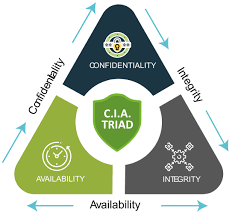
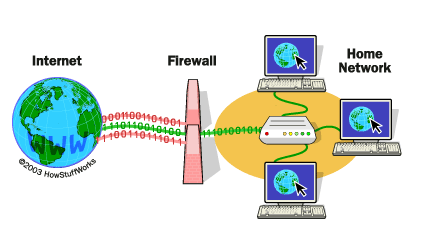
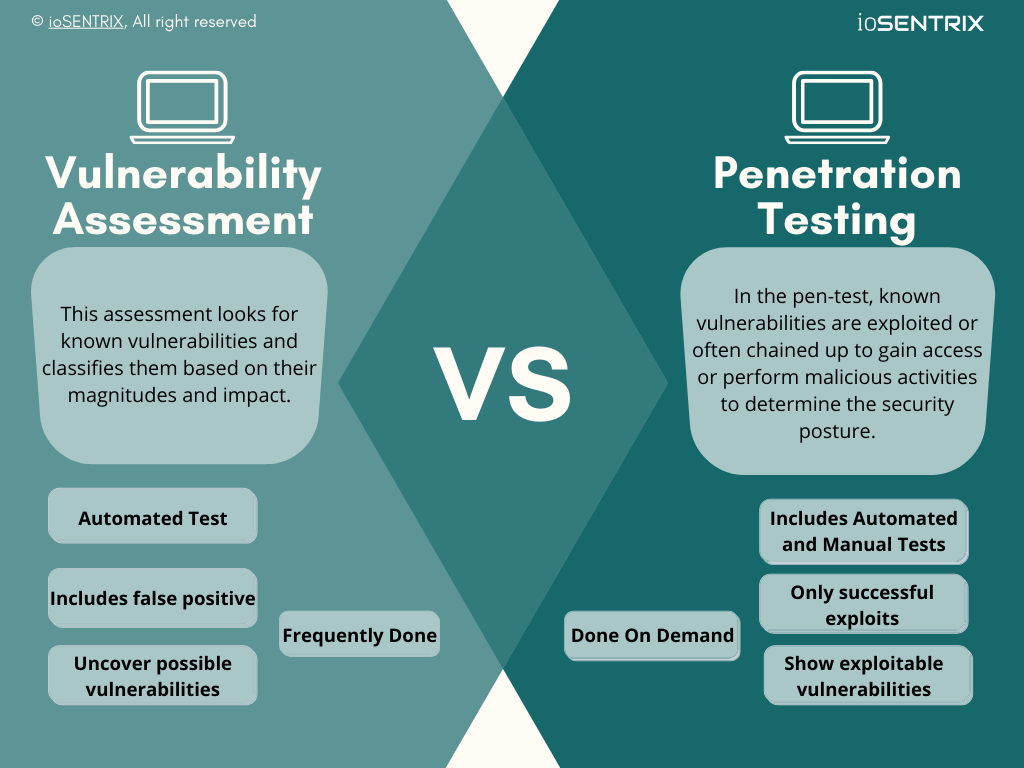
1. ***Term - 4 ====&Gt; Ech - Introduction To Ethical Hacking***
2. **Explain CIA Triad:**
   1. The CIA Triad is a cornerstone of cybersecurity, representing the three essential principles required to protect data:
   2. **Confidentiality:** Ensures that sensitive information is accessible only to authorized individuals. It involves measures like encryption, access controls, and authentication to prevent unauthorized access.
   3. **Integrity:** Ensures that data remains accurate, consistent, and unaltered during storage or transmission. Hashing and digital signatures are commonly used to verify integrity.
   4. **Availability:** Ensures that systems, applications, and data are accessible to authorized users whenever needed. This involves redundancy, fault tolerance, and protection against denial-of-service attacks.



