

Lab 7: Perform DNS Footprinting

Lab Scenario

As a professional ethical hacker, you need to gather the DNS information of a target domain obtained during the previous steps. You need to perform DNS footprinting to gather information about DNS servers, DNS records, and types of servers used by the target organization. DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, and much more about a target network.

Using this information, you can determine key hosts connected in the network and perform social engineering attacks to gather even more information.

Lab Objectives

- Gather DNS information using nslookup command line utility and online tool
- Perform reverse DNS lookup using reverse IP domain check and DNSRecon

Overview of DNS

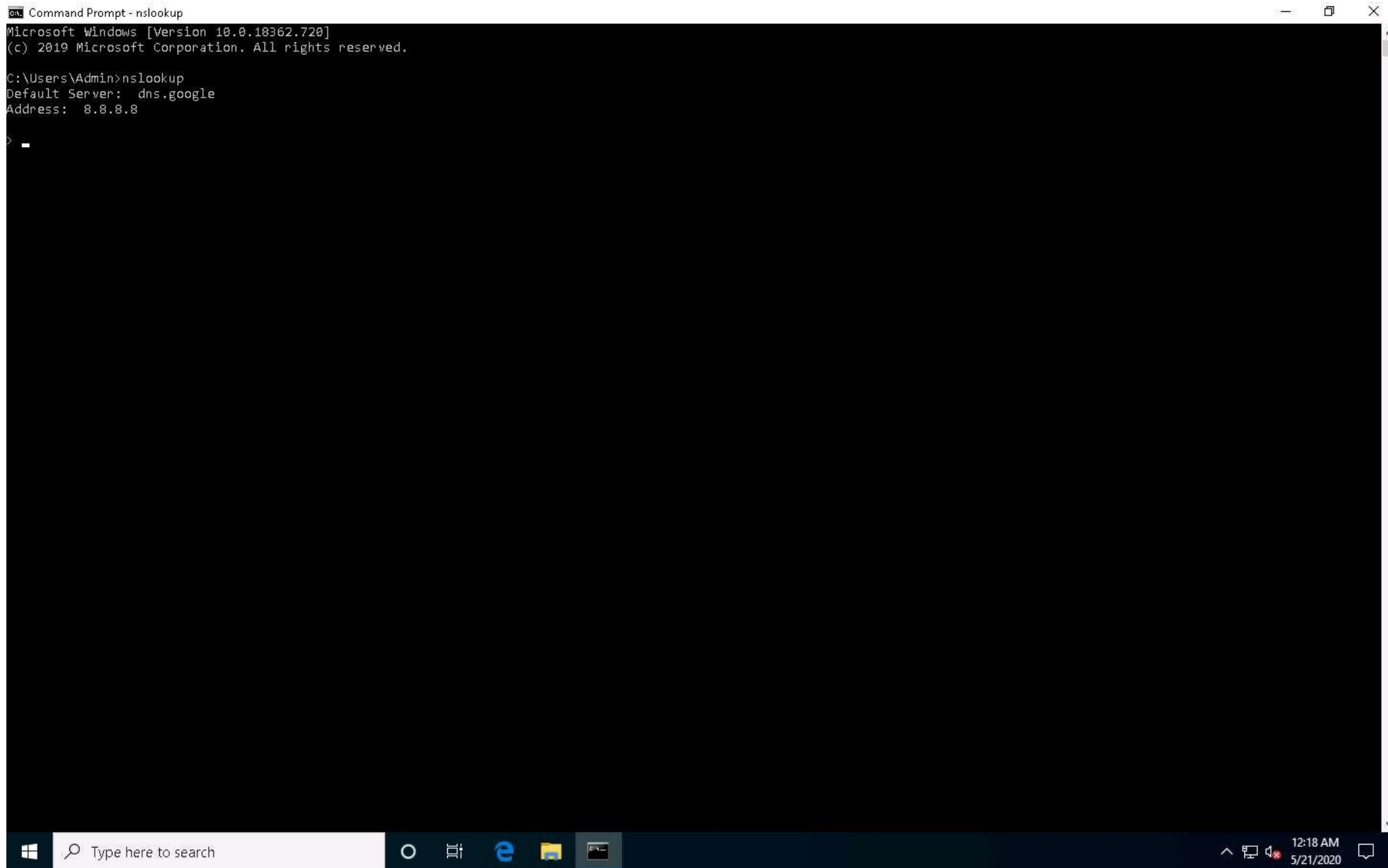
DNS considered the intermediary source for any Internet communication. The primary function of DNS is to translate a domain name to IP address and vice-versa to enable human-machine-network-internet communications. Since each device has a unique IP address, it is hard for human beings to memorize all 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. ☐ Click [Windows 10](#) to switch to the **Windows 10** machine, launch a **Command Prompt**, type **nslookup** and press **Enter**. This displays the default server and its address assigned to the **Windows 10** machine.



