UNIT-1

Fundamentals

Introduction to Cyber Security

Cyber Security Basics: Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organizations, are all being impacted.

Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

The term **cyber security** refers to techniques and practices designed to protect digital data. The data that is stored, transmitted or used on an information system.

OR

Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks.

It is made up of two words one is cyber and other is security, Cyber is related to the technology which contains systems, network and programs or data. Whereas security related to the protection which includes systems security, network security and application and information security

Cyberspace : Cyberspace is a world-wide network of computer networks that uses the TCP/IP for communication to facilitate transmission and exchange of data.

Cyberspace is a place where you can chat, explore, research and play (INTERNET).

1.1 What is Cyber Security?:

A crime conducted in which a computer was directly and significantly instrumental is known as "**Computer Crime**".

Computer crime as also other various definitions :

- Any threats to the computer itself, such as theft of hardware or software and demands for ransom.
- Any financial dishonesty that takes place in a computer environment.

A crime committed using a computer and the Internet to steal a person's identity or sell illegal or smuggled goods or disturb any operations with malicious programs is known as "Cyber Crime".

Another definition is :

- Any illegal activity done through the internet.
- Any criminal activities done using cyberspace and WWW.

Need of Cyber Security

- Cyber security becomes so important in our predominant digital world
- Cyber-attacks can be extremely expensive for businesses to endure.
- In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
- Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber-attacks.
- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

1.2 History, Evolution and standards of cyber security:

A Short History of Cybersecurity

The first comprehensive published work Security Controls for Computer Systems [Ware, 1970] which became the foundation in the field of cybersecurity was a technical report commonly called the Ware Report.

This report, published in 1970, was the result of a study carried out by a task force on computer security organized by the department of defense of the United States of America.

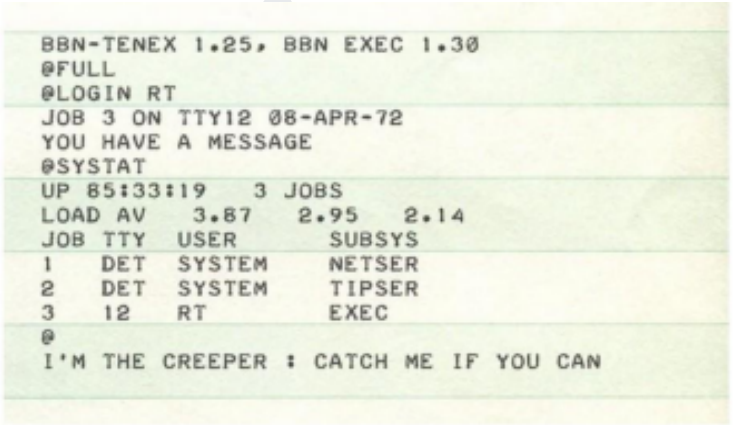


Figure 1.2: An example of the message produced by the Creeper: source [corewar.co.uk, 2021]

The report concluded that a comprehensive security of a computer system requires a combination of hardware, software, communications, physical, personnel and administrative controls. The first computer program (also the first non-self-replicating benign virus in history) that could move across a network was written in 1971, leaving a message trail (**I am the creeper, catch me if you can**) behind wherever it went.

The program was called the Creeper.

An example of the message produced by the Creeper is shown in Figure 1.2. The first example of an antivirus program (it performed the same functions that an antivirus does today)was written in the year 1973 called the **Reaper,** which chased and deleted the Creeper. **Reaper was also the first self-replicating program and hence making it the first benign computer worm (a self-replicating computer program that moves across the network).**

In 1977 the **CIA** triad, of **Confidentiality, Integrity, and Availability** shown in Figure 1.3, was introduced [Ruthberg and McKenzie, 1977]. These are the three basic principles for cybersecurity and are still widely used benchmarks to evaluate the effectiveness of a cybersecurity system.

Figure 1.3: The CIA Triad

Confidentiality — The confidential information and data should be prevented from reaching the wrong hands. Confidentiality deals with the access, operation, and disclosure of system elements.

Integrity — The information and data should not be corrupted or edited by a third party without authorization. Integrity deals with the modification, manipulation, and destruction of system elements.

Availability — The information and data should be available all the time and adaptive recovery mechanisms should be established to restore the system and the services provided by the system. Availability deals with the presence, accessibility, readiness, and continuity of service of system elements.

Evolution of Cyber Security :

The words “hacking”, “virus,” and “data breaches” ring alarm bells today, but they had humble beginnings back in the 1970s. The first known digital virus was popularly called “the creeper.” An engineer from US technology company BBN Technologies created a code

for a program that could travel from one computer to another connected by the advanced research projects agency network (ARPANET) – the Internet's predecessor.

The virus did not particularly inflict much damage other than causing slight inconvenience to the reader.

It would display the message "I'm the creeper, catch me if you can!" In response, his colleague wrote another code, which went one step ahead, as the code would not just move between systems but also copy itself as it traveled.

This program would delete the creeper message, thus e**arning the name "reaper."**

What is a cybersecurity standard?

Cybersecurity standards can be defined as the critical means by which the direction described in an enterprise's cybersecurity strategy and policies are translated into actionable and measurable criteria.

Cybersecurity standards are statements that describe what must be achieved in terms of security outcomes in order to fulfill an enterprise's stated security objectives.

How the standards are to be implemented and what solutions are used to achieve the standard normally are not part of the standard itself. Instead, these activities should be described in ensuing plans and operational procedures that are developed to implement the standard at a given point in time.

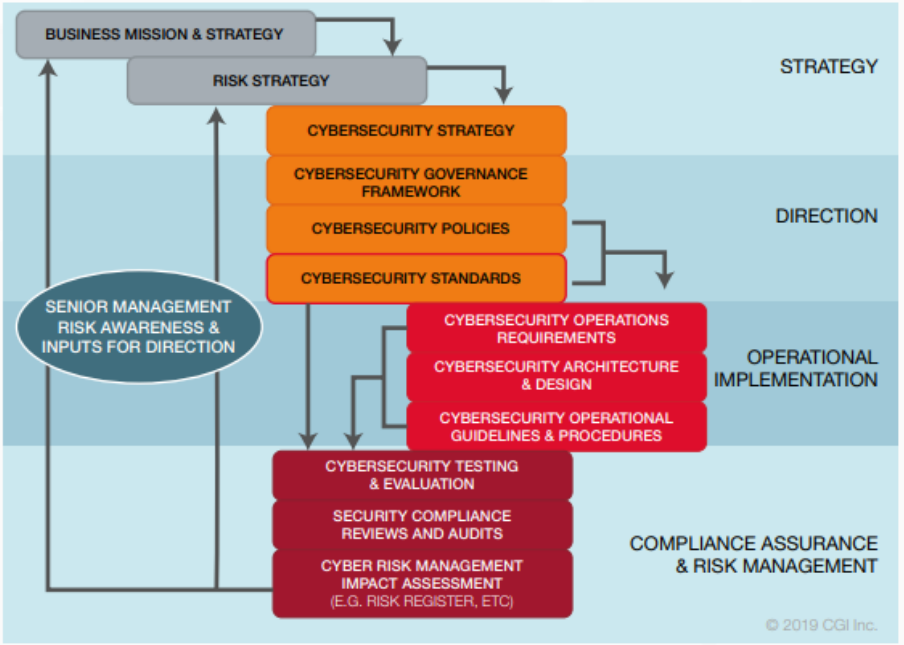
Cybersecurity standards in IT governance :

Cybersecurity standards represent a key step in the IT governance process. As a means for managing and containing risk to acceptable levels, the standards must be wholly consistent with IT governance instruments and closely aligned with and driven by the enterprise's cybersecurity policies.

The diagram below represents the typical elements of an IT governance hierarchy. Cybersecurity standards sit at the critical interface between the Direction elements and the Operational Implementation elements.

Standards provide essential direction for the objectives and outcomes to be achieved through subsequent implementation activities, such as the development of functional and technical requirements, architecture and design, operational guidelines and operating procedures.

Figure 1 - Cybersecurity Standards in the IT Governance Hierarchy



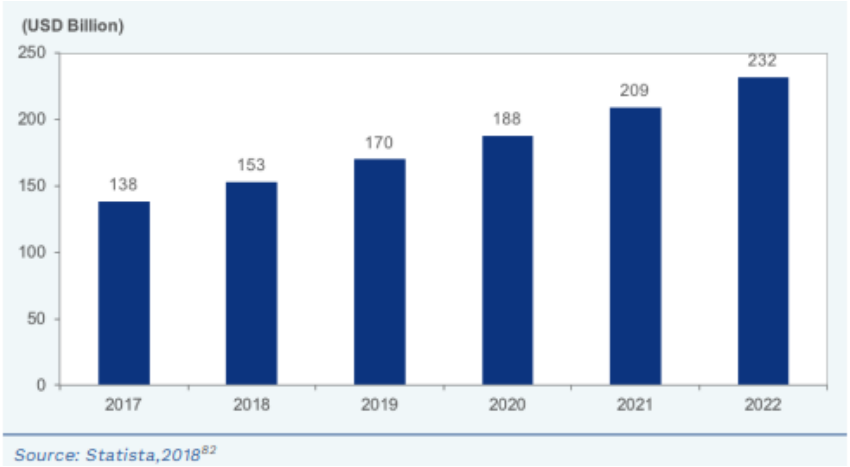
1.3 Cybersecurity: Industry Trends and Future Prospects

The global cybersecurity market grew from $3.5 billion in 2004 to about $138 billion in 2017 –over 39x in 13 years.

In 2017, the aerospace and defense vertical had the largest share in the cybersecurity market. However, going ahead, government, BFSI and IT and telecom verticals are expected to gain traction. During 2017 to 2022, the cybersecurity market is expected to grow at a CAGR of 11% to reach $231.94 billion.

North America dominated the global cybersecurity market in 2017, this trend is also expected to change as APAC is estimated to grow at the fastest pace during 2017-2022.

Size of the Cybersecurity Market Worldwide



Source: Statista,2018[82]

1.4 Types of Cyber security:

1. **Network Security**

   Focuses on securing computer networks from unauthorized access, data breaches, and other network-based threats. It involves technologies such as Firewalls, Intrusion detection systems (IDS), Virtual private networks (VPNs), and Network segmentation.

   Guard your internal network against outside threats with increased network security.

   Sometimes we used to utilize free Wi-Fi in public areas such as cafes, Malls, etc. With this activity, 3rd Party starts tracking your Phone over the internet. If you are using any payment gateway, then your bank account can be Empty.

   So, avoid using Free Network because free network Doesn't support Securities.

2. **Application Security**

   Concerned with securing software applications and preventing vulnerabilities that could be exploited by attackers. It involves secure coding practices, regular software updates and patches, and application-level firewalls.

   Most of the Apps that we use on our Cell-phone are Secured and work under the rules and regulations of the Google Play Store.

   There are 3.553 million applications in Google Play, Apple App Store has 1.642 million, while Amazon App Store has 483 million available for users to download. When we have other choices, this does not mean that all apps are safe.

   Many of the apps pretend to be safe, but after taking all the information from us, the app shares the user information with the 3rd-party.

   The app must be installed from a trust-worthy platform, not from some 3rd party website in the form of APK (Android Application Package).

3. **Information or Data Security**

   Focuses on protecting sensitive information from unauthorized access, disclosure, alteration, or destruction. It includes Encryption, Access controls, Data classification, and Data loss prevention (DLP) measures.

   Incident response refers to the process of detecting, analyzing, and responding to security incidents promptly.

   Promoting security awareness among users is essential for maintaining information security. It involves educating individuals about common security risks, best

practices for handling sensitive information, and how to identify and respond to potential threats like phishing attacks or social engineering attempts.

Encryption is the process of converting information into an unreadable format (ciphertext) to protect it from unauthorized access.

4. Cloud Security

It involves securing data, applications, and infrastructure hosted on cloud platforms, and ensuring appropriate access controls, data protection, and compliance. It uses various cloud service providers such as AWS, Azure, Google Cloud, etc., to ensure security against multiple threats.

Cloud base data storage has become a popular option over the last decade. It enhances privacy and saves data on the cloud, making it accessible from any device with proper authentication.

These platforms are free to some extent if we want to save more data than we have to pay.

AWS is also a new Technique that helps to run your business over the internet and provides security to your data.

5. Mobile Security

It involves securing the organizational and personal data stored on mobile devices such as cell phones, tablets, and other similar devices against various malicious threats. These threats are Unauthorized access, Device loss or Theft, Malware, etc.

Mobile is a very common device for day to day work. Everything we access and do is from our mobile phone. Ex- Online class, Personal Calls, Online Banking, UPI Payments, etc.

Regularly backing up mobile device data is important to prevent data loss in case of theft, damage, or device failure.

Mobile devices often connect to various networks, including public Wi-Fi, which can pose security risks. It is important to use secure networks whenever possible, such as encrypted Wi-Fi networks or cellular data connections.

6. Endpoint Security

Refers to securing individual devices such as computers, laptops, smartphones, and IoT devices. It includes antivirus software, intrusion prevention systems (IPS), device encryption, and regular software updates.

- Antivirus and Anti-malware software that scans and detects malicious software, such as Viruses, Worms, Trojans, and Ransomware. These tools identify and eliminate or quarantine malicious files, protecting the endpoint and the network from potential harm.
- Firewalls are essential components of endpoint security. They monitor and control incoming and outgoing network traffic, filtering out potentially malicious data packets.
- Keeping software and operating systems up to date with the latest security patches and updates is crucial for endpoint security.

1.5 Applications of Cyber security:

DDoS security:

DDoS stands for Distributed Denial for Service attack. In this digital attack, the attacker uses multiple numbers of devices to keep the web server engaged in accepting the requests sent by him from the multiple devices. It creates fake website traffic on the server.

To deal with this, Cybersecurity helps to provide a DDoS mitigation service to help cope with it which diverts the traffic to the other cloud-based servers and the situation gets resolved.

Web Firewall:

A web application server-based firewall gets applied on a large area network and it checks all the incoming and outgoing traffic on the server and it automatically tracks and removes fake and malicious website traffic. This Cybersecurity measure helps to determine and enable auto-traffic monitoring by reducing attack risk.

Bots:

Nowadays, many hackers and attackers use bots to cause multiple device traffic on the server to make it crash. Cybersecurity helps to deal with identifying fake users i.e. bots and make them log out of their sessions so they don't affect the experience of the normal users.

Antivirus and Antimalware:

Cybersecurity is used to develop Antivirus and Antimalware software for preventing all the digital attacks on the computer and protecting these devices from data breaches, digital attacks, and unauthorized attacks from hackers. It also helps in maintaining network security and firewall systems for all the connected devices on the network.

Threat management systems:

Cybersecurity helps to deal with digital threats and attacks on computer systems. It identifies different points of vulnerabilities and bugs in the system that can be used by hackers and attackers to defy it and it automatically optimizes all the defects in it with the ability to improve in performance issues.

It also improves the ability to quickly overcome a digital attack and provide effective control to the users about the vulnerability issues.

Critical systems:

Cybersecurity helps to deal with the critical issue attacks that are carried out on large servers connected to wide-area networks. It maintains the standard high safety protocols for the users to comply with the cybersecurity measures so as to protect the devices.

It monitors all the applications in real-time and regularly checks the safety of the servers, the network used by it, and the users themselves.

Rules and regulations:

Cybersecurity helps to create new rules and regulations for the users, attackers, and the people on the network to follow and comply with certain rules and norms while they are using the Internet.

It gives the power to the authorities to look into security issues and optimize the network accordingly.Cybersecurity helps to create new rules and regulations for the users, attackers, and the people on the network to follow and comply with certain rules and norms while they are using the Internet. It gives the power to the authorities to look into security issues and optimize the network accordingly.

UNIT-2

Cyber Threats & Suggested Security Measures

2.1 Malware:

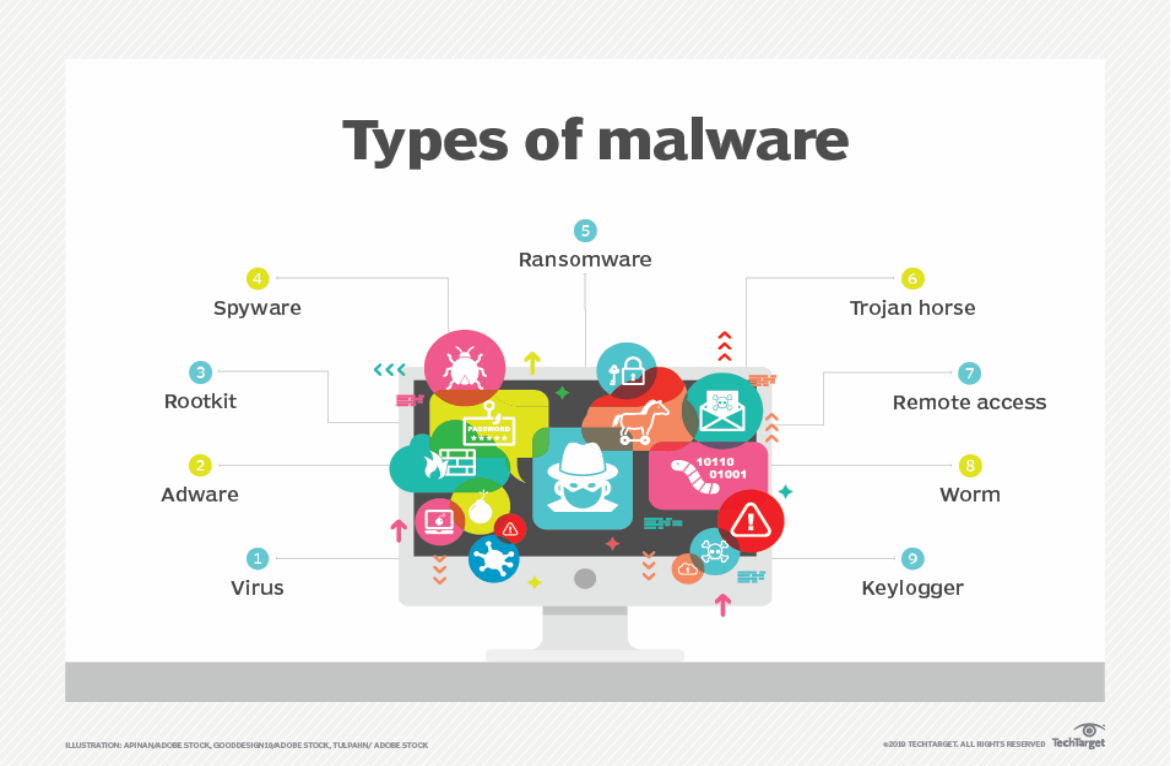
Any malicious software intended to harm or exploit any programmable device, service, or network is referred to as malware.

