# Lab 5: Perform DNS Enumeration

**Lab Scenario**

As a professional ethical hacker or penetration tester, the next step after NFS enumeration is to perform DNS enumeration. This process yields information such as DNS server names, hostnames, machine names, usernames, IP addresses, and aliases assigned within a target domain.

**Lab Objectives**

- Perform DNS enumeration using zone transfer

**Overview of DNS Enumeration**

DNS enumeration techniques are used to obtain information about the DNS servers and network infrastructure of the target organization. DNS enumeration can be performed using the following techniques:

- Zone transfer

Task 1: Perform DNS Enumeration using Zone Transfer

DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. In most cases, the DNS server maintains a spare or secondary server for redundancy, which holds all information stored in the main server.

If the DNS transfer setting is enabled on the target DNS server, it will give DNS information; if not, it will return an error saying it has failed or refuses the zone transfer.

Here, we will perform DNS enumeration through zone transfer by using the dig (Linux-based systems) and nslookup (Windows-based systems) utilities.

1. We will begin with DNS enumeration of Linux DNS servers. Click Parrot Security to switch to the **Parrot Security** machine and login with **attacket/toor**.
2. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

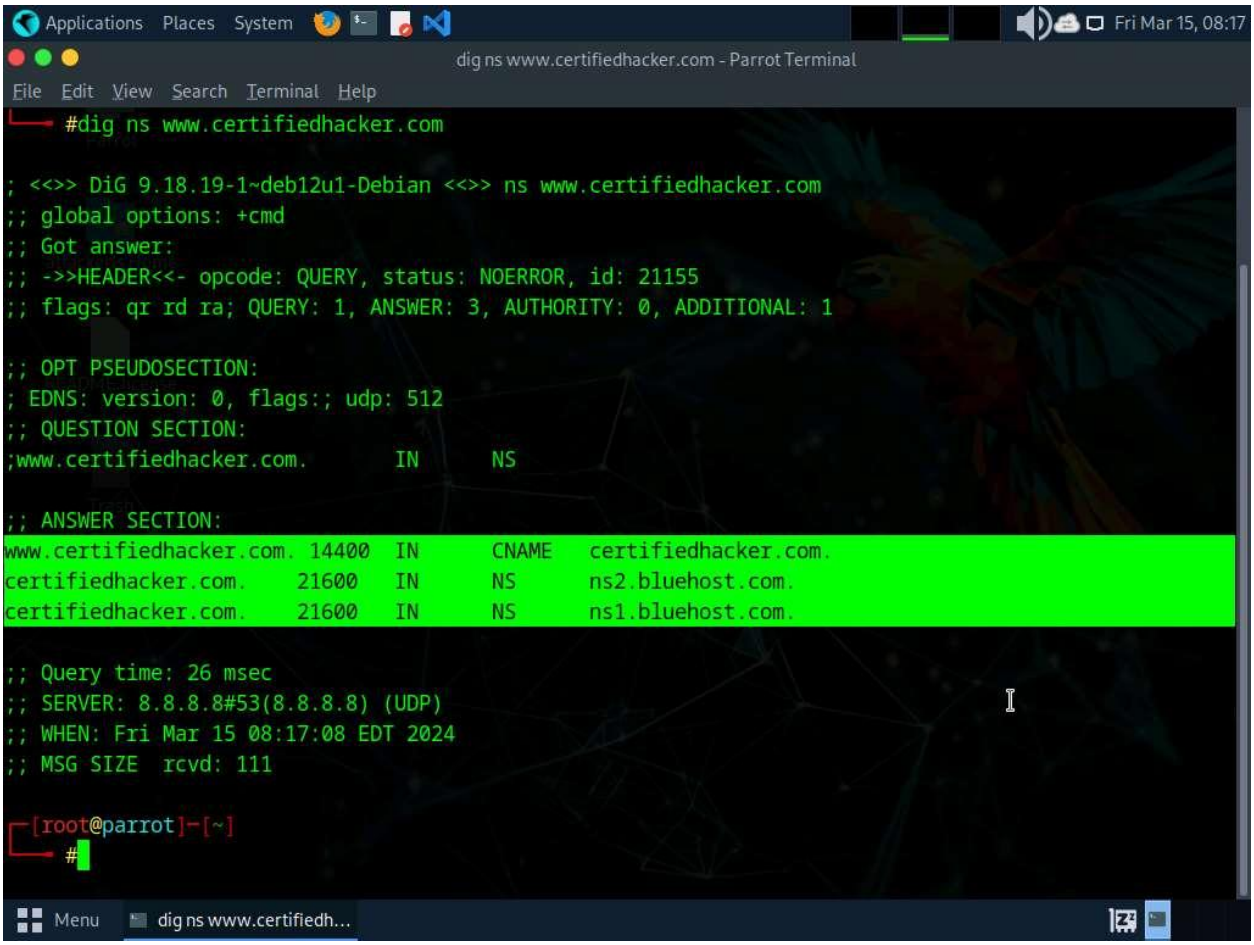
The password that you type will not be visible.

