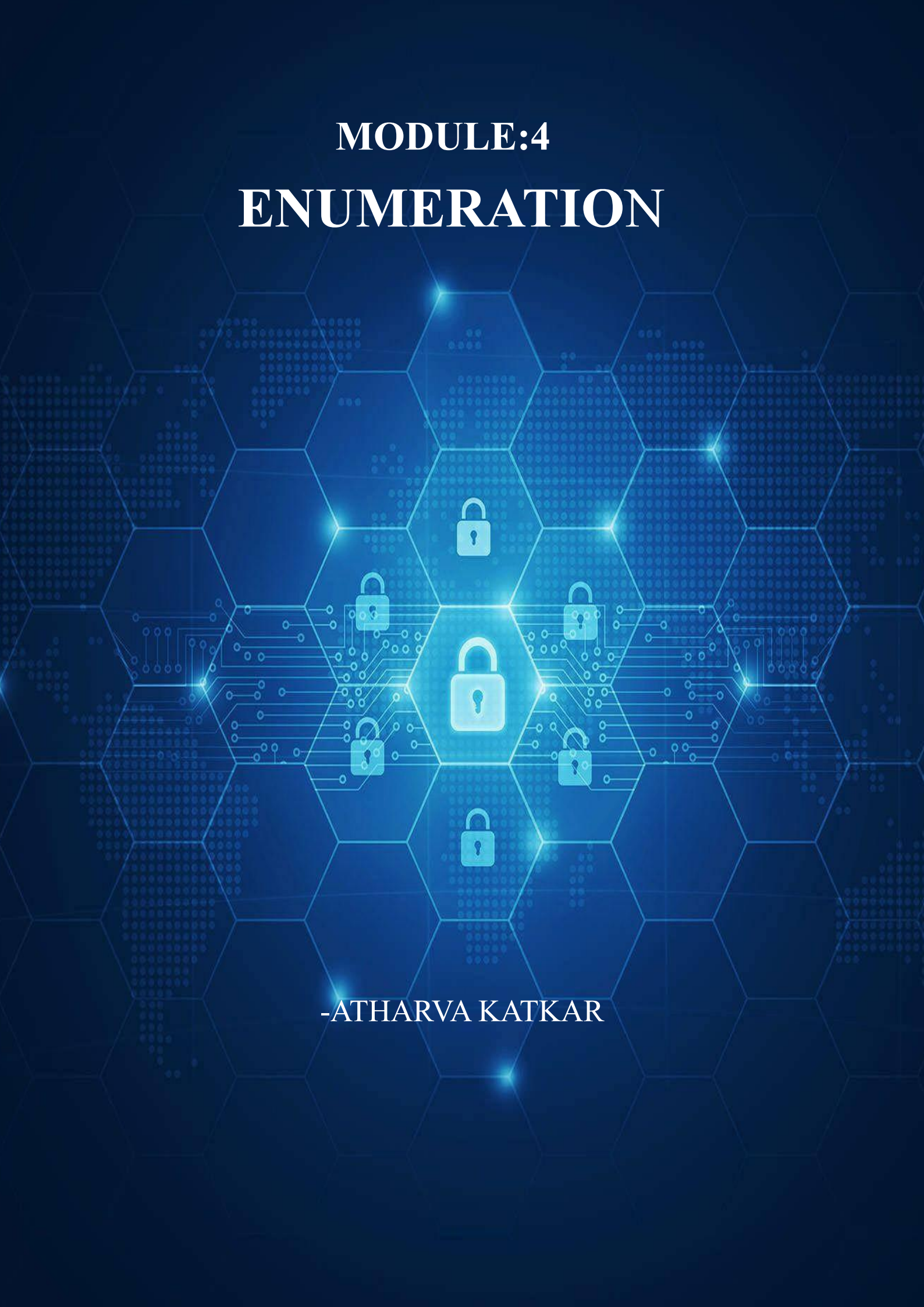
MODULE:4

ENUMERATION



-ATHARVA KATKAR

ENUMERATION

Enumeration is the active process of extracting detailed information about a target system during a penetration test. It comes after scanning and involves making direct connections to the target to gather valuable data that can help exploit vulnerabilities. Enumeration requires active communication, meaning the target system may log or detect your activity.

