17. Encrypt your files

The thought of a hacker getting inside your networks is a major cause for alarm. Imagine, however, their surprise when all they find is a bunch of gibberish? Encryption can protect sensitive data on Windows or macOS using software specifically designed to mask your IP address. You can identify whether a website has been secured using encryption by looking for "https" in the address bar along with a padlock icon.

18. Secure personal devices

Employees increasingly use their smartphones and other personal devices to access information at work. Consider implementing a policy for using personal devices to ensure individuals are following security protocols. Some quick tips for securing both personal information and sensitive work data include turning off your Bluetooth, never using unsecured public Wi-Fi, and following the same advice for complex personal device passcodes as you would for your work computer systems.

19. Ask for Help

When you're managing your IT internally, the pressure is on to make sure you're adequately protected against hacking and viruses. While having all these measures in place and ensuring employees are following best practices, it's still difficult to keep up with the latest cyber threats. It only takes one employee to forget to change default settings or to click on what seemed an innocent link from someone they thought they knew.

Possibly the best way to overcome these challenges is to enlist the help of a **Managed IT** provider that stays up on the latest threats and whose job it is to make your systems as secure as possible. When you work with a Managed IT provider, you get laser-focused monitoring and attention, 24/7/365.

Their expertise is in ensuring maximum system and computer uptime, making sure all of your system's latest updates are installed, and even providing resources to educate your employees. They can help you with day-to-day issues and be there to tackle questions and ensure they're addressed quickly and resolved accurately.

1.6 Security Review of Protocols

Computer network technology is developing rapidly. A computer network, or simply a network, is a collection of connected computing devices to share information and/or recourses. Network security is a main issue in computing because different kinds of attacks are increasing daily. With the development and popularization of Internet application technology, network security needs to be paid more and more attention.

Network security covers all phases associated with the security of the sensitive information resources present on the network. It deals with all the measures to protect data throughout their transmission. The specific goals of network security are confidentiality, integrity and availability. To formalize and maintain the secure and well-organized network, abundant research has been devoted to offer a sophisticated methodology for data communication. The TCP/IP model is not same as the **OSI model,** which is a seven-layered standard, whereas TCP/IP is a four-layered standard. The model has been influential in the growth and development of TCP/IP standard, and that is why much of OSI terminology is applied to TCP/IP. The TCP/IP reference model that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

One formal system that has been present as a conceptual model is the TCP/IP protocol suite that was formed in 1980 as an internetworking solution with only slight concern for protection aspects. That is the reason that serious security faults are in the TCP/IP protocol, despite its implementation. TCP/IP model is divided into four layers and each layer works using a variety of protocols with specific functions. The lower protocols have flaws with open possibilities for attacks on the security of data exchange.

1.6.1 Strengthening the Different Layers of IT Networks

The *Open Systems Interconnection* **(OSI)** model was developed in 1983 by the *International Organization for Standardization* **(ISO).** Ever since then, it has been the go-to model for understanding and analyzing how networks function. Its influence has been so great that the majority of **communications protocols** in use today are structured around it.

Nonetheless, the OSI model was born from a theoretical perspective, and despite its precision in encapsulating how a network functions, it ended up relinquishing the practical ground to new designs built on top of it, such as **TCP/IP -** the most commonly used model today. More than a model, it is a stack or **suite of protocols** used simultaneously, which allows the network to function.

OSI	TCP/IP
Application	Application
Presentation	
Session	
Transport	Transport
Network	Network
Data link	Network Host
Physical	

Fig. 1.6.1 OSI and TCP/IP reference model

As well as helping in the development of telecommunications protocols, this can be used as a basis for understanding how we can apply security strategies right across the length and breadth of an IT network's structure. In the same way that the failure of one of these layers to provide its respective services results in the layers above it not being able to successfully fulfill its objectives, a vulnerability that compromises any layer renders useless any other protection measure that has been implemented in the layers of abstraction above it.

We can make a comparison between network security layers and the layers of an onion: it's a question of implementing measures to compensate for weak points throughout **all the layers,** making sure to correctly configure the protocols in the protocol stack used, on **all the mechanisms** involved in the network. For purposes of analysis, we will put together a new reference model combining the characteristics of the OSI model and the TCP/IP stack, as shown below.

1) Physical layer

This deals with sending bits via analog and digital signals through various means of communication. In this layer, we find protocols like ethernet, PPP and frame relay, among others.

From an IT security perspective, at this level we are concerned with preventing unauthorized **third parties** from getting into the system. Measures include implementing a warning and surveillance system and arranging barriers and mechanisms to **control access to the system** on which the IT network is deployed.

Another risk to keep in mind is the **"internal threat,"** in other words, authenticated staff carrying out unauthorized actions, or pursuing a harmful goal. The arrangement of cables must not allow **eavesdropping** and to achieve this it is necessary to restrict access

to the telecommunications room and protect the cabling and equipment so they cannot be deliberately damaged for the purpose of **attacking the availability** of the service.

2) Data Link Layer (DLL)

This deals with addressing at the level of ***frames,*** acting as a link between the network layer (packets with IP addresses) and the physical layer (signals). ***Switches*** are the most important mechanism at this level, and as such, data link security focuses on the correct configuration of these devices. For example, we have to combine the blocking of physical access with **deactivation at the logic level** of unused ports, in order to prevent fraudulent connections which could lead to eavesdropping, flooding attacks, or ARP spoofing.

This layer also includes the correct choice of **secure protocols** for communication. For example, in the case of **wireless,** we should use the WPA2 or WPA protocol whenever possible, in preference to WEP.

Another important element of this instance is the correct configuration of **virtual networks.** A VLAN is a local area network that, although it has all the attributes of a network at the logic level, does not exist as such on a physical level, but rather is created through the individual indication of identifiers on frames flowing through the network.

VLANs play a critical role in the system's security, contributing to **segmentation** of the network and **separation of traffic,** allowing it to be better organized and quickly analyzed.

3) Network layer

This deals with the routing of packets between networks, connecting different broadcasting domains. The addressing model used at this level is that of **IP addresses,** and the mechanism that centralizes traffic management is the ***router.***

Activating the various security characteristics included in this equipment is important for preventing **unauthorized control** of it. Use of **strong passwords** and correct configuration of management protocols through **encrypted connections** are some of the measures that can be taken to protect this equipment.

Additionally, we have to keep in mind **vulnerabilities** that could exist in routing protocols, such as RIP and OSPF, as they could lead to the injection of false *routers.* Understanding these protocols will facilitate secure management of the network.

The **IPv4** protocol does not include security mechanisms to protect communications, so the network administrator must consider other additional measures for protecting data. For example, they can choose to encrypt all network packets, or exchange a session key to protect the connection.

For this reason, we should consider implementing **IPSec** : the suite of protocols responsible for providing security features to the IP protocol, serving for the use of **Virtual Private Networks,** or VPNs. Its optional use of IPv4 will become obligatory for IPv6. It supports two modes of implementation

- **Transport mode,** whereby the ends of the communication protect it by encrypting only the packet's payload
- **Tunnel mode,** used for secure connection between networks, where each IP packet is encrypted and encapsulated within another

In addition, there is a series of other problems that affect this layer. In particular, the possibility of an attacker trying to send data from equipment with a certain IP address when in reality they are doing so from another address - a process called **IP *spoofing.*** One way to minimize such attacks is to include authentication processes in the application layer, together with data encryption mechanisms.