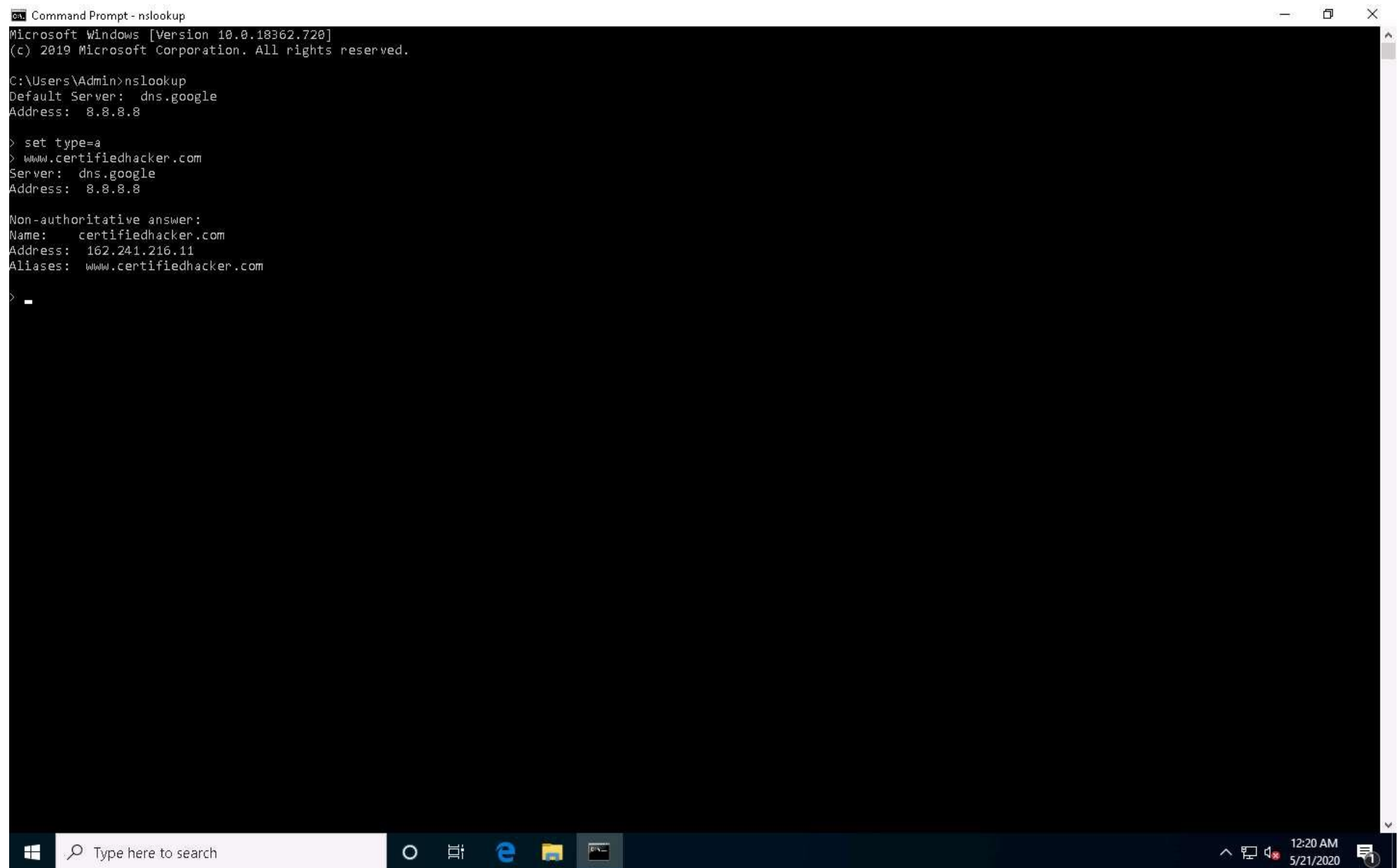
```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

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

>
```