Ethical hackers perform enumeration to:

- Identify usernames
- Find network shares
- Discover services and versions
- Collect system information
- Extract configuration details
- Identify potential vulnerabilities

Types of Enumeration:

Here are the major types used in ethical hacking:

A. Network Enumeration

- Identifying live hosts
- Mapping IPs
- Detecting routers, firewalls, gateways
- Tools: Nmap, Netdiscover, Traceroute

B. Service Enumeration

- Listing running services and versions
- Discovering service banners
- Tools: Nmap -sV, Netcat, Telnet

C. User Enumeration

- Extracting usernames or accounts
- Common on: SMB, SNMP, FTP, SMTP
- Tools: enum4linux, smtp-user-enum

D. SMB Enumeration

- Accessing Windows shares and users
- Tools: enum4linux, smbclient, rpcclient

E. SNMP Enumeration

- Extracting network device information
- Tools: snmpwalk, snmp-check

F. DNS Enumeration

- Extracting DNS records
- Zone transfers
- Tools: dig, nslookup, dnsenum, fierce

G. Web Enumeration

- Finding hidden files/folders
- Identifying server technologies
- Tools: Gobuster, Dirb, WhatWeb, Wappalyzer

Common Enumeration Commands :

1)Network + Service Enumeration

- nmap -sV <target>
- nmap -A <target>

2)SMB Enumeration

- enum4linux -a <target>
- smbclient -L //<target>

3)DNS Enumeration

- dig axfr @<nameserver> <domain>
- dnsenum <domain>

4)SNMP Enumeration

- snmpwalk -v1 -c public <target>

5)Web Directory Enumeration

- gobuster dir -u http://target -w wordlist.txt

Enumeration may provide:

✓ Usernames
✓ Groups and roles
✓ System banners
✓ Network shares
✓ Running services
✓ OS version
✓ SNMP data (uptime, interfaces, ARP table)
✓ DNS records
✓ Web directories and files

NetBIOS Enumeration

NetBIOS enumeration is a process of obtaining sensitive information about the target such as a list of computers belonging to a target domain, network shares, policies, etc.

NetBIOS stands for Network Basic Input Output System. Windows uses NetBIOS for file and printer sharing. A NetBIOS name is a unique computer name assigned to Windows systems, comprising a 16-character ASCII string that identifies the network device over TCP/IP. The first 15 characters are used for the device name, and the 16th is reserved for the service or name record type.

The NetBIOS service is easily targeted, as it is simple to exploit and runs on Windows systems even when not in use. NetBIOS enumeration allows attackers to read or write to a remote computer system (depending on the availability of shares) or launch a denial of service (DoS) attack.

Nbtstat is a Windows command used to troubleshoot NetBIOS over TCP/IP and to display:

- NetBIOS name tables
- NetBIOS sessions
- Registered names
- Remote machine names
- MAC address
- Open connections

It is commonly used in network enumeration and Windows system information gathering.

NetBIOS Enumeration Using NetBIOS Enumerator:

Step1: Open NetBIOS Enumerator

Step2: Provide IP range and click on scan.

