T.Y.B.Sc. (CS) Sem VI Ethical Hacking Question Bank

Unit 1

1) What is hacking also explain what are hacker classes in short.

Ans:-
Hacking refers to the unauthorized access, manipulation, or exploitation of computer systems, networks, or data.
It can involve a variety of activities, including breaking into systems, stealing information, disrupting services, or causing damage.

White Hat Hackers: Also known as ethical hackers, they use their skills to improve security by identifying vulnerabilities in systems and networks. They work with organizations to strengthen their defenses and protect against cyber threats.

Black Hat Hackers: These hackers engage in illegal activities for personal gain, such as stealing data, spreading malware, or causing harm to systems and networks. They are motivated by financial gain, personal vendettas, or ideological reasons.

Grey Hat Hackers: Grey hats fall somewhere between white hats and black hats. They may perform activities without authorization, but not necessarily for malicious purposes. For example, they might uncover vulnerabilities in systems and networks without permission but then disclose them to the owners.

Script Kiddies: These are amateur hackers who lack technical expertise and rely on pre-written scripts or tools to carry out attacks. They typically don't fully understand the technology behind their actions and may cause damage without realizing the consequences.

Hacktivists: Hacktivists are motivated by social or political causes and use hacking techniques to promote their agendas. They may target government agencies, corporations, or other organizations to protest or raise awareness about issues they care about.

State-Sponsored Hackers: These hackers operate on behalf of governments and intelligence agencies. They conduct cyber espionage, gather intelligence, or carry out cyber attacks against other countries, organizations, or individuals to further their nation's interests.

2) Explain the types of Ethical Hacking

Ans:

Network Penetration Testing: This involves assessing the security of a network infrastructure, including routers, switches, firewalls, and other network devices. Ethical hackers attempt to exploit vulnerabilities in the network to gain unauthorized access or extract sensitive information.

Web Application Testing: Web applications are often vulnerable to various attacks, such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms. Ethical hackers assess the security of web applications by attempting to exploit these vulnerabilities and gain access to sensitive data or perform unauthorized actions.

Wireless Network Testing: Wireless networks, including Wi-Fi and Bluetooth, are susceptible to attacks such as eavesdropping, spoofing, and unauthorized access. Ethical hackers assess the security of wireless networks by attempting to exploit vulnerabilities in encryption protocols, authentication mechanisms, and network configurations.

Social Engineering: Social engineering involves manipulating individuals to divulge confidential information or perform actions that compromise security. Ethical hackers use social engineering techniques, such as phishing emails, pretexting, and impersonation, to test the susceptibility of employees to social engineering attacks and raise awareness about security risks.

Physical Security Testing: Physical security testing involves assessing the security of physical premises, such as offices, data centers, and server rooms. Ethical hackers attempt to bypass physical security measures, such as locks, access control systems, and surveillance cameras, to gain unauthorized access to sensitive areas or assets.

IoT (Internet of Things) Security Testing: With the proliferation of IoT devices, securing these devices and their ecosystems is crucial. Ethical hackers assess the security of IoT devices, such as smart home devices, industrial sensors, and medical devices, by identifying vulnerabilities in firmware, communication protocols, and access controls.

Red Team Exercises: Red team exercises simulate real-world cyber attacks to test an organization's detection and response capabilities. Ethical hackers, acting as adversaries, attempt to breach the organization's defenses, escalate privileges, and exfiltrate sensitive data. These exercises help organizations identify weaknesses in their security posture and improve incident response procedures.

3) Explain Hacking Technology and its types in detail

Ans: **As Refer que no 1 same ans he**

4) What are the phases to understand Ethical Hacking explain it in detail

Ans:

Understanding ethical hacking involves following a structured approach to identify, assess, and mitigate security vulnerabilities in systems, networks, or applications. This process typically consists of several phases, each designed to provide insights into the security posture of the target environment. Here are the phases of ethical hacking explained in detail:

Reconnaissance (Information Gathering):
Gathering information about the target system or network.
Collecting publicly available data, such as domain names, IP addresses, and employee information.
Conducting passive reconnaissance to avoid detection.

Scanning:
Scanning the target system or network for open ports, running services, and vulnerabilities.
Using tools like Nmap to identify potential entry points.

Identifying weaknesses that could be exploited in the next phase.

Gaining Access:
Exploiting vulnerabilities identified during scanning to gain unauthorized access.
Using techniques like SQL injection, buffer overflows, or exploiting weak credentials.
Leveraging exploits or malware to compromise systems.

Maintaining Access:
Establishing persistent access to the compromised system or network.
Installing backdoors or rootkits to maintain control.
Avoiding detection by security mechanisms or administrators.

Covering Tracks:
Erasing evidence of the intrusion to evade detection.
Deleting log files, modifying timestamps, and cleaning up system artifacts.
Covering tracks to maintain anonymity and avoid attribution.

Reporting:
Documenting the findings of the ethical hacking exercise.
Reporting vulnerabilities, exploits, and compromised systems to the appropriate stakeholders.
Providing recommendations for improving security and mitigating risks.

5) Define Hacktivism and explain ways to manifest it

Ans:

Hacktivism is the act of using hacking techniques and technology to promote social or political causes. It involves using digital tools to carry out online protests, raise awareness, or enact social change. Here are some ways hacktivism can manifest:

Website Defacement: Hacktivists may deface websites by altering the content, images, or layout to convey a message or protest. This could involve replacing the homepage with a statement or manifesto related to their cause.

Distributed Denial of Service (DDoS) Attacks: Hacktivists may launch DDoS attacks against websites or online services to disrupt their operations. By overwhelming servers with traffic, they can temporarily render websites inaccessible to users.

Data Leaks and Exposures: Hacktivists may leak confidential or sensitive information to expose wrongdoing or corruption. This could involve releasing private emails, documents, or databases that shed light on unethical or illegal activities.

Social Media Campaigns: Hacktivists may use social media platforms to spread their message and organize protests or boycotts. They may create viral hashtags, memes, or videos to raise awareness and mobilize support for their cause.

Hacking and Defacement of Social Media Accounts: Hacktivists may gain unauthorized access to social media accounts belonging to individuals or organizations associated with their cause. They may then use these accounts to post messages, images, or videos that promote their agenda.

Online Petitions and Activism Websites: Hacktivists may create online petitions or activism websites to collect signatures, organize events, and coordinate grassroots

movements. These platforms serve as hubs for like-minded individuals to connect and take action.

Cyber Espionage and Sabotage: In more extreme cases, hacktivists may engage in cyber espionage or sabotage against governments, corporations, or organizations perceived as adversaries. This could involve stealing classified information, disrupting critical infrastructure, or causing financial harm.

6) Explain any five hacker classes

Ans: **Refer the Qno 1**

7) What are the skills required for becoming an Ethical Hacker

Ans:

Understanding of Computer Networks: Knowledge of computer networks, including TCP/IP protocols, routing, switching, and network architecture, is fundamental for understanding how data flows across systems and networks.

Proficiency in Operating Systems: A strong understanding of operating systems like Windows, Linux, and Unix is necessary for identifying vulnerabilities, configuring systems securely, and conducting penetration testing.

Programming Skills: Proficiency in programming languages like Python, Perl, or Ruby is essential for developing custom scripts and tools, automating tasks, and understanding the inner workings of software and systems.

Cybersecurity Concepts: Familiarity with cybersecurity principles, such as encryption, authentication, access control, and secure coding practices, is crucial for assessing security controls and identifying vulnerabilities.

Vulnerability Assessment and Penetration Testing (VAPT): Skills in conducting vulnerability assessments, penetration testing, and ethical hacking techniques are necessary for identifying and exploiting security vulnerabilities in systems, networks, and applications.

Ethical and Legal Understanding: A strong ethical mindset and understanding of legal and regulatory frameworks governing cybersecurity are essential for conducting ethical hacking activities responsibly and within the bounds of the law.

Problem-Solving Skills: The ability to think critically, analyze complex systems, and solve problems creatively is essential for identifying security weaknesses and devising effective countermeasures.

Continuous Learning and Adaptability: The field of cybersecurity is constantly evolving, so a willingness to stay updated with the latest security trends, tools, and techniques is crucial for remaining effective as an ethical hacker.

Communication Skills: Effective communication skills, both written and verbal, are essential for documenting findings, presenting reports to stakeholders, and collaborating with team members effectively.

Attention to Detail: Ethical hackers must pay close attention to detail when analyzing systems for vulnerabilities, as even small oversights can lead to security breaches.

8) Define vulnerability research and several key

Ans:

Vulnerability research involves the process of discovering, analyzing, and understanding security vulnerabilities in software, hardware, or systems. The goal of vulnerability research is to identify weaknesses that could be exploited by malicious actors to compromise the confidentiality, integrity, or availability of information or systems. Here are several key aspects of vulnerability research:

Discovery: Vulnerability researchers actively search for vulnerabilities by examining software, systems, protocols, and devices for potential weaknesses. This may involve analyzing source code, reverse engineering binaries, or probing network communications.

Analysis: Once a potential vulnerability is discovered, researchers analyze its root cause, impact, and potential exploitation scenarios. This often involves understanding the underlying technology, architecture, and security mechanisms involved.

Proof of Concept (PoC): Researchers develop proof-of-concept exploits or demonstrations to validate the existence and severity of vulnerabilities. These PoCs demonstrate how an attacker could exploit the vulnerability to gain unauthorized access or compromise system integrity.

Documentation: Detailed documentation of vulnerabilities is crucial for effective communication with vendors, developers, and the cybersecurity community. Researchers document their findings, including vulnerability descriptions, risk assessments, and mitigation recommendations, in reports or advisories.

Responsible Disclosure: Ethical vulnerability researchers follow responsible disclosure practices when reporting vulnerabilities to vendors or affected parties. This involves notifying the vendor of the vulnerability, allowing them time to develop and release patches or mitigations before publicly disclosing details of the vulnerability.

Collaboration and Community Engagement: Vulnerability research often benefits from collaboration within the cybersecurity community. Researchers may share findings, collaborate on vulnerability analysis, or contribute to open-source security projects to advance knowledge and improve security for all.

Continuous Learning and Adaptation: The field of vulnerability research is dynamic, with new technologies, attack vectors, and mitigation techniques emerging regularly. Researchers must stay updated with the latest developments, tools, and techniques to remain effective in their work.

Legal and Ethical Considerations: Vulnerability researchers must adhere to legal and ethical guidelines when conducting research. This includes obtaining proper authorization before testing systems, respecting intellectual property rights, and avoiding unauthorized access or data breaches.

9) What are the ways to conduct Ethical Hacking

Ans: **Refer Qno2**

10) Define Footprinting and its types

Ans1:

Footprinting is the process of gathering information about a target system, network, or organization to gather intelligence for the purpose of planning a cyber attack. It involves systematically collecting data from various sources to understand the target's infrastructure, technology stack, personnel, and other relevant information. Footprinting helps attackers identify potential entry points, vulnerabilities, and attack vectors. Here are the types of footprinting:

Passive Footprinting: Passive footprinting involves gathering information without directly interacting with the target system or network. This typically includes collecting publicly available data from sources such as websites, social media profiles, news articles, public records, and internet archives. Passive footprinting aims to avoid detection by the target and is often the first step in reconnaissance.

Active Footprinting: Active footprinting involves directly interacting with the target system or network to gather information. This may include conducting network scans, port scans, DNS queries, traceroute analysis, and other probing techniques to discover live hosts, open ports, and network topology. Active footprinting may raise alarms on intrusion detection systems and is generally riskier than passive footprinting.

External Footprinting: External footprinting focuses on gathering information about the target system or organization from external sources, such as the internet, public databases, and third-party services. This includes identifying domain names, IP addresses, email addresses, and other publicly accessible information related to the target.

Internal Footprinting: Internal footprinting involves gathering information about the target system or organization from internal sources, such as employees, partners, or contractors. This may include social engineering tactics, physical reconnaissance, dumpster diving, or other methods to obtain insider information about the target's infrastructure, security policies, and personnel.

11) Explain the methods to perform Information Gathering

Ans:

There are the following three methods of information gathering:

Footprinting
Scanning
Enumeration

Footprinting
In this technique, the information of a target network or system or victim is collected as much as possible. Footprinting provides various ways to intrude on the system of an organization. The security posture of the target is also determined by this technique. It can be active as well as passive. In Passive footprinting, the information of any user is collected without knowing him. If the user's sensitive information gets released intentionally and consciously or by the direct contact of the owner, active footprinting will

be created.

Scanning: Network scanning involves probing a target network to discover active hosts, open ports, and services running on those ports. Tools like Nmap are commonly used for network scanning, providing detailed information about the network infrastructure.

Enumeration: Enumeration involves extracting additional information about the target network, such as usernames, group memberships, and shares. This process can be performed using tools like enum4linux for Windows systems or rpcenum for UNIX systems.

Social Engineering: Social engineering techniques involve manipulating individuals to divulge sensitive information. This can include pretexting, phishing emails, or even physically entering a facility and gaining unauthorized access.

Packet Sniffing: Packet sniffing involves capturing and analyzing network traffic to gather information about network communications. Tools like Wireshark allow for the interception and analysis of packets, revealing valuable insights about network architecture and potential vulnerabilities.

DNS Interrogation: DNS interrogation involves querying DNS servers to gather information about domain names, IP addresses, and network services. Tools like nslookup or dig can be used to perform DNS queries and gather information about a target domain.

Web Scraping: Web scraping involves automatically extracting data from websites. This can include information about web servers, directories, files, and potentially sensitive information inadvertently exposed on web pages.

Vulnerability Scanning: Vulnerability scanning involves using automated tools to identify weaknesses in target systems or networks. Tools like Nessus or OpenVAS scan for known vulnerabilities in software and configurations, providing a list of potential security issues.

Dumpster Diving: Dumpster diving involves physically searching through trash or recycling bins to find discarded documents or electronic devices containing sensitive information. This method can yield valuable information such as passwords, network diagrams, or confidential documents.

Social Media Analysis: Analyzing social media profiles and posts can provide insights into an organization's employees, activities, and potential security risks. Information such as employee names, job titles, and relationships can be gathered from platforms like LinkedIn, Facebook, or Twitter.

12) What are the competitive Intelligence in Ethical Hacking

Ans:

Competitive intelligence in ethical hacking involves gathering information about competitors' security posture, technologies, and vulnerabilities using ethical and legal means. This information helps organizations understand their competitive landscape and make informed decisions to enhance their own security defenses. Essentially, it's about studying what others are doing in terms of cybersecurity to stay ahead in the game while staying within ethical boundaries.

OSINT (Open Source Intelligence): OSINT techniques involve gathering publicly available information about competitors from sources such as social media, public databases, websites, and online forums. This information can include details about an organization's infrastructure, technologies in use, key personnel, recent security incidents, and industry partnerships.

Vulnerability Assessment: Conducting vulnerability assessments on competitors' systems and networks can help identify weaknesses that may be exploited by malicious actors. This involves scanning for open ports, outdated software, misconfigurations, and other vulnerabilities using tools like Nessus, OpenVAS, or Nmap.

Penetration Testing: With proper authorization, ethical hackers may perform penetration tests on competitors' networks and applications to identify security flaws and assess the effectiveness of existing security controls. Penetration testing simulates real-world attacks to uncover weaknesses that could be exploited by adversaries.

Social Engineering: Social engineering attacks, such as phishing emails or pretexting, can be used to gather information about competitors' employees, systems, and processes. By exploiting human vulnerabilities, ethical hackers can gain access to sensitive information or credentials that may be used to compromise security.

Analysis of Publicly Disclosed Incidents: Monitoring public disclosures of security incidents involving competitors can provide valuable insights into the types of threats they face, their incident response capabilities, and areas where security improvements may be needed.

Dark Web Monitoring: Monitoring the dark web for mentions of competitors' data, credentials, or vulnerabilities can help organizations stay ahead of potential threats. Ethical hackers can use specialized tools and services to search for mentions of specific organizations or sensitive information that may have been leaked or compromised.

Benchmarking: Comparing an organization's security posture to that of its competitors can help identify areas of strength and weakness. Benchmarking allows organizations to prioritize security investments, allocate resources effectively, and stay competitive in their industry.

Regulatory Compliance Analysis: Analyzing competitors' compliance with industry regulations and standards can provide insights into their commitment to security and privacy. Understanding regulatory requirements and compliance gaps can help organizations assess their own risk exposure and prioritize remediation efforts.

Threat Intelligence Sharing: Participating in threat intelligence sharing communities and industry forums can provide access to information about emerging threats, attack techniques, and vulnerabilities affecting competitors and similar organizations. Sharing threat intelligence helps strengthen collective defenses and improve overall security posture.

Ethical Considerations: It's important for ethical hackers to adhere to legal and ethical guidelines when conducting competitive intelligence activities. Unauthorized access to competitors' systems or data, or any actions that could cause harm or disruption, are strictly prohibited and may result in legal consequences.

13) Write a short note on DNS Enumeration .(Website name ko ip me translate karta he)

Ans:

Domain Name System(DNS) is nothing but a program that converts or translates a website name into an IP address and vice versa.

DNS enumeration is the process of gathering information about a target network by querying its Domain Name System (DNS) servers.

DNS Enumeration and the process of DNS enumeration with a practical approach.

This technique allows ethical hackers and security professionals to uncover details such as domain names, IP addresses, mail servers, and other network-related information.

By querying DNS servers, attackers can map out the network infrastructure, identify potential entry points, and discover misconfigurations or vulnerabilities that could be exploited.

Example: A user enters www.geeksforgeeks.org in a browser, now the DNS will intercept this request and will fetch the corresponding IP address and connect the user to that fetched IP address.

DNS Enumeration is a technique used for Reconnaissance for better understanding of surface area of the Target systems(i.e. IP addresses).

The process of DNS Enumeration returns various important information about the target like DNS record types, host names, IP addresses and much more depending upon the configuration of that target system.

To perform DNS enumeration there are various open source tools, scripts available like Nmap, DNS recon etc.

Importance and Impacts:
Importance:

It helps in discovering the various services and hosts that are running on the domain.
It makes the target surface larger as we enumerate further.
Furthermore, it exposes the critical information about the target.

Impact:

The attacker can read about the system data and also can modify it.
It can also lead to various other potential DNS attacks.
It gives the Threat actor very critical details about the system that the attack can leverage to other attacks.

14) Explain WHOIS and ARIN Lookups in detail

Ans:

WHOIS Lookup:WHOIS is a protocol used to query databases that store registration information for domain names, IP addresses, and other internet resources.

WHOIS databases contain details such as the domain registrant's contact information, registration date, expiration date, name servers, and more.

