Introduction to Ethical Hacking

Technical Skills Needed as an Ethical Hacker

Basic skills:

* Linux(Kali)

* Networking(OSI Models, protocols, etc)

* Scripting skills(Python, Bash, etc.)

* Solid Hacking methodology

* Tool familiarity (Metasploit, Burp Suite, Nessus, etc.)

Preferred skills(Added Advantage)

* Active directory

* Wireless Attacks

* OWASP Top 10

* Coding skills (Python, Bash, etc)

Soft Skills Needed

* Strong Desire to learn

* Non-complacency- always want to move up

* Social/people skills

* Perseverance

* Blog/Twitter/Podcasts/GitHub- give back to the community, stay updated

Effective NoteKeeping

KeepNote- Linux, Mac, Window

Cherrytree- Kali

Joplin-Mac

OneNote

For screenshots- Greenshot, Flameshot, etc.

Networking Refresher

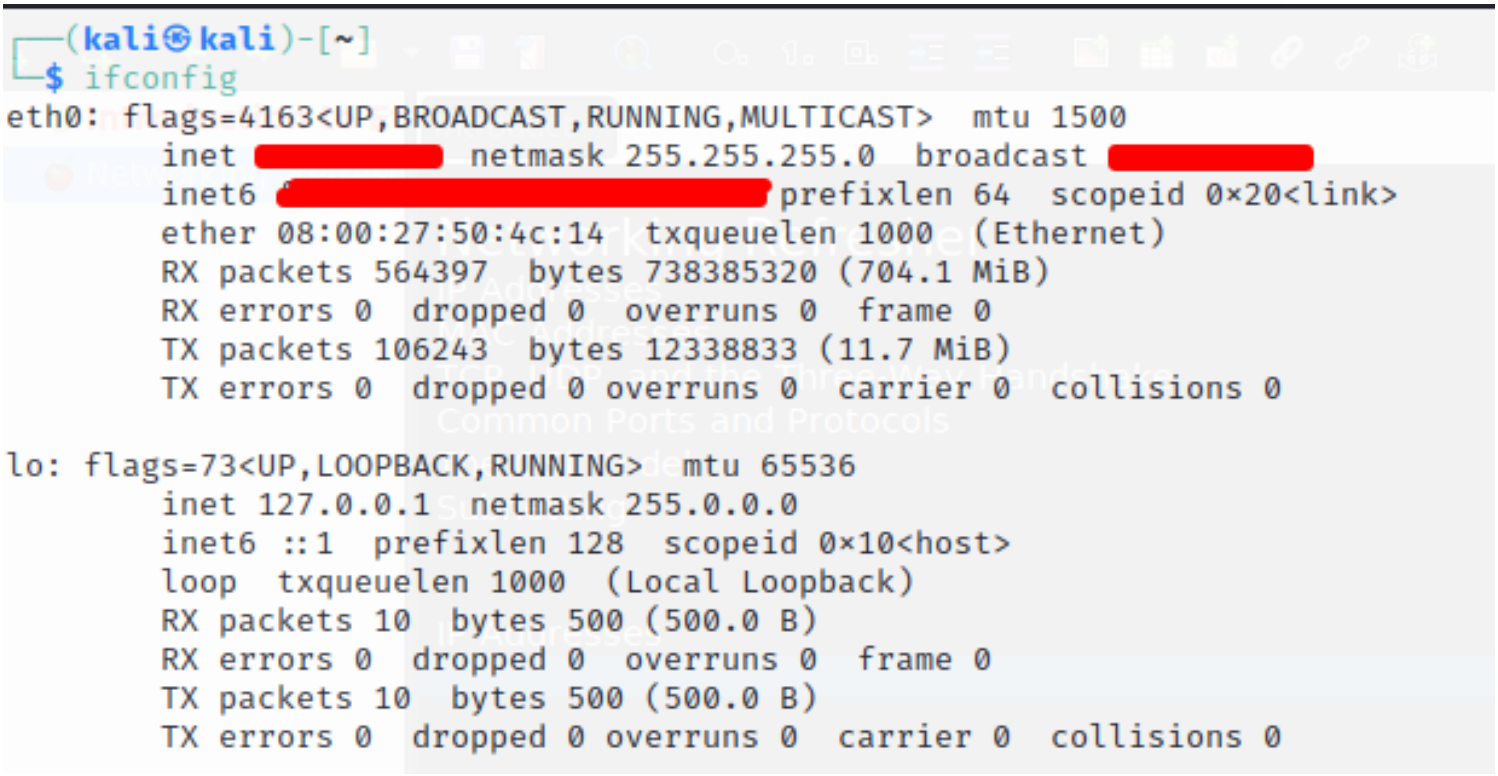
Networking Refresher

- IP Addresses
- MAC Addresses
- TCP, UDP, and the Three-Way Handshake
- Common Ports and Protocols
- The OSI Model
- Subnetting

IP Address

IP Addresses

An IP address, or Internet Protocol address, is a series of numbers that identifies any device on a network. Computers use IP addresses to communicate with each other both over the internet as well as on other networks
To check the IPaddress of your computer use the ifconfig command



inet- IPv4
inet6- IPv6
ether-MAC Address/ Physical Address

There are two types of IP addresses: IPv4 and IPv6.
IPv4 addresses contain a series of four numbers, ranging from 0 (except the first one) to 255, each separated from the next by a period — such as 5.62.42.77.
IPv6 addresses are represented as eight groups of four hexadecimal digits, with the groups separated by colons. A typical IPv6 address might look like this: 2620:0aba2:0d01:2042:0100:8c4d:d370:72b4.
IPv4 addresses are 32-bit numbers, and the total number of possible addresses of that length is 232 —about 4.3 billion. That number seemed sufficient in the early days of the internet, but began to loom as a potential crisis as internet-connected devices multiplied
The anxiety that IPv4 addresses were going to run out is what drove the development of IPv6. . IPv6 addresses are 128-bit numbers, which means that there are 2128 possible addresses, a number that we're not going to bother writing out because it's 39 digits long, but it's called 340 undecillion.

Parts of an IPv4 Address
