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

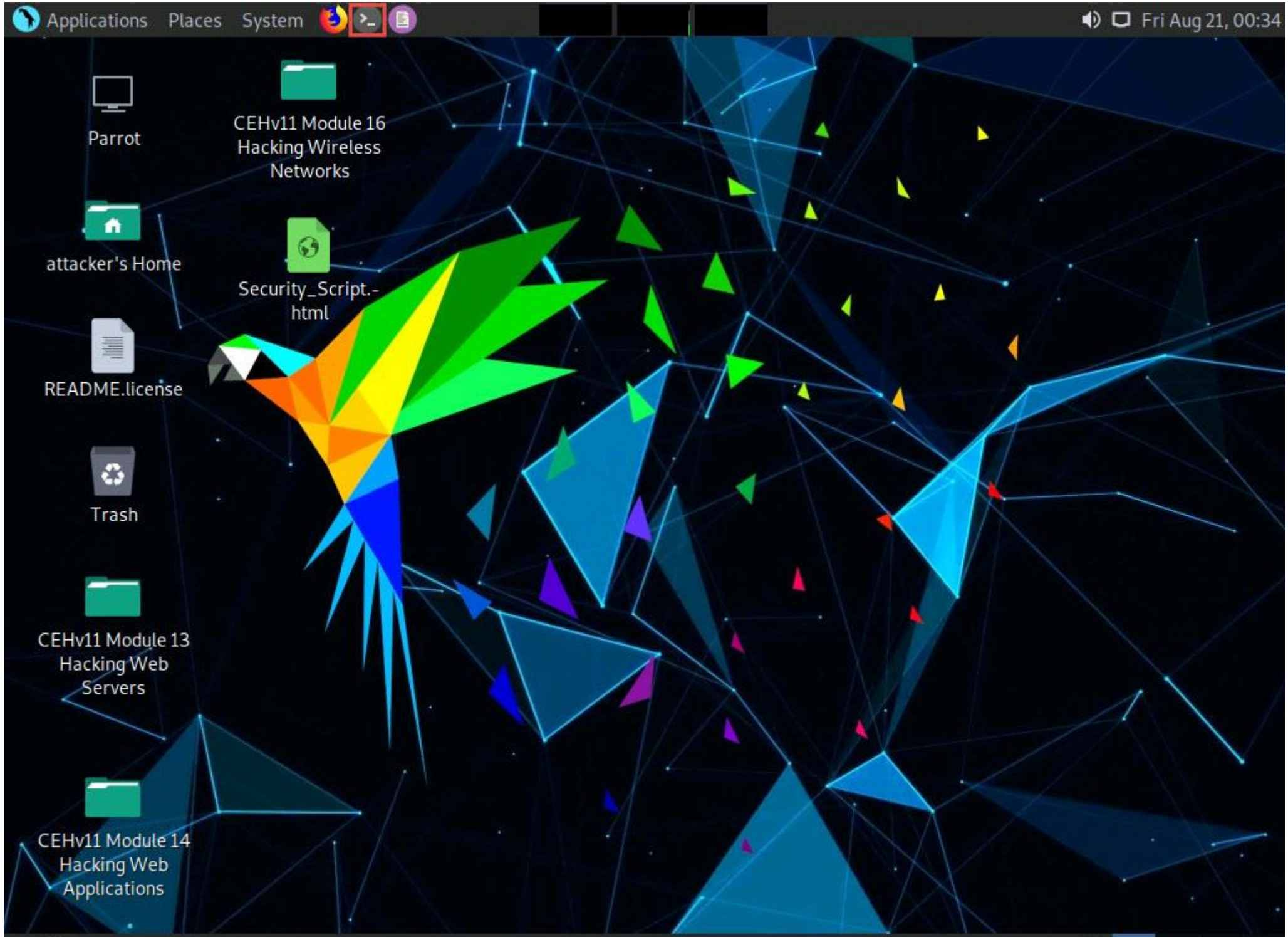
DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. In most cases, the DNS server maintains a spare or secondary server for redundancy, which holds all information stored in the main server.

