Cyber Security Tutorial 1

Instructions

In this tutorial you should work preferably in pairs or alone. Try to answer all the questions together and discuss the possible answers/solutions. You will be given 30 minutes to complete this task and, in the end, a general discussion will take place in class based on the content of this tutorial. Try to answer as many questions as you can!

Your answers might be slightly different in some questions are your perspective differs too. There are more discussion based questions than right/wrong in this tutorial.

Question 1

What is the difference when a website has an https:// instead of an http:// in a URL?

Sample answer: http is the protocol used for transferring data between a browser and the website that is connected to. The addition of "s" is the protocol's secure version which means that any exchange of data between the browser and the targeted website is encrypted.

Question 2

Discuss and come up with at least four criteria (either to do or not to do practices) that someone must follow when choosing a password.

Sample answer: To do or do not practices; 1) use of a combination of letters, numbers and symbols; 2) never use the same password for different services; 3) never use the same password for a long period of time; 4) never use words inside your password, birthdays and other information that is personal and can be obtained by outsiders.

Question 3

The human factor is claimed to be one of the most common factors responsible for an occurred cyber-attack to an organisation. Is this true? Explain why and how the human factor can play a role in a cyber-attack.

Sample answer: Human factor is one of the key aspects in every working environment. The knowledge of computing and especially cyber security is not common to be on a high level for all employees in a company. Therefore increasing cyber awareness through different types of training is necessary nowadays. Some of the things that can lead to a cyber-attack; leaving your work password on a post it note that anyone can access with a bit of effort is a bad practice that can still be encountered today; taking your work laptop home or leaving your work laptop with not any security mechanisms employed, while containing confidential work files; leaving important files unprotected or sharing them on possibly vulnerable cloud services; avoid the installation of any security updates of the manufacturer or installation of antivirus; not maintaining your security mechanisms in place; opening all emails and their content.

Question 4

Discuss the term Cyberwarfare and explain its importance by giving some well-known examples.

Sample answer: Cyberwarfare is the new type of battlefield. It describes any type of cyber attack against a nation state with political, military or other purposes. It is normally relevant to espionage and sabotage. Also, it describes both defensive and offensive activities. One well known example is

Stuxnet where the target was the Iranian nuclear facility, and no one has officially claimed their involvement, although there is a strong belief that other nations were involved in the role of the attacker.

Question 5

Pick a recent occurred cyber-attack and discuss this within your group, regarding the type, impact, and techniques used by the attackers. How this attack could be avoided?

Sample answer: The most important thing that you will notice is that when a cyber-attack is reported an investigation must originally take place. For this reason, the purpose of attack might not be obvious from the beginning alongside with the techniques used. This makes also the prevent mechanisms harder to be identified. Company X cyber-attack: Around 230000 clients' credit card details, billing information was stolen from the company. The type is not clear, but it is obvious that the attackers were passively gathering information as they remained undetected for more than 3 weeks. It is obvious that the company should have used encryption in their transaction system and had employed more secure ways of storing their customer data. For example, this valuable information should have been stored in a separate server and only accessed by authorized personnel which was necessary to do so.

Question 6

Kate is going to a café between classes, so she can work on her thesis; she has chosen the TEXT coffee shop as it has free WIFI connection. Is it safe for Kate to use the TEXT's WIFI? Can you suggest any techniques to Kate, in order to keep her online activities' secure?

Some ideas: Do not keep essential data on the laptop using with untrusted networks. Have antivirus employed and updated. Use of VPN, encryption. Do not log in to any accounts while on free Wi-Fi. If the free Wi-Fi asks you to register with an email and more details, does not mean that this connection is more secure because an authentication mechanism exists

Question 7

The board of Phoenix Corp is debating whether they should employ the use of Cloud Services for their data; What do you think can be the downfall and on the other hand the positive impact of this decision (on a cyber security aspect)?

Some ideas: Data stored on other countries? Be careful when choosing vendors. Same space shared with other companies. Do you know who is sharing the space with your company? Loss of data and leakage; unable to access data. Store only necessary data that will not cause data breach. Accessibility, outsourcing storage → decrement of necessary budget as the service is outsourced and most of the times it is cheaper than having your own infrastructure. One good solution is to build you own cloud service which gives more control but at the same time is more expensive. If the outsourcing solution is preferred, then attention to the contract is important so all the previously mentioned points will be taken into serious consideration and any necessary legalities will be put into place.