Likewise, **activating *firewalls*** on the network layer can reduce such attacks, as these devices can delineate the inside of the network from the outside, making its internal/external ports correspond with the assigned address space. That is, a *firewall* can detect a packet that claims to come from inside, but in fact came in through the external port, and can therefore **reject** it or generate the corresponding **warning.**

Another key component of IT security at the network layer is the *Access Control List.* This allows or refuses connections with equipment belonging to other networks, depending on the protocol, ports, or IP addresses involved in the communication.

Correctly configuring ACLs is a task of considerable magnitude, as it requires knowledge of the protocols that will be used on the network, and knowledge of the network's design. Any incorrect configuration could lead to authorizing **fraudulent traffic** or refusing legitimate connections.

4) Transport layer

This takes data from the application and splits it into **segments** which will then be sent to the network layer. The preferred protocols at this level are TCP and UDP, which are responsible for establishing a real link from origin to destination. As such, the addressing model is the port number.

The security concerns at this level relate to **encryption** of the data transferred, authentication of the parties involved, prevention of tampering with data integrity, and avoidance of **replay attacks.**

With regard to TCP, one of the best-known types of attacks is the **SYN attack.** This takes advantage of some of the weaknesses in the three-channel model for establishing a connection. It involves malicious equipment sending multiple SYN requests to another terminal, and then stopping responding. The destination host will await confirmation, keeping the attempted connection on hold. If the maximum number of threads of **unconfirmed connections** that the host can support is exceeded, the host will be rendered **unable** to accept new communications, resulting in a denial of service.

One **solution** to this problem is to increase the number of unconfirmed connections on the server, or to decrease the amount of time the server will wait for confirmation (75 seconds by default).

The use of **layer 4 secure communication protocols,** such as SSL, TLS or SSH, enables data to be protected by encrypting it, and should be considered when setting up connections for remote management of devices.

Finally, as the connection is end-to-end in the transport layer, increasing **protection at the terminals** is the first step for preventing fraudulent connections. Updating your applications in order to protect the network from any vulnerabilities and errors that might arise is the very first measure for reinforcing your equipment.

5) Application layer

The application layer in the TCP/IP stack, and its equivalent layers in the OSI model, deals with session management and applications executed on the equipment.

Here, we find a varied combination of protocols that allow the terminals to access numerous services. These include SMTP, POP, IMAP, DNS, HTTP, HTTPS, DHCP, FTP, and TFTP. Configuration of these services is dependent on the administrator's experience, and it is important to be careful to prevent **bad configurations** from returning an access port to the network.

Implementing a ***high-level firewall*** enables increased control of network traffic. Unlike firewalls at the network layer or transport layer, firewalls at the application layer allow packet filtering based on a wide range of options, including a vast array of protocols.

In addition, at this layer we find Intrusion Detection Systems **(IDS),** *Intrusion Prevention Systems* **(IPS),** and other complete security solutions. These applications function on the entire TCP/IP stack, being able to detect dangerous behavior according to various criteria, and issuing warnings as appropriate.

Another relevant aspect, once this layer of abstraction has been implemented, is **user education** and the definition of **security policies** for the IT department. Ensuring the

security of IT equipment is a case of pairing the correct implementation of the technical defense mechanisms with the right instructions to the users of the equipment, and the administrators who have power over them. We cannot consider any one of these alone.

1.7 Web Threats or Cyber Attack or Menace

1.7.1 Web Threats

A web threat is anything on the Internet that facilitates cybercrimes, including computer viruses, denial-of-service attacks and malware that target computer networks and devices. Other cybercrimes include cyber stalking, fraud and identity theft, information warfare, and phishing scams, all of which use computer networks and devices to facilitate other crimes. Financial damages, identity theft, loss of confidential information or data, damage to a company's brand or a person's reputation, and declining consumer confidence are just some of the risks posed by Web threats.

Web threats are malicious software programs such as spyware, adware, trojan horse programs, bots, viruses, or worms, etc. that are installed on your computer without your knowledge or permission. These programs utilize the Web to spread, hide, update themselves and send stolen data back to criminals. They can also be combined to do the crime - for example, a trojan can download spyware or a worm can be used to infect your computer with a bot.

Threat actors :

- **Social :** People are the primary attack vector
- **Operational :** Failures of policy and procedure
- **Technological :** Technical issues with the system
- **Environmental :** From natural or physical facility factors
- **Threat modelling :** Helps determine the threat surface, assign risk and drive vulnerability mitigation

1.7.2 Cyber Attack and Types of Cyber Attacks

A **cyber attack** is any type of offensive action that targets computer information systems, infrastructures, computer networks or personal computer devices, using various methods to steal, alter or destroy data or information systems.

A **cyber attack** refers to an action designed to target a computer or any element of a computerized information system to change, destroy, or steal data, as well as exploit or harm a network. Cyber attacks have been on the rise, in sync with the digitization of business that has become more and more popular in recent years.

Types of cyber attacks

1. DoS and DDoS Attacks

A denial-of-service (DoS) attack is designed to overwhelm the resources of a system to the point where it is unable to reply to legitimate service requests. A distributed denial-of-service (DDoS) attack is similar in that it also seeks to drain the resources of a system. A **DDoS attack** is initiated by a vast array of malware-infected host machines controlled by the attacker. These are referred to as "denial of service" attacks because the victim site is unable to provide service to those who want to access it.

With a DoS attack, the target site gets flooded with illegitimate requests. Because the site has to respond to each request, its resources get consumed by all the responses. This makes it impossible for the site to serve users as it normally does and often results in a complete shutdown of the site.

DoS and DDoS attacks are different from other types of attacks that enable the hacker to either obtain access to a system or increase the access they currently have. With these types of attacks, the attacker directly benefits from their efforts. With DoS and DDoS attacks, on the other hand, the objective is simply to interrupt the effectiveness of the target's service. If the attacker is hired by a business competitor, they may benefit financially from their efforts.

A DoS attack can also be used to set up the target for another type of attack. With a successful DoS or DDoS attack, the system often has to come offline, which can leave it vulnerable to other types of attacks. One common way to prevent DoS attacks is to use a firewall that detects whether requests sent to your site are legitimate. Imposter requests can then be discarded, allowing normal traffic to flow without interruption.

There are different types of DoS and DDoS attacks; the most common are TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack and botnets.

a. TCP SYN flood attack

In this attack, an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake. The attacker's device floods the target system's small in-process queue with connection requests, but it does not respond when the target system replies to those requests. This causes the target system to time out while waiting for the response from the attacker's device, which makes the system crash or become unusable when the connection queue fills up.

There are a few countermeasures to a TCP SYN flood attack :

- Place servers behind a firewall configured to stop inbound SYN packets.
- Increase the size of the connection queue and decrease the timeout on open connections.

b. Teardrop attack

This attack causes the length and fragmentation offset fields in sequential Internet Protocol (IP) packets to overlap one another on the attacked host; the attacked system attempts to reconstruct packets during the process but fails. The target system then becomes confused and crashes.

If users don't have patches to protect against this DoS attack, disable SMBv2 and block ports 139 and 445.

c. Smurf attack

This attack involves using IP spoofing and the ICMP to saturate a target network with traffic. This attack method uses ICMP echo requests targeted at broadcast IP addresses. These ICMP requests originate from a spoofed "victim" address. For instance, if the intended victim address is 10.0.0.10, the attacker would spoof an ICMP echo request from 10.0.0.10 to the broadcast address 10.255.255.255. This request would go to all IPs in the range, with all the responses going back to 10.0.0.10, overwhelming the network. This process is repeatable, and can be automated to generate huge amounts of network congestion.