WHOIS lookups can be performed using various online tools or command-line utilities.

However, the level of detail provided may vary depending on the WHOIS server and the information disclosed by the registrant.

Domain WHOIS: When performing a WHOIS lookup for a domain name, you can retrieve information about the domain registrar, registrant name, organization, email address, registration date, expiration date, name servers, and domain status (e.g., whether it's active or suspended).

IP WHOIS: An IP WHOIS lookup provides information about the allocation and registration of IP addresses. It typically includes details such as the IP address range, allocation date, organization or ISP that owns the IP address block, contact information, and sometimes the geographic location associated with the IP address.

.

ARIN Lookup:ARIN is one of the Regional Internet Registries (RIRs) responsible for allocating and managing IP address space in North America, parts of the Caribbean, and sub-Saharan Africa.

ARIN maintains a public database of IP address allocations, known as the ARIN WHOIS database.

ARIN lookup tools can be accessed through the ARIN website or using command-line utilities that query the ARIN WHOIS database directly.

IP Address Lookup: ARIN lookup allows you to query the ARIN WHOIS database to retrieve information about IP address allocations and assignments within the ARIN region.

This includes details such as the organization or ISP that holds the IP address block, allocation date, registration status, and technical contact information.

AS Number Lookup: In addition to IP addresses, ARIN also manages the assignment of autonomous system numbers (ASNs), which are used for routing purposes.

An ARIN ASN lookup provides information about the organization or ISP that holds the ASN, along with contact information and ASN registration details.

15) What are the types of DNS Records in Ethical Hacking

Ans:

A Record (Address Record):
Maps a domain name to an IPv4 address.
Used to translate domain names to IP addresses, allowing clients to connect to web servers, mail servers, etc.

AAAA Record (IPv6 Address Record):
Similar to A records but maps a domain name to an IPv6 address.
Used for connecting to services over IPv6 networks.

CNAME Record (Canonical Name Record):
Creates an alias for a domain name, pointing it to another domain name.
Often used for creating subdomains or pointing multiple domain names to the same website.

MX Record (Mail Exchange Record):
Specifies the mail server responsible for receiving email messages on behalf of a domain.
Essential for email delivery as it directs incoming emails to the correct mail server.

NS Record (Name Server Record):
Specifies the authoritative name servers for a domain.
Used to delegate authority over a domain to a specific set of name servers.

PTR Record (Pointer Record):
Maps an IP address to a domain name (reverse DNS lookup).
Used to verify the authenticity of an IP address and can be helpful in network troubleshooting.

TXT Record (Text Record):
Stores arbitrary text data associated with a domain.
Used for various purposes such as domain ownership verification, SPF records for email authentication, and providing additional information about a domain.

SOA Record (Start of Authority Record):
Specifies authoritative information about a DNS zone, including the primary name server, contact email address, and other zone settings.
Essential for maintaining and administrating DNS zones.

SRV Record (Service Record):
Specifies the location of services (e.g., SIP, LDAP, XMPP) in the domain.
Used by clients to discover available services within a domain.

DNSSEC Records:
Various records used in DNSSEC (DNS Security Extensions) to provide cryptographic authentication and integrity for DNS data.
Includes records like DNSKEY, RRSIG, NSEC, and DS records.

16) What is Traceroute in Footprinting

Ans:

Traceroute is a network reconnaissance technique used to map out the network infrastructure of a target organization.

By utilizing Traceroute, ethical hackers or security professionals can identify the network topology, including routers, switches, and other network devices, that lie between the source

and destination.

Traceroute provides valuable information about the path packets take from the source system to the target system.

This information helps in understanding the organization's network layout, potential points of entry, and possible vulnerabilities.

By analyzing the hops revealed by Traceroute, security analysts can assess the resilience of the network architecture and identify areas where additional security measures may be necessary.

In essence, Traceroute serves as a reconnaissance tool in the footprinting process, allowing security professionals to gather intelligence about the target organization's network infrastructure, which can then be used to plan further security assessments or penetration testing activities.

17) Define E-mail Tracking and explain its working

Ans:

Email tracking is a method used to monitor the delivery, opening, and interaction with emails sent to recipients. It allows senders to gather information about when, where, and how recipients engage with their emails.

Embedding Tracking Pixels or Images: The sender of the email embeds a tiny, transparent image or tracking pixel into the body of the email. This image is usually hosted on a remote server controlled by the sender or a third-party email tracking service.

Unique Identifiers: Each tracking pixel is associated with a unique identifier or tracking code. When the email is opened by the recipient, their email client or webmail service fetches the image from the sender's server to display it in the email.

Logging Activity: When the tracking pixel is loaded, it sends a request to the sender's server, which logs information such as the time the email was opened, the recipient's IP address, the type of device used, and sometimes the geographic location.

Link Tracking: In addition to tracking pixels, links within the email may also be modified to include tracking parameters. When a recipient clicks on a tracked link, they are redirected through the sender's server or a tracking domain before being taken to the intended destination. This allows the sender to monitor click-through rates and track user engagement with the email content.

Analytics Reporting: The sender can access analytics reports provided by their email tracking service or software. These reports typically include metrics such as open rates, click-through rates, bounce rates, and the time and location of email opens.

Privacy Implications: It's important to note that email tracking raises privacy concerns as it allows senders to collect information about recipients without their explicit consent. In some jurisdictions, email tracking may be subject to legal restrictions, such as requirements to disclose tracking practices or obtain consent from recipients.

18) Explain following attacks in detail

a) Key Stroke logging:

Ans:

Keylogging, also known as keystroke logging, is the act of tracking and recording every keystroke made on a computer or mobile device. This technique is often used by attackers to capture sensitive information such as usernames, passwords, credit card numbers, and other confidential data.

How it works:

Software-based Keyloggers: Malicious software or malware is installed on the victim's device, which silently records keystrokes as the user types. This software may run in the background without the user's knowledge, capturing all keystrokes and storing them locally or transmitting them to a remote server controlled by the attacker.

Hardware-based Keyloggers: Physical devices are installed between the keyboard and the computer or inserted into the USB port. These devices intercept and log keystrokes as they pass through, without the user's awareness.

b) Denial – of Service attack:

Ans ;

A Denial-of-Service (DoS) attack is an attempt to disrupt the normal functioning of a targeted system, network, or service by overwhelming it with a flood of malicious traffic, requests, or messages.

How it works:

Volume-Based Attacks: Flood the target system or network with a high volume of traffic, consuming all available bandwidth, server resources, or network capacity.

Protocol-Based Attacks: Exploit vulnerabilities in network protocols or services to exhaust system resources, such as TCP SYN floods or UDP floods.

Application Layer Attacks: Target specific applications or services with excessive requests or malicious payloads, causing them to crash or become unresponsive.

c) Watering hole attack

Ans:

A watering hole attack is a targeted cyberattack that involves infecting websites frequented by the victim's intended targets with malware. The goal is to compromise the systems of visitors to these websites, typically through drive-by downloads or malicious scripts, to gain access to sensitive information or conduct further attacks.

How it works:

Identifying Targeted Websites: Attackers research and identify websites regularly visited by their intended targets, such as industry-specific forums, news portals, or community websites.

Injecting Malware: The attacker compromises the targeted websites by injecting malicious code or malware into the web pages, often exploiting vulnerabilities in the website's content management system (CMS) or plugins.

Drive-by Downloads: When visitors access the infected website, their devices may be automatically infected with malware without their knowledge or interaction, through drive-by downloads or malicious scripts executed in the background.

d) Brute force attack

Ans:

A brute force attack is a trial-and-error method used to gain unauthorized access to a system, application, or account by systematically trying all possible combinations of usernames, passwords, or encryption keys until the correct one is found.

How it works:

Enumeration: The attacker first identifies the target, such as a login page, network service, or encrypted file, and enumerates the possible usernames, passwords, or keys to be tested.

Automated Tools: The attacker uses automated tools or scripts to generate and test a large number of combinations rapidly, often leveraging dictionaries of commonly used passwords or random character sequences.

Credential Stuffing: In the case of online accounts, the attacker may use stolen credentials obtained from data breaches or phishing attacks to conduct credential stuffing attacks, attempting to reuse the same username and password combinations across multiple websites or services.

e) Phishing and fake WAP

Ans:

Phishing is a cyberattack technique that involves tricking individuals into providing sensitive information, such as usernames, passwords, credit card numbers, or personal details, by impersonating a legitimate entity or organization.

How it works:

Email Phishing: Attackers send fraudulent emails masquerading as reputable companies, government agencies, or financial institutions, often containing urgent requests or enticing offers to lure recipients into clicking on malicious links or downloading malicious attachments.

Spear Phishing: Targeted phishing attacks customized for specific individuals or organizations, leveraging personal information obtained through reconnaissance or social engineering techniques to increase credibility and effectiveness.

Smishing and Vishing: Phishing attacks conducted via SMS text messages (smishing) or voice calls (vishing), typically using social engineering tactics to deceive victims into revealing sensitive information or performing actions such as transferring funds or installing malware.

OR

a) Eaves dropping attack

Ans:

An eavesdropping attack, also known as sniffing or snooping, is a form of cyberattack where an unauthorized party intercepts and monitors communication between two parties without their knowledge or consent. This type of attack is commonly used to capture sensitive information such as usernames, passwords, credit card numbers, and other confidential data transmitted over a network.

How it works:

Packet Sniffing: The attacker uses specialized software or hardware, known as packet sniffers or network analyzers, to capture and analyze network traffic passing through a network interface.
Passive Monitoring: The attacker passively monitors the network, capturing data packets as they are transmitted between devices. This may include unencrypted data sent over protocols such as HTTP, FTP, Telnet, or SMTP.
Data Interception: By analyzing the intercepted data packets, the attacker can extract sensitive information, such as login credentials, personal messages, or financial transactions, contained within the network traffic.

b) Man in the middle attack

Ans:

A man-in-the-middle (MitM) attack is a cyberattack where an attacker secretly intercepts and relays communication between two parties, impersonating each party to the other. This allows the attacker to eavesdrop on the communication, manipulate the data transmitted between the parties, or inject malicious content into the communication stream.

How it works:

Interception: The attacker positions themselves between the communication path of the two parties, intercepting and capturing data packets as they are transmitted between them.

Impersonation: The attacker impersonates the legitimate parties to establish separate encrypted connections with each party, allowing them to decrypt, inspect, modify, or inject data into the communication stream.

Data Manipulation: The attacker may modify the contents of the communication, such as altering messages, redirecting traffic to malicious websites, or injecting malware into file transfers, without the knowledge or consent of the legitimate parties.

c) Session hijacking

Ans:

Session hijacking, also known as session fixation, is a type of cyberattack where an attacker steals or hijacks an active session between a user and a web application to gain unauthorized access to the user's account or sensitive information.

How it works:

Session Identification: The attacker intercepts the session identifier or session cookie used by the web application to authenticate the user's session.

Session Impersonation: The attacker uses the stolen session identifier to impersonate the legitimate user's session, bypassing authentication mechanisms and gaining unauthorized access to the user's account.

Session Manipulation: Once hijacked, the attacker can perform actions on behalf of the legitimate user, such as viewing private information, making unauthorized transactions, or modifying account settings.

d) Clikjacking

Ans:

Clickjacking, also known as UI redressing or user interface (UI) manipulation, is a type of cyberattack where an attacker tricks a user into clicking on a concealed or disguised element on a web page, leading to unintended actions or unauthorized transactions.

How it works:

Concealed Element: The attacker overlays or embeds a hidden or transparent layer on a legitimate web page, containing malicious content or functionality, such as a button or link.

User Interaction: The attacker entices the user to interact with the legitimate web page, typically by enticing them to click on a seemingly innocuous element, such as a play button, download link, or social media widget.

Unauthorized Action: When the user clicks on the concealed element, they unwittingly trigger a malicious action or transaction, such as submitting a form,

sharing sensitive information, or executing arbitrary code, without their knowledge or consent.

e) Cookie Theft

Ans:

Cookie theft, also known as session hijacking or cookie hijacking, is a type of cyberattack where an attacker steals session cookies from a user's browser to gain unauthorized access to their web application accounts.

How it works:

Cookie Interception: The attacker intercepts the session cookies transmitted between the user's browser and the web application during authentication or subsequent requests.

Session Impersonation: Using the stolen session cookies, the attacker can impersonate the legitimate user's session, bypassing authentication mechanisms and gaining unauthorized access to the user's account.

Session Manipulation: Once hijacked, the attacker can perform actions on behalf of the legitimate user, such as viewing private information, making unauthorized transactions, or modifying account settings.

19) What is scanning/Explain Port Scanning in detail

Ans:

Scanning is a fundamental technique in cybersecurity used to gather information about computer systems, networks, and services.

It involves probing target systems to identify open ports, available services, and potential vulnerabilities.

One of the key scanning techniques is port scanning, which involves systematically scanning a range of network ports on a target system to determine which services are running and accessible.

Port Scanning
Port scanning is the process of systematically scanning a target system or network to discover open ports and services.

A port is a virtual endpoint for communication in a network, and each service running on a system typically listens on a specific port for incoming connections.

Port scanning helps identify which ports are open, closed, or filtered, providing insights into the network topology and potential attack vectors.

Technical port scanning:

TCP Connect Scan: This method involves attempting to establish a full TCP connection to each port in the target system's port range. If a connection is

successfully established, the port is considered open.

SYN Scan (Half-open Scan): SYN scanning is a stealthier approach that sends TCP SYN packets to the target ports. If the port is open, the system responds with a SYN-ACK packet, indicating that the port is listening. If the port is closed, the system responds with a RST packet. SYN scanning does not complete the TCP handshake, making it less detectable than TCP Connect scanning.

UDP Scan: UDP scanning involves sending UDP packets to the target ports and analyzing the responses. Since UDP is connectionless and does not provide acknowledgments, determining the state of UDP ports can be more challenging. Open UDP ports may not always respond to scanning packets, and filtering can further complicate detection.

ACK Scan: ACK scanning involves sending TCP ACK packets to the target ports and analyzing the responses. This technique is primarily used to determine whether ports are filtered by firewalls. Filtered ports typically do not respond to ACK packets, while open or closed ports may respond with RST or ICMP unreachable messages.

20) Define port Scanning with example
Ans: **Refers Q no 19 an same answer.**

21) Write a brief note on Network Scanning
Ans:

Network scanning is a crucial phase in cybersecurity and penetration testing that involves systematically probing target networks to gather information about their infrastructure, services, and potential vulnerabilities.

Network scanning is the process of systematically exploring a target network to identify active hosts, open ports, running services, and other network resources.

It serves as a reconnaissance technique used by security professionals, ethical hackers, and system administrators to assess the security posture of a network and discover potential points of entry for attackers.

During network scanning, various scanning techniques and tools are employed to gather information about the target network. These techniques include:

Port Scanning:
Port scanning involves sending packets to target hosts and analyzing their responses to determine which ports are open, closed, or filtered.
Common port scanning techniques include SYN scans, TCP connect scans, UDP scans, and stealth scans (e.g., FIN, XMAS, NULL scans).

Service Enumeration:
Once open ports are identified, service enumeration is performed to determine the specific services and applications running on those ports.
This involves querying the identified ports to gather information about the services' version numbers, banners, and configurations.

Host Discovery:

Host discovery techniques are used to identify active hosts within the target network. Methods such as ICMP ping sweeps, ARP scans, and DNS queries are commonly used to determine which hosts are online and reachable.

Operating System Detection:
Operating system detection involves analyzing responses from target hosts to infer the type and version of the operating system running on them.
Techniques such as TCP/IP stack fingerprinting and passive OS fingerprinting are used to identify the characteristics of target operating systems.

22) Explain Vulnerability Scanning in detail
Ans:
Vulnerability scanning is the process of identifying security weaknesses and flaws in systems and software running on them.

This is an integral component of a vulnerability management program, which has one overarching goal – to protect the organization from breaches and the exposure of sensitive data.

These programs rely on assessment to gauge security readiness and minimize risk, and vulnerability scanning is a critical tool in the cybersecurity toolbox.

A vulnerability scan is automated high-level test that looks for potential security vulnerabilities, while a penetration test is an exhaustive examination that includes a live person actually digging into your network's complexities to exploit the weakness in your systems.

A vulnerability scan only identifies vulnerabilities, while a penetration tester digs deeper to identify the root cause of the vulnerability that allows access to secure systems or stored sensitive data.

The pen tester also looks for business logic vulnerabilities that might be missed by an automatic scanner.

Vulnerability scans can be instigated manually or on an automated basis, and will complete in as little as several minutes to as long as several hours.
Two types of vulnerability scanning

Authenticated Scans: Allow users to log in to the target system or network using valid credentials. ...
Unauthenticated Scans: Instead of relying on credentials, unauthenticated scans leverage external data and probes.

23) Explain CEH Scanning Methodology in brief
Ans:
Pre-engagement Preparation:
Define the scope and objectives of the scanning activity, including the target network or systems to be scanned and the goals of the assessment.
Obtain proper authorization and permission from the relevant stakeholders before conducting any scanning activities.

Footprinting and Reconnaissance:
Gather information about the target network, such as IP addresses, domain names, network topology, and organizational structure, through passive reconnaissance techniques.

Use open-source intelligence (OSINT) sources, search engines, social engineering, and other methods to collect publicly available information about the target organization.

Scanning:
Perform active reconnaissance by scanning the target network using various scanning techniques, such as port scanning, network mapping, and service enumeration.
Identify live hosts, open ports, running services, and potential vulnerabilities within the target environment.
Utilize tools like Nmap, Nessus, OpenVAS, and Nikto to conduct comprehensive scans and gather detailed information about target systems.

Enumeration:
Enumerate additional information about the identified services and systems, such as user accounts, network shares, software versions, and configuration settings.
Use techniques like SNMP enumeration, LDAP enumeration, DNS enumeration, and SMB enumeration to gather detailed information about target systems and network resources.

Vulnerability Analysis:
Analyze the results of the scanning and enumeration phases to identify potential security vulnerabilities and weaknesses within the target environment.
Prioritize vulnerabilities based on their severity, exploitability, and potential impact on the organization's security posture.

Reporting:
Document the findings of the scanning and vulnerability analysis phases in a detailed report, including descriptions of discovered vulnerabilities, their potential impact, and recommendations for remediation.
Present the findings to the relevant stakeholders, such as IT administrators, security teams, and management, in a clear and understandable format.

Post-assessment Activities:
Collaborate with the organization's IT and security teams to address and remediate identified vulnerabilities and weaknesses.
Provide ongoing support and guidance to ensure that security recommendations are implemented effectively and that the organization's security posture is improved.

