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
* Perform DNS enumeration using DNSSEC zone walking

**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
* DNS cache snooping
* DNSSEC zone walking

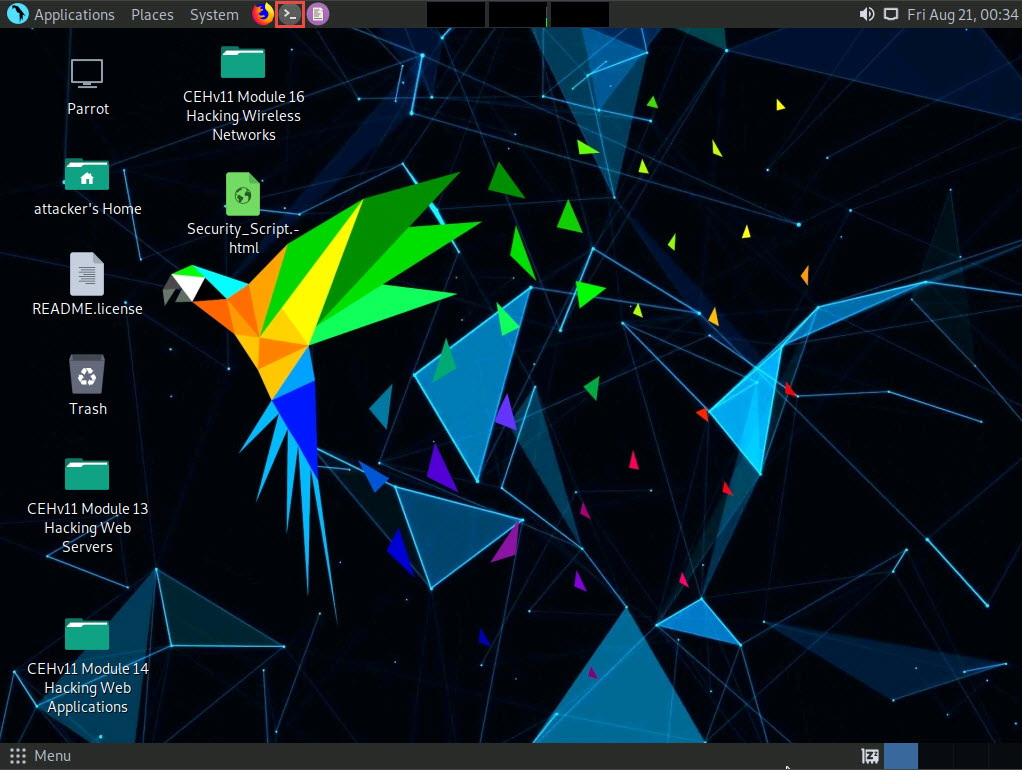
Task 1: Perform DNS Enumeration using Zone Transfer

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) tool.

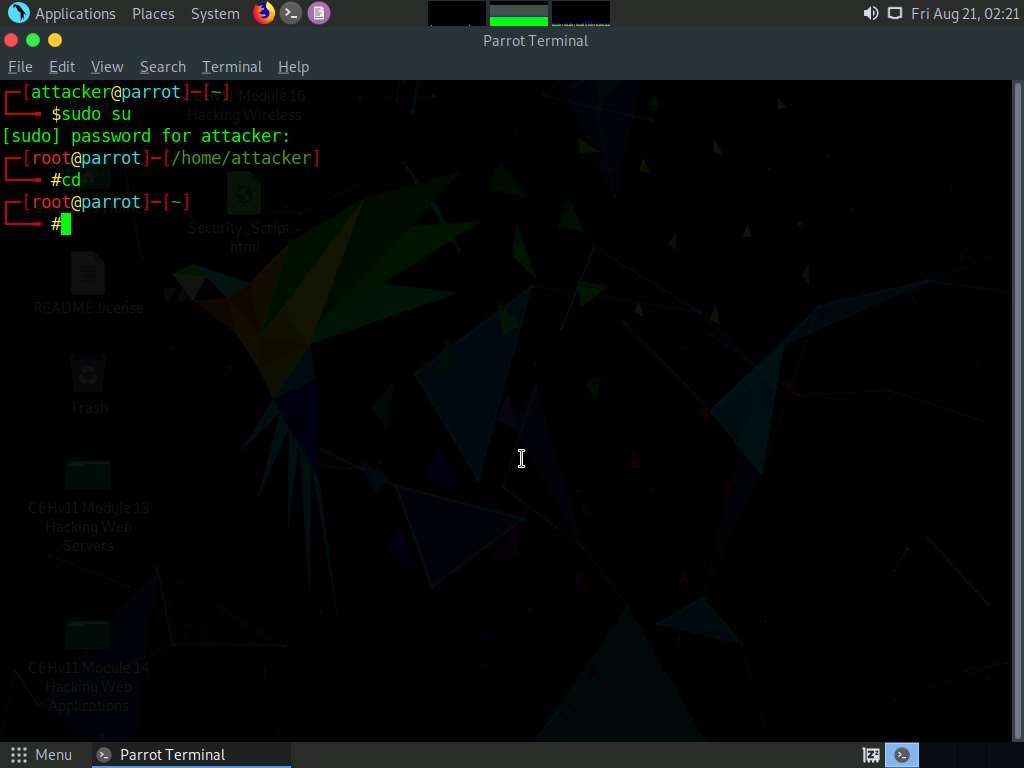
1. We will begin with DNS enumeration of Linux DNS servers.
2. Click [Parrot Security](https://labclient.labondemand.com/Instructions/fbc14e54-d7e0-48c8-a161-917c8a669df5?rc=10) to switch to the **Parrot Security** machine.
3. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** window to open a **Terminal** window.



1. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
2. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

1. Now, type **cd** and press **Enter** to jump to the root directory.

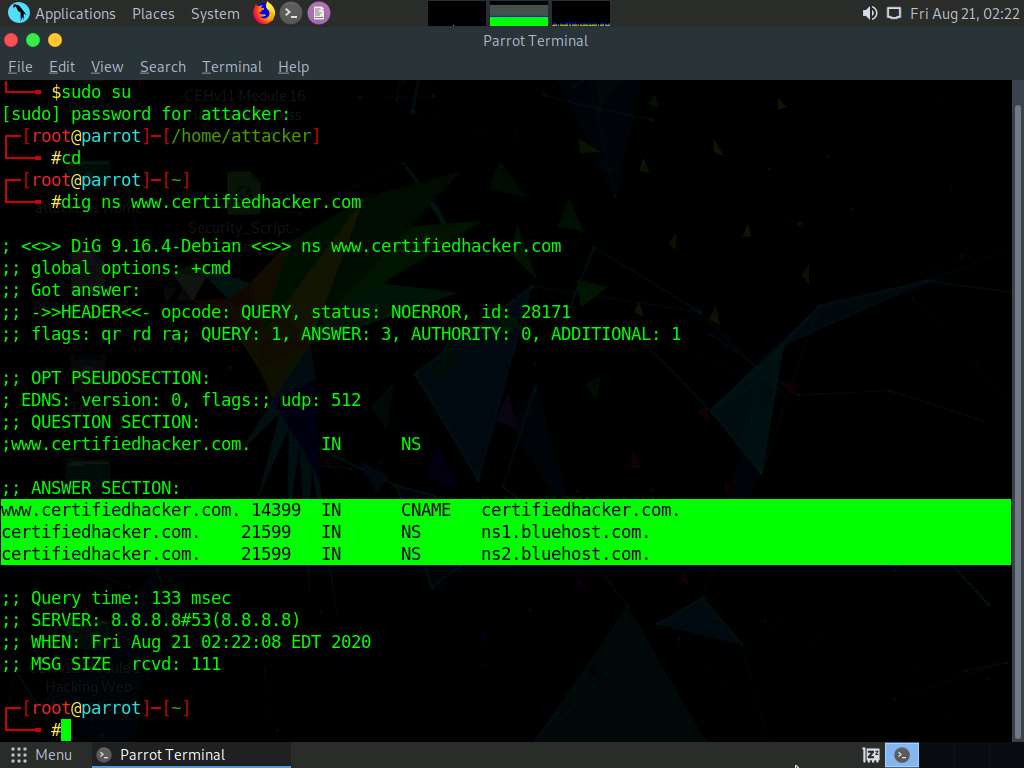


1. A **Parrot Terminal** window appears. In the terminal window, type **dig ns [Target Domain]** (in this case, the target domain is **www.certifiedhacker.com**); press **Enter**.

