURODNS.COM (has 306,244 domains)

NS2.EURODNS.COM (has 306,244 domains)

NS3.EURODNS.COM (has 306,244 domains)

NS4.EURODNS.COM (has 306,244 domains)

Reconnaissance(STEP 3 NMAP) NMAP

SCANNING – VULNWEB.COM

Hostnames: ec2-44-228-249-3.us-west-2.compute.amazonaws.com

OS Linux 2.6.32 has been released in December 3rd 2009.

Starting Nmap 7.40 (https://nmap.org) at 2024-02-19 07:51 UTC Nmap scan report for ec2-44-228-249-3.us-west- 2.compute.amazonaws.com (44.228.249.3)

PORT STATE SERVICE

21/tcp filtered ftp

22/tcp filtered ssh

23/tcp filtered telnet 80/tcp open http

110/tcp filtered pop3

143/tcp filtered imap

443/tcp filtered https

3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.00 seconds

Conclusion on my report

The website vulnweb.com, hosted on Amazon Web Services, has port 80 open. This vulnerability was confirmed during an With the port open, an attacker could leverage tools like Metasploit on Kali Linux to gain unauthorized access to the vulnerable website. The site is running on a Linux 2.6.32 kernel, which dates back to December 2009, making it old and susceptible to various security vulnerabilities.

Sk.Zahida
208x1a4240
Kallam haranadha reddy institute of technology(k.H.I.T)