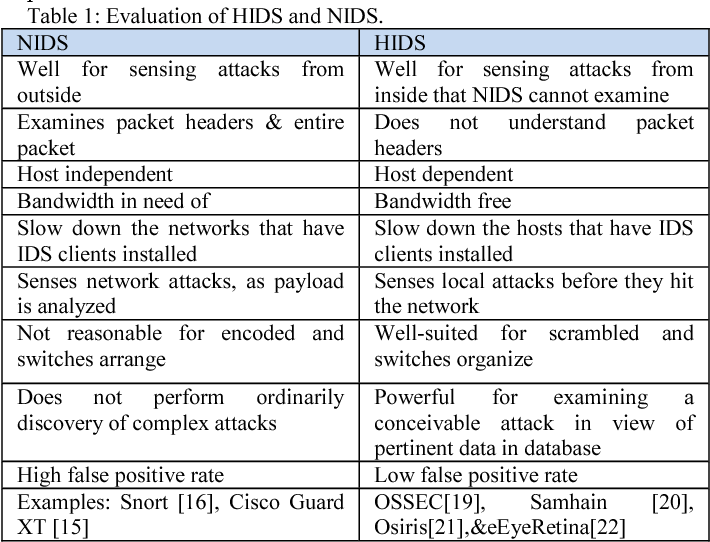
1. **What is a Firewall and Why is it Used?**
   1. A firewall is a network security device or software that monitors and controls incoming and outgoing traffic based on predefined security rules. Firewalls are used to:
   2. Block unauthorized access to a network.
   3. Prevent malicious traffic from entering or leaving the network.
   4. Act as a barrier between internal networks and untrusted external networks, such as the internet.



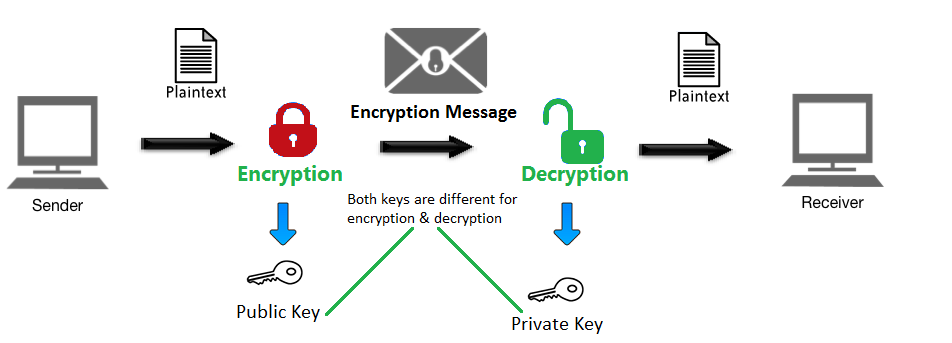
1. **Difference Between VA (Vulnerability Assessment) and PT (Penetration Testing):**
   1. **Vulnerability Assessment (VA):** Focuses on identifying, classifying, and prioritizing vulnerabilities in a system, network, or application. It involves scanning tools and is non-intrusive.
   2. **Penetration Testing (PT):** Simulates real-world attacks to exploit vulnerabilities and assess the security posture of systems. It involves active attempts to breach defenses and requires skilled professionals.



