Scoring Indicators

COURSE NAME :ETHICAL HACKING

COURSE CODE : 5133B **QID : 2109230296**

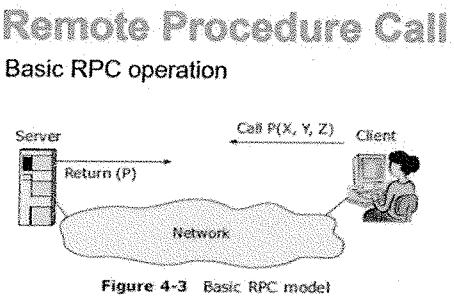
PART A

I. Answer all the following questions in one word or sentence.

(9 x 1 = 9 Marks)

Q.No.	Scoring Indicators	Split score	Max. marks Sub Total	Total score
	PART A			9
I.1	Confidentiality		1	
I.2	Denial of Service (DoS) attack		1	
I.3	DNS zone transfer		1	
I.4	Piggy backing		1	
I.5	IP spoofing		1	
I.6	ext,ext2,ext3,xfs,ext4	(Any two)0.5*2	1	
I.7	The 'sudo apt update' command is used to update package repositories, and 'sudo apt upgrade' is used to install available updates on Debian-based Linux distributions.		1	
I.8	Metasploit,MPack,Zeus	(any two)0.5*2	1	
I.9	Directory traversal		1	
	PART B			24
II.1	**script kiddies :**a term for unskilled hackers or crackers who use scripts or programs written by others to penetrate networks. White hat hackers, also known as ethical hackers or "good hackers," are individuals or cybersecurity professionals who use their technical skills and knowledge to identify and address security vulnerabilities in computer systems, networks, and software applications. Unlike malicious hackers (black hat hackers) who engage in cybercrime, white hat hackers operate within the boundaries of the law and adhere to ethical guidelines.	1.5*2	3	

II.2	A type of attack carried out by e-mail; e-mails includes links to fake Web sites intended to entice victims into disclosing private information or installing malware. The targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.		3	
II.3	The Server Message Block (SMB) protocol is a network file-sharing protocol used by Windows and other operating systems to enable the sharing of files, printers, and other resources over a network. Over the years, there have been various vulnerabilities discovered in the SMB protocol, some of which have been exploited by malware and attackers to compromise Windows systems. One of the most notable SMB vulnerabilities is the EternalBlue exploit, which was used in the WannaCry ransomware attack in 2017.		3	
II.4	PASSWORDS AND AUTHENTICATION The weakest security link in any network is authorized users. A comprehensive password policy to be adopted by companies to address this issue. A password policy should include the following: • Change passwords regularly on system-level accounts (every 60 days at minimum). • Require users to change their passwords regularly (at least quarterly). • Require a minimum password length of at least eight characters (and 15 characters for administrative accounts). • Require complex passwords; in other words, passwords must include letters, numbers, symbols,punctuation characters, and preferably both uppercase and lowercase letters. • Passwords can't be common words, words found in the dictionary (in any language), or slang, jargon, or dialect. • Passwords must not be identified with a particular user, such as birthdays, names, or company related words. • Never write a password down or store it online or in a file on the user's computer. • Don't hint at or reveal a password to anyone over the	Any 3*1	3	

	phone, in e-mail, or in person. • Use caution when logging on to make sure no one sees you entering your password. • Limit reuse of old passwords.			
II.5	REMOTE PROCEDURE CALL Remote Procedure Call (RPC) is an interprocess communication mechanism that allows a program running on one host to run code on a remote host. RPC uses client/server model. The requesting program is a client and the service providing program is the server. The client stub act as a proxy for the remote procedure. The server stub acts as a correspondent to the client stub.  Figure 4-3 Basic RPC model The Conficker worm took advantage of vulnerability in RPC to run arbitrary code on susceptible hosts. Microsoft advised users of this critical vulnerability that allowed attackers to run their own code and offered a patch to correct the problem. Microsoft Baseline Security Analyzer (MBSA) is an excellent tool for determining whether a system is vulnerable because of an RPC-related issue.		3	
II.6	NTFS (New Technology File System) and FAT32 (File Allocation Table 32) are two different file systems used in Windows operating systems. NTFS offers several advantages over FAT32, which make it a more robust and feature-rich file system. Here are the advantages of NTFS over FAT32: File and Volume Size: NTFS supports much larger file sizes and volume sizes compared to FAT32. FAT32 has a maximum file size limit of 4 GB and a maximum volume size of 2 TB, while NTFS supports much larger files and volumes.	Any 2*1.5	3	