3. Now, run **cd** command to jump to the root directory.
4. Run **dig ns [Target Domain]** command (here, the target domain is **www.certifiedhacker.com**).

In this command, **ns** returns name servers in the result

5. 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.

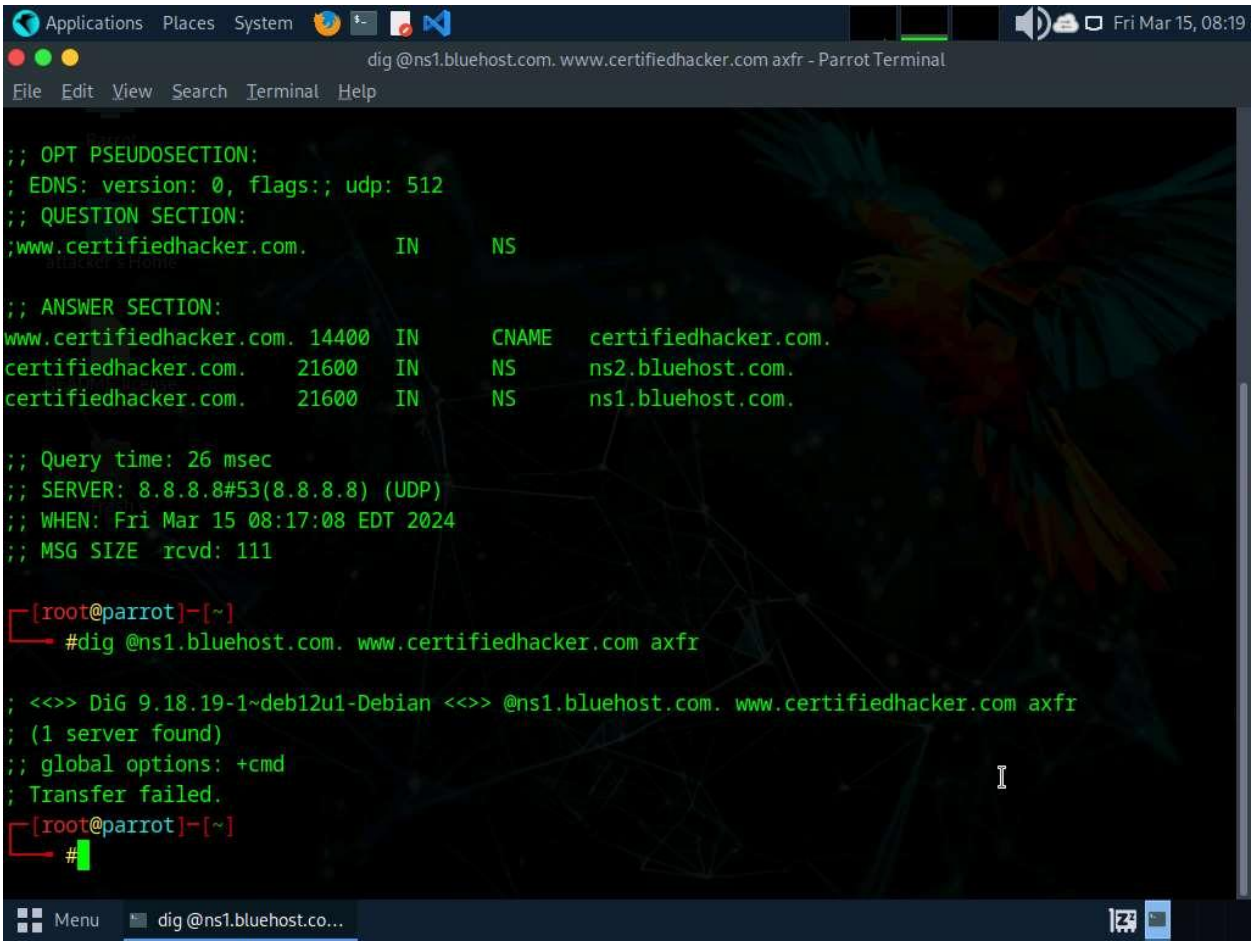
On Linux-based systems, the dig command is used to query the DNS name servers to retrieve information about target host addresses, name servers, mail exchanges, etc.




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

In this command, **axfr** retrieves zone information.

