Basic Security Problems:

A security issue is any unmitigated risk or vulnerability in your system that hackers can use to do damage to systems or data. This includes vulnerabilities in the servers and software connecting your business to customers, as well as your business processes and people. A vulnerability that hasn't been exploited is simply a vulnerability that hasn't been exploited yet. Web security problems should be addressed as soon as they are discovered, and effort should be put into finding them because exploit attempts are inevitable.

1. **Ransomware Attack**

The goal of a ransomware attack is to gain exclusive control of critical data. The hacker encrypts and holds your data hostage and then demands a ransom payment in exchange for the decryption key you need to access the files. The attacker may even download and threaten to release sensitive data publicly if you do not pay by a deadline. Ransomware is the type of attack you're most likely to see reported in major news media.

How to Prevent: The most effective ransomware attack protection is to have a thorough, frequent backup of critical data in a safe location. The attacker loses leverage with a solid backup and recovery plan, allowing you to erase and restore the affected data.

2. Code Injection (Remote Code Execution)

To attempt a code injection, an attacker will search for places your application accepts user input – such as a contact form, data-entry field, or search box. Then, through experimentation, the hacker learns what various requests and field content will do. For example, if your site's search function places terms into a database query, they will attempt to inject other database commands into search terms. Alternatively, if your code pulls functions from other locations or files, they will attempt to manipulate those locations and inject malicious functions.

How to Prevent: Besides server or network-level protections like CloudFlare and Liquid Web's Server Secure Plus, it is also important to address this security issue from a development perspective.

3. Cross-Site Scripting (XSS) Attack

JavaScript and other browser-side scripting methods are commonly used to dynamically update page content with external information such as a social media feed, current market information, or revenue-generating advertisements.

Hackers use XSS to attack your customers by using your site as a vehicle to distribute malware or unsolicited advertisements. As a result, your company's reputation can be tarnished, and you can lose customer trust.

How to Prevent: Adjust content security policies on your site to limit source URLs of remote scripts and images to only your domain and whatever external URLs you specifically require. This small and often-overlooked step can prevent many XSS attacks from even getting off the ground.

4. Data Breach

A data breach occurs whenever an unauthorized user gains access to your private data. They may not have a copy of the data or control it, but they can view it and possibly make changes.

You may not even know there's a breach immediately. For example, the attacker may have an administrative account password but hasn't used it to make any changes yet.

How to Prevent: This Internet security issue can be challenging to address because an attacker at this stage is generally taking careful steps to remain hidden. Many systems will print connection information from your previous session when you log in. Be aware of this information where available, and be mindful of activity that isn't familiar.

5. Malware and Virus Infection

Malware is short for malicious software. Malware on a workstation can encrypt data for ransomware purposes or even log keystrokes to capture passwords. Hackers typically use malware to expand existing access to your site or spread access to others on the same network. If malware is present, you've already been breached. Therefore, it's crucial to determine which Internet security issues led to the breach before any malware cleanup or restoration.

How to Prevent: On workstations, mitigate the risk of this security problem by being careful about what you download and using antivirus software to find and safely remove any malware. Keeping these antivirus applications regularly updated is critical, as the malware is constantly updated and improved. In addition, workstation logins should be users without administrative access. In a worst-case scenario, keep good backups to restore the workstation if it is compromised too deeply to clean.

6. DDoS Attack

Distributed Denial of Service (DDoS) attacks are generally not attempting to gain access. However, they are sometimes used in conjunction with brute force attacks (explained below) and other attack types as a way to make log data less useful during your investigation.

For example, the hacker may directly attack your application layer by overwhelming your site with more requests than it can handle. They may not even view an entire page - just a single image or script URL with a flood of concurrent requests. Beyond the traffic flood making your site unreachable (which any volumetric attack will do), a Layer 7 attack can inflict further damage by flooding order queues or polling data with bogus transactions that require extensive and costly manual verification to sort out.

How to Prevent: Blocking such an attack can be nearly impossible by conventional means. There is generally no security issue being exploited. The requests themselves are not malicious and deliberately blend in with normal traffic. The more widely distributed the attack, the more difficult it is to distinguish legitimate requests from those that are not.

7. Credential Stuffing Attack

Credential stuffing is a common term we now give to hackers abusing the re-use of passwords across multiple accounts. If a hacker gains access to one of your account passwords, you can be assured they will attempt to log into dozens of other common services with the same username and password they just captured.

How to Prevent: The best and easiest way to avoid this security issue is to simply never use the same username or password for multiple services. Multi-factor authentication also helps prevent this by keeping the login secure even if the primary password is weak.