	Security: NTFS provides better security features. It supports file and folder-level permissions, allowing you to control access to specific files and directories. This is essential for multi-user environments and networked systems. File Compression: NTFS supports built-in file compression, which can help save disk space without the need for third-party tools. This feature is not available in FAT32. File Encryption: NTFS supports file-level encryption through the Encrypting File System (EFS). This provides a higher level of data protection for sensitive files.			
II.7	Sniffing and pharming are both types of web server attacks, but they target different aspects of web communication and have distinct methods and goals **Sniffing**– Unencrypted data sent over the network may be intercepted and used to gain unauthorized access to the web server. Sniffing attacks involve capturing and monitoring network traffic, often through techniques like ARP (Address Resolution Protocol) spoofing or the use of packet capture tools like Wireshark. **Pharming**– With this type of attack, the attacker compromises the Domain Name System (DNS) servers or on the user computer so that traffic is directed to a malicious site. Pharming attacks manipulate DNS records or hosts files to redirect users to fraudulent websites. This is typically achieved through malware, DNS cache poisoning, or compromising DNS servers. Users are unknowingly directed to malicious sites that may appear legitimate.	2*1.5	3	
II.8	Effects of successful attacks • An organization's reputation can be ruined if the attacker edits the website content and includes malicious information or links to a porn website • The web server can be used to install malicious software on users who visit the compromised website. The malicious software downloaded onto the visitor's computer can be a virus, Trojan or Botnet Software, etc. • Compromised user data may be used for fraudulent activities which may lead to business loss or lawsuits from the users who entrusted their details with the organization		3	

II.9	Tools for War Driving: The tools for war driving are typically software and hardware components that allow individuals to detect and map wireless networks while on the move. Here are some common tools used in war driving: Wireless Scanning Software: There are various software applications available for scanning and mapping wireless networks. Popular options include NetStumbler, Kismet, Vistumbler, and inSSIDer. GPS Receiver: A GPS receiver is used to capture the location data of detected networks. Many laptops and mobile devices come with built-in GPS capabilities, or external GPS receivers can be connected. Wi-Fi Adapters: External Wi-Fi adapters with better reception and capabilities for packet capture are often used to improve the range and accuracy of scanning. Mapping Software: Some war drivers use mapping software to overlay the detected networks on maps, allowing for the creation of visual representations of wireless network coverage. Vehicle: A vehicle, such as a car or bicycle, is used for mobility during the war driving activity.	Any 3 *1	3	
II.10	**Access Point (AP):** An access point is a hardware device that connects a wired network to a wireless network. It acts as a bridge between wireless devices and the wired local area network (LAN). Access points broadcast wireless signals, allowing Wi-Fi-enabled devices to connect to the network. **Router:** A router is a networking device that manages the flow of data between a local network and the internet. In wireless networks, routers often include built-in access points for Wi-Fi connectivity. Routers assign IP addresses to devices on the network, manage network traffic, and provide security features like firewalls. **Wireless Network Interface Cards (NICs):** Wireless NICs are hardware components or adapters installed in computers, laptops, smartphones, and other	Any 2*1.5	3	