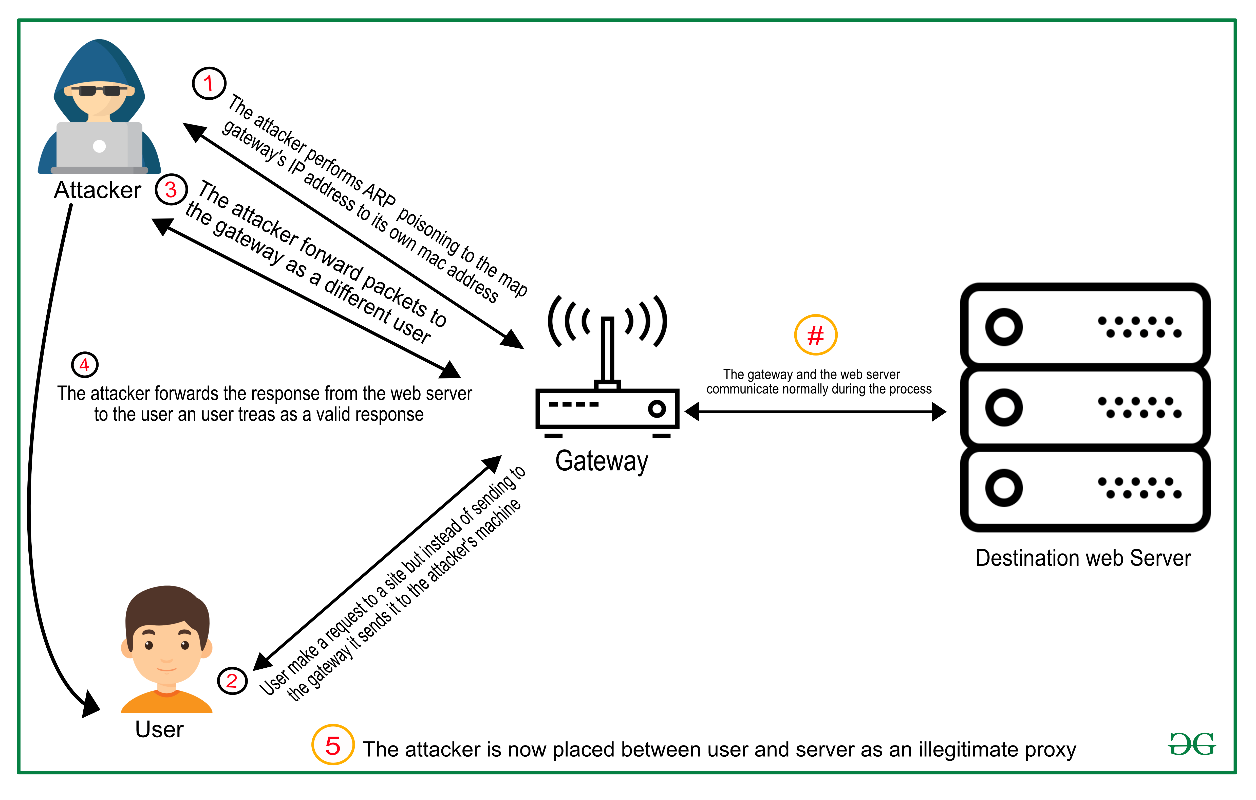
1. **Difference Between HIDS and NIDS:**
   1. **HIDS (Host-based Intrusion Detection System):** Monitors activities on individual hosts or devices, such as file modifications, system logs, and user activity. It provides detailed, host-specific insights.
   2. **NIDS (Network-based Intrusion Detection System):** Monitors network traffic to detect suspicious activities or potential threats across the entire network. It focuses on patterns, anomalies, and signatures in network packets.



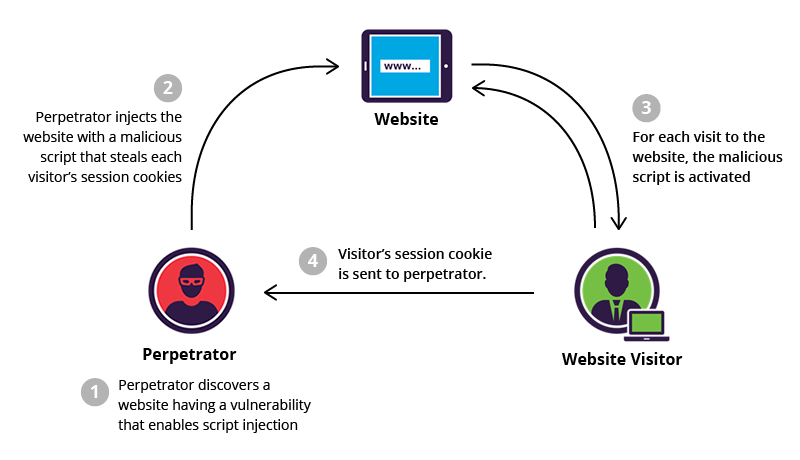
1. **Explain SSL Encryption:**
   1. SSL (Secure Sockets Layer) is a protocol that encrypts data transmitted between a client (e.g., browser) and a server. It ensures:
   2. Data confidentiality: Preventing unauthorized access.
   3. Data integrity: Protecting data from being altered during transmission.
   4. Authentication: Verifying the server's identity. Though SSL is now deprecated, its successor, TLS (Transport Layer Security), is widely used for secure communication.