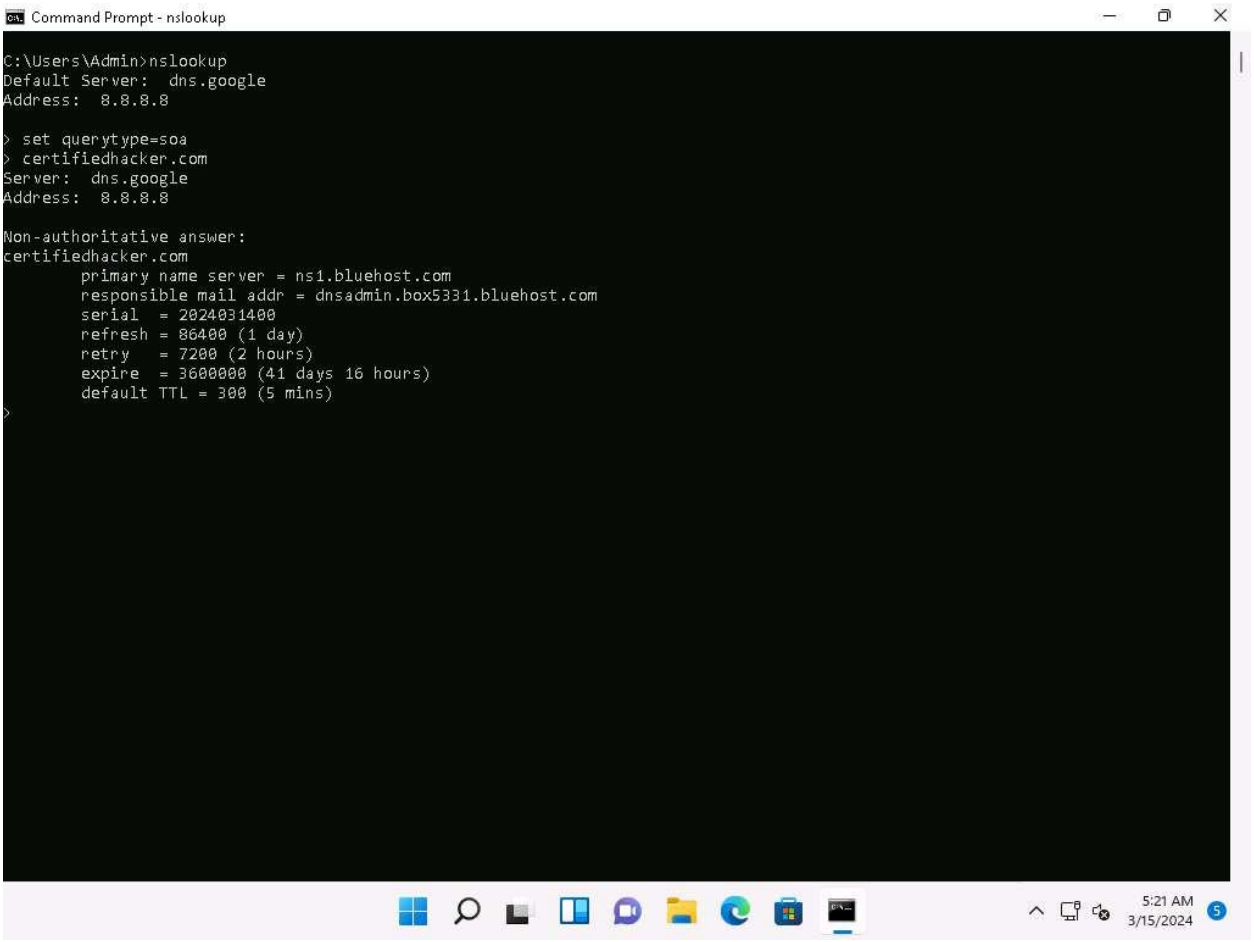
7. The result appears, displaying that the server is available, but that the **Transfer failed**., as shown in the screenshot.




8. After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. here, zone transfers are not allowed for the target domain; this is why the command resulted in the message: Transfer failed. A penetration tester should attempt DNS zone transfers on different domains of the target organization.
9. Now, we will perform DNS enumeration on Windows DNS servers.
10. Click Windows 11 to switch to the **Windows 11** machine.
11. Click windows **Search** icon ( ) on the **Desktop**. Search for **cmd** in the search field, the **Command Prompt** appears in the results, click **Open** to launch it.
12. The **Command Prompt** window appears; execute command **nslookup**.
13. In the nslookup **interactive** mode, execute command **set querytype=soa**.
14. Type the target domain **certifiedhacker.com** and press **Enter**. This resolves the target domain information.

set **querytype=soa** sets the query type to SOA (Start of Authority) record to retrieve administrative information about the DNS zone of the target domain **certifiedhacker.com**.