	devices to enable wireless connectivity. These NICs communicate with access points and other wireless devices using radio waves. **Wireless Antennas:** Antennas are used to transmit and receive radio signals in wireless networks. They come in various shapes and sizes, including omni-directional and directional antennas. The type of antenna used can affect the range and coverage of the wireless network. **Wireless Standards (e.g., Wi-Fi Standards):** Wireless standards define the specifications and protocols that devices must follow to communicate over wireless networks. Common standards include Wi-Fi 6 (802.11ax), Wi-Fi 5 (802.11ac), and earlier versions like Wi-Fi 4 (802.11n) and Wi-Fi 3 (802.11g). These standards determine the maximum data transfer rates, frequency bands, and other technical details of wireless communication. **Wireless Channels:** Wireless networks use specific channels within the radio frequency spectrum to transmit data. Channels are like separate lanes on a highway, allowing multiple devices to communicate without interference. Channels help avoid signal congestion and interference from nearby networks. **Wireless Security Protocols:** To secure wireless communication, wireless networks use encryption and authentication protocols like WPA3 (Wi-Fi Protected Access 3) and WPA2. These protocols protect data from unauthorized access. **Wireless Clients:** Wireless clients are devices that connect to the wireless network, such as laptops, smartphones, tablets, and IoT devices. These devices use wireless NICs to communicate with access points and other network resources. **Wireless Controllers (in Enterprise Networks):**			

	In larger enterprise networks, wireless controllers are used to manage multiple access points centrally. They help with configuration, monitoring, and load balancing across access points. **Network Infrastructure:** Beyond access points and routers, wireless networks rely on the existing wired network infrastructure, including switches, cables, and servers, to connect to the internet and other network resources. These components work together to create a wireless network that enables users to access the internet and share data without the need for physical network cables. The choice of components and their configuration can significantly impact the performance, security, and reliability of a wireless network.			
	PART C			42
III	Viruses and worms are both types of malicious software (malware) that can infect computer systems, but they differ in several key ways. Virus: A computer virus is a type of malware that attaches itself to legitimate program files or documents. When the infected program or document is executed, the virus code is activated and can replicate itself by attaching to other files or programs. Worm: A computer worm is a standalone, self-replicating malware program that doesn't need to attach itself to other files or programs to spread. It can independently exploit vulnerabilities to replicate and propagate across a network. **Method of Propagation:** Virus: Viruses typically spread through the execution of infected files or documents. They rely on users running or opening infected files for propagation. Viruses can also spread through shared files, removable media, and email attachments. Worm: Worms are capable of self-propagation and spreading independently, without relying on user actions. They often exploit vulnerabilities in network services, email systems, or software to infect and spread to other computers on a network or over the internet. **Attachment to Host Files:** Virus: Viruses attach themselves to host files, modifying or replacing the code of those files. When an infected file is executed, the virus code runs and may perform malicious actions.	Definition 2marks+ Any 3 comparison 5 marks	7	

	Worm: Worms do not attach themselves to host files. They exist as standalone programs and use their own code for replication and spreading. **Activation:** Virus: Viruses become active when the infected file or program is executed by a user. The virus code is then triggered, and it can perform various malicious actions, such as data corruption, file deletion, or unauthorized access. Worm: Worms are active as soon as they infect a system. They do not require user interaction to become active and can immediately start replicating and spreading to other vulnerable systems. **Payload:** Virus: Viruses may have a payload, which is the malicious action they are designed to carry out. This payload can vary and may include actions like data destruction, system crashes, or unauthorized access. Worm: Worms can also have payloads, but their primary function is to propagate and replicate. The payload in a worm may include actions like creating backdoors, installing additional malware, or launching distributed denial-of-service (DDoS) attacks. **Spread Speed:** Virus: The speed at which a virus spreads depends on user interactions (e.g., opening infected files). It may spread relatively slowly compared to worms. Worm: Worms can spread rapidly, especially if they exploit network vulnerabilities. They are designed for quick and widespread dissemination.			
IV	Cyber threats are constantly changing and new issues may have emerged day by day. Some of the major security issues are: 1. Ransomware Attacks: Ransomware continues to be a significant threat, where cybercriminals encrypt a victim's data and demand a ransom for its release. These attacks have targeted various industries, including healthcare, government agencies, and businesses, causing significant disruption and financial losses. 2. Phishing and Social Engineering: Cyber attackers frequently use phishing emails, fake websites, and social engineering techniques to deceive users into revealing sensitive information, such as passwords or financial details. 3. Insider Threats: Organizations face challenges in protecting their data from internal threats, whether it's from malicious insiders or employees who inadvertently compromise security through negligence.	Any 7*1	7	

