

16/02/2024

Friday



Durgapu Sai Krishna
B.tech iv year, IT
208X1A1206
KALLAM
HARANADHAREDDY
INSTITUTE OF TECH.

ASSIGNMENT-1

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
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)

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

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

Port-80 Is Opened In Above Website Which Is Vulnweb.Com(Hosting using amazon web server) Confirmed During The Nmap Scanning It Is In Open State Which Can Attacker Easily Entered Using Metasploit Tool In Kali Linux To That Website And Access The All Content Available In That Vulnerable Site That Site Is Used Linux 2.6.32 Which Is Released In December 2009 Which Is Old And Vulnerable Machine

-D.Sai Krishna