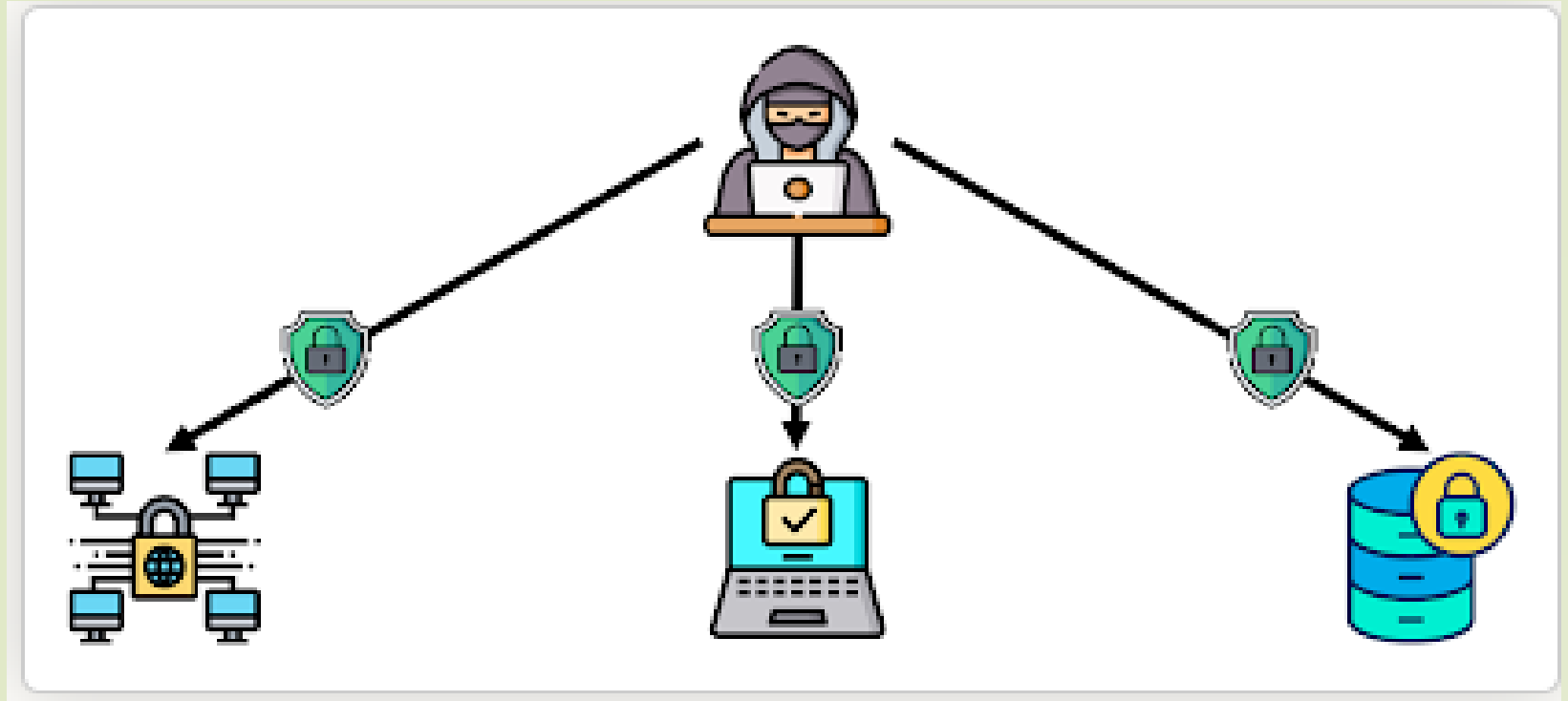


What is web security?

Web security refers to networks, computer system and data are protected from unauthorized person or group.



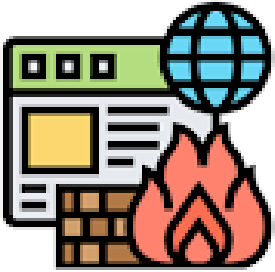


Purpose of Web Security

The purpose of web security is to prevent security attack like Passive attack and Active Attack.

Web security maintains the smooth operation of any business that uses computers and prevents hackers and malware from manipulating your systems, software, or network.

