Lab Objectives

- Gather DNS information using nslookup command line utility and online tool

Overview of DNS

DNS considered the intermediary source for any Internet communication. The primary function of DNS is to translate a domain name to IP address and vice-versa to enable human-machine-network-internet communications. Since each device has a unique IP address, it is hard for human beings to memorize all IP addresses of the required application. DNS helps in converting the IP address to a more easily understandable domain format, which eases the burden on human beings.

Task 1: Gather DNS Information using nslookup Command Line Utility and Online Tool

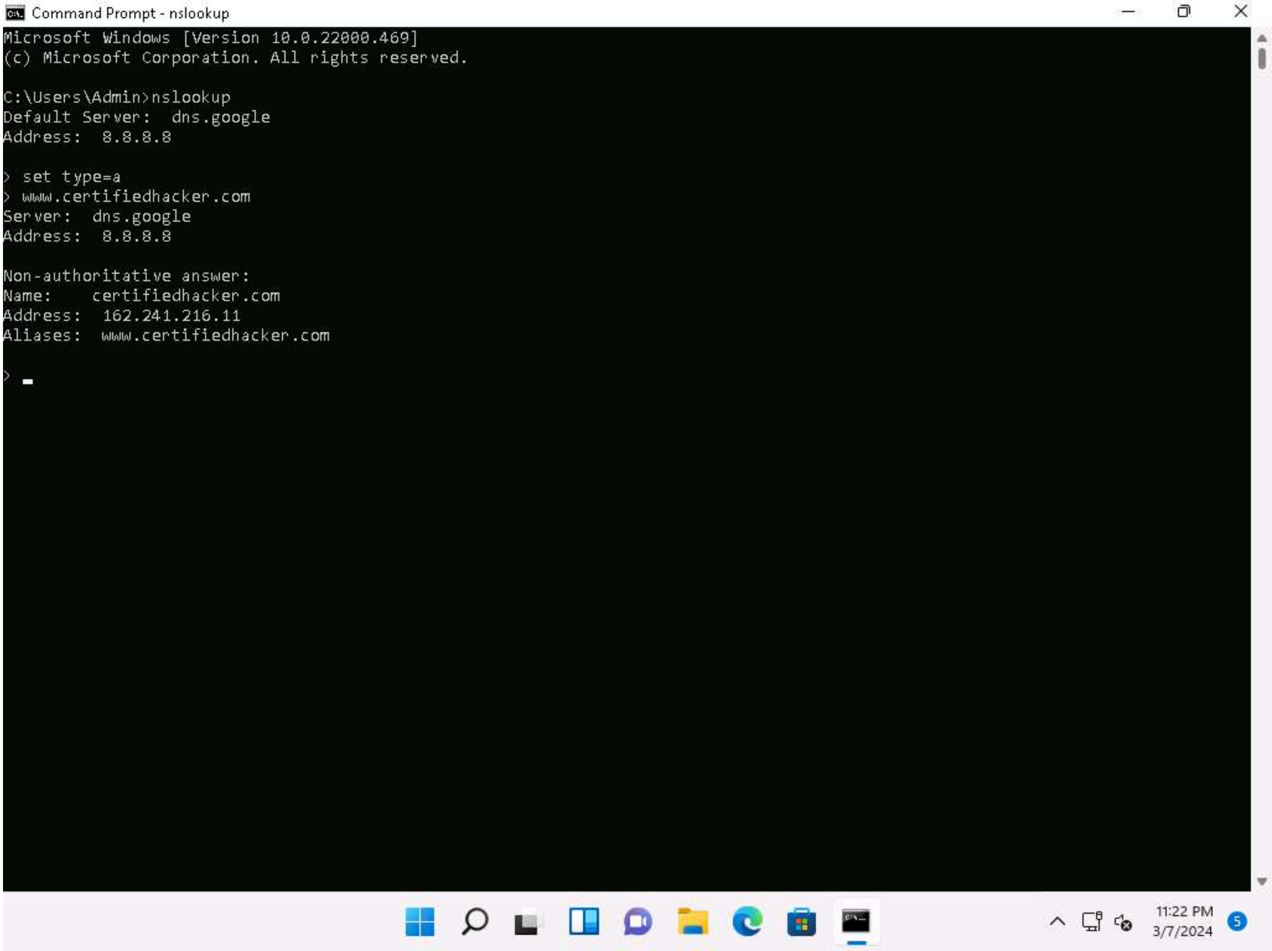
nslookup is a network administration command-line utility, generally used for querying the DNS to obtain a domain name or IP address mapping or for any other specific DNS record. This utility is available both as a command-line utility and web application.