To protect your devices from this attack, you need to disable IP-directed broadcasts at the routers. This will prevent the ICMP echo broadcast request at the network devices. Another option would be to configure the end systems to keep them from responding to ICMP packets from broadcast addresses.

d. Ping of death attack

This type of attack uses IP packets to 'ping' a target system with an IP size over the maximum of 65,535 bytes. IP packets of this size are not allowed, so attacker fragments the IP packet. Once the target system reassembles the packet, it can experience buffer overflows and other crashes.

Ping of death attacks can be blocked by using a firewall that will check fragmented IP packets for maximum size.

e. Botnets

Botnets are the millions of systems infected with malware under hacker control in order to carry out DDoS attacks. These bots or zombie systems are used to carry out attacks against the target systems, often overwhelming the target system's bandwidth and processing capabilities. These DDoS attacks are difficult to trace because botnets are located in differing geographic locations.

Botnets can be mitigated by,

- RFC3704 filtering, which will deny traffic from spoofed addresses and help ensure that traffic is traceable to its correct source network. For example, RFC3704 filtering will drop packets from bogon list addresses.
- Black hole filtering, which drops undesirable traffic before it enters a protected network. When a DDoS attack is detected, the BGP (Border Gateway Protocol) host should send routing updates to ISP routers so that they route all traffic heading to victim servers to a null0 interface at the next hop.

2. Session hijacking / MITM attacks

Man-in-the-middle (MITM) attacks refer to breaches in **cyber security** that make it possible for an attacker to eavesdrop on the data sent back and forth between two people, networks, or computers. It is called a "man in the middle" attack because the attacker positions themselves in the "middle" or between the two parties trying to communicate. In effect, the attacker is spying on the interaction between the two parties.

In a **MITM attack,** the two parties involved feel like they are communicating as they normally do. What they do not know is that the person actually sending the message illicitly modifies or accesses the message before it reaches its destination. Some ways to protect yourself and your organization from MITM attacks is by using strong encryption on access points or to use a virtual private network (VPN).

3. Phishing Attacks

A **phishing attack** occurs when a malicious actor sends emails that seem to be coming from trusted, legitimate sources in an attempt to grab sensitive information from the target. Phishing attacks combine social engineering and technology and are so-called because the attacker is, in effect, "fishing" for access to a forbidden area by using the "bait" of a seemingly trustworthy sender.

To execute the attack, the bad actor may send a link that brings you to a website that then fools you into downloading malware or giving the attacker your private information. In many cases, the target may not realize they have been compromised,

which allows the attacker to go after others in the same organization without anyone suspecting malicious activity.

You can prevent phishing attacks from achieving their objectives by thinking carefully about the kinds of emails you open and the links you click on. Pay close attention to email headers, and do not click on anything that looks suspicious. Check the parameters for "Reply-to" and "Return-path." They need to connect to the same domain presented in the email.

4. Whale-phishing attacks

A whale-phishing attack is so-named because it goes after the "big fish" or whales of an organization, which typically include those in the C-suite or others in charge of the organization. These individuals are likely to possess information that can be valuable to attackers, such as proprietary information about the business or its operations.

If a targeted "whale" downloads ransomware, they are more likely to pay the ransom to prevent news of the successful attack from getting out and damaging their reputation or that of the organization. Whale-phishing attacks can be prevented by taking the same kinds of precautions to avoid phishing attacks, such as carefully examining emails and the attachments and links that come with them, keeping an eye out for suspicious destinations or parameters.

5. Spear-phishing attacks

Spear phishing refers to a specific type of targeted phishing attack. The attacker takes the time to research their intended targets and then write messages the target is likely to find personally relevant. These types of attacks are aptly called "spear" phishing because of the way the attacker hones in on one specific target. The message will seem legitimate, which is why it can be difficult to spot a spear-phishing attack.

Often, a spear-phishing attack uses email spoofing, where the information inside the "From" portion of the email is faked, making it look like the email is coming from a different sender. This can be someone the target trusts, like an individual within their social network, a close friend, or a business partner. Attackers may also use website cloning to make the communication seem legitimate. With website cloning, the attacker copies a legitimate website to lull the victim into a sense of comfort. The target, thinking the website is real, then feels comfortable entering their private information.

Similar to regular phishing attacks, spear-phishing-attacks can be prevented by carefully checking the details in all fields of an email and making sure users do not click on any link whose destination cannot be verified as legitimate.

6. Insider threat

As the name suggests, an insider threat does not involve a third party but an insider. In such a case; it could be an individual from within the organization who knows everything about the organization. Insider threats have the potential to cause tremendous damages.

Insider threats are rampant in small businesses, as the staff there hold access to multiple accounts with data. Reasons for this form of an attack are many, it can be greed, malice, or even carelessness. Insider threats are hard to predict and hence tricky.

To prevent the insider threat attack,

- Organizations should have a good culture of security awareness.
- Companies must limit the IT resources staff can have access to depending on their job roles.
- Organizations must train employees to spot insider threats. This will help employees understand when a hacker has manipulated or is attempting to misuse the organization's data.

7. Password attack

Passwords are the access verification tool of choice for most people, so figuring out a target's password is an attractive proposition for a hacker. This can be done using a few different methods. Often, people keep copies of their passwords on pieces of paper or sticky notes around or on their desks. An attacker can either find the password themselves or pay someone on the inside to get it for them.

An attacker may also try to intercept network transmissions to grab passwords not encrypted by the network. They can also use social engineering, which convinces the target to input their password to solve a seemingly "important" problem. In other cases, the attacker can simply guess the user's password, particularly if they use a default password or one that is easy to remember.

Attackers also often use brute-force methods to guess passwords. A brute-force password hack uses basic information about the individual or their job title to try to guess their password. For example, their name, birthdate, anniversary or other personal but easy-to-discover details can be used in different combinations to decipher their password. Information that users put on social media can also be leveraged in a brute-force password hack. What the individual does for fun, specific hobbies, names of pets, or names of children are sometimes used to form passwords, making them relatively easy to guess for brute-force attackers.

A hacker can also use a dictionary attack to ascertain a user's password. A dictionary attack is a technique that uses common words and phrases, such as those listed in a dictionary, to try and guess the target's password.

One effective method of preventing brute-force and dictionary password attacks is to set up a lock-out policy. This locks out access to a device, website, or application automatically after a certain number of failed attempts. With a lock-out policy, the attacker only has a few tries before they get banned from access. If you have a lockout policy in place already and discover that your account has been locked out because of too many login attempts, it is wise to change your password.

If an attacker systematically uses a brute-force or dictionary attack to guess your password, they may take note of the passwords that did not work. For example, if your password is your last name followed by your year of birth and the hacker tries putting your birth year before your last name on the final attempt, they may get it right on the next try.

8. SQL injection attack

Structured Query Language (SQL) injection is a common method of taking advantage of websites that depend on databases to serve their users. Clients are computers that get information from servers, and an SQL attack uses an SQL query sent from the client to a database on the server. The command is inserted, or "injected", into a data plane in place of something else that normally goes there, such as a password or login. The server that holds the database then runs the command and the system is penetrated.