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

1. 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.

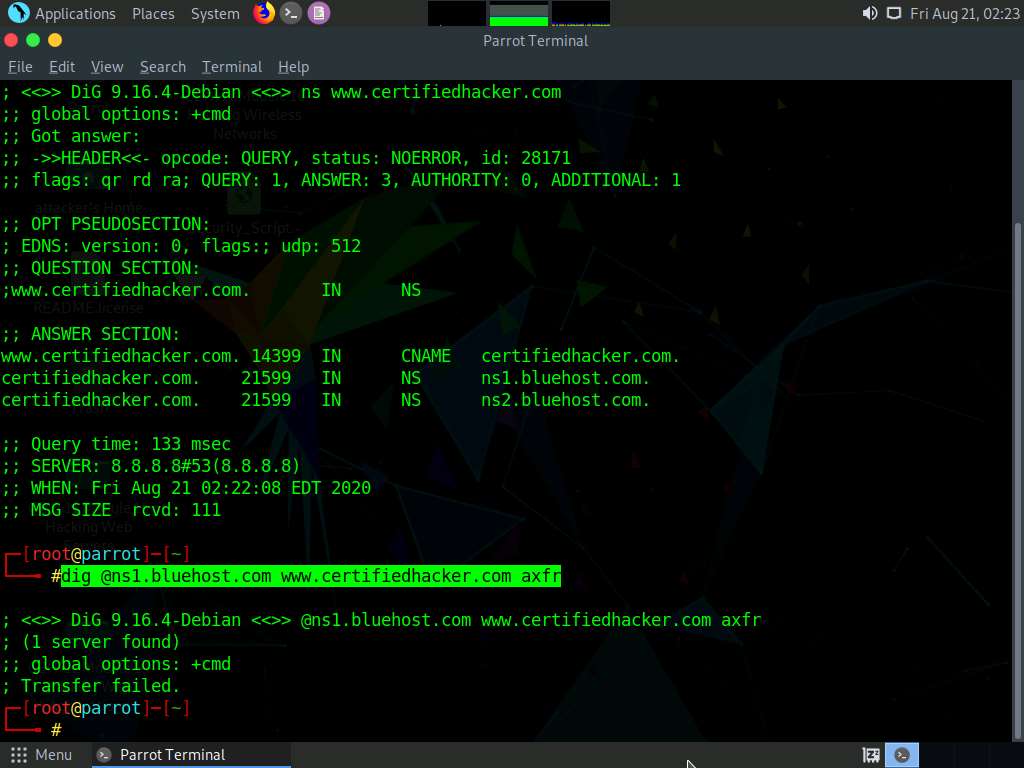
On Linux-based systems, the dig command is used to query the DNS name servers to retrieve information about target host addresses, name servers, mail exchanges, etc.



1. In the terminal window type **dig @[[NameServer]] [[Target Domain]] axfr** (in this example, the name server is **ns1.bluehost.com** and the target domain is **www.certifiedhacker.com**); press **Enter**.