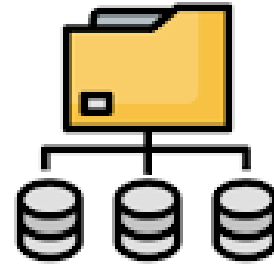
How can achieve Web



**Web & N/W
Firewall**



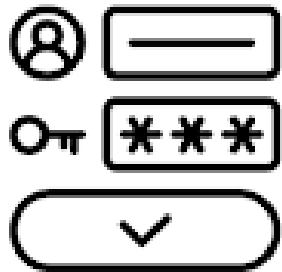
**Keep your S/W
Up to date**



**Backup
your data**



**Keep your
website clean**



**Strong
Password Policy**



**Password
Cracking Tools**



**Scan your website
for vulnerabilities**



**Use
Antivirus**

How can achieve Web Security?

- **Web & Network Firewall:** Web Application firewall sets between your website server and the data Connection. The purpose is to read every bit of data that passes through it and to protect your site.
- **Keep your software & plugins up to date:** If your website's s/w or applications are not up-to-date, your site is not secure. Updates are vital to the health and security of your website. Take all software and plugins update request seriously. Also use https and SSL Certificate to secure your website.
- **Backup your data:** Back up your site regularly. You should maintain backups of all your website files in case your site becomes inaccessible or your data is lost.



How can achieve Web Security?

- **Keep your website clean:** Every database, application or plugins on your website is another possible point of entry for hackers. You should delete any files, databases or applications from your website that are no longer in use.
- **Strong password policy:** It is important to use strong passwords to protect against brute force, password should be complex, containing uppercase and lowercase letters, numbers and special characters. Your password should be at least 10 characters long.



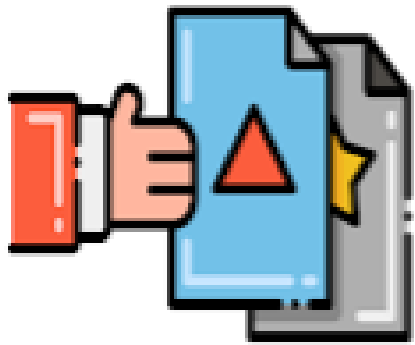
How can achieve Web Security?

- ➡ **Password cracking tools:** Password cracking tools help restore lost password, whether you have forgotten a password or your password has been hacked, a password Cracking tools can help you recover it.
 - ➡ **Scan your website for vulnerabilities:** It is important to regularly perform web security scans to check for website and server vulnerabilities. web security scans should be performed on a schedule and after any change or addition to your web Components.
- 

How can achieve Web Security?

- ➡ **Use of Antivirus:** Antivirus software helps protect your computer against malwares and other incoming threats. Antivirus software looks at data - like webpage, files, software applications – which are travelling over the network to your device. It searches for known threats and monitors the behavior of all programs and flagging suspicious behavior.

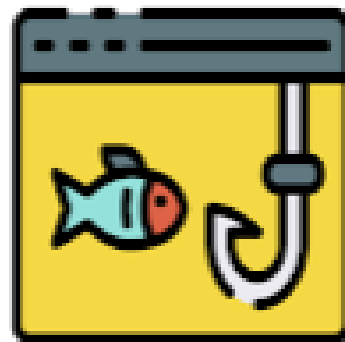
What are Web Security Threats?



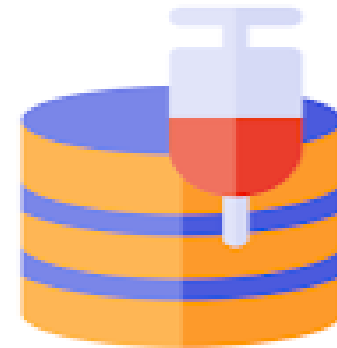
**Modification of
Message**



**Denial of
Services**



Phishing



SQL Injection



Malwares



What are Web Security Threats?

- **Modification of Message:** Message should not be altered during transmission it is also called as data breach. It means some confidential and sensitive information gets exposed. It is one kind of threat.
- **Denial of Services:** It is known as DDOS (Distributed Denial of Services). It is a web security threat that involves attackers flooding servers with large volumes of internet traffic to disrupt service and take websites offline. The sheer volume of fake traffic results in the target network or server being overwhelmed, which leaves them inaccessible.




What are Web Security Threats?