Cyber Security Tutorial 2

Instructions

In this tutorial you should work preferably in pairs or alone. Try to answer all the questions together and discuss the possible answers/solutions. You will be given 30 minutes to complete this task and, in the end, a general discussion will take place in class based on the content of this tutorial. Try to answer as many questions as you can!

Question 1

You are given a variety of port numbers. Please fill in the table with the protocols normally associated with these port numbers and briefly explain what every protocol is used for.

Port Number	Protocol	Description
23	TELNET(tcp/udp)	Default port for telnet connection; transport layer can use either tcp or udp. Telnet is a text based two-way communication protocol, used for accessing remote hosts. Lacks authentication policies and encryption.
53	DNS (Domain Name System) (tcp/udp)	Default port for dns; transport layer can use either tcp or udp. DNS deals with any dns requests as mentioned in our lectures. No use of cryptographic signatures.
43	NICNAME/WHOIS (tcp/udp)	Default port for nicname/whois; transport layer can use either tcp or udp. Nicname/whois deals with requests on databases that hold information about internet resources like IP address allocations, domain names and more. Lacks access control, integrity and confidentiality.
20	FTP-data (File Transfer Protocol) (tcp/udp/sctp)	Default port (active) for ftp-data; transport layer can use either tcp, udp or sctp (stream control transmission protocol). FTP-data is used for transferring files. No encryption used.
69	TFTP (Trivial File Transfer Protocol) (tcp/udp)	Default port for tftp; transport layer can use either tcp or udp. TFTP (more limited features than FTP) mostly used for reading/writing files/mail to or from a remote server. No security or authentication while transferring files.
25	SMTP (Simple Mail Transfer Protocol) (tcp/udp)	Default port for smtp; transport layer can use either tcp or udp. SMTP is an Internet standard for email transmissions. No authentication.
22	SSH (Secure Shell) (tcp/udp/sctp)	Default port for SSH connection; transport layer can use either tcp, udp or sctp (stream control transmission protocol). SSH is used for accessing remote hosts; described by many as the secure version of telnet.
80	HTTP (HyperText Transfer Protocol) (tcp/udp/sctp)	Default port for http; transport layer can use either tcp, udp or sctp. HTTP is encounterented on the World Wide Web in order to access web content. No use of encryption.
366	ODMR (On-Demand Mail Relay) (tcp/udp)	Default port for odmr; transport layer can use either tcp or udp. ODMR is an Internet standard for email transmissions and is an extension of SMTP. The main difference is that it uses dynamic IP addresses instead of static ones.
110	POP3 (Post Office Protocol) (tcp/udp)	Default port for pop3; transport layer can use either tcp or udp. POP3 is the most recent protocol for email transmissions but only on the receiving side (protocol which deals with receival of emails). Can support encryption.
443	HTTPS	Default port for https; transport layer can use either tcp, udp

	(tcp/udp/sctp)	or sctp. HTTPs is encounterented on the World Wide Web in order to access web content. HTTPS is the encrypted version of HTTP.
21	FTP (File Transfer Protocol) (tcp/udp/sctp)	Default port for ftp (passive); transport layer can use either tcp, udp or sctp (stream control transmission protocol). FTP is not responsible for transferring the data but for mainly dealing with control data. Like OK messages, relevant that the file has been received and more. No encryption used.
115	SFTP (Secure File Transfer Protocol) (tcp/udp)	Default port for sftp; transport layer can use either tcp or udp. That is for unsecured connection. If SSH is used for authentication and then a secure file access, transfer and management is ensured then is port 22.
989	FTPS-data (File Transfer Protocol) (tcp/udp)	Default port for ftps-data; transport layer can use either tcp or udp. FTPS-data is used for transferring files. The difference with ftp-data is that ftps is using TLS which is secure transfer of data by using encryption.
123	NTP (Network Time Protocol) (tcp/udp)	Default port for ntp; transport layer can use either tcp or udp. NTP is used for the clock synchronization between the computing systems.
137	NETBIOS-NS (Network Basic Input Output System-Name Service) (tcp/udp)	Default port for netbios-ns; transport layer can use either tcp or udp. NETBIOS-NS is used for similar purposes like DNS, but in this case is asking information about NETBIOS names. This is normally traffic you would encounter on Windows machines and the names which help specify the workgroups.
445	MICROSOFT-DS (Directory Service) (tcp/udp)	Default port for microsoft-ds; transport layer can use either tcp or udp. MICROSOFT-DS is used to provide access to file and print sharing services (Wannacry exploit).

