Lecture Notes: Introduction to Cybersecurity

1. Introduction to the Internet and Infrastructure

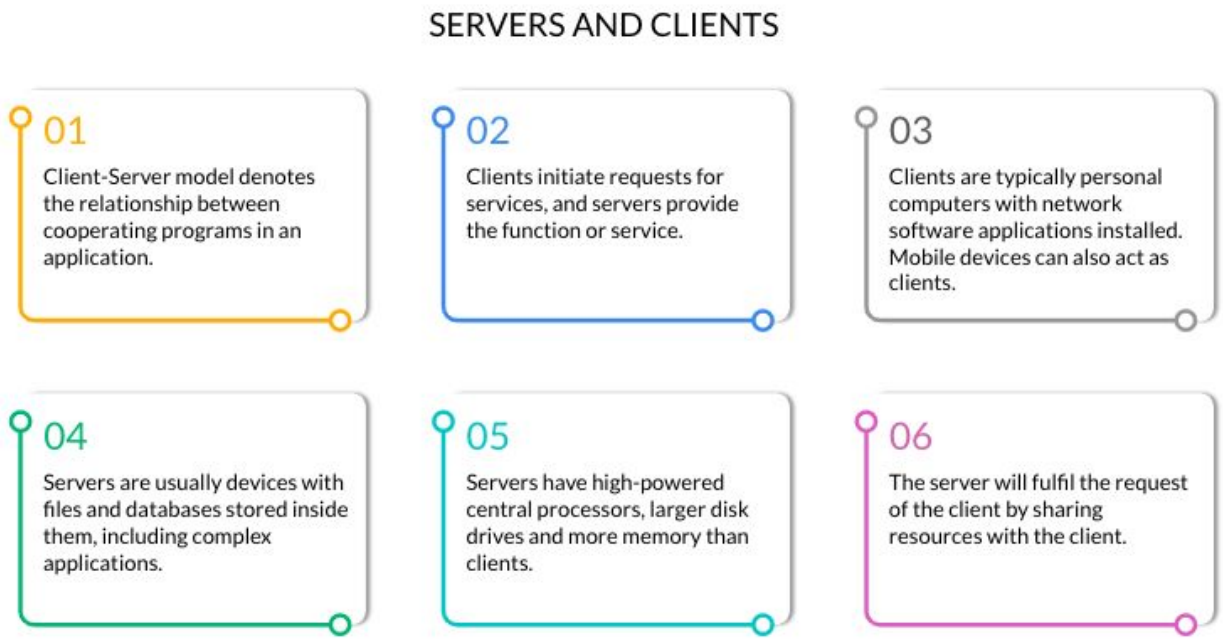
The Internet is a network of networks, with billions of computers and other electronic devices that are connected to each other. With the Internet, it is possible for us to access any information or communicate with anyone, and also do much more.

And you can do all of this by just connecting to the Internet with a computer, also known as going online. When you say someone is online, it is just another way of saying that they are connected to the Internet.

A network consists of multiple computers that are connected to each other for exchanging files or allowing electronic communications. The computers may be connected via cables, telephone lines, radio waves, satellites or infrared light beams.

- With the help of the Internet, it is possible to access almost any information, communicate with anyone in the world, etc.
- The Internet is a global network of physical cables, and wireless connections rely on these physical cables.
- A computer sends a request over these wires to a server, and the server sends back the correct data to the computer.

The Internet can be considered to have two broader categories of devices: Clients and servers.



Client–Server Network

- A client–server network is a network model that is designed for end users, called clients, to access resources, such as songs, videos, from a central computer, known as the server.
- A server is a system that provides functionality to other programs or devices, called 'clients'.
- A server performs all the primary operations, such as network management and security.
- A server manages all the resources, such as directories, files and printers, and all the communication between one client, the client side, and others happens through the server.
- Everyone uses Google search. So, in this case, Google is the server, which takes requests from people as clients and processes them in order to return the results for a searched keyword.

