# Introductory Networking

**An introduction to networking theory and basic networking tools**

## Task 2: The OSI Model: An Overview

| Question | Answer |
|---|---|
| Which layer would choose to send data over TCP or UDP? | 4 |
| Which layer checks received information to make sure that it hasn't been corrupted? | 2 |
| In which layer would data be formatted in preparation for transmission? | 2 |
| Which layer transmits and receives data? | 1 |
| Which layer encrypts, compresses, or otherwise transforms the initial data to give it a standardized format? | 6 |
| Which layer tracks communications between the host and receiving computers? | 5 |
| Which layer accepts communication requests from applications? | 7 |
| Which layer handles logical addressing? | 3 |
| When sending data over TCP, what would you call the "bite-sized" pieces of data? | Segments |
| **[Research]** Which layer would the FTP protocol communicate with? | 7 |
| Which transport layer protocol would be best suited to transmit a live video? | UDP |

## Task 3: Encapsulation

| Question | Answer |
|---|---|
| How would you refer to data at layer 2 of the encapsulation process (with the OSI model)? | Frames |
| How would you refer to data at layer 4 of the encapsulation process (with the OSI model), if the UDP protocol has been selected? | Datagrams |
| What process would a computer perform on a received message? | De-encapsulation |
| Which is the only layer of the OSI model to add a *trailer* during encapsulation? | Data Link |
| Does encapsulation provide an extra layer of security **(Aye/Nay)**? | Aye |

## Task 4  The TCP/IP Model

| Question | Answer |
|---|---|
| Which model was introduced first, OSI or TCP/IP? | TCP/IP |

| | |
|---|---|
| Which layer of the TCP/IP model covers the functionality of the Transport layer of the OSI model **(Full Name)**? | Transport |
| Which layer of the TCP/IP model covers the functionality of the Session layer of the OSI model **(Full Name)**? | Application |
| The Network Interface layer of the TCP/IP model covers the functionality of two layers in the OSI model. These layers are Data Link, and?.. **(Full Name)**? | Physical |
| Which layer of the TCP/IP model handles the functionality of the OSI network layer? | Internet |
| What kind of protocol is TCP? | Connection-based |
| What is SYN short for? | Synchronise |
| What is the second step of the three-way handshake? | SYN/ACK |
| What is the short name for the "Acknowledgement" segment in the three-way handshake? | ACK |

## Task 5: Networking Tools Ping

Ping is a utility tool used to check the reachability of a host and measure the round-trip time for packets to travel to and from that host. Also, when you ping a host by its domain name, the "ping" command will display the IP address in the output.

- To provide answers to the questions in this task, start your attack box and type the command **"man ping"**
- The man ping command will display the manual page/documentation for the "ping" command where you will have detailed information about how to use the "ping" command, its various options, and the meaning of its output.

| **Question** | **Answer** |
|---|---|
| What command would you use to ping the bbc.co.uk website? | ping bbc.co.uk |
| Ping *muirlandoracle.co.uk*<br>What is the IPv4 address? | 217.160.0.152 |
| What switch lets you change the interval of sent ping requests? | -i |
| What switch would allow you to restrict requests to IPv4? | -4 |
| What switch would give you a more verbose output? | -v |

## Task 6: Networking Tools Traceroute

Traceroute is another networking utility tool used to trace the route that data packets take from your computer to a destination host or server.

- To provide answers to the questions in this task, start your attack box and type the command **"man traceroute"**

