**Explain various types of threats?**

**Identifying Types of Threats:**

Most attacks can be categorized as one of six broad classes:

■ **Malware:** This is a generic term for software that has a malicious purpose. It includes virus attacks,

worms, adware, Trojan horses, and spyware. This is the most prevalent danger to your system.

1. **Virus** – They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. The most common method for spreading a virus is using the victim’s email account to spread the virus to everyone in their address book. Some viruses don’t actually harm the system itself, but all of them cause network slowdowns due to the heavy network traffic caused by the virus replication. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.
2. **Worms** – Worms are also self-replicating in nature but they don’t hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network-aware. They can easily travel from one computer to another if network is available and on the target machine, they will not do much harm, they will, for example, consume hard disk space thus slowing down the computer.
3. **Trojan Horse** – The Concept of Trojan is completely different from the viruses and worms. The name Trojan is derived from the ‘Trojan Horse’ tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside. Their purpose is to conceal themselves inside the software that seem **legitimate** and when that software is executed. they will do their task of either stealing information or any other purpose for which they are designed. They often provide **backdoor gateway** for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission. Examples include **FTP Trojans, Proxy Trojans, Remote Access Trojans etc.**

1. **Spyware** – It is a program or we can say software that monitors your activities on computer and reveal collected information to an interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they install themselves and sits silently to avoid detection. One of the most common examples of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus, capturing interesting information like username, passwords, credit card details etc.
2. **Adware** – Adware is not exactly malicious but they do breach privacy of the users. They display ads on a computer’s desktop or inside individual programs. They come attached with free-to-use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
3. [**Ransomware**](https://www.malwarebytes.com/ransomware/) is a form of malware that locks you out of your device and/or encrypts your files, then forces you to pay a ransom to regain access. Ransomware has been called the cybercriminal’s weapon of choice because it demands a quick, profitable payment in hard-to-trace [cryptocurrency](https://www.malwarebytes.com/blog/101/2017/11/cryptocurrency-works-cybercriminals-love/). The code behind ransomware is easy to obtain through online criminal marketplaces and defending against it is very difficult. While ransomware attacks on individual consumers are down at the moment, attacks on businesses are up 365 percent for 2019. As an example, the [Ryuk](https://www.malwarebytes.com/ryuk-ransomware/) ransomware specifically targets high-profile organizations that are more likely to pay out large ransoms. For more, check out the [Malwarebytes Labs Ransomware Retrospective](https://www.malwarebytes.com/blog/reports/2019/08/labs-quarterly-report-finds-ransomwares-gone-rampant-against-businesses/).
4. [**Rootkit**](https://www.malwarebytes.com/blog/glossary/rootkit/) is a form of malware that provides the attacker with administrator privileges on the infected system, also known as “root” access. Typically, it is also designed to stay hidden from the user, other software on the system, and the operating system itself.
5. A [**keylogger**](https://www.malwarebytes.com/keylogger) is malware that records all the user’s keystrokes on the keyboard, typically storing the gathered information and sending it to the attacker, who is seeking sensitive information like usernames, passwords, or credit card details.
6. [**Malicious cryptomining**](https://www.malwarebytes.com/blog/101/2018/02/how-to-protect-your-computer-from-malicious-cryptomining/)**,** also sometimes called drive-by mining or [cryptojacking](https://www.malwarebytes.com/cryptojacking/), is an increasingly prevalent malware usually installed by a Trojan. It allows someone else to use your computer to mine cryptocurrency like Bitcoin or Monero. So instead of letting you cash in on your own computer’s horsepower, the cryptominers send the collected coins into their own account and not yours. Essentially, a malicious cryptominer is stealing your resources to make money.
7. [**Exploits**](https://www.malwarebytes.com/exploits) are a type of malware that takes advantage of bugs and [vulnerabilities](https://www.malwarebytes.com/glossary/software-vulnerability) in a system in order to give the attacker access to your system. While there, the attacker might steal your data or drop some form of malware. A zero-day exploit refers to a software vulnerability for which there is currently no available defense or fix.

■ **Security breaches:**

* This group of attacks includes any attempt to gain unauthorized access to your system.
* This includes **cracking passwords, elevating privileges, breaking into a server**… all the things you probably associate with the term hacking.

**Common Causes of Security Breaches:**

1. **Hacking:** Exploiting vulnerabilities in software or hardware to gain unauthorized access.
2. **Insider Threats:** Employees or contractors intentionally or unintentionally causing breaches.
3. **Phishing:** Deceptive attempts to obtain sensitive information by masquerading as a trustworthy entity.
4. **Malware:** Installing malicious software that facilitates unauthorized access.
5. **Unpatched Software:** Exploiting known vulnerabilities in outdated software.