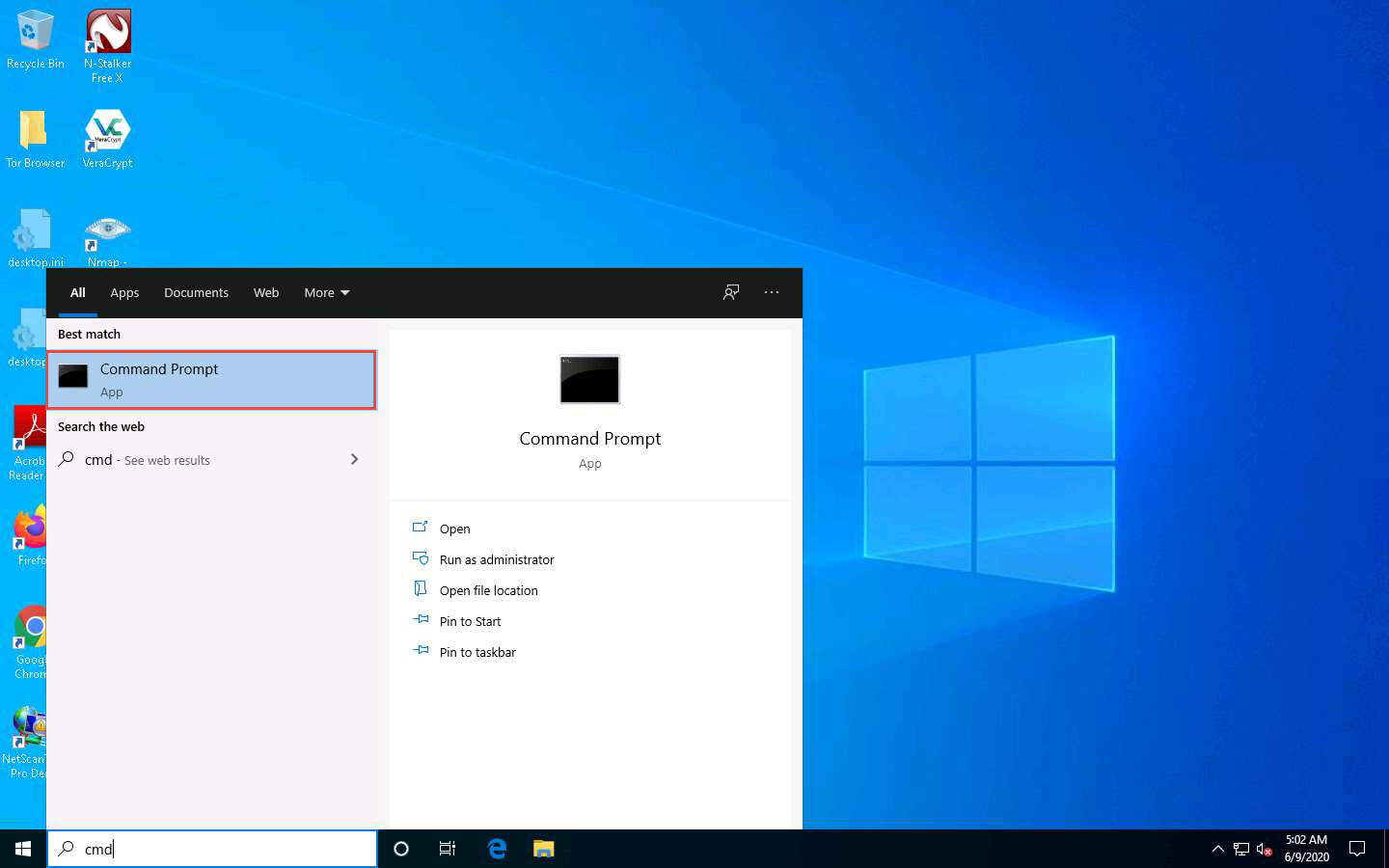
In this command, **axfr** retrieves zone information.

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



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. In this case, 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.