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.



```
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 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 10**) 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.

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

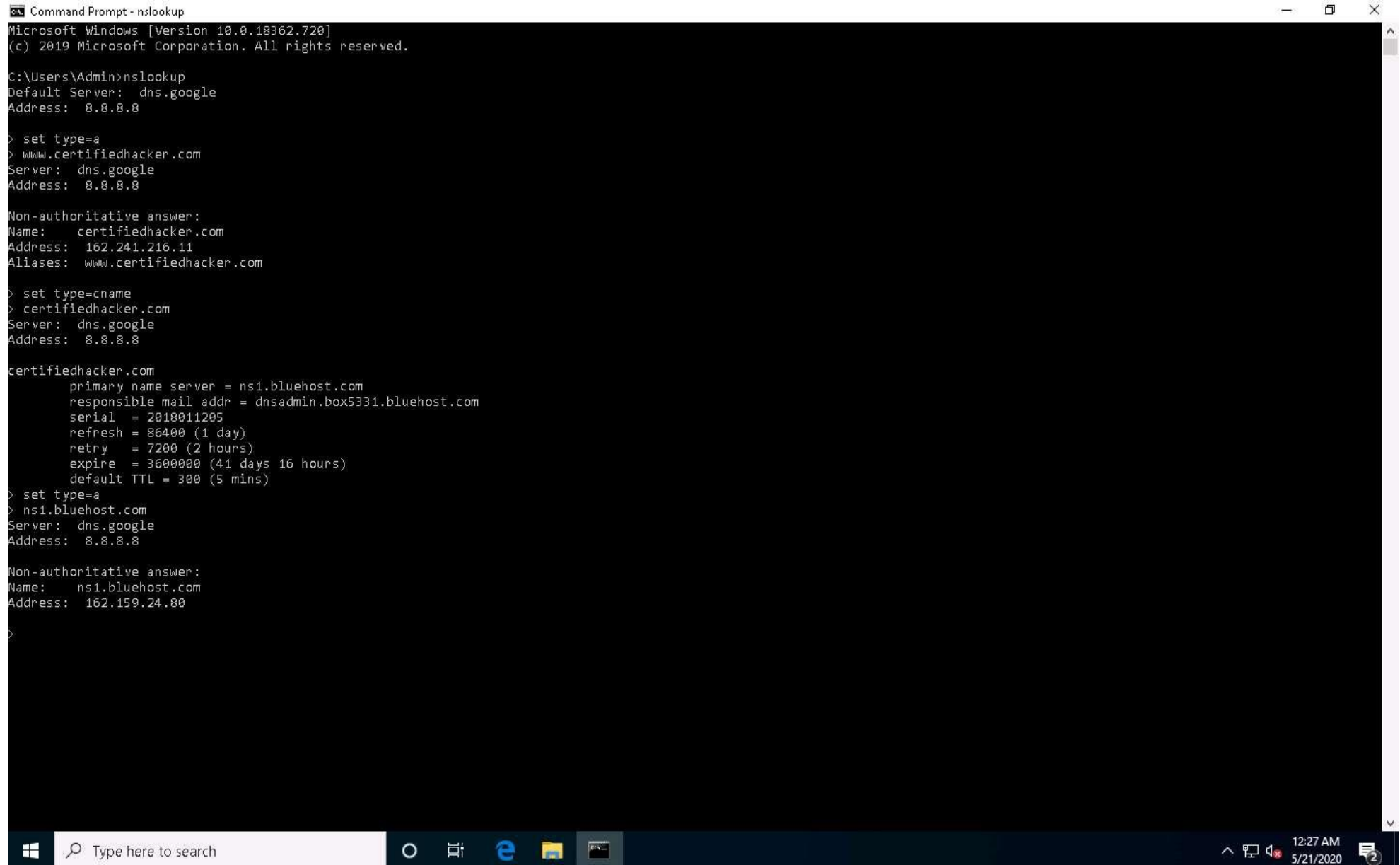
Non-authoritative answer:
Name:   certifiedhacker.com
Address: 162.241.216.11
Aliases: www.certifiedhacker.com

> 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 = 2018011205
    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.



```
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 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 = 2018011205
    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 (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and click <http://www.kloth.net/services/nslookup.php> and press **Enter**.
17. ☐ **NSLOOKUP** website appears, as shown in the screenshot.

KLOTH.NET - NSLOOKUP - DN: X

www.kloth.net/services/nslookup.php

KLOTH.NET Services Radio Internet Software Support Aircraft Links...

www.kloth.net > services > nslookup

Helping educate 10 million youths

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 (UBEJUICE 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: ... the name of the machine to look up.