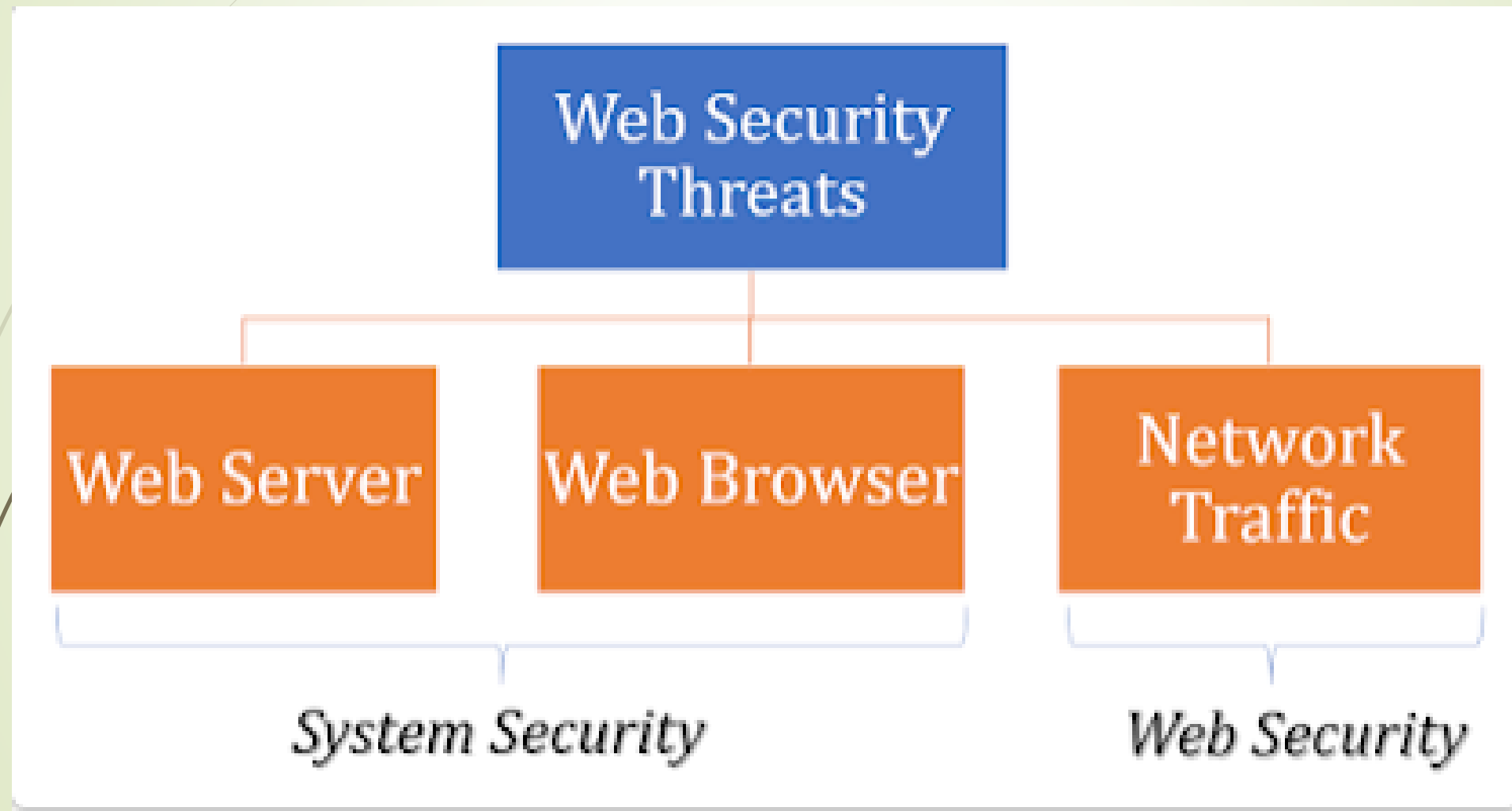
- **Phishing:** Phishing attack targeting users through email, text message or social media messaging sites. Attackers impersonate of real user or website, users can trust that link and click on given link and provide sensitive information like account number, credit/debit card data and login credentials. User Can lost their money, sensitive information etc.....
- **SQL Injection:** SQL stands for structured query language. SQL is used to search and query database. SQL Injection is a website security threats. SQL injection is the placement of malicious code in SQL statement, via webpage input. Using SQL injection hacker can retrieve credential and some sensitive information.



What are Web Security Threats?