Here, we will perform DNS information gathering about target organizations using the nslookup command-line utility and NSLOOKUP web application.

1. In the **Windows 11** machine, launch a **Command Prompt**, and run **nslookup** command. This displays the default server and its address assigned to the **Windows 11** machine.

2. In the nslookup **interactive** mode, type **set type=a** and press **Enter**. Setting the type as **"a"** configures nslookup to query for the IP address of a given domain.

3. Type the target domain **www.certifiedhacker.com** and press **Enter**. This resolves the IP address and displays the result, as shown in the screenshot.



```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

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

> set type=a
> www.certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  162.241.216.11
Aliases:  www.certifiedhacker.com

> _
```

4. The first two lines in the result are:

   Server: **dns.google** and Address: **8.8.8.8**

   This specifies that the result was directed to the default server hosted on the local machine (**Windows 11**) that resolves your requested domain.

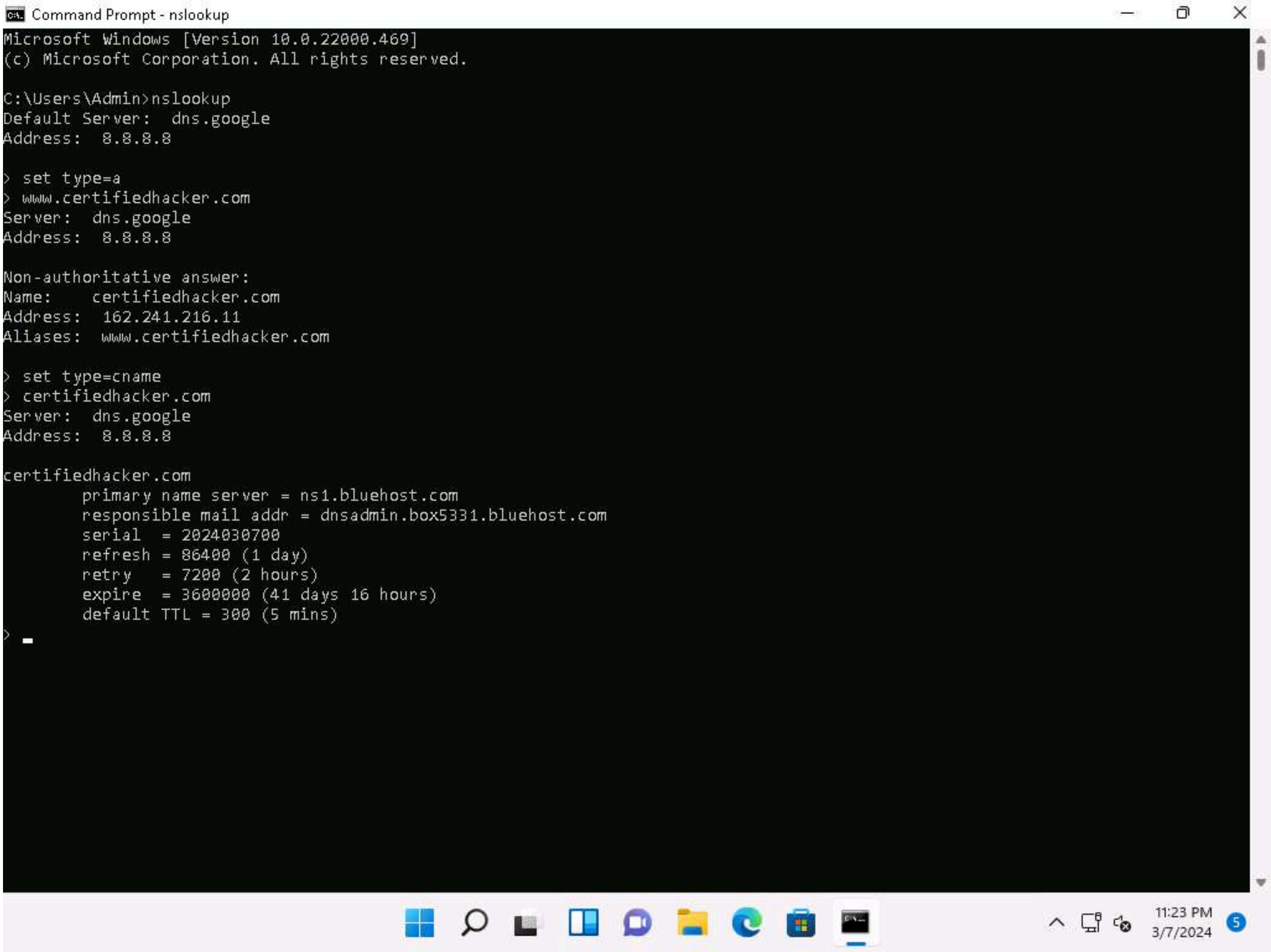
5. Thus, if the response is coming from your local machine's server (Google), but not the server that legitimately hosts the domain **www.certifiedhacker.com**; it is considered to be a non-authoritative answer. Here, the IP address of the target domain **www.certifiedhacker.com** is **162.241.216.11**.