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

Query:

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 manual (man page). Basically, DNS maps domain names to IP addresses. Although this web online service can query a specific DNS server, in most cases it may be sufficient and convenient just to use the KLOTH.NET default nameserver "localhost"/127.0.0.1. To resolve an IP address by reverse lookup (get a computer's name if you only have its IP address), try to perform a PTR query instead of ANY. This reverse lookup will only work if the IP address owner has inserted a PTR record in the DNS. The PTR information is informal only and it may mostly be true, but sometimes not. If you don't get a PTR information about a specific computer from a NSLOOKUP query, you may want to try our [whois](#) service to find out the owner of this IP address. Like the PTR, other records are also not mandatory: LOC, RP, TXT. They are not strictly required in the DNS and their content may be true or not. You can't trust on the LOC to locate a host, because most hosts don't have this record defined.

If you prefer dig over nslookup, you may try our [dig](#) service.

This page is also available in [German](#), [French](#) and [Portuguese](#). Enjoy.
>>> If you would like to see this service in **your** or any other language, please send a translation.

 If you like this service, please, consider to make a small donation to fund and continue this site. Thank you.

[Link to www.kloth.net.](#)

Recommended books about [Networking](#).

You are coming from IP address **199.101.110.10** using port 53835.
A DNS reverse lookup on this IP address does not work.

You are talking to server www.kloth.net (78.46.75.45) on port 80 using the protocol HTTP/1.1.
Current date and time (UTC) on the server is 2020-05-21 (Thu) 04:31:46. It is the 142nd day of this year.

Document URL : <http://www.kloth.net/services/nslookup.php>
Copyright © 1999-2020 Ralf D. Kloth, Ludwigsburg, DE (GRQ software). <hostmaster at kloth.net > [don't send spam]
Created 1999-09-13. Last modified 2011-01-30. Your visit 2020-05-21 04:31:46. Page created in 0.1225 sec.

12:32 AM 5/21/2020

18. ☐ Once the site opens, in the **Domain:** field, enter **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 - DN: X

www.kloth.net/services/nslookup.php

KLOTH.NET Services Radio Internet Software Support Aircraft Links...

www.kloth.net > services > nslookup

Helping educate 10 million youths

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 (UBEJUICE 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: ... the name of the machine to look up.

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

Query:

... here is the **nslookup** result for **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:
Name: certifiedhacker.com
Address: 162.241.216.11
```

[Query 1 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 manual \(man page\)](#). Basically, DNS maps domain names to IP addresses. Although this web online service can query a specific DNS server, in most cases it may be sufficient and convenient just to use the KLOTH.NET default nameserver "localhost"/127.0.0.1. To resolve an IP address by reverse lookup (get a computer's name if you only have its IP address), try to perform a PTR query instead of ANY. This reverse lookup will only work if the IP address owner has inserted a PTR record in the DNS. The PTR information is informal only and it may mostly be true, but sometimes not. If you don't get a PTR information about a specific computer from a NSLOOKUP query, you may want to try our [whois](#) service to find out the owner of this IP address. Like the PTR, other records are also not mandatory: LOC, RP, TXT. They are not strictly required in the DNS and their content may be true or not. You can't trust on the LOC to locate a host, because most hosts don't have this record defined.

If you prefer dig over nslookup, you may try our [dig](#) service.

This page is also available in [German](#), [French](#) and [Portuguese](#). Enjoy.
>>> If you would like to see this service in **your** or any other language, please send a translation.

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

KLOTH.NET - NSLOOKUP - DN: X

www.kloth.net/services/nslookup.php

KLOTH.NET Services Radio Internet Software Support Aircraft Links...

www.kloth.net > services > nslookup

Helping educate 10 million youths

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 (UBEJUICE 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: ... the name of the machine to look up.

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

Query:

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

DNS section: **certifiedhacker.com** type: A value: 10.1.1.1

Non-authoritative Name: **certifiedhacker.com** type: NS value: 10.1.1.1

MX (mail exchange) type: MX value: 10.1.1.1

PTR (domain pointer) type: PTR value: 10.1.1.1

SOA (start of authority) type: SOA value: 10.1.1.1

TXT (text) type: TXT value: 10.1.1.1

LOC (location) type: LOC value: 10.1.1.1

RP (responsible person) type: RP value: 10.1.1.1

SRV (service) type: SRV value: 10.1.1.1

AXFR (zone transfer) type: AXFR value: 10.1.1.1

NSLOOKUP is a utility that can be used to query a DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to learn more, here is the nslookup manual (man page).

Basically, DNS is a system that maps domain names to IP addresses. Although this is not strictly required in the DNS and their content may be true or not, it may mostly be true or not. Like the PTR, you can't trust on the LOC to locate a host, because most hosts don't have this record defined.

If you prefer dig over nslookup, you may try our **dig** service.

This page is also available in **German, French and Portuguese**. Enjoy.

>>> If you would like to see this service in **your** or any other language, please send a translation.

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.

The screenshot shows a web browser window with the address bar displaying `www.kloth.net/services/nslookup.php`. The page has a dark blue header with navigation links: KLOTH.NET, Services, Radio, Internet, Software, Support, Aircraft, and Links... Below the header, a breadcrumb trail reads `www.kloth.net > services > nslookup`. A sidebar on the right contains an advertisement for "Free Internet Speed Test Tool" from speedtest-guide.com with an "OPEN" button.

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: ... the name of the machine to look up.

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

Query:

... here is the **nslookup** result for **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:
*** Can't find certifiedhacker.com: No answer

Authoritative answers can be found from:
certifiedhacker.com
  origin = ns1.bluehost.com
  mail addr = dnsadmin.box5331.bluehost.com
  serial = 2018011205
  refresh = 86400
  retry = 7200
  expire = 3600000
  minimum = 300
```