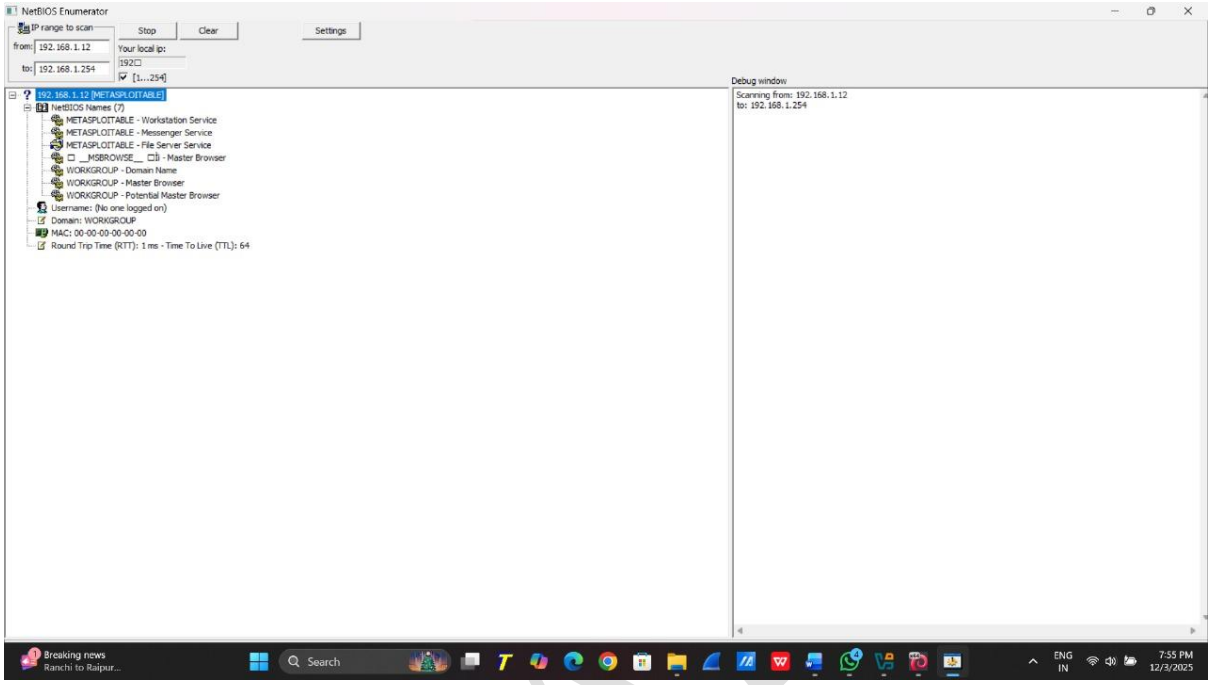


Figure 1

Output:

Host Detected: 192.168.1.12 [METASPLOITABLE]

NetBIOS Names (7 entries)

- METASPLOITABLE – Workstation Service
- METASPLOITABLE – Messenger Service
- METASPLOITABLE – File Server Service
- MSBROWSE – Master Browser
- WORKGROUP – Domain Name
- WORKGROUP – Master Browser
- **User Details:**
- Username: No one logged on

Domain:

- WORKGROUP

SNMP Enumeration

SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP (User Datagram Protocol) and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on networking devices on Windows and UNIX networks.
SNMP enumeration uses SNMP to create a list of the user accounts and devices on a target computer. SNMP employs two types of software components for communication: the SNMP agent and SNMP management station.

Why SNMP is Vulnerable?

Many devices still use default community strings:

- public → read-only (RO)
- private → read-write (RW)

If an attacker gets RW access, they can:

⚠️ Change network settings
⚠️ Reboot devices
⚠️ Modify routing tables
⚠️ Break the network

SnmpWalk is a command line tool that scans numerous SNMP nodes instantly and identifies a set of variables that are available for accessing the target network. It is issued to the root node so that the information from all the sub nodes such as routers and switches can be fetched.

Snmpwalk is used for:

- Enumerating SNMP devices
- Extracting system information
- Getting network configuration
- Extracting ARP/routing tables
- Listing running processes
- Discovering hardware details
- Finding users, services, software

LDAP Enumeration

LDAP (Lightweight Directory Access Protocol) is an Internet protocol for accessing distributed directory services over a network. LDAP uses DNS (Domain Name System) for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a DSA (Directory System Agent), typically on TCP port 389, and sends an operation request to the DSA, which then responds.

Tools for LDAP Enumeration (Kali Linux):

✓ ldapsearch (most used)

✓ nmap LDAP scripts

✓ ldapdomaindump

✓ windapsearch

✓ Enum4linux-ng

✓ bloodhound (for AD mapping)

What LDAP Enumeration Reveals (Very Important)

✓ Usernames (sAMAccountName)

✓ Emails

✓ Password policy

✓ Domain admins

✓ Privileged users

✓ Computers

✓ Service accounts

✓ Organizational Units (OUs)

✓ Kerberos SIDs

NFS Enumeration

NFS enumeration is a method by which exported directories and shared data on target systems is extracted.

NFS (Network File System) is a type of file system that enables computer users to access, view, store, and update files over a remote server. This remote data can be accessed by the client computer in the same way that it is accessed on the local system.