Cybercriminals typically use it to extract data they can use against victims to their advantage in order to profit financially. Financial information, medical records, personal emails, and passwords are just a few examples of the types of information that could be compromised.

In simple words, malware is short for malicious software and refers to any software that is designed to cause harm to computer systems, networks, or users.

Why Do Cybercriminals Use Malware?

1. Cybercriminals use malware, which includes all forms of malicious software including viruses, for a variety of purposes.
2. Using deception to induce a victim to provide personal information for identity theft.
3. Theft of customer credit card information or other financial information.
4. Taking over several computers and using them to launch denial-of-service attacks against other networks.
5. Using infected computers to mine for cryptocurrencies like bitcoins.



2.2 Phishing:

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email.

The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine. Phishing is a common type of cyber-attack that everyone should learn about in order to protect themselves.

How does phishing work?

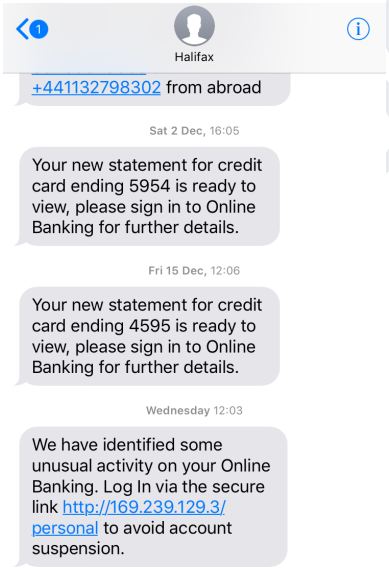
Phishing starts with a fraudulent email or other communication that is designed to lure a victim. The message is made to look as though it comes from a trusted sender.

If it fools the victim, he or she is coaxed into providing confidential information, often on a scam website. Sometimes malware is also downloaded onto the target's computer.

What are the dangers of phishing attacks?

Sometimes attackers are satisfied with getting a victim's credit card information or other personal data for financial gain. Other times, phishing emails are sent to obtain employee login information or other details for use in an advanced attack against a specific company.

Cybercrime attacks such as advanced persistent threats (APTs) and ransomware often start with phishing.



2.3 E-Mail Related Frauds:

Email fraud refers to a variety of scams and malicious activities that are carried out through email. These attacks can range from simple advance-fee scams targeting unsuspecting individuals, to sophisticated business email compromise (BEC) attacks that aim to trick large accounting departments into paying fraudulent invoices.

Email fraud attackers often use social engineering tactics, such as posing as a trusted authority figure or using urgent or emotionally charged language, to manipulate their victims into taking action detrimental to themselves or their organization.

What is an example of email fraud?

There are many examples of email fraud, but one of the most notorious examples is the advanced fee scam or the "Foreign Prince" email. In this scam, an individual posing as a wealthy prince promises to transfer a large sum of money to the victim's account in exchange for a small upfront payment or transfer fee. Once the payment is made, the promised funds never materialize.

This scam has been around for centuries. Its origin can be traced back to the late 1800s, when it was known as the Spanish Prisoner scam. In this version, a con artist would contact victims claiming to be helping a wealthy Spanish prisoner escape, and promising a reward in exchange for a guard bribe fee.

The scam has evolved and will continue to evolve, but its underlying principle remains: promising something for nothing while taking advantage of people's vulnerabilities.

Preventive Measures/Precautions:

1. Use two-factor authentication. Two-factor identification requires you to enter a code sent to you in a text message or another service to access your account after you enter your username and password. This makes it more difficult for a hacker to access your information, even if they are able to crack your password.
2. Do not open SPAM mails or emails sent from unknown senders. Do not click on any link sent on such mails.
3. Be cautious while opening links sent in unsolicited emails even if they are sent from someone in your contact-list. Such known contacts' email accounts may have been compromised and thereafter used to send malicious codes to unsuspecting contacts.
4. Do not click on attractive and tempting links sent over a WhatsApp message or routine SMS. They may lead you to malicious pages and cause malware intrusion on your system/device. Hackers use social engineering to trick you in clicking the links. Don't fall for it.
5. Keep your email password long and difficult. Passwords should have at least 8 characters and there should be at least one upper-case, one lower-case, one numeral and one special character in your password.
6. Don't store your passwords in your device (phone/tablet. etc). Anyone getting access (physical or remote) to your device will easily get to know your passwords.
7. Don't disclose your password to anyone and keep changing it at regular intervals (2-4 months).
8. Always have a lock screen on your smartphone, tablet, laptop, etc protected by a PIN or password. Do not keep your device open and unattended even for a minute, esp. in public places and your workplace.

2.4 SQL injection:

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.

It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access.

In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behaviour.

What is the impact of a successful SQL injection attack?

A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information.

Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines.

In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period.

How to detect SQL injection vulnerabilities.

SQL injection can be detected manually by using a systematic set of tests against every entry point in the application. This typically involves:

1. Submitting the single quote character ' and looking for errors or other anomalies.
2. Submitting some SQL-specific syntax that evaluates to the base (original) value of the entry point, and to a different value, and looking for systematic differences in the resulting application responses.
3. Submitting Boolean conditions such as OR 1=1 and OR 1=2, and looking for differences in the application's responses.
4. Submitting payloads designed to trigger time delays when executed within a SQL query, and looking for differences in the time taken to respond.
5. Submitting OAST payloads designed to trigger an out-of-band network interaction when executed within a SQL query, and monitoring for any resulting interactions.

SQL injection examples:

There are a wide variety of SQL injection vulnerabilities, attacks, and techniques, which arise in different situations. Some common SQL injection examples include:

- Retrieving hidden data, where you can modify a SQL query to return additional results.
- Subverting application logic, where you can change a query to interfere with the application's logic.
- UNION attacks, where you can retrieve data from different database tables.
- Blind SQL injection, where the results of a query you control are not returned in the application's responses.

2.5 Cross-Site Scripting (XSS) & Cross-Site Request Forgery (CSRF) :

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side scripts into Web pages viewed by other users.

A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy.

XSS Type

There are Three Types of XSS

- Persistent (Stored) XSS
- Attack is stored on the website's server

The persistent (or stored) XSS vulnerability is a more devastating variant of a cross-site scripting flaw it occurs when the data provided by the attacker is saved by the server, and then permanently displayed on "normal" pages returned to other users in the course of regular browsing, without proper HTML escaping.

A classic example of this is with online message boards where users are allowed to post HTML formatted messages for other users to read.

- Non-Persistent (reflect) XSS
    - user has to go through a special link to be exposed

The non-persistent (or reflected) cross-site scripting vulnerability is by far the most common type. These holes show up when the data provided by a web client, most commonly in HTTP query parameters or in HTML form submissions, is used immediately by server-side scripts to generate a page of results for that user, without properly sanitizing the request.

- DOM-based XSS
    - problem exists within the client-side script

DOM-based vulnerabilities occur in the content processing stages performed by the client, typically in client-side JavaScript. The name refers to the standard model for representing HTML or XML contents which is called the Document Object Model (DOM) JavaScript programs manipulate the state of a web page and populate it with dynamically-computed data primarily by acting upon the DOM.

Cross-Site Request Forgery (CSRF):

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.

With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing.

If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

Prevention measures

A number of flawed ideas for defending against CSRF attacks have been developed over time. Here are a few that we recommend you avoid.

Using a secret cookie

Remember that all cookies, even the secret ones, will be submitted with every request. All authentication tokens will be submitted regardless of whether or not the end-user was tricked into submitting the request. Furthermore, session identifiers are simply used by the application container to associate the request with a specific session object. The session identifier does not verify that the end-user intended to submit the request.

Only accepting POST requests

Applications can be developed to only accept POST requests for the execution of business logic. The misconception is that since the attacker cannot construct a malicious link, a CSRF attack cannot be executed. Unfortunately, this logic is incorrect. There are numerous methods in which an attacker can trick a victim into submitting a forged POST request, such as a simple form hosted in an attacker's Website with hidden values. This form can be triggered automatically by JavaScript or can be triggered by the victim who thinks the form will do something else.

Multi-Step Transactions

Multi-Step transactions are not an adequate prevention of CSRF. As long as an attacker can predict or deduce each step of the completed transaction, then CSRF is possible.

URL Rewriting

This might be seen as a useful CSRF prevention technique as the attacker cannot guess the victim's session ID. However, the user's session ID is exposed in the URL. We don't recommend fixing one security flaw by introducing another.

HTTPS

HTTPS by itself does nothing to defend against CSRF.

ZeroDay:

The term "zero-day" refers to the fact that the vendor or developer has only just learned of the flaw – which means they have "zero days" to fix it.

A zero-day attack takes place when hackers exploit the flaw before developers have a chance to address it. Zero-day is sometimes written as 0-day.

- A **zero-day vulnerability** is a software vulnerability discovered by attackers before the vendor has become aware of it. Because the vendors are unaware, no patch exists for zero-day vulnerabilities, making attacks likely to succeed.
- A **zero-day exploits** the method hackers use to attack systems with a previously unidentified vulnerability.
- A **zero-day attack** is the use of a zero-day exploit to cause damage to or steal data from a system affected by a vulnerability.

How to protect yourself against zero-day attacks

For zero-day protection and to keep your computer and data safe, it's essential for both individuals and organizations to follow cyber security best practices. This includes:

Keep all software and operating systems up to date. This is because the vendors include security patches to cover newly identified vulnerabilities in new releases. Keeping up to date ensures you are more secure.

Use only essential applications. The more software you have, the more potential vulnerabilities you have. You can reduce the risk to your network by using only the applications you need.

Use a firewall. A firewall plays an essential role in protecting your system against zero-day threats. You can ensure maximum protection by configuring it to allow only necessary transactions.

Within organizations, educate users. Many zero-day attacks capitalize on human error. Teaching employees and users good safety and security habits will help keep them safe online and protect organizations from zero-day exploits and other digital threats.

Use a comprehensive antivirus software solution.

DDoS Attack:

It means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

A **DDoS attack** aims to overwhelm the devices, services, and network of its intended target with fake internet traffic, rendering them inaccessible to or useless for legitimate users.

DoS vs. DDoS

A distributed denial-of-service attack is a subcategory of the more general denial-of-service (DoS) attack.

In a DoS attack, the attacker uses a single internet connection to barrage a target with fake requests or to try and exploit a cybersecurity vulnerability.

DDoS is larger in scale. It utilizes thousands (even millions) of connected devices to fulfill its goal. The sheer volume of the devices used makes DDoS much harder to fight.

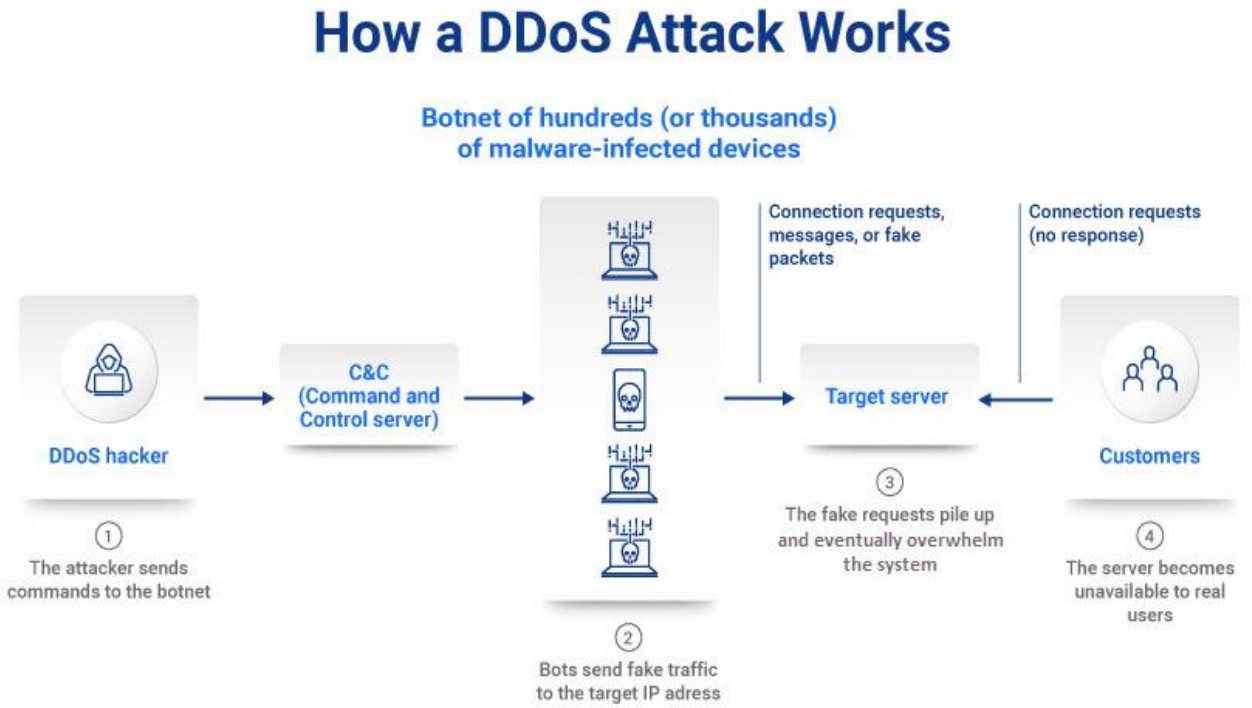
Botnets

Botnets are the primary way distributed denial-of-service-attacks are carried out.

The attacker will hack into computers or other devices and install a malicious piece of code, or malware, called a bot.

Together, the infected computers form a network called a botnet. The attacker then instructs the botnet to overwhelm the victim's servers and devices with more connection requests than they can handle.

How DDos Attack works:



Types of DDoS Attacks

Different attacks target different parts of a network, and they are classified according to the network connection layers they target.

A connection on the internet is comprised of seven different “layers," as defined by the Open Systems Interconnection (OSI) model created by the International Organization for Standardization.

The model allows different computer systems to be able to "talk" to each other.

Volume-Based or Volumetric Attacks

This type of attack aims to control all available bandwidth between the victim and the larger internet. Domain name system (DNS) amplification is an example of a volume-based attack. In this scenario, the attacker spoofs the target's address, then sends a DNS name lookup request to an open DNS server with the spoofed address.

When the DNS server sends the DNS record response, it is sent instead to the target, resulting in the target receiving an amplification of the attacker’s initially small query.

Protocol Attacks

Protocol attacks consume all available capacity of web servers or other resources, such as firewalls. They expose weaknesses in Layers 3 and 4 of the OSI protocol stack to render the target inaccessible.

A SYN flood is an example of a protocol attack, in which the attacker sends the target an overwhelming number of transmission control protocol (TCP) handshake requests with spoofed source Internet Protocol (IP) addresses. The targeted servers attempt to respond to each connection request, but the final handshake never occurs, overwhelming the target in the process.

Application-Layer Attacks

These attacks also aim to exhaust or overwhelm the target's resources but are difficult to flag as malicious. Often referred to as a Layer 7 DDoS attack—referring to Layer 7 of the OSI model—an application-layer attack targets the layer where web pages are generated in response to Hypertext Transfer Protocol (HTTP) requests.

A server runs database queries to generate a web page. In this form of attack, the attacker forces the victim's server to handle more than it normally does. An HTTP flood is a type of application-layer attack and is similar to constantly refreshing a web browser on different computers all at once.

In this manner, the excessive number of HTTP requests overwhelms the server, resulting in a DDoS.

UNIT-3

Cryptography, Authentication & Authorization

3.1 Encryption & Cryptography:

Encryption is the method by which information is converted into secret code that hides the information's true meaning.

Encryption is a way of scrambling data so that only authorized parties can understand the information.

In technical terms, it is the process of converting human-readable **plaintext** to incomprehensible text, also known as **ciphertext**.

In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a cryptographic key: a set of mathematical values that both the sender and the recipient of an encrypted message agree on.

The science of encrypting and decrypting information is called **cryptography**.

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it.

The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce.