6. Since the result returned is non-authoritative, you need to obtain the domain's authoritative name server.

7. Type **set type=cname** and press **Enter**. The CNAME lookup is done directly against the domain's authoritative name server and lists the CNAME records for a domain.

8. Type **certifiedhacker.com** and press **Enter**.

9. This returns the domain's authoritative name server (**ns1.bluehost.com**), along with the mail server address (**dnsadmin.box5331.bluehost.com**), as shown in the screenshot.

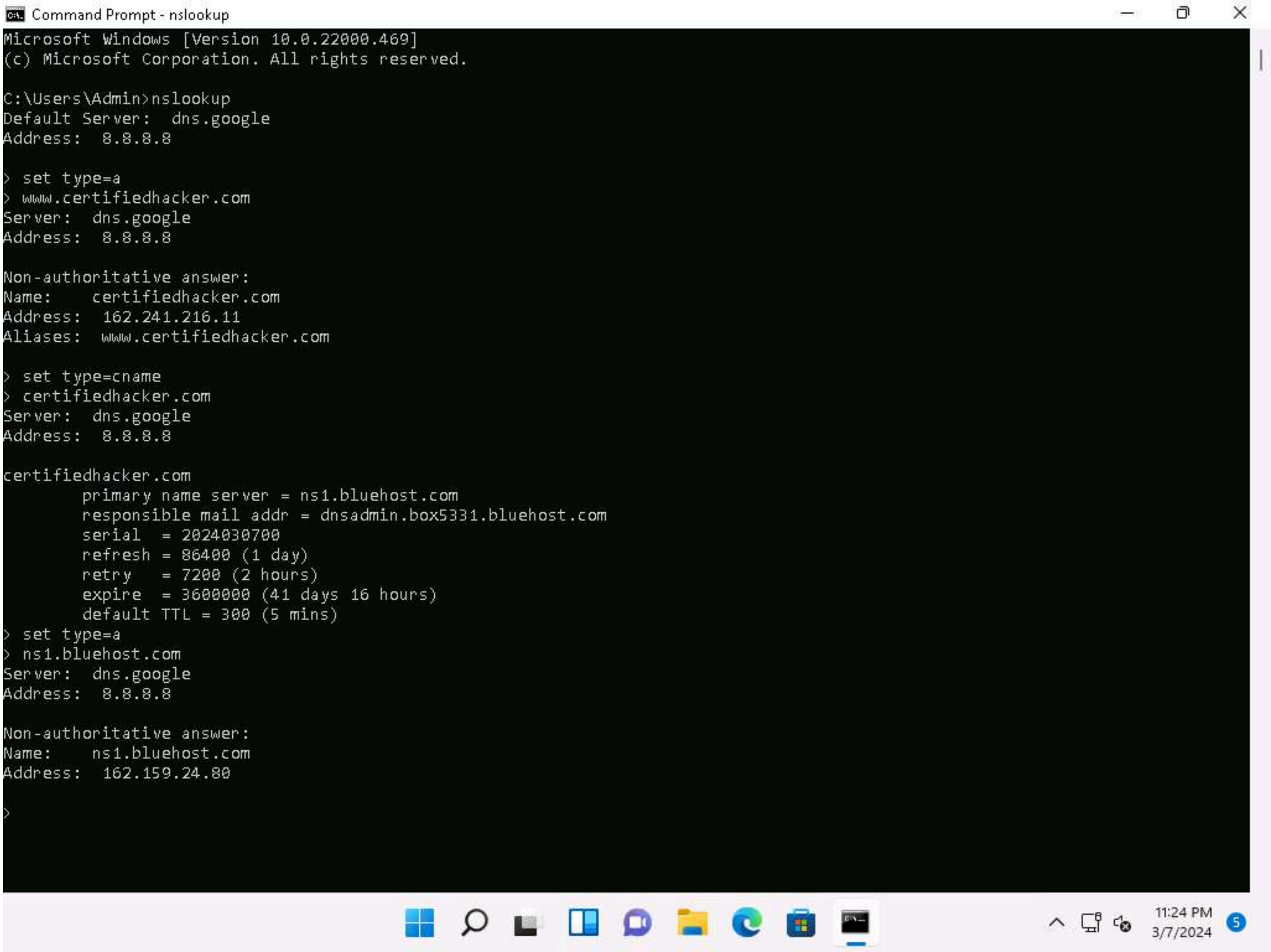


```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

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

> set type=a
> www.certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  162.241.216.11
Aliases:  www.certifiedhacker.com

> set type=cname
> certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

certifiedhacker.com
        primary name server = ns1.bluehost.com
        responsible mail addr = dnsadmin.box5331.bluehost.com
        serial  = 2024030700
        refresh = 86400 (1 day)
        retry   = 7200 (2 hours)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)
> _
```

10. Since you have obtained the authoritative name server, you will need to determine the IP address of the name server.

11. Issue the command **set type=a** and press **Enter**.

12. Type **ns1.bluehost.com** (or the primary name server that is displayed in your lab environment) and press **Enter**. This returns the IP address of the server, as shown in the screenshot.



```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

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

> set type=a
> www.certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  162.241.216.11
Aliases:  www.certifiedhacker.com

> set type=cname
> certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

certifiedhacker.com
        primary name server = ns1.bluehost.com
        responsible mail addr = dnsadmin.box5331.bluehost.com
        serial  = 2024030700
        refresh = 86400 (1 day)
        retry   = 7200 (2 hours)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)
> set type=a
> ns1.bluehost.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    ns1.bluehost.com
Address:  162.159.24.80

>
```

13. The authoritative name server stores the records associated with the domain. So, if an attacker can determine the authoritative name server (primary name server) and obtain its associated IP address, he/she might attempt to exploit the server to perform attacks such as DoS, DDoS, URL Redirection, etc.