An IP address has two parts: the network ID, comprising the first three numbers of the address, and a host ID, the fourth number in the address. So on your home network — 192.168.1.1, for example – 192.168.1 is the network ID, and the final number is the host ID.
The Network ID indicates which network the device is on. The Host ID refers to the specific device on that network. (Usually your router is .1, and each subsequent device gets assigned .2, .3, and so on.)
You may not always want the outside world to know exactly which device and network you're using. In this case, it's possible to mask your IP address from the outside world through a Virtual Private Network (VPN). When you use a VPN, it prevents your network from revealing your address.

Public and Private Networks
A typical home or corporate network connects to the public internet via a router, and it's this router that's assigned an IP address by the ISP. From the perspective of the outside world, all traffic from devices on that local network are coming from that public IP address; but inside the network, each device (including the router) has a local private IP address, usually assigned by the router via Dynamic Host Configuration Protocol (DHCP).

These addresses are considered private because they’re only used for directing packets within the local, private network, and can’t be seen by anyone outside the network. As result, the same IP address can be used on an infinite number of private networks without causing confusion. In fact, there are blocks of IP addresses specifically set aside for use on these private networks. (For small home networks, addresses starting with 192.168 are quite common.)

Private IP address

Network Class	Network Numbers	Network Mask	No. of Networks	No. of Hosts per Network
CLASS A	10.0.0.0	255.0.0.0	126	16,646,144
CLASS B	172.16.0.0 to 172.31.0.0	255.255.0.0	16,383	65,024
CLASS C	192.168.0.0 to 192.168.255.255	255.255.255.0	2,097,151	254
LOOPBACK (localhost)	127.0.0.0 to 127.0.0.7	255.255.255.0	-	-

MAC Address

MAC Address

While the IP address helps identify a device connected to a network, the Media Access Control address (MAC address) is a hardware identifier that uniquely identifies each device on a network. Primarily, the manufacturer assigns it. They are often found on a device's network interface controller (NIC) card. A MAC address can also be referred to as a burned-in address, Ethernet hardware address, hardware address, or physical address.