Question 2

Discuss between your team why it is important to know which protocol is associated with a port number. Is there any good reason considering the cyber security aspect?

Port scanning is used to identify which ports are open and which are closed. This helps experts to identify if the security policies which are employed are active and on the other side hackers can identify what is open and might be exploitable. Just see it as a door that can be identified, and someone can try to break through. By identifying this port, they can search for any known services that use this port or known vulnerabilities if the system is unpatched and start to plan the next step of their multistage attack.

Question 3

Identify different types of DNS records and explain their meaning. Try to identify through your research at least five of them.

DNS server provides important information about a domain/hostname and its relevant IP address. This information is provided by the creation of something known as DNS records. Some common types of DNS records are the following:

1) Address Mapping (A) → DNS host record; stores hostname and corresponding IPv4 address.
2) IPv6 Address record (AAAA) → Exactly the same as previously but instead of IPv4, the IPv6 address is stored.
3) Name Server records (NS) → redirects to a specific Authoritative Name server and provides the address of the name server, as in our schema from the lecture with Amazon.
4) Certificate record (CERT) → stores encryption certificates.
5) Start of Authority (SOA) → this record is encountered in the beginning of the DNS file and has

important information; the relevant Authoritative Name Server, domain serial number, refreshing rate of DNS information, contact details for the domain administrator.

6) Text record (TXT) → contains machine readable data like sender policy framework and more.
7) Mail exchanger record (MX) → information regarding the SMTP email server for the domain (responsible for routing outgoing email to an email server).
8) Canonical Name record (CNAME) → Basically when a record of another hostname is requested (aliases).
9) Service Location (SRV) → Same with MX but for other communication protocols.
10) Reverse-lookup Pointer records (PTR) → for reverse DNS lookup (provide IP and receive hostname).

Question 4

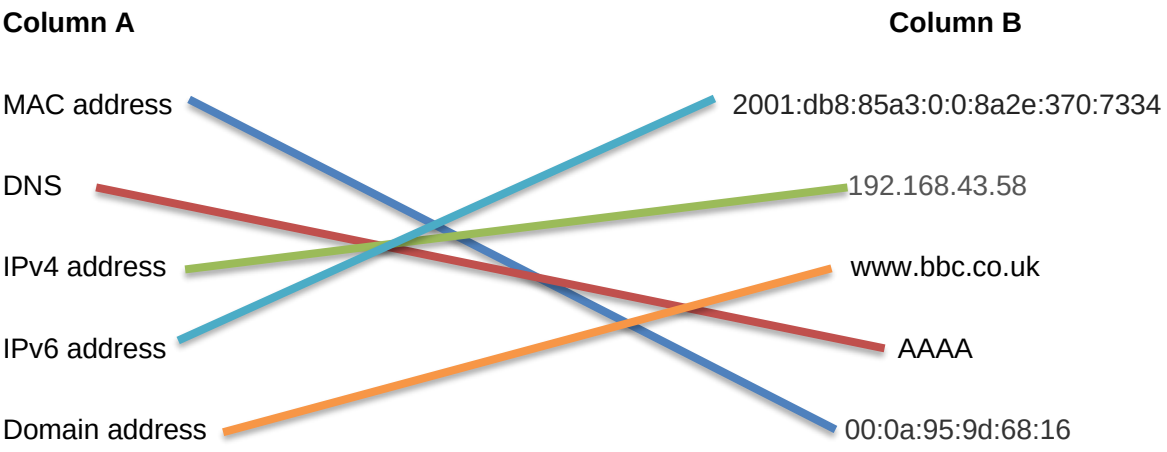
How many versions of IP addresses exist and what are their differences?

There are two versions of IP addresses; IPv4 and IPv6. IPv6 is the successor of IPv4 (32 bit addresses). Most of IPv4 addresses have been assigned, so the creation of IPv6 was necessary (128 bit addresses).