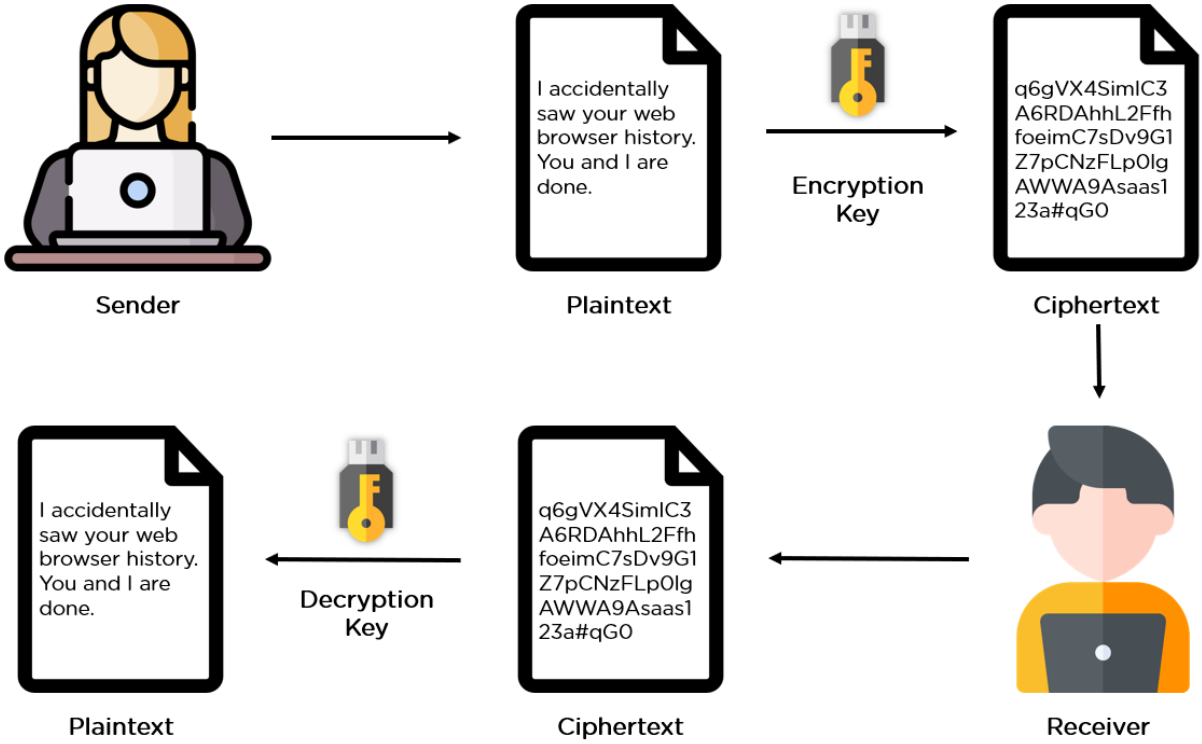
How does encryption work?

Encryption is a mathematical process that alters data using an encryption algorithm and a key.

Imagine if Person1 sends the message "Hello" to Person2, but he replaces each letter in his message with the letter that comes two places later in the alphabet.

Instead of "Hello," his message now reads "Jgnnq." Fortunately, person2 knows that the key is "2" and can decrypt her message back to "Hello."

Person1 used an extremely simple encryption algorithm to encode his message to Person2. More complicated encryption algorithms can further scramble the message:

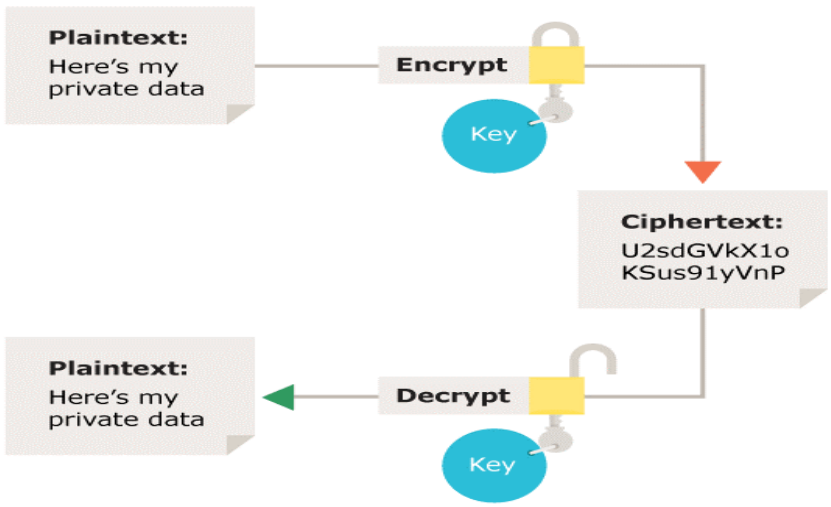


Types of Encryption

There are two types of encryption in use today: **symmetric** and **asymmetric** encryption. The name derives from whether or not the same key is used for encryption and decryption.

What is Symmetric Encryption?

In symmetric encryption the same key is used for encryption and decryption. It is therefore critical that a secure method is considered to transfer the key between sender and recipient.

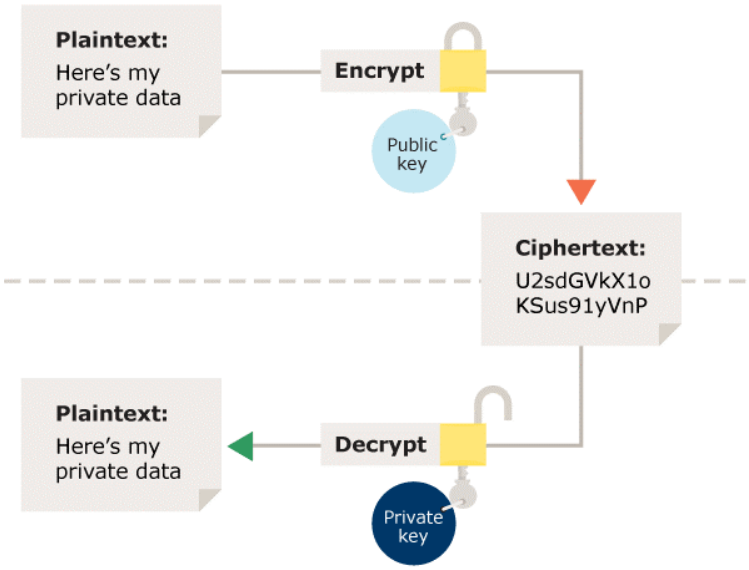


What is Asymmetric Encryption?

Asymmetric encryption uses the notion of a key pair: a different key is used for the encryption and decryption process. One of the keys is typically known as the private key and the other is known as the public key.

The private key is kept secret by the owner and the public key is either shared amongst authorised recipients or made available to the public at large.

Data encrypted with the recipient's public key can only be decrypted with the corresponding private key. Data can therefore be transferred without the risk of unauthorised or unlawful access to the data.



Why is encryption important?

Privacy: Encryption ensures that no one can read communications or data at rest except the intended recipient or the rightful data owner. This prevents attackers, ad networks, Internet service providers, and in some cases governments from intercepting and reading sensitive data, protecting user privacy.

Security: Encryption helps prevent data breaches, whether the data is in transit or at rest. If a corporate device is lost or stolen and its hard drive is properly encrypted, the data on that device will still be secure. Similarly, encrypted communications enable the communicating parties to exchange sensitive data without leaking the data.

Data integrity: Encryption also helps prevent malicious behavior such as on-path attacks. When data is transmitted across the Internet, encryption ensures that what the recipient receives has not been viewed or tampered with on the way.

Regulations: For all these reasons, many industry and government regulations require companies that handle user data to keep that data encrypted.

3.2 Decrypt Secret Message:

Caesar Cipher:

- The Caesar cipher is a simple encryption technique that was used by Julius Caesar to send secret messages to his allies. It works by shifting the letters in the plaintext message by a certain number of positions, known as the “shift” or “key”.
- The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.
- Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.
- The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

Here is an example of how to use the Caesar cipher to encrypt the message “HELLO” with a shift of 3:

1. Write down the plaintext message: HELLO
2. Choose a shift value. In this case, we will use a shift of 3.
3. Replace each letter in the plaintext message with the letter that is three positions to the right in the alphabet.

   H becomes K (shift 3 from H)

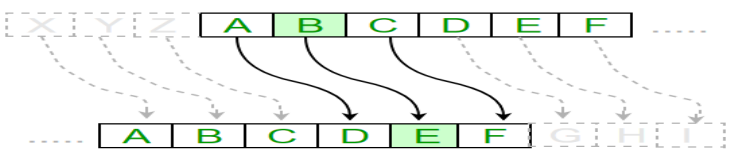
   E becomes H (shift 3 from E)

   L becomes O (shift 3 from L)

   L becomes O (shift 3 from L)

   O becomes R (shift 3 from O)

4. The encrypted message is now “KHOOR”.



Examples :

Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Shift: 23

Cipher: XYZ ABCDEFGHIJKLMNOPQRSTUVW

Text : ATTACKATONCE

Shift: 4

Cipher: EXXEGOEXSRGI

```
#A python program to illustrate Caesar Cipher Technique
def encrypt(text,s):
    result = ""
     # traverse text
    for i in range(len(text)):
        char = text[i]
         # Encrypt uppercase characters
        if (char.isupper()):
            result += chr((ord(char) + s-65) % 26 + 65)
         # Encrypt lowercase characters
        else:
            result += chr((ord(char) + s - 97) % 26 + 97)
     return result
 #check the above function
text = "ATTACKATONCE"
s = 4
print ("Text  : " + text)
print ("Shift : " + str(s))
print ("Cipher : " + encrypt(text,s))
```

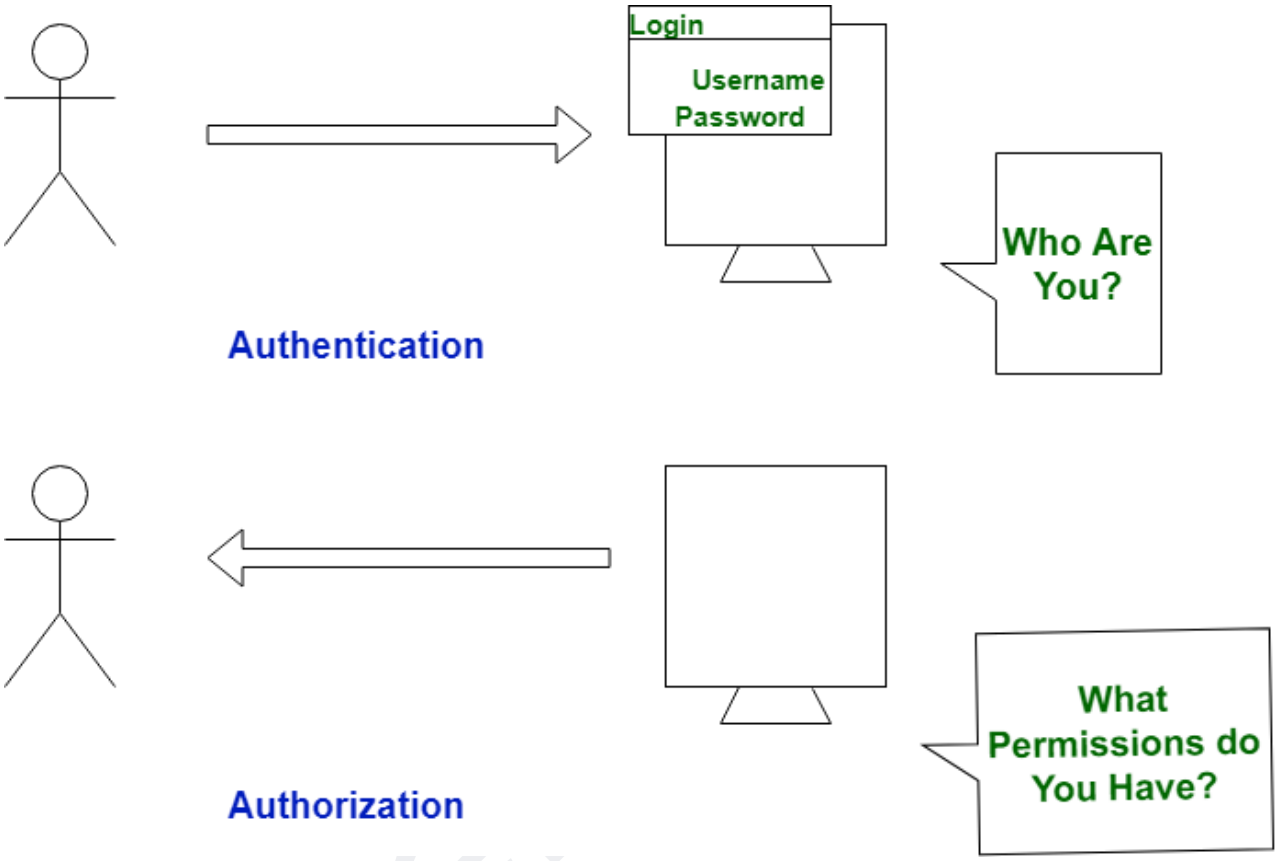
3.3 Authentication & Authorization:

Both Authentication and Authorization area units are utilized in respect of knowledge security that permits the safety of an automatic data system.

Each area unit terribly crucial topics usually related to the online as key items of its service infrastructure. However, each of the terms area units is completely different with altogether different ideas. whereas indeed, they're usually employed in an equivalent context with an equivalent tool, they're utterly distinct from one another.

In the authentication process, the identity of users is checked for providing access to the system. While in the authorization process, a person's or user's authorities are checked for accessing the resources.

Authentication is done before the authorization process, whereas the authorization process is done after the authentication process.



Authentication	Authorization
In the authentication process, the identity of users are checked for providing access to the system.	While in the authorization process, the person's or user's authorities are checked for accessing the resources.
In the authentication process, users or persons are verified.	While in this process, users or persons are validated.
It is done before the authorization process.	While this process is done after the authentication process.
It usually needs the user's login details.	While it needs the user's privilege or security levels.
Authentication determines whether the person is a user or not.	While it determines **What permission does the user have?**

Generally, transmit information through an ID Token. The OpenID Connect (OIDC) protocol is an authentication protocol that is generally in charge of the user	Generally, transmit Access Token. The OAuth 2.0 protocol governs the overall system of user authorization process.
Popular Authentication Techniques- ● Password-Based Authentication ● Passwordless Authentication ● 2FA/MFA (Two-Factor Authentication / Multi-Factor Authentication) ● Single sign-on (SSO) ● Social authentication	Popular Authorization Techniques- ● Role-Based Access Controls (RBAC) ● JSON web token (JWT) Authorization ● SAML Authorization ● OpenID Authorization ● OAuth 2.0 Authorization
The authentication credentials can be changed in part as and when required by the user.	The authorization permissions cannot be changed by the user as these are granted by the owner of the system and only he/she has the access to change it.
The user authentication is visible at the user end. The user authentication is identified with username, password, face recognition, retina scan, fingerprints, etc.	The user authorization is not visible at the user end. The user authorization is carried out through the access rights to resources by using roles that have been pre-defined.
Example: Employees in a company are required to authenticate through the network before accessing their company email.	**Example:** After an employee successfully authenticates, the system determines what information the employees are allowed to access.

3.4 Online Secure Transaction:

1. **Never use public Wi-Fi or a public computer for online transaction or money transfer:**

   Never attempt an online transaction on a public Wi-Fi. They often have fewer security features than a private network. So always switch to your phone data.If you have to do an emergency transaction on a public wifi out of emergency, be sure to change it ASAP.

2. **Firewalls and Antivirus**

   If you don't have an antivirus app, get one -- ideally if it's a paid one. Put your antivirus on auto update. This will ensure that it’s updated all the time. There's new malware on the internet every day.

An updated firewall will protect you from these. Turn your firewall on. Firewalls often block sites that are malicious or suspicious. If your firewall blocks a certain website, be sure to avoid it.

3. **Never reply to fraud emails and texts**

   Phishing or the attempt to gain your personal information generally over email or text is rampant. Your inbox is probably full of emails, claiming that you've won a contest or you've been credited a certain amount of money.

   Never open these emails. Never reply to them. Learn to identify such spam mail and ignore them, or if you have the time, delete them.

4. **Check for digital certificates:**
   Always check for the digital certificates when using a third party payment method. Often you can see a symbol like 'VeriSign' on the window, and you can click on it to get information on the website's certification.

5. **Prefer virtual keyboard**

   There are malware and viruses that can make a log of what you type on your keyboard. So it's advisable to use a virtual keyboard when doing an online transaction. Banks have an option for a virtual keyboard on their login pages. Use it.

6. **Enable two-step verification**

   If your device doesn't have a mandatory two-step verification, make sure to turn it on. Two-step verification involves passing two security walls to perform an operation on your phone. For example, Google's two-step verification asks you to verify yourself by asking you your password, pattern or fingerprint first and then they divert you to your bank's website.

7. **Check if the connection is secure**

   Always check for the lock symbol on the address bar and check if 'https://' is in green. It means that the connection is secure. If it's yellow or red, never attempt an online transaction as it might make your information vulnerable.

8. **Always track your online spending**

   Keep track of your bank balance and how much you spend online. It's better to dedicate just one credit or debit card for online transactions. This makes tracking

your online spending easier. If you find any suspicious behaviour, check with your bank immediately.

9. **Private Browsing**

   Another way to protect your information is private browsing like the incognito mode on google chrome. Private browsing doesn't save passwords or create history and it clears all the cookies and cache data from your device.