NFS enumeration is the process of identifying:

✓ Shared directories

✓ Mount permissions

✓ User/Group ID mapping

✓ Read/write access

✓ Misconfigured exports

✓ Potential privilege escalation paths

Tools for NFS Enumeration (Kali Linux):

✓ showmount
✓ nmap
✓ mount (for testing access)
✓ rpcinfo

Defenses Against NFS Attacks

✓ Disable NFS if not needed
✓ Remove no_root_squash
✓ Allow only trusted subnet/IPs
✓ Use firewall to block internet access
✓ Use Kerberos (NFSv4 security

DNS Enumeration

DNS Enumeration is the process of extracting **DNS records** and information about a domain to identify:

- Subdomains
- DNS servers
- Mail servers
- IP addresses
- Zone transfer info
- TXT / SPF / DMARC records
- Hidden services

It helps attackers build a map of the target's online infrastructure.

Why DNS Enumeration is Important?

From DNS enumeration, an attacker can discover:

✓ Internal IPs
✓ Hidden subdomains
✓ Mail servers
✓ Cloud services
✓ Dev/test subdomains
✓ Login portals
✓Admin panels

This information helps:

- ➢ Footprinting
- ➢ Attack surface mapping
- ➢ Finding vulnerable subdomains
- ➢ Phishing preparation
- ➢ Web enumeration

1)Run **dig ns** [Target Domain] command (here, the target domain is www.certifiedhacker.com).

Note: In this command, ns returns name servers in the result

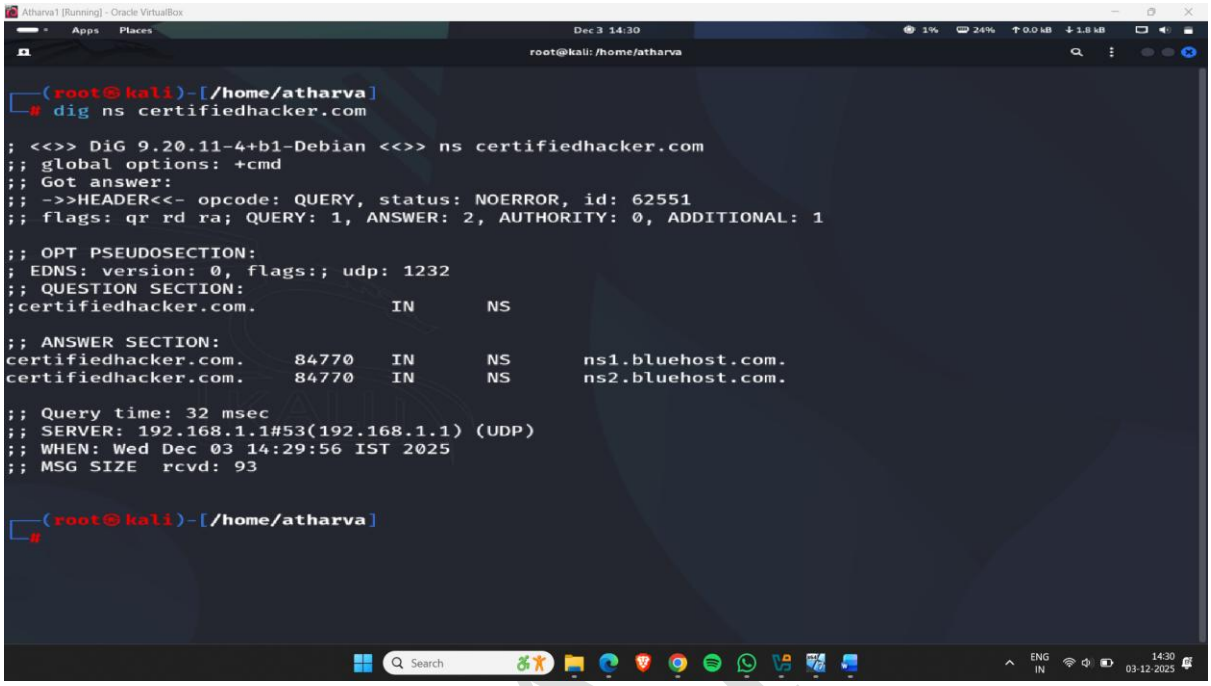


Figure 2

The above command retrieves information about all the DNS name servers of the target domain and displays it in the ANSWER SECTION, as shown in the screenshot.