Question 5

Below you will be given two columns that you will be asked to match accordingly. One column refers to different type of addresses in networking and the other gives examples. You are being asked to make the correct connection.

There is an intentional confusing bit in this question. For the DNS in column A, DNS is not really represented with AAAA as this is not an address. However, AAAA is referring to a type of DNS record.



Question 6

What is the range of local IPv4 addresses?

This what is known as RFC 1918 addresses which is a standard that assigns IP addresses in a private network. The following table demonstrates addresses that cannot be routed on the Internet and are reserved for use in private networks.

10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

Question 7

DISCLAIMER: UNDER NO CIRCUMSTANCE YOU MUST USE WIRESHARK OTHER THAN WHAT INSTRUCTED BY YOUR LECTURER. YOU WILL ONLY OPEN THE SAMPLE WHICH WAS PROVIDED THROUGH MOODLE FOR EXAMINATION. YOUR LECTURER WILL NOT BE RESPONSIBLE FOR ANY OTHER USE.

You will be given a networking sample that you can open with Wireshark. All necessary files have been uploaded to Moodle. Investigate the sample and try to identify important information:

1) What is the communication about?

   In this communication we can identify lots of things that we discussed in the lecture. First of all, we have a DNS request going through our router asking for the IP address, both IPv4 (A) and IPv6 (AAAA) for the website: www.gla.ac.uk. The purple area describes the functionality of the browser for a secure communication; so, it enables the https functionality of the website and you will see that port 443 is activated (https). After this a response will come through our router to our host system (refer it as laptop for simplicity) with the information we asked, which is the IP address of the website. Afterwards, a handshake is taking place between the machine that made the initial request (laptop) and the server IP address of the website. After the handshake the laptop will get access to the website and load the webpage. GET request is satisfied.

2) Which protocols can you identify and what is their use?

   DNS, TCP and TLS. DNS is for identifying the IP address. TCP for exchanging the information and the request. TLS is for enabling the secure communication in the browser.

3) What is the source IP address, port and the destination IP, port?

   Source IP (laptop): 10.0.2.15

   Source port (laptop): 39769 for DNS request 51424 for webpage connection

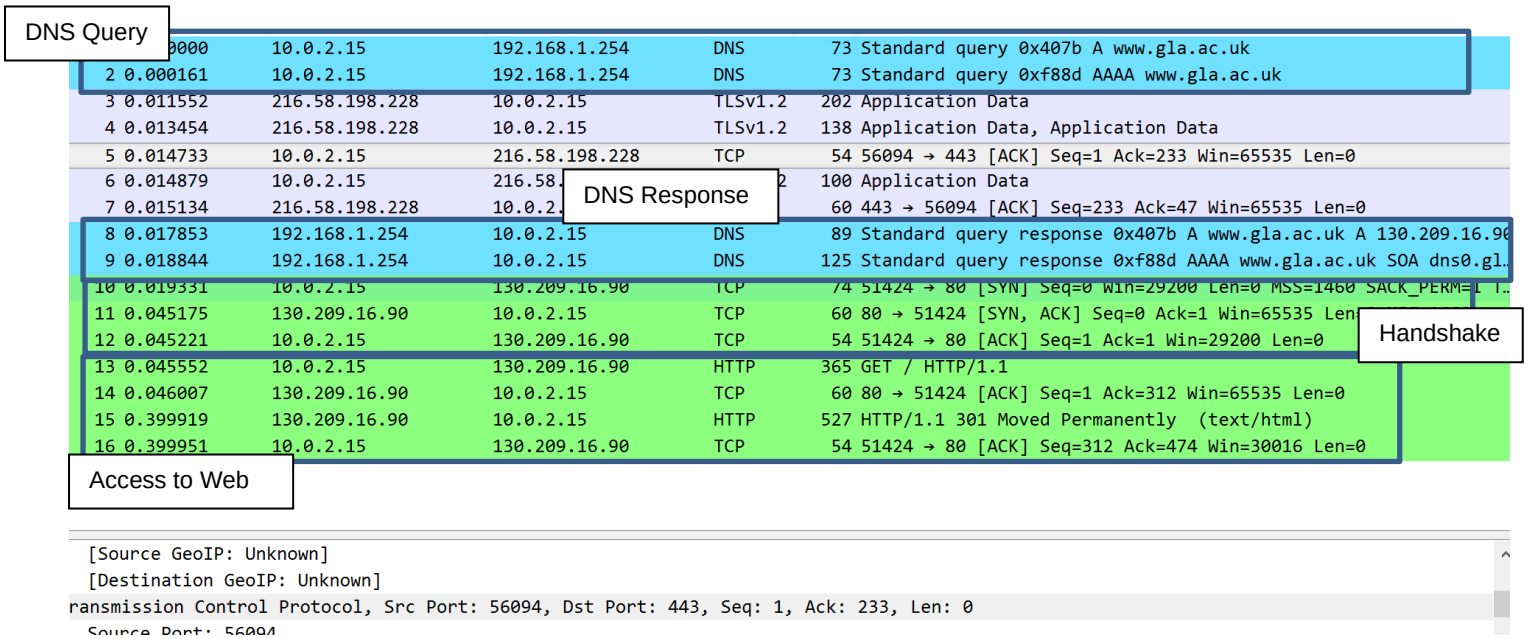
   Destination IP (webpage): 130.209.16.90