10. **Always mind your password**

    Protecting your password is extremely critical and there are several key points you must remember:

    - Never share your password with anyone, even your family members.
    - If you've written it down on a piece of paper, make sure to keep it safe. Writing your passwords anywhere is inadvisable, though.
    - Change your password often, preferably after 2-3 months.
    - Never keep the same password for all your accounts. If one of your accounts is hacked, your other accounts become extremely vulnerable.
    - Never allow browsers to save your password.
    - Make your passwords difficult to guess. Make a long password with alphanumeric characters and symbols. Make use of both uppercase and lowercase letters.

11. **Don't forget to log out**

    Never just leave your device without logging out of your account. Most banks now have a system, where they automatically log you out after a period of inactivity, but it's better to do it yourselves.

Since most of our life is spent online, it's out for everybody. Thus it's critical to protect your information; money being one of them. No one likes losing their money, because it's hard earned. So being careful will save you from losing it.

UNIT-4

Network Security Basics

4.1 Network Security basics:

Network Security refers to the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats.

The most basic example of Network Security is password protection which the user of the network oneself chooses. In recent times, Network Security has become the central topic of cyber security with many organizations inviting applications from people who have skills in this area. The network security solutions protect various vulnerabilities of the computer systems such as:

- Users
- Locations
- Data
- Devices
- Applications

Benefits of Network Security

Network Security has several benefits, some of which are mentioned below:

- Network Security helps in protecting clients' information and data which ensures reliable access and helps in protecting the data from cyber threats.
- Network Security protects the organization from heavy losses that may have occurred from data loss or any security incident.
- It overall protects the reputation of the organization as it protects the data and confidential items.

Working on Network Security

The basic principle of network security is protecting huge stored data and networks in layers that ensure the bedding of rules and regulations that have to be acknowledged before performing any activity on the data.

These levels are:

Physical Network Security

Technical Network Security

Administrative Network Security

These are explained below:

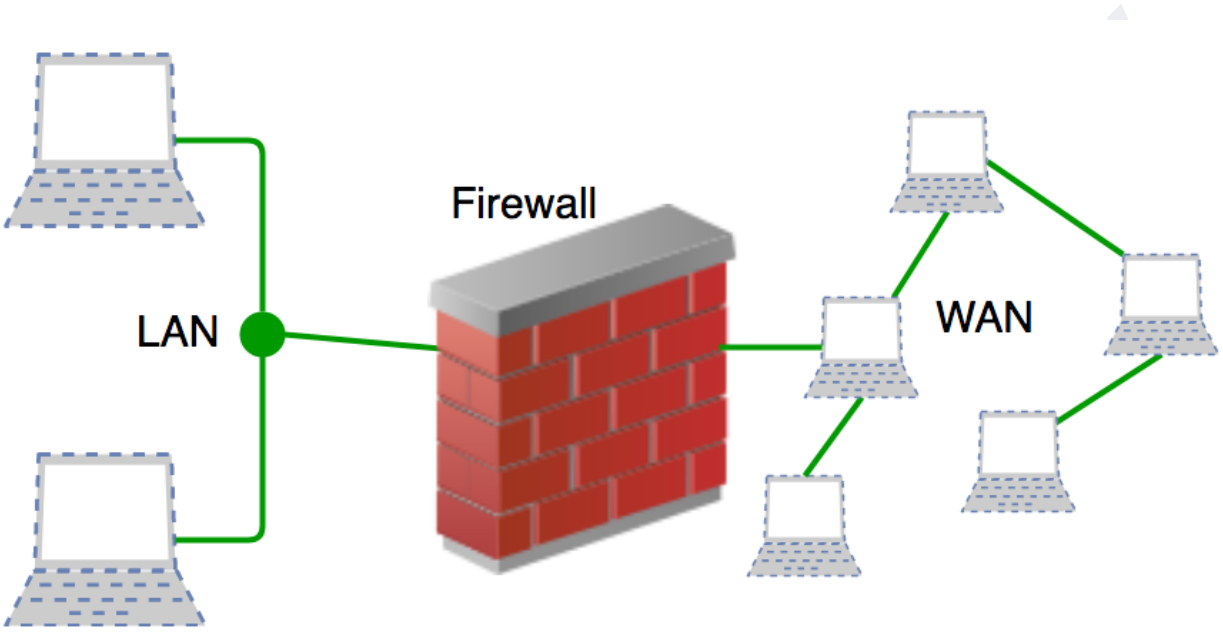
1. **Physical Network Security:** This is the most basic level that includes protecting the data and network through unauthorized personnel from acquiring control over the confidentiality of the network. These include external peripherals and routers that might be used for cable connections. The same can be achieved by using devices like biometric systems.
2. **Technical Network Security:** It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One is protected from unauthorized users, and the other is protected from malicious activities.
3. **Administrative Network Security:** This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.

Types of Network Security

The few types of network securities are discussed below:

1. **Access Control:** Not every person should have a complete allowance for the accessibility to the network or its data. One way to examine this is by going through each personnel's details. This is done through Network Access Control which ensures that only a handful of authorized personnel must be able to work with the allowed amount of resources.
2. **Antivirus and Anti-malware Software:** This type of network security ensures that any malicious software does not enter the network and jeopardize the security of the data. Malicious software like Viruses, Trojans, and Worms is handled by the same. This ensures that not only the entry of the malware is protected but also that the system is well-equipped to fight once it has entered.
3. **Cloud Security:** Nowadays, a lot of organizations are joining hands with cloud technology where a large amount of important data is stored over the internet. This is very vulnerable to the malpractices that few unauthorized dealers might pertain to. This data must be protected and it should be ensured that this protection is not jeopardized by anything. Many businesses embrace SaaS applications for providing some of their employees the allowance of accessing the data stored in the cloud. This type of security ensures creating gaps in the visibility of the data.

4. **Email Security:** Email Security depicts the services, and products designed to protect the Email Account and its contents safe from external threats. For Example, you generally see, fraud emails are automatically sent to the Spam folder. because most email service providers have built-in features to protect the content.
5. **Firewalls:** A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules accepts, rejects, or drops that specific traffic. Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers.



6. **Application Security:** Application security denotes the security precautionary measures utilized at the application level to prevent the stealing or capturing of data or code inside the application. It also includes the security measurements made during the advancement and design of applications, as well as techniques and methods for protecting the applications whenever.
7. **Intrusion Prevention System(IPS):** An intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. The major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it, and attempt to block or stop it.

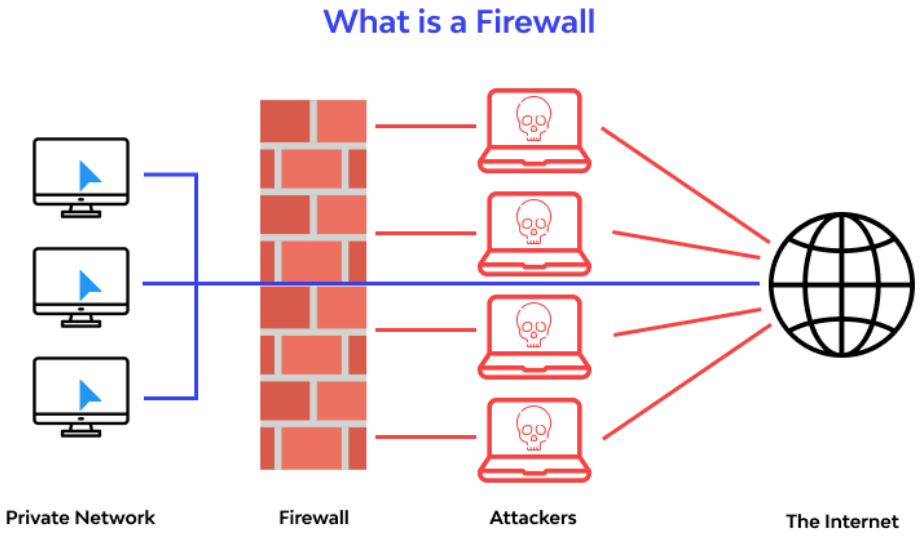
4.2 Network Security Devices:

1. Firewalls:

Firewalls are network security devices that monitor and 'curate' network traffic based on a rigid set of rules. A firewall establishes a protective wall between your internal private network and the global internet.

As we'll see soon enough, firewalls can be both software applications and hardware devices. Hardware firewalls can serve multiple purposes along with network protection, like dynamically assigning identifying IP addresses to devices present in the network.

Firewalls are used at the 'boundary' of a private network to prevent unauthorized access via the internet. All inbound and outbound messages are scanned by the firewall before they can leave or enter the private network. During the scan, the firewall passes the message (also called a network packet) through a security checklist, which is basically a list of rules that qualify a message as safe. Only if a message checks all the boxes, is it allowed to travel forward.



2. Routers:

Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

Features of Routers

- A router is a layer 3 or network layer device.

- It connects different networks together and sends data packets from one network to another.
- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
- It transfers data in the form of IP packets. In order to transmit data, it uses the IP address mentioned in the destination field of the IP packet.
- Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
- In order to prepare or refresh the routing table, routers share information among each other.
- Routers provide protection against broadcast storms.
- Routers are more expensive than other networking devices like hubs, bridges, and switches.

Routers are manufactured by some popular companies like –

Cisco

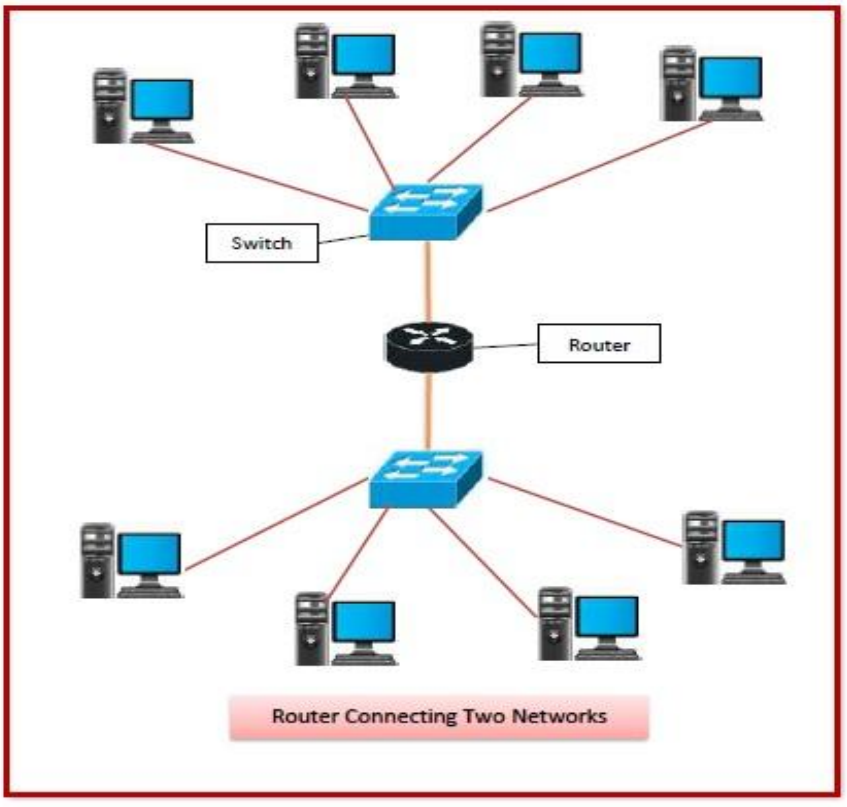
D-Link

HP

3Com

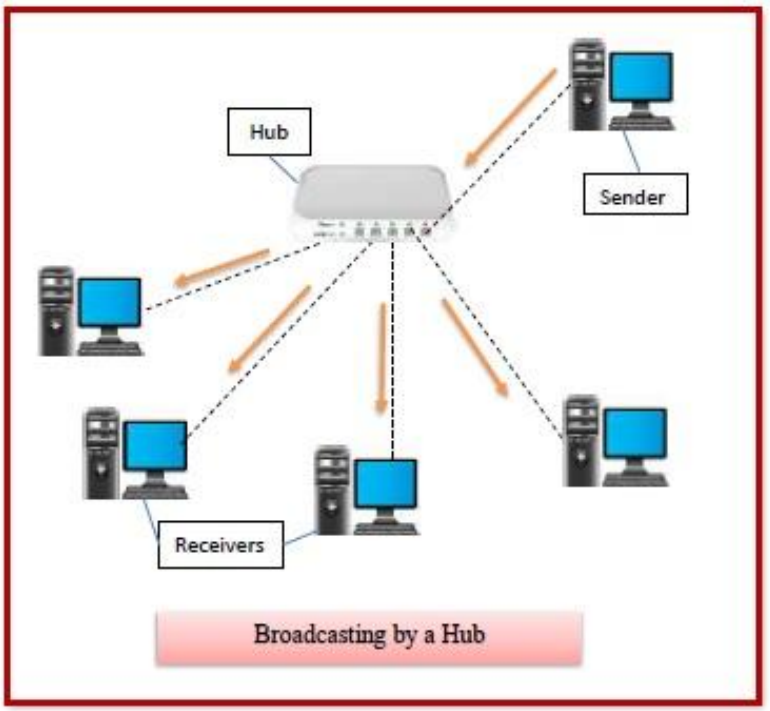
Juniper

Nortel



3. Hub:

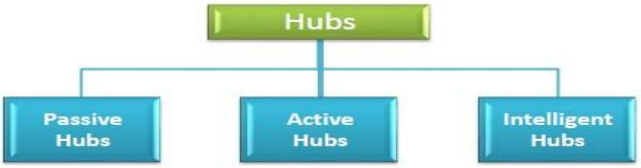
Hubs are networking devices operating at a physical layer of the OSI model that are used to connect multiple devices in a network. They are generally used to connect computers in a LAN.



Features of Hubs

- A hub operates in the physical layer of the OSI model.
- A hub cannot filter data. It is a non-intelligent network device that sends messages to all ports.
- It primarily broadcasts messages. So, the collision domain of all nodes connected through the hub stays one.
- Transmission mode is half duplex.
- Collisions may occur during setup of transmission when more than one computer places data simultaneously in the corresponding ports.
- Since they lack intelligence to compute the best path for transmission of data packets, inefficiencies and waste occur.
- They are passive devices, they don't have any software associated with it.

Types of Hubs :



Passive Hubs – Passive hubs connect nodes in a star configuration by collecting wiring from nodes. They broadcast signals onto the network without amplifying or regenerating them. As they cannot extend the distance between nodes, they limit the size of the LAN.

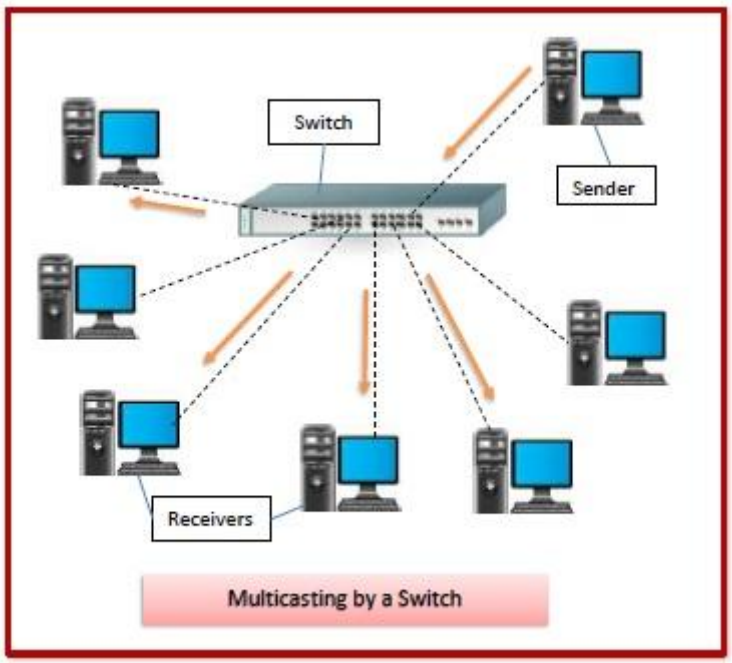
Active Hubs – Active hubs amplify and regenerate the incoming electrical signals before broadcasting them. They have their own power supply and serve both as a repeater as well as connecting centre. Due to their regenerating capabilities, they can extend the maximum distance between nodes, thus increasing the size of LAN.

Intelligent Hubs – Intelligent hubs are active hubs that provide additional network management facilities. They can perform a variety of functions of more intelligent network devices like network management, switching, providing flexible data rates etc.

4. **Switch:**

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s). It supports unicast, multicast as well as broadcast communications.

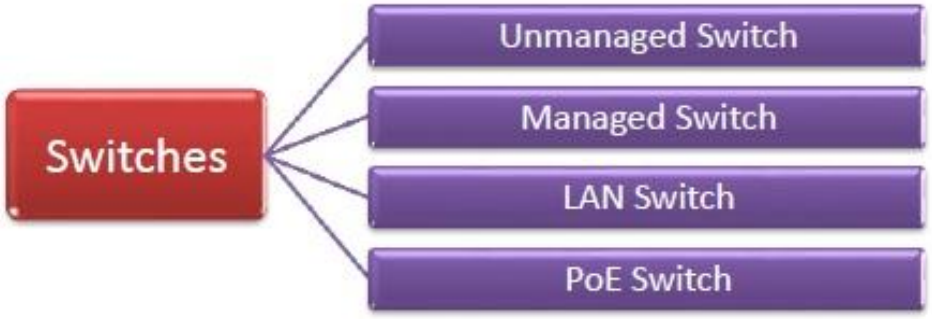


Features of Switches:

- A switch operates in the layer 2, i.e. data link layer of the OSI model.
- It is an intelligent network device that can be conceived as a multiport network bridge.