	4. Supply Chain Attacks: Supply chain attacks are an emerging threats that target software developers and suppliers. The goal is to access source codes, build processes, or update mechanisms by infecting legitimate apps to distribute malware. 5. IoT Vulnerabilities: As the Internet of Things (IoT) expands, so do its security challenges. Many IoT devices lack proper security measures, making them vulnerable to exploitation and being used as entry points into larger networks. 6. Cloud Security: With the increased adoption of cloud services, there is a growing need to ensure data stored in the cloud is adequately protected from unauthorized access and data breaches. 7. Zero-Day Exploits: Unknown vulnerabilities in software and systems are exploited before vendors can release patches, leaving organizations exposed to attacks until fixes are available. 8. Nation-State Attacks: Attacks by expert cyber criminals, or groups funded by nations, to lead cyber attacks against other countries. These threat actors target states' critical infrastructure like media, healthcare, military, communication, financial institutions, and industrial facilities. 9. Data Breaches: High-profile data breaches regularly make headlines, exposing sensitive information and affecting the privacy of millions of individuals. 10. AI and Cybersecurity: While artificial intelligence (AI) has potential benefits in cybersecurity, it can also be leveraged by attackers to develop more sophisticated and targeted attacks			
V	**Brute Force Attack:** A brute force attack is a method used by attackers to gain access to a system by systematically trying all possible combinations of usernames and passwords until the correct credentials are found. Brute force attacks can be time-consuming and resource-intensive but can be effective if the target's login credentials are weak or easily guessable. Countermeasures against brute force attacks include	Listing 1 mark Explanation 3marks 1+2*3	7	

	account lockouts, rate limiting, and the use of strong, complex passwords. **Dictionary Attack** A dictionary attack is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document. Dictionary attacks work because many computer users and businesses insist on using ordinary words as passwords. Dictionary attacks are rarely successful against systems that employ multiple-word phrases, and unsuccessful against systems that employ random combinations of uppercase and lowercase letters mixed up with numerals. In those systems, the brute-force method of attack (in which every possible combination of characters and spaces is tried up to a certain maximum length) can sometimes be effective, although this approach can take a long time to produce results. **Counter measures** **Delayed Response**: A slightly delayed response from the server prevents a hacker or spammer from checking multiple passwords within a short period of time. **Strengthen password requirements** - Increase password complexity, limiting the number of attempts allowed within a given period of time, and by wisely choosing the password or key. **Failed Login Attempts Lockout** **Disable root login for remote connections**.			
VI	**Distributed Denial of Service (DDoS):** A DDoS attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic. In a DDoS attack, multiple compromised computers, often referred to as "botnets," are used to send an enormous amount of traffic to the target simultaneously. The goal of a DDoS attack is to make the targeted resource inaccessible to legitimate users, causing service downtime. REPLAY ATTACK A replay attack occurs when a cybercriminal eavesdrops on a secure network communication, intercepts it, and	2*3.5 marks	7	

