K.S.R. COLLEGE OF ENGINEERING(Autonomous)

Vision of the Institution

- We envision to achieve status as an excellent educational institution in the global knowledge hub, making self-learners, experts, ethical and responsible engineers, technologists, scientists, managers, administrators and entrepreneurs who will significantly contribute to research and environment friendly sustainable growth of the nation and the world.

Mission of the Institution

- To inculcate in the students self-learning abilities that enable them to become competitive and considerate engineers, technologists, scientists, managers, administrators and entrepreneurs by diligently imparting the best of education, nurturing environmental and social needs.
- To foster and maintain a mutually beneficial partnership with global industries and Institutions through knowledge sharing, collaborative research and innovation.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Vision of the Department

- To create ever green professionals for software industry, academicians for knowledge cultivation and researchers for contemporary society modernization.

Mission of the Department

- To produce proficient design, code and system engineers for software development.
- To keep updated contemporary technology and fore coming challenges for welfare of the society.

Programme Educational Objectives (PEOs)

PEO1 : Figure out, formulate, analyze typical problems and develop effective solutions by imparting the idea and principles of science, mathematics, engineering fundamentals and computing.

PEO2 : Competent professionally and successful in their chosen career through life-long learning.

PEO3 : Excel individually or as member of a team in carrying out projects and exhibit social needs and follow professional ethics.

K.S.R. COLLEGE OF ENGINEERING(Autonomous)

Department of Computer Science and Engineering

Subject Name: Ethical Hacking(Elective)

Subject Code: 16CS762 **Year/Semester: IV/VII**

Course Outcomes: On completion of this course, the student will be able to

CO1 Understand the concepts of legal and illegal activities on Internet.

CO2 Acquire knowledge on foot printing tools and port scanning concepts.

CO3 Learn about tools to identify vulnerabilities on Microsoft systems and services.

CO4 Understand the concepts of hacking web server and learn about tools to protect web oriented services

CO5 Ability to impart the knowledge of cryptography algorithms to provide security from attacks.

Program Outcomes (POs) and Program Specific Outcomes (PSOs)

A. Program Outcomes (POs)

Engineering Graduates will be able to :

PO1 **Engineering knowledge:** Ability to exhibit the knowledge of mathematics, science, engineering fundamentals and programming skills to solve problems in computer science.

PO2 **Problem analysis:** Talent to identify, formulate, analyze and solve complex engineering problems with the knowledge of computer science. .

PO3 **Design/development of solutions:** Capability to design, implement, and evaluate a computer based system, process, component or program to meet desired needs.

PO4 **Conduct investigations of complex problems:** Potential to conduct investigation of complex problems by methods that include appropriate experiments, analysis and synthesis of information in order to reach valid conclusions.

PO5 **Modern tool Usage:** Ability to create, select, and apply appropriate techniques, resources and modern engineering tools to solve complex engineering problems.

PO6 **The engineer and society:** Skill to acquire the broad education necessary to understand the impact of engineering solutions on a global economic, environmental, social, political, ethical, health and safety.

PO7 **Environmental and sustainability:** Ability to understand the impact of the professional engineering solutions in societal and Environmental contexts and demonstrate the knowledge of, and need for sustainable development.

PO8 **Ethics:** Apply ethical principles and commit to professional ethics and responsibility and norms of the engineering practices.

PO9 **Individual and team work:** Ability to function individually as well as on multi-disciplinary teams.

PO10 **Communication:** Ability to communicate effectively in both verbal and written mode to excel in the career.

PO11 **Project management and finance:** Ability to integrate the knowledge of engineering and management principles to work as a member and leader in a team on diverse projects.

PO12 **Life-long learning:** Ability to recognize the need of technological change by independent and life-long learning.

B. Program Specific Outcomes (PSOs)

PSO1 Develop and Implement computer solutions that accomplish goals to the industry, government or research by exploring new technologies.

PSO2 Grow intellectually and professionally in the chosen field.

K.S.R COLLEGE OF ENGINEERING (AUTONOMOUS), TIRUCHENGODE – 637 215

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

18CS312 – COMPUTER ORGANIZATION AND ARCHITECTURE

UNIT I (FUNDAMENTALS OF ETHICAL HACKING)(CO 1)

PART-A (2 MARKS)

1.What are the advantages and disadvantages of hacking?(Understanding)

Advantages	Disadvantages
It can be used to foil security attacks	It creates massive security issues
To plug the bugs and loopholes	Get unauthorized system access
It helps to prevent data theft	Stealing private information
Hacking prevents malicious attacks	Violating privacy regulations

2. What is Ethical Hacking? (Remembering)

Ethical Hacking is when a person is allowed to hacks the system with the permission of the product owner to find weakness in a system and later fix them.