- It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
- It uses packet switching technique to receive and forward data packets from the source to the destination device.
- It supports unicast (one-to-one), multicast (one-to-many), and broadcast (one-to-all) communications.
- Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.
- Switches are active devices, equipped with network software and network management capabilities.
- Switches can perform some error checking before forwarding data to the destined port.
- The number of ports is higher – 24/48.

Types of Switches



Unmanaged Switch – These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices need to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.

Managed Switch – These are costly switches that are used in organisations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.

LAN Switch – Local Area Network (LAN) switches connect devices in the internal LAN of an organization. They are also referred to as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.

PoE Switch – Power over Ethernet (PoE) switches are used in PoE Gigabit Ethernets. PoE technology combines data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplify the cabling connections.

5. **Hotspot**:

A hotspot is a physical location where people can access the Internet, typically using Wi-Fi, via a wireless local area network (WLAN) with a router connected to an Internet service provider. Most people refer to these locations as "Wi-Fi hotspots" or "Wi-Fi connections." Simply put, hotspots are the physical places where users can wirelessly connect their mobile devices, such as smartphones and tablets, to the Internet.

A hotspot can be in a private location or a public one, such as in a coffee shop, a hotel, an airport, or even an airplane. While many public hotspots offer free wireless access on an open network, others require payment. Later in the article you'll learn how to connect a mobile device to a Wi-Fi hotspot.

Mobile hotspot:

A mobile hotspot (sometimes called a portable hotspot) is a hotspot that's just that mobile! While a "regular" Wi-Fi hotspot is tied to a physical location, you can create a mobile hotspot by using your smartphone's data connection to connect your laptop to the Internet. This process is called "tethering." More on this process later.

You should also know these terms when you're talking about Wi-Fi hotspots.

Access point (wireless access point):

A wireless access point (WAP) is a networking device that allows a Wi-Fi compliant device to connect to a wired network. The WAP can either be physically connected to a router or be integrated into the router itself. A WAP is not a hotspot, which is the physical location where Wi-Fi access to a WLAN is available.

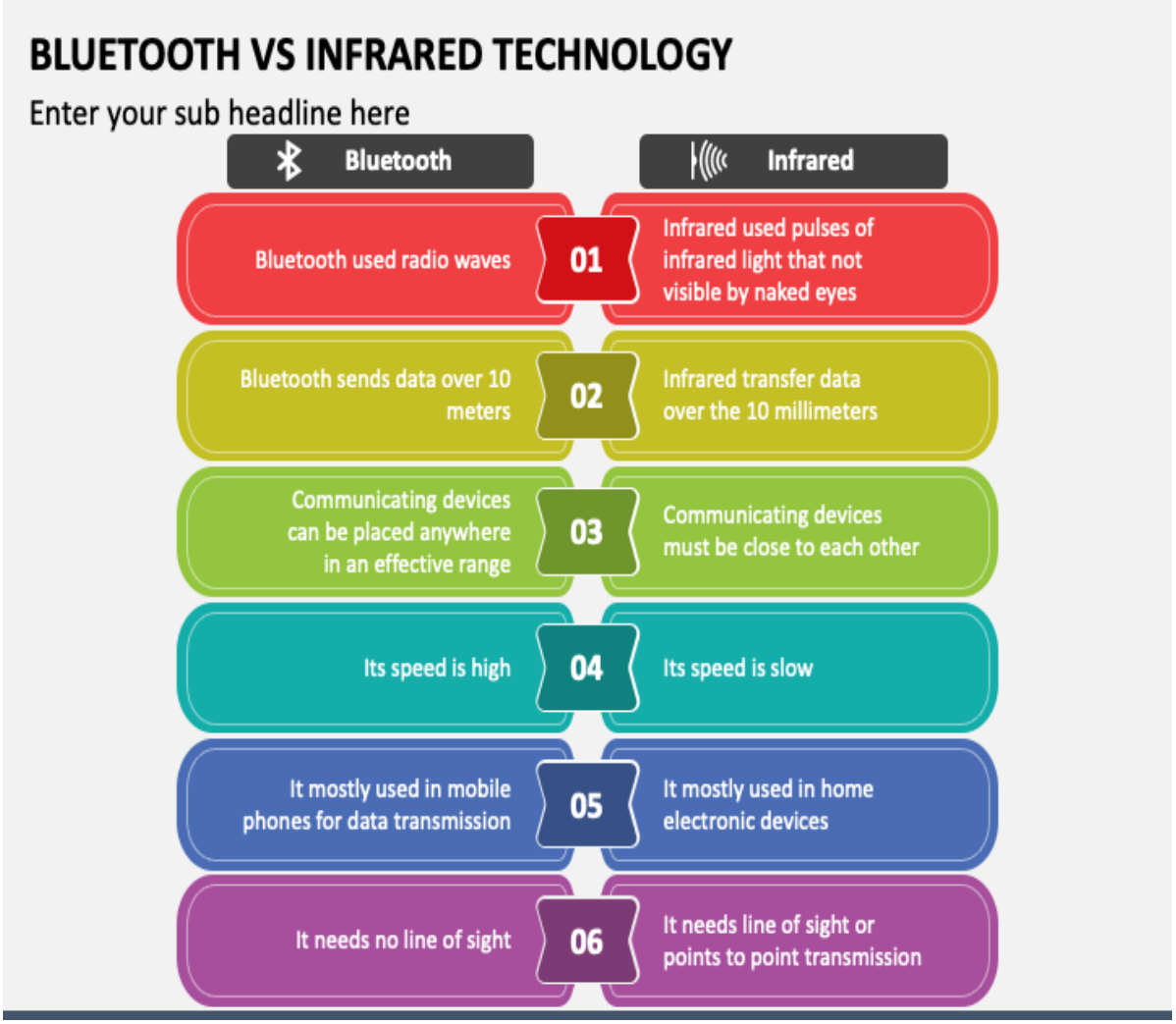
Wi-Fi:

Wi-Fi is the technology that allows your smartphone or computer to access the Internet through a wireless connection. It uses radio signals to send and receive data between your enabled device and the WAP.

SSID:

A service set identifier (more commonly known as an SSID) is the unique name of a wireless network. You'll need to know the name of the wireless network to connect to it. Your computer or smartphone can search for available wireless networks; often people name their network for easy identification—anything from "Bob's phone" to "hotel guests" to "Get off my LAN."

6. Bluetooth and Infrared:



UNIT - 5

Security of Personal Devices

5.1 Basics of Security of personal devices:

These days nearly everyone has a mobile device, right? What you may not know about your smartphone is that it represents one of the fastest growing "attack surfaces" for cybercriminals. They are exposed daily to more networks and other devices than any piece of equipment you own. Not to mention the fact that taking them wherever you go makes them more likely to be lost or stolen than most other devices.

Mobile phones contain a great deal of personal information about you. Many apps on your phone provide access to your bank accounts or other accounts that contain sensitive information. Your phone probably contains direct access to your email, text messages and social media accounts that can be used to steal your identity and to trick your friends into providing their sensitive information as well.

Things like this can happen when an attacker physically gets ahold of your mobile device. But did you know that there are a growing number of exploits that take advantage of your phone's Bluetooth, WiFi and cellular connections to gain virtual access to your phone. Phones can be infected with malware just like a computer can!

So what should you do to make sure your mobile phone is secure?

The following is a list of tips we recommend.

- Use a strong pin or password on your phone
- Consider enabling fingerprint or face logins to your device
- Disable WiFi and/or Bluetooth when you don't need them
- Be careful what apps you download and what services you allow them to access
- Disable location services when you don't need them
- Be careful about where you plug in your phone
- Employ remote wiping software (Find my iPhone, Android Device manager, etc)
- Backup your phone often

5.2 Best practice to secure personal devices, social media :

Threats to mobile devices are more prevalent and increasing in scope and complexity. Users of mobile devices desire to take full advantage of the features available on those devices, but many of the features provide convenience and capability but sacrifice security. This best practices guide outlines steps the users can take to better protect personal devices and information.

WHAT CAN I DO TO PREVENT/MITIGATE?

THREAT/VULNERABILITY	Update Software & Apps	Only Install Apps from Official Stores	Turn Off Cellular, WiFi, Bluetooth	Do Not Connect to Public Networks	Use Encrypted Voice/ Text/Data Apps	Do Not Click Links or Open Attachments	Turn Device Off & On Weekly	Use Mic-Drowning Case, Cover Camera	Avoid Carrying Device/No Sensitive Conversations Around Device	Lock Device with PIN	Maintain Physical Control of Device	Use Trusted Accessories	Turn Off Location Services
Spearphishing (To install Malware)	◒	◒				◒	◒						
Malicious Apps	◒	◒				◒							
Zero-Click Exploits	◒			◒			◒						
Malicious Wi-Fi Network/Close Access Network Attack	◒		●	◒	◒								
Foreign Lawful Intercept/ Untrusted Cellular Network	◒	◒	◒		◒								
Room Audio/ Video Collection	◒	◒						●	●				
Call/Text/Data Collection Over Network		◒	●	◒	◒								
Geolocation of Device		◒	◒	◒					●				◒
Close Access Physical Attacks	◒									◒	◒	◒	
Supply Chain Attacks												◒	

Does not prevent (no icon) ◒ Sometimes prevents ● Almost always prevents

5.2.1 Mobile Device Security Best Practices

1. **Turn User Authentication On:**

   It's so easy for company laptops, tablets, and smartphones to get lost or stolen as we leave them in taxi cabs, restaurants, airplanes..the list goes on.

   The first thing to do is to ensure that all your mobile user devices have the screen lock turned on and that they require a password or PIN to gain entry. There is a ton of valuable information on the device!

   Most devices have biometric security options like Face ID and Touch ID, which definitely makes the device more accessible, but not necessarily more secure. That's why it is a good idea to take your mobile security practices a step further and implement a Multi-Factor Authentication (MFA, also known as two-factor authentication) policy for all end-users as an additional layer of security.

2. **Use A Password Manager**

   Let's be honest, passwords are not disappearing any time soon, and most of us find them cumbersome and hard to remember. We're also asked to change them frequently, which makes the whole process even more painful.

   Enter the password manager, which you can think of as a "book of passwords" locked by a master key that only you know.

   Not only do they store passwords, but they also generate strong, unique passwords that save you from using your cat's name or child's birthday...over and over.

   Although Microsoft has enabled password removal on their Microsoft 365 accounts, we're still far from being rid of them forever! As long as we have sensitive data and corporate data to protect, passwords will be a critical security measure.

3. **Update Your Operating Systems (OS) Regularly**

   If you're using outdated software, your risk of getting hacked skyrockets. Vendors such as Apple (IOS), Google, and Microsoft constantly provide security updates to stay ahead of security vulnerabilities.

   Don't ignore those alerts to upgrade your laptop, tablet, or smartphone. To help with this, ensure you have automatic software updates turned on by default on your

mobile devices. Regularly updating your operating system ensures you have the latest security configurations available!

When it comes to your laptop, your IT department or your IT services provider should be pushing you appropriate software updates on a regular basis.

Be sure to take a moment to hit "restart"; otherwise, it won't do you much good!

Although it's very tempting to use that free Wi-Fi at the coffee shop, airport or hotel lobby - don't do it.

Any time you connect to another organization's network, you're increasing your risk of exposure to malware and hackers.

There are so many online videos and easily accessible tools that even a novice hacker can intercept traffic flowing over Wi-Fi, accessing valuable information such as credit card number, bank account numbers, passwords and other private data.

Interestingly, although public Wi-Fi and bluetooth are a huge security gap and most of us (91%) know it, 89% of us choose to ignore

4. **Avoid Public Wi-Fi**

Although it's very tempting to use that free Wi-Fi at the coffee shop, airport or hotel lobby - don't do it.

Any time you connect to another organization's network, you're increasing your risk of exposure to malware and hackers. There are so many online videos and easily accessible tools that even a novice hacker can intercept traffic flowing over Wi-Fi, accessing valuable information such as credit card number, bank account numbers, passwords, and other private data.

The only caveat here is...if you absolutely must use a public Wi-Fi network, make sure you are also using a VPN to encrypt your internet activity and make it unreadable to cyber criminals. But remember, even this tactic may not offer the cybersecurity protection you need to be truly secure when using public internet access.

Interesting but disturbing fact: although public Wi-Fi and Bluetooth are a considerable security gap and most of us (91%) know it, 89% of us ignore it. Choose to be in the minority here!

5. **Remote Lock and Data Wipe**

Every business should have a Bring Your Own Device (BYOD) policy that includes a strict remote lock and data wipe policy.

Under this policy, whenever a mobile device is believed to be stolen or lost, the business can protect the lost data by remotely wiping the device or, at minimum, locking access.

Where this gets a bit sticky is that you're essentially giving the business permission to delete all personal data as well, as typically in a BYOD situation the employee is using the device for both work and play.

6. **Cloud Security and Data Backup**

Keep in mind that your public cloud-based apps and services are also being accessed by employee-owned mobile devices, increasing your company's risk of data loss.

That's why, for starters, back up your cloud data! If your device is lost or stolen, you'll still want to be able to access any data that might have been compromised as quickly as possible.

Select a cloud platform that maintains a version history of your files and allows you to roll back to those earlier versions, at least for the past 30 days.

Google's G Suite, Microsoft Office 365, and Dropbox support this.

Once those 30 days have elapsed, deleted files or earlier versions are gone for good.

You can safeguard against this by investing in a cloud-to-cloud backup solution, which will back up your data for a relatively nominal monthly fee.

7. **Understand and Utilize Mobile Device Management (MDM) and Mobile Application Management (MAM)**

Mobile security has become the hottest topic in the IT world. How do we allow users to access the data they need remotely, while keeping that data safe from whatever lurks around on these potentially unprotected devices?

The solution is two-fold: Mobile Device Management (MDM) and Mobile Application Management (MAM).

Mobile Device Management is the configuration, monitoring, and management of your employees' personal devices, such as phones, tablets, and laptops.

Mobile Application Management is configuring, monitoring, and managing the applications on those mobile devices. This includes things like Microsoft 365 and authenticator apps.

When combined, MDM and MAM can become powerful security solutions, preventing unauthorized devices from accessing your company network of applications and data.

Note that both solutions should be sourced, implemented, and managed by IT experts - in-house or outsourced-familiar with mobile security. For example, you can look at this short case study on how we implemented Microsoft Intune MDM for a healthcare provider, including the details behind the implementation.

5.3 Hardening your device (Windows & Linux)

Operating system (OS) hardening, a type of system hardening, is the process of implementing security measures and patching for operating systems, such as Windows, Linux, or Apple OS X, to strengthen them against cyberattacks. The goal is to protect sensitive computing systems, reducing the system's attack surface, in order to lower the risk of data breaches, unauthorized access, systems hacking, or malware.

OS hardening can include practices such as:

- Following security best practices and ensuring secure configuration.
- Updating the operating system, and automatically applying patches and service packs. This is typically done via software applications that MSPs or IT admins run on the system to install updates.
- Establishing strict access rules, limiting and authenticating system access permissions, and limiting creation of user accounts.
- Deploying additional security measures such as firewalls and endpoint protection systems.
- Using operating system security extensions such as AppArmor for Linux.
- Removing unnecessary applications and services and uninstalling unnecessary device drivers.
- Turning on only the ports and services required

- Encrypting the HDD or SSD that stores and hosts the OS

OS Hardening Security Benefits

Here are a few key benefits of hardening operating systems:

- Improve security and reduce a system's attack surface, minimizing a computer's exposure to threats.
- Lower the risk of data breaches, unauthorized access, systems hacking, or malware.
- Protect sensitive computing systems that run mission critical workloads or store sensitive data.
- Supports compliance with industry-specific regulations and standards.
- Increases system stability and reliability by removing unused services and applications.
- Minimizes IT support costs and frequency of support calls due to fewer security incidents.

Practical:-5

Evaluate Network Defence tools for Following

1. IP spoofing

2. DOS Attacks

1. IP Spoofing:

IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both. It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure.

Sending and receiving IP packets is a primary way in which networked computer and other devices communicate and constitutes the basis of the modern internet. All IP packets contain a header which precedes the body of the packet and contains important routing information, including the source address. In a normal packet, the source IP address is the address of the sender of the packet. If the packet has been spoofed, the source address will be forged.