	then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. During replay attacks the intruder sends to the victim the same message as was already used in the victim's communication. The message is correctly encrypted, so its receiver may treat is as a correct request and take actions desired by the intruder. The attacker might either have eavesdropped a message between two sides before or he may know the message format from his previous communication with one of the sides. This message may contain some kind of the secret key and be used for authentication. Counter measures • Use right method of encryption • Both sender and receiver should establish a completely random session key, which is a type of code that is only valid for one transaction and can't be used again. • Use timestamps on all messages. This prevents hackers from resending messages sent longer ago than a certain length of time. • Another method to avoid becoming a victim is to have a password for each transaction that's only used once and discarded. That ensures that even if the message is recorded and resent by an attacker, the encryption code has expired and no longer works.			
VII	Footprinting is the process of collecting as much information as possible about a target system or network to identify potential vulnerabilities, weaknesses, and entry points for cyberattacks. Foot printing tools : google dorking,whois,nslookup, trace route etc. Google dorking, also known as Google hacking or Google dork searching, is a technique used by hackers and security researchers to find sensitive information or vulnerabilities on websites using specific search queries in Google's search engine. It involves using advanced operators and search strings to refine search results and uncover information that might not be easily accessible through conventional browsing. Some common operators used in Google dorking include: site: - Limits the search to a specific website or domain. Example: site:example.com intitle: - Searches for pages with a specific word or	Introduction – 1marks +Example tool and use 6 marks		

	phrase in the title. Example: intitle:"index of" inurl: - Searches for pages with a specific word or phrase in the URL. Example: inurl:admin filetype: - Limits results to specific file types (e.g., PDF, DOC, XLS). Example: filetype:pdf intext: - Searches for pages with a specific word or phrase in the body text. Example: intext:password Whois" is a widely used internet protocol and service that provides information about domain names, IP addresses, and their registrants. The term "whois" is a combination of "who is," and the service allows users to query a database to retrieve information about the owner of a domain name, the domain's registration date, expiration date, and more. Example, *whois example.com* will show, *Domain Name: example.com* *Registrar: Example Registrar, Inc.* *Registrant Name: John Doe* *Registrant Organization: Example Company* *Registrant Email: john.doe@example.com* *Registrant Phone: +1.1234567890* *Creation Date: 2020-01-15* *Expiration Date: 2023-01-15* *Name Servers:* *ns1.example.com* *ns2.example.com* *Status: Active* **nslookup,:** "Name Server Lookup," is a command-line tool used for querying Domain Name System (DNS) servers to obtain DNS-related information about domain names and IP addresses. It is available on most operating systems, including Windows, macOS, and various Unix-like systems.			

	Here are some common uses of the nslookup command: Domain Name Resolution: You can use nslookup to translate a domain name into an IP address. For example: *nslookup example.com* will show, *Server: UnKnown* *Address: 192.168.1.1* *Non-authoritative answer:* *Name: example.com* *Addresses: 93.184.216.34*			
VIII	Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing. It allows you to scan networks, find open ports, discover services running on remote systems, and gather information about those systems. Below are some common Nmap commands with examples to help you get started: **1. Basic Host Discovery:** - Command: nmap -sn <target> - Example: nmap -sn 192.168.1.0/24 - Purpose: Discover hosts in the specified IP range without scanning open ports. **2. Scan a Single Host:** - Command: nmap <target> - Example: nmap 192.168.1.100 - Purpose: Perform a basic scan on a single host, showing open ports and services. **3. Scan Multiple Hosts:**	Example commands - 5marks Explanation 2 marks	7	

	- Command: nmap <target1> <target2> - Example: nmap 192.168.1.100 192.168.1.101 - Purpose: Scan multiple hosts in a single command. **4. Scan Specific Ports:** - Command: nmap -p <port(s)> <target> - Example: nmap -p 80,443 192.168.1.100 - Purpose: Scan specific ports on a target. **5. Operating System Detection:** - Command: nmap -O <target> - Example: nmap -O 192.168.1.100 - Purpose: Attempt to identify the operating system of the target.			
IX	DUMPSTER DIVING Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list,calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash. PIGGYBACKING Piggybacking is a method attackers use to gain access to restricted areas in a company. The attacker follows an employee closely and enters the area with that	2*3.5	7	