8. Brute Force Attack

In a brute force attack, the hacker (usually with the help of automation) tries multiple password guesses in various combinations until one is successful. In simpler terms, think of it as opening a combination padlock by trying every possible combination of numbers in order.

How to Prevent: Many CMS and mainstream applications include software that monitors your system for repeated login failures or offers a plugin system that provides this information. These software and plugins are the best preventions for brute force attacks, as they severely limit the number of guesses allowed.

9. Weak Passwords and Authentication Issues

A chain is only as strong as its weakest link, and a computer system is only as secure as its weakest password. Therefore, for any level of access, all passwords should be of sufficient length and complexity. A strong password should include 18 characters minimum, and the longer, the better. Password length increases security more than complexity.

A password like “dK3(7PL” can be cracked faster than a password like “ThisPasswordIsSixWordsLong” even though the latter contains dictionary words.

How to Prevent: Use two-factor authentication wherever available. This can protect a login even if the correct password is obtained or guessed. Also, change your passwords on a regular schedule, such as every 60 or 90 days, and never use the same one twice.

10. Social Engineering

Social engineering encompasses all of the non-technical ways an attacker may use to gain access or do damage to your systems or data. The most common method is the oldest: lying or using fabricated information to gain trust.

A malicious actor may impersonate your bank, a utility provider, or even law enforcement. They may claim to be a customer or pose as an executive from your organization. The goal of such attacks is generally to either obtain sensitive information or trick an insider into unknowingly performing destructive actions.

They may try to:

- Obtain confidential contact details.
- Obtain account or credit card numbers.
- Obtain or reset passwords.
- Persuade staff to suspend or cancel essential services.
- Persuade staff to disable critical infrastructure.

- Persuade staff to upload or install malicious software.

Social engineering attacks can be devastatingly effective because the people who launch them are well-practiced in persuasion and deceit. Many have years of experience and finely-honed characters. For example, an attacker posing as law enforcement may give such a skilled performance that they'd fool an actual law enforcement officer. You absolutely cannot rely on your ability to judge character to protect yourself from these attacks.

How to Prevent: Watch for some of these common red-flag cues to become aware of social engineering at play:

- Aggressive language and demanding behavior designed to make you feel like you've done something wrong.
- A sense of urgency around fixing a problem before you have time to fact-check.
- Threats of legal action or financial penalty if you do not immediately comply.
- Evasion and escalated emotion when you ask identity-verification questions.

Routing: Routing is fundamental to how the Internet works. Routing protocols direct the movement of packets between your computer and any other computers it is communicating with. The Internet's routing protocol, Border Gateway Protocol (BGP) is known to be susceptible to errors and attacks. These problems can literally knock entire networks off the Internet or divert traffic to an unintended party.

Routing Security: Routing security aims to reduce the number of potentially invalid announcements that your network accepts by actively rejecting invalid route announcements, and by ensuring you only announce the correct prefixes yourself.

What is DNS?

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

How does DNS work?

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.

In order to understand the process behind the DNS resolution, it's important to learn about the different hardware components a DNS query must pass between. For the web browser, the DNS lookup occurs "behind the scenes" and requires no interaction from the user's computer apart from the initial request.

The 8 steps in a DNS lookup:

1. A user types 'example.com' into a web browser and the query travels into the Internet and is received by a DNS recursive resolver.
2. The resolver then queries a DNS root nameserver (.)
3. The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD.
4. The resolver then makes a request to the .com TLD.
5. The TLD server then responds with the IP address of the domain's nameserver, example.com.
6. Lastly, the recursive resolver sends a query to the domain's nameserver.
7. The IP address for example.com is then returned to the resolver from the nameserver.
8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially.

Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser is able to make the request for the web page:

9. The browser makes a HTTP request to the IP address.
10. The server at that IP returns the webpage to be rendered in the browser (step 10).

The Most Common Cybersecurity Weaknesses:

1. **Lack of a high-level strategy.** Many businesses, especially new and small ones, simply lack a high-level strategy for their cybersecurity needs. They don't have any security infrastructure in place, either because they don't take the topic seriously or because they deem it a comparatively low priority. However, this high-level strategy that sets the course for your main security priorities and your general approach to preventing and mitigating attacks is vital for success.
2. **Unsecured networks.** If the network isn't secured, it's trivially easy for nefarious parties to gain access to your system. And once they've infiltrated the network, they can gain access to practically all devices and systems connected to that network. This is a simple step to take, but it's one that many business owners still neglect. It's also a great opportunity to demonstrate your expertise.
3. **Unsecured communication channels.** If the business is regularly exchanging sensitive data, it's also important to incorporate secure communication channels. For example, you might invest in an encrypted, secure email platform that you use to communicate directly with clients. Or you might establish protocols for using multifactor authentication when sending certain types of messages.
4. **Unknown bugs.** Sometimes, a bug or flaw in a given app can be responsible for giving cybercriminals an easy backdoor to your accounts. This could be an aspect of software you're using from a third party, or it could be a flaw in the API that connects two different apps together. It's impossible to prevent or detect all bugs, but you can improve your security by proactively scanning for bugs when possible, and vetting your vendors carefully before choosing them for your applications.
5. **Outdated systems.** Fortunately, most software developers and hardware manufacturers are constantly on the lookout for security threats that could hurt their users. When they find a problem,

