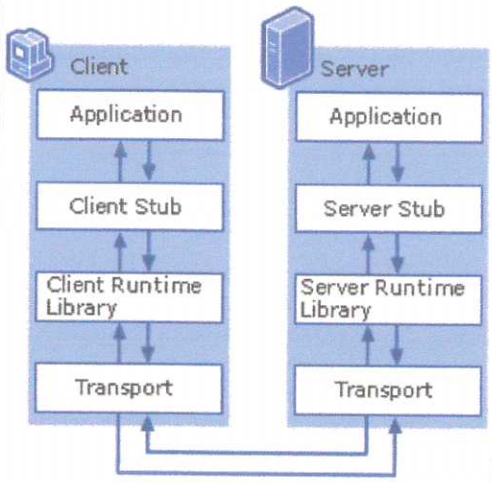
Code 3131 (15)
ETHICAL HACKING

Qno.	Key	Split Score	Total Score
I.1	Hacking which is done to find weakness in a computer and network system for testing pupose is called the ethical hacking.	2	2
I.2.	Worms,virus,Trojan,spyware,adware rootkits,bots,ransomeware any four	1/2 *4	2
I.3.	Cyberkit,Samspade,Pinger,Superscan,WUPS,Active ports any 4	1/2 *4	2
I.4.	A null session is an anonymous connection to an inter-process communication network service on Windows-based computers.The service is designed to allow named pipe conections but may be used by attackers to remotely gather information about the system.	2	2
I.5.	Database,Messaging,OSGi,Transaction Processing,User Registry,Connect out, connect in,Monitored file,HTTP Listener. Any four	1/2 *4	2
Part B			
II.1	- Make sure your PC is updated and secure - Be very sceptical of random pop-up windows,error messages and attachments. - Remove spam - Think thrice before installing any new software - Behave on line as you would in real life	6	6
II 2.	**Competitive intelligence** is the result of a company's efforts to gather and analyze information about its industry, business environment, **competitors**, and **competitive** products and services. The information-gathering and analysis process can help a company develop its strategy or identify **competitive** gaps.1 mark Competitive intelligence information can be gathered through online searches and other data-gathering methods, or by talking to people. 1 mark Information sources for online and other searches include: › Company websites for insights into target audiences or shifts in strategy, product pricing, product benefits, and so on. › Company press releases for new product, staff, or expansion news. › Social media postings, particularly if the company begins sharing information related to a product or service that hasn't yet been introduced. › Online job postings, since the types and number of open positions could indicate efforts to staff up for a new product or category development. 4 marks › Company information aggregators such as Dun & Bradstreet or	1+1+4	6

	Hoover's Online. User's groups on social networks that include LinkedIn and Facebook and elsewhere on the Internet.		
II 3.	- Piggybacking in a wireless communication context is the unauthorized accessof a wireless network - Also reffered as WI-FI squatting - Pupose is to gainfree network access and not a malicious intent - It can slow down the data transfer for the legitimate users of the network - Can also be used for data theft, dissemination of virus or some illicit activity - It is simple to access the unsecured network - It is illegal - To protect netwotk from piggybacking -ensure that encryption is enables for the router -use wireless encryption protocol -use Wireless Protected Access WPA or WPA2 - use strong password for the encryption key.	6	6
II4.	Remote procedure call (**RPC**), as it's name implies, is a mechanism that enable the programmer to call a procedure remotely be it a different machine or another process by making a local, ordinary, procedure call. **RPC** can use different protocols to achieve it. Windows Remote Procedure Call (RPC) defines a powerful technology for creating distributed client/server programs. The RPC run-time stubs and libraries manage most of the processes relating to network protocols and communication. This enables us to focus on the details of the application rather than the details of the network.  2 marks system from where the call originates is known as client and system where the method is executed is known as server(roughly speaking). This server peace is in remote place in the network hence the name RPC. Client should have idea about the method or procedure which	2+4	6