	allow specified traffic into or out of the network. Objectives of Port scanning ✓ Determining the system is alive? ✓ Identifying both the TCP and UDP services running on the target system. ✓ Identifying the type of operating system of the target system ✓ Identifying specific applications or versions of a particular service. Types of port scans • SYN scan—In a normal TCP session, a packet is sent to another computer with the SYN flag set. The receiving computer sends back a packet with the SYN/ACK flag set, indicating an acknowledgment. The sending computer then sends a packet with the ACK flag set. If the port the SYN packet is sent to is closed, the computer responds with an RST/ACK (reset/acknowledgment) packet. If an attacker's computer receives a SYN/ACK packet, it responds quickly with an RST/ACK packet, closing the session. This is done so that a full TCP connection is never made and logged as a transaction. In this sense, it's "stealthy." After all, attackers don't want a transaction logged showing their connection to the attacked computer and listing their IP addresses. • **XMAS scan**—In this type of scan, the FIN, PSH, and URG flags are set. Closed ports respond to this type of packet with an RST packet. This scan can be used to determine which ports are open. For example, an attacker could send this packet to port 53 on a system and see whether an RST packet is returned. If not, the DNS port might be open. • **UDP scan**—In this type of scan, a UDP packet is sent to the target computer. If the port sends back an ICMP "Port Unreachable" message, the port is closed. Again, not getting that message might imply the port is open, but this isn't always true. A firewall or packet-filtering device could undermine your assumptions.			
XI	**HARDENING WINDOWS SYSTEMS** A security tester must not only find vulnerabilities; he or she must be familiar with methods of correcting them. There are some general things you can do to make and keep a network secure.	Any 7*1marks		

	employee. Piggybacking is trailing closely behind an employee who has access to an area without the person realizing you didn't use a PIN or a security badge to enter the area. Those skilled in piggybacking watch authorized personnel enter secure areas and wait for the opportune time to join them quickly atthe security entrance. They count on human nature and the desire of others to be polite and hold open a secured door. Preventive measures ➢ Use turnstiles (a form of gate which allows one person to pass at a time) at areas where piggybacking can occur ➢ Train personnel to notify security; when they notice a stranger in a restricted area. ➢ Ensure all employees use access cards to gain entry.			
X	Port scanning, also referred to as service scanning, is the process of examining a range of IP addresses to determine what services are running on a system or network. Open ports : An open port allows access to applications and can be vulnerable to an attack. Closed ports : Ports that aren't listening or responding to a packet. Filtered ports : Ports protected with a network-filtering device, such as a firewall. Port scanning helps you answer questions about open ports and services by enabling you to scan thousands or even tens of thousands of IP addresses quickly. Many port-scanning tools produce reports of their findings, and some give you best-guess assessments of which OS is running on a system. Most scanning programs report open ports, closed ports, and filtered ports in a matter of seconds. When a Web server needs to communicate with applications or other computers, for example, port 80 is opened. A closed port doesn't allow entry or access to a service. For instance, if port 80 is closed on a Web server, users can't access Web sites. A port reported as filtered might indicate that a firewall is being used to	Introduction 2.5 marks+ 1.5*3	7	

	❖ **Patching systems** ❖ **Antivirus solutions** ❖ **Enable logging and review logs regularly** ❖ **Disable unused services and filtering ports** ❖ **Other security practices** • Use TCP/IP filtering. • Delete unused scripts and sample applications. • Delete default hidden shares and unnecessary shares. • Use a different unique naming scheme and passwords for public interfaces. • Be careful of default permissions. • Use packet-filtering technologies such as firewalls • Use open-source or commercial tools to assess system security. • Use a file-integrity checker to monitor unauthorized file system modifications • Disable the Guest account. • Rename the default Administrator account. • Make sure there are no accounts with blank passwords.			
XII	**LINUX OS VULNERABILITIES** Like any OS, linux can be made more secure if users are aware of its vulnerabilities and keep current on new releases and fixes. A typical linux distribution has thousands of packages developed by many contributors around the world. These programming flaws may lead to vulnerabilities. **Samba** To address the issue of interoperability, a group of programmers created Samba (www.samba.org) in 1992 as an open-source implementation of CIFS. With Samba, *nix servers can share resources with Windows clients, and Windows clients can access a *nix resource without realizing that the resource is on a *nix computer. **Tools for identifying Linux vulnerabilities** ▪ Visiting the CVE website for discovering possible vulnerabilities **Tools** • Open VAS – is an enumeration tool used widely. • chkrootkit ,Tripwire - can detect rootkits installed on Linux systems • SELinux – is a built-in tool available for configuring linux systems securely. • Nikto – web vulnerability scanner for linux • Metasploit – is apenetration testing tool **Countermeasures against Linux attacks** ➢ **User awareness training** ➢ **Keeping current** – do not run outdated versions ➢ **Secure configuration** – Built-in Linux tools, such as SELinux, are available for configuring systems securely. In addition, free benchmark tools are available			