If an SQL injection succeeds, several things can happen, including the release of sensitive data or the modification or deletion of important data. Also, an attacker can execute administrator operations like a shutdown command, which can interrupt the function of the database.

To shield yourself from an SQL injection attack, take advantage of the least-privileged model. With least-privileged architecture, only those who absolutely need to access key databases are allowed in. Even if a user has power or influence within the organization, they may not be allowed to access specific areas of the network if their job does not depend on it.

For example, the CEO can be kept from accessing areas of the network even if they have the right to know what is inside. Applying a least-privileged policy can prevent not just bad actors from accessing sensitive areas but also those who mean well but accidentally leave their login credentials vulnerable to attackers or leave their workstations running while away from their computers.

9. URL interpretation

With URL interpretation, attackers alter and fabricate certain URL addresses and use them to gain access to the target's personal and professional data. This kind of attack is also referred to as URL poisoning. The name "URL interpretation" comes from the fact that the attacker knows the order in which a web-page's URL information needs to be entered. The attacker then "interprets" this syntax, using it to figure out how to get into areas they do not have access to.

To execute a URL interpretation attack, a hacker may guess URLs they can use to gain administrator privileges to a site or to access the site's back end to get into a user's account. Once they get to the page they want, they can manipulate the site itself or gain access to sensitive information about the people who use it.

For example, if a hacker attempts to get into the admin section of a site called GetYourKnowledgeOn.com, they may type in **http://getyourknowledgeon.com/admin,** and this will bring them to an admin login page. In some cases, the admin username and password may be the default "admin" and "admin" or very easy to guess. An attacker may also have already figured out the admin's password or narrowed it down to a few possibilities. The attacker then tries each one, gains access, and can manipulate, steal, or delete data at will.

To prevent URL interpretation attacks from succeeding, use secure authentication methods for any sensitive areas of your site. This may necessitate multi-factor authentication (MFA) or secure passwords consisting of seemingly random characters.

10. DNS spoofing

With Domain Name System (DNS) spoofing, a hacker alters DNS records to send traffic to a fake or "spoofed" website. Once on the fraudulent site, the victim may enter sensitive information that can be used or sold by the hacker. The hacker may also construct a poor-quality site with derogatory or inflammatory content to make a competitor company look bad.

In a DNS spoofing attack, the attacker takes advantage of the fact that the user thinks the site they are visiting is legitimate. This gives the attacker the ability to commit crimes in the name of an innocent company, at least from the perspective of the visitor.

To prevent DNS spoofing, make sure your DNS servers are kept up-to-date. Attackers aim to exploit vulnerabilities in DNS servers, and the most recent software versions often contain fixes that close known vulnerabilities.

11. Brute force attack

A **brute-force attack** gets its name from the "brutish" or simple methodology employed by the attack. The attacker simply tries to guess the login credentials of someone with access to the target system. Once they get it right, they are in.

While this may sound time-consuming and difficult, attackers often use bots to crack the credentials. The attacker provides the bot with a list of credentials that they think may give them access to the secure area. The bot then tries each one while the attacker sits back and waits. Once the correct credentials have been entered, the attacker gains access.

To prevent brute-force attacks, have lock-out policies in place as part of your authorization security architecture. After a certain number of attempts, the user attempting to enter the credentials gets locked out. This typically involves "freezing" the account so even if someone else tries from a different device with a different IP address, they cannot bypass the lockout.

It is also wise to use random passwords without regular words, dates, or sequences of numbers in them. This is effective because, for example, even if an attacker uses software to try to guess a 10-digit password, it will take many years of non-stop attempts to get it right.

12. Web attacks

Web attacks refer to threats that target vulnerabilities in web-based applications. Every time you enter information into a web application, you are initiating a command that generates a response. For example, if you are sending money to someone using an online banking application, the data you enter instructs the application to go into your account, take money out, and send it to someone else's account. Attackers work within the frameworks of these kinds of requests and use them to their advantage.

Some common web attacks include SQL injection and cross-site scripting (XSS), which will be discussed later in this article. Hackers also use cross-site request forgery (CSRF) attacks and parameter tampering. In a CSRF attack, the victim is fooled into performing an action that benefits the attacker. For example, they may click on something that launches a script designed to change the login credentials to access a web application. The hacker, armed with the new login credentials, can then log in as if they are the legitimate user.

Parameter tampering involves adjusting the parameters that programmers implement as security measures designed to protect specific operations. The operation's execution depends on what is entered in the parameter. The attacker simply changes the

parameters, and this allows them to bypass the security measures that depended on those parameters.

To avoid web attacks, inspect your web applications to check for and fix - vulnerabilities. One way to patch up vulnerabilities without impacting the performance of the web application is to use anti - CSRF tokens. A token is exchanged between the user's browser and the web application. Before a command is executed, the token's validity is checked. If it checks out, the command goes through - if not, it is blocked. You can also use SameSite flags, which only allow requests from the same site to be processed, rendering any site built by the attacker powerless.

13. Drive - by attack

A 'drive-by-download' attack is where an unsuspecting victim visits a website which in turn infects their device with malware. The website in question could be one that is directly controlled by the attacker, or one that has been compromised.

In some cases, the malware is served in content such as banners and advertisements. These days exploit kits are available which allow novice hackers to easily setup malicious websites or distribute malicious content through other means.

14. Trojan horses

A **Trojan horse** attack uses a malicious program that is hidden inside a seemingly legitimate one. When the user executes the presumably innocent program, the malware inside the Trojan can be used to open a backdoor into the system through which hackers can penetrate the computer or network. This threat gets its name from the story of the Greek soldiers who hid inside a horse to infiltrate the city of Troy and win the war. Once the "gift" was accepted and brought within the gates of Troy, the Greek soldiers jumped out and attacked. In a similar way, an unsuspecting user may welcome an innocent-looking application into their system only to usher in a hidden threat.

To prevent Trojan attacks, users should be instructed not to download or install anything unless its source can be verified. Also, NGFWs can be used to examine data packets for potential threats.

15. AI - Powered attacks

The use of Artificial Intelligence to launch sophisticated cyber-attacks is a daunting prospect, as we don't yet know what such attacks will be capable of. The most notable AI - powered attack we've seen to-date involved the use of AI-powered botnets which used slave machines to perform a huge DDoS attack.

However, we're likely to see much more sophisticated attack vectors to come.

AI-powered software is able to learn what kinds of approaches work best and adapt their attack methods accordingly. They can use intelligence feeds to quickly identify software vulnerabilities, as well as scan systems themselves for potential vulnerabilities. AI-generated text, audio and video will be used to impersonate company executives, which can be used to launch very convincing Phishing attacks. Unlike humans, AI-powered attacks can work around the clock. They are fast, efficient, affordable and adaptable.

16. XSS attacks

With XSS, or **cross - site scripting,** the attacker transmits malicious scripts using clickable content that gets sent to the target's browser. When the victim clicks on the content, the script is executed. Because the user has already logged into a web application's session, what they enter is seen as legitimate by the web application. However, the script executed has been altered by the attacker, resulting in an unintended action being taken by the "user."

For example, an XSS attack may change the parameters of a transfer request sent through an online banking application. In the falsified request, the intended recipient of the transferred money has their name replaced with that of the attacker. The attacker may also change the amount being transferred, giving themselves even more money than the target initially intended to send.