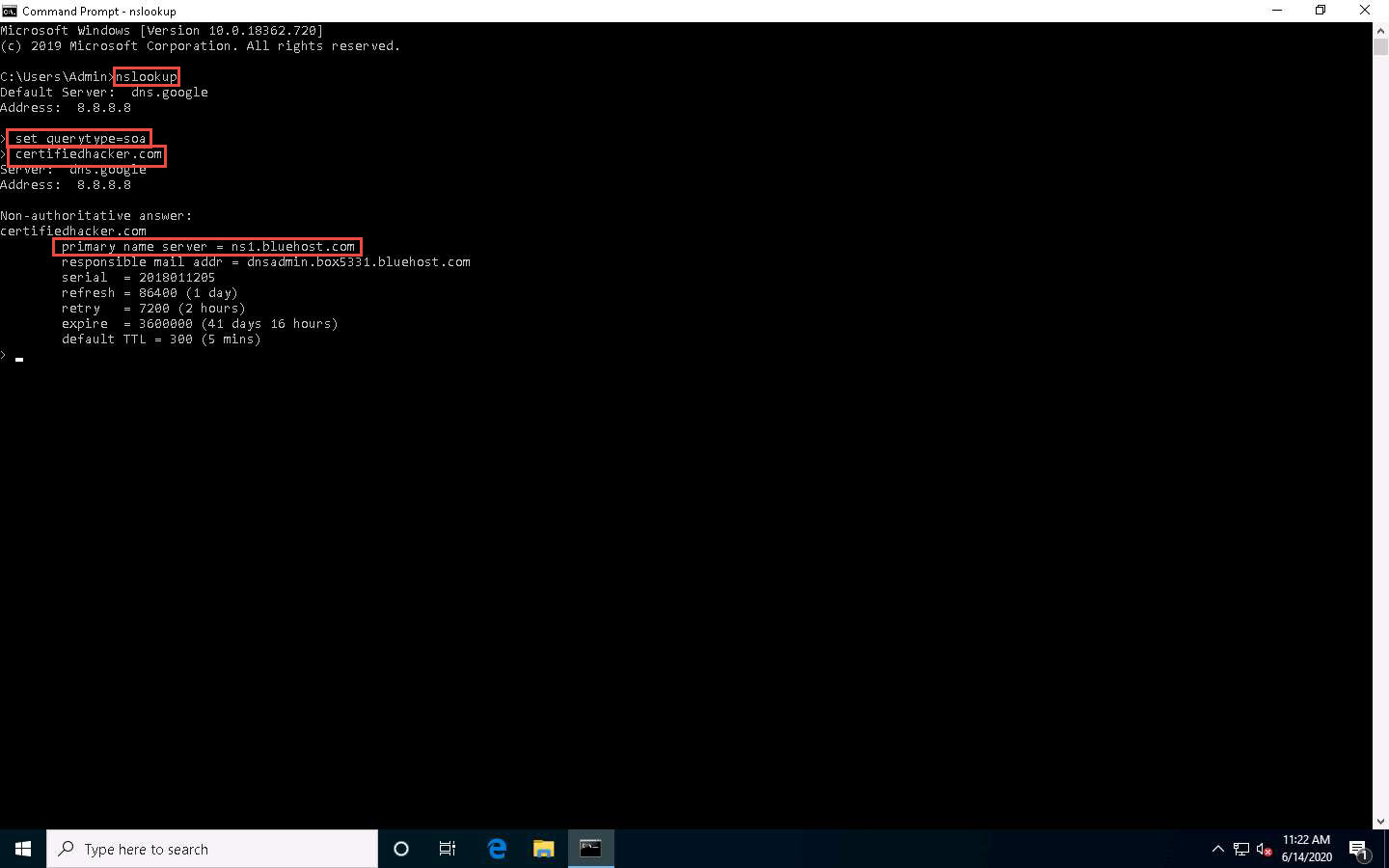
1. We now move on to DNS enumeration of Windows DNS servers.
2. Click [Windows 10](https://labclient.labondemand.com/Instructions/fbc14e54-d7e0-48c8-a161-917c8a669df5?rc=10) to switch to the **Windows 10** machine.
3. Click **Start** at the bottom of **Desktop**, click **Type here to search**, and type **cmd**; click **Command Prompt**.



1. The **Command Prompt** window appears; type **nslookup**, and press **Enter**.
2. In the nslookup **interactive** mode, type **set querytype=soa**, and press **Enter**.
3. 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**.