24) What are the ping Sweep Techniques and define its approaches
Ans :
Ping sweep techniques, also known as ICMP (Internet Control Message Protocol) sweeps or network sweeps, are used in ethical hacking and network reconnaissance to identify live hosts within a target network.

Ping sweep techniques are commonly used in the initial phase of network reconnaissance to create an inventory of live hosts within a target network.

These techniques involve sending ICMP Echo Request (ping) packets to a range of IP addresses and analyzing the responses to determine which hosts are online.

several approaches to conducting ping sweeps:

Basic ICMP Ping Sweep:
In this approach, the attacker sends ICMP Echo Request packets (pings) to a range of IP addresses within the target network, typically using a tool like ping or fping.
The attacker then analyzes the responses received. If a host is online and reachable, it will

respond with an ICMP Echo Reply packet.

ARP Ping Sweep:
ARP (Address Resolution Protocol) ping sweeps are used in local networks to discover hosts that may not respond to ICMP ping requests.
Instead of sending ICMP Echo Request packets, the attacker sends ARP requests for each IP address in the target network range.
If a host is online and connected to the same local network segment as the attacker, it will respond with an ARP reply, indicating its presence.

TCP Ping Sweep:
TCP ping sweeps involve sending TCP packets to a range of IP addresses and analyzing the responses to determine which hosts are online.
Common TCP ping sweep techniques include sending SYN or ACK packets to well-known ports (e.g., TCP port 80 for HTTP) and analyzing the responses received.
Hosts that respond with SYN/ACK or ACK packets are likely to be online and accepting TCP connections
.
ICMP Timestamp Ping Sweep:
This approach involves sending ICMP Timestamp Request packets to a range of IP addresses within the target network.
If a host is online and reachable, it will respond with an ICMP Timestamp Reply packet, providing information about the host's system time.

Mixed Techniques:
Ethical hackers may combine multiple ping sweep techniques to increase the likelihood of identifying live hosts and to overcome limitations of individual methods.
For example, combining ICMP and ARP ping sweeps can provide more comprehensive coverage in heterogeneous network environments with a mix of hosts that respond to different types of requests.

25) What are the Nmap Command Switches
Ans:

Nmap, a powerful network scanning tool used in ethical hacking and network security, offers a wide range of command-line switches to customize and control its scanning behavior. Here are some commonly used Nmap command switches:

-sS or --syn:
Performs a SYN scan, also known as a half-open scan, to determine open ports on target systems.

-sT or --connect:
Conducts a TCP connect scan, establishing a full TCP connection to each target port to determine its state.

-sU or --udp:
Executes a UDP scan to identify open UDP ports on target systems.

-sV or --version-intensity:
Enables version detection, which attempts to determine the version of services running on open ports.
-O or --osscan-guess:
Performs OS detection to identify the operating system running on target systems.

-p or --ports:
Specifies the ports or port ranges to scan. For example, -p 1-1000 scans ports 1 through 1000.

-A:
Enables aggressive scanning, which combines various scan types (SYN scan, version detection, OS detection) to provide comprehensive information about target systems.

-v or --verbose:
Increases verbosity level, providing more detailed output during the scanning process.

-T or --timing:
Sets the timing template for the scan, ranging from paranoid (slowest) to insane (fastest).

-oN, -oX, -oG, -oA:
Specifies the output format of the scan results. Options include normal (-oN), XML (-oX), grepable (-oG), and all formats (-oA).

-iL or --input-file:
Reads target IP addresses or hostnames from a specified file.

-exclude:
Excludes specified hosts or networks from the scan.

--script:
Runs Nmap scripts against target systems to perform additional enumeration and vulnerability scanning.

-Pn:
Treats all hosts as online and skips host discovery. Useful when dealing with firewalled or unresponsive hosts.

-h or --help:
Displays the Nmap help menu, listing all available command-line switches and their descriptions.

26) Explain how SYN is getting used to transfer the connection in Ethical Hacking

Ans:

In ethical hacking, the SYN (Synchronize) flag in the TCP (Transmission Control Protocol) header is not used to transfer the connection itself; instead, it's a crucial part of the TCP three-way handshake process, which is used to establish connections between devices on a network.
the SYN flag is often leveraged in scanning techniques, such as SYN scanning, to probe target systems and identify open ports without establishing full TCP connections.

In this context, the attacker sends SYN packets to various ports on the target system and analyzes the responses to determine which ports are open, closed, or filtered by firewalls.

This allows ethical hackers to gather information about potential entry points into the target system without triggering security alerts.

Let's break down how the SYN flag is used in the context of establishing connections:

Initiating a Connection:
When a client device wants to establish a connection with a server, it sends a TCP packet with the SYN flag set and specifies the initial sequence number (ISN) it's choosing for the connection.
This packet is commonly referred to as a SYN packet or a SYN segment.

Acknowledging the Connection Request:
Upon receiving the SYN packet, the server acknowledges the request by sending a TCP packet with both the SYN and ACK (Acknowledgment) flags set.
This packet indicates that the server has received the client's SYN packet and is ready to establish a connection. It also includes its own ISN for the connection.

Completing the Connection:
In response to the server's SYN-ACK packet, the client sends an ACK packet back to the server.
This ACK packet confirms that the client has received the server's acknowledgment and is also ready to establish the connection.

Connection Established:
Once both the client and server have exchanged SYN and ACK packets, a TCP connection is considered established, and data can be transmitted between them.

27) Define Stealth in Ethical Hacking
Ans:
In ethical hacking, "stealth" refers to the practice of conducting hacking activities in a discreet and undetectable manner to minimize the risk of detection by security mechanisms, such as intrusion detection systems (IDS), firewalls, or network monitoring tools.

Stealth techniques are employed to avoid triggering alarms, raising suspicion, or leaving traces of unauthorized access during penetration testing or security assessments.

Stealthy hacking techniques aim to emulate the behavior of legitimate network traffic or system interactions, making it challenging for defenders to distinguish between normal and malicious activities.

The primary goal of employing stealth in ethical hacking is to gather information, identify vulnerabilities, and assess the security posture of target systems or networks without alerting defenders or disrupting business operations.

Stealth techniques in ethical hacking may include:

Covert Scanning: Using scanning techniques, such as SYN scans, FIN scans, or XMAS scans, that generate minimal network traffic and do not establish full TCP connections to avoid detection by IDS or firewall logs.

Traffic Obfuscation: Modifying network traffic patterns or payloads to disguise malicious activities as legitimate traffic, making it difficult for network monitoring tools to detect anomalies.

Encryption: Encrypting communication channels and payloads to prevent eavesdropping and data interception by network defenders or security appliances.

Evasion Techniques: Leveraging evasion techniques, such as packet fragmentation, protocol manipulation, or traffic shaping, to bypass network security controls and inspection mechanisms.

Staging Attacks: Breaking complex hacking activities into smaller, less detectable stages to minimize the likelihood of detection and increase the chances of success.

Hiding Artifacts: Removing or obfuscating artifacts, such as log entries, audit trails, or file timestamps, that could reveal evidence of unauthorized access or compromise.

28) Explain how XMAS Scanning techniques is used in Ethical Hacking

Ans:

XMAS scanning is a stealthy scanning technique used in ethical hacking and penetration testing to probe target systems and identify potential vulnerabilities.

This scanning technique gets its name from the pattern of TCP flags used in the packets sent to the target ports, which resembles the pattern of lights on a Christmas tree.

Here's how XMAS scanning works and its role in ethical hacking:

Understanding TCP Flags:
TCP (Transmission Control Protocol) packets contain a set of flags in the TCP header that indicate various aspects of the packet's purpose and behavior.
Common TCP flags include SYN (Synchronize), ACK (Acknowledgment), FIN (Finish), RST (Reset), PSH (Push), and URG (Urgent).

XMAS Scan Technique:
In an XMAS scan, the attacker sends TCP packets to the target ports with specific flag combinations.
XMAS packets have the FIN, URG, and PSH flags set to "on" (1), while all other flags, such as SYN, ACK, and RST, are set to "off" (0).
This flag combination is unusual and can trigger different responses from target systems, depending on how they interpret and handle such packets.

Response Analysis:
If the target port is closed, the target system is expected to respond with a TCP RST (Reset) packet, indicating that the port is closed and not accepting connections.
If the target port is open, the response from the target system may vary:
Some systems may not respond at all to XMAS packets, treating them as invalid or malformed and silently dropping them.
Other systems may respond with a TCP RST packet, similar to how they would respond to a closed port.
In some cases, the target system may respond with no flags set, indicating that the port is open but no services are listening on that port.

Role in Ethical Hacking:
XMAS scanning is valuable in ethical hacking for reconnaissance and vulnerability assessment purposes.
It allows ethical hackers to identify open ports on target systems and gather information about potential vulnerabilities without triggering intrusion detection systems (IDS) or firewall logs.
By analyzing the responses from the target system, ethical hackers can determine the state

of target ports and assess the security posture of the target environment.

Considerations:
While XMAS scanning can be stealthy and effective, it may not work reliably on all target systems or network configurations.
Some operating systems and network devices may respond to XMAS packets in unexpected ways, potentially leading to false positives or inaccurate scan results.
Additionally, some modern intrusion detection and prevention systems may be configured to detect and block XMAS scan attempts as part of their security measures.

29) What is the term NULL defines in Ethical Hacking

Ans:
The term "NULL" refers to a scanning technique used to probe target systems and identify potential vulnerabilities.

Specifically, a NULL scan is a type of TCP scanning technique where the attacker sends TCP packets with no TCP flags set (i.e., all flags set to zero) to target ports. This technique exploits the behavior of certain operating systems and network devices in response to malformed or unexpected TCP packets.
When a NULL scan is performed:

> If the target port is closed, the TCP packet is expected to be rejected, and the target system should respond with a TCP RST (Reset) packet.
>
> If the target port is open, the TCP packet may be silently dropped, and the target system may not respond at all.

By analyzing the responses (or lack thereof) from the target system, the attacker can determine whether the target ports are open or closed.

Like other scanning techniques such as SYN scans or FIN scans, NULL scans are commonly used in ethical hacking and penetration testing to gather information about target systems and assess their security posture.

30) Explain the role of IDLE Scan in Ethical Hacking

Ans:
Stealthy Reconnaissance:
The IDLE scan is designed to be stealthy, allowing ethical hackers to gather information about target systems without triggering intrusion detection systems (IDS) or firewall logs. By leveraging the predictable behavior of certain operating systems and exploiting existing connections with zombie systems, the IDLE scan avoids direct interaction with the target, making it difficult to detect.

Identification of Open Ports:
One of the primary objectives of the IDLE scan is to identify open ports on target systems. By analyzing changes in the IP ID field of packets forwarded through a zombie system, ethical hackers can determine whether a port on the target system is open or closed without directly probing it.

Vulnerability Assessment:

Identifying open ports through the IDLE scan enables ethical hackers to conduct further analysis to assess the security vulnerabilities present on the target systems.
Once open ports are identified, ethical hackers can perform additional testing, such as service version detection or vulnerability scanning, to identify potential weaknesses that could be exploited by attackers.

Covert Operations:
The stealthy nature of the IDLE scan makes it suitable for conducting covert operations in penetration testing scenarios.
Ethical hackers can use the IDLE scan to gather reconnaissance information discreetly, helping them understand the target environment's security posture and identify potential attack vectors without alerting defenders.

Risk Mitigation:
By identifying open ports and vulnerabilities through the IDLE scan, ethical hackers play a vital role in helping organizations mitigate security risks.
Ethical hackers can provide actionable insights and recommendations to organizations based on the findings of the IDLE scan, enabling them to strengthen their defenses and protect against potential cyber threats.

31) Explain in FIN scans and its role in Ethical Hacking

Ans:

A FIN scan is a type of port scanning technique used in ethical hacking to identify open ports on target systems.

In a FIN scan, the attacker sends TCP packets with the FIN (Finish) flag set to the target system's ports.

This technique exploits a subtle behavior in the TCP protocol specification.

While FIN scans are stealthy and can evade detection by some network defenses, they may not work reliably on all target systems or network configurations.

Some operating systems and network devices may respond to FIN packets in unexpected ways, potentially leading to false positives or inaccurate scan results.

Additionally, some modern intrusion detection and prevention systems may be configured to detect and block anomalous or suspicious network traffic patterns, including FIN scans.

Ethical hackers should use FIN scans in conjunction with other scanning techniques and exercise caution to avoid inadvertently triggering security alerts or disrupting network operations.

Role in Ethical Hacking:

FIN scans are valuable tools in ethical hacking for reconnaissance and vulnerability assessment. They help identify open ports on target systems, providing insights into the network topology and potential attack vectors.

Unlike more aggressive scanning techniques, such as SYN scans or UDP scans, FIN scans are often less detectable by intrusion detection systems (IDS) or firewall logs. This makes

them useful for stealthy scanning operations where the attacker wants to minimize the risk of detection.

FIN scans can help ethical hackers identify potential security vulnerabilities or misconfigurations in network devices or services. Open ports may indicate services running on target systems that could be vulnerable to exploitation if not properly secured or patched.

Additionally, FIN scans can help organizations assess the effectiveness of their network defenses, such as firewalls, IDS, or access control lists (ACLs). By simulating attack scenarios using FIN scans, organizations can identify gaps in their security posture and take proactive measures to mitigate potential risks.

32) What are the anonymizers in Ethical Hacking
Ans:

Anonymizers are tools or services used in ethical hacking and cybersecurity to conceal or obfuscate the source of network traffic, providing anonymity and privacy for users.

These tools route network traffic through intermediary servers, masking the user's IP address and other identifying information from the destination server or service.

Anonymizers can be used for legitimate purposes, such as protecting user privacy and circumventing censorship, but they can also be exploited by malicious actors for illicit activities.

Here are some common types of anonymizers used in ethical hacking:

Proxy Servers:
Proxy servers act as intermediaries between clients and destination servers, forwarding requests on behalf of clients and relaying responses back to clients.
Anonymizing proxy servers, also known as high-anonymity or elite proxies, conceal the client's IP address from the destination server, making it appear as though the requests originate from the proxy server's IP address.
Proxy servers can be configured to route traffic through multiple proxy chains or proxy cascades, further enhancing anonymity by obfuscating the source of traffic.

Virtual Private Networks (VPNs):
VPNs establish encrypted tunnels between the client's device and VPN servers, encrypting all traffic passing through the tunnel and masking the client's IP address.
VPNs provide a secure and private connection to the internet, preventing network eavesdropping and surveillance by ISPs, governments, or malicious actors.
VPNs offer a wide range of server locations, allowing users to select exit nodes in different countries to bypass geo-restrictions and access region-restricted content.

Tor (The Onion Router):
Tor is a decentralized network of volunteer-operated servers, called relays or nodes, that route encrypted traffic through multiple layers of encryption and anonymization.
Tor anonymizes internet traffic by encrypting data multiple times and routing it through a series of randomly selected relays before reaching its destination, concealing the source IP address and online activities of users.
Tor is commonly used for anonymous browsing, accessing the dark web, and circumventing internet censorship in restrictive environments.

Anonymous Proxy Services:
Anonymous proxy services provide dedicated proxy servers that users can connect to for

anonymous web browsing and online activities.
These services often offer features such as rotating IP addresses, HTTP header manipulation, and traffic obfuscation to enhance anonymity and evade detection by network monitoring tools.
Anonymous proxy services may charge subscription fees or offer free and paid tiers with varying levels of anonymity and performance.

Web-based Proxies:
Web-based proxies are online services that allow users to access blocked or restricted websites by proxying HTTP requests on their behalf.
Users can simply enter the URL of the desired website into the web-based proxy's interface, and the proxy server will fetch the content and relay it back to the user's browser, masking their IP address in the process.
Web-based proxies are often used for bypassing content filters, accessing region-restricted content, and preserving user privacy while browsing the web.

33) What are the HTTP Tunneling Techniques in Ethical Hacking

Ans:

HTTP tunneling is a technique used in ethical hacking to bypass network restrictions or security controls by encapsulating non-HTTP traffic within HTTP packets. This allows otherwise blocked or restricted traffic, such as arbitrary data or protocols, to traverse firewalls, proxy servers, or other network devices that only allow HTTP traffic.

Here are some simple explanations of common HTTP tunneling techniques:

HTTP CONNECT Method:
The HTTP CONNECT method is commonly used for establishing secure HTTPS connections through proxy servers.
In HTTP tunneling, the CONNECT method is exploited to establish a bidirectional communication channel between the client and the destination server
The client sends an HTTP CONNECT request to the proxy server, specifying the destination host and port it wants to connect to.
If the proxy server allows the CONNECT request, it establishes a TCP connection with the destination server on behalf of the client.
Once the TCP connection is established, the client can send non-HTTP traffic through the tunnel, bypassing any restrictions imposed by the proxy server.

HTTP POST Requests:
HTTP POST requests are commonly used to send data from clients to servers, such as form submissions or file uploads.
In HTTP tunneling, arbitrary data or protocols can be encapsulated within the body of an HTTP POST request.
The client constructs an HTTP POST request with the desired data payload and sends it to a web server that supports POST requests.
The web server receives the POST request and forwards the data payload to the destination server specified by the client.
The destination server processes the data payload as if it were a legitimate HTTP request, allowing non-HTTP traffic to traverse the network undetected.

HTTP Headers Manipulation:

HTTP headers, such as Host, User-Agent, or Referer, contain metadata about HTTP requests and responses.
In HTTP tunneling, attackers can manipulate HTTP headers to disguise non-HTTP traffic as legitimate HTTP requests.
For example, attackers may use the Host header to specify the destination server's hostname and port, allowing them to establish a connection without triggering network filters.
By crafting custom HTTP headers and payloads, attackers can obfuscate tunneling traffic to evade detection by intrusion detection systems (IDS) or web application firewalls (WAF).

Web-based Proxies:
Web-based proxies are online services that allow users to access blocked or restricted websites by proxying HTTP requests on their behalf.
In HTTP tunneling, attackers can leverage web-based proxies to establish encrypted tunnels and bypass network restrictions.
Attackers connect to the web-based proxy server using standard HTTP requests, and the proxy server forwards their requests to the desired destination servers.
The web-based proxy server acts as an intermediary, relaying responses between the client and the destination server, allowing non-HTTP traffic to traverse the network securely.

34) What are the IP Spoofing Techniques in Ethical Hacking

Ans:

IP Spoofing is essentially a technique used by a hackers to gain unauthorized access to Computers.

Concepts of IP Spoofing was initially discussed in academic circles as early as 1980. IP Spoofing types of attacks, had been known to Security expert on the theoretical level.