[Query 2 of max 100]

Read pagead2.googleadsyndication.com 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 manual (man page).

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 **Professional Toolset** (<https://tools.dnsstuff.com>), **DNS Records** (<https://network-tools.com>), etc. to extract additional target DNS information.
 23. ☐ Close all open windows and document all the acquired information.
-

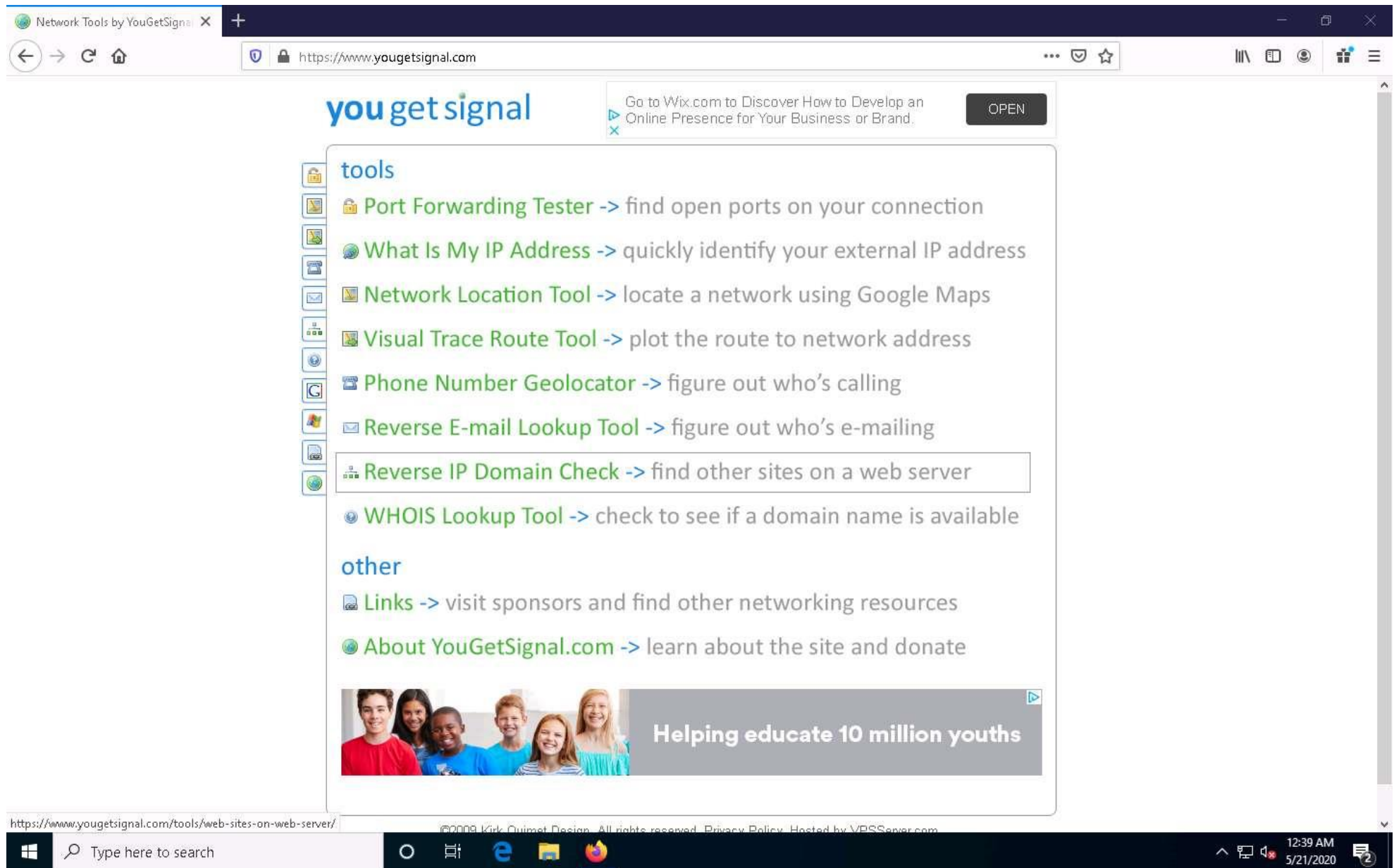
Task 2: Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon

DNS lookup is used for finding the IP addresses for a given domain name, and the reverse DNS operation is performed to obtain the domain name of a given IP address.

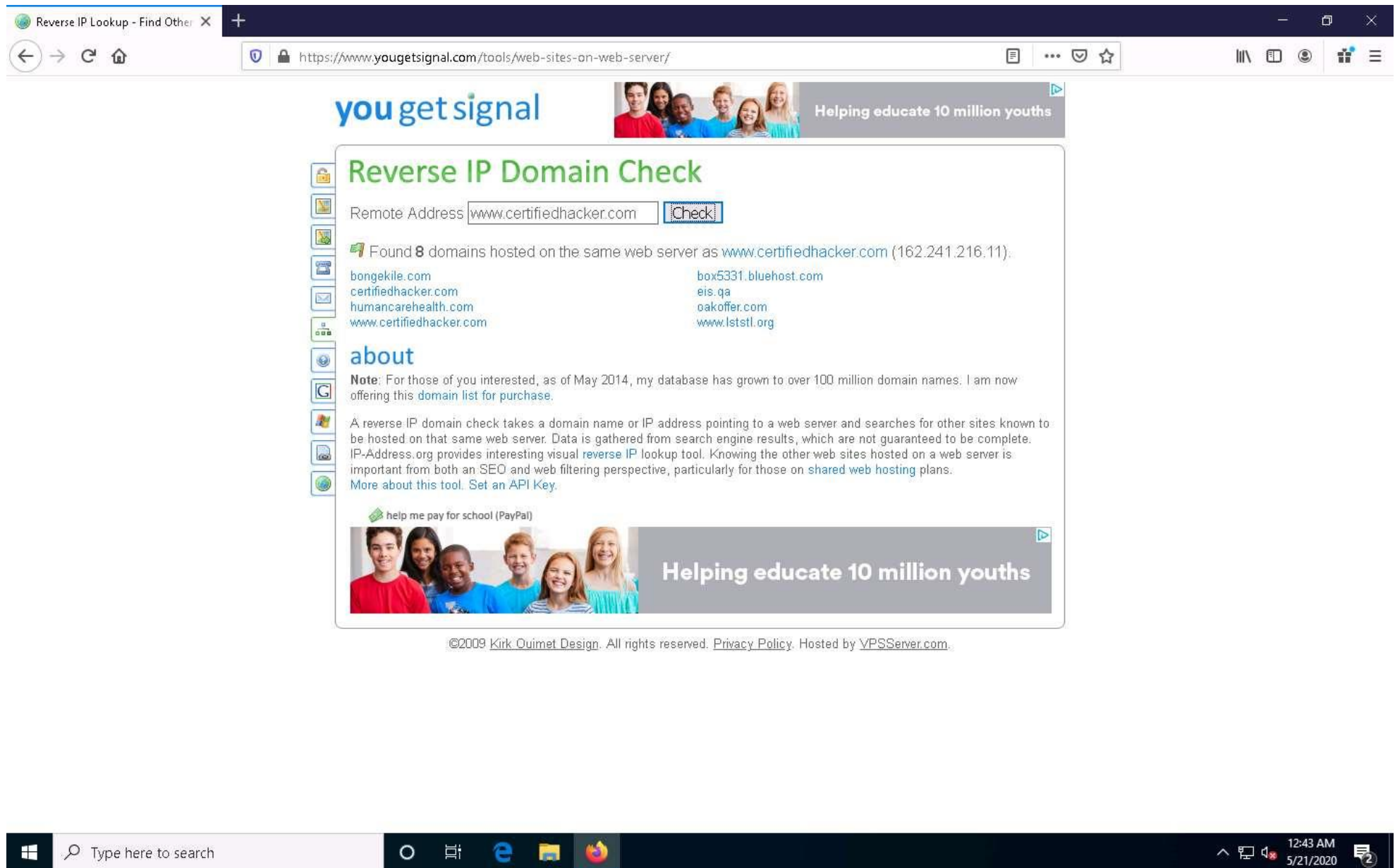
Here, we will perform reverse DNS lookup using you get signal's Reverse IP Domain Check tool to find the other domains/sites that share the same web server as our target server.