The IPv4 and IPv6 addresses operate on layer 3(communicate using routers) of the OSI model whereas the MAC addresses operate on layer 2(communicate using switches)
Identified as ‘ether’ in the ifconfig command
A MAC address is a 48-bit hexadecimal address. It is usually six sets of two digits or characters, separated by colons. An example MAC address would be 00:00:5e:00:53:af.

How a MAC address and IP address work together

The bridge between them: ARP
While MAC and IP addresses have many differences, they are not islands unto themselves. The Address Resolution Protocol (ARP) is the bridge that connects them. This protocol works between Layer 2 and Layer 3 on a local area network (LAN). It maps IPv4 addresses to network devices’ MAC addresses and vice versa.
(Note: IPv4 uses the ARP protocol. On newer IPv6 networks, the Neighbor Discovery Protocol provides the equivalent functionality.)

Here’s how it works: A device wants to communicate with another device on the local network segment. It puts its request with both the source IP address and a destination IP address into an IP packet. An Ethernet frame then encapsulates the IP packet. The frame contains both a source and destination MAC address as well.

But sometimes the MAC address of the destination device is unknown. In steps ARP.

Computer A wants to send an IP packet to computer B. But it does not know the MAC address of computer B. Computer A will then broadcast an ARP request received by all computers on the local network segment.
The request will essentially say, “This is my IP address. This is my MAC address. And I am looking for the MAC address associated with this IP address. If this IP address is yours, please respond and give me your MAC address.”

Computer B receives the ARP request and will do two things.
First, every device has its own ARP table. Each time a computer wants to send a packet on the LAN, it will look in its ARP table first. If an entry for Computer A does not already exist in Computer B’s table, it will make one. It will add computer A’s MAC and IP addresses based on what is in the frame. Then, it will send an ARP reply with its IP address and MAC address. Computer A will receive the reply and add the info to its ARP table. With the right MAC address, Computer A can now send the Ethernet frame to Computer B.

• It is 12 digits or 6-byte hexadecimal number, which is represented in colon-hexadecimal notation format. It is divided into six octets, and each octet contains 8 bits.
• The first three octets are used as the **OUI or Organisationally Unique Identifier**. These MAC prefixes are assigned to each organization or vendor by the IEEE Registration Authority Committee.
• Some example of OUI of known vendors are:
CC:46:D6 - Cisco
3C:5A:B4 - Google, Inc.
3C:D9:2B - Hewlett Packard
00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD

• The last three octets are NIC specific and used by the manufacturer to each NIC card. Vendors or manufacturers can use any sequence of digits to the NIC specific digits, but the prefix should be the same as provided by the IEEE.

TCP, UDP, 3-Way Handshake

TCP, UDP, 3-WAY HANDSHAKE
Layer 4- Transport Layer of the OSI model

TCP-Transmission Control Protocol (Connection Oriented)

The TCP stands for Transmission Control Protocol. If we want the communication between two computers and communication should be good and reliable. For example, we want to view a web page, then we expect that nothing should be missing on the page, or we want to download a file, then we require a complete file, i.e., nothing should be missing either it could be a text or an image. This can only be possible due to the TCP. It is one of the most widely used protocols over the TCP/IP network.Used by HTTPS, HTTP, SMTP, POP, FTP, etc

UDP- User Datagram Protocol (Connectionless)

The UDP stands for User Datagram Protocol. Its working is similar to the TCP as it is also used for sending and receiving the message. The main difference is that UDP is

a connectionless protocol. Here, connectionless means that no connection establishes prior to communication. It also does not guarantee the delivery of data packets. It does not even care whether the data has been received on the receiver's end or not, so it is also known as the "fire-and-forget" protocol. It is also known as the "fire-and-forget" protocol as it sends the data and does not care whether the data is received or not. UDP is faster than TCP as it does not provide the assurance for the delivery of the packets. Video conferencing, streaming, DNS, VoIP, etc