	exist in the remote system and this information needs to be sent in server, this might include method name, parameters and return type etc.. Typically stub is generated which is replica of the server side objects this helps in making call to server side function, because to client it looks like a local call, behind the scene it will be sending this data to server through network call and return the response. When client calls the local method this call needs to be translated into the format that can travel over the network this is known as marshaling, on the similar lines when client receives response form server it is in raw format when it gets converted to object this is known as unmarshaling. Usually this is taken care by RPC library.		
II 5.	*SQL Injection -backend SQL statements altered -unintended commands and gives access to unauthorized data. -The SQL command which when executed by web application can also expose the back-end database. **Implication** • An attacker can inject malicious content into the vulnerable fields. • Sensitive data like User Names, Passwords, etc. can be read from the database. • Database data can be modified (Insert/Update/ Delete). • Administration Operations can be executed on the database **Vulnerable Objects** • Input Fields • URLs interacting with the database.2 Countermeasures 1.White listing the input fields 2.Avoid displaying detailed error messages that are useful to an attacker. * Cross Site Scripting	2 + 2+ 2	6

-XSS vulnerabilities target scripts embedded in a page that are executed on the client side
-XSS is an attack which allows the attacker to execute the scripts on the victim's browser.

Implication:

- Making the use of this security vulnerability, an attacker can inject scripts into the application, can steal session cookies, deface websites, and can run malware on the victim's machines.

Vulnerable Objects

- Input Fields
- URLs

Countermeasures.
1.White Listing input fields
2.Input Output encoding

* Broken Authentication and session management
The websites usually create a session cookie and session ID for each valid session, and these cookies contain sensitive data like username, password, etc. When the session is ended either by logout or browser closed abruptly, these cookies should be invalidated i.e. for each session there should be a new cookie.
If the cookies are not invalidated, the sensitive data will exist in the system. For example, a user using a public computer (Cyber Cafe), the cookies of the vulnerable site sits on the system and exposed to an attacker. An attacker uses the same public computer after some time, the sensitive data is compromised.

Vulnerable Objects

- Session IDs exposed on URL can lead to session fixation attack.
- Session IDs same before and after logout and login.
- Session Timeouts are not implemented correctly.
- Application is assigning same session ID for each new session.
- Authenticated parts of the application are protected using SSL and passwords are stored in hashed or encrypted format.
- The session can be reused by a low privileged user.

Implication

- Making use of this vulnerability, an attacker can hijack a session, gain unauthorized access to the system which allows disclosure and modification of unauthorized information.
- The sessions can be high jacked using stolen cookies or sessions using XSS.

Countermeasures

1.All the authentication and session management requirements should be defined as per OWASP Application Security Verification Standard.
2.Never expose any credentials in URLs or Logs.
3.Strong efforts should be also made to avoid XSS flaws which can be used to steal session IDs.

*Insecure Direct Object References

It occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key as in URL or as a FORM parameter. The attacker can use this information to access other objects and can create a future attack to access the unauthorized data.

Implication

- Using this vulnerability, an attacker can gain access to unauthorized internal objects, can modify data or compromise the application.

Vulnerable Objects

- In the URL.

Countermeasures

1. Implement access control checks.

2Avoid exposing object references in URLs.

3.Verify authorization to all reference objects.

***Cross site request Forgery**

CSRF attack is an attack that occurs when a malicious website, email, or program causes a user's browser to perform an unwanted action on a trusted site for which the user is currently authenticated.
A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application.

Implication

- Using this vulnerability as an attacker can change user profile information, change status, create a new user on admin behalf, etc.

Vulnerable Objects

- User Profile page
- User account forms
- Business transaction pag

Countermeasures
1.Mandate user's presence while performing sensitive actions.
2.Implement mechanisms like CAPTCHA, Re-Authentication, and Unique

Request Tokens.

*Security misconfiguration
Security Configuration must be defined and deployed for the application, frameworks, application server, web server, database server, and platform. If these are properly configured, an attacker can have unauthorized access to sensitive data or functionality.
Sometimes such flaws result in complete system compromise. Keeping the software up to date is also good security.

Implication

- Making use of this vulnerability, the attacker can enumerate the underlying technology and application server version information, database information and gain information about the application to mount few more attacks.

Vulnerable objects

- URL
- Form Fields
- Input fields

Countermeasures

1. A strong application architecture that provides good separation and security between the components.
2. Change default usernames and passwords.
3. Disable directory listings and implement access control checks.

***Insecure Cryptographic storage**
nsecure Cryptographic storage is a common vulnerability which exists when the sensitive data is not stored securely.
The user credentials, profile information, health details, credit card information, etc. come under sensitive data information on a website.