It was primarily theoretical until Robert Morris discovered a security weakness in the TCP protocol known as sequence prediction.

Occasionally IP spoofing is done to mask the origins of a Dos attack. In fact Dos attacks often mask actual IP address from where attack has originated from.

Raw IP Packet Spoofing: This technique involves crafting custom IP packets with spoofed source IP addresses using low-level networking libraries or tools like Scapy. By forging the source IP address in packet headers, attackers can impersonate trusted hosts or evade network filtering and access controls.

Source Routing Spoofing: Source routing allows the sender of a packet to specify the route it should take through the network. In IP spoofing attacks, attackers may manipulate source routing options to bypass network filtering or redirect traffic through intermediate hosts under their control.

DNS Spoofing: Domain Name System (DNS) spoofing involves manipulating DNS responses to redirect traffic intended for legitimate servers to malicious destinations controlled by the attacker. By spoofing DNS responses, attackers can impersonate legitimate websites, intercept communications, and conduct phishing attacks.

Man-in-the-Middle (MitM) Spoofing: In MitM attacks, attackers position themselves between communicating parties to intercept and manipulate traffic. IP spoofing can be used to impersonate one of the parties, allowing attackers to intercept sensitive information,

modify data in transit, or inject malicious payloads into communication streams.

UDP/TCP Spoofing: Spoofing attacks can target both UDP and TCP protocols, with attackers forging source IP addresses in packet headers to deceive network devices and services. UDP spoofing attacks are commonly used in distributed denial-of-service (DDoS) attacks to amplify traffic and overwhelm target servers.

Session Hijacking: Session hijacking attacks involve stealing session cookies or tokens to impersonate authenticated users and gain unauthorized access to web applications or services. IP spoofing can be used in conjunction with session hijacking techniques to evade detection and maintain persistence in compromised systems

35) Explain SNMP Enumeration in detail

Ans:-

Simple Network Management Protocol (SNMP) is an application layer protocol that runs on UDP and maintains and manages IP network routers, hubs, and switches.

SNMP agents run on networking devices in Windows and UNIX networks.

SNMP (Simple Network Management Protocol) is an application layer protocol that utilizes the UDP protocol to manage routers, hubs, and switches on an IP network.

SNMP is a widely used protocol that is enabled on a wide range of operating systems, including Windows Server, Linux servers, and network devices such as routers and switches.

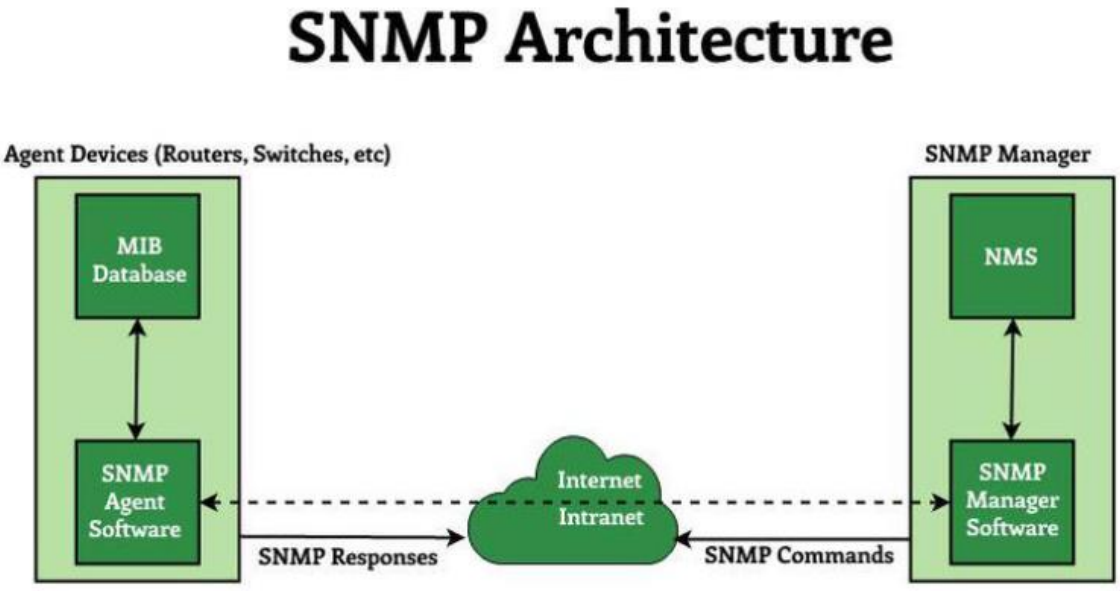
On a target system, SNMP enumeration is used to list user accounts, passwords, groups, system names, and devices.

SNMP Enumeration is made up of three major parts:

Managed Device: A managed device is a device or a host (technically referred to as a node) that has the SNMP service enabled. These devices include routers, switches, hubs, bridges, computers, and so on.

Agents: An agent is a software component that runs on a managed device. Its primary function is to convert data into an SNMP-compatible format for network management via the SNMP protocol.

Network Management System (NMS) : NMS are software systems that are employed to monitor network devices.



36) What are the steps involved in Enumeration

Ans:

Reconnaissance:

Passive Reconnaissance: Gather publicly available information about the target organization, such as domain names, IP addresses, email addresses, and employee names, using sources like search engines, social media, and public databases.

Active Reconnaissance: Perform active scanning and probing of the target network using tools like Nmap, Masscan, or Shodan to discover live hosts, open ports, and available services. This helps identify potential entry points and attack surfaces.

Network Scanning:

Port Scanning: Conduct port scanning to identify open ports and services running on target systems. Use techniques like TCP SYN scans, UDP scans, or comprehensive scans to enumerate available services and potential attack vectors.

Service Version Detection: Identify the versions of services running on open ports using tools like Nmap or banner grabbing techniques. This helps assess the potential vulnerabilities associated with specific service versions.

Vulnerability Scanning:

Vulnerability Identification: Use vulnerability scanning tools like Nessus, OpenVAS, or Nexpose to identify known vulnerabilities and misconfigurations in target systems and applications. This involves scanning for missing patches, outdated software versions, and common security weaknesses.

Exploitability Assessment: Evaluate the exploitability of identified vulnerabilities based on factors such as exploit availability, severity, and impact on the target environment. Prioritize vulnerabilities that pose the highest risk to the organization.

Enumeration of Services:

Enumeration of User Accounts: Enumerate user accounts, groups, and permissions on target systems and applications using techniques like LDAP enumeration, Windows enumeration, or Unix/Linux enumeration. Identify privileged accounts and potential points of access for further exploitation.

Enumeration of Network Shares: Enumerate network shares and file systems accessible to authenticated users. Identify sensitive data, configuration files, or proprietary information stored in shared folders that could be leveraged by attackers.

Active Directory Enumeration:

Enumeration of Domain Information: Enumerate domain information, such as domain controllers, domain trusts, user accounts, groups, and organizational units (OUs), using tools like BloodHound or enum4linux. This helps identify potential attack paths and lateral movement opportunities within the Active Directory environment.

Enumeration of Group Policy Objects (GPOs): Enumerate Group Policy Objects (GPOs) applied to domain objects to identify security configurations, restrictions, and settings that could impact the security posture of target systems and users.

Web Application Enumeration:

Enumeration of Web Servers: Enumerate web servers, web applications, and directories hosted on target systems using tools like dirb, dirbuster, or gobuster. Identify hidden or unlinked pages, administrative interfaces, or vulnerable scripts that could be exploited for unauthorized access or information disclosure.

Enumeration of Web Technologies: Identify web technologies, frameworks, and libraries used in target web applications. This helps assess the potential security risks associated with specific technologies and identify known vulnerabilities or weaknesses.

Post-Enumeration Analysis:

Data Analysis: Analyze the gathered information, enumeration results, and vulnerability assessment findings to prioritize remediation efforts and develop a comprehensive security strategy.
Reporting: Document the enumeration process, findings, and recommendations in a detailed report for stakeholders, including management, IT teams, and security personnel. Provide actionable insights and mitigation strategies to address identified risks and vulnerabilities.

Unit 2

1. Explain password hacking techniques.

Ans:
Password hacking techniques involve various methods used by attackers to gain unauthorized access to password-protected accounts, systems, or networks.

These techniques exploit weaknesses in passwords, authentication mechanisms, or human behavior to bypass security measures.

Here are some common password hacking techniques:

Brute Force Attack:
In a brute force attack, the attacker tries every possible combination of characters until the correct password is found.
Brute force attacks can be performed offline (using pre-computed hash tables like rainbow tables) or online (attempting login with each password guess).
Advanced variants include dictionary attacks (using wordlists) and hybrid attacks (combining dictionary words with character substitutions or permutations).

Dictionary Attack:
A dictionary attack involves trying a list of commonly used passwords, words from dictionaries, or previously leaked passwords against a target account.
Attackers often use automated tools to quickly test thousands or millions of passwords from wordlists.

Credential Stuffing:
In credential stuffing attacks, attackers use previously leaked username-password pairs (obtained from data breaches) to attempt unauthorized logins on other online services.
Since many users reuse passwords across multiple accounts, attackers exploit this behavior to gain access to additional accounts.

Phishing:
Phishing involves tricking users into revealing their passwords or sensitive information by impersonating legitimate entities through emails, websites, or messages.
Phishing attacks often employ social engineering techniques to deceive users into providing their login credentials willingly.

Keylogging:
Keylogging involves installing malicious software (keyloggers) on a victim's device to record their keystrokes, including passwords typed during login sessions.
Attackers retrieve the captured keystrokes later to obtain the victim's passwords.

Shoulder Surfing:
Shoulder surfing occurs when attackers observe or record a victim entering their password directly (e.g., by looking over their shoulder or using hidden cameras).
Attackers may target victims in public places, such as cafes or airports, to capture passwords during login sessions.

Social Engineering:
Social engineering techniques exploit human psychology and trust to manipulate individuals into revealing their passwords or providing access to secure systems.
Techniques include pretexting, baiting, tailgating, and impersonation to deceive victims into divulging sensitive information.

Rainbow Tables:
Rainbow tables are pre-computed tables containing hash values and their corresponding plaintext passwords.
Attackers use rainbow tables to quickly look up password hashes obtained from compromised systems and retrieve the original passwords.

Pass the Hash:
In pass the hash attacks, attackers capture password hashes from compromised systems and use them directly (without cracking) to authenticate and gain access to other systems within the same network.

2. List and explain different types of passwords used.
Ans:
Alphanumeric Passwords:
Alphanumeric passwords contain a combination of letters (both uppercase and lowercase), numbers, and special characters. They offer increased complexity and entropy, making them more resistant to brute-force attacks. Example: "P@ssw0rd123!"

Passphrases:
Passphrases are longer, multi-word phrases or sentences used as passwords. They provide higher entropy and are easier to remember than complex alphanumeric passwords.
Passphrases are often composed of random words or memorable phrases. Example: "correct horse battery staple".

PINs (Personal Identification Numbers):
PINs are short numeric passwords typically used for authentication in ATM transactions, access control systems, or mobile devices. They offer a simpler form of authentication but are susceptible to brute-force attacks due to their limited length. Example: "1234".

Biometric Passwords:
Biometric passwords use unique biological traits, such as fingerprints, facial recognition, iris scans, or voice recognition, for authentication. Biometric authentication provides a high level of security and convenience, as it is based on physical characteristics that are difficult to replicate.

One-Time Passwords (OTP):
One-time passwords are temporary passwords generated for single-use authentication purposes. OTPs are typically delivered to users via SMS, email, or authentication apps and expire after a short period or after being used once. They provide an additional layer of security, especially for online banking, two-factor authentication (2FA), or multi-factor authentication (MFA) systems.

Pattern-Based Passwords:
Pattern-based passwords involve creating a password by tracing a specific pattern or sequence on a keyboard or touchscreen. Users select a series of characters, numbers, or symbols in a predefined pattern to create their password. Example: "1qaz@WSX" (a pattern across the keyboard).

Graphical Passwords:
Graphical passwords replace traditional text-based passwords with images, patterns, or symbols. Users select or draw specific images or patterns as their password instead of typing alphanumeric characters. Graphical passwords offer an alternative authentication method, particularly suitable for touchscreen devices.

Randomly Generated Passwords:
Randomly generated passwords are created using password generators or password management tools. These passwords consist of a random combination of characters, numbers, and symbols, with no logical patterns or sequences. Randomly generated passwords provide high security but can be challenging to remember without the use of a password manager.

3. Explain,spyware technologies in detail
ANS:
Spyware is a breach of cyber security as they usually get into the laptop/ computer system when a user unintentionally clicks on a random unknown link or opens an unknown attachment, which downloads the spyware alongside the attachment.

It is a best practice to be cautious of the sites that are used for downloading content on the system.

Spyware is a type of software that unethically without proper permissions or authorization steals a user's personal or business information and sends it to a third party.

Spyware may get into a computer or laptop as a hidden component through free or shared wares.

Spywares perform the function of maliciously tracking a user's activity, having access to data, or even resulting in the crashing of the computer/ laptop system.

Spyware in many cases runs as a background process and slows down the normal functioning of the computer system.

Spyware enters the laptop/computer system through the below-listed ways:

Phishing: It is a form of a security breach where spyware enters the system when a suspicious link is clicked or an unknown dangerous attachment is downloaded.

Spoofing: It goes alongside phishing and makes the unauthorized emails appear to come from legitimate users or business units.

Free Softwares or Shared Softwares: It gets into the system when a user installs software that is free of cost but has additional spyware added to them.

Misleading software: This is advertised as very beneficial for the system and would boost up the speed of the system but lead to stealing confidential information from the system.

4. What are the preventions used in root notes
Ans:
Securing root nodes in a network or system is crucial for maintaining the integrity, confidentiality, and availability of critical resources and infrastructure. Here are several prevention measures commonly used to enhance the security of root nodes:

Strong Authentication:
Implement strong authentication mechanisms, such as multi-factor authentication (MFA) or biometric authentication, to control access to root nodes. Require unique and complex passwords or passphrase combinations and enforce regular password rotation.

Role-Based Access Control (RBAC):
Use RBAC policies to assign permissions and privileges to users based on their roles and responsibilities. Limit access to root nodes to only authorized personnel who require administrative privileges for legitimate purposes.

Least Privilege Principle:
Adhere to the principle of least privilege by granting users the minimum level of access necessary to perform their duties. Restrict root-level access to only those individuals who need it to carry out specific administrative tasks.

Audit Logging and Monitoring:
Enable comprehensive logging and monitoring of activities on root nodes to track changes, access attempts, and security incidents. Regularly review audit logs for suspicious or unauthorized activities and promptly investigate any anomalies.

Encryption:
Encrypt sensitive data stored on root nodes, including configuration files, credentials, and other critical information. Use strong encryption algorithms and ensure that encryption keys are securely managed and protected.

Patch Management:
Implement a robust patch management process to regularly update the operating system, applications, and firmware on root nodes. Apply security patches promptly to address known vulnerabilities and mitigate the risk of exploitation by attackers.

Network Segmentation:
Implement network segmentation to isolate root nodes from other less secure parts of the network. Use firewalls, VLANs (Virtual Local Area Networks), or network access control lists (ACLs) to restrict communication between network segments and control traffic flow.

Intrusion Detection and Prevention Systems (IDPS):
Deploy IDPS solutions to detect and prevent unauthorized access, malicious activities, or potential security breaches on root nodes. Configure IDPS sensors to monitor network traffic, system logs, and file integrity for signs of compromise.

Backup and Disaster Recovery:
Implement regular backup procedures to create redundant copies of critical data stored on root nodes. Store backups securely off-site or in encrypted formats to protect against data loss, corruption, or ransomware attacks. Develop and test a comprehensive disaster recovery plan to ensure business continuity in the event of a security incident.

Security Awareness Training:

Provide security awareness training to system administrators and users with access to root nodes. Educate them about security best practices, common threats, and social engineering tactics to help them recognize and respond to potential security risks effectively.

5. What are DNS spoofing technique?
Ans:
A Domain Name System (DNS) converts a human-readable name (such as www.geeksforgeeks.org) to a numeric IP address.

The DNS system responds to one or more IP-address by which your computer connects to a website (such as geeksforgeeks.org) by using one of the IP-address.

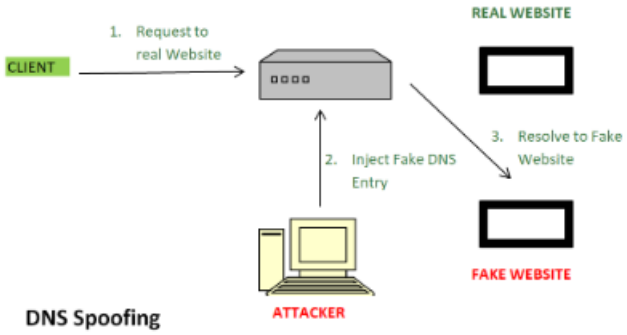
There is not only one DNS server. There are series of DNS servers used to resolve the domain name.

DNS uses cache to work efficiently so that it can quickly refer to DNS lookups it's already performed rather than performing a DNS lookup over and over again.

Although DNS caching increase the speed of the domain name resolution process But the major change in the domain then takes a day to reflect worldwide.

DNS Spoofing means getting a wrong entry or IP address of the requested site from the DNS server.

Attackers find out the flaws in the DNS system and take control and will redirect to a malicious website



6. Explain protocol susceptible to sniffing
Ans:

Sniffing refers to the unauthorized interception and monitoring of network traffic to capture sensitive information, such as passwords, usernames, or confidential data, as it travels across a network. While any network protocol can be vulnerable to sniffing if not adequately protected, some protocols are more susceptible to sniffing due to their inherent characteristics**.**
Here are some protocols commonly targeted by sniffing attacks:

HTTP (Hypertext Transfer Protocol):
HTTP is the foundation of data communication on the World Wide Web. When transmitted over unencrypted channels (HTTP rather than HTTPS), HTTP traffic is susceptible to sniffing, allowing attackers to intercept and capture sensitive information, such as login credentials or session cookies.

FTP (File Transfer Protocol):

FTP is a standard protocol used for transferring files between a client and a server on a computer network. Unless FTPS (FTP Secure) or SFTP (SSH File Transfer Protocol) is used to encrypt the FTP traffic, FTP sessions are vulnerable to sniffing, exposing usernames, passwords, and file contents to potential interception.

Telnet:
Telnet is a network protocol used for remote terminal connections, allowing users to access and manage devices or servers remotely. Telnet transmits data, including login credentials and command output, in plain text, making it susceptible to sniffing attacks. SSH (Secure Shell) should be used instead of Telnet to encrypt remote connections.