	TCP	UDP
Full form	It stands for **Transmission Control Protocol**.	It stands for **User Datagram Protocol**.
Type of connection	It is a connection-oriented protocol, which means that the connection needs to be established before the data is transmitted over the network.	It is a connectionless protocol, which means that it sends the data without checking whether the system is ready to receive or not.
Reliable	TCP is a reliable protocol as it provides assurance for the delivery of data packets.	UDP is an unreliable protocol as it does not take the guarantee for the delivery of packets.
Speed	TCP is slower than UDP as it performs error checking, flow control, and provides assurance for the delivery of	UDP is faster than TCP as it does not guarantee the delivery of data packets.
Header size	The size of TCP is 20 bytes.	The size of the UDP is 8 bytes.
Acknowledgment	TCP uses the three-way-handshake concept. In this concept, if the sender receives the ACK, then the sender will send the data. TCP also has the ability to resend the lost data.	UDP does not wait for any acknowledgment; it just sends the data.
Flow control mechanism	It follows the flow control mechanism in which too many packets cannot be sent to the receiver at the same time.	This protocol follows no such mechanism.
Error checking	TCP performs error checking by using a checksum. When the data is corrected, then the data is retransmitted to the receiver.	It does not perform any error checking, and also does not resend the lost data packets.
Applications	This protocol is mainly used where a secure and reliable communication process is required, like military services, web browsing, and e-mail.	This protocol is used where fast communication is required and does not care about the reliability like VoIP, game streaming, video and music streaming, etc.

Three Way Handshake

TCP uses a three-way handshake to establish a reliable connection. The connection is full duplex, and both sides synchronize (SYN) and acknowledge (ACK) each other.

• **Step 1 (SYN):** In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with

• **Step 2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with

• **Step 3 (ACK):** In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer

Common Ports and Protocols

Common ports and Protocols

A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection.

There are 65,535 possible port numbers, although not all are in common use. Some of the most commonly used ports, along with their associated networking protocol, are:
• **Ports 20 and 21:** File Transfer Protocol (FTP). FTP is for transferring files between a client and a server. It basically lays down all the rules which are to be followed during the transfer of data. Due to the concern of security, it also asks for authentication by the user before the transfer of data. It is associated with the TCP protocol. Port 20 performs the task of forwarding and transferring of data. It takes over the task of transferring FTP data when it is in active mode. Port 21 performs the task of signaling for FTP. It listens to all of the commands and provides a flow control for data. It is quite essential for maintaining the flow of data.

• **Port 22:** Secure Shell (SSH). SSH is one of many tunneling protocols that create secure network connections.- encrypted version of telnet. It operates on the port number 22 of the TCP protocol. It carries out the task of remotely connecting to a remote server or host. It allows you to execute a number of commands and move your files remotely as well. However, it is one of the most secure ways of accessing your files remotely. Using this port, you can remotely connect to a computer and move your files with ease. This port sends the data over the network in an encrypted form which adds an extra layer of security on it. In addition to this, only authorized people will be able to remotely log on to their systems using the Port 22 which makes sure that the information does not get into unauthorized hands.

• **Port 23:** Telnet(ability to log into a machine remotely). Its main function is to establish a connection between a server and a remote computer. It establishes a connection once the authentication method has been approved. However, this port is not suitable to establish secure connections and does not cater to the concern of security. It enables the remote connection of a computer to be established with routers and switches as well. It makes use of a virtual terminal protocol to make a connection with the server. It comes into existence during the application layer of the TCP/IP protocol.

• **Port 25:** Simple Mail Transfer Protocol (SMTP). SMTP is used for email.The primary purpose of this protocol is to make sure that email messages are communicated over the network securely. This port usually comes into being during the Application layer. Not only does this protocol carry out the task of delivering messages within networks, i can also successfully deliver messages between different networks. This makes it one of the most important ports for the communication of messages over the network due to the security and it provides along with other features. However, you do not have the privilege to download the emails in order to read them; it is just intended for the purpose of transferring them over the network.

• **Port 53:** Domain Name System (DNS). DNS is an essential process for the modern Internet; it matches human-readable domain names to machine-readable IP addresses, enabling users to load websites and applications without memorizing a long list of IP addresses.

• **Port 67, 68:** DHCP.DHCP is also known as 'Dynamic Host Configuration Protocol'. It basically runs on the UDP protocol. The basic purpose of DHCP is to assign IP Address related information to the clients on a network automatically. This information may comprise of subnet mask, IP Address etc. Many of the devices are automatically configured to look for IP Addresses using DHCP when they

connect on a network. It makes it quite reliable to assign all the devices on a network with automatically produced IP Addresses. It generally operates on the Application layer of the TCP/IP Model. DHCP basically makes use of 2 ports; Port 67 and Port 68.