   Destination port (webpage): 80

   Port 443 (https) is enabled by the browser before the handshake.

4) Anything else that is notable in the sample?

   Code 301 Moved permanently is used for permanently redirection, meaning that current links should be updated. The 301 redirection is a good practice from upgrading from http to https.



Cyber Security Tutorial 3

Instructions

In this tutorial you should work preferably in pairs or alone. Try to answer all the questions together and discuss the possible answers/solutions. You will be given 30 minutes to complete this task and, in the end, a general discussion will take place in class based on the content of this tutorial. Try to answer as many questions as you can!

Question 1: Please choose the right answer from the given choices by filling in the gaps where necessary.

1) When a group of computers is being used from hackers for malicious activities, we talk about a/an _____.
   - Network Scanning
   - Trojan Horse
   - **Botnet**
   - Army of hacks

2) When someone has stolen your data, encrypted them and try to extort money; we have a/an _____attack.
   - DDOS (Distributed Denial of Service)
   - **Ransomware**
   - Phishing
   - Man in the middle
   - Identity Theft

3) If you share lots of information about your life on social media, you are exposed to possible _____.
   - DDOS (Distributed Denial of Service)
   - Ransomware
   - Phishing
   - Man in the middle
   - **Identity Theft**

4) When you have received a/an_____email, it is better to make the IT team aware of this incident.
   - DDOS (Distributed Denial of Service)
   - Ransomware
   - **Phishing**
   - Man in the middle
   - Identity Theft

5) ARP Spoofing is one of the most common strategies for a successful_____attack.
   - DDOS (Distributed Denial of Service)
   - Ransomware
   - Phishing
   - **Man in the middle**
   - Identity Theft

6) Someone can use a Zombie Network in order to employ a/an_____attack.
   - **DDOS (Distributed Denial of Service)**
   - Ransomware
   - Phishing
   - Man in the middle
   - Identity Theft

Question 2

Identify and explain the following terms; give some examples if needed; 1) pulsing zombie, 2) shoulder surfing, 3) sandbox, 4) dumpster diving, 5) walled garden.

1) Pulsing zombie; A regular zombie paralyzes a system with a steady stream of attack traffic. However, the pulsing zombie use irregular small bursts of attack traffic from multiple sources on a single target over an extended period. These attacks are more difficult to detect and trace because they are slow and gradual, so they do not immediately appear as malicious.
2) Shoulder surfing; act of obtaining personal or private information through direct observation. Looking over a person's shoulder to gather pertinent information while the victim is unaware. Binoculars, video cameras and vision-enhancing devices can be used, depending on location and situation.
3) Sandbox; testing environment that enables the isolated execution of software or programs for independent evaluation, monitoring or testing.
4) Dumpster diving; general searching through trash or garbage looking for something useful. Trying to uncover useful information that may help an individual get access to a network.
5) Walled garden; various meanings → quarantining computers prone to attacks, such as computers showing the symptoms of botnet activity from malware. → restricted environment in which in order to leave the environment and unauthenticated user should create an account. → web environment with restrictions to certain content and areas.