One of the most straightforward ways of preventing XSS attacks is to use a whitelist of allowable entities. This way, anything other than approved entries will not be accepted by the web application. You can also use a technique called sanitizing, which examines the data being entered, checking to see if it contains anything that can be harmful.

17. Eavesdropping attacks

Eavesdropping attacks involve the bad actor intercepting traffic as it is sent through the network. In this way, an attacker can collect usernames, passwords, and other confidential information like credit cards. Eavesdropping can be active or passive.

Eavesdropping can be passive or active :

- **Passive eavesdropping :** A hacker detects the information by listening to the message transmission in the network.
- **Active eavesdropping :** A hacker actively grabs the information by disguising himself as friendly unit and by sending queries to transmitters. This is called probing, scanning or tampering.

Detecting passive eavesdropping attacks is often more important than spotting active ones, since active attacks requires the attacker to gain knowledge of the friendly units by conducting passive eavesdropping before.

With active eavesdropping, the hacker inserts a piece of software within the network traffic path to collect information that the hacker analyzes for useful data. Passive eavesdropping attacks are different in that the hacker "listens in," or eavesdrops, on the transmissions, looking for useful data they can steal.

Both active and passive eavesdropping are types of MITM attacks. One of the best ways of preventing them is by encrypting your data, which prevents it from being used by a hacker, regardless of whether they use active or passive eavesdropping.

18. Birthday attack

In a birthday attack, an attacker abuses a security feature: hash algorithms, which are used to verify the authenticity of messages. The hash algorithm is a digital signature, and the receiver of the message checks it before accepting the message as authentic. If a hacker can create a hash that is identical to what the sender has appended to their message, the hacker can simply replace the sender's message with their own. The receiving device will accept it because it has the right hash.

The name "birthday attack" refers to the birthday paradox, which is based on the fact that in a room of 23 people, there is more than a 50% chance that two of them have the same birthday. Hence, while people think their birthdays, like hashes, are unique, they are not as unique as many think.

To prevent birthday attacks, use longer hashes for verification. With each extra digit added to the hash, the odds of creating a matching one decrease significantly.

19. Malware attack

Malware is a general term for malicious software, hence the "mal" at the start of the word. Malware infects a computer and changes how it functions, destroys data, or spies on the user or network traffic as it passes through. Malware can either spread from one device to another or remain in place, only impacting its host device.

Several of the attack methods described above can involve forms of malware, including MITM attacks, phishing, ransomware, SQL injection, Trojan horses, drive-by attacks and XSS attacks.

In a malware attack, the software has to be installed on the target device. This requires an action on the part of the user. Therefore, in addition to using firewalls that can detect malware, users should be educated regarding which types of software to avoid, the kinds of links they should verify before clicking, and the emails and attachments they should not engage with.

Some of the most common types of malware,

- **Macro viruses :** These viruses infect applications such as Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence. When the application is opened, the virus executes instructions before transferring control to the application. The virus replicates itself and attaches to other code in the computer system.
- **File infectors :** File infector viruses usually attach themselves to executable code, such as .exe files. The virus is installed when the code is loaded. Another version of a file infector associates itself with a file by creating a virus file with the same name, but an .exe extension. Therefore, when the file is opened, the virus code will execute.
- **System or boot-record infectors :** A boot-record virus attaches to the master boot record on hard disks. When the system is started, it will look at the boot sector and load the virus into memory, where it can propagate to other disks and computers.
- **Polymorphic viruses :** These viruses conceal themselves through varying cycles of encryption and decryption. The encrypted virus and an associated mutation engine are initially decrypted by a decryption program. The virus proceeds to infect an area of code. The mutation engine then develops a new decryption routine and the virus encrypts the mutation engine and a copy of the virus with an algorithm corresponding to the new decryption routine. The encrypted package of mutation engine and virus is attached to new code, and the process repeats. Such viruses are difficult to detect but have a high level of entropy because of the many modifications of their source code. Anti-virus software or free tools like Process Hacker can use this feature to detect them.
- **Stealth viruses :** Stealth viruses take over system functions to conceal themselves. They do this by compromising malware detection software so that the software will report an infected area as being uninfected. These viruses conceal any increase in the size of an infected file or changes to the file's date and time of last modification.
- **Trojans :** A Trojan or a Trojan horse is a program that hides in a useful program and usually has a malicious function. A major difference between viruses and Trojans is that Trojans do not self-replicate. In addition to launching attacks on a system, a Trojan can establish a back door that can be exploited by attackers. For example, a Trojan can be programmed to open a high-numbered port so the hacker can use it to listen and then perform an attack.

- **Logic bombs :** A logic bomb is a type of malicious software that is appended to an application and is triggered by a specific occurrence, such as a logical condition or a specific date and time.
- **Worms :** Worms differ from viruses in that they do not attach to a host file, but are self-contained programs that propagate across networks and computers. Worms are commonly spread through email attachments; opening the attachment activates the worm program. A typical worm exploit involves the worm sending a copy of itself to every contact in an infected computer's email address In addition to conducting malicious activities, a worm spreading across the internet and overloading email servers can result in denial-of-service attacks against nodes on the network.
- **Droppers :** A dropper is a program used to install viruses on computers. In many instances, the dropper is not infected with malicious code and, therefore might not be detected by virus-scanning software. A dropper can also connect to the internet and download updates to virus software that is resident on a compromised system.
- **Ransomware :** Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key. In some cases, ransomware authors design the code to evade traditional virus protection software. It is therefore important for users to remain vigilant regarding which sites they visit and which links they click. You can also prevent many ransomware attacks by using a next-generation firewall (NGFW) that can perform deep data packet inspections using artificial intelligence (AI) that looks for the characteristics of ransomware.
- **Adware :** Adware is a software application used by companies for marketing purposes; advertising banners are displayed while any program is running. Adware can be automatically downloaded to your system while browsing any website and can be viewed through pop-up windows or through a bar that appears on the computer screen automatically.
- **Spyware :** Spyware is a type of program that is installed to collect information about users, their computers or their browsing habits. It tracks everything you do without your knowledge and sends the data to a remote user. It also can download and install other malicious programs from the internet. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware application.

20. Cryptojacking

The term cryptojacking is closely related to cryptocurrency. Cryptojacking takes place when attackers access someone else's computer for mining cryptocurrency.

The access is gained by infecting a website or manipulating the victim to click on a malicious link. They also use online ads with JavaScript code for this. Victims are unaware of this as the Crypto mining code works in the background; a delay in the execution is the only sign they might witness.

Cryptojacking can be prevented by following the below-mentioned steps :

- Update your software and all the security apps as cryptojacking can infect the most unprotected systems.
- Have cryptojacking awareness training for the employees; this will help them detect crypotjacking threats.
- Install an ad blocker as ads are a primary source of cryptojacking scripts. Also have extensions like MinerBlock, which is used to identify and block crypto mining scripts.

21. Zero - day exploit

A zero-day exploit happens after the announcement of a network vulnerability; there is no solution for the vulnerability in most cases. Hence the vendor notifies the vulnerability so that the users are aware; however, this news also reaches the attackers.

Depending on the vulnerability, the vendor or the developer could take any amount of time to fix the issue. Meanwhile, the attackers target the disclosed vulnerability. They make sure to exploit the vulnerability even before a patch or solution is implemented for it.