• **Port 80:** Hypertext Transfer Protocol (HTTP). HTTP is the protocol that makes the World Wide Web possible. The main purpose of port 80 is to allow the browser to connect to the web pages on the internet. Port 80 basically expects or waits for the web client to ask for a connection. Once this connection has been made, you will get the privilege to connect to the World Wide Web and get access to various web pages out there. In fact, HTTP - 80 is one of the most important ports associated with the TCP protocol. Moreover, this port is generally used during the application layer of the TCP/IP Model.

• **Port 110:** POP3. POP3 is also referred to as Post Office Protocol Version 3. It operates on the port 110 of TCP Protocol. It allows the email messages to be retrieved from the SMTP servers. Using this port, you can download the messages from the server and then read them. However, this means that you will not be able to access the messages and read them without downloading them. Furthermore, the messages are also deleted from the server once they are downloaded. However, this port does not cater to the issue of security. The authentication details transferred over the network are not encrypted and sent in plain text. This means that any hacker can easily intercept this information and misuse it. Port 110 generally operates on the Application layer of the TCP/IP Model.

• **Port 123:** Network Time Protocol (NTP). NTP allows computer clocks to sync with each other, a process that is essential for encryption.
• **Port (139+445):** SMB-file shares. Eternal Blue utilized a SMB exploit to navigate through networks

• **Port 143:** IMAP. IMAP is the abbreviation of 'Internet Message Access Protocol'. The IMAP -143 Port lies under the category of TCP protocol. The primary purpose of this port is to retrieve emails from a remote server without having the need to download the email. You have the liberty to access the emails from anywhere by connecting to the server and viewing your email after providing authentication. This opportunity has been provided to you because of the existence of this port. It reserves a virtual memory for the email which enables you to read it by connecting to the server. However, you may also download the mail if you wish to. It also provides you the ability to search for your messages from a bunch of them to get to your desired one. IMAP 143 Port generally operates at the Application Layer of a TCP/IP Model. In addition to this, it also makes sure that the data remain secure during this connection.

• **Port 179:** Border Gateway Protocol (BGP). BGP is essential for establishing efficient routes between the large networks that make up the Internet (these large networks are called autonomous systems). Autonomous systems use BGP to broadcast which IP addresses they control.
• **Port 443:** HTTP Secure (HTTPS). HTTPS is the secure and encrypted version of HTTP. All HTTPS web traffic goes to port 443. Network services that use HTTPS for encryption, such as DNS over HTTPS, also connect at this port. This lets you connect to the World Wide Web. However, this port has an added feature of security to it, which HTTP port 80 does not have. This port is intended for establishing secure connections to make sure that the data is transmitted over a secure network. The use receives a warning if the browser is trying to access a webpage which is not secure. This port comes into being during the application layer. It basically encrypts and authenticates the network packets before transferring them over the network to increase the security. This feature of security is introduced by the use of SSL, which can also be referred to as Secure Socket Layer.

• **Port 500:** Internet Security Association and Key Management Protocol (ISAKMP), which is part of the process of setting up secure IPsec connections.
• **Port 3389:** Remote Desktop Protocol (RDP). RDP enables users to remotely connect to their desktop computers from another device.

OSI Model

The OSI Model
Please Do Not Throw Sausage Pizza Away :)

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s.

7. **Application Layer**
The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

6. **Presentation Layer**
The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