	from the Center for Internet Security, and commercial tools with templates can be used totighten security configurations quickly and easily.			
XIII	A web application comprises various interconnected components that work together to deliver a dynamic and interactive user experience. Components are, Web Pages: These are the individual screens or pages of the application that users navigate through. Each page serves a specific purpose, such as displaying content, forms, or user profiles. HTML (Hypertext Markup Language): HTML defines the structure and content of web pages, using elements like headings, paragraphs, links, and lists. It forms the backbone of web content. CSS (Cascading Style Sheets): CSS styles the HTML content, controlling elements' layout, appearance, fonts, colors, and responsive design. It ensures the pplication's visual consistency and attractiveness. JavaScript: JavaScript is a programming language that enables dynamic behavior in web applications. It adds interactivity, validates user input, and communicates with the backend through APIs (Application Programming Interfaces). Server: A web server, such as Apache, Nginx, or Microsoft IIS, hosts the application and handles incoming client requests. It routes requests to the appropriate backend code. Application Logic: Backend code written in languages like Python, Ruby, PHP, Node.js, and Java processes user requests, performs calculations, implements business rules, and generates dynamic content for the UI. Databases: Databases store and manage structured data. Backend code communicates with databases to retrieve, modify, or store data. Common databases include MySQL, PostgreSQL, MongoDB, and others. APIs (Application Programming Interfaces): APIs define the rules and methods for communication between the frontend and backend. They enable data exchange and integration with third-party services and systems.	7*1	7	
XIV	**WIRELESS HACKING** The term "wireless" is generally used to describe	Introduc tion	7	

	equipment and technologies operating in the radio frequency (RF) spectrum between 3 Hz and 300 GHz. Wireless hacking, also known as Wi-Fi hacking or wireless network penetration testing, refers to the unauthorized or illegal attempt to gain access to a wireless network, such as a Wi-Fi network, without the owner's permission. This activity is generally considered illegal and unethical. Wireless hacking typically involves exploiting vulnerabilities in wireless network security protocols, routers, or connected devices to gain unauthorized access to the network **Countermeasures against wireless attack** Some methods for protecting a wireless network are disabling SSID broadcasts, renaming default SSIDs, using an authentication server, placing the AP in the DMZ , using EAP , upgrading to WPA2, assigning static IP addresses to wireless clients and using router to filter unauthorized MAC and IP addresses and prevent them from having network access. ➢ Use anti-war driving software to make it more difficult for attackers to discover your WLAN. ➢ There are measures for preventing radio waves from leaving or entering a building so that wireless technology can be used only by people in the facility. One is using a certain **type of paint** on the walls. ➢ Use a router to filter unauthorized MAC and IP addresses and prevent them from having network access. ➢ Use an authentication server such as RADIUS that can refer all users to a server. ➢ Use EAP, which allows using different protocols that enhance security. ➢ Place access point in the demilitarized zone (DMZ) and use firewall . ➢ Assign static IP addresses to wireless clients instead of using DHCP. ➢ Change the default SSID and disable SSID broadcasts.	3marks+ couterm easures 4 MARKS		