Here, we will also perform a reverse DNS lookup using DNSRecon on IP range in an attempt to locate a DNS PTR record for those IP addresses.

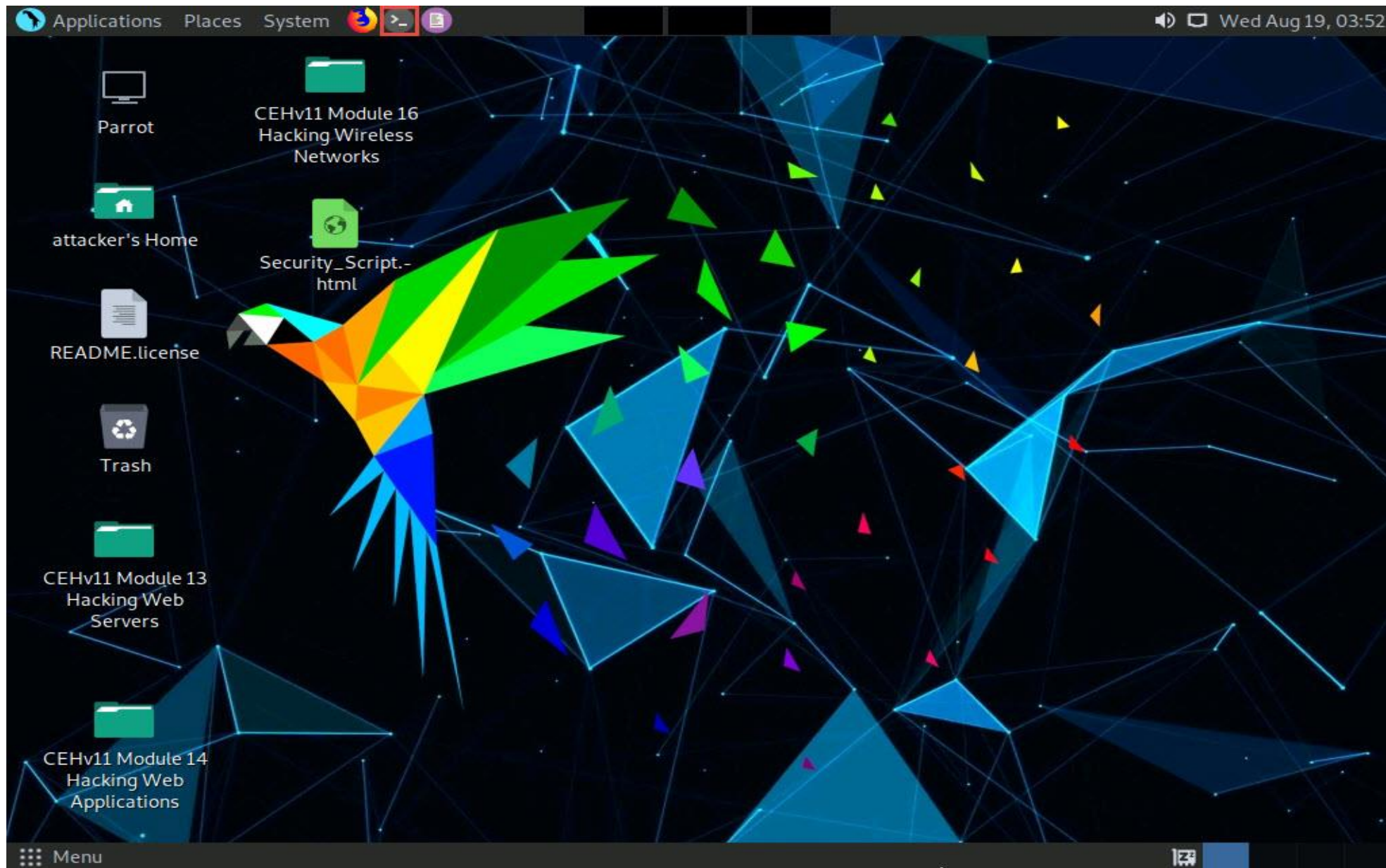
1. ☐ Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and click <https://www.yougetsignal.com> and press **Enter**.
2. ☐ **you get signal** website appears, click **Reverse IP Domain Check**.