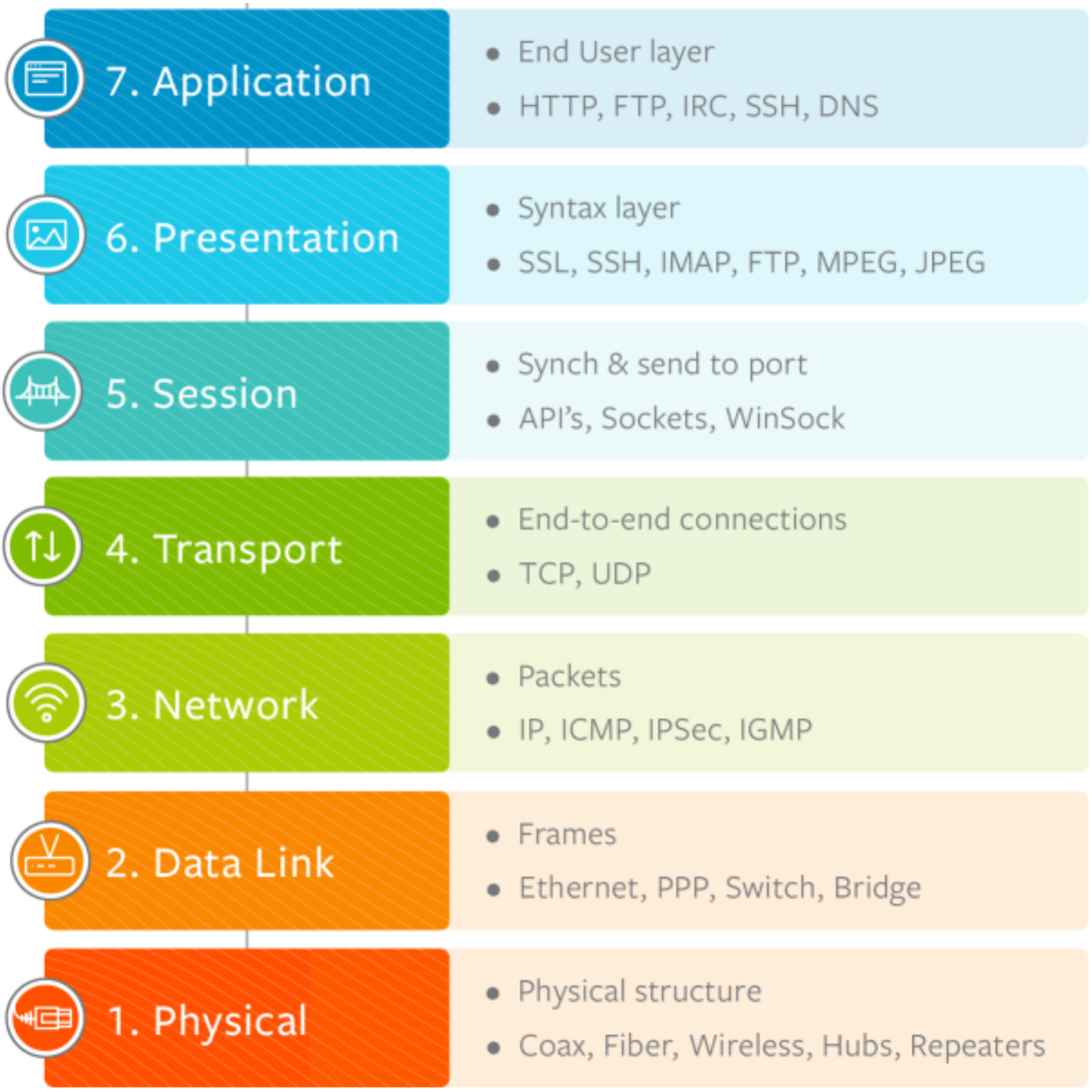
5. **Session Layer**
The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

4. **Transport Layer**
The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

3. **Network Layer**
The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

2. **Data Link Layer**
The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

1. **Physical Layer**
The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.



When we receive data moves from physical to application
When we transmit data moves from application to physical
Troubleshoot-start with physical

Subnetting

Subnetting

What Is Subnetting?
Subnetting is the process of stealing bits from the HOST part of an IP address in order to divide the larger network into smaller sub-networks called subnets. After subnetting, we end up with NETWORK SUBNET HOST fields. We always reserve an IP address to identify the subnet and another one to identify the broadcast subnet address.