3. What is the difference between IP address and Mac address? (Understanding)

IP address: To every device IP address is assigned, so that device can be located on the network. In other words IP address is like your postal address, where anyone who knows your postal address can send you a letter.

MAC (Machine Access Control) address: A MAC address is a unique serial number assigned to every network interface on every device. Mac address is like your physical mail box, only your postal carrier (network router) can identify it and you can change it by getting a new mailbox (network card) at any time and slapping your name (IP address) on it.

4. List out some of the common tools used by Ethical hackers?(Remebering)

- Meta Sploit
- Wire Shark
- NMAP
- John The Ripper
- Maltego

5. What are the types of ethical hackers?(Remembering)

The types of ethical hackers are

- Grey Box hackers or Cyberwarrior
- Black Box penetration Testers
- White Box penetration Testers
- Certified Ethical hacker

6. What is Brute Force Hack? (Remembering)

Brute force hack is a technique for hacking password and get access to system and network resources, it takes much time, it needs a hacker to learn about JavaScripts. For this purpose, one can use tool name "Hydra".

7. What is DOS (Denial of service) attack? What are the common forms of DOS attack? (Understanding)

Denial of Service, is a malicious attack on network that is done by flooding the network with useless traffic. Although, DOS does not cause any theft of information or security breach, it can cost the website owner a great deal of money and time.

- Buffer Overflow Attacks
- SYN Attack
- Teardrop Attack
- Smurf Attack
- Viruses

8. What can an ethical hacker do? (Understanding)

An ethical hacker is a computer system and networking master who systematically endeavours to infiltrate a PC framework or network for the benefit of its owners to find security vulnerabilities that a malicious hacker could potentially exploit.

9. What is network sniffing? (Remembering)

System sniffing includes utilizing sniffer tools that empower real- time monitoring and analysis of data streaming over PC systems. Sniffers can be utilized for various purposes, regardless of whether it's to steal data or manage systems.

Network sniffing is utilized for ethical and unethical purposes. System administrators utilize these as system monitoring and analysis tool to analyse and avoid network related issues, for example, traffic bottlenecks. Cyber criminals utilize these devices for untrustworthy purposes, for example, character usurpation, email, delicate information hijacking etc.

10.What Is Tcp/ip? (Remembering)

TCP/IP is a name given to the collection (or suite) of networking protocols that have been used to construct the global Internet. The protocols are also referred to as the DoD (dee-oh-dee) or Arpanet protocol suite because their early development was funded by the Advanced Research Projects Agency (ARPA) of the US Department of Defense (DoD).

11. What Is Tcp/ip Model? (Understanding)

TCP/IP model is an implementation of OSI reference model. It has five layers.

They are: Network layer, Internet layer, Transport layer and Application layer.

12.Explain range of TCP/IP classes

CLASS A = 1 to 126
CLASS B = 128 to 191
CLASS C = 192 to 223
CLASS D = 224 to 239 (Multicasting)
CLASS E = 240 to 255 (Research)

12. What are Pvt. IP address ? (Understanding)

Pvt. IP are IPs which are not used in Internet or which are not routable in Internet. They are also called as non-routable IP's. Class A = 10.0.0.0 to 10.255.255.255

Class B = 172.16.0.0 to 172.31.255.255
Class C = 192.168.0.0. to 192.168.255.255

13. What is function of Router ?(Understanding)
Router is a device or PC which is used to connect two or more IP networks.

14. What is Default Gateway ? (Remembering)
Default gateway is the address of router.

15. What is Subnet Mask ?(Analyzing)
Answer : Subnet mask is used to differentiate Network ID and Host ID from a given IP address. The default subnet mask are as under
Class A = 255.0.0.0
Class B = 255.255.0.0
Class C = 255.255.255.0

16. What is Loopback address ?(Remembering)
Answer : The loopback address is 127.0.0.1. This address is used to check local TCP/IP suite or local machine.

17. What protocol is used by PING ? (Understanding)
Answer : Ping uses ICMP(Internet Control Management Protocol)

18. What is used of Tracert ?(Understanding)
Answer : Tracert is a to find path information between source and desitnation. It show no. of hops between source and desitination. Tracert also uses ICMP protocol.