Advantages of a Client–Server Network

A client–server network has the following advantages:

- It contains a centralised system. Therefore, it is easy to back up data.
- It has a dedicated server, which takes care of the overall performance of the system.

- Security is better in a client–server network, since the data is well protected due to its centralised architecture.
- Client–server networks are highly scalable. The number of clients and servers can be increased whenever required.

Disadvantages of a Client–Server Network

A client–server network has the following drawbacks:

- It is expensive due to the requirement of large memory.
- It requires a dedicated network administrator who can manage all the resources.
- A server has a network operating system, which is quite costly.

IP Address

IP address stands for Internet protocol address. Just like a house address is used to identify a unique house, each computer is also assigned a unique address, which is used to identify that particular computer over the Internet. Therefore, an IP address is an identifying number that is associated with a specific computer or a computer network. It allows the computer to send and receive information to and from the correct destination.

IP addresses are generally of the following four types:

- Public
- Private
- Static
- Dynamic

IP addresses allow sharing information among the correct parties. This means they can be used to track down the physical location of a computer.

Caching

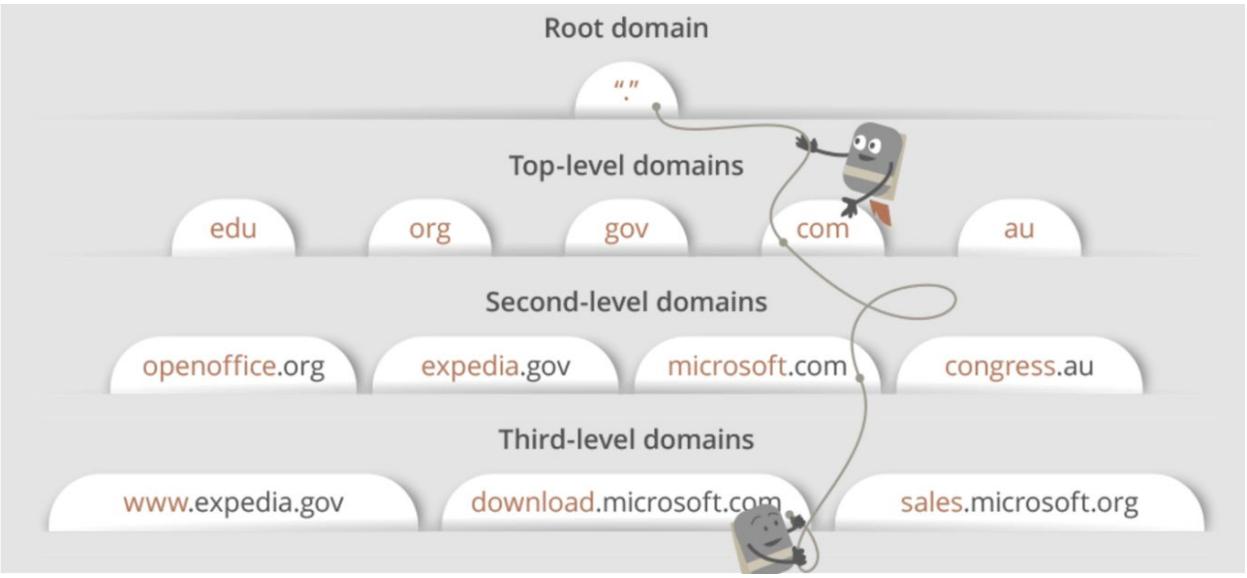
Caching is nothing but a technique with which a copy of a given resource is stored and returned when requested. Cache helps web pages load faster, since the browser does not have to download the content again when the same web pages are revisited. This eases the load on the server while improving the performance on the client side.

Caches are of several different types:

- Browser caching
- OS caching
- Router caching
- ISP caching

Domain Name System (DNS)
The Domain Name System (DNS) functions as a phonebook of the Internet. We access the Internet through domain names, such as upgrad.com, youtube.com and so on. The web browsers would utilise the Internet protocol (IP) address to match the domain names to load the Internet resources.