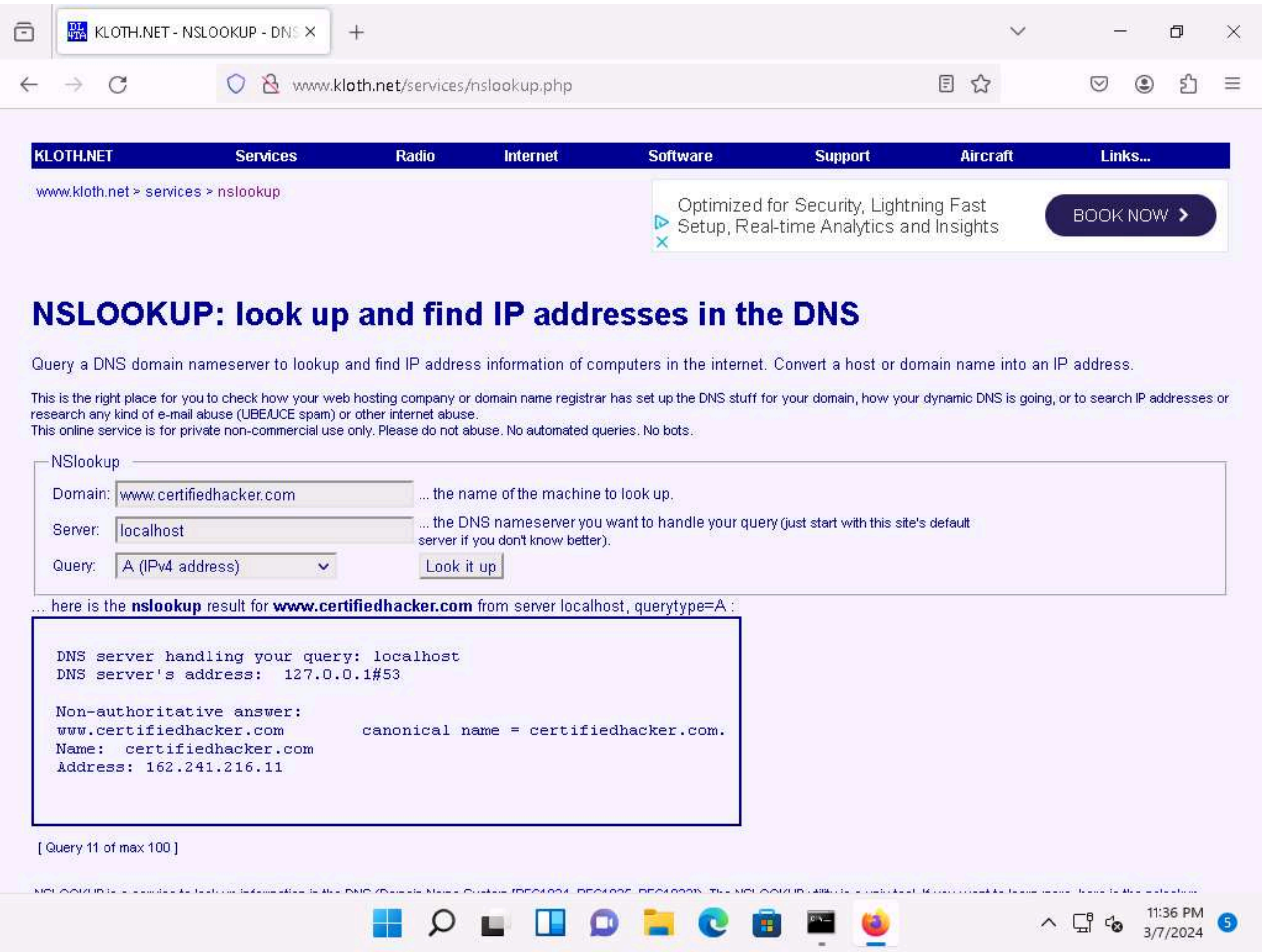
14. You can also perform the same operations using the NSLOOKUP online tool. Conduct a series of queries and review the information to gain familiarity with the NSLOOKUP tool and gather information.