3. ☐ On the **Reverse IP Domain Check** page, enter **www.certifiedhacker.com** in the **Remote Address** field and click **Check** to find other domains/sites hosted on a certifiedhacker.com web server. You will get the list of domains/sites hosted on the same server as **www.certifiedhacker.com**, as shown in the screenshot.



4. ☐ Now, click [Parrot Security](#) to switch to the **Parrot Security** machine.
5. ☐ Click the **MATE Terminal** icon at the top-left corner of the **Desktop** window to open a **Terminal** window.



6. ☐ In the **Parrot Terminal** window, type **dnsrecon -r 162.241.216.0-162.241.216.255** and press **Enter** to locate a DNS PTR record for IP addresses between 162.241.216.0 - 162.241.216.255.

Here, we will use the IP address range, which includes the IP address of our target, that is, the `certifiedhacker.com` domain (162.241.216.11), which we acquired in the previous steps.

-r option specifies the range of IP addresses (first-last) for reverse lookup brute force.


```
Applications Places System Parrot Terminal Wed Aug 19, 05:04
File Edit View Search Terminal Help
[attacker@parrot]~$ dnsrecon -r 162.241.216.0-162.241.216.255
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 162.241.216.0 to 162.241.216.255
[+] {'type': 'PTR', 'name': '162-241-216-1.unifiedlayer.com', 'address': '162.241.216.1'}
[+] {'type': 'PTR', 'name': '162-241-216-0.unifiedlayer.com', 'address': '162.241.216.0'}
[+] {'type': 'PTR', 'name': '162-241-216-5.unifiedlayer.com', 'address': '162.241.216.5'}
[+] {'type': 'PTR', 'name': '162-241-216-2.unifiedlayer.com', 'address': '162.241.216.2'}
[+] {'type': 'PTR', 'name': '162-241-216-3.unifiedlayer.com', 'address': '162.241.216.3'}
[+] {'type': 'PTR', 'name': '162-241-216-4.unifiedlayer.com', 'address': '162.241.216.4'}
[+] {'type': 'PTR', 'name': '162-241-216-7.unifiedlayer.com', 'address': '162.241.216.7'}
[+] {'type': 'PTR', 'name': '162-241-216-8.unifiedlayer.com', 'address': '162.241.216.8'}
[+] {'type': 'PTR', 'name': '162-241-216-9.unifiedlayer.com', 'address': '162.241.216.9'}
[+] {'type': 'PTR', 'name': '162-241-216-10.unifiedlayer.com', 'address': '162.241.216.10'}
[+] {'type': 'PTR', 'name': '162-241-216-6.unifiedlayer.com', 'address': '162.241.216.6'}
[+] {'type': 'PTR', 'name': 'box5331.bluehost.com', 'address': '162.241.216.11'}
[+] {'type': 'PTR', 'name': 'box5348.bluehost.com', 'address': '162.241.216.17'}
[+] {'type': 'PTR', 'name': '162-241-216-12.unifiedlayer.com', 'address': '162.241.216.12'}
[+] {'type': 'PTR', 'name': '162-241-216-13.unifiedlayer.com', 'address': '162.241.216.13'}
[+] {'type': 'PTR', 'name': '162-241-216-16.unifiedlayer.com', 'address': '162.241.216.16'}
[+] {'type': 'PTR', 'name': 'box5334.bluehost.com', 'address': '162.241.216.14'}
[+] {'type': 'PTR', 'name': '162-241-216-15.unifiedlayer.com', 'address': '162.241.216.15'}
[+] {'type': 'PTR', 'name': '162-241-216-18.unifiedlayer.com', 'address': '162.241.216.18'}
[+] {'type': 'PTR', 'name': '162-241-216-19.unifiedlayer.com', 'address': '162.241.216.19'}
[+] {'type': 'PTR', 'name': 'box5350.bluehost.com', 'address': '162.241.216.20'}
[+] {'type': 'PTR', 'name': 'box5353.bluehost.com', 'address': '162.241.216.23'}
[+] {'type': 'PTR', 'name': '162-241-216-22.unifiedlayer.com', 'address': '162.241.216.22'}
[+] {'type': 'PTR', 'name': '162-241-216-21.unifiedlayer.com', 'address': '162.241.216.21'}
[+] {'type': 'PTR', 'name': '162-241-216-25.unifiedlayer.com', 'address': '162.241.216.25'}
[+] {'type': 'PTR', 'name': '162-241-216-24.unifiedlayer.com', 'address': '162.241.216.24'}
```

7. ☐ This concludes the demonstration of gathering information about a target organization by performing reverse DNS lookup using “you get signal’s” Reverse IP Domain Check and DNSRecon tool.

8. ☐ Close all open windows and document all the acquired information.