Question 3

What is spyware and how does it work? Give an example of a well-known spyware.

Infiltration software that secretly monitors users and enables malicious entities to obtain sensitive information, such as passwords, from the user's computer. It exploits user and application vulnerabilities and is often attached to free online software downloads or to links that are clicked by users.

Question 4

What procedure do you think is the hardest for a malicious entity when he/she initiates a cyber-attack? Discuss between your team the different opinions you might have.

The answer can be so different depending on different perspectives. For example, one of the students in class replied that the biggest challenge is the payload. As it can be so tricky to execute an attack because of complications that might come up due to the different defend mechanisms that might be in place. However, we will go through all steps in detail in class and you can also consider that trying to stay anonymous as an attacker is a huge challenge too. As once an attacker is caught then this is it.

Question 5

What is DNS poisoning/spoofing? Explain this type of attack and how it can be successfully implemented. What would be considered a good mitigation method?

The process of illegitimately modification of DNS records to replace a website address with a different one. DNS cache poisoning is used to redirect visitors of a website to their defined/desired website (malicious). Some mitigation: Disable DNS recursion; the DNS server allows recursive queries for other domains and this means it allows third-party hosts to query the name servers as they want. Regular patching of DNS servers. Use of DNSSEC (DNS System Security Extensions) protocol using a set of extensions for extra authentication.

Question 6

Use one laptop if possible and try to ping a website you are interested in; by typing in command line “ping <website>” or use the IP address instead of the website. What are the replies you get? After, completion instead of ping try the tracert command. Explain in both cases the information presented to you.

Pinging the university website externally:

```
Pinging www.gla.ac.uk [130.209.16.90] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 130.209.16.90:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

This means that either the website is down; which is not true or that the provider has disabled external ping requests.

Pinging another website like facebook:

```
C:\Users\Maria>ping www.facebook.com

Pinging star-mini.c10r.facebook.com [2a03:2880:f11a:83:face:b00c:0:25de] with 32 bytes of data:
Reply from 2a03:2880:f11a:83:face:b00c:0:25de: time=17ms
Reply from 2a03:2880:f11a:83:face:b00c:0:25de: time=17ms
Reply from 2a03:2880:f11a:83:face:b00c:0:25de: time=16ms
Reply from 2a03:2880:f11a:83:face:b00c:0:25de: time=15ms

Ping statistics for 2a03:2880:f11a:83:face:b00c:0:25de:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 17ms, Average = 16ms
```

First thing is that the host is running plus we can see the use of IPv6 addresses. The first four groups of digits represent the network portion of the IPv6 address, while the last four groups represent the specific host within that network. Default ping requests number for windows is 4; therefore, you can see 4 replies.

Use of tracert:

```
C:\Users\Maria>tracert www.facebook.com

Tracing route to star-mini.c10r.facebook.com [2a03:2880:f129:83:face:b00c:0:25de]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  broadband.  .com
  2     *        *        *     Request timed out.
  3    15 ms    13 ms    14 ms  2a00:2302::1103:100:32
  4    14 ms    14 ms    15 ms  2a00:2302::1103:100:3b
  5    15 ms    14 ms    14 ms  2a00:2380:3013:8000::22
  6    18 ms    14 ms    14 ms  peer2-et0-1-1.slough.ukcore.bt.net [2a00:2380:13::89]
  7    15 ms    16 ms    16 ms  2a00:2380:2015:2000::11
  8    15 ms    15 ms    15 ms  po111.asw01.lhr3.tfbnw.net [2620:0:1cff:dead:beef::3eb4]
  9    15 ms    15 ms    15 ms  po556.psw04.lhr6.tfbnw.net [2620:0:1cff:dead:beef::3f1f]
 10    15 ms    15 ms    15 ms  po1.msw1ax.01.lht6.tfbnw.net [2a03:2880:f01a:ffff::32f]
 11    18 ms    16 ms    16 ms  edge-star-mini6-shv-01-lht6.facebook.com [2a03:2880:f129:83:face:b00c:0:25de]

Trace complete.
```

Tracert; track the pathway taken by a packet on an IP network from source to destination. Traceroute also records the time taken for each hop the packet makes during its route to the destination. In this example you can see how many hops needed to reach facebook's website.