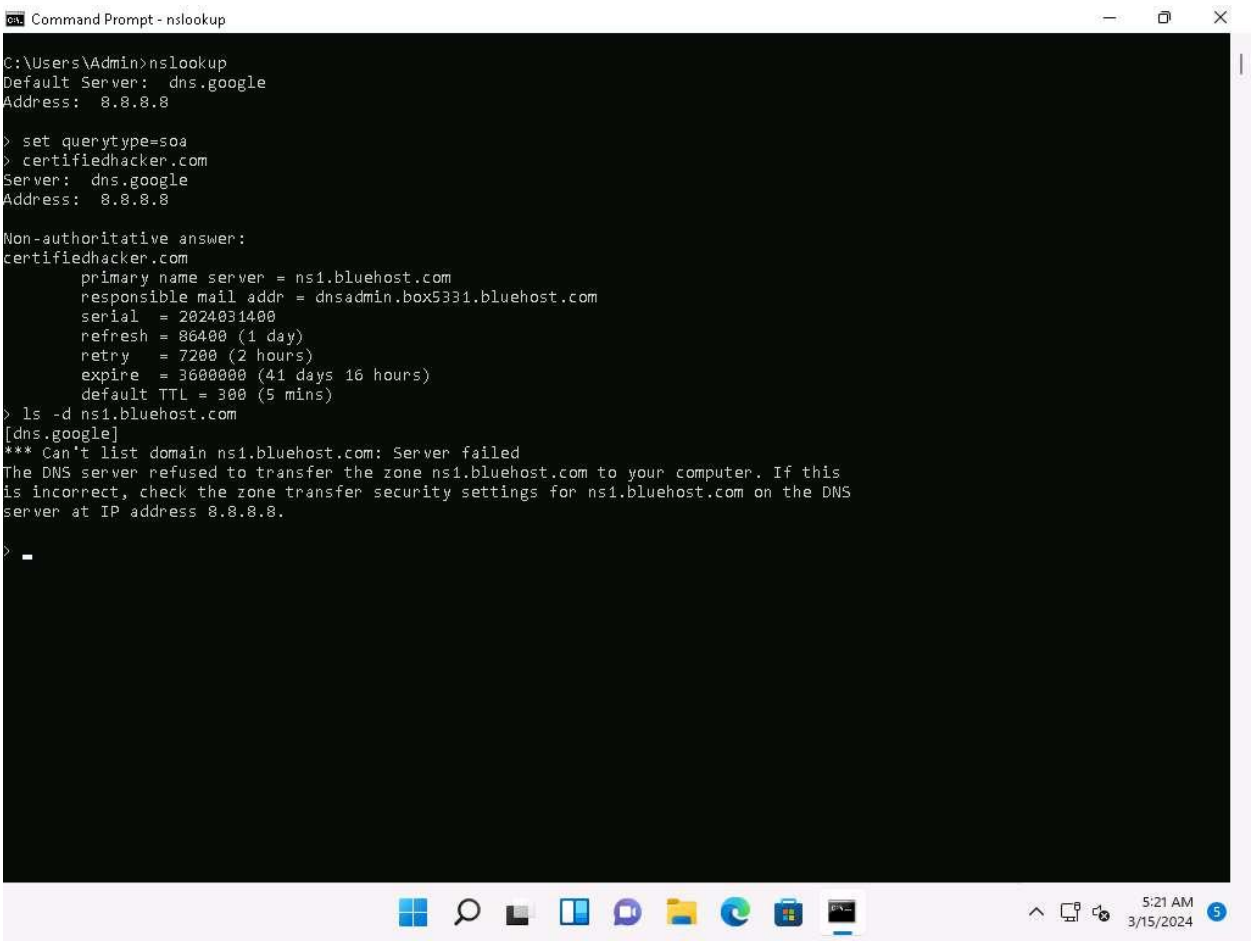
15. The result appears, displaying information about the target domain such as the **primary name server** and **responsible mail addr**, as shown in the screenshot.




16. In the **nslookup** interactive mode, execute command **ls -d [Name Server]** (here, the name is **ns1.bluehost.com**).

In this command, **ls -d** requests a zone transfer of the specified name server.

17. The result appears, displaying that the DNS server refused the zone transfer, as shown in the screenshot.




18. After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. Here, the zone transfer was refused for the target domain. A penetration tester should attempt DNS zone transfers on different domains of the target organization.
19. This concludes the demonstration of performing DNS zone transfer using dig and nslookup commands.
20. Close all open windows and document all the acquired information.

**Question 4.5.1.1**

Can you perform zone transfer on the primary host of certifiedhacker.com? (Yes/No)

**Question 4.5.1.2**

Perform DNS enumeration and find the “responsible mail address” for the domain certifiedhacker.com.