they issue a patch to eliminate that problem—but to make use of this patch, you have to update your hardware or software. If the business is using outdated systems because it isn't updating regularly, the business could be at risk.

6. **Lack of monitoring.** Do you know what kind of traffic you're seeing? Do you know the hallmarks of an attack like a distributed denial of service (DDoS) attack, or a ransomware attack? Would you be capable of identifying an attack in progress, and responding accordingly? Without proper monitoring and alert systems in place, the business will be vulnerable to these types of attacks.
7. **IoT and multiple connection points.** Many businesses are leveraging the power of the Internet of Things (IoT), with multiple connection points on a single network. While this is often associated with higher efficiency or productivity, it also means more points of vulnerability.
8. **Untrained employees.** Close to 90 percent of data breaches are caused by human error. Instead of some ultra-skilled hacker brute-forcing his way into your system, an employee volunteers his password after getting duped, providing an opportunist an easy way to gain access to the business's data. That's why untrained employees are one of your biggest vulnerabilities. It's vital to train employees on best practices in cybersecurity, like teaching them to use strong passwords, helping them identify different types of attacks, and giving them instructions on how and when to use networks that aren't theirs. It's also important to retrain employees regularly, and make sure they've retained this information. All it takes is one slip from one person to jeopardize the health of the entire company.

Link Layer: Link layer is the first lowest layer of the TCP/IP reference model, which describes how data should be physically generated and transmitted over the physical medium by the network devices.

Description: The physical layer and data link layer of OSI reference model is combined together to form a link layer. Following are the functions and responsibilities of link layer:

At physical level:

- At physical level data consist of a stream of bits (sequence of 0's and 1's).
- Defines how the bits are encoded into electrical signals by the network devices.
- Synchronizing the sender and receiver at the bit level.
- Line configuration - point-to-point or point-to-multipoint
- Transmission mode - simplex, half duplex or full duplex
- Topology - star, ring, tree, bus etc.
- Mechanical specification of cables and connectors.
- Specification of electronic factors like voltage, frequency, impedance etc.

At logical level:

- At logical level data consists of frames.
- Encapsulates IP packets or message received from the higher layer into frames.
- Synchronization of frames.
- Flow control, error detection and correction of frames at LLC sublayer.
- Physical addressing, access control at MAC sub layer.

TCP/IP in Computer Networking

TCP/IP stands for **Transmission Control Protocol/ Internet Protocol.** It is a set of conventions or rules and methods that are used to interconnect network devices on the Internet.
The internet protocol suite is commonly known as TCP/IP, as the foundational protocols in the suite are Transmission Control Protocol and Internet Protocol.

It chooses how the information will be traded over the web through end-to-end communications that incorporate how the information ought to be organized into bundles (bundles of data), addressed, sent, and received at the goal.
This communication protocol can also be utilized to interconnect organize devices in a private network such as an intranet or an extranet.

Characteristics of TCP/IP:

- **Share Data Transfer:** The TCP allows applications to create channels of communications across a network. It also permits a message to be separated into smaller packets before they are transmitted over the web and after that collected in the right order at the destination address. So, it guarantees the solid transmission of data across the channel.
- **Internet Protocol:** The IP address tells the packets the address and route so that they reach the proper destination. It includes a strategy that empowers portal computers on the internet-connected to arrange forward the message after checking the IP address.
- **Reliability:** The most vital feature of TCP is solid data delivery. In arrange to supply unwavering quality, TCP must recover information that’s harmed, misplaced, copied, or conveyed out of arranging by the Arrange Layer.
- **Multiplexing:** Multiplexing can be achieved through the number of ports.
- **Connections:** Before application forms can send information by utilizing TCP, the devices must set up a connection. The associations are made between the harbor numbers of the sender and the collector devices.