SMTP (Simple Mail Transfer Protocol):
SMTP is the standard protocol used for sending and relaying email messages between mail servers. When SMTP traffic is transmitted over unencrypted channels, such as SMTP without TLS (Transport Layer Security), email contents, sender and recipient addresses, and attachments can be intercepted by sniffing attackers.

POP3 (Post Office Protocol version 3) and IMAP (Internet Message Access Protocol):
POP3 and IMAP are email retrieval protocols used by email clients to fetch emails from mail servers. Similar to SMTP, POP3 and IMAP traffic transmitted without encryption (e.g., POP3/IMAP without SSL/TLS) is susceptible to sniffing, exposing email contents and authentication credentials.

DNS (Domain Name System):
DNS is a hierarchical naming system that translates domain names into IP addresses, enabling users to access websites using human-readable domain names. While DNS itself does not transmit sensitive data, DNS queries and responses can be intercepted and analyzed by sniffing attackers to reveal users' browsing habits and potentially facilitate DNS spoofing attacks.

7. What is ARP spoofing? Explain in detail.
Ans:
ARP stands for Address Resolution Protocol.

It is a communication protocol that is one of the important network layer protocols in the OSI model and is used to determine a device's Media Access Control (MAC) address based on its Internet Protocol (IP) address in order to communicate with other devices on the network
ARP spoofing is a cyber attack that allows hackers to intercept communications between network devices on a network.

ARP (Address Resolution Protocol) spoofing, also known as ARP poisoning or ARP cache poisoning, is a type of network attack where an attacker sends falsified or malicious ARP messages over a local area network (LAN) to associate the attacker's MAC address with the IP address of another host on the network.

This manipulation of ARP messages allows the attacker to intercept, modify, or redirect network traffic intended for the targeted host, leading to various security risks and potential exploitation.

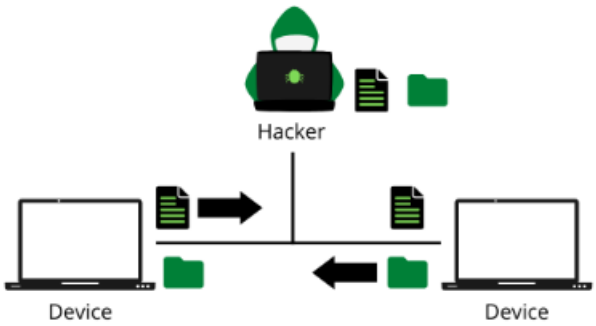
Hackers can also use ARP spoofing to alter or block all traffic between devices on the network.

Types of ARP Spoofing:

Man-in-the-Middle: In the Man-in-the-Middle Attack, hackers use ARP spoofing to intercept communications that occur between devices on a network to steal information that is transmitted between devices. Sometimes, hackers also use man-in-the-middle to modify traffic between network devices.

Session hijacking: In Session hijacking, With the help of ARP spoofing hackers are able to easily extract the session ID or gain inauthentic access to the victim's private systems and data.

Denial-of-service attacks: Denial-of-service attack is a type of attack in which one or more victims deny to access the network. With the help of ARP spoofing, A single target victim's mac address is linked with multiple IP addresses. Due to this whole traffic is shifted toward the target victim's mac address which causes overloading of the network of the target victim with traffic.



8. Write short note on MAC flooding
Ans:
MAC flooding is a network attack that targets switches to overwhelm their MAC address tables, leading to a loss of network connectivity or potential security vulnerabilities.

MAC flooding exploits the limited capacity of a switch's MAC address table by flooding the switch with a large number of spoofed MAC addresses.

The attacker sends numerous Ethernet frames to the switch, each containing a different source MAC address.

When the switch receives these frames, it adds each MAC address to its MAC address table to associate it with the corresponding port.

However, because the table has a finite size and is not designed to handle such a large volume of MAC addresses, it eventually becomes full.

Once the MAC address table is full, the switch enters into a fail-open mode known as "unknown unicast flooding." In this mode, the switch forwards incoming frames to all ports except the one on which the frame was received, effectively turning the switch into a hub-like device.

This flooding of traffic can lead to network congestion, performance degradation, and potentially enable attackers to intercept or eavesdrop **o**n network traffic intended for other devices.

To defend against MAC flooding attacks, network administrators can implement port security features on switches, such as MAC address limiting, MAC address aging timers, or

dynamic ARP inspection

9. Explain how DNS attack works.
Ans:

DNS (Domain Name System) attacks target the Domain Name System, which is responsible for translating domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.2.1) to facilitate communication over the internet. There are several types of DNS attacks, each with its own method and purpose**.**
Here's an overview of how DNS attacks work:

DNS Spoofing/Cache Poisoning:
In DNS spoofing or cache poisoning attacks, attackers manipulate the DNS cache of a DNS server to redirect users to malicious websites or IP addresses.
Attackers send falsified DNS response packets containing forged information (e.g., incorrect IP addresses for legitimate domain names) to the DNS server, which caches the bogus information.
When users attempt to access the affected domain name, their systems query the compromised DNS server, which returns the spoofed IP address, leading users to the attacker-controlled site instead of the legitimate one.

DNS Amplification:
DNS amplification attacks exploit vulnerable open DNS servers to amplify and reflect malicious traffic to a target victim.
Attackers send DNS queries with spoofed source IP addresses to open DNS resolvers, requesting large DNS response packets for a specific domain name.
The DNS server, unaware of the spoofed source IP addresses, sends the amplified DNS responses (much larger than the original queries) to the victim's IP address, overwhelming its network bandwidth and resources.

DNS Flood:
DNS flood attacks overwhelm DNS servers with a high volume of DNS query traffic, exhausting server resources and causing service disruption.
Attackers use botnets or distributed networks to generate a large number of DNS query requests, flooding the target DNS server with more queries than it can handle.
The flood of DNS queries consumes server resources such as CPU, memory, and network bandwidth, leading to degraded performance or downtime.

DNS Hijacking:
DNS hijacking attacks involve modifying DNS records or compromising DNS servers to redirect users to malicious websites or IP addresses.
Attackers gain unauthorized access to DNS servers or domain registrar accounts to change DNS records, replacing legitimate IP addresses with malicious ones.
When users attempt to access the affected domain name, their systems receive the forged DNS responses, directing them to the attacker-controlled site instead of the intended destination.

DNS Tunneling:
DNS tunneling attacks covertly exfiltrate data or bypass network security controls by encoding data within DNS queries and responses.
Attackers encode data payloads within DNS queries or responses, leveraging DNS as a communication channel to bypass firewalls or intrusion detection systems.
DNS tunneling allows attackers to establish command-and-control (C2) channels, exfiltrate

sensitive information, or evade network monitoring and filtering mechanisms.

10. Give different techniques of common DOS attack

11. Explain Smurf attack in detail.

Ans:

A Smurf attack is a type of amplification DDoS attack that exploits the Internet Control Message Protocol (ICMP) and IP broadcast addresses to flood a victim's network with a large volume of traffic, causing it to become overwhelmed and unavailable.

The Smurf attack relies on the ability to forge the source IP address of ICMP echo request (ping) packets, leading to a reflection and amplification effect that magnifies the impact of the attack.

Here's how a Smurf attack typically works:

Attacker Spoofs Source IP Address: The attacker sends ICMP echo request packets (ping) to a network's broadcast address, but with the source IP address spoofed to appear as the victim's IP address.

Broadcast Amplification: The ICMP echo request packets are broadcast to all devices within the targeted network, prompting them to respond with ICMP echo reply packets (pings). Since the source IP address in the echo request packets is spoofed as the victim's IP address, all responses are directed back to the victim's network.

Traffic Overload: As the responses flood the victim's network, the volume of incoming traffic overwhelms its capacity, saturating bandwidth, consuming network resources, and potentially causing network devices to crash or become unreachable.

Smurf attacks are particularly effective because they leverage the broadcast nature of ICMP and the amplification effect of IP broadcasts, allowing attackers to generate a large volume of traffic with relatively little effort.

Additionally, the attack traffic appears to originate from legitimate sources within the network, making it challenging to filter out or block using traditional network security measures.

12. Differentiate between Bots and Botnets

Ans:

Point of Comparison	Bots	Botnets
Definition	Automated software programs	Networks of infected computers
Purpose	Perform automatic chores, whether good or bad.	Controlled by a central command server
Communication	It is possible to communicate with a command server.	Inter-botnet communication
Infection Method	Infected by malware or social engineering techniques	Malware infection, followed by replication via self-propagation or command and control servers
Botmaster/Bot Herder	Controls and manages the bots	Controls and commands the botnet
Size	Individual instances	The number of people might range from a few to millions.
Payload Delivery	Spamming, DDoS attacks, data theft, and more uses are possible.	Executes coordinated assaults, spamming, data theft, cryptocurrency mining, and so on.
Persistence	It is possible that it will remain on the system until it is deleted.	Remains connected to the botnet may.
Botnet Size and Reach	Individual bot	Can span globally
Examples	Web crawlers, chatbots	Mirai, Zeus, Necurs, Emotet, Conficker

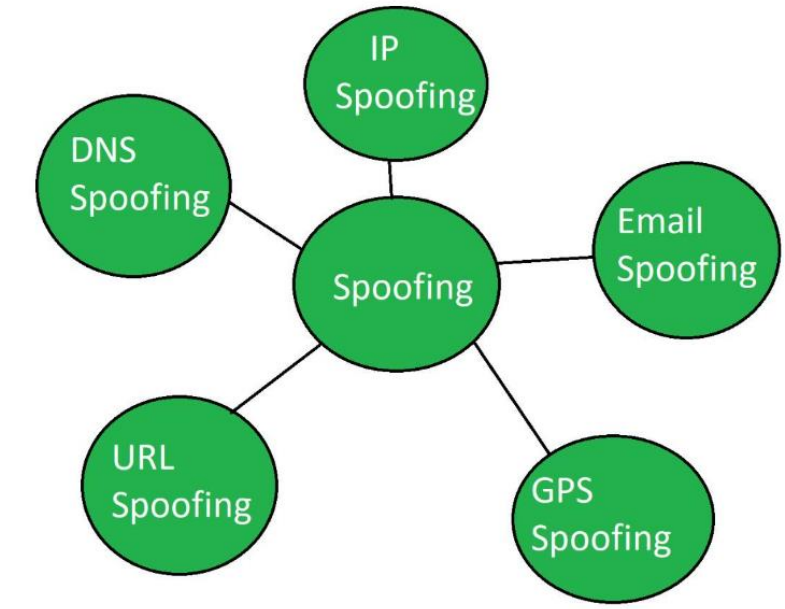
13. Explain DoS/DDoS countermeasures

Ans:

DOS	DDOS
DOS Stands for Denial of service attack.	DDOS Stands for Distributed Denial of service attack.
In Dos attack single system targets the victim system.	In DDoS multiple systems attacks the victims system..
Victim PC is loaded from the packet of data sent from a single location.	Victim PC is loaded from the packet of data sent from Multiple location.
Dos attack is slower as compared to DDoS.	DDoS attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations.
In DOS Attack only single device is used with DOS Attack tools.	In DDoS attack,The volumeBots are used to attack at the same time.
DOS Attacks are Easy to trace.	DDOS Attacks are Difficult to trace.
Volume of traffic in the Dos attack is less as compared to DDos.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim network.
Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack 4. Flooding Attack	Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks 4. Protocol Attack.

14. What is spoofing? Give its types.

Ans:**Refer q No 15 defination**



Types of Spoofing:

IP Spoofing:
IP spoofing involves forging the source IP address in packets to impersonate a trusted source or evade detection.
Attackers use IP spoofing to launch various types of attacks, such as denial-of-service (DoS) attacks, distributed denial-of-service (DDoS) attacks, or bypassing access controls by impersonating trusted hosts.

Email Spoofing:
Email spoofing involves forging the sender's email address in email messages to impersonate a legitimate sender or organization.
Attackers use email spoofing to deceive recipients into believing that the email is from a trusted source, leading to phishing scams, malware distribution, or social engineering attacks.

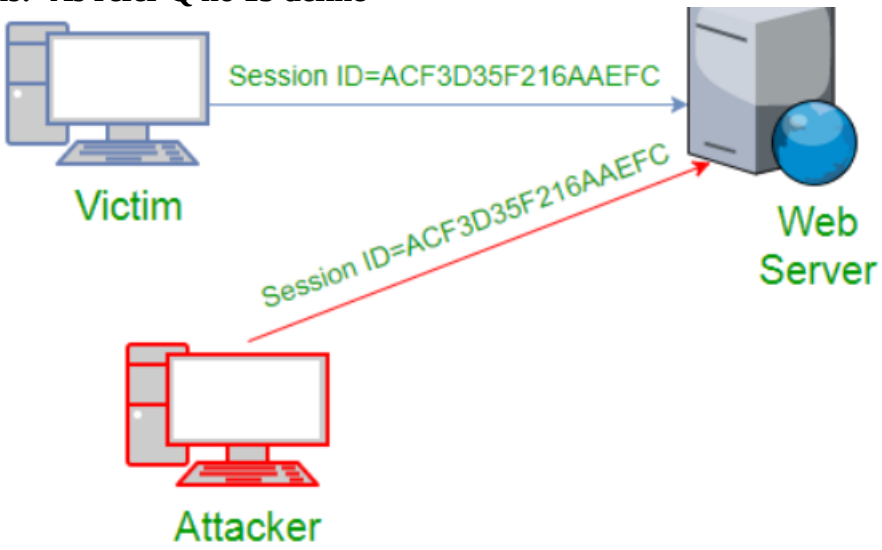
DNS Spoofing:
DNS spoofing, also known as DNS cache poisoning or DNS hijacking, involves manipulating DNS (Domain Name System) responses to redirect users to malicious or fake websites.
Attackers modify DNS records or compromise DNS servers to associate malicious IP addresses with legitimate domain names, leading users to unintended destinations.

GPS Spoofing
Here, cybercriminals may try to manipulate a user's device's GPS receiver into signalling inaccurate pop-ups.
The logic behind it is pretty different from regular spoofing, and it is mainly done to give long-term losses to the target. For example, a CEO who is in a hurry for an important meeting with a potential business partner may take a wrong turn, only to get stuck in traffic and be late for the conference, leading to the deal getting cancelled.

URL /Website Spoofing:
As the name suggests here, the hackers try to copy the layout, branding, and sign-in forms of original web pages and Pair them with the DNS spoofing trick to hack the data.
Sometimes backdoor tactic is also combined with this which may also lead to identity theft.

15. What are preventive measures on hijacking.

14. What is hijacking give its types.
Ans:- As refer Q no 15 define



Types of Hijacking:

Session Hijacking:
Session hijacking, also known as TCP hijacking or cookie hijacking, involves intercepting and taking control of an existing communication session between two parties.
Attackers exploit vulnerabilities in network protocols or session management mechanisms to hijack session identifiers (e.g., session cookies) and impersonate legitimate users.
Common techniques include session fixation, where attackers force users to use predetermined session IDs, and session sniffing, where attackers capture session cookies from network traffic.

DNS Hijacking:
DNS hijacking, also known as DNS redirection or DNS poisoning, involves redirecting DNS (Domain Name System) queries to malicious or unauthorized DNS servers controlled by attackers.
Attackers manipulate DNS records or compromise DNS servers to redirect users to malicious websites, phishing pages, or spoofed servers.
DNS hijacking can lead to traffic interception, data theft, and the redirection of users to fake or malicious websites without their knowledge.

ARP Hijacking (ARP Spoofing):
ARP (Address Resolution Protocol) hijacking, also known as ARP spoofing or ARP poisoning, involves manipulating ARP cache entries to associate the attacker's MAC address with the IP address of a legitimate network resource.
By impersonating the MAC address of a legitimate device, attackers can intercept, modify, or redirect network traffic intended for that device.
ARP hijacking attacks are commonly used in man-in-the-middle (MITM) attacks to eavesdrop on communications, perform packet sniffing, or launch further attacks on the compromised network.

Clickjacking:
Clickjacking, also known as UI redress attack or user interface (UI) manipulation, involves

tricking users into clicking on hidden or disguised elements on a web page.
Attackers overlay transparent or opaque layers over legitimate web content to deceive users into unknowingly clicking on malicious elements or performing unintended actions.
Clickjacking attacks can lead to the theft of sensitive information, unauthorized actions on web applications, or the installation of malware on users' devices.

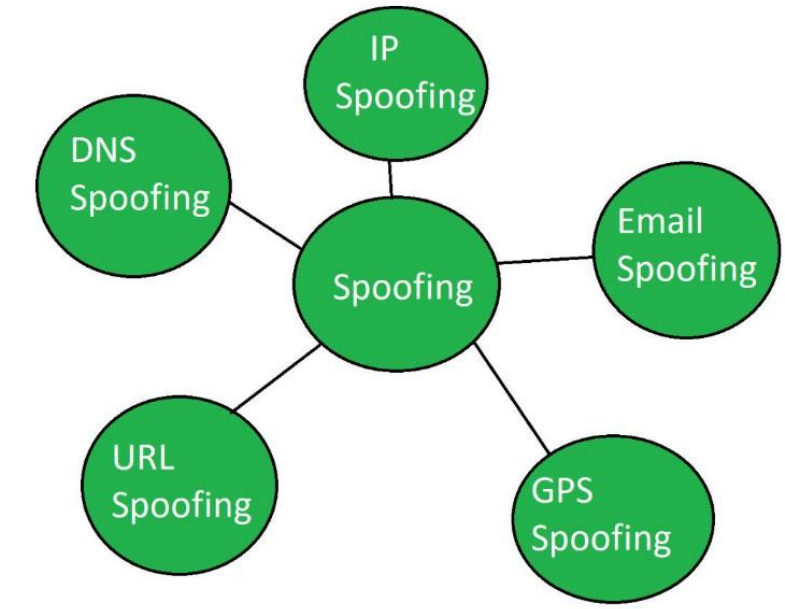
App Hijacking (Mobile App Hijacking):
App hijacking involves compromising or taking control of mobile applications to perform unauthorized actions, access sensitive data, or manipulate user interactions.
Attackers may exploit vulnerabilities in mobile apps, operating systems, or third-party libraries to inject malicious code, tamper with app behavior, or bypass security controls.
App hijacking can result in the theft of personal information, financial fraud, or unauthorized access to device resources and permissions.