The image below will help you better understand how the DNS searches domains at different levels.



Secure IP Connectivity and DNS Security

Have you ever thought what would happen if your IP address was exposed or was not secured? A hacker who has your computer's IP address can target you with several types of attacks.

Secure IP Connectivity
Attacks are of many different types, as mentioned below, and to secure your connection from these attacks, you need secure IP connectivity:

IP spoofing: IP spoofing is the specific type of attack in which IP packets are created with a false source IP address to impersonate another computing system.
Man-in-the-middle (MITM) attacks: An MITM attack is a cyberattack in which the attacker secretly tampers with the connection and possibly alters the communications between two parties who believe that they are directly communicating with each other.

How to Secure an IP Connection?
Use of VPN: A virtual private network, or a VPN, creates a private network on a public network to provide privacy and anonymity online, and it enables users to send and receive data securely. A VPN helps to mask your IP address so your online activities are virtually untraceable.

DNS Security

It protects Internet users from counterfeit DNS data. It does so by verifying digital signatures, which are embedded in the data. This allows the users to validate that the DNS records that they received came from the correct source.

DNS cache poisoning: DNS cache poisoning is an attack in which DNS records are altered and used to redirect traffic away from a legitimate server to a fake one.

Basic Networking Commands

Networking commands are utilities that are used for network troubleshooting. These commands include the following:

ipconfig: It displays all the current TCP/IP network configuration values and refreshes the dynamic host configuration protocol (DHCP) and DNS settings.
Ping: It is used to test whether a particular IP is reachable across a network. A ping measures the time taken by the packets to reach the destination computer and return back.
nslookup: It is a network command for querying the DNS in order to obtain domain name or IP address mapping, or other DNS records.
tracert: It tracks in real-time the path taken by a packet over the network from the source to the destination. It also reports the IP addresses of all the routers that it pinged in between.

2. Basics of Cybersecurity

Cybersecurity refers to the protection of computer devices, systems, networks and programs from cyberattacks. Cyberattacks are a globally increasing and evolving threat to sensitive data. Attackers use new methods, which are powered by social engineering, artificial intelligence and machine learning, to bypass security checks.

Our reliance on new technology is increasing, and this reliance would continue as we introduce smart Internet devices, which have access to our networks via Bluetooth and Wi-Fi.

Cybersecurity is important, because it helps us protect our sensitive data, personally identifiable information (PII), protected health information (PHI), private information, intellectual property data, and governmental and industry information systems from theft and damage attempted by criminals and adversaries.

Governments around the world are focusing increased attention on cybercrimes. The General Data Protection Regulation (GDPR) is a great example of this. It has increased the reputational damage for data breaches by requiring all the organisations that operate in the EU to:

- Communicate data breaches,
- Appoint a data protection officer,
- Obtain user consent to process information and
- Anonymise data for privacy.

3. Terminologies and Challenges in Cybersecurity

Information stealing is the most expensive and fastest growing segment of cybercrime. It is largely driven by the increasing exposure of identity information to the web via cloud services. However, this is not the only target. Industrial systems that manage power grids and other infrastructure can also be disrupted or destroyed. And identity theft is not the only goal; cyberattacks may aim to compromise data integrity (destroy or change data) to generate distrust in an organisation or government.

Cybercriminals are becoming more skilled with each passing day, changing what they target, how they affect organisations and their methods of attack for different security systems. Other factors that are driving the growth in cybercrime include:

- The distributed nature of the Internet;
- The ability of cybercriminals to attack targets outside their jurisdiction, thus rendering policing extremely difficult;
- The increasing profitability and ease of doing commerce on the dark web; and
- The rapid proliferation of mobile devices and the Internet of Things.

CIA Triad
The CIA triad is an information security model that helps or guides organisations in fulfilling their security requirements and creating policies to keep data safe/secure. The three pillars of the CIA triad include Confidentiality, Integrity and Availability.

Confidentiality: Only authorised users and systems should be able to access or modify data.
Integrity: Data should not be tampered with by any person either accidentally or maliciously. It should be maintained in a correct state.
Availability: Authorised users should be able to access data whenever they need to do so.