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 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.


Applications
Places
System
Fri Aug 21, 00:34
Parrot
CEHv11 Module 16 Hacking Wireless Networks
attacker's Home
Security_Script.-html
README.license
Trash
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications

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

The password that you type will not be visible.

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

Applications Places System Fri Aug 21, 02:21

Parrot Terminal

File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

7. ☐ 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

8. ☐ 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.

Applications Places System Fri Aug 21, 02:22

Parrot Terminal

File Edit View Search Terminal Help

```
└─$sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└─#cd
┌─[root@parrot]─[~]
└─#dig ns www.certifiedhacker.com

; <<>> DiG 9.16.4-Debian <<>> ns www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28171
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com.       IN      NS

;; ANSWER SECTION:
www.certifiedhacker.com. 14399  IN      CNAME   certifiedhacker.com.
certifiedhacker.com.    21599   IN      NS      ns1.bluehost.com.
certifiedhacker.com.    21599   IN      NS      ns2.bluehost.com.

;; Query time: 133 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Aug 21 02:22:08 EDT 2020
;; MSG SIZE  rcvd: 111

┌─[root@parrot]─[~]
└─#
```

9. 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.

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

Applications Places System Fri Aug 21, 02:23

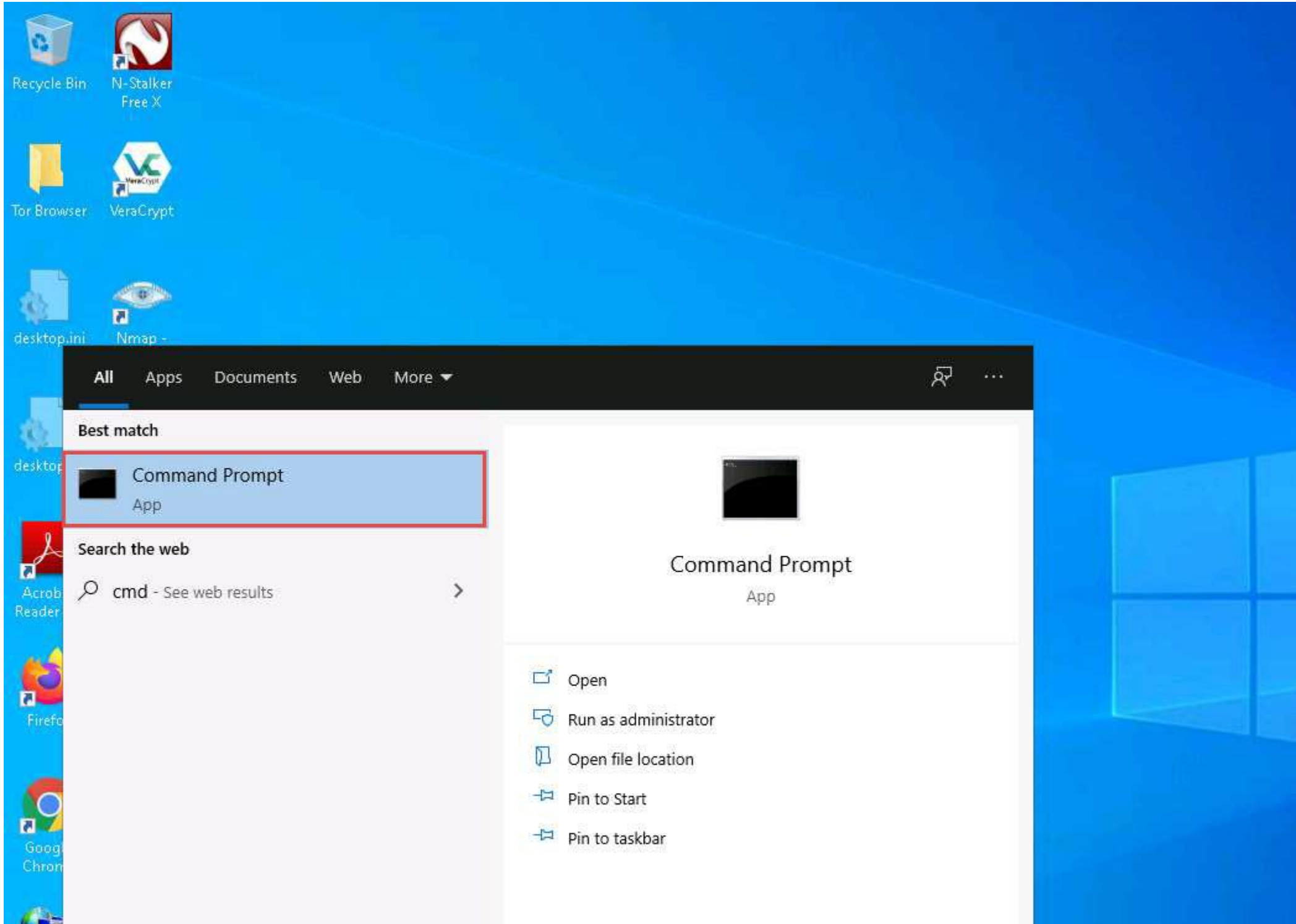
Parrot Terminal

File Edit View Search Terminal Help

```
; <<>> DiG 9.16.4-Debian <<>> ns www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28171
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com.       IN      NS

;; ANSWER SECTION:
www.certifiedhacker.com. 14399  IN      CNAME   certifiedhacker.com.
certifiedhacker.com.    21599   IN      NS      ns1.bluehost.com.
certifiedhacker.com.    21599   IN      NS      ns2.bluehost.com.

;; Query time: 133 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Aug 21 02:22:08 EDT 2020
;; MSG SIZE  rcvd: 111

┌─[root@parrot]─[~]
└──╼ #dig @ns1.bluehost.com www.certifiedhacker.com axfr