15. Explain the difference between spoofing and hijacking

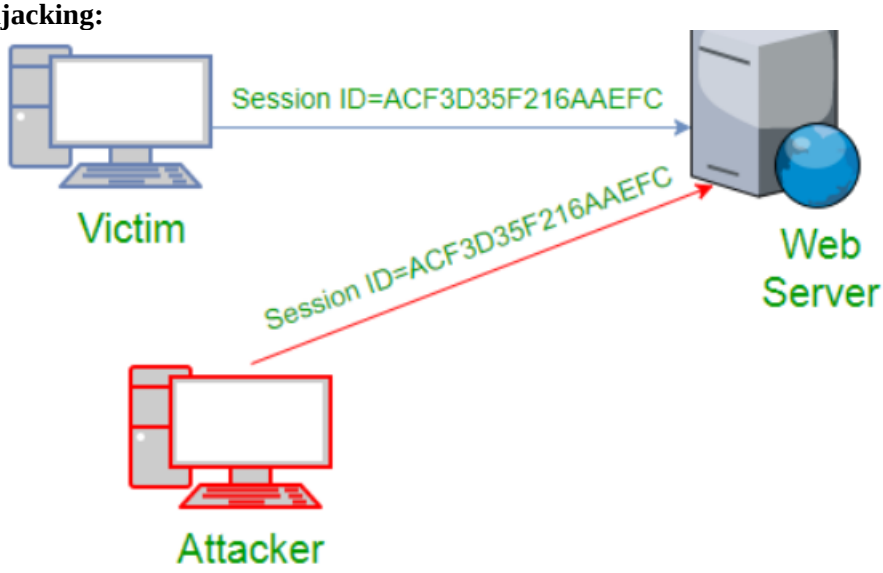
Ans:

Feature	Spoofing	Hijacking
Definition	Impersonating another entity or source	Taking control of an existing legitimate entity
Objective	Deceive or manipulate recipients or systems	Gain unauthorized access or control over resources
Nature	Precedes or initiates a communication	Involves interception or takeover of ongoing communication
Types	IP spoofing, email spoofing, DNS spoofing	Session hijacking, DNS hijacking, ARP hijacking
Method	Manipulating headers, forging identities	Intercepting or redirecting traffic, taking control of sessions
Impact	Can lead to identity theft, data breaches	Enables unauthorized access, data tampering, or denial of service
Examples	- IP spoofing in DDoS attacks - Email spoofing in phishing scams	- Session hijacking in man-in-the-middle attacks - DNS hijacking to redirect traffic

Spoofing diagram:



Hijacking:



16. Explain sniffing countermeasures.

Ans:

Sniffing, also known as packet sniffing or network sniffing, is the process of intercepting and analyzing network traffic to capture sensitive information, such as usernames, passwords, or confidential data.

Sniffing attacks pose a significant security risk, as attackers can eavesdrop on unencrypted network communications and collect sensitive information without the knowledge of the users or system administrators.

To mitigate the risk of sniffing attacks, several countermeasures can be implemented:

Encryption:

Implement strong encryption protocols, such as SSL/TLS for web traffic or IPSec for network communication, to encrypt sensitive data transmitted over the network. Encryption ensures that even if the traffic is intercepted, it remains unreadable and secure.

Use of Virtual Private Networks (VPNs):

Encourage or mandate the use of VPNs, especially for remote access or when connecting to untrusted networks. VPNs create secure, encrypted tunnels for data transmission, protecting traffic from sniffing attacks on insecure networks.

Network Segmentation:
Segment the network into separate subnets or VLANs (Virtual Local Area Networks) and use firewalls or access control lists (ACLs) to restrict access between segments. By isolating sensitive systems and data from other parts of the network, the impact of sniffing attacks can be minimized.

Switched Networks:
Deploy switched networks instead of traditional hub-based networks. Switched networks isolate traffic between network devices, making it more difficult for attackers to capture network packets intended for other devices.

Port Security:
Enable port security features, such as MAC address filtering or port lockdown, on network switches to prevent unauthorized devices from connecting to the network and potentially conducting sniffing attacks.

Network Monitoring and Intrusion Detection:
Deploy network monitoring tools and intrusion detection systems (IDS) to detect anomalous or suspicious network activity indicative of sniffing attacks. IDS can analyze network traffic in real-time and raise alerts when unusual patterns or behaviors are detected.

Use of Encrypted Protocols:
Use encrypted communication protocols, such as HTTPS for web browsing, SSH for remote access, and SFTP for file transfers, to protect data transmitted over the network. Encrypted protocols ensure that sensitive information is protected from eavesdropping.

Regular Security Audits and Penetration Testing:
Conduct regular security audits and penetration tests to identify vulnerabilities in the network infrastructure and detect potential sniffing vulnerabilities. Addressing identified weaknesses and implementing security best practices helps strengthen the overall security posture of the network.

Employee Training and Awareness:
Educate employees and system users about the risks associated with sniffing attacks and the importance of secure communication practices. Promote awareness of phishing scams, social engineering tactics, and safe browsing habits to minimize the likelihood of successful sniffing attacks.

17. What is web server explain types of attacks against web server
Ans:
Web servers are where websites are stored.

They are computers that run an operating system and are connected to a database to run multiple applications.

A web server's primary responsibility is to show website content by storing, processing, and distributing web pages to users.

Types of attacks:

1. DENIAL-OF-SERVICE (DOS) / DISTRIBUTED DENIAL-OF-SERVICE (DDOS): Denial of Service is when an internet hacker causes the web to provide a response to a large number of requests. This causes the server to slow down or crash and users authorized to use the server will be denied service or access. Government services, credit card companies under large corporations are common victims of this type of attack

2. WEB DEFACEMENT ATTACK: 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.

3. SSH BRUTE FORCE ATTACK: 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

4. CROSS SITE SCRIPTING (XSS): 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.

5. DIRECTORY TRAVERSAL: Directory Traversal Attack is usually effective on older servers with vulnerabilities and misconfiguration. The root directory is where web pages are stored, however, in this attack, the hacker is after directories outside of the root directory.

6. DNS SERVER HIJACKING: 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.

7. MITM ATTACK: 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.

8. HTTP RESPONSE SPLITTING ATTACK: 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.

18. Explain patch management techniques.

Ans:
A patch is a piece of software code (usually made up of one or more files) written by a programmer to fix and update an application or file.

Patches are created to fix problems and improve the functionality of computer applications and operating systems.

They can be applied to both the Linux and Windows platforms, but do not work on Mac

computers.

Patches or updates are released by the utility vendors to fix existing bugs and provide new features.

Updating your system with patches is an important part of protecting it from cyberattacks and exploits.

Patch Management is a tactic in which an ethical hacker focuses on the software compatibility of various versions for a number of devices, computers, and operating systems.

It is significant to know the differences between each patch and what the implications are for different types of devices.

A patch manager can help determine which patches are appropriate and when they should be deployed.

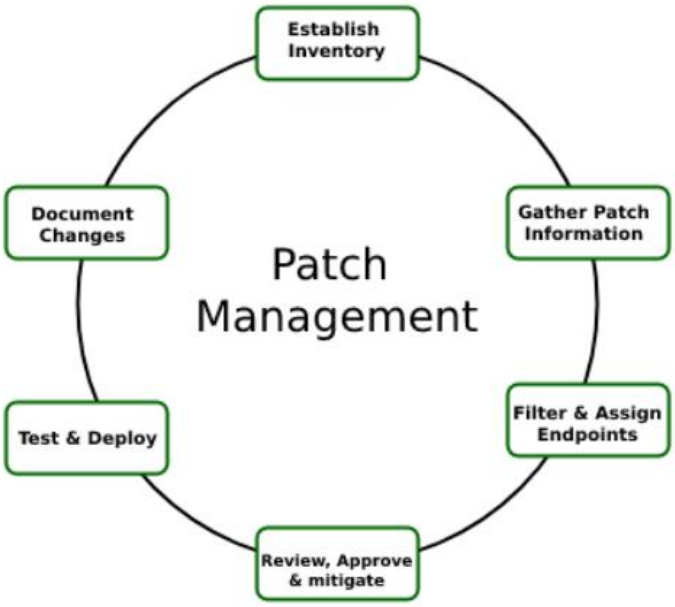
When there is a brand-new OS release, such as iOS 8 or Windows 8, there may be many new patches released even before it has been released to consumers, so it is essential that organizations have a strategy in place to patch these machines in timely releases as well as ensure that these patches reach their target audience.

Types of Patches:

General distribution release (GDR) – An update that contains fixes for bugs that have been reported and verified.

Security-only distribution release (SDR) – Released on Microsoft Update when only security fixes are available in the GDR branch. Fixes and enhancements will be included in the next GDR branch availability, where applicable.

Structure of Patch Management System



19. Write steps for web server hardening.

20. What is vulnerability, explain web server vulnerabilities.

Unit 3

1. What is web application ? Explain the vulnerabilities in web application.
Ans:
A web application is a software application that runs on a web server and is accessed via a web browser over a network, typically the internet.

These applications are designed to provide interactive experiences to users, allowing them to perform various tasks or access information through a user-friendly interface.

Web applications can range from simple websites with static content to complex systems with dynamic functionality, such as online banking portals, e-commerce platforms, social media networks, and more.

They often rely on server-side scripting languages (like PHP, Python, or Ruby) and client-side technologies (like HTML, CSS, and JavaScript) to deliver content and interactivity.

Some common vulnerabilities in web applications include:

Injection Attacks: Injection flaws, such as SQL injection and cross-site scripting (XSS), occur when an attacker injects malicious code into a web application, which can then be executed within the application's environment. This can lead to unauthorized access, data leakage, or manipulation of sensitive information.

Broken Authentication: Weaknesses in authentication mechanisms can allow attackers to compromise user accounts, gain unauthorized access to sensitive data, or perform actions on behalf of legitimate users. Common examples include weak passwords, session hijacking, and brute force attacks.

Sensitive Data Exposure: If sensitive data, such as user credentials or financial information, is not properly protected, it may be exposed to unauthorized parties. This can occur due to insecure storage, improper encryption, or inadequate access controls.

Cross-Site Request Forgery (CSRF): CSRF attacks exploit the trust that a web application has in a user's browser by tricking the user into unknowingly executing malicious actions on the application. This can lead to unauthorized transactions, data manipulation, or account compromise.

Security Misconfigurations: Improperly configured servers, frameworks, or security controls can leave web applications vulnerable to exploitation. This includes default settings, unnecessary services, outdated software, and incomplete access controls.

Broken Access Control: Flaws in access control mechanisms can allow unauthorized users to access restricted functionality or data within a web application. This includes privilege escalation, directory traversal, and insecure direct object references.

Insecure Deserialization: Deserialization vulnerabilities occur when untrusted data is

deserialized by a web application, leading to potential remote code execution or other attacks. Attackers can exploit this weakness to execute arbitrary code, manipulate objects, or bypass security controls.

Insecure File Uploads: If a web application allows users to upload files without proper validation and sanitization, it can be vulnerable to various attacks, such as executable file uploads, file overwrite, or malicious file inclusion.

2. What are the phases of web application hacking.

Reconnaissance: This phase involves gathering information about the target web application and its environment. Techniques may include passive reconnaissance (e.g., browsing the application's website, searching for publicly available information) and active reconnaissance (e.g., using tools like web scrapers, WHOIS lookup, DNS enumeration).

Scanning: In this phase, the attacker scans the target web application for potential vulnerabilities and weaknesses. This may involve automated tools (such as vulnerability scanners) and manual inspection to identify entry points, exposed services, and known vulnerabilities**.**

Enumeration: Enumeration involves actively probing the target application to gather more detailed information about its structure, functionality, and potential attack surface. Techniques may include directory and file enumeration, parameter enumeration, and probing for hidden functionality or APIs.

Vulnerability Analysis: Once potential vulnerabilities are identified, the attacker analyzes them to assess their impact and exploitability. This may involve further investigation, testing, and verification of vulnerabilities to determine their severity and potential impact on the application's security.

Exploitation: In this phase, the attacker attempts to exploit the identified vulnerabilities to gain unauthorized access or perform malicious actions within the target application. Depending on the nature of the vulnerabilities, exploitation may involve various techniques, such as injection attacks, authentication bypass, privilege escalation, or session hijacking.

Post-Exploitation: After successfully exploiting vulnerabilities, the attacker may perform post-exploitation activities to maintain access, escalate privileges, or extract sensitive information from the target application. This may involve installing backdoors, escalating privileges, planting malware, or exfiltrating data.

Covering Tracks: To avoid detection and maintain access to the compromised system, the attacker may attempt to cover their tracks by deleting logs, modifying timestamps, and removing evidence of their activities. This helps prolong the unauthorized access and makes it more challenging for defenders to detect and respond to the attack.

3. Define web application threats and its types

Ans: Refer q no 1 In unit 3

4. Define term

A. Threats

B. Malware

C. Phishing

Ans :

A. Threats:

Threats refer to potential dangers or risks that can harm individuals, organizations, systems, or assets.

In the context of cybersecurity, threats encompass various malicious activities, tactics, and vulnerabilities that can compromise the confidentiality, integrity, and availability of information and resources.

These threats can include attacks from malicious actors, such as hackers, malware, and insiders, as well as natural disasters, human errors, and other unforeseen events that pose risks to security and operations.

B. Malware:

Malware, short for malicious software, is any type of software intentionally designed to cause damage, disrupt operations, or gain unauthorized access to computer systems, networks, or data.

Malware includes a wide range of malicious programs, such as viruses, worms, trojans, ransomware, spyware, and adware.

It typically spreads through various vectors, including email attachments, infected websites, removable media, and network vulnerabilities.

Once installed on a system, malware can perform various malicious activities, such as stealing sensitive information, encrypting files, disrupting services, or remotely controlling the infected device.

C. Phishing:

Phishing is a type of cyber attack that involves the use of deceptive emails, messages, or websites to trick individuals into disclosing sensitive information, such as login credentials, financial details, or personal data.

Phishing attacks often impersonate trusted entities, such as banks, social media platforms, or government agencies, and typically employ psychological manipulation techniques to persuade victims to take action, such as clicking on malicious links, downloading malicious attachments, or entering their information into fake forms.

Phishing attacks can lead to identity theft, financial fraud, account compromise, and other security incidents

.

5. What is Google hacking

Ans :

Google hacking, also known as Google dorking or Google hacking database (GHDB), refers to the use of advanced search techniques and operators in Google's search engine to discover sensitive information, vulnerabilities, and misconfigurations on websites and web servers.

Despite its name, Google hacking does not involve exploiting Google's security; rather, it leverages Google's powerful search capabilities to uncover potentially valuable or sensitive data that is publicly accessible on the internet.

Google hacking relies on operators and search syntax to refine search queries and uncover specific types of information.

Some common Google operators used in Google hacking include:

site: Limits the search to a specific domain or website.

Example: site:example.com

inurl: Searches for URLs containing a specific string.

Example: inurl:admin

intitle: Searches for pages with a specific keyword or phrase in the title.

Example: intitle:"index of"

filetype: Limits the search to specific file types or extensions.

Example: filetype:pdf

cache: Retrieves the cached version of a webpage as indexed by Google.

Example: cache:example.com

By combining these operators with specific keywords and search strings, users can uncover a wide range of information, including sensitive files, directories, login pages, error messages, exposed services, and more.

This information can be valuable for security professionals, researchers, and attackers alike to identify potential security risks, vulnerabilities, and misconfigurations that may exist within a target organization's web presence.

It's important to note that while Google hacking can provide valuable insights into the security posture of a website or web server, it should only be performed ethically and in accordance with applicable laws and regulations.

Unauthorized access to or exploitation of sensitive information discovered through Google hacking is illegal and unethical.

6. What are countermeasures to prevent web application vulnerabilities

Ans:

To prevent web application vulnerabilities and enhance overall security, organizations should implement a combination of technical measures, best practices, and security controls throughout the development lifecycle.

Here are some countermeasures to consider:

Secure Coding Practices: Train developers on secure coding principles and best practices, such as input validation, output encoding, proper error handling, and secure authentication mechanisms. Use secure coding guidelines, frameworks, and libraries to minimize the risk of introducing vulnerabilities during development.

Input Validation and Sanitization: Validate and sanitize all user inputs to prevent injection attacks, such as SQL injection (SQLi) and Cross-Site Scripting (XSS). Use whitelisting and parameterized queries to mitigate injection risks and ensure that user-supplied data is safe to use.

Output Encoding: Encode output data to prevent XSS attacks and ensure that user-generated content is displayed safely within web pages. Use appropriate encoding techniques, such as HTML entity encoding, to escape special characters and prevent script

execution in browsers.

Authentication and Access Controls: Implement strong authentication mechanisms, such as multi-factor authentication (MFA), strong password policies, and account lockout mechanisms, to protect user accounts from unauthorized access. Enforce least privilege access controls to restrict user permissions and limit exposure to sensitive functionality and data.

Session Management: Use secure session management practices, such as session tokens with strong entropy, secure cookies with the "HttpOnly" and "Secure" flags, and session expiration controls, to protect user sessions from hijacking and fixation attacks.

Security Headers: Utilize security headers, such as Content Security Policy (CSP), HTTP Strict Transport Security (HSTS), and X-Content-Type-Options, to mitigate various web security risks, including XSS, clickjacking, and MIME sniffing attacks.

Regular Security Testing: Perform regular security assessments, including vulnerability scanning, penetration testing, and code reviews, to identify and remediate security vulnerabilities in web applications proactively. Consider using automated scanning tools and manual testing techniques to identify vulnerabilities across different layers of the application stack.

Patch Management: Keep software dependencies, frameworks, libraries, and web server components up to date with the latest security patches and updates. Establish a patch management process to ensure timely deployment of security fixes and minimize exposure to known vulnerabilities.

Web Application Firewalls (WAF): Deploy WAF solutions to monitor and filter incoming web traffic for suspicious activities and known attack patterns. Configure WAF rulesets to block malicious requests, prevent common web attacks, and enforce security policies at the network perimeter.

Security Education and Awareness: Train employees, developers, and stakeholders on web security best practices, common vulnerabilities, and emerging threats. Foster a security-aware culture within the organization and encourage proactive reporting of security incidents and concerns.

7. Define term password hacking and what are web based cracking techniques

Ans: Refer Answer for unit 2 Qno 1.

8. Define term authentication and its types

Ans:

Authentication is the process of verifying the identity of a user or system entity attempting to access a resource, system, or application.

It ensures that only authorized individuals or entities are granted access to protected resources or services.

Authentication typically involves presenting credentials, such as usernames and passwords, tokens, biometric data, or digital certificates, to validate the identity of the user or entity.

There are several types of authentication methods used to verify identities and grant access to resources.

Here are some common types of authentication:

Password-based Authentication: Password-based authentication requires users to provide a username and password to access a system or application. The system compares the provided credentials against stored credentials in a database or directory service. While passwords are widely used, they are susceptible to security risks such as brute force attacks, phishing, and password reuse.