■ **Denial of Service Attacks**

* In a denial of service (DoS), the attacker does not actually access the system.
* Rather, he or she simply blocks access from legitimate users (CERT, 2003).
* One common way to do prevent legitimate service is to flood the targeted system with so many false connection requests, that the system cannot respond to legitimate requests.
* DoS is probably the most common attack on the Web.

■ **Web Attacks**

* By their nature, web servers have to allow communications.
* Oftentimes, websites allow users to interact with the website. Any part of a website that allows for user interaction is also a potential point for attempting a web-based attack.
* SQL injections involve entering SQL (Structured Query Language) commands into login forms (username and password text fields) in an attempt to trick the server into executing those commands.
* The most common purpose is to force the server to log the attacker on, even though the attacker does not have a legitimate username and password. While SQL injection is just one type of web attack, it is the most common.

■ **Session Hijacking**

* Session hijacking can be rather complex to perform.
* For that reason, it is not a very common form of attack.
* Simply put, the attacker monitors an authenticated session between the client machine and the server, and takes that session over.

■ **DNS Poisoning**

* Most of your communication on the Internet will involve DNS, or Domain Name Service.
* DNS is what translates the domain names you and I understand (like www.ChuckEasttom.com) into IP addresses that computers and routers understand.
* DNS poisoning uses one of several techniques to compromise that process and redirect traffic to an malicious site, often for the purpose of stealing personal information.

**Explain OSI Reference model in Detail?**

* OSI stands for **Open Systems Interconnection,** where open stands to say non-proprietary.
* It is a 7-layer architecture with each layer having **specific functionality to perform.**
* All these 7 layers work collaboratively to transmit the data from one person to another across the globe.
* The OSI reference model was developed by ISO – **‘International Organization for Standardization’**, in the year **1984.**
* The OSI model consists of seven abstraction layers arranged in a top-down order:

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

**Physical Layer – Layer 1**

* The lowest layer of the OSI reference model is the physical layer.
* It is responsible for the actual physical connection between the devices.
* The physical layer contains information in the form of bits.
* It is responsible for transmitting individual bits from one node to the next.
* When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

**Functions of the Physical Layer**

1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
4. **Transmission mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

**Data Link Layer (DLL) – Layer 2**

* The data link layer is responsible for the node-to-node delivery of the message.
* The main function of this layer is to make sure data transfer is **error-free** from one node to another, over the physical layer.
* When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.
* Protocols Used: **Serial Line Internet Protocol, Point-to Point Protocol.**

The Data Link Layer is divided into two sublayers:

* Logical Link Control (LLC)
* Media Access Control (MAC)

**Functions of the Data Link Layer**

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing**: After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.
3. **Error control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
5. **Access control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

**Network Layer – Layer 3**

* The network layer works for the transmission of data from one host to the other located in different networks.
* It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.
* The sender & receiver’s IP addresses are placed in the header by the network layer.
* Protocols Used: **IP, ARP, ICMP Protocol.**

**Functions of the Network Layer**

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
2. **Logical Addressing:** To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender & receiver’s IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

**Transport Layer – Layer 4**

* The transport layer provides services to the application layer and takes services from the network layer.
* The data in the transport layer is referred to as Segments. It is responsible for the end-to-end delivery of the complete message.
* The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.
* At the sender’s side: The transport layer receives the formatted data from the upper layers, performs Segmentation, and also implements Flow and error control to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.
* Protocols Used: **TCP, UDP.**

**Functions of the Transport Layer**

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
2. **Service Point Addressing:** To deliver the message in the correct process, the transport layer header includes a type of address called **service point address or port address.** Thus, by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

**Session Layer – Layer 5**

* This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.
* Protocols Used: **NetBIOS.**

**Functions of the Session Layer**

1. **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use, and terminate a connection.
2. **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

**Presentation Layer – Layer 6**

* The presentation layer is also called the Translation layer.
* The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

**Functions of the Presentation Layer**

1. **Translation:** For example, ASCII to EBCDIC.
2. **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. **Compression:** Reduces the number of bits that need to be transmitted on the network.