; <<>> DiG 9.16.4-Debian <<>> @ns1.bluehost.com www.certifiedhacker.com axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.
┌─[root@parrot]─[~]
└──╼ #
```

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.

11. ☐ We now move on to DNS enumeration of Windows DNS servers.
12. ☐ Click Windows 10 to switch to the **Windows 10** machine.
13. ☐ Click **Start** at the bottom of **Desktop**, click **Type here to search**, and type **cmd**; click **Command Prompt**.


Recycle Bin
N-Stalker Free X
Tor Browser
VeraCrypt
desktop.ini
Nmap -
All
Apps
Documents
Web
More
Best match
Command Prompt
App
Search the web
cmd - See web results
Command Prompt
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar

14. ☐ The **Command Prompt** window appears; type **nslookup**, and press **Enter**.
15. ☐ In the nslookup **interactive** mode, type **set querytype=soa**, and press **Enter**.
16. ☐ 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**.

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

Command Prompt - nslookup

```
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set querytype=soa
> certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
certifiedhacker.com
        primary name server = ns1.bluehost.com
        responsible mail addr = dnsadmin.box5331.bluehost.com
        serial  = 2018011205
        refresh = 86400 (1 day)
        retry   = 7200 (2 hours)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)
>
```

18. 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.

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

Command Prompt - nslookup

```
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set querytype=soa
> certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
certifiedhacker.com
        primary name server = ns1.bluehost.com
        responsible mail addr = dnsadmin.box5331.bluehost.com
        serial  = 2018011205
        refresh = 86400 (1 day)
        retry   = 7200 (2 hours)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)
> ls -d ns1.bluehost.com
[dns.google]
*** Can't list domain ns1.bluehost.com: Server failed
The DNS server refused to transfer the zone ns1.bluehost.com to your computer. If this
is incorrect, check the zone transfer security settings for ns1.bluehost.com on the DNS
server at IP address 8.8.8.8.

>
```

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. 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.