Multi-factor Authentication (MFA): Multi-factor authentication (MFA), also known as two-factor authentication (2FA) or multi-step verification, requires users to provide two or more types of credentials to authenticate their identity. This typically involves combining something the user knows (e.g., a password) with something they have (e.g., a mobile device or hardware token) or something they are (e.g., biometric data such as fingerprints or facial recognition). MFA enhances security by adding an extra layer of verification beyond just a password.

Biometric Authentication: Biometric authentication uses unique physical characteristics of an individual, such as fingerprints, iris patterns, facial features, or voice recognition, to verify their identity. Biometric authentication provides a high level of security and convenience, as biometric traits are difficult to forge or replicate. However, biometric systems may face challenges related to accuracy, privacy, and compatibility with different devices and environments.

Token-based Authentication: Token-based authentication involves issuing and validating cryptographic tokens, such as one-time passwords (OTPs), security tokens, or digital certificates, to authenticate users. Tokens are typically generated by a trusted authority and are used as temporary credentials to prove the user's identity during the authentication process. Token-based authentication is commonly used in MFA systems and secure communication protocols.

Single Sign-On (SSO): Single Sign-On (SSO) is a centralized authentication mechanism that allows users to access multiple related systems or applications using a single set of credentials. Once authenticated, users are granted access to all associated resources without the need to re-enter their credentials for each application. SSO enhances user convenience and productivity while simplifying identity management for administrators.

Adaptive Authentication: Adaptive authentication analyzes various factors, such as user behavior, location, device information, and network context, to dynamically adjust the authentication requirements based on the perceived risk level. By continuously evaluating risk factors, adaptive authentication systems can adapt their security measures to provide appropriate levels of protection while minimizing user friction.

9. What is password cracking and name tools used in password cracking

Ans: Refer this answer for the unit 2 Qno 1.

10. Define SQL injection and name it's types

Ans:

SQL injection (SQLi) is a type of security vulnerability that occurs when an attacker inserts malicious SQL code into input fields or parameters of a web application's SQL query, thereby manipulating the application's database and executing unauthorized SQL commands.

SQL injection attacks can have various consequences, including unauthorized access to sensitive data, modification of database records, data leakage, and even complete takeover of the underlying server.

SQL injection attacks pose a significant threat to web applications that use SQL databases to store and retrieve data.

To mitigate the risk of SQL injection vulnerabilities, developers should adopt secure coding practices, such as using parameterized queries or prepared statements, input validation and sanitization, least privilege access controls, and regular security testing and code reviews.

Here are some common types of SQL injection attacks:

In-band SQL Injection (Classic SQLi):

In-band SQL injection is the most common type of SQLi attack.

In this type of attack, the attacker uses the same communication channel to both inject the malicious SQL code and retrieve the results.

Examples include UNION-based SQL injection and error-based SQL injection.

Blind SQL Injection:

Blind SQL injection occurs when the application does not directly reveal the results of the injected SQL queries to the attacker.

Instead, the attacker must infer information about the database by observing differences in the application's behavior, such as response times or error messages.

Blind SQL injection can be further classified into:

Boolean-based Blind SQL Injection: The attacker sends SQL queries that rely on Boolean conditions to extract information from the database.

Time-based Blind SQL Injection: The attacker uses time delays in SQL queries to infer information about the database.

Out-of-band SQL Injection:

Out-of-band SQL injection occurs when the attacker is able to trigger the execution of SQL queries, but cannot directly retrieve the results through the same channel.

Instead, the attacker leverages alternative communication channels, such as DNS requests or HTTP requests, to extract data from the database.

Out-of-band SQL injection is less common but can be effective in certain scenarios, particularly when traditional in-band techniques are not feasible.

11. Define vulnerabilities in SQL server

Ans:

SQL Server vulnerabilities are weaknesses or flaws in Microsoft SQL Server, a relational database management system (RDBMS), that can be exploited by attackers to compromise the confidentiality, integrity, or availability of data stored in the database.

These vulnerabilities can arise from various sources, including software bugs, configuration errors, insecure coding practices, and design flaws.

Exploiting SQL Server vulnerabilities can lead to unauthorized access, data leakage, data manipulation, denial of service, and other security incidents.

It is essential for organizations to regularly monitor for and remediate SQL Server vulnerabilities to protect sensitive information and maintain a secure database environment.

Vulnerabilities in SQL Server refer to weaknesses or flaws in the Microsoft SQL Server database management system that could be exploited by attackers to compromise the security, integrity, or availability of the database and associated data.

These vulnerabilities can arise due to coding errors, misconfigurations, design flaws, or weaknesses in the software itself, making the database susceptible to various types of attacks and security breaches.

Common vulnerabilities in SQL Server include:

SQL Injection (SQLi): SQL injection vulnerabilities occur when input provided by users or external sources is not properly sanitized or validated before being included in SQL queries. Attackers can exploit these vulnerabilities to inject malicious SQL code, manipulate database queries, and execute unauthorized commands, potentially leading to data leakage, data manipulation, or unauthorized access.

Weak Authentication and Authorization: Weak or misconfigured authentication and authorization mechanisms in SQL Server can lead to unauthorized access to sensitive data or administrative privileges. This includes default or weak passwords, misconfigured permissions, and inadequate access controls, which may allow attackers to gain unauthorized access to databases or escalate privileges.

Insecure Configuration: Insecure configuration settings in SQL Server, such as default configurations, unnecessary services, and weak encryption settings, can expose databases to various security risks. Attackers may exploit these vulnerabilities to gain unauthorized access, perform denial-of-service (DoS) attacks, or extract sensitive information from the database.

Unpatched Software: Failure to apply security patches and updates to SQL Server can leave databases vulnerable to known vulnerabilities and exploits. Attackers may target unpatched systems to exploit known vulnerabilities and gain unauthorized access, execute arbitrary code, or compromise data stored in the database.

Data Exposure and Leakage: Improper handling of sensitive data, such as plaintext storage of passwords or encryption keys, can lead to data exposure and leakage vulnerabilities in SQL Server. Attackers may exploit these vulnerabilities to steal sensitive information, such as personally identifiable information (PII), financial data, or intellectual property, stored in the database.

Buffer Overflows and Memory Corruption: Buffer overflows and memory corruption vulnerabilities in SQL Server can be exploited by attackers to execute arbitrary code, crash the database server, or gain unauthorized access to sensitive data. These vulnerabilities may arise due to coding errors, memory management issues, or insecure programming practices in the software.

Denial-of-Service (DoS) Attacks: SQL Server may be vulnerable to denial-of-service

(DoS) attacks that overload the database server with excessive requests, causing it to become unresponsive or crash. These attacks can disrupt services, cause downtime, and impact the availability of critical business applications relying on the database.

12. What is buffer overflow explain its types

Ans:

A buffer overflow is a type of software vulnerability that occurs when a program attempts to write data beyond the boundaries of a fixed-size buffer, leading to memory corruption and potentially exploitable behavior. Buffer overflows can be exploited by attackers to execute arbitrary code, crash the program, or gain unauthorized access to system resources.

There are several types of buffer overflow vulnerabilities, each with its own characteristics and exploitation techniques:

Stack-based Buffer Overflow:

In a stack-based buffer overflow, the buffer overflow occurs on the program's call stack, typically in local variables or function parameters.

Attackers exploit stack-based buffer overflows by overwriting return addresses, function pointers, or other critical data stored on the stack to redirect program execution to malicious code or shellcode injected by the attacker.

Stack-based buffer overflows are one of the most common types of buffer overflow vulnerabilities and are often found in programs written in languages like C and C++ that use fixed-size buffers without proper bounds checking.

Heap-based Buffer Overflow:

In a heap-based buffer overflow, the buffer overflow occurs in dynamically allocated memory on the program's heap.

Attackers exploit heap-based buffer overflows by corrupting heap metadata, such as heap block headers or allocation metadata, to manipulate memory allocations or overwrite adjacent memory regions.

Heap-based buffer overflows are typically more complex and less predictable than stack-based buffer overflows but can still be exploited to achieve arbitrary code execution or other malicious outcomes.

Integer Overflow:

Integer overflow vulnerabilities occur when arithmetic operations on integers result in overflow, leading to unexpected behavior or buffer overflow conditions.

Attackers can exploit integer overflow vulnerabilities to bypass boundary checks, allocate insufficient memory, or cause other unintended consequences that may lead to buffer overflows or other security issues.

Integer overflow vulnerabilities are common in programs written in languages like C and C++ that perform arithmetic operations without proper overflow checks.

Format String Vulnerability:

Format string vulnerabilities occur when user-controlled input is passed directly to format string functions, such as printf or sprintf, without proper validation or formatting.

Attackers can exploit format string vulnerabilities to read or write arbitrary memory addresses, leak sensitive information, or execute arbitrary code by supplying carefully crafted format strings containing format specifiers and corresponding arguments.

Format string vulnerabilities are prevalent in programs written in C and C++ and can lead to serious security issues if not properly mitigated.

13. Define stack based buffer overflow

Ans:

A stack-based buffer overflow is a type of software vulnerability that occurs when a program writes data beyond the bounds of a fixed-size buffer allocated on the call stack, leading to memory corruption and potential exploitation.

The call stack is a region of memory used by a program to manage function calls, local variables, and return addresses during program execution.

In a stack-based buffer overflow, the buffer overflow occurs within the stack frame of a function, typically in local variables or function parameters.

The vulnerability arises when the program copies or receives input data into a buffer without proper bounds checking, allowing an attacker to overwrite adjacent memory regions, such as return addresses or function pointers, stored on the stack.

Here's how a stack-based buffer overflow typically occurs:

The program allocates a fixed-size buffer on the stack to store input data, such as user input or network data.

The program copies or receives input data into the buffer without verifying its length or ensuring that it fits within the allocated buffer size.

If the input data exceeds the size of the buffer, it overflows beyond the buffer boundaries and overwrites adjacent memory regions on the stack, such as return addresses, function pointers, or saved registers.

By carefully crafting the input data, an attacker can overwrite critical stack data, manipulate program execution flow, and potentially execute arbitrary code or trigger unintended behavior.

Exploiting a stack-based buffer overflow typically involves injecting malicious payload data, such as shellcode or exploit payloads, into the buffer to hijack control flow and execute arbitrary code.

By overwriting return addresses or function pointers with addresses pointing to the injected payload, the attacker can redirect program execution to the injected code, leading to unauthorized actions or system compromise.

To mitigate stack-based buffer overflow vulnerabilities, developers should adopt secure coding practices, such as using safe string manipulation functions, implementing bounds checking, and validating input data sizes to prevent buffer overflows.

Additionally, compilers and runtime environments may offer security features, such as stack canaries and address space layout randomization (ASLR), to detect or mitigate buffer overflow exploits at runtime.

14. Define term mutation in EH and explain mutation techniques

Ans:

In the context of exploit development and security testing, "mutation" refers to the process of modifying or altering the characteristics of a software vulnerability or exploit payload to evade detection, bypass security controls, or achieve specific objectives.

Mutation techniques are employed by attackers and security researchers to modify exploit payloads, shellcode, or malicious code in ways that make them more resilient to detection, prevention, or mitigation by security defenses.

Mutation techniques are commonly employed in exploit development, malware creation, and penetration testing to enhance the stealth, effectiveness, and resilience of malicious code against security defenses and detection mechanisms.

However, defenders and security practitioners also leverage mutation techniques to develop robust security controls, such as behavior-based detection systems, anomaly detection algorithms, and machine learning models, capable of identifying and mitigating mutated or polymorphic threats.

Mutation techniques aim to achieve various goals, including:

Polymorphism: Polymorphic techniques involve changing the appearance or structure of malicious code while preserving its functionality. This makes the code more difficult to detect using static signatures or pattern matching techniques employed by antivirus software and intrusion detection systems (IDS).

Obfuscation: Obfuscation techniques involve intentionally complicating the code structure or disguising its intent to hinder analysis and reverse engineering efforts by security researchers or malware analysts. Obfuscation may include techniques such as code encryption, variable renaming, control flow obfuscation, and data encoding.

Encoding and Encryption: Encoding and encryption techniques involve transforming the payload or code into a different representation, such as base64 encoding or cryptographic encryption. This helps conceal the payload's true content and make it more challenging for security tools to recognize and analyze.

Metamorphism: Metamorphic techniques go beyond polymorphism by completely restructuring or transforming the code each time it is executed, making it more resistant to signature-based detection techniques. Metamorphic malware continuously evolves its code to produce new variants that retain the same functionality but have different byte patterns.

Environment-awareness: Environment-aware mutation techniques adapt the behavior or characteristics of the payload based on environmental factors, such as the target system's architecture, operating system, installed software, or security controls. This allows attackers to tailor their attacks to specific target environments and increase their chances of success.

15. Explain WEP (wired equivalent privacy)in detail

Ans:

Refer the Que no 15

16. Write different ways to accomplish wireless hacking

Ans:

Wireless hacking refers to unauthorized access, exploitation, or manipulation of wireless networks, devices, and protocols.

Attackers employ various techniques and tools to compromise wireless networks and gain unauthorized access to sensitive information, exploit vulnerabilities, or disrupt network operations.

Here are different ways attackers can accomplish wireless hacking:

Wireless Sniffing: Attackers use wireless sniffing tools to capture and analyze wireless network traffic, including data packets transmitted over Wi-Fi, Bluetooth, or other wireless protocols. By intercepting and inspecting network traffic, attackers can eavesdrop on communications, capture sensitive information, and identify security vulnerabilities.

Brute Force Attacks: Attackers conduct brute force attacks against wireless networks to guess or crack passwords used for network authentication. Brute force attacks involve systematically trying all possible combinations of characters until the correct password is discovered. Tools like Aircrack-ng and Hashcat are commonly used for brute force attacks on Wi-Fi networks.

Dictionary Attacks: Similar to brute force attacks, dictionary attacks involve attempting to guess passwords by trying a list of commonly used words, phrases, or dictionary entries. Attackers use automated tools to systematically test each entry in the dictionary against the target network's authentication mechanism.

WPS Exploitation: Wi-Fi Protected Setup (WPS) is a feature designed to simplify the process of connecting devices to Wi-Fi networks. However, WPS implementations often contain security vulnerabilities that can be exploited by attackers to bypass authentication and gain access to the network. Tools like Reaver and Bully are used to exploit WPS vulnerabilities.

Evil Twin Attacks: In an evil twin attack, attackers set up a rogue wireless access point (AP) that mimics a legitimate AP within the vicinity. Unsuspecting users may connect to the rogue AP, thinking it is a legitimate network, allowing attackers to intercept traffic, capture credentials, or launch further attacks.

Packet Injection: Attackers inject malicious packets into wireless networks to manipulate network traffic, exploit vulnerabilities, or launch denial-of-service (DoS) attacks. Packet injection techniques can be used to send forged or spoofed packets, deauthenticate legitimate clients, or disrupt network operations.

Rogue Access Points: Attackers deploy rogue access points within target environments to lure unsuspecting users into connecting to them. Once connected, attackers can intercept traffic, capture credentials, or launch further attacks. Rogue access points can be set up using off-the-shelf hardware or compromised wireless routers.

Signal Jamming: Attackers use signal jamming devices to disrupt wireless communications by transmitting interference signals on the same frequency used by Wi-Fi networks. Signal jamming attacks can prevent legitimate users from connecting to wireless networks or disrupt network operations by causing interference and packet loss.

Man-in-the-Middle (MitM) Attacks: Attackers position themselves between the client device and the wireless access point to intercept and manipulate communication between the two parties. MitM attacks allow attackers to eavesdrop on traffic, capture sensitive

information, and inject malicious payloads into communication streams.

Social Engineering: Attackers may employ social engineering tactics to trick users into revealing sensitive information, such as Wi-Fi passwords or network credentials. Phishing emails, fake Wi-Fi hotspots, and pretexting are common social engineering techniques used to exploit human vulnerabilities and gain unauthorized access to wireless networks.

17. Explain wired equivalent privacy in detail

Ans:

The foundation of the contemporary digital era is wireless networks.

They have completely changed how we exchange information and communicate.

Yet, there are certain disadvantages to this innovation, particularly in terms of security. The WEP crack method is one example of a hacking technique that can be used on wireless networks.

Wireless networks are protected by the security standard known as WEP (Wired Equivalent Privacy).

It was first released in 1999 to take the place of the unsafe WEP protocol. Its purpose was to offer security protections comparable to those in wired networks.

However, it was eventually discovered that WEP had significant security holes that hackers could exploit.

A WEP-secured wireless network can be broken into using the WEP crack method.

Data packets sent over the network are intercepted and examined as part of the approach. The wireless network is secured by the WEP protocol, which employs a shared key authentication system.

Data sent over the network is encrypted using the shared key.

The WEP protocol's flaw is that it makes use of a fixed encryption key.

Hence, if a hacker gets their hands on the key, they can quickly decrypt all data packets sent across the network.

The WEP crack technique takes advantage of this flaw by intercepting a significant portion of data packets being sent over the network. The network's encryption key can then be broken by the hacker using a cracking programme.

The keys to WEP encryption can be cracked using a variety of techniques.

These tools analyse the intercepted data packets using a number of different methods in order to identify the encryption key.

Aircrack-ng is one of the most widely used tools for WEP cracking. Powerful software called Aircrack-ng can quickly decrypt WEP keys.

18. Explain WPA Authentication Mechanism.

Ans:

Wi-Fi Protected Access (WPA) is a security protocol designed to secure wireless networks by providing stronger data protection and authentication mechanisms than its predecessor, Wired Equivalent Privacy (WEP).

WPA employs several authentication mechanisms to authenticate users and devices connecting to a Wi-Fi network securely.

One of the primary authentication mechanisms used in WPA is known as WPA-PSK (Pre-Shared Key) or WPA-Personal. Here's an explanation of the WPA authentication mechanism:

Pre-Shared Key (PSK):

In WPA-PSK mode, a pre-shared key (also known as a passphrase or password) is configured on both the wireless access point (AP) and the client devices wishing to connect to the network.

The pre-shared key is a secret value that is shared between the AP and the client devices. It serves as the basis for generating encryption keys used to encrypt and decrypt data transmitted over the wireless network.

When a client device attempts to connect to the network, it sends an authentication request to the AP and includes the pre-shared key in the request.

The AP verifies the pre-shared key provided by the client device. If the key matches the one configured on the AP, the client device is granted access to the network.

Once authenticated, the client device and the AP use the pre-shared key to derive encryption keys for securing data transmissions using encryption protocols such as TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard).

Four-Way Handshake:

In WPA-PSK mode, the process of authenticating a client device involves a four-way handshake between the client device and the AP.