2)Run dig @[NameServer] [Target Domain] axfr command (here, the name server is ns1.bluehost.com and the target domain is www.certifiedhacker.com).

Note: In this command, axfr retrieves zone information.

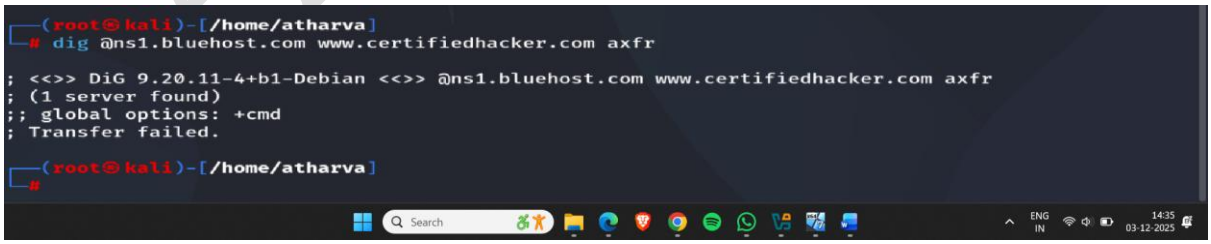


Figure 3

The result appears, displaying that the server is available, but that the Transfer failed., as shown in the screenshot

DNS Enumeration on windows:

- Execute command nslookup.
- Execute command set querytype=soa.
- Type the target domain certifiedhacker.com and press Enter.
- The result appears, displaying information about the target domain such as the primary name server and responsible mail addr, as shown in the screenshot.
- Execute command Is -d [Name Server] (here, the name is ns1.bluehost.com) as shown in the screenshot.

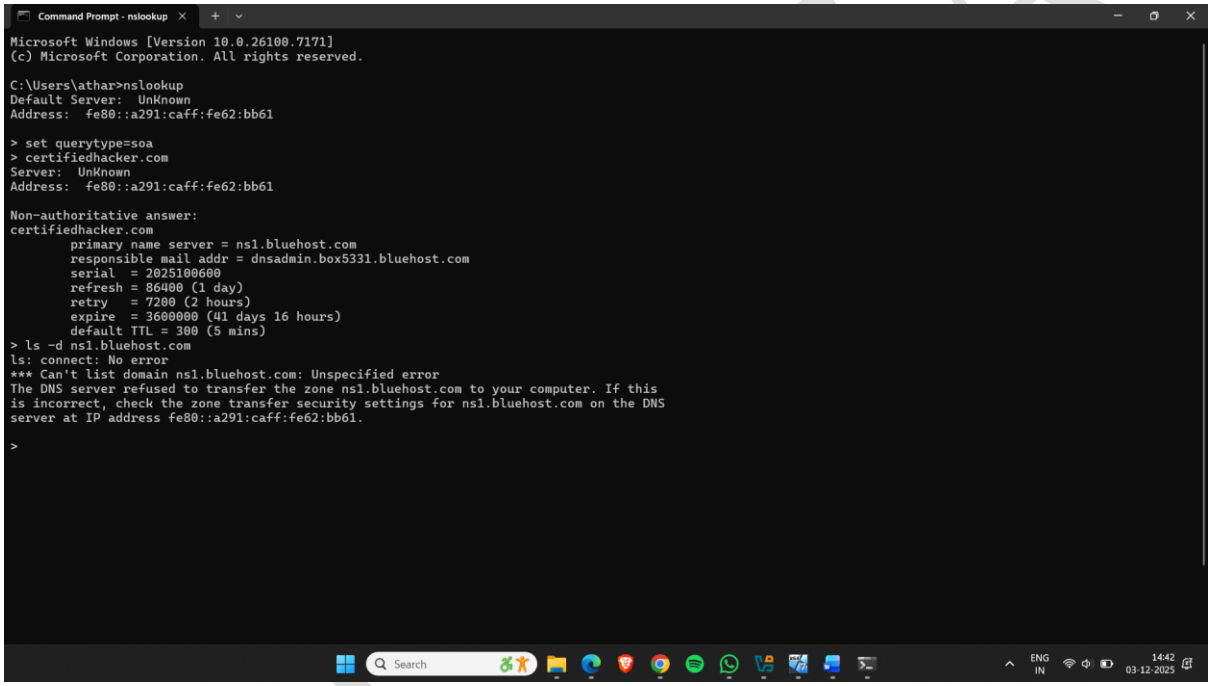


Figure 4

DNS Enumeration Using Hacker Target Website

- Step 1 : open Browser and search hackertarget
- Step 2 : click the first website
- Step 3 : click on Tools and then click on DNS lookup
- Step 4 : provide a domain name and click on get the DNS record
-