Macchanger:

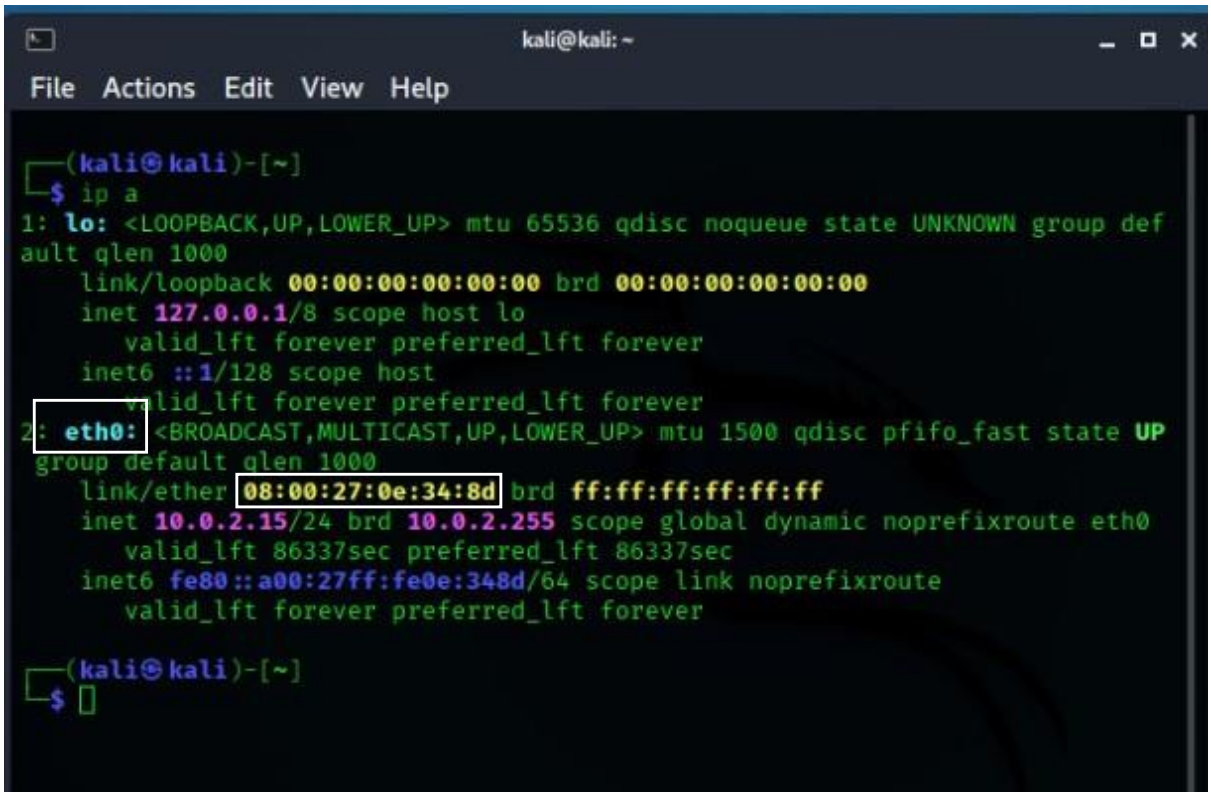
A Media Access Control (MAC) address is a unique number that gets assigned to every network interface, including Ethernet and wireless. It's used by many system programs and protocols in order to identify a network interface. One of the most common examples would be in the case of DHCP, where a router assigns an IP address to a network interface automatically. The router will know which device it has assigned an IP address to by referring to the MAC address.

Unlike an IP address, which is temporary and can be changed easily, MAC addresses are hardcoded into a network interface from the manufacturer. However, it's still possible to change or "spoof" a MAC address temporarily. On Linux systems, one of the easiest ways to do this is with the macchanger command line program. There are both legitimate and shady reasons for why a Linux user may find the need to change a MAC address.

In this guide, we'll show how to install the macchanger program on major Linux distros and then use the macchanger command to change the MAC address of a network interface either to a random value or some specific number.

Example:

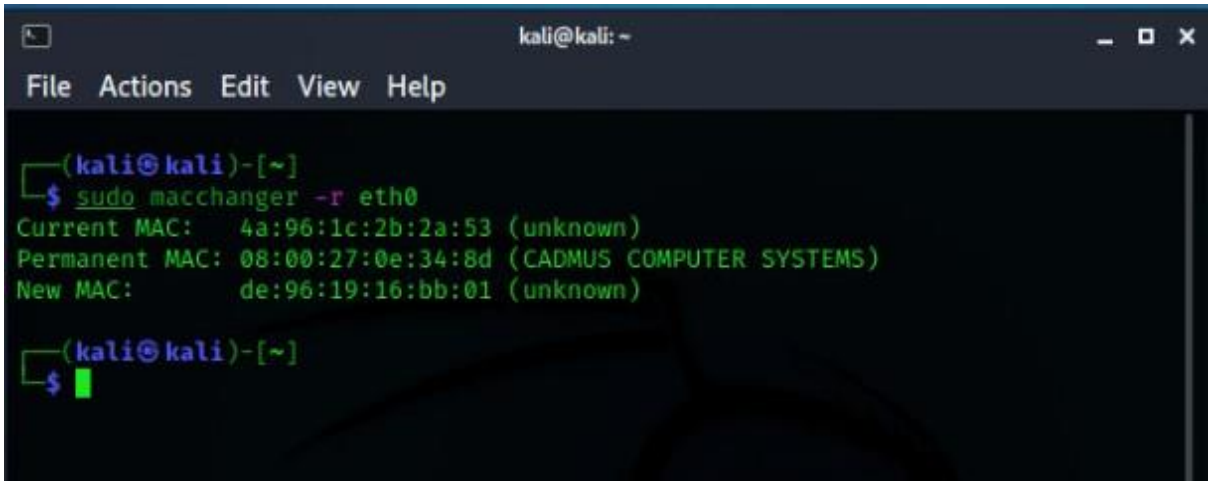
Before we start using the **macchanger** command, you'll need to know the name of the network interface that you want to work with. You can execute the **ip a** command to see a list of all the available network interfaces on your system. In most cases this will include a wired, wireless, and loopback interface.



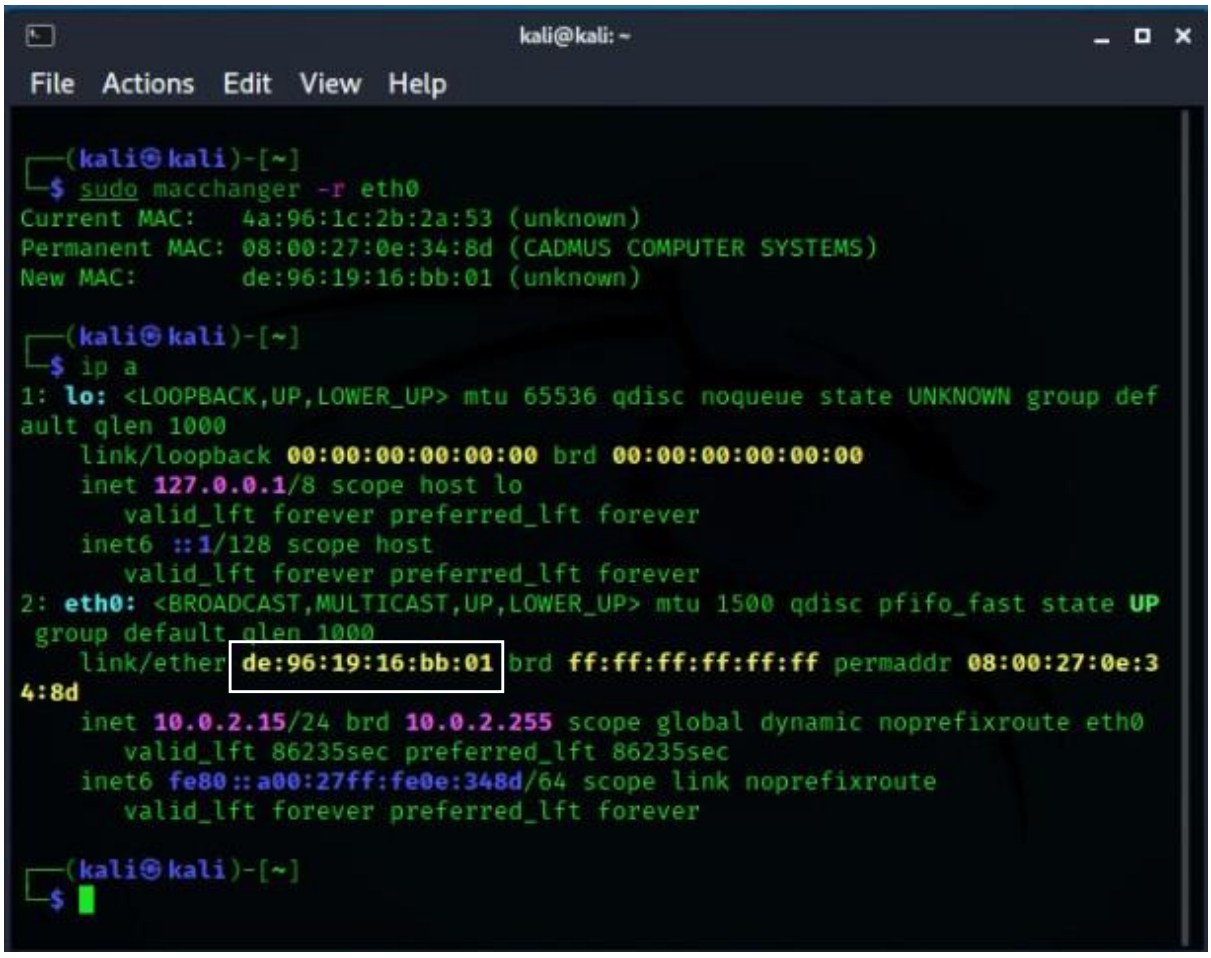
The name of network interface is **eth0** and MAC address of system is **08:00:27:0e:34:8d**.

Step:-1 Use -r command to get a random MAC address.

Sudo macchanger -r <network interface>



Step:-2 To verify the change run **ip a** command.



2. DoS attack:

DoS (Denial of Service) is an attack performed on a computer or a network that reduces, restricts or prevents accessibility of system resources to legitimate users. In simple terms, Attacker floods the victim system with the malicious traffic to overload its resources. A DoS attack can do temporary or permanent damage to a website. It can also slow down network performance.

Tools for DoS/DDoS attack:

1. Slowloris
2. LOIC (Low Orbit Iron Canon)
3. HOIC (High Orbit Iron Canon)
4. Pyloris

Slowloris:

Slowloris is a free and open source tool available on Github. We can perform a denial of service attack using this tool. It's a framework written in python. This tool allows a single machine to take down another machine's web server using perfectly legitimate HTTP traffic. It makes a full TCP connection and then requires only a few hundred requests at long-term and regular intervals. As a result, the tool doesn't need to spend a lot of traffic to exhaust the available connections on a server.

Use of Slowloris:

- Slowloris sends multiple requests to the target as a result generates heavy traffic botnets.
- Slowloris can be used to perform ddos attacks on any web server.
- It is an open-source tool, so you can download it from github free of cost.
- It uses perfectly legitimate HTTP traffic.
- Denial of service attack can be executed with the help of Slowloris by generating heavy traffic of botnets.

Installation and step-by-step implementation of slowloris tool:

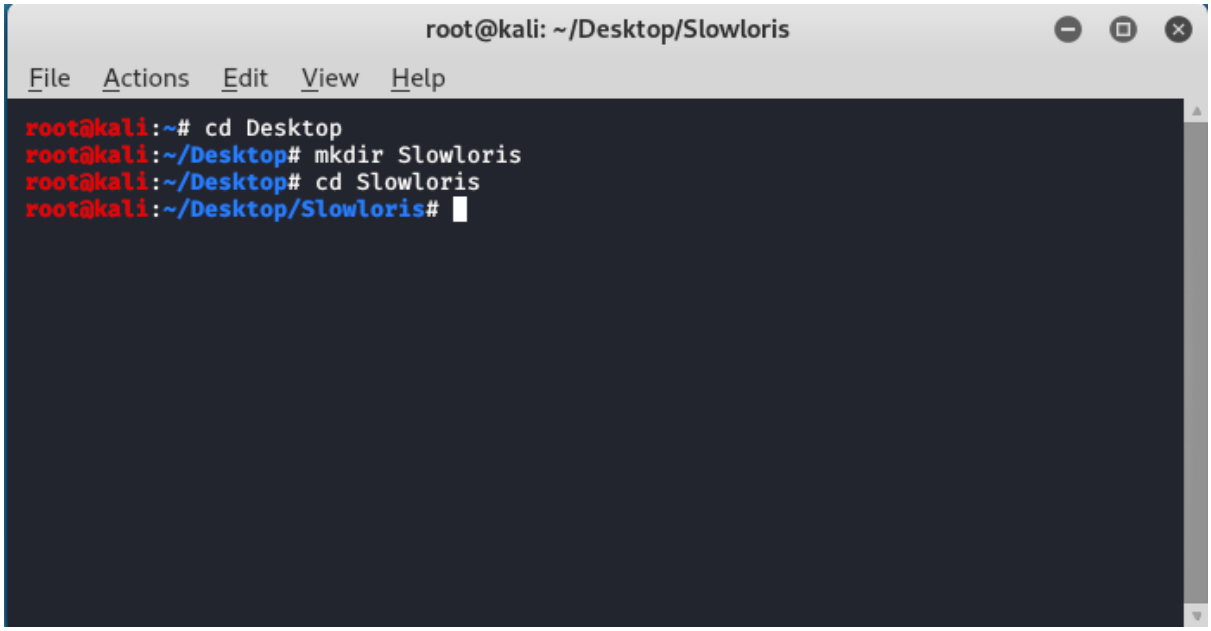
Step:-1 Open your Kali Linux and then Open your Terminal.

Step:-2 Create a new Directory on Desktop named Slowloris using the following command.

mkdir Slowloris

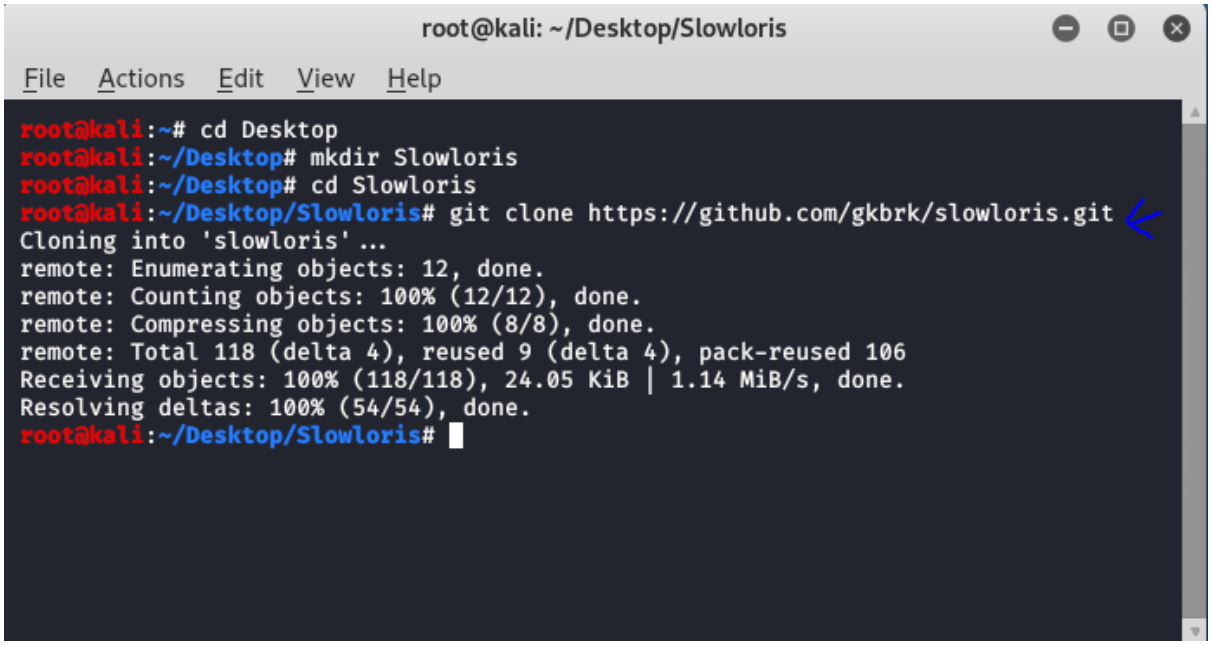
Step:-3 Move to the directory that you have to create (Slowloris).

cd Slowloris



Step:-4 Now you have to clone the Slowloris tool from Github so that you can install it on your Kali Linux machine. For that, you only have to type the following URL in your terminal within the Slowloris directory that you have created.

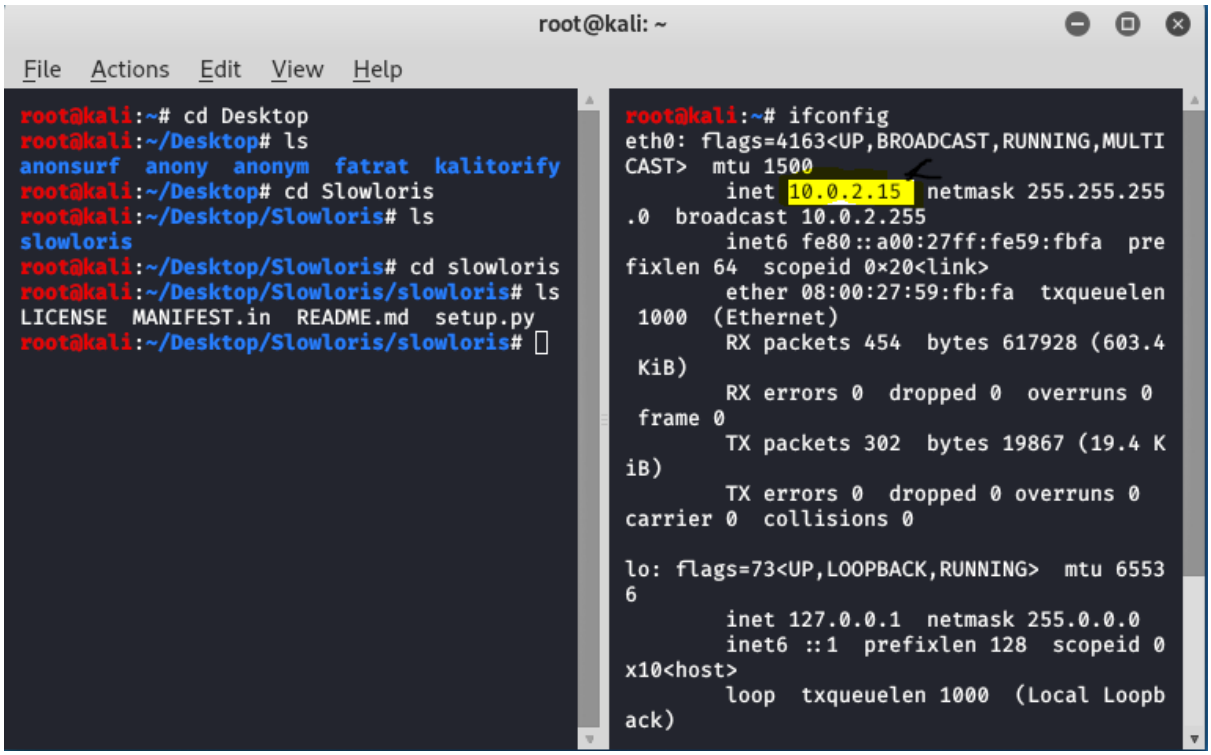
git clone https://github.com/gkbrk/slowloris.git



Step:-5 Now go to the Action bar and click on split terminal vertically then you will see that the two-terminal screen has been opened now.