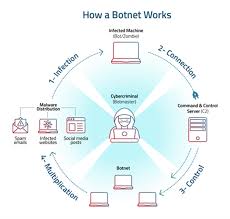
1. **What is Data Leakage?**
   1. Data leakage occurs when sensitive or confidential information is unintentionally or maliciously exposed to unauthorized parties. It can result from human error, insider threats, or cyberattacks. Examples include sharing sensitive files over unsecured channels or sending emails to the wrong recipients.
2. **What is a Brute Force Attack? How Can You Prevent It?**
   1. A brute force attack is a trial-and-error method where an attacker systematically guesses passwords or encryption keys until access is gained. Preventative measures include:
   2. **Account lockout policies:** Temporarily disabling accounts after multiple failed attempts.
   3. **Strong passwords:** Using complex, lengthy passwords with a mix of characters.
   4. **Multi-factor authentication (MFA):** Adding an extra layer of security.
   5. **Rate limiting:** Restricting the number of login attempts within a specific timeframe.
3. **Explain MITM Attack and How to Prevent It:**
   1. A Man-in-the-Middle (MITM) attack occurs when an attacker intercepts and manipulates communication between two parties without their knowledge. It is used to steal sensitive data or inject malicious content. Prevention strategies include:
   2. Using HTTPS with SSL/TLS encryption.
   3. Avoiding untrusted or public Wi-Fi networks or using Virtual Private Networks (VPNs).
   4. Implementing mutual authentication mechanisms.



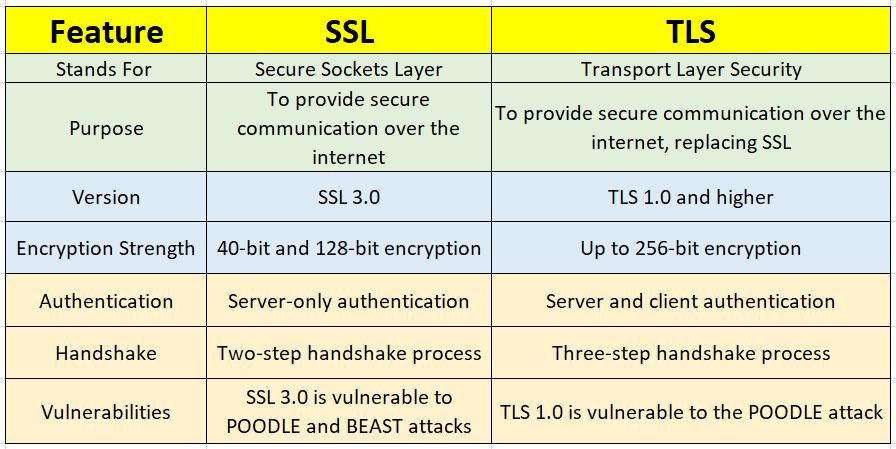
1. **Explain XSS Attack and How to Prevent It:**
   1. Cross-Site Scripting (XSS) is a vulnerability where attackers inject malicious scripts into trusted websites. It can be used to steal session cookies, redirect users, or deface websites. Prevention measures include:
   2. Input validation and output sanitization to filter malicious code.
   3. Encoding special characters to prevent script execution.
   4. Implementing Content Security Policies (CSPs) to restrict scripts from unauthorized sources.