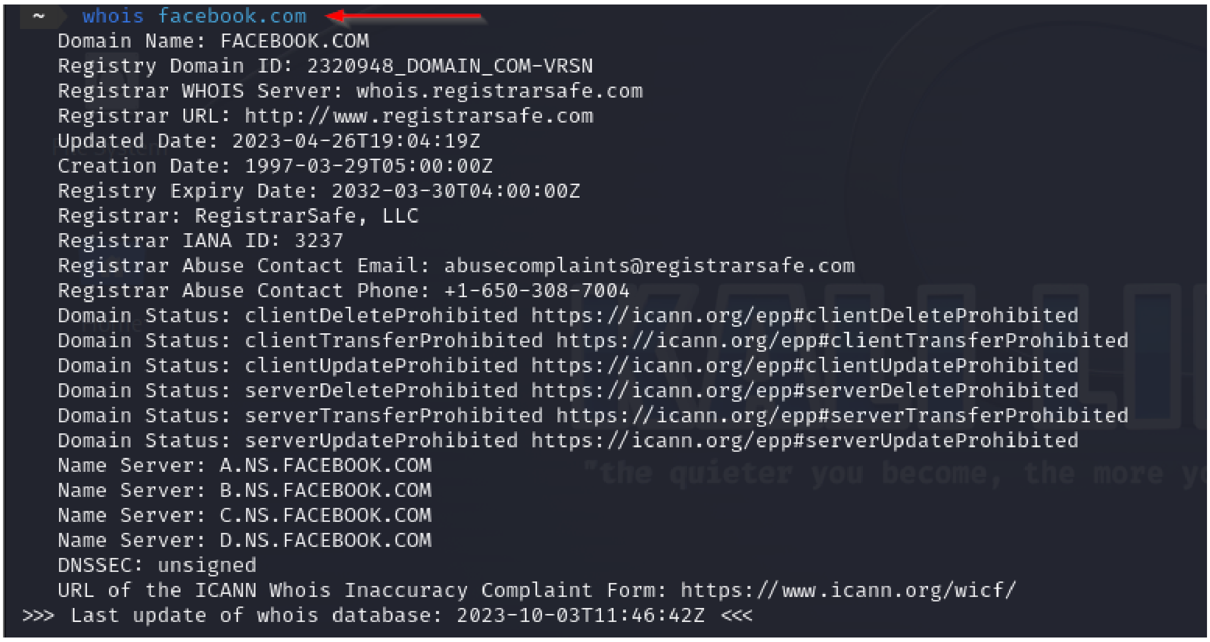
| **Question** | **Answer** |
|---|---|
| What switch would you use to specify an interface when using Traceroute? | -i |

|  |  |
|---|---|
| What switch would you use if you wanted to use TCP SYN requests when tracing the route? | -T |
| **[Lateral Thinking]** Which layer of the ***TCP/IP*** model will traceroute run on by default (Windows)? | Internet |