TCP/IP Layers

- **Application Layer** An application layer is the topmost layer within the TCP/IP model. When one application layer protocol needs to communicate with another application layer, it forwards its information to the transport layer.
- **Transport Layer** It is responsible for the reliability, flow control, and correction of data that is being sent over the network. There are two protocols used in this layer are User Datagram Protocol and Transmission control protocol.
- **Internet/Network Layer** It is the third layer of the TCP/IP Model and also known as the Network layer. The main responsibility of this layer is to send the packets from any network, and they arrive at the goal irrespective of the route they take.
- **Network Access Layer** It is the lowest layer of the TCP/IP Model. It is the combination of the Physical Layer and the Data link layer which present in the OSI Model. Its main responsibility is to the transmission of information over the same network between two devices.

How TCP/ IP works?

- TCP/IP employs the client-server demonstration of communication in which a client or machine (a client) is given a benefit (like sending a webpage) by another computer (a server) within the network.
- Collectively, the TCP/IP suite of conventions is classified as stateless, which suggests each client request is considered new since it is irrelevant to past requests. Being stateless liberates up network paths so they can be utilized continuously.
- The transport layer itself, is stateful. It transmits a single message, and its connection remains open until all the packets in a message have been received and reassembled at the destination.
- The TCP/IP model differs from the seven-layer Open System Interconnection (OSI) model designed after it.

Application/Uses of TCP/IP

Some Real-Time Applications are:

- **Simple Mail Transfer Protocol(SMTP):** It helps to send email to another email address.
- **File Transfer Protocol(FTP):** It is used for sending large files.
- **Dynamic Host Configure Protocol(DHCP):** It assigns the IP address.
- **Telnet:** Bi-directional text communication via a terminal application.
- **HyperText Transfer Protocol(HTTP):** Used to transfer the web pages.
- **Domain Name System(DNS):** It translates the website name to IP addresses.
- **Simple Network Time Protocol(SNTP):** It provides the time of a day to the network devices.

Benefits of TCP/IP

- It is an **industry–standard demonstrate** that can be viably deployed in commonsense organizing problems.
- It is **interoperable**, i.e., it permits cross-platform communications among heterogeneous networks.
- It is an **open convention suite.** It isn’t claimed by any specific established and so can be utilized by any individual or organization.
- It may be **versatile, client-server engineering.** This permits systems to be included without disturbing the current services.
- It allots an **IP address to each computer on the organize,** hence making each device to be identifiable over the arrange. It allots each location a space title. It gives the title and addresses determination administrations.

Challenges of TCP/IP:

- It is **not generic in nature.** So, it comes up short to represent any protocol stack other than the TCP/IP suite. For the case, it cannot depict the Bluetooth connection.
- It does **not clearly isolate** the concepts of services, interfacing, and protocols. So, it isn’t appropriate to portray unused advances in modern networks.
- It does **not recognize between the data link and the physical layers,** which has exceptionally distinctive functionalities.
- The **information interface layer** ought to concern with the **transmission of outlines.** On the other hand, the physical layer ought to lay down the physical characteristics of the transmission.
- In this, model the transport layer does not guarantee delivery of packets.

Packet Filters:

- It works in the network layer of the OSI Model. It applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.
- Packet filter firewall controls access to packets on the basis of packet source and destination address or specific transport protocol type. It is done at the OSI (Open Systems Interconnection) data link, network, and transport layers. Packet filter firewall works on the network layer of the OSI model.
- Packet filters consider only the most basic attributes of each packet, and they don't need to remember anything about the traffic since each packet is examined in isolation. For this reason, they can decide packet flow very quickly.
- Example: Filter can be set to block all UDP segments and all Telnet connections. This type of configuration prevents outsiders from logging onto internal hosts using Telnet and insider from logging onto external hosts using Telnet connections.

Application Gateways:

- Application-level gateway is also called a bastion host. It operates at the application level. Multiple application gateways can run on the same host but each gateway is a separate server with its own processes.
- These firewalls, also known as application proxies, provide the most secure type of data connection because they can examine every layer of the communication, including the application data.
- Example: Consider FTP service. The FTP commands like getting the file, putting the file, listing files, and positioning the process at a particular point in a directory tree. Some system admin blocks put command but permits get command, list only certain files, or prohibit changing out of a particular directory. The proxy server would simulate both sides of this protocol exchange. For example, the proxy might accept get commands and reject put commands.

It works as follows:

Step-1: User contacts the application gateway using a TCP/IP application such as HTTP.

Step-2: The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.

Step-3: After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.

Packet filter	**Application-level**
Simplest	Even more complex
Screens based on connection rules	Screens based on behaviour or proxies
Auditing is difficult	Activity can audit
Low impact on network performance	High impact on network performance
Network topology can not hide	Network topology can hide from the attacker

Transparent to user	Not transparent to the user
See only addresses and service protocol type	Sees full data portion of a packet