This data will be stored on the application database. When this data are stored improperly by not using encryption or hashing*, it will be vulnerable to the attackers.

Implication

- By using this vulnerability, an attacker can steal, modify such weakly protected data to conduct identity theft, credit card fraud or other crimes.

Vulnerable objects

- Application database.

Countermeasures

1. Ensure appropriate strong standard algorithms. Do not create own cryptographic algorithms. Use only approved public algorithms such as AES, RSA public key cryptography, and SHA-256, etc.
2. Ensure offsite backups are encrypted, but the keys are managed and backed up separately.

***Failure to restrict URL access**

Web applications check URL access rights before rendering protected links and buttons. Applications need to perform similar access control checks each time these pages are accessed.

In most of the applications, the privileged pages, locations and resources are not presented to the privileged users.

By an intelligent guess, an attacker can access privilege pages. An attacker can access sensitive pages, invoke functions and view confidential information.

Implication

- Making use of this vulnerability attacker can gain access to the unauthorized URLs, without logging into the application and exploit the vulnerability. An attacker can access sensitive pages, invoke functions and view confidential information.

Vulnerable objects:

- URLs

Countermeasures

1. Implement strong access control checks.
2. Authentication and authorization policies should be role-based.
3. Restrict access to unwanted URLs.

*** insufficient transport layer protection**

Deals with information exchange between the user (client) and the server (application). Applications frequently transmit sensitive information like authentication details, credit card information, and session tokens over a network.

By using weak algorithms or using expired or invalid certificates or not using SSL can allow the communication to be exposed to untrusted users, which may compromise a web application and or steal sensitive information.

Implication

- Making use of this web security vulnerability, an attacker can sniff legitimate user's credentials and gaining access to the application.
- Can steal credit card information.

Vulnerable objects

	• Data sent over the netw Countermeasures 1. Enable secure HTTP and enforce credential transfer over HTTPS only. 2. Ensure your certificate is valid and not expired. ***Unvalidated redirects and forwards** The web application uses few methods to redirect and forward users to other pages for an intended purpose. If there is no proper validation while redirecting to other pages, attackers can make use of this and can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages. **Implication** • An attacker can send a URL to the user that contains a genuine URL appended with encoded malicious URL. A user by just seeing the genuine part of the attacker sent URL can browse it and may become a victim. **Recommendations** 1. Simply avoid using redirects and forwards in the application. If used, do not involve using user parameters in calculating the destination. 2. If the destination parameters can't be avoided, ensure that the supplied value is valid, and authorized for the user. Any 3		
II 6.	n Wireless network interface cards (WNICs), which transmit and receive wireless signals, and access points (APs), which are the bridge between wired and wireless networks n Wireless networking protocols, such as Wi-Fi Protected Access (WPA) n A portion of the RF spectrum, which replaces wire as the connection medium 3marks explanation of each 3marks	3 + 3	6
II 7.	Web Service - is available over the Internet or private networks - uses a standardized XML messaging system - is not tied to any one operating system or programming language - is selg describing via a common XML grammar - is discoverable via asimple find mechanism	6	6

	Components of Web services basic web service platform – XML + HTTP components SOAP- Simple Object Access Protocol UDDI- Universal Description, Discovery and Integration WSDL- Web Services Description Languages Working Web service enables communication among various applicatiions by open standards such as HTML,XML,WSDL and SOAP. XML used to Tag the data SOAP to transfer a messgae WSDL to describe the availability of service.		
Part C			
III	Denial-of-Service Attacks Distributed Denial of services attack Buffer over flow attack Ping of death attack Session hijacking Explain the above 3 marks each	3*5	15
IV	*Virus - is a malicious code that attaches to and become part of another program -are destructive - attaches to the executable files - execute in tandum with host file - spreads through networks, disks,fike sharing or email attachments *Worm - amalicious code that can spread from one computer to another without requiring host file -designed to exploit vulnerabilities,and spread by taking advantages of networks and internet connections *Trojan - malicious code that masquerades as a legitimate benign application. - opens connection to command and control server and owns the machine. -do not replicate by infecting other files, nor do they self replicate - spreads through user interaction such as opening an email attachment downloading running a file from the internet *Bots - also known as robots are snippets of code designed to automate tasks and respond to instruction - can self-replicate or replicate via user action - installed in a system without user's knowledge botnet – entire network of compromized device botnet launch DdoS *Ramsomare	3*5	15