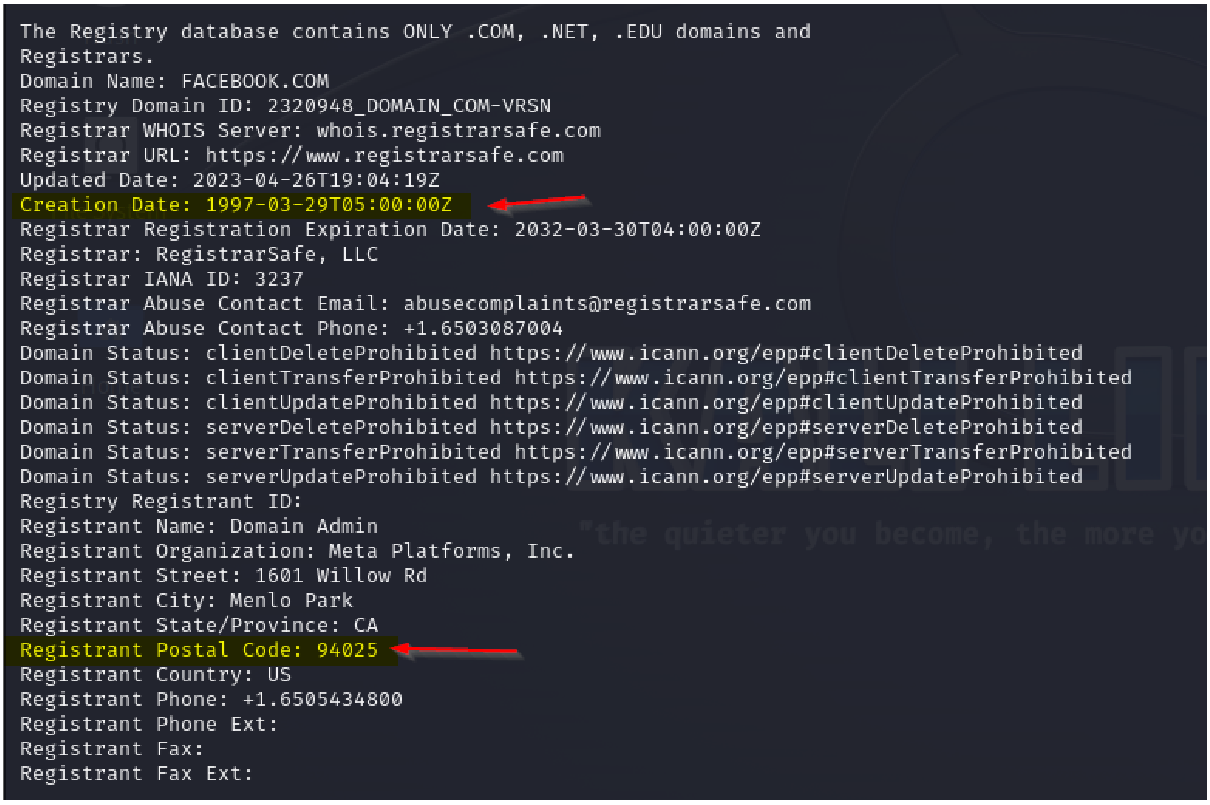
## Task 7: Networking Tools WHOIS

Whois is a networking utility tool that allows you to query who a domain name is registered to.

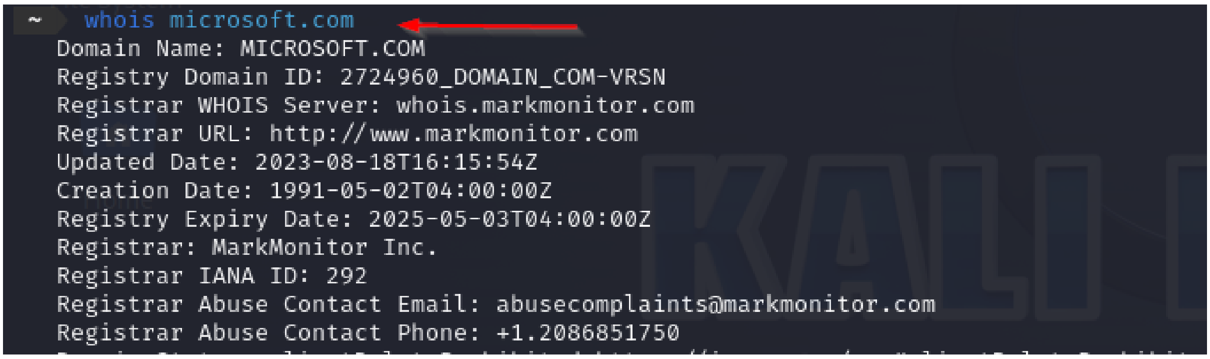
- Perform a whois search on facebook.com using **"whois facebook.com"**
- Perform whois search on Microsoft.com
- All answers to the questions will be found except when you have to use Google to search for the golf course that is near the registrant address for microsoft.com



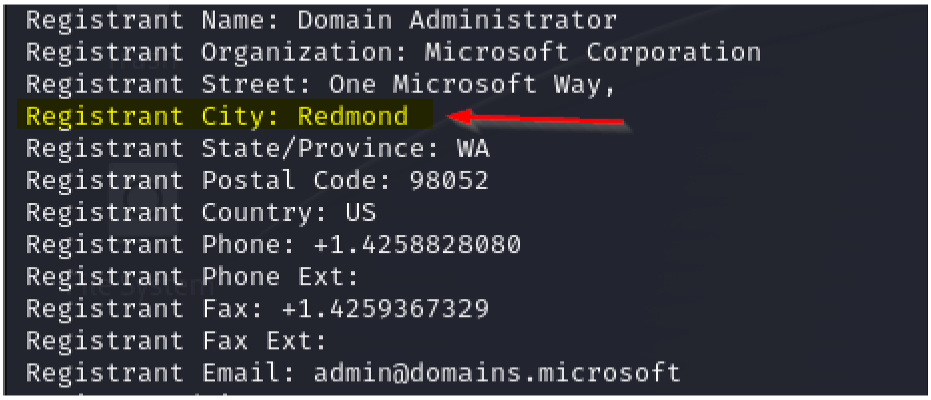
```
~  whois facebook.com
   Domain Name: FACEBOOK.COM
   Registry Domain ID: 2320948_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrarsafe.com
   Registrar URL: http://www.registrarsafe.com
   Updated Date: 2023-04-26T19:04:19Z
   Creation Date: 1997-03-29T05:00:00Z
   Registry Expiry Date: 2032-03-30T04:00:00Z
   Registrar: RegistrarSafe, LLC
   Registrar IANA ID: 3237
   Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
   Registrar Abuse Contact Phone: +1-650-308-7004
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: A.NS.FACEBOOK.COM
   Name Server: B.NS.FACEBOOK.COM
   Name Server: C.NS.FACEBOOK.COM
   Name Server: D.NS.FACEBOOK.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-10-03T11:46:42Z <<<
```