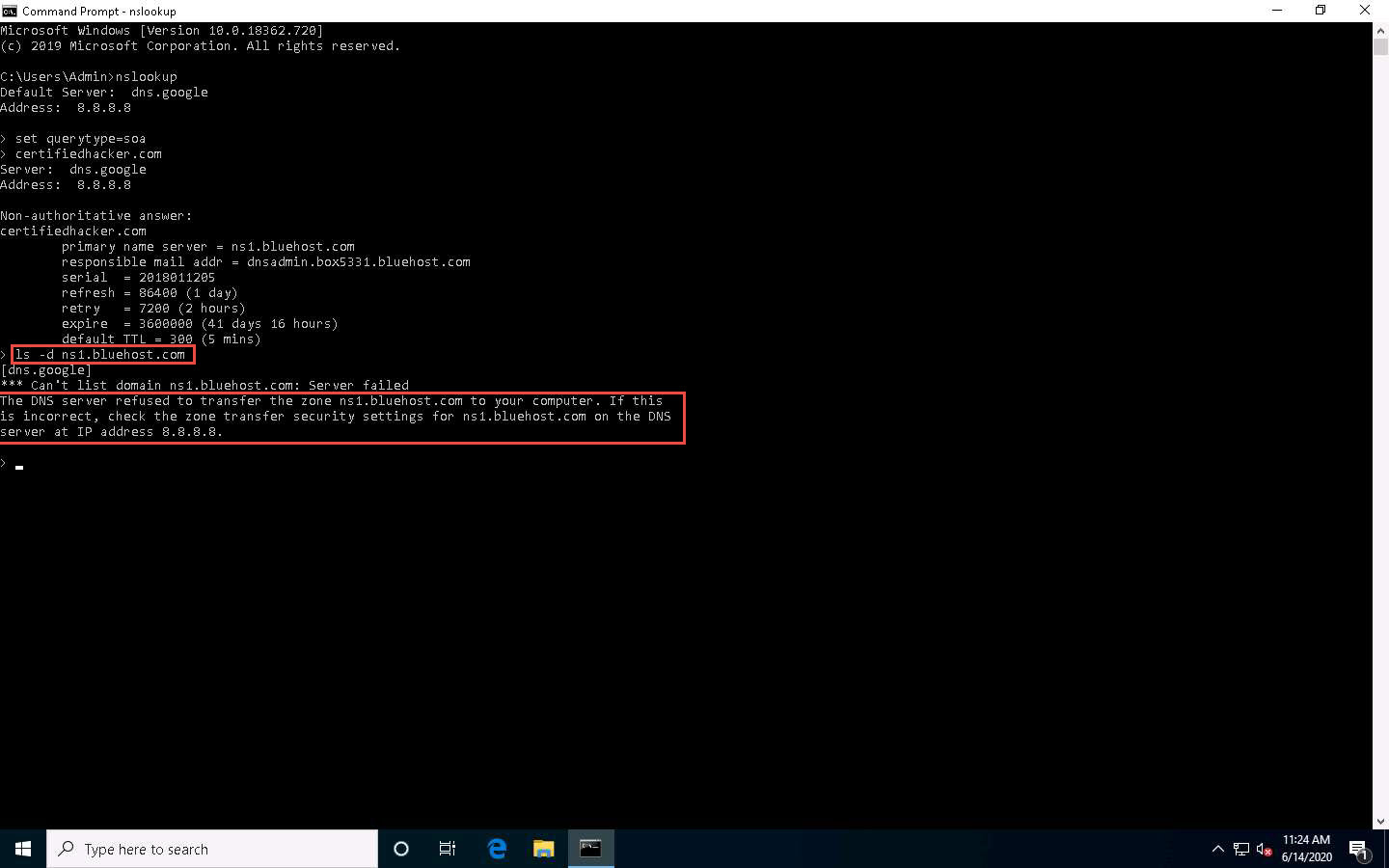
1. The result appears, displaying information about the target domain such as the **primary name server** and **responsible mail addr**, as shown in the screenshot.



1. In the **nslookup** interactive mode, type **ls -d [Name Server]** (in this example, the name is **ns1.bluehost.com**) and press **Enter**, as shown in the screenshot.

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

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



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. In this case, the zone transfer was refused for the target domain. A penetration tester should attempt DNS zone transfers on different domains of the target organization.

1. This concludes the demonstration of performing DNS zone transfer using dig and nslookup commands.
2. Close all open windows and document all the acquired information.

Task 2: Perform DNS Enumeration using DNSSEC Zone Walking

DNSSEC zone walking is a DNS enumeration technique that is used to obtain the internal records of the target DNS server if the DNS zone is not properly configured. The enumerated zone information can assist you in building a host network map.