	- is a type of malware that takes a computer or its data hostage in an effort to exortmoney from victims -Lockscreen Ramsomware – displays a full screen image or a webpage that prevents the user from accessing his computer. - Encryption ramsomware - encrypts files thus demy access to thefiles *Rootkits - is a set of software tools that hides it presence in the lower layers of operating system's application layer, the operating system kernel or inthe BIOS with priviged access permissions. - intension is generally remote C and C -cannot self propagate or replicate -must be installed on a device -very difficult to detect and even more difficult to remove *Spyware - is a general term used todescribe software that without a user's consent and knowledge tracks Interner activitysuch as searches and web surfing collects data on personal habits and display advertisement. - sometimes affects the device configuration by changing the default browser,changing the browser home page, or installing "add-on" components. *Adware - is similar to spyware in that both are gathering informartion obout the user and their habits. - more marketing focused and may pop up advertisements or redirecrt a user's web browser to certain web sites in the hopes of making a sale. -adware will appempt to target the advertisement to fit the context of What THE user is doing. Any 5		
V	**Port Scanning** -is one of the most important step in gathering the information**about the** victim or gathering loop holes of one's own system for security sake. -states of the ports scanned are = port is open =port is closed = port is filtered or prevented. 3 marks Types of port scans *TCP Scanning *SYN Scanning *UDP Scanning *ACK Scanning *Window Scanning *FIN Scanning Explain the above 2marks each(6*2)	3+6*2=15	15
VI	**--DNS ZONE TRANSFER** **-is a type of DNS transaction** **-is one of the many mechanism available for administrators to replicate DNS databases across a set of DNS servers** **DNS uses name serversused to resolve names. After you determine what name server a company is using, you can attempt to transfer all the records for which the DNS server is responsible.**	3+5	15

This process, called a zone transfer.
-a zone transfer uses theTCP for transport,and takes the form of client-sever transaction. The portion of the database that is replicated is a zone
To determine a company's primary DNS server, you can look for a DNS server containing a Start of Authority (SOA) record. An SOA record shows for which zones or IP addresses the DNS server is responsible. After you determine the primary DNS server, you can perform another
zone transfer to see all host computers on the company network. In other words, the zone transfer give you an organization's network diagram. You can use this informa-tion to attack other servers or computers that are part of the network infrastructure.
Shoulder Surfing
A methodof social engineers used to gain access to information is shoulder surfing. A shoulder surfer is skilled at reading what users enter on their keyboards, especially logon names and passwords. This skill certainly takes practice, but with enough time, it can be mastered easily. Shoulder surfers also use this skill to read PINs entered at ATMs or to detect long-distance authorization codes that callers dial. ATM theft is much easier than computer shoulder surfing because a keypad has fewer characters to memorize than a computer keyboard. If the person throws away the receipt in a trash can near the ATM, the shoulder surfer can match the PIN with an account number and then create a fake ATM card. Often shoulder surfers use binoculars or high-powered telescopes to observe PINs being entered, making it difficult to protect against this attack.
Many keyboard users don't follow the traditional fingering technique taught in typing classes. Instead, they hunt and peck with two or three fingers. However, shoulder surfers train themselves to memorize key positions on a standard keyboard. Armed withthis knowledge, they can determine which keys are pressed by noticing the location
on the keyboard, not which finger the typist is using.
Shoulder surfers also know the popular letter substitutions most people use when creating passwords: $ for s, @ for a, 1 for i, 0 for o, and so forth. Many users think p@$$w0rd is difficult to guess, but it's not for a skilled shoulder surfer. In addition, many users are required to use passwords containing special characters, and often they type these passwords more slowly to make sure they enter the correct characters.
Slower typing makes a shoulder surfer's job easier.
To help prevent shoulder-surfing attacks, you must educate users not to type logonnames and passwords when someone is standing directly behind them—or even standing nearby. You should also caution users about typing passwords when someone nearby is talking on a cell phone because of the wide availability of camera phones. To further reduce the risk of shoulder surfing, make sure all computer monitors face away from the door or the cubicle entryway. Warn your users to change their passwords immediately if they suspect someone might have observed them entering their passwords.
*Dumpster Diving
Another method social engineers use to gain access to information is