15. Now, we will use an online tool NSLOOKUP to gather DNS information about the target domain.

16. Open any web browser and go to **http://www.kloth.net/services/nslookup.php** (here, we are using **Mozilla Firefox**).

17. **NSLOOKUP** website appears, as shown in the screenshot.

18. Once the site opens, in the **Domain:** field, enter **www.certifiedhacker.com**. Set the **Query:** field to default [**A (IPv4 address)**] and click the **Look it up** button to review the results that are displayed.



KLOTH.NET - NSLOOKUP - DNS
www.kloth.net/services/nslookup.php
KLOTH.NET
Services
Radio
Internet
Software
Support
Aircraft
Links...
www.kloth.net > services > nslookup

NSLOOKUP: look up and find IP addresses in the DNS

Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address.

This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is going, or to search IP addresses or research any kind of e-mail abuse (UBE/UCE spam) or other internet abuse.
This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots.

NSlookup

Domain: www.certifiedhacker.com ... the name of the machine to look up.

Server: localhost ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query: A (IPv4 address)

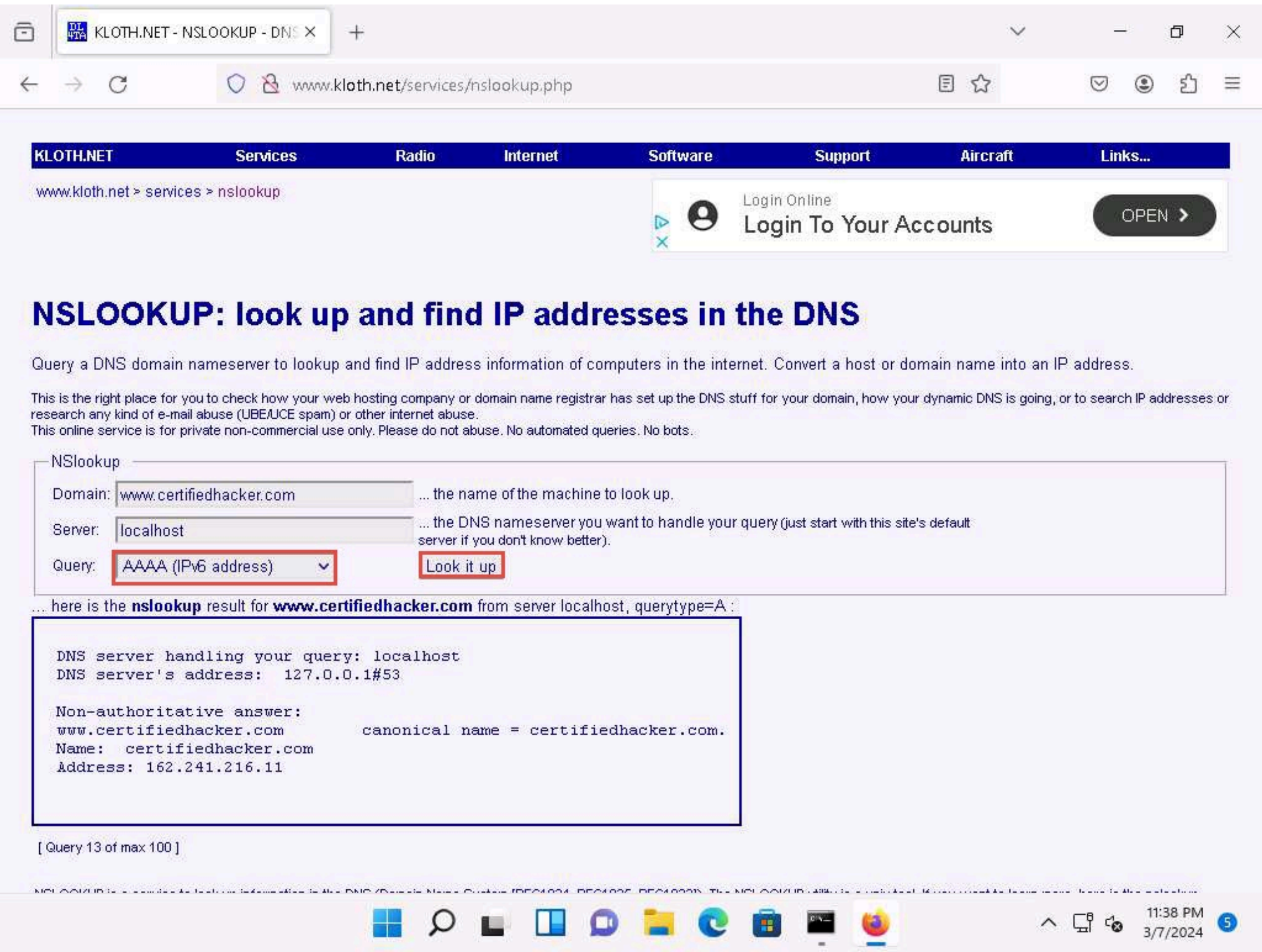
... here is the **nslookup** result for **www.certifiedhacker.com** from server localhost, querytype=A :

```
DNS server handling your query: localhost
DNS server's address:  127.0.0.1#53

Non-authoritative answer:
www.certifiedhacker.com       canonical name = certifiedhacker.com.
Name:  certifiedhacker.com
Address: 162.241.216.11
```