Case Study: ATM
We will take the example of an ATM and see how it ensures each of the three aspects of the CIA triad: Confidentiality, Integrity and Availability.

Confidentiality: It provides confidentiality through two-factor authentication; for example, a person who owns a card should know its PIN.
Integrity: It provides data integrity by ensuring that any transaction made via the machine is reflected in the user's bank account only.
Availability: It provides availability because it is in a public place and is accessible even when the bank branch is closed.

4. Introduction to Hacking and Its Types

We frequently come across news on company websites being hacked or someone's valuable data getting leaked. Have you ever wondered who the people responsible for such activities are and what their intentions are behind carrying out these activities?

Hacker

A hacker is someone who keeps exploring methods to break defences and exploit the weaknesses of a computer system or a network.

Incentive for Hacking

There are enough reasons or motivations for hackers to do hacking. Below is some useful information on the type of data that is targeted by hackers and the types of threats that an organisation faces.

Information sought by cyber criminals

1. Personal information (17%)
2. Transaction information (12%)
3. Planning information (12%)
4. Key stakeholder information (11%)
5. Password information (11%)
6. Innovation and Research (9%)

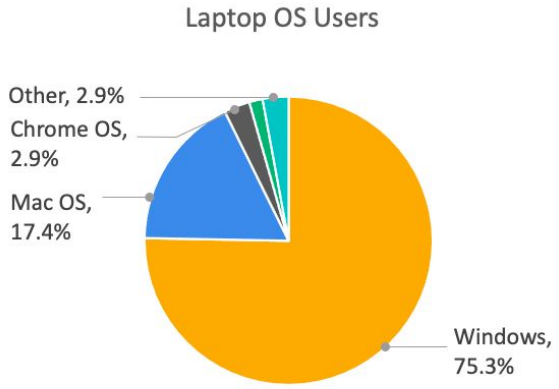
Organisations have to deal with major threats

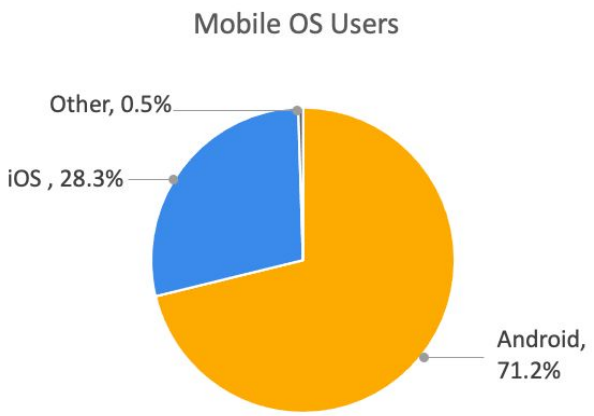
1. Phishing (22%)
2. Malware (20%)
3. Fraud (10%)
4. Spam (6%)
5. Internal attacks (5%)
6. Natural disasters (2%)

Hacking the Common versus Hacking the Unique

Have you ever wondered why Windows or Android-based devices are targeted more by hackers?

Let's take a look at the diagram below to understand the reason.





People generally are drawn more to common tools or devices. The same applies here. The more the number of users, the greater would be the hacking activities. This is why Android-based and Windows systems are drawing more cyberattackers.

Hacker

As mentioned previously, a hacker is someone who explores methods to breach the defences and exploit the weaknesses of a computer system or a network.

Hackers are mainly of the following three types:

- **Black hat hackers:** They are criminals who breach computer networks with malicious intent. They may also publish malware, which destroys files; holds computers hostage; or steals passwords, credit card numbers and other personal information.
- **Grey hat hackers:** They are computer hackers or computer security experts who may sometimes overstep the laws or the typical ethical standards. These individuals do not have malicious intent, unlike a black hat hacker.
- **White hat hackers:** They are ethical computer hackers, or computer security experts, who specialise in penetration testing and other methodologies, which ensure the security of an organisation's information systems.