19. Difference between NetBEUI and TCP/IP(Understanding)

TCP/IP	NetBEUI
a. Industry standard	Microsoft propertiery
b. IP address	NO addressing
c. Supports routing	Non routable
d. Large network	Small network
e. More confiugration	No configuration

20. What is MAC Flooding? (Remembering)

MAC Flooding is a kind of a technique wherever the protection of given network switch is compromised. In MAC flooding the hacker floods the switch with sizable amounts of frames, than what a switch can handle. This makes switch behaving as a hub and transmits all packets to all the ports existing. Taking the advantage of this the attacker can attempt to send his packet within the network to steal the sensitive information.

PART B

1.Briefly explain the legal and illegal actions on NET.(Understanding)

2.Illustrate IP Addressing and number systems.(Remembering)

3.Narrate Malware and protecting against Malware attacks.(Analyzing)

UNIT II (FOOT PRINTING AND PORT SCANNING)(CO 2)

PART A (2 Marks)

1. What do you understand by footprinting in ethical hacking?(Understanding)

Footprinting is nothing but accumulating and revealing as much as data about the target network before gaining access into any network.

2. **What are the techniques utilized for foot printing? (Remembering)**

Open Source Footprinting

Network Enumeration

Scanning

Stack Fingerprinting

3.What is Open Source Footprinting? (Remembering)

It will search for the contact data of administrators that will be utilized for guessing password in Social Engineering

4.Define Network Enumeration (Remembering)

The hacker attempts to distinguish the domain names and the network blocks of the target network

5.What is Scanning ? (Remembering)

After the network is known, the second step is to spy the active IP addresses on the network. For distinguishing active IP addresses (ICMP) Internet Control Message Protocol is a functioning IP addresses

6.Define Stack Fingerprinting (Remembering)

The final stage of foot printing step can be performed, once the hosts and port have been mapped by examining the network, this is called Stack fingerprinting.

7.What is a tool for performing footprinting undetected?(Analyzing)

Whois search

8.Which of the following tools are used for footprinting? (Understanding)

Whois

Sam Spade

Nslookup

9. What is the next step to be performed after footprinting?(Analyzing)

Scanning

10. What is footprinting? (Remembering)

Footprinting is gathering information about a target organization.

11. Nslookup can be used to gather information regarding what?(understanding)

Host names and IP addresses
Nslookup queries a DNS server for DNS records such as host names and IP addresses.

12. Give a type of social engineering?(understanding)

Shoulder surfing

13.Give an example of social engineering?(Creating)

Calling a help desk and convincing them to reset a password for a user account

14. What is the best way to prevent a social-engineering attack?(understanding)

Employee training and education

15.What are the three types of scanning? (Remembering)

Port, network, and vulnerability

16.What is the goal of port scanning? (Remembering)

The main goal of port scanning is to find out which ports are open, which are closed, and which are filtered.

17.Define nmap. (Remembering)

nmap stands for network map. nmap is actually more than just a port scanner. In addition to listing the open ports on a network, it also tries to construct an inventory of all the services running in a network. It also tries to detect as to which operating system is running on each machine,

18.Give the top five most popular portscanners tools used in the infosec field.(understanding)

Nmap. Nmap stands for "Network Mapper", it is the most popular network discovery and **port scanner**in the history. ...
Unicornscan. Unicornscan is the second most popular free **port scanner** after Nmap. ...
Angry IP **Scan**. ...
Netcat. ...
Zenmap.

PART B

1.Briefly explain the webtools used for food printing(Understanding)

2.Illustrate about Social Engineering(Remembering)

3.Demonstrate port scanning(Analyzing)

4.Write Short notes on Scanning tools.(Remembering).

UNIT III (VULNERABILITIES IN OPERATING SYSTEM)(CO3)

PART(2 MARKS)

1.Define vulnerability in OS. **(Remembering)**

A OS vulnerability is a glitch, flaw, or weakness present in an OS (Operating System).

2.Give some tools to identify vulnerabilities in Microsoft systems.(Understanding)

Attack Surface Analyzer
BinScope Binary Analyzer
Microsoft Baseline Security Analyzer
Microsoft Safety Scanner
Microsoft Security Compliance Manager
Threat Modeling Tool
Windows Defender Offline

3. What is the use of BinScope Binary Analyzer?(Analyzing)
The BinScope Binary Analyzer tool can be helpful for both developers and IT professionals that are auditing the security of applications that they are developing or deploying / managing. Auditing the software deployed in an environment and determining if it is making use of security mitigations can help risk managers make more meaningful assessments.