Zero-day exploits can be prevented by,

- Organizations should have well-communicated patch management processes. Use management solutions to automate the procedures. Thus it avoids delays in deployment.
- Have an incident response plan to help you deal with a cyber attack. Keep a strategy focusing on zero-day attacks. By doing so, the damage can be reduced or completely avoided.

22. Watering hole attack

The victim here is a particular group of an organization, region, etc. In such an attack, the attacker targets websites which are frequently used by the targeted group. Websites are identified either by closely monitoring the group or by guessing.

After this, the attackers infect these websites with malware, which infects the victims' systems. The malware in such an attack targets the user's personal information. Here, it is also possible for the hacker to take remote access to the infected computer.

Watering hole attack can be prevented by using below techniques,

- Update your software and reduce the risk of an attacker exploiting vulnerabilities. Make sure to check for security patches regularly.
- Use your network security tools to spot watering hole attacks. Intrusion prevention systems(IPS) work well when it comes to detecting such suspicious activities.
- To prevent a watering hole attack, it is advised to conceal your online activities. For this, use a VPN and also make use of your browser's private browsing feature. A VPN delivers a secure connection to another network over the Internet. It acts as a shield for your browsing activity. NordVPN is a good example of a VPN.

23. Business Email Compromise (BEC)

A BEC attack is where the attacker targets specific individuals, usually an employee who has the ability to authorize financial transactions, in order to trick them into transferring money into an account controlled by the attacker.

BEC attacks usually involve planning and research in order to be effective. For example, any information about the target organization's executives, employees, customers, business partners and potential business partners, will help the attacker convince the employee into handing over the funds.

BEC attacks are one of the most financially damaging forms of cyber-attack.

1.7.3 TCP/IP Model

The TCP/IP protocol suite is a group of different communication protocols working through the internet and other private communication networks and it carries most of the essential services running over the network. It provides end-to-end connectivity by establishing, maintaining, and releasing connections between the sender and receiver. It provides for flow control, error control, IP addressing and the routing of network traffic and an interface between the node and the physical network. The layers with their protocols and functions are described below.

1. Network access layer (*Host to Network Layer*)

The network access layer is the fourth layer in the TCP/IP protocol suite and is responsible for the host-to-host delivery of datagram . The main liability network layers generate a connection between the source computers to the destination computer. The communication at the network layer is host to host. The network layer is responsible for choosing the best route for each packet, routing packets from source to destination incoming or outgoing a subnet. The network layer focal function is path tenacity and logical addressing. This layer provides logical addresses to the packets received which in turn helps them to find their path.

The key functionality of a network layer is end-to-end routing of packets, from the source computer to the targeted computer, from the use of first to last next-hop-routing approach. For getting point-to-point communication, it supports three features:

- **Forwarding**

Forwarding is a packet switching. When a node after communication receives input interfaces through an IP packet, the appropriate output process selecting of an interface to transmit the packet based on the node's packet's destination, routing table and the IP address, it is called forwarding.

- **Routing**

The process of the calculating a job from various sources is known as routing, route or the best next hop node. This is for reaching different networks and sub network's target from a given node and storing it in tables recognized by routing tables. The processes' lists of routing protocols are termed as the control plane or path control, as they control the actual path taken by data packets.

- **Logical addressing (IP Addresses)**

The communication over a network with every device must associate with it a logical address. For defining the rules and structure related to IP addresses, the network layer is answerable. Network interfaces of communicating nodes are unique end-point identifiers of IP addresses. On the public Internet, every communicating node needs to have at least one public IP address to communicate successfully with other computers on the internet.

- **Other features of networking layer**

For receiving point-to-point communication, it supports three specific features - forwarding, routing and logical addressing - after that network layer also support services like packet fragmentation/ multicasting, reassembly, network layer error reporting (ICMP), broadcasting, IP Security (IPSec), QOS, etc.

Network layer protocols include : Ethernet, FDDI, Token Ring, ATM, OC, HSSI, or even Wi-Fi. The purpose of a network interface is to allow your computer to access the wire, wireless, or fibre optic network infrastructure and send data to other computers.

The network layer offers two types of protocols for delivering the packets over the network.

- **Connection-oriented :** Connection-oriented services provided by the transport layer for example (TCP) is connection-oriented.
- **Connectionless services :** In different protocol groups, the network layer protocol is known as a connectionless protocol. For example, in TCP/IP, the IP is connectionless,
  - Dropped packets (when packets are arriving too fast to be processed)
  - Connectivity failure (when a destination host cannot be reached)
  - Redirection (which tells a sending host to use another).

2. Internet layer

The internet layer is the third layer in TCP/IP model, and it is equivalent to the network layer in the OSI model. The main function for the Internet layer is to handle communication from one PC to another. This layer is responsible to request and send a packet from the transport layer by knowing to which PC it will be delivered. Moreover, it is more responsible for packing, addressing and routing. The most important protocol in the internet layer is TCP/IP which known as internet protocol.

The internet protocol is the structure block of the Internet beside the block it's functions are defining the datagram, which is the basic unit of transmission in the Internet, defining the Internet addressing scheme, moving data between the network access layer and the host-to-host transport layer, routing datagram to remote hosts and performing fragmentation and re-assembly of datagram. The Internet software will deeply encapsulate the transport packet in an IP packet. The Internet layer includes four core protocols and it can be listed as :

- **Internet Protocol (IP) :** The main functions for IP are addressing, routing and transmitting the packets over the network.
- **Address Resolution Protocol (ARP) :** The main function for APR is the linking and translation from the Internet layer address to the Network Interface layer address such as a MAC address.

- **Internet Control Message Protocol (ICMP) :** The main function for ICMP is to generate the error message for an unsuccessful delivering message then report it to the source IP address. This is the protocol responsible for detecting network error conditions and reporting on them. Reports include :
  - Dropped packets (when packets are arriving too fast to be processed).
  - Connectivity failure (when a destination host cannot be reached).
  - Redirection (which tells a sending host to use another router).
- **Internet Group Management Protocol (IGMP) :** The main function for IGMP is the communication between hosts and multicast routers.

3. Transport layer

The transport layer is the second layer in TCP/IP model, it is responsible for a flow of data between two hosts (client and server). It provides end-to-end connections efficiently, offering delivery of data in sequence, avoiding duplication or dropping.Two protocols are in this layer, whereas TCP refers to Transmission Control Protocol, UDP refers to User Datagram Protocol. These two protocols are different depending on reliability.

Using TCP ensures high reliability and a special mechanism to make sure that the data reaches the destination completely. It provides reliability in the flow of data which has led to ignoring all reliability issues in an application layer. The data is divided into a suitable size to pass to the next layer and then acknowledging messages are sent by a receiver to make sure that the packets are sent.

In contrast to TCP, UDP uses a simple mechanism that depends on the lower layer to transmit the data, and upper-layer protocols to make sure the data is transmitted successfully to the required level. It is simple protocol, and the responsibility of this protocol is to send the packet (datagram) without concern for reliability, which is handled on the application layer. Furthermore, TCP is used by the applications whereas reliability is more important than performance. This can be seen in case of transferring files or important data between two hosts, the application such HTTP, SMTP and FTP use TCP. All messages sent in this protocol are acknowledged, so the reliability is achieved, and lost data will be resent automatically.

On the other hand, UDP is used when losing a byte of data will not be a significant effect, and the application layer will be responsible for detecting lost data and retransmitted when the application layer chooses to use UDP. It has been seen in case of small amount of data, and streaming data and video.