Red, Blue and Purple Teams

Are there any teams or any specific names given to the people who are working to defend organisations from cyberattacks or cybercrimes?

Well there are three teams that work on cybersecurity to ensure the security of cyberspace. These teams include the following:

- **Red team:** This team is typically independent of the company and is hired to test its defences.
- **Blue team:** This team comprises a company's own cybersecurity personnel, typically within a Security Operations Centre (SOC). It is expected to detect, oppose and weaken the red team.
- **Purple team:** This team is not permanent but has a transient function to oversee and optimise the red and blue team exercise.

Threat, Vulnerability and Risk

Risk is a function of threats, which make use of vulnerabilities to obtain, damage or destroy assets. Threats may exist, but risk depends upon the vulnerabilities; if there

are no vulnerabilities, then there is little or no risk. Similarly, if vulnerability exists, then risk depends upon the threat; if you have no threat, then you have little or no risk.

Let us understand each of them separately:

- **Threat:** It is a potential negative action that exploits a weakness or a vulnerability and which results in an unwanted impact on or a potential damage to a computer system or application.
  In simple terms, threats are some incidents with potential to harm systems.
- **Vulnerability:** These are weaknesses or gaps in security, which can be exploited by threats to gain unauthorised access to an asset.
  In simple terms, vulnerabilities are the weaknesses of a system or an application that hackers could exploit for their benefits.
- **Risk:** This is the potential for loss or damage to the confidentiality, integrity or availability of data.
  In simple terms, risk is the possibility or the chance of something bad happening to your system or application.

5. Introduction to Security Technologies and Domains

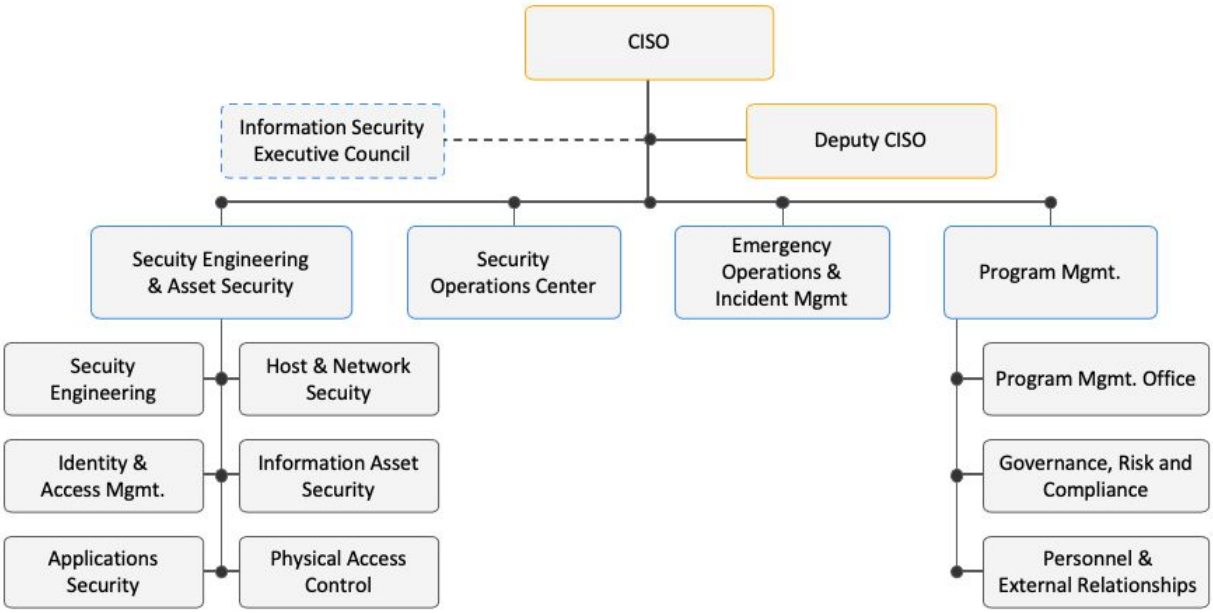
During winters, we often wear multiple layers of clothing to protect ourselves from the cold weather. The same applies for IT network security: The more the layers that you have, the better would the protection be. Given below are the different layers of security that help organisations protect themselves from attacks. Each layer has its own functionality and purpose.

