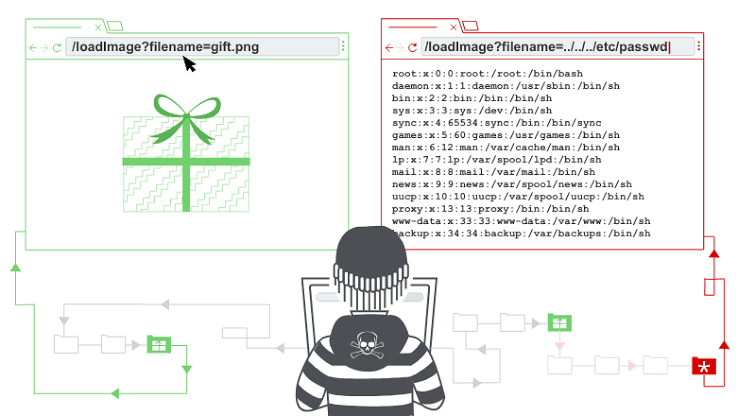
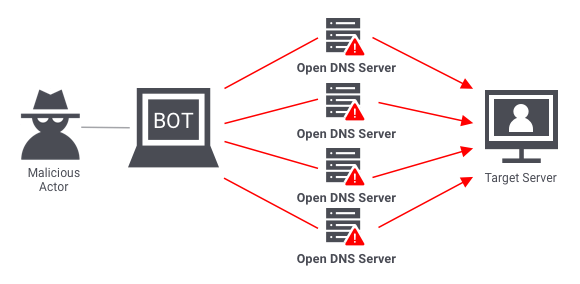
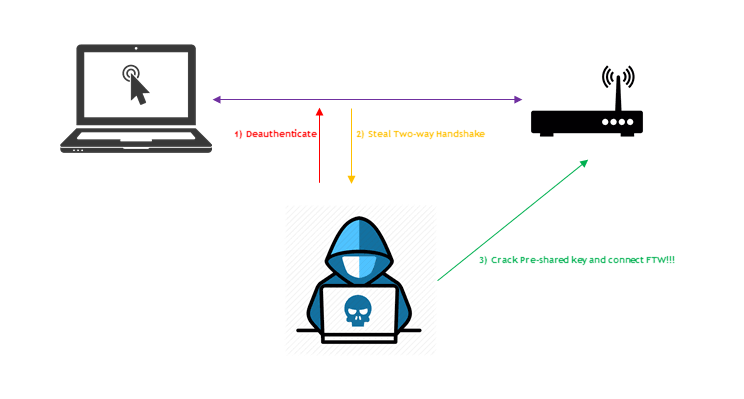
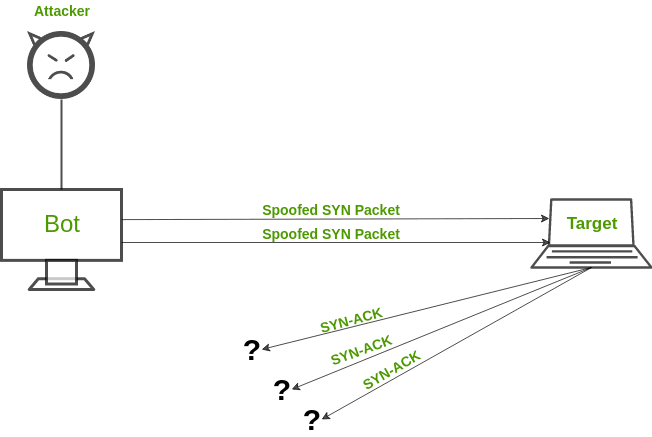
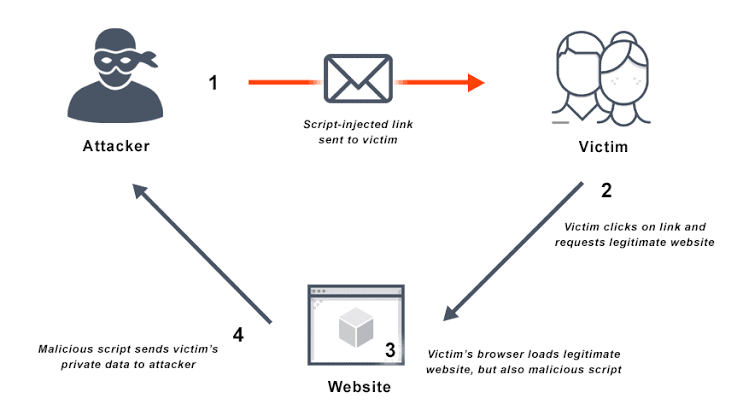
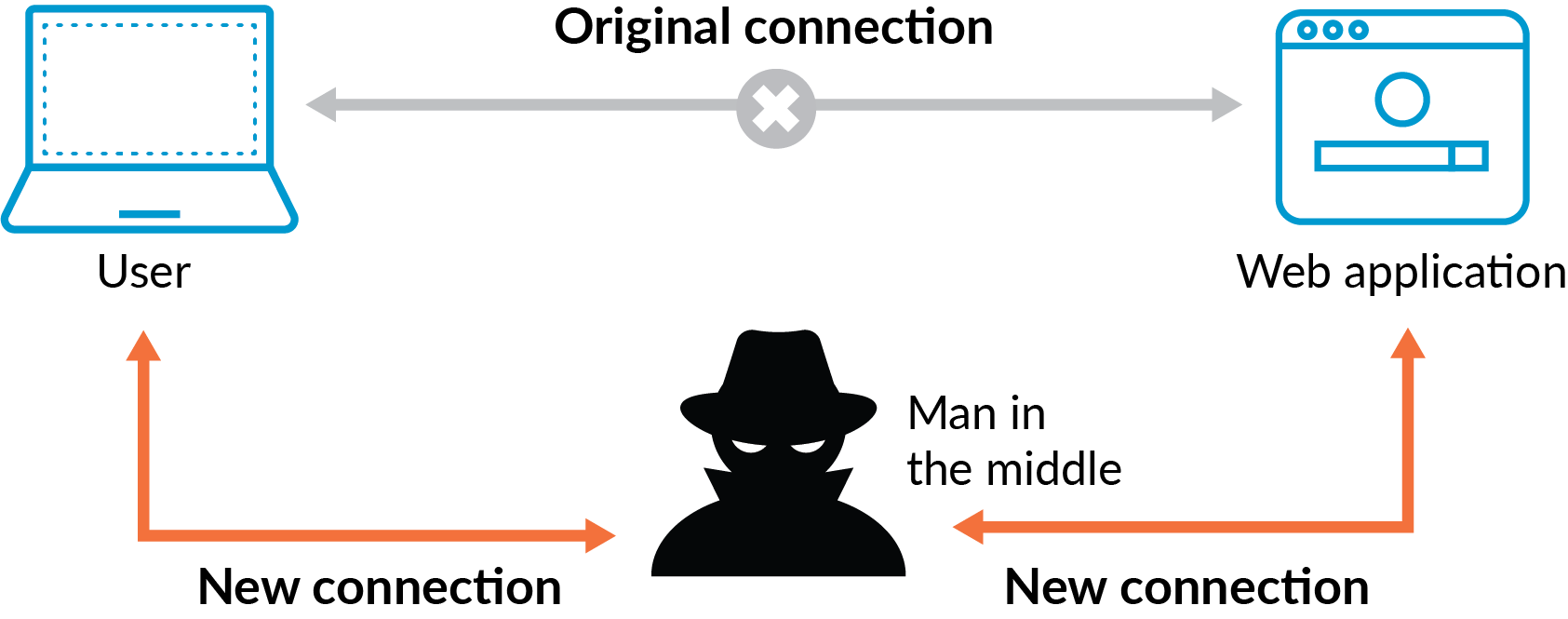
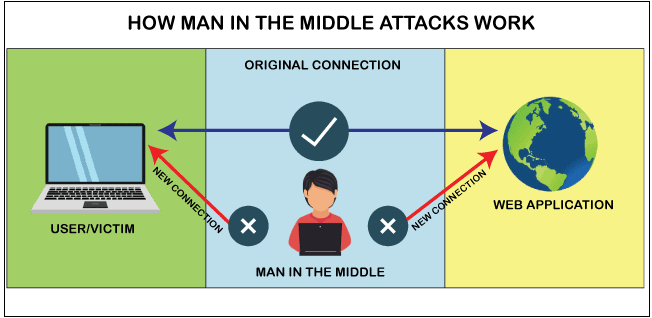
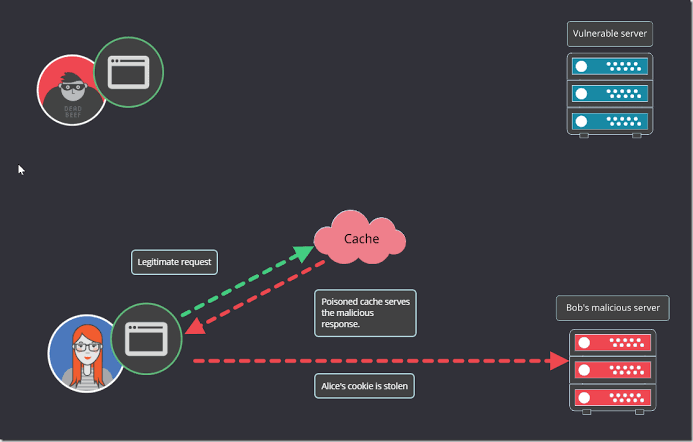
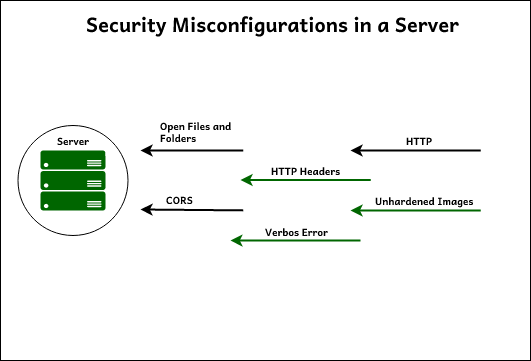
-> Understanding of web-server attacks :-

* 1.) Directory traversal :-
* Description : Directory traversal, also known as path traversal or directory climbing, is a vulnerability in a web application server caused by a HTTP exploit. The exploit allows an attacker to access restricted directories, execute commands, and view data outside of the web root folder where application content is stored.



* Business Impact :- When using this attack, the directory traversal can lead to unauthorized access of sensitive information stored in files outside of the web root