4. Application layer

The application layer is the uppermost layer of the four-layer TCP/IP model and it merges the three most significant layers of the OSI model: application, presentation and session. This layer is primarily concerned with human interaction and how software applications are implemented. The application layer consists of interface methods and underlying communication protocols that can be applied in process-to-process communications. It standardizes communication and does not define specific rules or data formats that applications need to consider when connecting; the original description does depend on and recommend the general design guideline for software.

The application layer is concerned with providing network services to applications. It provides a mechanism to the next level, transport services, for interfacing with host programs for efficient use of network. At this layer each application's path and session can be distinguished by the use of specific sockets and port numbers. Application layer includes all the higher-level protocols like :

- **Hypertext Transfer Protocol (HTTP) :** The HTTP protocol enables the connection between a web server and a client and also distributes the information on the World Wide Web (WWW). It uses port number 80.On server side, the main examples are Apache Web Server and Internet Information Server (IIS), while on client sideFirefox, Internet Explorer, Mozilla and Google Chrome are most common.
- **Simple Mail Transfer Protocol (SMTP) :** SMTP is the only standard for electronic mail (E-mail) over the TCP/IP network; it handles the message services by the use of well-known port 25.
- **Dynamic Host Configuration Protocol (DHCP) :** It is used to dynamically (automatically) allocate TCP/IP configuration constraints (DNS server, **Subnet Mask, IP address,** Default Gateway etc.) to network devices.
- **Domain Name System (DNS) :** The IP addresses which are the actual addresses of network recourses are very difficult for the users to remember, DNS is an excellent solution to this problem it contains the distributed database of the mapping records of user-friendly alphanumeric names with that of embedded IP addresses to make network resources easy to remember.
- **Simple Network Management Protocol (SNMP) :** This is a popular protocol that allows for remote and local management of network devices such as servers, workstations, hubs, routers, switches and other managed devices.

- **File Transfer Protocol (FTP) :** The passive mode protocol used to send and receive large files from remote servers without requiring a - host connection established previously.
- **Trivial File Transfer Protocol (TFTP) :** This protocol is a simplified version of FTP, especially designs for UDP and resource hungry computers. It contains only a small subset of the capabilities of FTP lacking packet-monitoring and error-handling capabilities, hence the process overhead is lower than FTP. Then again, and these limitations also reduce the process overhead. Security is of evident concern when using TFTP. Examples :
  - o Telnet
  - o SSH
  - o X Windows
  - o RDP (Remote Desktop Protocol)

By using applications and application protocols, data can be moved between hosts, and remote users can communicate easily.

1.7.4 Security Problems in TCP/IP Models Protocol

1. Application Protocol

One of the main purposes of an application is the encryption and decryption as a technique for securing the data. The security threat of this layer is at the application level. Applications need to secure sensitive data that is sent to the network, hence applications needs to be well formulated to protect the data. The security vulnerabilities at the two most common protocols of the application layer are being discussed below.

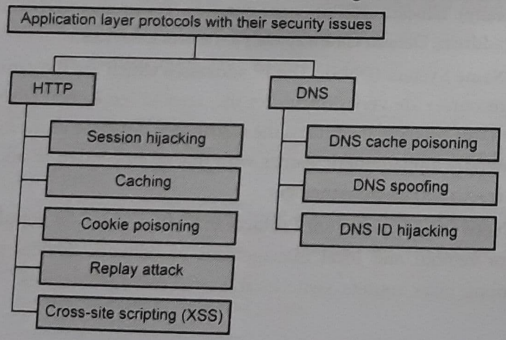

Fig. 1.7.1 Application layer protocols with their security issues

1.7.4.1 Security Threats on HTTP

HTTP is the default communication protocol used by all web browsers. The transfer of files in the form of web pages is done in plain text and therefore is prone to security attacks as listed:

1.7.4.2 Session Hijacking

Hijacking means stealing an HTTP session. A cyber-terrorist usually uses a packet sniffer to capture the packets for stealing the session; hijacking can be possible if in the initialization session strong authentications procedures are not used, opening the way for picking up the session ID or Token ID. Session hijacking provides access to the account as an authentic user and hence attacks the integrity of the target user.

1.7.4.3 Caching

Web browsers temporarily save web pages on a user's machine as he/she visits them to speed up and ease access in case the user wants to visit those pages again. This is known as cashing. The hacker has gained the access of the user's machine and views all the cashed contents of the user that may contain user IDs, passwords and pictorial data without any authentication password. The hacker then can take the user's credentials for misuse.

1.7.4.4 Cookie Poisoning

Cookies are created by the web servers when a user visits a website. Cookies are used to save credentials and the interaction information of the user with the website, which the web server can use later when processing the sessions of that particular user. Cookie poisoning is the alteration or stealing of cookie in a user's machine by a hacker to reprieve personal information. If the hacker gets a hold of a cookie containing a password and username, he or she can use the cookie on his or her machine and the web server will not demand any verification.

1.7.4.5 Replay Attack

A replay attack is made possible by man in middle. By repeating the sent data to the server, it is a more serious threat than session hijacking. The resent data can be altered and hence producing wrong or totally different results. More critically, the attacker can take off the client's IP address and thus redirect his/her machine.

1.7.4.6 Cross-Site Scripting (XSS)

This attack involves the hacker inserting malicious code in a web application or browser and is executed on the client side. The essence of this attack is to perform a session hijack by stealing session tokens and cookies of a genuine user's session.

1.7.4.7 Domain Name System

The domain name system (DNS) is used to translate domain names to IP addresses for the sake of user convenience, as they use alphabetical names. The security issue started in DNS when a hacker changed record to resolve to an incorrect IP address; hackers can direct all traffic for a site to the wrong server or client computer. The most common security attacks for this protocol are :

1.7.4.8 DNS Cache Poisoning

Caching poisoning through DNS is a reliability attack that involves modifying the information saved in the DNS cache. This fabricated information will map the name to a wrong IP address and mislead the request to a false site[17]. This attack can lead to pharming or phishing. The most critical situation can occur if the user does not notice anything and enters a user name and

1.7.4.9 DNS Spoofing

A DNS spoofing attack uses a fake IP address of a computer to match the DNS server's IP address. The user request then will be directed to the hacker's machine. In this attack, the clients and other servers will consider the hacker's machine to be a genuine DNS server and send their requests and receive the reply from the wrong server.

1.7.4.10 DNS ID Hijacking

The most common method for DNS ID hijacking is through installing malware on a user's computer that changes the DNS. This malware changes the default DNS service provider to something that the cybercriminals want. From there, they control user's URL resolutions (DNS lookups) and then they keep on poisoning the DNS cache.

Transport PROTOCOL (TCP)

The main purpose of this layer is that controlling the flow of data between client and server, avoiding repetitions, or omitting part of data. TCP is one of its protocols that concerned with reliability and delivering data completely to the destination. In this part, the most security threats and attacks at this protocol will be discussed.