There are mainly five different layers of security:

- **Perimeter security:** This layer includes tools to monitor network traffic for anything unusual and report issues to the administrator.
- **Network security:** This layer includes components such as hardware firewalls, and firewall monitoring and reporting.
- **Endpoint security:** This layer includes both antivirus software and DNS filtering to shore up defences.
- **Application security:** This layer includes Windows and antivirus firewalls to protect both mobile- and web-based applications.
- **Data security:** This layer includes tools for authentication and encryption of data to secure it against unauthorised access.

Organisation Structure

Every domain has its own team structure, and, therefore, cybersecurity also has its own. Let's take a look at the diagram below to understand what are the roles available and what the associated responsibilities are.



Along with an organisation's members, third-party services providers also play a very important role in the security of an organisation. A third-party service provider is a specialist company that provides a range of distribution, storage, transport and fulfillment services to customers.

6. Introduction to Cyberattacks

Let us consider the following scenario: You might have received fake emails with unbelievable offers or messages urging you to provide your bank details to claim a bumper cash prize. This has happened with all of us at some point, right? So, have you ever wondered why we get such emails?

This is because the person who is sending you the email is trying to fool you and wants you to open the links provided in or the files attached with that email. There are many more such kinds of attacks.

Cyberattacks
An attack is any attempt to expose, alter, disable, destroy, steal, or gain unauthorised access to or make the unauthorised use of an asset.

Let's take a look at some popular cyberattacks, which are listed below:

- **Phishing attacks:** Phishing is a cybercrime where targets are contacted by text message, email or telephone by someone pretending to be a legitimate institution to attract them and obtain sensitive data, such as banking and credit card details, or passwords and personally identifiable information.
- **Trojan attacks:** Trojan is a type of malicious code or software that looks admissible but can take control of your computer. These are designed to

damage, disrupt, steal or, in general, carry out some other harmful action on your data or network.

- **Ransomware attacks:** Ransomware is malicious software that contaminates your computer and displays a message demanding a fee to be paid in order to get the system to work again. This class of malware is a criminal money-making scheme that can be installed through specious links in an instant message, an email message or a website.
- **Man-in-the-middle attacks:** A man-in-the-middle attack is a general term for when a criminal positions themselves in between the conversation of a user and an application, to either monitor or impersonate one of these parties, thus making it appear as though a normal exchange of information is underway.

Case Study: Stuxnet

Stuxnet is a computer worm (a standalone malware computer program that replicates itself in order to spread to other computers) that was discovered in June 2010. The points below would help you better understand Stuxnet and how it was utilised to carry out a cyberattack:

- Stuxnet was aimed to destroy the centrifuge machines in Iran's Natanz refining plant by causing them to burn themselves out.
- The original Stuxnet malware attack targeted the programmable logic controllers (PLCs), which are used to automate machine processes.
- It was the most complicated worm ever discovered.
- It was unusual for a worm/virus to contain 1 zero-day vulnerability. Stuxnet had 4.
- Stuxnet also acted as a rootkit, and thus, its action and presence remained hidden.
- It was the first worm to include a code to attack supervisory control and data acquisition (SCADA) systems.
- Over time, other groups modified the virus to target facilities including water treatment plants, power plants and gas lines.

The OWASP Framework

The Open Web Application Security Project (OWASP) is an open-source community that produces freely available articles, methodologies, documentation, tools and technologies in the field of web application security.

Here is a list of the top 10 web application security risks:

1. **Injection:** It occurs when untrusted data is supplied to an interpreter as part of a command or a query in order to alter the execution of that program. Some flaws include SQL, NoSQL, OS and LDAP injection.
2. **Broken authentication:** It occurs when application authentication and session management functions are implemented poorly and allow attackers to trade-off passwords, keys or session tokens, or make use of other implementation flaws to explore other users' identities.