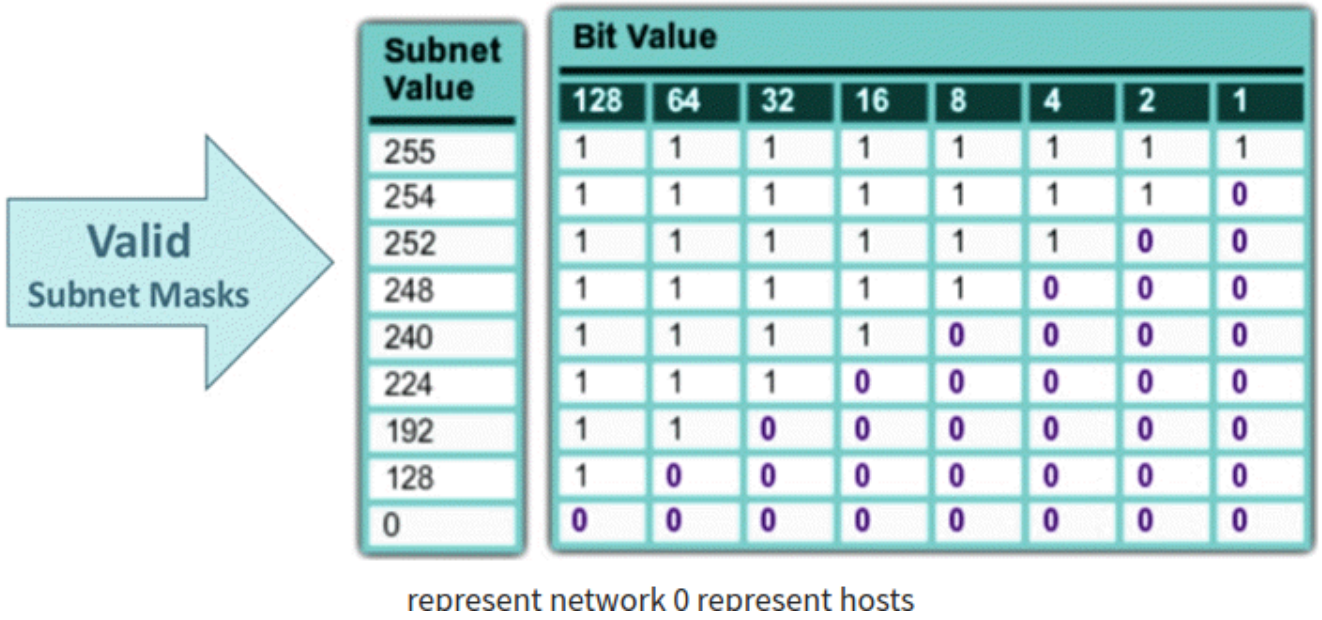
Why Use Subnetting?
1. Conservation of IP addresses: Imagine having a network of 20 hosts. Using a Class C network will waste a lot of IP addresses (254-20=234). Breaking up large networks into smaller parts would be more efficient and would conserve a great amount of addresses.

2. Reduced network traffic: The smaller networks that created the smaller broadcast domains are formed, hence less broadcast traffic on network boundaries.

3. Simplification: Breaking large networks into smaller ones could simplify fault troubleshooting by isolating network problems down to their specific existence.

255.255.255.0- The /24 network, 256 hosts

[8bits.8bits.8bits.8bits]



The Cyber Mentor's Subnetting Sheet								
	Subnet x.0.0.0							
CIDR	/1	/2	/3	/4	/5	/6	/7	/8
Hosts	2,147,483,648	1,073,741,824	536,870,912	268,435,456	134,217,728	67,108,864	33,554,432	16,777,216
	Subnet 255.x.0.0							
CIDR	/9	/10	/11	/12	/13	/14	/15	/16
Hosts	8,388,608	4,194,304	2,097,152	1,048,576	524,288	262,144	131,072	65,536
	Subnet 255.255.x.0							
CIDR	/17	/18	/19	/20	/21	/22	/23	/24
Hosts	32,768	16,384	8,192	4,096	2,048	1,024	512	256
	Subnet 255.255.255.x							
CIDR	/25	/26	/27	/28	/29	/30	/31	/32
Hosts	128	64	32	16	8	4	2	1
Subnet Mask (Replace x)	128	192	224	240	248	252	254	255

Notes:	*Hosts double each increment of a CIDR
	*Always subtract 2 from host total:
	Network ID - First Address
	Broadcast - Last Address