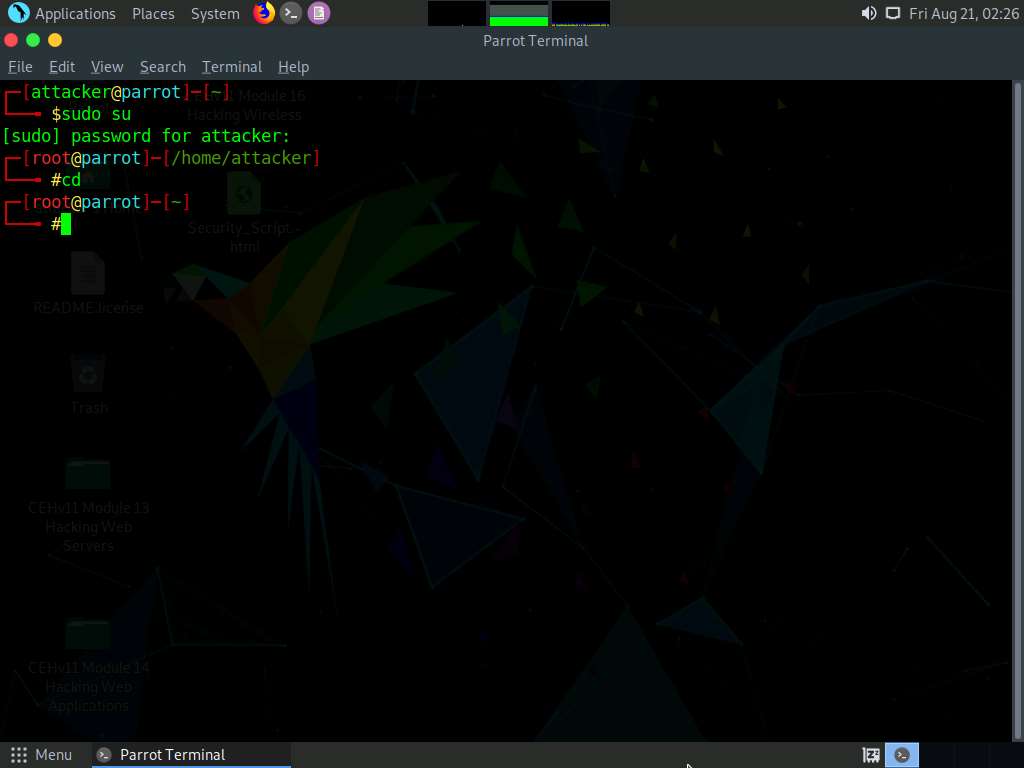
There are various DNSSEC zone walking tools that can be used to enumerate the target domain’s DNS record files.

Here, we will use the DNSRecon tool to perform DNS enumeration through DNSSEC zone walking.

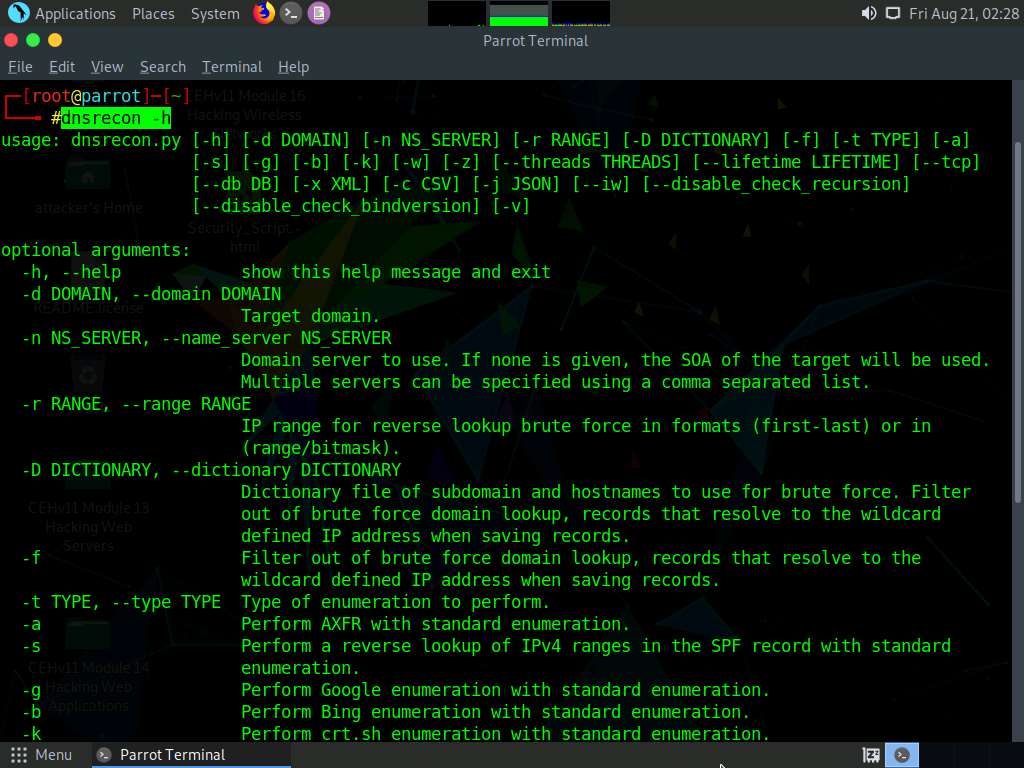
1. Click [Parrot Security](https://labclient.labondemand.com/Instructions/fbc14e54-d7e0-48c8-a161-917c8a669df5?rc=10) to switch to the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to open a **Terminal** window.
2. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