[Query 11 of max 100]

19. In the **Query:** field, click the drop-down arrow and check the different options that are available, as shown in the screenshot.

20. As you can see, there is an option for **AAAA (IPv6 address)**; select that and click **Look it up**. Perform queries related to this, since there are attacks that are possible over IPv6 networks as well.


KLOTH.NET - NSLOOKUP - DNS
www.kloth.net/services/nslookup.php
KLOTH.NET Services Radio Internet Software Support Aircraft Links...
www.kloth.net > services > nslookup

NSLOOKUP: look up and find IP addresses in the DNS

Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address.

This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is going, or to search IP addresses or research any kind of e-mail abuse (UBE/UCE spam) or other internet abuse.
This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots.

NSlookup

Domain: www.certifiedhacker.com ... the name of the machine to look up.

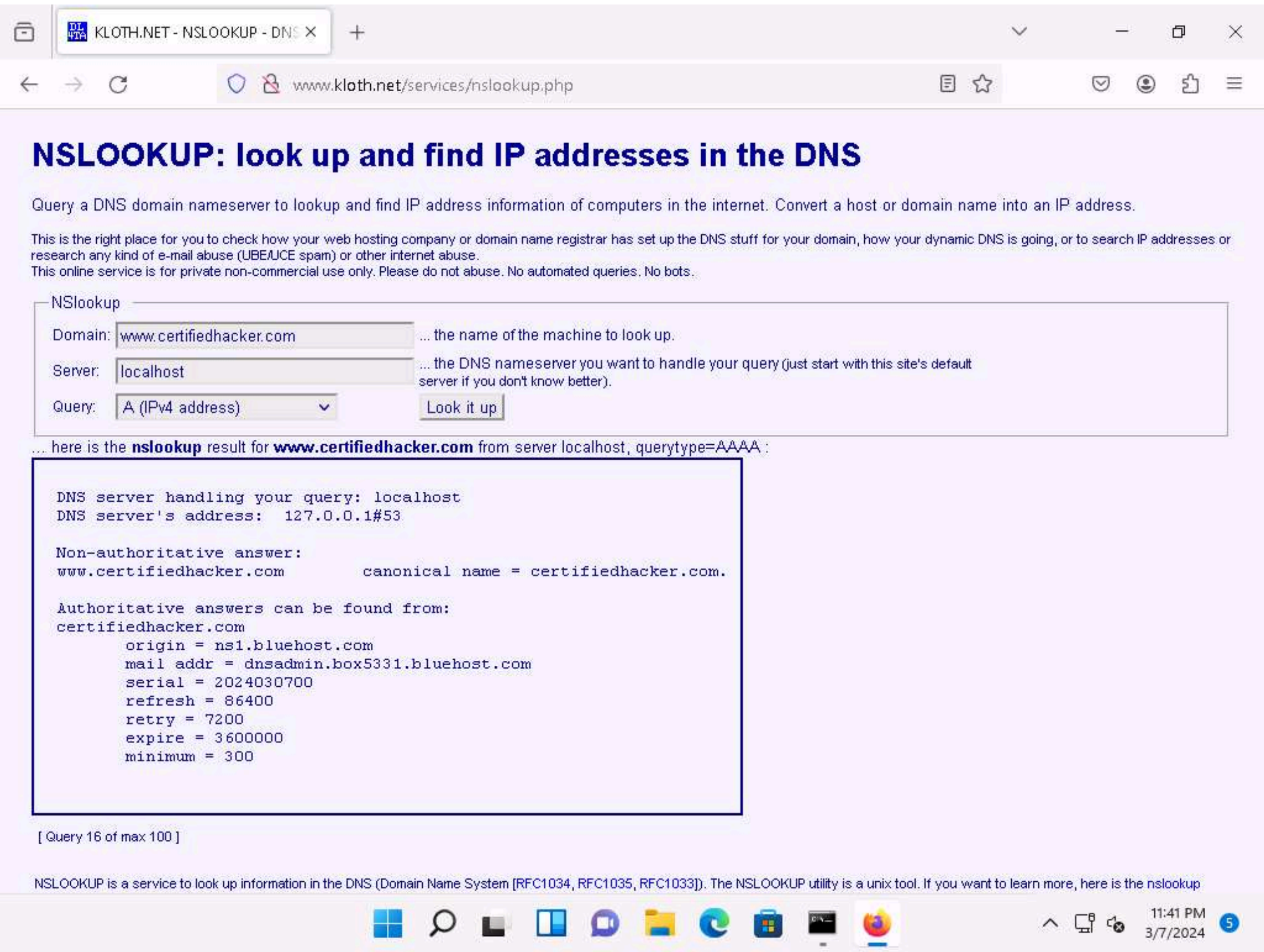
Server: localhost ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query: AAAA (IPv6 address) Look it up

... here is the **nslookup** result for **www.certifiedhacker.com** from server localhost, querytype=A :

```
DNS server handling your query: localhost
DNS server's address:  127.0.0.1#53

Non-authoritative answer:
www.certifiedhacker.com       canonical name = certifiedhacker.com.
Name:  certifiedhacker.com
Address: 162.241.216.11
```

[Query 13 of max 100]


KLOTH.NET - NSLOOKUP - DNS
www.kloth.net/services/nslookup.php