During the four-way handshake, the client device and the AP exchange messages to negotiate encryption keys and establish a secure connection.

The four-way handshake ensures that both the client device and the AP possess the correct pre-shared key and derive identical encryption keys for securing communications.

Key Derivation:

After successful authentication, both the client device and the AP derive encryption keys for securing data transmissions.

The encryption keys are derived from the pre-shared key and additional information exchanged during the four-way handshake.

These encryption keys are used to encrypt data transmitted between the client device and the AP, providing confidentiality and integrity protection for wireless communications.

Group Key Handshake:

In addition to the four-way handshake between individual client devices and the AP, WPA also supports a group key handshake to manage encryption keys for multicast and broadcast traffic.

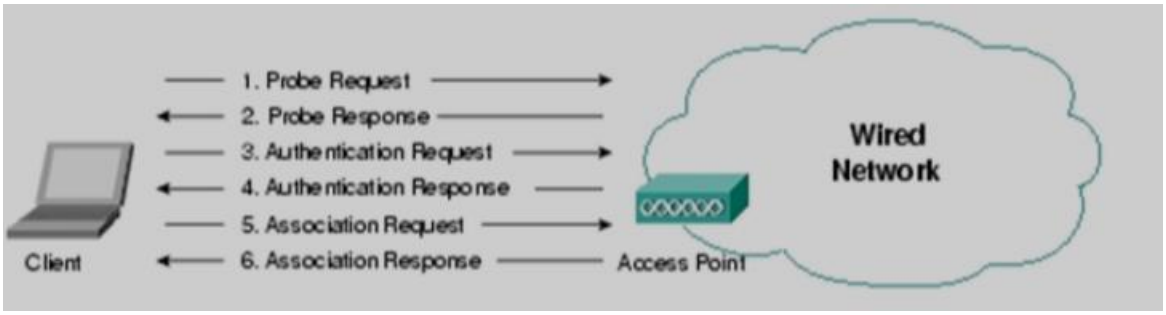
During the group key handshake, the AP periodically updates the encryption keys used for multicast and broadcast transmissions, ensuring that all connected client devices have access to the latest encryption keys.

19. Explain in detail Wireless Sniffing and its working.

Ans:

Wireless sniffing, also known as wireless packet sniffing or wireless network sniffing, is the process of capturing and analyzing wireless network traffic to monitor communications, troubleshoot network issues, and detect security threats.

Wireless sniffing allows network administrators, security professionals, and attackers to inspect data packets transmitted over wireless networks, including Wi-Fi, Bluetooth, and other wireless protocols.



Here's how wireless sniffing works:

Promiscuous Mode: To capture wireless network traffic, the wireless network interface card (NIC) of the sniffing device must be configured to operate in promiscuous mode. In this mode, the NIC is set to listen to all wireless traffic on the same channel, regardless of whether the traffic is intended for the sniffing device or not. This allows the device to capture all data packets within its range, including those not addressed to it.

Packet Capture: Once the wireless NIC is set to promiscuous mode, it begins capturing wireless data packets transmitted over the air. These packets contain information such as source and destination MAC addresses, IP addresses, TCP/UDP ports, payload data, and other metadata. The sniffing device captures the packets and stores them in a packet capture file for later analysis.

Channel Selection: Wireless networks operate on specific channels within the radio frequency spectrum. To capture traffic from a particular wireless network, the sniffing device must tune its wireless NIC to the same channel used by the target network. This ensures that the device can intercept and capture packets transmitted on that channel.

Decryption (if applicable): If the wireless network uses encryption, such as WPA2-PSK or WPA3, the sniffing device must have the necessary credentials (e.g., pre-shared key) to decrypt encrypted traffic. Without decryption, the sniffing device will only be able to capture encrypted packets, which may contain payload data that is not readable without decryption.

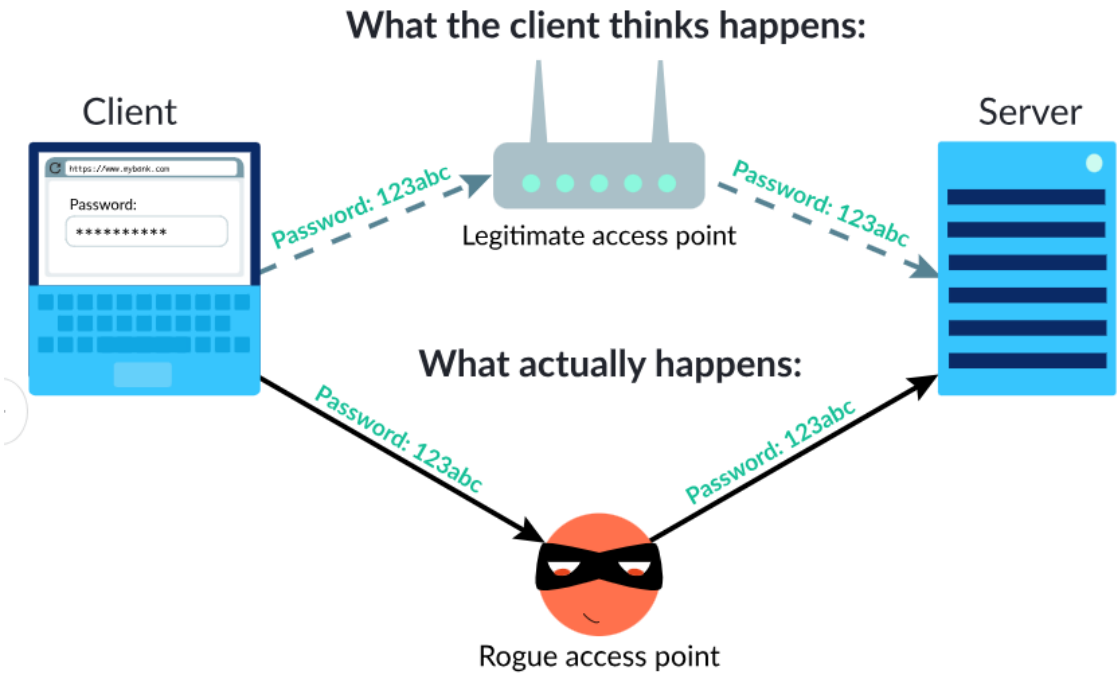
Packet Analysis: After capturing wireless packets, the sniffing device analyzes the captured data to extract useful information, identify network devices, understand communication patterns, and detect anomalies or security threats. This analysis may involve examining packet headers, inspecting payload data, correlating network events, and applying filtering or search criteria to isolate relevant packets.

Protocol Decoding: In addition to analyzing packet headers and payload data, the sniffing device may decode and interpret various network protocols used in the captured packets, such as IP, TCP, UDP, HTTP, DNS, and others. Protocol decoding allows the device to understand the purpose and context of network communications and identify specific applications or services generating the traffic.

Visualization and Reporting: Finally, the results of the packet analysis are typically presented in a user-friendly format, such as graphs, charts, tables, or reports. Visualization tools may be used to graphically represent network traffic patterns, highlight significant events, and provide insights into network performance, security posture, and potential issues. Reports generated from the analysis may include findings, recommendations, and actionable insights for network administrators, security teams, or other stakeholders.

20. Define the term Rogue Access Point and explain its working.

Ans:



A rogue access point — or rogue AP — is a wireless access point plugged into an organization's network that the security team does not know exists.

While rogue access points can be used as part of a coordinated attack, employees unaware of proper cybersecurity protocol often install them.

Most of the time, a rogue access point is a personal router that an employee connected to the network for work purposes, but they could look like anything from a wireless card jutting out of a server to a small device attached to a company firewall.

Whether installed maliciously or not, rogue access points add to the attack surface.

They do not have the same security features as the rest of the network, are not monitored by the security team, and grant easy access to the greater network.

If taken advantage of by cybercriminals, rogue access points can lead to enormous organizational damage.

One particularly effective method for preventing rogue access points is adopting an endpoint technology that can detect, report, and alert for rogue access points across your extended enterprise (IT, OT, cloud, work-from-anywhere, third-party and public wi-fi locations).

For a deeper understanding of the topic, this article explains how rogue access points and other attacker techniques can be prevented.

21. Explain penetration testing methodology.

Ans:

Penetration testing methodology is a systematic approach or framework used by security professionals to plan, execute, and analyze the results of a penetration test.

The methodology outlines the steps and procedures to be followed throughout the testing process to identify security vulnerabilities, assess risks, and recommend remediation measures effectively.

While specific methodologies may vary depending on factors such as the scope of the test, target environment, and testing objectives, most penetration testing methodologies follow a similar structure consisting of several phases:

Pre-engagement: In the pre-engagement phase, the penetration testing team establishes the scope, objectives, and rules of engagement for the test. This includes defining the target systems, applications, and networks to be tested, specifying testing methodologies and techniques, obtaining necessary permissions and approvals from stakeholders, and setting expectations for the testing process.

Reconnaissance: The reconnaissance phase involves gathering information and intelligence about the target environment to identify potential entry points, vulnerabilities, and attack vectors. This may include conducting passive reconnaissance, such as gathering publicly available information from sources like search engines, social media, and company websites, as well as active reconnaissance, such as network scanning and enumeration to discover live hosts, open ports, and services running on target systems.

Enumeration: In the enumeration phase, the penetration testing team performs active probing and enumeration of target systems to gather detailed information about their configuration, users, services, and vulnerabilities. This may include conducting port scanning, service fingerprinting, user enumeration, and other techniques to identify potential security weaknesses and attack surfaces.

Vulnerability Analysis: The vulnerability analysis phase involves identifying and assessing security vulnerabilities and weaknesses in the target environment. This includes analyzing the results of reconnaissance and enumeration activities, conducting vulnerability scans and assessments using automated tools, and manually verifying identified vulnerabilities to determine their exploitability and potential impact on the organization.

Exploitation: In the exploitation phase, the penetration testing team attempts to exploit identified vulnerabilities to gain unauthorized access, escalate privileges, and compromise target systems. This may involve using known exploits, custom scripts, or manual techniques to bypass security controls, execute arbitrary code, or access sensitive information. The goal is to demonstrate the feasibility and impact of potential attacks and assess the effectiveness of existing security controls.

Post-exploitation: The post-exploitation phase focuses on maintaining access and establishing persistence within the target environment after a successful compromise. This may include escalating privileges, pivoting to other systems or networks, exfiltrating data, and covering tracks to avoid detection. The penetration testing team may also simulate advanced persistent threats (APTs) or insider threats to assess the organization's ability to detect and respond to ongoing attacks.

Reporting: The reporting phase involves documenting the findings, analysis, and recommendations derived from the penetration test in a comprehensive report. The report typically includes an executive summary, detailed technical findings, risk assessments, remediation recommendations, and actionable insights for improving the organization's

security posture. The penetration testing team may also conduct a debriefing session with stakeholders to discuss the results and answer questions.

Follow-up and Remediation: The follow-up and remediation phase involve collaborating with the organization's IT and security teams to prioritize and address identified vulnerabilities and security weaknesses. This may include implementing security patches and updates, configuring security controls, updating policies and procedures, and providing training and awareness programs for employees. The penetration testing team may also conduct retesting or validation to verify the effectiveness of remediation efforts and ensure that security risks have been adequately mitigated.

22. Write short note on pen test deliverables.

Ans:

Penetration testing deliverables are the tangible outputs or documentation produced as a result of conducting a penetration test.

These deliverables serve to communicate the findings, analysis, and recommendations derived from the testing process to stakeholders, including management, IT teams, and clients.

Here are some common penetration testing deliverables:

Executive Summary: An executive summary provides a high-level overview of the penetration test findings, including key vulnerabilities, risk ratings, and recommendations. It is tailored for non-technical stakeholders, such as executives and decision-makers, to provide them with a concise understanding of the security posture and potential risks**.**

Detailed Report: A detailed report provides a comprehensive analysis of the penetration test results, including detailed descriptions of identified vulnerabilities, exploitation techniques, evidence of compromise, and impact assessments. It typically includes screenshots, logs, and other supporting evidence to validate findings and assist with remediation efforts.

Technical Findings: Technical findings documents provide in-depth details of each identified vulnerability, including technical descriptions, root causes, attack vectors, and recommended remediation steps. These documents are intended for IT and security teams responsible for addressing vulnerabilities and implementing security controls.

Risk Assessment: A risk assessment report evaluates the severity and potential impact of identified vulnerabilities on the organization's business operations, data assets, and reputation. It may include risk ratings, prioritized lists of vulnerabilities, and recommendations for risk mitigation and remediation.

Remediation Plan: A remediation plan outlines specific actions and timelines for addressing identified vulnerabilities and improving the overall security posture of the organization. It includes prioritized recommendations, resource allocation, and implementation guidelines to guide remediation efforts effectively.

Exploitation Proof-of-Concepts: Exploitation proof-of-concept (PoC) documents provide step-by-step instructions and demonstration videos showing how identified vulnerabilities can be exploited by attackers. These PoCs help validate the severity of vulnerabilities and assist with understanding the potential impact on the organization's systems and data.

Recommendations and Best Practices: Recommendations and best practices documents provide guidance and actionable advice for improving the organization's security posture and reducing the risk of future security incidents. This may include recommendations for security controls, policies, procedures, and employee training initiatives.

Presentation and Debrief: A presentation or debriefing session with stakeholders is often conducted to discuss the penetration test findings, answer questions, and provide additional context and insights. This interactive session allows stakeholders to gain a deeper understanding of the security risks and make informed decisions about security investments and priorities.

23. Explain automated tools used in penetration testing.

Ans:

Automated tools play a crucial role in penetration testing by automating various tasks involved in assessing the security of systems, networks, and applications. These tools help security professionals identify vulnerabilities, assess risks, and test the effectiveness of security controls efficiently.

Here are some common types of automated tools used in penetration testing:

Vulnerability Scanners: Vulnerability scanners automate the process of identifying security vulnerabilities in systems, networks, and applications by scanning for known security weaknesses, misconfigurations, and software flaws. These tools analyze target systems and generate reports listing identified vulnerabilities, along with recommendations for remediation. Examples of vulnerability scanners include Nessus, OpenVAS, and QualysGuard.

Network Scanners: Network scanners automate the discovery and enumeration of devices, hosts, and services within a network by scanning network ranges and probing for open ports, running services, and potential security risks. These tools help security professionals map the network topology, identify potential entry points, and assess the attack surface. Examples of network scanners include Nmap, Masscan, and Angry IP Scanner.

Web Application Scanners: Web application scanners automate the process of testing web applications for security vulnerabilities, such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms. These tools crawl web applications, analyze input parameters, and simulate attacks to identify vulnerabilities and security weaknesses. Examples of web application scanners include OWASP ZAP, Burp Suite, and Acunetix.

Exploitation Frameworks: Exploitation frameworks automate the process of testing and exploiting security vulnerabilities discovered during penetration testing. These tools provide a collection of pre-built exploits, payloads, and post-exploitation modules that can be used to exploit vulnerabilities and gain unauthorized access to target systems. Examples of exploitation frameworks include Metasploit Framework, Cobalt Strike, and Canvas.

Password Crackers: Password crackers automate the process of recovering passwords by attempting to guess or crack password hashes stored in files, databases, or authentication systems. These tools use various techniques, such as dictionary attacks, brute force attacks, and rainbow table attacks, to crack passwords and gain unauthorized access to user accounts. Examples of password crackers include John the Ripper, Hashcat, and Hydra.

Wireless Tools: Wireless penetration testing tools automate the process of assessing the security of wireless networks by scanning for wireless access points, capturing network traffic, and testing encryption protocols and authentication mechanisms. These tools help security professionals identify vulnerabilities and weaknesses in wireless networks and recommend security improvements. Examples of wireless penetration testing tools include

Aircrack-ng, Kismet, and Wireshark.

Forensics Tools: Forensics tools automate the process of collecting, analyzing, and preserving digital evidence during penetration testing and incident response activities. These tools help security professionals investigate security incidents, identify attack vectors, and reconstruct the timeline of events. Examples of forensics tools include Autopsy, The Sleuth Kit, and Volatility Framework.

24. Explain steps to secure wireless networks.

Ans:

Securing wireless networks is essential to protect against unauthorized access, data breaches, and other security threats. Here are steps to secure wireless networks effectively:

Change Default Settings: Start by changing default settings, including the SSID (Service Set Identifier), administrator credentials, and default Wi-Fi encryption keys. Default settings are well-known and can be easily exploited by attackers.

Use Strong Encryption: Employ strong encryption protocols, such as WPA2 (Wi-Fi Protected Access 2) or WPA3, to encrypt data transmitted over the wireless network. Avoid using older and less secure encryption methods like WEP (Wired Equivalent Privacy).

Enable Network Encryption: Ensure that all network traffic is encrypted using protocols like HTTPS (Hypertext Transfer Protocol Secure) for web browsing and SSL/TLS (Secure Sockets Layer/Transport Layer Security) for secure communication with servers and services.
Implement Network Segmentation: Divide the wireless network into separate segments or VLANs (Virtual Local Area Networks) to isolate sensitive or critical systems from less secure areas. Implement access controls and firewall rules to regulate traffic between network segments.

Use Strong Passwords: Set strong and unique passwords for Wi-Fi networks, administrator accounts, and other network devices. Use a combination of uppercase and lowercase letters, numbers, and special characters to create strong passwords that are difficult to guess or brute-force.

Enable Network Authentication: Implement network authentication mechanisms, such as WPA2-Enterprise or 802.1X, to require users and devices to authenticate before connecting to the wireless network. This adds an extra layer of security by verifying the identity of users and devices.

Disable SSID Broadcast: Disable SSID broadcasting to prevent the wireless network from being discoverable by nearby devices. While this does not provide strong security on its own, it can help reduce the visibility of the network to casual attackers.

Enable MAC Address Filtering: Use MAC address filtering to allow only authorized devices to connect to the wireless network. Create a whitelist of approved MAC addresses and configure the wireless access point to only accept connections from devices with MAC addresses on the whitelist.

Regularly Update Firmware and Software: Keep wireless access points, routers, and other network devices up to date by installing firmware updates and security patches released by the manufacturer. Outdated software may contain vulnerabilities that can be

exploited by attackers.

Monitor Network Activity: Use network monitoring tools to monitor network activity and detect suspicious behavior, such as unauthorized access attempts or unusual traffic patterns. Implement intrusion detection systems (IDS) or intrusion prevention systems (IPS) to automatically block malicious activity.

Educate Users: Educate users about wireless security best practices, such as avoiding public Wi-Fi networks, being cautious when connecting to unknown networks, and avoiding sharing sensitive information over unsecured connections.