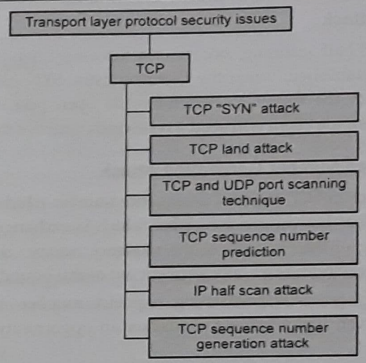

Fig. 1.7.2 Transport layer protocol security issues

1.7.5 TCP "SYN" Attack

This happens during a three-way handshake between a client and server when the client sends a synchronization request and then the server send back synchronization and acknowledgment and reserve all resources for this request. However, an acknowledgment message will not be sent, which makes half of the connection open, and the attacker sends many synchronous requests to make the server busy without responding to the server.

1.7.6 TCP Land Attack

This attack happens when the attacker pretends to be an authorized person by spoofing the source IP address, then he or she tries to send a SYN packet to open the TCP post in the server.

1.7.7 TCP and UDP Port Scanning Technique

This is an attacker port scanning to find an available port in the machine.

Categories of : denial of service (DoS), disclosure, modification, destructive and escalation of privilege.

1.7.8 TCP Sequence Number Prediction

Each packet sent between a client and server has a sequence number. The client and server exchange the sequence number, which has limited boundaries. In this case, an attacker predicts a sequence number counterfeit packet to pretend to be an authorized person, and tries to send these packets after spoofing the IP victim .

1.7.9 IP half scan attack

SYN-scanner, or IP half scanning, occurs in a three-way handshake when the TCP connection is never established, when the client sendsthe SYN packet, and waits for a SYN/ACK or rest from the server to determine the open post. When the SYK/ACK received from the server, the client will send a rest which destroys the connection .

1.7.10 TCP Sequence Number Generation Attack

The most crucial part in TCP segment is sequence number which is helpful in tracking the data, every data sent has sequence number which is exchange between server and client at the beginning of the connection, the sequence number must be within bound which is called receiver window size, any segment out of this bound will be discarded.

One of the security issues is predicating sequence number without receiving any response from the server, which gives the attacker an opportunity to spoof the trusted host in the lock network.

Internet Protocol

The Internet layer mostly depends on the communications between the nodes and deals with secure nodes from sources to destinations. Common attacks for the Internet layer can be in the

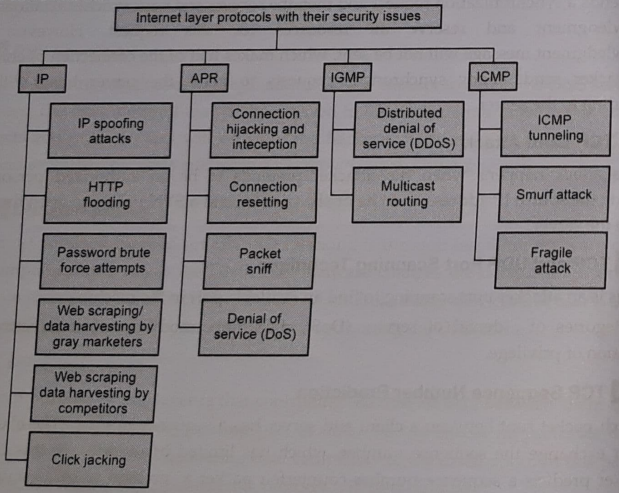

Fig. 1.7.3 Internet layer protocols with their security issues

1.7.11 IP

1.7.11.1 IP Spoofing Attacks

The purpose for this attack is to hide the identity for the IP sender. As a result, it will generate the wrong source IP address. There are two ways that IP spoofing attacks can be used to overload targets with traffic. One method is to simply flood a selected target with packets from multiple spoofed addresses. This method works by directly sending a victim more data than it can handle. The other method is to spoof the target's IP address and send packets from that address to many different recipients on the network. When another machine receives a packet, it will automatically transmit a packet to the sender in response. Since the spoofed packets appear to be sent from the target's IP address, all responses to the spoofed packets will be sent to (and flood) the target's IP address.

1.7.11.2 HTTP Flooding

This technique involves full-page reloads of dynamic content, fetching large elements and by passing the cache. It is also known as a DoS, which happens when a large number of routing messages are flooding into the server via network, then as a result the server will be weighted and led toa DoS.

1.7.11.3 Password Brute-Force Attempts

This attack mostly happens in HTTP and FTP.For each simultaneous client it is issues one request for each IP then it will return back with generating 100 password attempts.

1.7.11.4 Web Scraping / Data Harvesting by Grey Marketers

The aim of this attack is to extract the data from websites by scraping interfaces or software. It targets an online site that supports buying or selling.

1.7.11.5 Web Scraping / Data Harvesting by Competitors

This is similar to the above-mentioned attack with the difference being that this attack is executed to collect competitive pricing and plagiarize content.

1.7.11.6 Click Jacking (Split The Sentence)

Also known as user interface (UI) redressing, this is an attack that traps a web client into clicking a catch, a connection or a photo, that the web client did not plan to click, normally by overlaying the site page with an iframe.

1.7.12 APR

1.7.12.1 Connection Hijacking and Interception

The premise for session hijacking includes a hacker to assume control over a current session between a client and host machine. By assuming control over the legitimate session, the aggressor then abuses or endeavours the session.

1.7.12.2 Connection Reseating

This type of attack is made to cut the connection between the user and the server. This can be done by using crafted code and special software.

1.7.12.3 Packet Sniff

A packet sniffs the demonstration of catching packets of data flowing over a computer network. The software or device used to do this is known as packet sniffer.

1.7.12.4 Denial of Service (DoS)

A DoS attack is among the most widely recognized dangers to Internet operations. These attacks immerse the system transfer speed to make the system occupied to its proposed clients. They include impacting a site with enough movement to surge the associations between the Internet and the business. This attack happens when numerous frameworks flood the bandwidth or resources of a targeted system .

1.7.13 IGMP

1.7.13.1 Distributed Denial of Service (DDoS)

This attack is similar to a DoS attack with the difference being that a DoS attack can be done by using one computer and one internet connection, while in this attack; they use more than one computer and more internet connections.

1.7.13.2 Multicast Routing

The effect of an attack in a multicast environment is significantly higher compared to its unicast partner, as a single attacker can influence transmissions to numerous goals at the same time.

1.7.14 ICMP

1.7.14.1 ICMP Tunnelling

ICMP tunnels are one type of clandestine channel that is made where in the data stream is not controlled by any security component. An ICMP tunnel burrow sets up a channel between the client and server, constraining a firewall not to trigger caution if information are sent via ICMP. ICMP tunnelling is a covert connection between two endpoints using ICMP echo requests and reply packets. So by utilizing ICMP tunnelling, one can infuse discretionary information into an echo packet and send to a remote computer.

1.7.14.2 Smurf Attack

In a Smurf attack, an attacker will spoof the source address of the ICMP packet and send a broadcast to all computers on that network. If networking devices do not filter this traffic, then they will be broadcasted to all computers in the network. This congests the victim's network heavy traffic, which cuts down the profitability of the whole network.

1.7.14.3 Fraggle Attack

A fraggle attack is same as a smurf attack, but instead than ICMP, UDP is utilized. The aversion of these attacks is practically indistinguishable to a fraggle attack.

Review Questions

1. *What is network policy ?* **(Refer section 1.2.3)**
2. *Explain host based security.* **(Refer section 1.3)**
3. *Discuss security review of transport layer and application layer protocol.* **(Refer section 1.6)**
4. *Define and discuss cyber attacks.* **(Refer section 1.7.2)**
5. *Write a short note on security problems in TCP/IP model protocols.* **(Refer section 1.6.3)**

❑❑❑