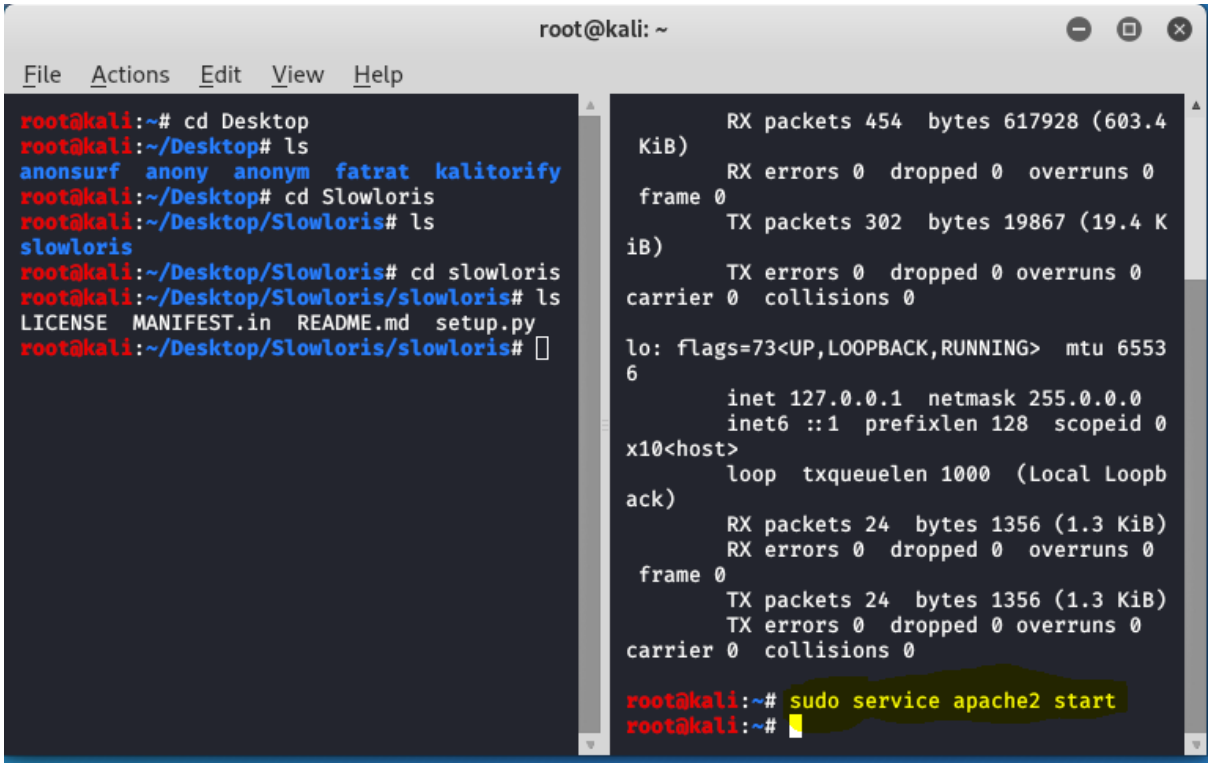
Step:-6 Now you have to check the IP address of your machine to do that type following command.

Ifconfig



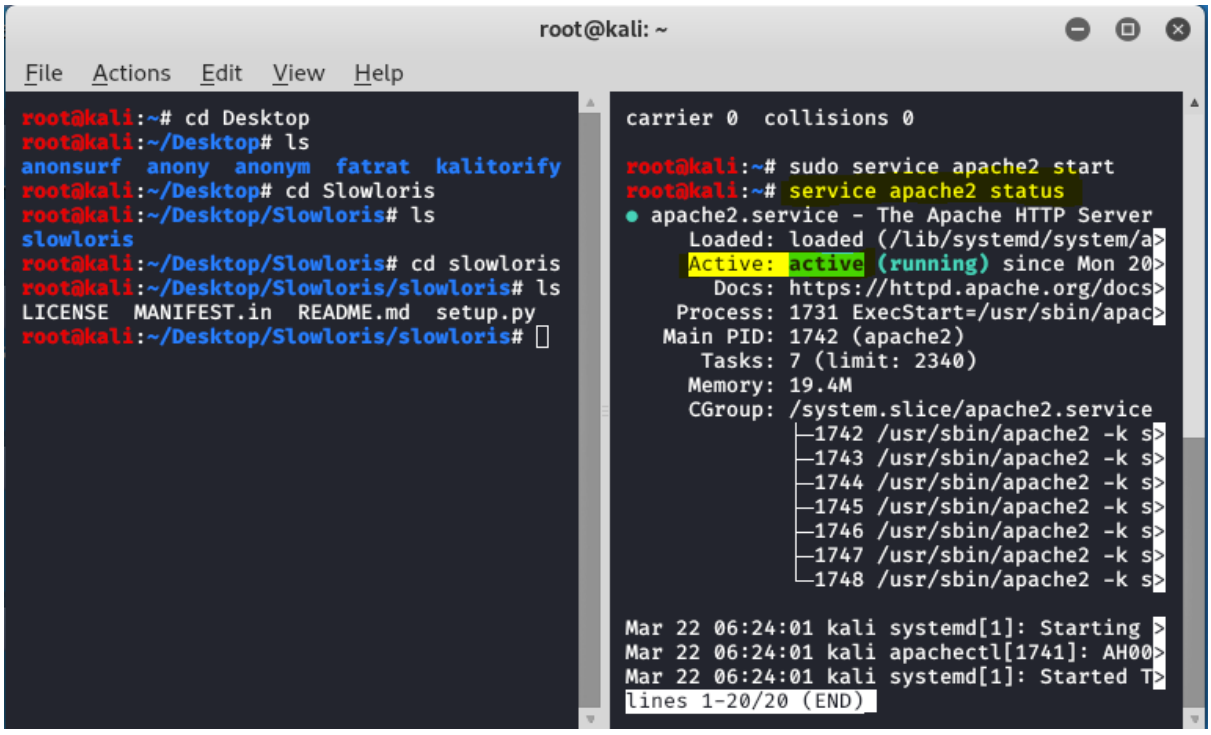
Step:-7 As you can see we got our IP address now it's time to start the apache server, to start the apache server using the following command.

sudo service apache 2 start



Step:-8 Now we have to check the status of your server whether it is active or not so to check the status of your server run the following command.

service apache2 status



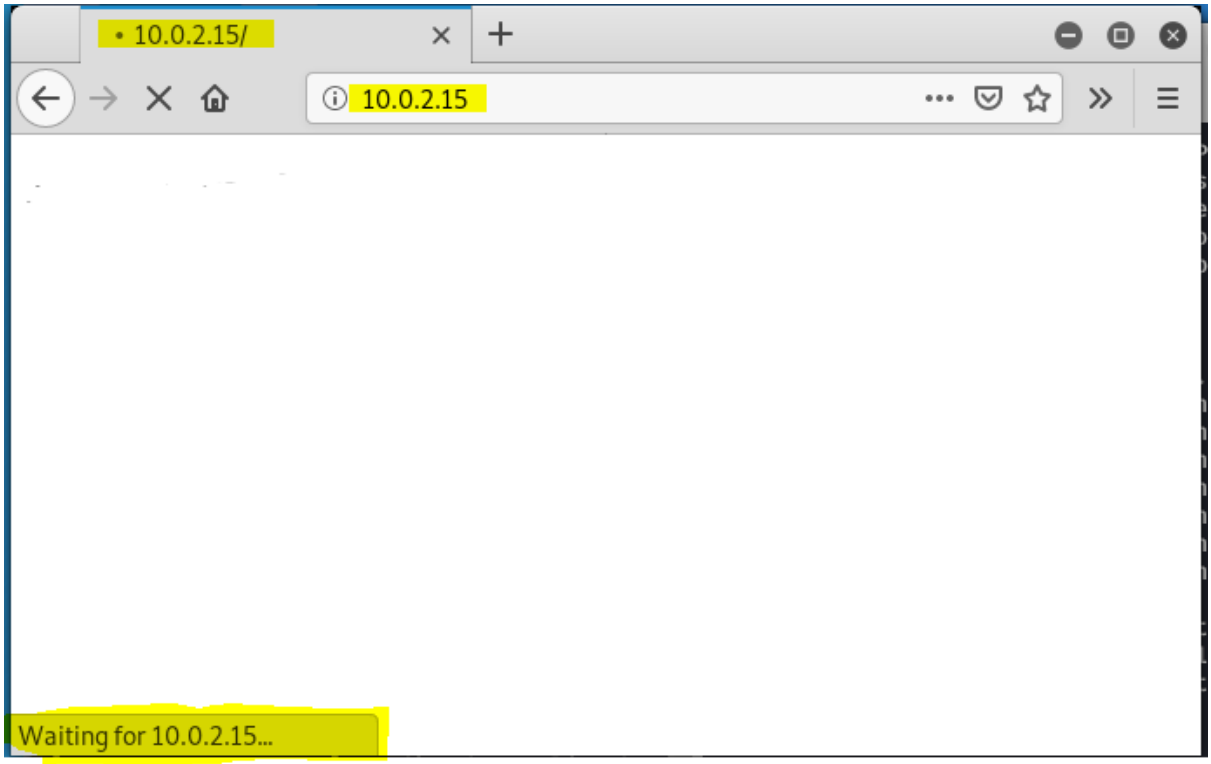
Step:-9 We can see that our server is under active status. It means it is running properly, now comes back to the first terminal, and to check permissions run the following command.

Ls –l

Step:-10 Now it's time to run the tool using the following command.

python3 slowloris .py (your ip address) -s 500

Step:-11 You can see the tool has started attacking on that particular IP address which we have given now to check whether its working or not go to your browser and on your URL bar type that IP address, and you will see the site is only loading and loading but not opening this is how Slowloris tool works.



Sign: _____

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
1	Which of the following is considered an element of cyber security?	Network security	Operational security	Application security	All of the Mentioned
2	Which of these is NOT involved in the CIA Triad?	Confidentiality	Availability	Integrity	Authenticity
3	Identify the first computer virus among the following.	Blaster	Creeper	Sasser	Trojan
4	Which one of the following can be considered as the class of computer threats?	Dos Attack	Phishing	Soliciting	Both A and C
5	Which of the below benefits of cyber security is not true?	System getting slower	Computer lagging and crashes	provide privacy to users	Secures system against viruses
6	Which of the following is considered an element of cyber security?	Network security	Operational security	Application security	All of the Mentioned
7	Part of the social media sites are the various games & 3rd party applications which helps _____ to get access to your data.	Ethical hackers	Penetration testers	Security auditors	Cyber-criminals
8	Which of the following is FALSE about the type of SQL Injection attack?	Install malicious program	Export valuable data	Get user login detail	None of the Mentioned
9	Full form of TCP/IP?	Transmission Control Protocol/ Internet Protocol	Transmission Control Product/ Internet Protocol	Transaction Control Protocol/ Information Protocol	Transport Contribution Protocol/ Internet Performance

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
10	Basically Trojan does_____	Only steal data	Control computer, stealing data and inserting more malware	Insert Malware	None of the Mentioned
11	Direct user to dodgy website is an exmple of ___	Protocol	Trojan	Phishing	Trojan Horse
12	What is/are the Email related frauds?	Email Spoofing	Email Spamming	Email Bombing	All of the Mentioned
13	Choose the default port number for Apache and other web servers.	80	20	27	87
14	What is the full form of DoS in Cyber Security?	Dark-of-Service	Distributed-of-Service	Denial-of-Service	Danger -of-Services
15	In which of the following Email Attack, millions of Eamil send to victim?	Email Spoofing	Email Spamming	Email Bombing	All of the Mentioned
16	What is the CIA triad also known as?	AIC(Availability, Integrity, Confidentiality)	NIC(Non-repudiation, Integrity, Confidentiality)	AIN(Availability, Integrity, Non-repudiation)	ANC(Availability, Non-repudiation, Confidentiality)
17	What is full form of NIC in Cyber Security?	Non-repudiation, Information, Confidentiality	Non-repudiation, Integrity, Confidentiality	Non-repudiation, Integrity, Concern	Non-report, Integrity, Confidentiality
18	What is full form of AIN in Cyber Security?	Availability, Information, Non-repudiation	Availability, Integrity, Non-report	Availability, Integrity, Non-repudiation	Average, Integrity, Non-repudiation
19	What is Cyber Security?	Cyber Security provides security against cyber-terrorists	Cyber Security protects a system from cyber attacks	Cyber Security provides security against malware	All of the Mentioned
20	What is full form of ANC in Cyber Security?	Availability, Non-repudiation, Confidentiality	Average, Non-repudiation, Confidentiality	Availability, Non-research, Confidentiality	Availability, Non-repudiation, circle

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
21	_____is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.	Cyber secrecy	Cyber security	Cyber scrutiny	Cyber policy
22	_____ is the protection of Internet-connected systems, including hardware, software and data from cyber attacks.	Cyber secrecy	Cyber security	Cyber scrutiny	Cyber policy
23	______is a world-wide network of computer networks that uses the TCP/IP for communication to facilitate transmission and exchange of data	Cyberinternet	Cyberposition	Cyberspace	Cyberconnection
24	Which of the following act violates cyber security?	Exploit	Attack	Threat	Vulnerability
25	A crime conducted in which a computer was directly and significantly instrumental is known as_____	Device Crime	Direct Crime	Calculator Crime	Computer Crime

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
26	The information and data should not be corrupted or edited by a third party without authorization is known as _____	Integrity	Watermarking	Confidentiality	None of the Mentioned
27	_____can be defined as the critical means by which the direction described in an enterprise's cybersecurity strategy and policies are translated into actionable and measurable criteria.	Cybersecurity	Cybersecurity standards	Cyberspace	Cybersecurity policies
28	What is full form of IDS in Cyber Security?	Internet detection systems	Information detection systems	Intellectual detection systems	Intrusion detection systems
29	What is the existence of weakness in a system or network is known as?	Attack	Exploit	Vulnerability	Threat
30	What is full form of CIA in Cyber Security?	Center, Integrity, and Availability	Confidentiality, Integrity, and Average	Confidentiality, Information, and Availability	Confidentiality, Integrity, and Availability
31	Firewall, IDS and VPN are examples of _____ security	Personal	Network	Software	None of the Mentioned
32	What is full form of VPNs in Cyber Security?	Virtual public networks	Virtual private networks	Voic private networks	Virtual policy networks

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
33	_____ is a popular tool used for discovering networks as well as in security auditing.	Ettercap	Metasploit	Nmap	Burp Suit
34	Secure coding practices, regular software updates and patches, and application-level firewalls are examples of _____ security	Personal	Network	Application	None of the Mentioned
35	Encryption, Access controls, Data classification, and Data loss prevention (DLP) measures are examples of _____ security	Information	Network	Information or Data	None of the Mentioned
36	Which of this Nmap do not check?	Services different hosts are offering	On what OS they are running	What kind of firewall is in use	What type of antivirus is in use
37	_____is a way to scramble data so that only authorized parties can unscramble it	Encryption	Watermarking	Sampling	None of the Mentioned
38	_____ is the process of converting an encrypted message back to its original (readable) format	Encryption	Decryption	Sampling	None of the Mentioned
39	Identify the legal form of hacking.	Cracking	Non-ethical hacking	Ethical hacking	Hacktivism
40	____ is an algorithm for performing encryption or decryption.	sampling	conversion	manuscript	cipher

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
41	The process of verifying a claimed identity of a user, device, or other entity in a computer system is known as _____	Authentication	Authorization	Right	None of the Mentioned
42	Malware stands for?	Multipurpose software	Malfunctioned software	Malicious software	Malfunctioning of security
43	_____ is a process by which a computer system/device determines if the client has permission to use a resource or access a file	Authentication	Authorization	Right	None of the Mentioned
44	_____ are examples of cloud service providers.	AWS	Azure	Google Cloud	All of the Mentioned
45	Which of the following is considered as the unsolicited commercial email?	Virus	Spam	Malware	Inbox
46	Spam is an email which is generally_____	Solicited	Authorized	Unsolicited	All of the Mentioned
47	In a bot attack, a bot is generally_____	Solicited user	Authorized user	Fake user	All of the Mentioned
48	Which of the following malware types does not clone or replicate itself through infection?	Viruses	Worms	Trojans	Rootkits
49	____ attacks are the practice of sending fraudulent communications that appear to come from a reputable source	Phishing	Spamming	Spoofing	Bombing