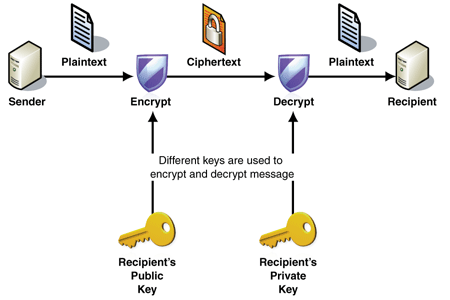
1. **What is a Botnet?**
   1. A botnet is a network of compromised devices (bots) controlled by an attacker to perform coordinated tasks. These tasks can include Distributed Denial of Service (DDoS) attacks, spam distribution, or cryptocurrency mining. Botnets are created by infecting devices with malware and exploiting them remotely.



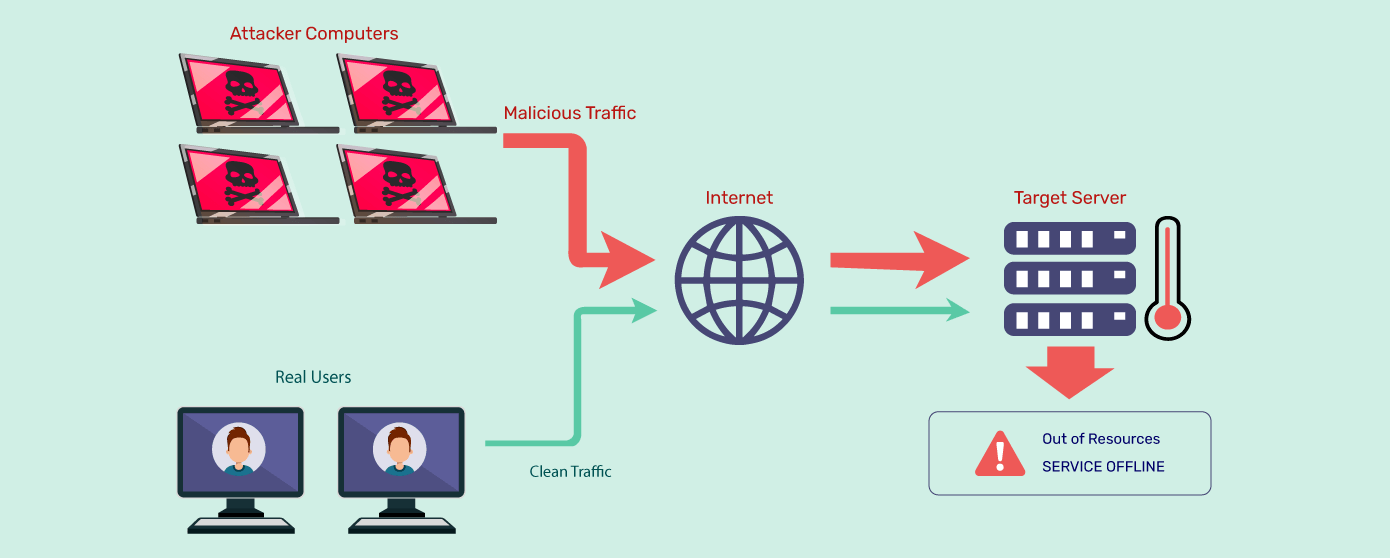
1. **Explain SSL and TLS:**
   1. **SSL (Secure Sockets Layer):** An older encryption protocol used to secure internet communications. It has known vulnerabilities and is no longer in use.
   2. **TLS (Transport Layer Security):** A more secure and modern version of SSL, providing enhanced encryption, authentication, and data integrity.



1. **Define Virus, Malware, and Ransomware:**
   1. **Virus:** A type of malicious software that spreads by attaching itself to files or programs and requires user interaction to propagate.
   2. **Malware:** A broad term for malicious software, including viruses, worms, Trojans, spyware, and ransomware, designed to harm or exploit systems.
   3. **Ransomware:** A type of malware that encrypts a victim's data and demands a ransom payment to restore access.
2. **What is Phishing? Provide an Example:**
   1. Phishing is a social engineering attack where attackers impersonate legitimate entities to trick victims into revealing sensitive information, such as passwords or credit card numbers. Example: A fake email claiming to be from a bank, asking users to click a link and update their account details.
3. **Define Encryption and Decryption:**
   1. **Encryption:** The process of converting plaintext into ciphertext to secure data from unauthorized access.
   2. **Decryption:** The process of converting ciphertext back into plaintext to make the data readable again.