	dumpster diving. Although it's certainly not a glamorous form of gathering information, you'd be surprised at what you can find by examining someone's trash. For example, discarded computer manuals can indicate what OS is being used. If the discarded manual is for **Windows NT 4.0, there's a good chance the new system is a more recent Windows OS,such as Windows Server 2003. Sometimes network administrators write notes in manuals or even jot down passwords, and social engineers can make use of this information. Company phone directories are another source of information. A dumpster diver who finds a directory listing company employees can use this information to pose as an employee for the purpose of gathering information. Company calendars with meeting schedules, employee vacation schedules, and so on can be used to gain access to offices that won't be occupied for a specified time period. Trash can be worth its** **weight in gold for the dumpster diver who knows what to do with it. Here are some other items that can be useful to dumpster divers:** ***Financial reports** *** Interoffice memos** **n Discarded computer programs** *** Company organizational charts showing managers' names** *** Resumes of employees** *** Company policies or systems and procedures manuals** *** Professional journals or magazines** *** Utility bills** *** Solicitation notices from outside vendors** *** Regional manager reports** *** Quality assurance reports** *** Risk management reports** *** Minutes of meetings** *** Federal, state, or city reports** **Dumpster diving can produce a tremendous amount of information, so educating your users on the importance of proper trash disposal is important. Disks or hard drives containing company information should be formatted with "disk-cleaning" software that writes binary 0s on all portions of the disks. This formatting should be done at least seven times to ensure that all previous data is unreadable. Old computer manuals should be discarded offsite so that dumpster divers can't associate the manuals with the company. Before disposal, all these items should be placed in a locked room with adequate physical, administrative, and technical safeguards. All documents should be shredded, even if the information seems innocuous. Social engineers know how to pull together information from many different sources. Putting a puzzle together from many small pieces makes it possible for attackers to break into a network.**		
VII	**Network security assessment tool** **Wireshark**	3*5=15	15

	Nmap **Metasploit** **OpenVas** **Aircrack** **Web Security assessment tools** **Nikto** **Samural frame work** **Safe3 scanner** **Websecurity** **SQLmap** **Explain any five # marks each**		
VIII	**Vulnerabilities** General lack of patch management for the OS Outdated third party application Lack of password enforcement General lack of system hardening lackof backups 6marks **Tools** Wireshark Nmap Metasploit OpenVas Aircrack explain any three 3*3 = 9	6+9	15
IX	Application Vulnerabilities - Software system flaws or weaknesses in an application that could be exploited to compromise the security of the application. Buffer Overflow - Buffer Overflows occur when there is more data in a buffer than it can handle, causing data to overflow into adjacent storage. Credentials Management- A credentials management attack attempts to breach username/password pairs and take control of user accounts. **CRLF Injection** - CRLF Injection attacks refer to the special character elements "Carriage Return" and "Line Feed." Exploits occur when an attacker is able to inject a CRLF sequence into an HTTP stream. **Cross-Site Request Forgery** - Cross-Site Request Forgery (CSRF) is a malicious attack that tricks the user's web browser to perform undesired actions so that they appear as if an authorized user is performing those actions. **Cross-Site Scripting** - XSS vulnerabilities target scripts embedded in a page that are executed on the client-side (in the user's web browser) rather than on the server-side. **Directory Traversal** - Directory traversal is a type of HTTP exploit that is used by attackers to gain unauthorized access to restricted directories and files.	15	15