- **Malware:** Malware stands for "Malicious Software". It is a file or code, typically delivered over a network, that infects, explores, steals or conduct virtually any behavior an attacker wants. Malware comes in so many variants, there are number of methods to infect computer systems.
- 

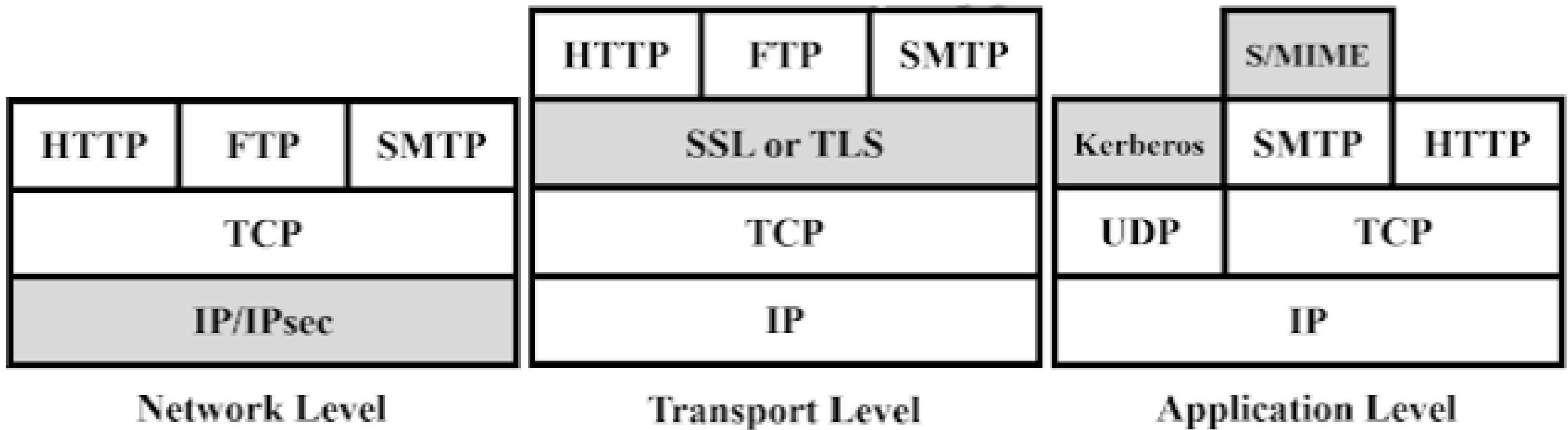
Classification of Web Security Threats



Web Security Threats

	Threats	Consequences	Countermeasures
Integrity	<ul style="list-style-type: none">• Modification of user data• Modification of memory• Modification of message traffic in transit	<ul style="list-style-type: none">• Loss of information• Compromise of machine• Vulnerability to all other threats	<ul style="list-style-type: none">• Cryptographic checksums
Confidentiality	<ul style="list-style-type: none">• Eavesdropping on the net• Theft of info from server• Theft of data from client• Info about network configuration• Info about which client talks to server	<ul style="list-style-type: none">• Loss of information• Loss of privacy	<ul style="list-style-type: none">• Encryption• Web proxies
Denial of Service	<ul style="list-style-type: none">• Killing of user threads• Flooding machine with bogus requests• Filling up disk or memory• Isolating machine by DNS attacks	<ul style="list-style-type: none">• Disruptive• Annoying• Prevent user from getting work done	<ul style="list-style-type: none">• Difficult to prevent
Authentication	<ul style="list-style-type: none">• Impersonation of legitimate users• Data forgery	<ul style="list-style-type: none">• Misrepresentation of user• Belief that false information is valid	<ul style="list-style-type: none">• Cryptographic techniques

Web Security Approaches





Web Security Approaches

- **Network Level:** One way to provide Web security is to use IP security (IPsec). The advantage of using IPsec is that it is transparent to end users and applications and provides a general-purpose solution. Furthermore, IPsec includes a filtering capability so that only selected traffic need incur the overhead of IPsec processing.




Web Security Approaches

- **Transport Level:** Another relatively general-purpose solution is to implement security just above TCP. The foremost example of this approach is the Secure Sockets Layer (SSL) and the follow-on Internet standard known as Transport Layer Security (TLS). At this level, there are two implementation choices. For full generality, SSL (or TLS) could be provided as part of the underlying protocol suite and therefore be transparent to applications. Alternatively, SSL can be embedded in specific packages. For example, Netscape and Microsoft Explorer browsers come equipped with SSL, and most Web servers have implemented the protocol.



Web Security Approaches

- **Application Level:** Application-specific security services are embedded within the particular application. The advantage of this approach is that the service can be tailored to the specific needs of a given application.
- 



Thank You