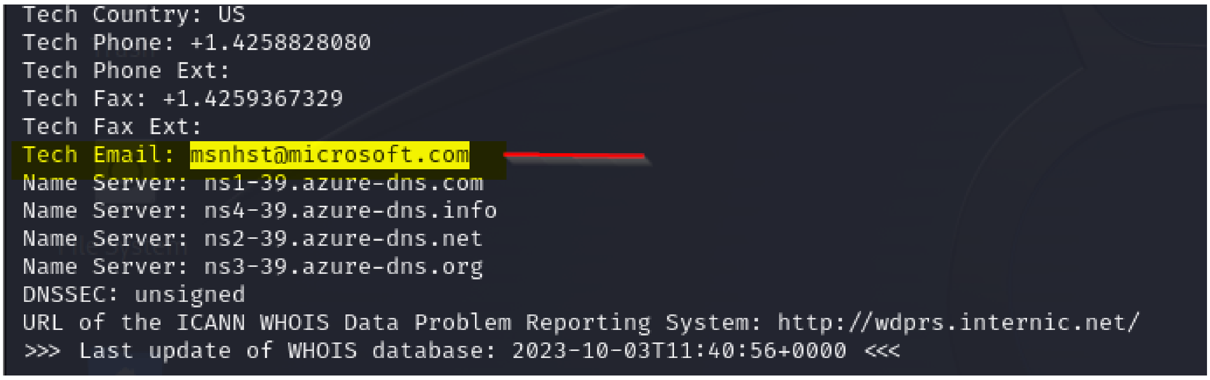
```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: https://www.registrarsafe.com
Updated Date: 2023-04-26T19:04:19Z
Creation Date: 1997-03-29T05:00:00Z
Registrar Registration Expiration Date: 2032-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1.6503087004
Domain Status: clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Meta Platforms, Inc.
Registrant Street: 1601 Willow Rd
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: US
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
```



```
~ whois microsoft.com
   Domain Name: MICROSOFT.COM
   Registry Domain ID: 2724960_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2023-08-18T16:15:54Z
   Creation Date: 1991-05-02T04:00:00Z
   Registry Expiry Date: 2025-05-03T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
```



```
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828080
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: admin@domains.microsoft
```



```
Tech Country: US
Tech Phone: +1.4258828080
Tech Phone Ext:
Tech Fax: +1.4259367329
Tech Fax Ext:
Tech Email: msnhst@microsoft.com
Name Server: ns1-39.azure-dns.com
Name Server: ns4-39.azure-dns.info
Name Server: ns2-39.azure-dns.net
Name Server: ns3-39.azure-dns.org
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-10-03T11:40:56+0000 <<<
```

| Question | Answer |
|---|---|
| What is the registrant postal code for facebook.com? | 94025 |
| When was the facebook.com domain first registered (Format: DD/MM/YYYY)? | 29/03/1997 |
| Which city is the registrant based in? | Redmond |
| **[OSINT]** What is the name of the golf course that is near the registrant address for microsoft.com? | Bellevue Golf Course |
| What is the registered Tech Email for microsoft.com? | msnhst@microsoft.com |

## Task 8  Networking Tools Dig

Domain Information Groper(Dig) tool is a utility tool for querying Domain Name System (DNS) servers to retrieve DNS information

- For the question “If a DNS query has a TTL of 24 hours, what number would the dig query show?”
- Since TTL is in seconds= 24 x60 x 60 = 86400

| Question | Answer |
|---|---|
| What is DNS short for? | Domain Name System |
| What is the first type of DNS server your computer would query when you search for a domain? | Recursive |
| What type of DNS server contains records specific to domain extensions (i.e. *.com*, .co.uk*, etc)*? Use the long version of the name. | Top-Level Domain |
| Where is the very first place your computer would look to find the IP address of a domain? | Local Cache |
| **[Research]** Google runs two public DNS servers. One of them can be queried with the IP 8.8.8.8, what is the IP address of the other one? | 8.8.4.4 |
| If a DNS query has a TTL of 24 hours, what number would the dig query show? | 86400 |