	Encapsulation- Encapsulation refers to a programming approach that revolves around data and functions contained, or encapsulated, within a set of operating instructions. Error Handling - Error Handling vulnerabilities occur when a system reveals detailed error messages or codes generated from stack traces, database dumps, and a wide variety of other problems, including out of memory, null pointer exceptions, and network timeout errors. **Failure to Restrict URL Access** - One of the common vulnerabilities listed on the Open Web Application Security Project's (OWASP) Top 10. The OWASP Top 10 details the most critical vulnerabilities in web applications. **Format String** - Format String attacks occur when an application interprets data as a command and allows an attacker to access the underlying code base. **Insecure Cryptographic Storage** - Insecure Cryptographic Storage is a common vulnerability that occurs when sensitive data is not stored securely from internal users. **Insufficient Transport Layer Protection** - Insufficient transport layer protection is a security weakness caused by applications not taking any measures to protect network traffic. **LDAP Injection** - LDAP injection is the technique of exploiting web applications that use client-supplied data in LDAP statements without first stripping potentially harmful characters from the request. **Malicious Code** - Analysis tools are designed to uncover any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. **OS Command Injection** - Command injection refers to a class of critical application vulnerabilities involving dynamically generated content. Attackers execute arbitrary commands on a host operating system using a vulnerable application. Race Condition- A race condition attack happens when a computing system that's designed to handle tasks in a specific sequence is forced to perform two or more operations simultaneously. **SQL Injection** - SQL injection is a type of web application security vulnerability in which an attacker is able to submit a database SQL command, which is executed by a web application, exposing the back-end database.		
X	**Reaver** Reaver implements a brute force attack against Wifi Protected Setup	3*5=15	15

(WPS) registrar PINs in order to recover WPA/WPA2 passphrases.

Reaver has been designed to be a robust and practical attack against WPS, and has been tested against a wide variety of access points and WPS implementations.

On average Reaver will recover the target AP's plain text WPA/WPA2 passphrase in 4-10 hours, depending on the AP. In practice, it will generally take half this time to guess the correct WPS pin and recover the passphrase

it requires the Kali linux

Aircrack-ng

Aircrack-ng is a complete suite of tools to assess WiFi network security.

It focuses on different areas of WiFi security:

- Monitoring: Packet capture and export of data to text files for further processing by third party tools
- Attacking: Replay attacks, deauthentication, fake access points and others via packet injection
- Testing: Checking WiFi cards and driver capabilities (capture and injection)
- Cracking: WEP and WPA PSK (WPA 1 and 2)

Cain and Abel
is a password recovery tool for Microsoft Windows. It can recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks. Cryptanalysis attacks are done via rainbow tables which can be generated with the winrtgen.exe program provided with Cain and Abel.
Cain & Abel uses dictionary lists as a basis for cracking passwords, brute-force attacks by trying different passwords many times every second and decoding information stored on the hard drives, the package attempts to determine the correct password. The software also removes the hidden passwords by showing passwords in certain software packages. Learns wireless network keys for forgotten Wi-Fi login information. The software has some security benefits too by indicating where passwords are insecure in an active system.
Cain & Abel Key Features:

• Locate Wi-Fi password information
• Discover likely passwords for Windows operating system
• Dictionary-based words, brute-force password checking and other methods are used
• Reveal hidden password fields
• Sniff out data stored on drives to discover where passwords may be located
• Can be used for security to verify what can be easily discovered on your

own system

NetCut
Netcut defender is a free tool offered by arcai.com to keep your network's (including WI-FI) internet speed super fast. protect your PC from ARP spoofing attack. typically arp spoofing from netCut

Wireshark
Wireshark is the world's leading network traffic analyzer, and an essential tool for any security professional or systems administrator. This free software lets you analyze network traffic in real time, and is often the best tool for troubleshooting issues on your network.

Common problems that Wireshark can help troubleshoot include dropped packets, latency issues, and malicious activity on your network. It lets you put your network traffic under a microscope, and provides tools to filter and drill down into that traffic, zooming in on the root cause of the problem. Administrators use it to identify faulty network appliances that are dropping packets, latency issues caused by machines routing traffic halfway around the world, and data exfiltration or even hacking attempts against your organization.

Wireshark intercepts traffic and converts that binary traffic into human-readable format. This makes it easy to identify what traffic is crossing your network, how much of it, how frequently, how much latency there is between certain hops, and so forth.

While Wireshark supports more than two thousand network protocols, many of them esoteric, uncommon, or old, the modern security professional will find analyzing IP packets to be of most immediate usefulness. The majority of the packets on your network are likely to be TCP, UDP, and ICMP.

Given the large volume of traffic that crosses a typical business network, Wireshark's tools to help you filter that traffic are what make it especially useful. Capture filters will collect only the types of traffic you're interested in, and display filters will help you zoom in on the traffic you want to inspect. The network protocol analyzer provides search tools, including regular expressions and colored highlighting, to make it easy to find what you're looking for.

explain each carry 3 marks

page number error