directory. This could include: system files, configuration files, or even user data. The unauthorized access of confidential data is a direct breach of privacy and can lead to information theft.
* 2.) Denial-of-Service (DoS) :-
* Description: A DoS (denial-of-service) attack is a cyberattack that makes a computer or other device unavailable to its intended users. This is usually accomplished by overwhelming the targeted machine with requests until normal traffic can no longer be processed.
* 
* Business Impact :-It will cause financial losses , if the online shop or website goes offline, the company can quickly start to lose money as orders and requests can't be processed. In the worst case scenario, customers can be tempted away by competitors.Businesses may not be able to carry out time critical actions. They may suffer reputational damage. Customers may choose to use a competitor.
* 3.) Web Defacement Attack :-
* Description : In a Web Defacement Attack, the hacker gains access to the site and defaces it for a variety of reasons, including humiliation and discrediting the victim. The attackers hack into a web server and replace a website hosted with one of their own.
* 
* Business Impact :-It causes more downtime and damage to reputation. It can also involve several components of your IT environment, so some of your business processes can be impacted. That may result in loss of business opportunities. Failure to patch vulnerabilities might also result in something that you would certainly dread – a re-defacement
* 4.) SSH BRUTE FORCE ATTACK: -
* Description :By brute-forcing SSH login credentials, an SSH Brute Force Attack is performed to attain access. This exploit can be used to send malicious files without being noticed. Unlike a lot of other tactics used by hackers, brute force attacks aren’t reliant on existing vulnerabilities.