20. ☐ This concludes the demonstration of performing DNS zone transfer using dig and nslookup commands.
21. ☐ 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 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.

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

Applications Places System Fri Aug 21, 02:26

Parrot Terminal

File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

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

Applications Places System Fri Aug 21, 02:28

Parrot Terminal

File Edit View Search Terminal Help

```
┌─[root@parrot]─[~]
└──╼ #dnsrecon -h
usage: dnsrecon.py [-h] [-d DOMAIN] [-n NS_SERVER] [-r RANGE] [-D DICTIONARY] [-f] [-t TYPE] [-a]
                   [-s] [-g] [-b] [-k] [-w] [-z] [--threads THREADS] [--lifetime LIFETIME] [--tcp]
                   [--db DB] [-x XML] [-c CSV] [-j JSON] [--iw] [--disable_check_recursion]
                   [--disable_check_bindversion] [-v]

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Target domain.
  -n NS_SERVER, --name_server NS_SERVER
                        Domain server to use. If none is given, the SOA of the target will be used.
                        Multiple servers can be specified using a comma separated list.
  -r RANGE, --range RANGE
                        IP range for reverse lookup brute force in formats (first-last) or in
                        (range/bitmask).
  -D DICTIONARY, --dictionary DICTIONARY
                        Dictionary file of subdomain and hostnames to use for brute force. Filter
                        out of brute force domain lookup, records that resolve to the wildcard
                        defined IP address when saving records.
  -f                    Filter out of brute force domain lookup, records that resolve to the
                        wildcard defined IP address when saving records.
  -t TYPE, --type TYPE  Type of enumeration to perform.
  -a                    Perform AXFR with standard enumeration.
  -s                    Perform a reverse lookup of IPv4 ranges in the SPF record with standard
                        enumeration.
  -g                    Perform Google enumeration with standard enumeration.
  -b                    Perform Bing enumeration with standard enumeration.
  -k                    Perform crt.sh enumeration with standard enumeration.
```

6. 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.

7. 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.

Applications Places System Fri Aug 21, 02:29

Parrot Terminal

File Edit View Search Terminal Help

```
  -c CSV, --csv CSV     Comma separated value file.
  -j JSON, --json JSON  JSON file.
  --iw                  Continue brute forcing a domain even if a wildcard records are discovered.
  --disable_check_recursion
                        Disables check for recursion on name servers
  --disable_check_bindversion
                        Disables check for BIND version on name servers
  -v                    Enable verbose
┌─[root@parrot]─[~]
└──╼ #dnsrecon -d www.certifiedhacker.com -z
[*] Performing General Enumeration of Domain: www.certifiedhacker.com
[-] DNSSEC is not configured for www.certifiedhacker.com
[*]     SOA ns1.bluehost.com 162.159.24.80
[*]     NS ns1.bluehost.com 162.159.24.80
[*]     Bind Version for 162.159.24.80 b'Salt-master'
[*]     NS ns2.bluehost.com 162.159.25.175
[*]     Bind Version for 162.159.25.175 b'Salt-master'
[*]     MX mail.certifiedhacker.com 162.241.216.11
[*]     CNAME www.certifiedhacker.com certifiedhacker.com
[*]     A certifiedhacker.com 162.241.216.11
[*]     TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[+] 0 Records Found
[*] Performing NSEC Zone Walk for www.certifiedhacker.com
[*] Getting SOA record for www.certifiedhacker.com
[*] Name Server 162.159.24.80 will be used
[*]     A www.certifiedhacker.com 162.241.216.11
[+] 1 records found
┌─[root@parrot]─[~]
└──╼ #
```

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.

8. ☐ This concludes the demonstration of performing DNS Enumeration using DNSSEC zone walking.
9. ☐ 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.
10. ☐ Close all open windows and document all the acquired information.