3. **Sensitive data exposure:** Many web applications or companies do not protect sensitive data properly, and attackers take advantage of such flaws to steal or modify such data to commit credit card fraud, identity theft or other crimes.
4. **XML external entities (XXE):** Many older systems or poorly configured XML processors evaluate external references while processing XML documents. External entities can be used to reveal internal files by using the file URI handler, internal file shares, remote code execution, internal port scanning and DoS attacks.
5. **Broken access control:** Some restrictions on authenticated users are not enforced properly. Some resources that are not supposed to be accessed, as they might be harmful or dangerous, are accessed. Attackers can make use of these flaws to get unauthorised access to functionality and data, for example, accessing other users' data.
6. **Security misconfiguration:** This includes attacks that occur when some features, such as default configurations, misconfigured HTTP headers, incomplete or ad hoc configurations, open cloud storage and verbose error messages containing sensitive information, are not implemented properly. All configurations must be patched or upgraded after a certain period of time.
7. **Cross-site scripting (XSS):** Such flaws occur whenever an application includes untrustworthy data without proper validation or updates the existing data with user-supplied untrustworthy data that can create an HTML or JavaScript. This allows the attackers to run scripts on the target browser, which can lead to user sessions getting hijacked or users being redirected to malicious websites.
8. **Insecure deserialisation:** Insecure deserialisation often leads to remote code implementation. Even if deserialisation flaws do not result in remote code execution, they can be used to carry out attacks, including injection attacks and privilege advance attacks.
9. **Using components with known vulnerabilities:** A few components of applications, such as libraries, frameworks and other software modules, execute with full privileges, just like the application itself. If a vulnerable component gets exploited, then such an attack can result in severe data loss or server takeover.
10. **Insufficient logging and monitoring:** Insufficient logging and monitoring occur when critical security events are not logged off properly. This allows attackers to further attack systems; maintain persistence; pivot to more systems; and tamper with, extract or destroy data.

OWASP releases the top-10 list every year, which means the vulnerabilities mentioned above are not fixed. They vary from time to time.

7. Introduction to Cybercrime and Cyberlaws

Cybercrime
Cybercrime is the crime that involves a computer and a network. A computer is used to commit the crime, or it may be a target.

Cybercrimes are mainly classified into the following four categories:

1. **Insider:** An insider threat is a destructive threat to an organisation that comes from the people who work for it (employees, former employees) and possess internal security information about it.
2. **Outsider:** Outsider threats are those threats that come to an organisation from people who are not part of it. They can be from hackers, white hat hackers or even someone who was hired by a business competitor and wanted to get important information or destroy your business.
3. **Structured:** Structured threats come mostly from people with higher level skills who are actively working to compromise a security measure. The targeted system might have been selected specifically and the attack is carried out with proper planning.
4. **Unstructured:** Unstructured threats often entail unfocused strikes on one or more network systems. These are often carried out by individuals whose developing skills are limited. The culprit probably knows the system that is being attacked or infected.

Cyberlaws

Cyberlaws are related to the law of information technology, which includes computing and the Internet. Cyberlaws help with stopping people from carrying out malicious cyber activities, and they also help prevent cybercrime.

Here are some important laws related to information technology:

- **ITA-2008:** The Information Technology Amendment Act of 2008 is a significant addition to India's Information Technology Act (ITA-2000). The Act was brought into effect to promote the IT industry, modulate e-commerce and prevent cybercrime.
- **Patent/IP:** A patent is an intellectual property right for a technical invention. It allows you to prevent others from using your invention for commercial purposes for up to 20 years.
- **Copyright:** Copyright is the legal right to a person that they may copy, print, reuse, etc. an original work, such as a computer program, some design or a song.
- **Cyber fraud:** Any individual who dishonestly or fraudulently uses any other person's password, electronic signature or any other unique identification shall be punished.