* 
* Business Impact :- Beyond the immediate loss, potential long-term ramifications may include damage to your company's reputation, loss of customer trust in your data protection protocols — and ultimately lack of trust in your brand.An SSH brute force attack exploits weak or default passwords that are commonly used on servers. These passwords can be easily guessed by attackers using common passwords lists and automated tools.
* 5.) CROSS SITE SCRIPTING (XSS): -
* Description : This type of attack is more likely to target websites with scripting flaws. The injection of malicious code into web applications is known as Cross-Site Scripting. The script will give the hacker access to web app data such as sessions, cookies, and so on.
* 
* Business Impact :- If successful, a cross site scripting attack can severely impact websites and web applications, damage their reputation and relationships with customers. XXS can deface websites, can result in compromised user accounts, and can run malicious code on web pages, which can lead to a compromise of the user's device.
* 6.) DNS SERVER HIJACKING: -
* Description : DNS Hijacking refers to any attack that tricks the end-user into thinking he or she is communicating with a legitimate domain name when in reality they are communicating with a domain name or IP address that the attacker has set up. DNS Redirection is another name for this.
* 
* Business Impact :- Domain Name System (DNS) hijacking is a serious threat to your system and can have very costly consequences. As the attack enables a malicious third party to take over the DNS settings and reroute users to fraudulent websites, this can affect a variety of different users.It is also resulting in the shutdown of cloud and on-premise applications and theft of data.
* 7.) MITM ATTACK :-
* Description : Man-in-the-Middle (MITM) attack allows the attacker to access sensitive information by blocking and modifying the connection between the end-user and web servers. In MITM attacks or smells, the hacker captures or corrects modified messages between the user and the web server by listening or intervening in the connection. This allows the attacker to steal sensitive user information such as online banking details, usernames, passwords, etc., which are transmitted online to the webserver. The attacker entices the victim to attach to an Internet server by pretending to be an agent.
* 
* Business Impact :- Once a criminal has this information, they can manipulate account credentials, steal funds, or make unauthorized purchases. Because of its scope, MITM attackers often target banking, online retailers, and software-as-a-service (SaaS) platform customers.
* 8.) HTTP RESPONSE SPLITTING ATTACK :-
* Description : HTTP Response Splitting is a protocol manipulation attack, similar to Parameter Tampering. Only programs that use HTTP to exchange data are vulnerable to this attack. Because the entry point is in the user viewable data, it works just as well with HTTPS. The attack can be carried out in a variety of ways.
* 
* Business Impact :- As HTTP Response Splitting can be used to manipulate and poison the web application's HTTP response headers, this could potentially lead to a range of different impacts, such as session hijacking, data theft, or the injection of malicious code into a victim's browser.
* 9.) DNS Amplification attacks :-
* Description : DNS amplification is a Distributed Denial of Service (DDoS) attack in which the attacker exploits vulnerabilities in domain name system (DNS) servers to turn initially small queries into much larger payloads, which are used to bring down the victim's servers.
* 
* Business Impact :- DNS amplification attacks generally relay DNS requests through one or more botnets – drastically increasing the volume of traffic directed at the targeted server or servers, and making it much harder to trace the attacker's identity.
* 10.)Web server Misconfiguration :-
* Description : Server Misconfiguration attacks exploit configuration weaknesses found in web servers and application servers. Many servers come with unnecessary default and sample files, including applications, configuration files, scripts, and web pages.
* 
* Business Impact :- A Server misconfigurations allow attackers to gain unauthorized access to networks, systems and data, which in turn can cause significant monetary and reputational damage to your organization. Server misconfigurations can lead to different types of cyberattacks, such as data theft, ransomware attacks, denial-of-service attacks, and malware infections. Cybercriminals exploit misconfigured systems and applications to gain unauthorized access, steal sensitive data, or disrupt business operations.