1. Now, type **cd** and press **Enter** to jump to the root directory.



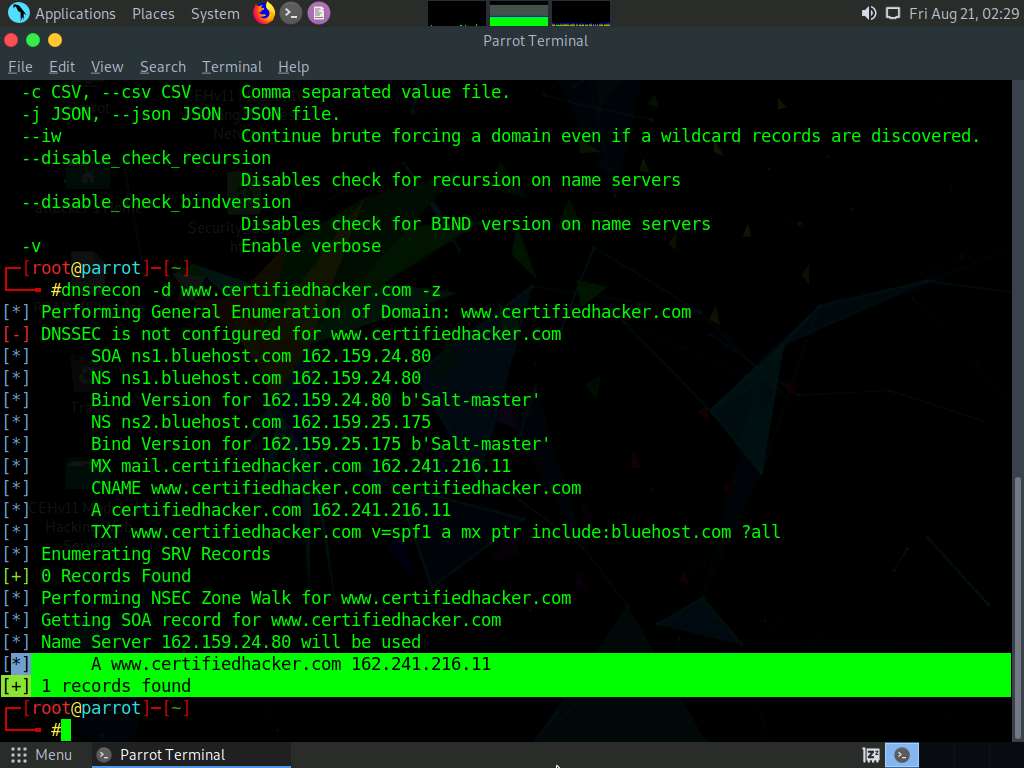
1. A **Parrot Terminal** window appears. Type **dnsrecon -h** and press **Enter** to view all the available options in the DNSRecon tool.



1. Type **dnsrecon -d [Target domain] -z** (in this example, the target domain is **www.certifiedhacker.com**); press **Enter**.

In this command, **-d** specifies the target domain and **-z** specifies that the DNSSEC zone walk be performed with standard enumeration.

1. The result appears, displaying the enumerated DNS records for the target domain. In this case, DNS record file **A** is enumerated, as shown in the screenshot.



Using the DNSRecon tool, the attacker can enumerate general DNS records for a given domain (MX, SOA, NS, A, AAAA, SPF, and TXT). These DNS records contain digital signatures based on public-key cryptography to strengthen authentication in DNS.

1. This concludes the demonstration of performing DNS Enumeration using DNSSEC zone walking.
2. You can also use other DNS enumeration tools such as **LDNS** (https://www.nlnetlabs.nl), **nsec3map** (https://github.com), **nsec3walker** (https://dnscurve.org), and **DNSwalk** (https://github.com) to perform DNS enumeration on the target domain.
3. Close all open windows and document all the acquired information.