1. **What is a DDoS Attack and How Does It Work?**
   1. A Distributed Denial of Service (DDoS) attack aims to overwhelm a server, network, or website by flooding it with excessive traffic from multiple sources (often a botnet). This disrupts normal operations, making services unavailable to legitimate users. DDoS attacks are mitigated through load balancing, firewalls, and traffic filtering.



1. **What is a Zero-Day Vulnerability?**
   1. A zero-day vulnerability is a software flaw that is unknown to the vendor and the public. Attackers exploit these vulnerabilities before a patch is released, making them highly dangerous. Organizations mitigate risks by using proactive security measures, like threat intelligence and intrusion detection systems.
2. **What is Network Sniffing?**
   1. Network sniffing involves capturing and analyzing network traffic to monitor data flow. While often used for legitimate purposes (e.g., network troubleshooting), it can also be used maliciously to intercept sensitive data like passwords and emails. Preventative measures include encryption and secure communication protocols.
3. **What is a Security Operations Center (SOC)?**
   1. A SOC is a centralized facility where a team of security professionals monitors, detects, analyzes, and responds to cybersecurity incidents in real-time. SOCs play a critical role in ensuring an organization’s IT infrastructure remains secure and compliant.



1. **Importance of Forensics in Cybersecurity:**
   1. Forensics is vital in identifying, analyzing, and mitigating cyber incidents. It helps:
   2. Determine the root cause of a breach.
   3. Collect evidence for legal proceedings.
   4. Identify vulnerabilities and attack vectors.
   5. Improve future security measures through post-incident analysis.
2. **Discuss the future trends in cyber security. Which skills are** 
   1. **important for cyber security professionals?**
   2. Future Trends in Cybersecurity:
   3. AI and Machine Learning Integration: AI-driven tools are being used to detect and mitigate threats in real-time. For example, systems like IBM Watson for Cyber Security can analyze massive datasets to predict attacks.
   4. Zero Trust Architecture: More organizations are adopting zero trust policies where no user or device is trusted by default.
   5. Cloud Security: As businesses migrate to the cloud, securing cloud-based systems has become critical.
   6. IoT Security: The rise of IoT devices increases vulnerabilities. For example, weakly secured smart home devices can be exploited as entry points for attacks.
   7. Quantum Computing: While quantum computers promise breakthroughs, they can also break current encryption methods.
   8. Important Skills:
   9. Network Security: Understanding firewalls, VPNs, and IDS/IPS systems.
   10. Penetration Testing: Identifying vulnerabilities and testing defenses. Tools like Metasploit or Burp Suite are commonly used.
   11. Forensics and Incident Response: Investigating breaches and implementing recovery plans.
   12. Programming Skills: Knowledge of languages like Python for scripting and automation.
   13. Awareness of Compliance Standards: Understanding regulations like GDPR, HIPAA, and ISO 27001.
3. **What is the difference between IDS and IPS?**
   1. IDS (Intrusion Detection System):
   2. Definition: Monitors network traffic for suspicious activity and alerts administrators.
   3. Example: If unusual login attempts are detected from different locations, the IDS logs it and sends an alert.
   4. Key Feature: Passive system; it doesn't block the activity.
   5. IPS (Intrusion Prevention System):
   6. Definition: Monitors traffic like IDS but actively blocks identified threats.
   7. Example: If a SQL injection attempt is detected, the IPS blocks the malicious query in real-time.
   8. Key Feature: Active system; it prevents the activity from occurring.
   9. Main Difference: IDS focuses on detection and reporting, while IPS takes action to stop the threats.