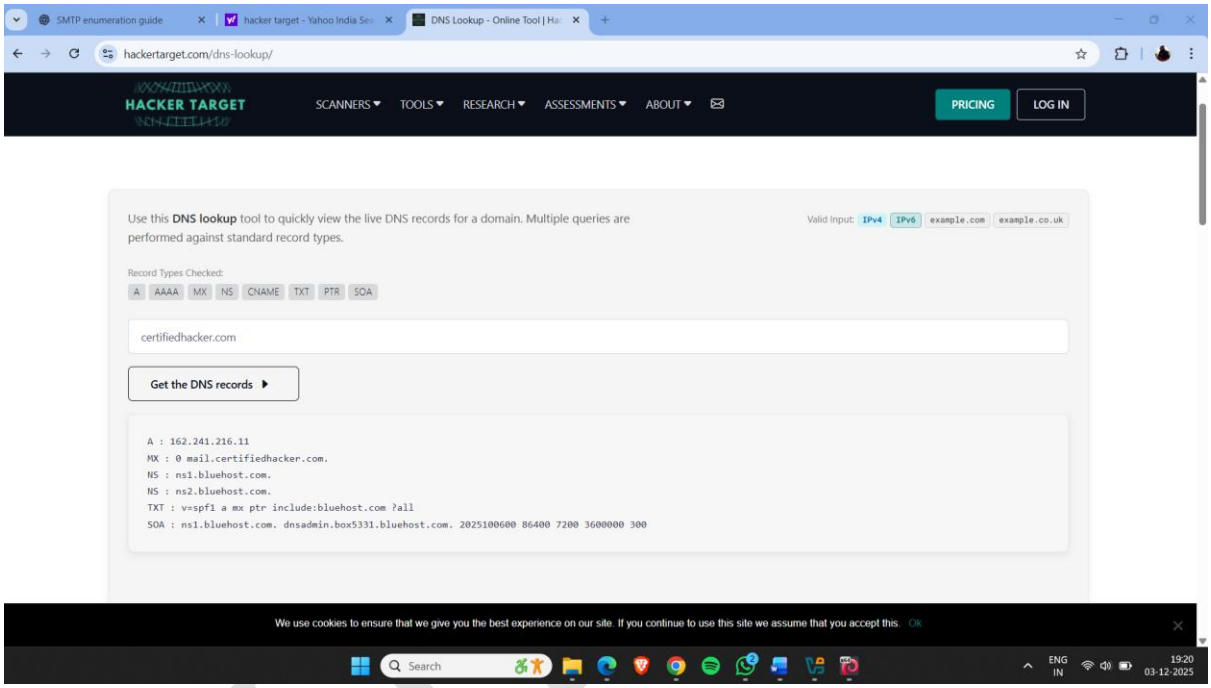


Figure 5

SMTP Enumeration

SMTP enumeration determines a valid list of user accounts on the SMTP server.

The Simple Mail Transfer Protocol (SMTP) is an internet standard based communication protocol for electronic mail transmission. Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail exchange (MX) servers to direct mail via DNS. It runs on TCP port 25, 2525, or 587.

SMTP (Simple Mail Transfer Protocol) commonly runs on ports:

- TCP 25
- TCP 465 (SMTPS)
- TCP 587 (Submission)

SMTP enumeration helps you find:

- Valid usernames (VRFY, EXPN, RCPT TO)
- Mail server software & version
- Internal domain names
- Possible misconfigurations
- Attack surface for phishing/social engineering simulations

To secure SMTP servers:

- Disable VRFY and EXPN commands
- Enable SMTP authentication
- Use TLS (ports 465/587)
- Enable greylisting
- Deploy rate limiting
- Configure SPF, DKIM, DMARC