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
50	____is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database	SQL object (SQLo)	SQL injection (SQLi)	SQL attack (SQLa)	SQL query (SQLq)
51	Which one of the following refers to the technique used for verifying the integrity of the message?	Digital signature	Message Digest	Protocol	Decryption algorithm
52	Which of the following technical aspect is not recommended for online payment/money transfer transaction?	Private Network	Private Computer	Public Wi-Fi	All of the Mentioned
53	Authorization is done ___ the authentication process	before	after	parellel	None of the Mentioned
54	Which of the following is the type of SQL Injection attack?	It inserts the data	It updates the data	It deletes the data	All of the Mentioned
55	Authentication is done ___ the authorization process	before	after	parellel	None of the Mentioned
56	In the ____ process, the identity of users is checked for providing access to the system	Authentication	Authorization	Right	None of the Mentioned

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
57	Select the correct statement which will return all the rows from the Table and then also deletes the Table_Add table?	SELECT * FROM Table; DROP TABLE Table_Add	SELECT * WHERE Table; REMOVE TABLE Table_Add	SELECT * FROM Table; DELETE TABLE Table_Add	SELECT * WHERE Table; DELETE TABLE Table_Add
58	How to drop table from database?	Remove TABLE TableName	DROP TABLE TableName	Delete TABLE TableName	DROP TableName
59	_____is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed	SQL Vector	SQL Code	SQL inquiry	SQL injection
60	Through which system, we can detect SQL Injection attacks?	Injection Detection System	Attack Detection System	Intrusion Detection System	None of the Mentioned
61	Which of the following type of password is recommended for high security?	weak password	strong password	public password	normal password
62	While using, third party paymnet method which of the following needs to check for the security?	Digital certificate	Public certificate	Network certificate	None of the Mentioned
63	What is the full form of DDoS in Cyber Security?	Distributed Danger-of-Service	Denial Distributed-of-Service	Distributed Denial-of-Service	Danger Denial-of-Services
64	Which of the following process usually needs the user's privileges/rights?	Authorization	web surfing	web browsing	None of the Mentioned

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
65	How can we prevent SQL Injection attack?	We should pre-define the input type, input field and length of the user data to validate the input for the user authentication.	Access privileges should be restricted for the users	Administrator accounts should not be used.	All of the Mentioned
66	Which of the following process usually needs the user's login details?	Authentication	web surfing	web browsing	None of the Mentioned
67	_____area units are utilized in respect of knowledge security that permits the safety of an automatic data system	SingUp and Authorization	Authentication and Login	Authentication and Authorization	Login and LogOut
68	Which of the following is TRUE about the type of SQL Injection attack?	Install malicious program	Export valuable data	Get user login detail	All of the Mentioned
69	The encryption can be represented using _____ by first transforming the letters into numbers	number arithmetic	modular arithmetic	modern arithmetic	main arithmetic
70	Why is encryption important?	Privacy	Security	Data integrity	All of the Mentioned
71	Asymmetric encryption uses a _____ key for the encryption and decryption process	Any	Null	Same	Different
72	In symmetric encryption the ____ key is used for encryption and decryption.	Any	Null	Same	Different

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
73	What defense will best help stop Cross Site Scripting (XSS)?	Input Validation	Output Encoding	Cryptographic Tokens	Rate Throttling
74	What is full form of XSS in Cyber Security?	Cross Site Scripting	Cross Stamp Scripting	Cross Site Sampling	Common Site Scripting
75	In which of the following attack, the attacker uses a single internet connection to barrage a target with fake requests or to try and exploit a cybersecurity vulnerability?	Phising attack	Spamming attack	Data attack	DoS attack
76	How many Layers are there is OSI Model?	5	7	8	9
77	A Web site that allows users to enter text, such as a comment or a name, and then stores it and later display it to other users, is potentially vulnerable to a kind of attack called a _____ attack.	Two-factor authentication	Cross-site request forgery	Cross-site scripting	Cross-site scoring scripting
78	What is full form of OSI?	Open Systems Interconnection	Open Systems Interface	Open Systems Internet	Open Systems Information
79	Which of the following attack aims to control all available bandwidth between the victim and the larger internet?	Protocol-Based attack	Application-Based attack	Volume-Based attack	Volue-Based attack

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
80	A SYN flood is an example of a _____ attack	server	client	data	protocol
81	Many applications use _____ where two independent factors are used to identify a user.	Two-factor authentication	Cross-site request forgery	Cross-site scripting	Cross-site scoring scripting
82	In which type of attack the excessive number of HTTP requests overwhelms the server?	Data-layer attack	Application-layer attack	Transport-layer attack	Network-layer attack
83	___attack targets the layer where web pages are generated in response to Hypertext Transfer Protocol (HTTP) requests	Data-layer	Application-layer	Transport-layer	Network-layer
84	__ is a computer crime in which a criminal breaks into a computer system for exploring details of information etc.	Spoofing	Eavesdropping	Hacking	Phishing
85	"Keep all software and systems up to date" is one of the way to protect our computer system from____	One-day vulnerability	Zero-day vulnerability	All-day vulnerability	Same-day vulnerability
86	In ethical hacking and cyber security, there are _____ types of scanning:	1	2	3	4

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
87	____is a software vulnerability discovered by attackers before the vendor has become aware of it	One-day vulnerability	Zero-day vulnerability	All-day vulnerability	Same-day vulnerability
88	Which of the following is one of the way to avoid CSRF attack?	Secret cookie	accept exe	allow permission	All of the Mentioned
89	___is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated	CSRR	CSRF	CSFF	CRPF
90	Which of the following are the types of scanning?	Port, network, and services	Client, Server, and network	Network, vulnerability, and port scanning	None of the above
91	Full form of CVV?	Card Version Value	Cash Verification Value	Card Verification Value	Cash Version Value
92	What is full form OTP?	One Terminal Password	One Time Password	One Time Passport	One Terminal Passport
93	Which of the following details can be shared over phone whenever you receive calls stating from banks or any other support team?	PIN/Password	OTP (One Time Password)	CVV Number	None of the Mentioned
94	What is/are main application(s) of cyber security?	Network security	Software security	Risk Management	All of the Mentioned
95	In which of the following attack many attackers attack on victim?	Trojan	DoS	DDoS	Trojan Horse

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
96	Which of the following was the first technical report for Computer Control & Security in 1970?	Secure Report	Ware Report	Virus Report	Hard Report
97	_____is a type of cyber security attack that occur on the same day the software, hardware or firmware flaw is detected by the manufacturer	Zero-day exploit	All-day exploit	Some-day exploit	Same-day exploit
98	What is full form of CSRF in Cyber Security?	Cross-Site Request Fragmentation	Common-Site Request Forgery	Cross-Site Request Forgery	Cross-Site Research Forgery
99	_____is the process of superimposing a logo or piece of text atop a document or image file.	Cryptography	Watermarking	Secrecy	Methodology
100	The science of encrypting and decrypting information is called_____	Cryptography	Watermarking	Secrecy	Methodology
101	What is transformed using cipher algorithms?	Scalar text	Complex text	Plain text	None of the Mentioned
102	Identify the type of symmetric key algorithm which uses a streaming cipher to encrypt information.	SHA	MD5	RC4	Blowfish

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
103	A _____ can be a hardware device or a software program that filters all the packets of data that comes through a network, the internet, etc.	Firewall	Antivirus	Malware	Cookies
104	_____ is a type of software designed to help the user's computer detect viruses and avoid them.	Malware	Adware	Antivirus	Adware and Antivirus
105	Which one of the following is a type of antivirus program?	Quick heal	Mcafee	Kaspersky	All of the Mentioned
106	To protect the computer system against the hacker and different kind of viruses, one must always keep _____ on in the computer system.	Antivirus	Firewall	Vlc player	Script
107	The encryption techniques are primarily used for improving the _____	Performance	Reliability	Longevity	Security
108	Which of the following statements is correct about the firewall?	It is a device installed at the boundary of a company to prevent unauthorized physical access.	It is a device installed at the boundary of an incorporate to protect it against the unauthorized access.	It is a kind of wall built to prevent files form damaging the corporate.	None of the Mentioned
109	In order to ensure the security of the data/ information, we need to _____ the data:	Encrypt	Decrypt	Delete	None of the Mentioned

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
110	How many types of firewalls.?	5	4	3	2
111	Which of the following is not a type of firewall?	Host-based Firewalls	Network-based Firewalls	Packet Filtering Firewall	Dual Host Firewall
112	Network layer firewall has two sub-categories as _____	Network & session layer firewall	State full firewall and stateless firewall	Bit & byte-oriented firewall	Frame firewall and packet firewall
113	Which of the following is the type of SQL Injection attack?	It inserts the data	It updates the data	It deletes the data	All of the Mentioned
114	Which of the following three is the strongest password?	starwars	1qaz2wsx	abc123	Bee@123*
115	What are the characteristics of a strong password?	Long	Long, unique	Long, random	Long, random and unique
116	Your business email account has been compromised and leaked in a data breach. What is the best course of action(s)?	Change your password immediately	Inform the security team of your organization	Change the Password on all sites where you use the same password	All of the above
117	If you receive a suspicious email, should you?	Reply to it	Open the attachments	Click the links	Report it to the phishing reporting mailbox of your government
118	Which month is considered or recognized as Cyber Security Month?	September	October	November	December
119	Which will not harm computer resources?	Firewall	Virus	Trojan horse	None of the Mentioned
120	What does SSL stand for?	Saving Sharing and Limits	Secure Socket Limbs	Safe, Secured and Locked	Secure Socket Layers

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
121	_____ gets propagated through networks and technologies like SMS, Bluetooth, wireless medium, USBs and infrared to affect mobile phones.	Worms	Antivirus	Malware	Multimedia files
122	Activate _____ when you're required it to use, otherwise turn it off for security purpose.	Flash Light	Bluetooth	App updates	Rotation
123	_____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.	Information Security	Network Security	Database Security	Physical Security
124	_____ technology is used for analyzing and monitoring traffic in network and information flow.	Managed detection and response (MDR)	Cloud access security brokers (CASBs)	Network traffic analysis (NTA)	Network Security Firewall
125	Possible threat to any information cannot be _____	reduced	protected	transferred	ignored
126	Which of the following is not a type of hacking any smart-phone.	Target mobile hardware vulnerabilities	Target apps' vulnerabilities	Snatching	Setup Keyloggers
127	Mobile security is also known as?	OS Security	APIs Security	Wireless Security	Database security

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
128	Which of the following is the most viral section of the internet?	Chat Messenger	Social networking sites	Tutorial sites	Chat-rooms
129	Increase your security for social media account by always _____ as you step away from the system.	Signing in	Logging out	Signing up	Logging in
130	Part of the social media sites are the various games & 3rd party applications which helps _____ to get access to your data.	Ethical hackers	Penetration testers	Security auditors	Cyber-criminals
131	You have received an email purportedly from Flipkart regarding a discount offer for a product with a link provided. What should you do about it?	Verify the display name of the sender and proceed to click on the link if it looks genuine	Click on the link immediately so that you do not miss out on the opportunity	Go directly to Flipkart website and look for the offer there	Verify the email id of the sender and proceed to click on the link if it looks genuine
132	It's okay to share passwords with:	Your Teacher	Your Friend	Your Principal	None of the Mentioned
133	Which of the following details can be shared over phone whenever you receive calls stating from banks or any other support team?	Account number	OTP (One Time Password)	CVV Number	All of the Mentioned
134	If you are an Android user, which of these sources are safe to install apps / games?	UC Browser	Google Play store	ShareIT	All of the Mentioned

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
135	_____ helps to keep your social media accounts safe and secure.	Enabling two factor authentication	Using strong password	Using unique password	All of the Mentioned
136	Which among the below is not a correct example of multi-factor authentication?	Entering PIN for a card transaction while withdrawing money at ATM	Password + SMS OTP	Password + PIN	Password + Face recognition
137	What type of malware disguises itself as legitimate software?	Virus	Worm	Trojan	Spyware
138	Which cybersecurity practice involves restricting access to authorized users only?	Encryption	Authentication	Firewall	Authorization
139	What is the primary purpose of a firewall in network security?	To encrypt data	To detect malware	To prevent unauthorized access	To monitor network traffic
140	Which of the following is an example of a strong password?	12345	Password123	Tr0ub@Dor!	Username
141	Which protocol is commonly used for secure communication over the internet?	HTTPS	FTP	SMTP	HTTP
142	What does “Phishing” typically involve?	Stealing physical documents	Social engineering to manipulate people	Hacking into computer systems	Encrypting data
143	Which cybersecurity principle involves keeping software and systems up to date with security patches?	Least Privilege	Vulnerability Scanning	Patch Management	Data Backup
144	What is the purpose of two-factor authentication (2FA)?	To use two different passwords	To provide a second layer of security	To simplify login procedures	To prevent login entirely

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
145	Which type of attack involves overwhelming a system with excessive traffic to make it unavailable?	Ransomware	Phishing	DoS (Denial of Service)	SQL Injection
146	What does “VPN” stand for in the context of cybersecurity?	Virtual Personal Network	Very Private Network	Virtual Public Network	Virtual Private Network
147	Which of the following is NOT a common encryption algorithm?	AES	SSL	RSA	DES
148	What is the term for the practice of enticing employees to reveal sensitive information?	Hacking	Insider Threat	Social Engineering	Encryption
149	What is the purpose of a penetration test in cybersecurity?	To develop new software	To detect vulnerabilities in a system	To encrypt data	To monitor network traffic
150	Which organization develops and maintains international standards for information security?	ISO (International Organization for Standardization)	FBI (Federal Bureau of Investigation)	CIA (Central Intelligence Agency)	NSA (National Security Agency)
151	What is the term for a program or device that captures and records keystrokes on a computer without the user's knowledge?	Firewall	Phishing	Keylogger	Ransomware
152	Which of the following best describes the principle of "Zero Trust" in cybersecurity?	Trust all users and devices by default	Verify and trust no one and nothing by default	Trust only external users and devices	Trust only internal users and devices
153	What is the primary purpose of a CAPTCHA in online security?	To prevent unauthorized access to a website	To verify that a user is human and not a bot	To encrypt user data	To generate strong passwords

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
154	Which cybersecurity concept involves making data unreadable without the proper decryption key?	Authentication	Encryption	Authorization	Intrusion Detection
155	What is the primary goal of a "honeypot" in cybersecurity?	To store sensitive data	To attract and monitor malicious activity	To provide encryption services	To prevent network traffic
156	Which security measure involves regularly copying and storing data to ensure it can be recovered in case of data loss or a cyber attack?	Data encryption	Data masking	Data backup	Data deduplication
157	What type of cyber attack involves intercepting communication between two parties and potentially altering the data being exchanged?	Ransomware	Phishing	Man-in-the-Middle (MitM)	DoS (Denial of Service)
158	Which of the following is a common method to protect against email-based phishing attacks?	Strong passwords	Multi-factor authentication (MFA)	Firewall configuration	Email filtering and awareness training
159	Which of the following is an example of a biometric authentication method?	PIN code	Password	Fingerprint scan	Security token

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
160	What is the primary purpose of a firewall in a network security system?	To prevent all incoming and outgoing network traffic	To monitor and control network traffic based on a set of rules	To encrypt all data transmitted over the network	To speed up network performance
161	Which type of firewall operates at the application layer of the OSI model and is capable of understanding specific applications and protocols?	Packet-filtering firewall	Stateful firewall	Proxy firewall	Intrusion Detection System (IDS)
162	What is the purpose of a hardware firewall?	To protect a specific device or computer	To secure an entire network or group of devices	To filter spam emails	To encrypt data during transmission
163	What is the main drawback of a firewall that uses a default "allow all" policy for network traffic?	It can slow down network performance.	It can lead to unauthorized access and security breaches.	It requires constant monitoring and configuration.	It is not compatible with modern networking protocols.
164	Which of the following firewall types is commonly used to protect individual devices or workstations?	Host-based firewall	Cloud-based firewall	Perimeter firewall	Deep packet inspection (DPI) firewall
165	What is the primary concern when it comes to personal devices and cybersecurity?	Hardware compatibility	Data storage capacity	Security and privacy	Battery life
166	Which of the following is NOT a common personal device that poses security risks?	Smartphone	Smart refrigerator	Laptop	Smartwatch

INFORMATION PROTECTION USING CYBER SECURITY (LEVEL-1): Suggested MCQ Question Bank					
Sr.No.	**Question**	**Option1**	**Option2**	**Option3**	**Option4**
167	Which security feature is essential to protect data on a lost or stolen personal device?	GPS tracking	Voice recognition	Biometric authentication	Screen resolution
168	When sharing personal information on social media, what should you consider to enhance your cybersecurity?	Using the same password for all accounts	Accepting friend requests from unknown profiles	Sharing personal details openly	Adjusting privacy settings
169	Which of the following actions is a potential red flag for social media account security?	Enabling two-factor authentication	Sharing sensitive information in private messages	Using strong, unique passwords	Clicking on suspicious links or attachments