NSLOOKUP: look up and find IP addresses in the DNS

Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address.

This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is going, or to search IP addresses or research any kind of e-mail abuse (UBE/UCE spam) or other internet abuse.
This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots.

NSlookup

Domain: www.certifiedhacker.com ... the name of the machine to look up.

Server: localhost ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query: A (IPv4 address) Look it up

... here is the **nslookup** result for **www.certifiedhacker.com** from server localhost, querytype=AAAA :

```
DNS server handling your query: localhost
DNS server's address:  127.0.0.1#53

Non-authoritative answer:
www.certifiedhacker.com       canonical name = certifiedhacker.com.

Authoritative answers can be found from:
certifiedhacker.com
        origin = ns1.bluehost.com
        mail addr = dnsadmin.box5331.bluehost.com
        serial = 2024030700
        refresh = 86400
        retry = 7200
        expire = 3600000
        minimum = 300
```

[Query 16 of max 100]

NSLOOKUP is a service to look up information in the DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to learn more, here is the nslookup

21. This concludes the demonstration of DNS information gathering using the nslookup command-line utility and NSLOOKUP online tool.

22. You can also use DNS lookup tools such as **DNSdumpster** (https://dnsdumpster.com) to extract additional target DNS information.

23. Close all open windows and document all the acquired information.