Note: Device or Protocol Use: **JPEG, MPEG, GIF**

**Application Layer – Layer 7**

* At the very top of the OSI Reference Model stack of layers, we find the Application layer which is **implemented by the network applications.**
* These applications produce the data to be transferred over the network.
* This layer also serves as a **window for the application services** to access the network and for displaying the received information to the user.
* Example: Application – **Browsers, Skype Messenger, etc.**
* Protocols Used: **POP, SMTP, DNS, FTP, and so on.**

**Functions of the Application Layer**

The main functions of the application layer are given below.

1. **Network Virtual Terminal (NVT):** It allows a user to log on to a remote host.
2. **File transfer access and management (FTAM):** This application allows a user to access files in a remote host, retrieve files in a remote host, and manage or control files from a remote computer.
3. **Mail Services:** Provide email service.
4. **Directory Services:** This application provides distributed database sources and access for global information about various objects and services.

**Explain basic network utilities?**

1. **ping**

* The ping command sends **ICMP echo request** **packets** to a destination. For example, you could run ping google.com or ping 173.194.33.174 to ping a domain name or IP address.
* These packets ask the remote destination to reply. If the remote destination is configured to reply, it will respond with packets of its own.
  + You'll be able to see how long the round-trip time is between your computer and the destination.
  + You'll see a "request timed out" message if packet loss is occurring, and
  + you'll see an error message if your computer can't communicate with the remote host at all.
* This tool can help you troubleshoot Internet connection problems, but bear in mind that many servers and devices are configured not to reply to pings.

1. **traceroute / tracert / tracepath**

* The traceroute, tracert, or tracepath command is similar to ping, but provides information about the path a packet takes.
* traceroute sends packets to a destination, asking each Internet router along the way to reply when it passes on the packet. This will show you the path packets take when you send them between your location and a destination.
* This tool can help troubleshoot connection problems. For example, if you can't communicate with a server, running traceroute may show you where the problem is occurring between your computer and the remote host.

1. **ipconfig / ifconfig**

* The ipconfig command is used on Windows, while the ifconfig command is used on Linux, Mac OS X, and other Unix-like operating systems.
* These commands allow you to configure your **network interfaces and view information** about them.
* For example, you can use the **ipconfig /all** command on Windows to view all your configured network interfaces, their IP addresses, **DNS** servers, and other information.
* Or, you can use the **ipconfig /flushdns** command to flush your DNS cache, forcing Windows to get new addresses from its DNS servers every time you contact a new hostname.
* Other commands can force your computer to release its IP address and get a new one from its DHCP server. This utility can quickly display your computer's IP address or help you troubleshoot problems.

1. **nslookup**

* The nslookup command will look up the IP addresses associated with a domain name. For example, you can run nslookup howtogeek.com to see the IP address of How-To Geek's server.
* Your computer is constantly querying its DNS servers to translate domain names to IP addresses. This command just allows you to do it manually.
* nslookup also allows you to perform a reverse lookup to find the domain name associated with an IP address. For example, nslookup 208.43.115.82 will show you that this IP address is associated with howtogeek.com.

1. **whois**

The whois command looks up the registration record associated with a domain name. This can show you more information about who registered and owns a domain name, including their contact information.

This command isn't included with Windows itself, but Microsoft's Windows Sysinternals provides a Whois tool you can download. This information is also available from many websites that can perform whois lookups for you.

1. **netstat**

* netstat stands for network statistics.
* This command displays incoming and outgoing network connections as well as other network information.
* It's available on Windows, Mac, and Linux -- each version has its own command-line options you can tweak to see different types of information.
* The netstat utility can show you the open connections on your computer, which programs are making which connections, how much data is being transmitted, and other information.

1. **Finger**

* The finger command is old and is no longer widely used.
* In theory, this command allows you to view information about users logged onto a remote computer.
* If the computer is running a finger service or daemon, you can use the finger command on your computer to see who's logged in on that remote computer, their email address, and their full name. In practice, almost no computers are running a finger service you can connect to.
* This utility was a cute idea in the early days of networking where you might want to see who was logged into the other few computers on your university network, but it's not suitable for a dangerous internet. You don't want people to see your full name and email address when you're using a computer.
* Still, the finger command lives on as a common network utility and is even still included in modern versions of Windows. Windows doesn't include a finger service that can share this information with others, though.

1. **Port Scan / nmap**

* The nmap utility is a common tool used for port scans, but there are many utilities that can run this sort of scan.
* A port scan is the process of attempting to connect to every port on a computer -- ports 1 through 65535 -- and seeing if they're open.
* An attacker might port-scan a system to find vulnerable services. Or, you might port scan your own computer to ensure that there are no vulnerable services listening to the network.