4.What is EMET? (Remembering)
Enhanced Mitigation Experience Toolkit

5.What do you mean by Microsoft Baseline Security Analyzer? (Remembering)
Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool designed for IT professionals and helps small and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. It is a standalone security and vulnerability scanner designed to provide a streamlined method for identifying common security misconfigurations and missing security updates.

6.What is Microsoft Safety Scanner? (Remembering)
The Microsoft Safety Scanner is a free stand-alone virus scanner that is used to remove malware or potentially unwanted software from a system. The tool is easy to use and packaged with the latest signatures, updated multiple times daily. The application is not designed to replace your existing antimalware software, but rather act as an on demand virus removal tool in situations where you suspect your real time antimalware software might not be working correctly.

7.What are the three types of linux vulnerabllities?(Understanding)
the vulnerabilities are divided into three types according to the consequences caused by exploiting these vulnerabilities.
A. Privilege Escalation
B. Denial of Service vulnerability(DoS)
C. IP Spoofing Vulnerability

8.What is DOS vulnerability? (Remembering)
DoS is the act of exploiting network protocol implemen -tation flaws deliberately or exhausting the attacked object's resources through brutal means directly,and the aim is to make the target computer or network can not provide normal services or access to resources, the target system to stop responding and even system services collapse

9.Define IP Spoofing Vulnerability(Remembering)

IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address,aims to conceal the identity of the sender or impersonating another computing system, which exploiting a fact that there is no any check for the source IP address of IP packets and a forged source IP address from attacker can't be observed. IP address spoofing commonly as a auxiliary method of other attack, which makes the defense relying on disable specific IP lose efficacy.

10.List top linux vulnerabilities in Linux(Understanding)

Top Vulnerabilities

BIND Domain Name System.

Remote Procedure Calls (RPC)

Apache Web Server.

General UNIX Authentication -- Accounts with No Passwords or Weak Passwords.

Clear Text Services.

Sendmail.

Simple Network Management Protocol (SNMP)

Secure Shell (SSH

11. What is the difference between VA and PT?(Undserstanding)

Vulnerability Assessment	**Penetration testing**
Vulnerability Assessment is an approach used to find flaws in an application/network	It is the practice of finding exploitable vulnerabilities like a real attacker will do
It is like travelling on the surface	It is digging for gold.

PART B

1.Briefly explain the tools to identify vulnerabilities on Microsoft systems(Understanding)

2.Briefly explain the vulnerabilities in Microsoft services(Understanding)

3. Explain the vulnerabilities in Linux OS.(Remembering)

UNIT IV(HACKING WEB SERVICES AND WIRELESS NETWORKS)(CO 4)
PART A(2 MARKS)

1. Explain how you can stop your website getting hacked?(Understanding)

By adapting following methodology you'll be able to stop your web site from obtaining hacked

- Using Firewall : Firewall may be accustomed drop traffic from suspicious information processing address if attack may be an easy DOS
- Encrypting the Cookies : Cookie or Session poisoning may be prevented by encrypting the content of the cookies, associating cookies with the consumer information processing address and temporal arrangement out the cookies once it slow

- Validating and confirmative user input : This approach is prepared to stop the type tempering by confirmative and verifying the user input before processing it
- Header Sanitizing and validation : This technique is beneficial against cross website scripting or XSS, this method includes verifying and sanitizing headers, parameters passed via the address, type parameters and hidden values to cut back XSS attacks.

2. What is ARP Spoofing or ARP poisoning? (Remembering)

ARP (Address Resolution Protocol) is a form of attack in which an attacker changes MAC (Media Access Control) address and attacks an internet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets.

3. How you can avoid or prevent ARP poisoning?(Analyzing)

ARP poisoning can be prevented by following methods

- Packet Filtering : Packet filters are capable for filtering out and blocking packets with conflicting source address information
- Avoid trust relationship : Organization should develop protocol that rely on trust relationship as little as possible
- Use ARP spoofing detection software : There are programs that inspects and certifies data before it is transmitted and blocks data that is spoofed
- Use cryptographic network protocols : By using secure communications protocols like TLS, SSH, HTTP secure prevents ARP spoofing attack by encrypting data prior to transmission and authenticating data when it is received

4.**Define Web Application (Remembering)**

Web application provides an interface between the web server and the client to communicate. Web pages are generated at the server, and browsers present them at the client side. The data is passed between client and server in the form of HTML pages through HTTP protocol.

There are client-side vulnerabilities and server-side vulnerabilities which lead to a web application attack.

5.**Give Web application Attacks(Understanding)**

Parameter Tampering:

This involves modifying parameters exchanged between client and server, which may lead to XSS attack and SQL injection attack. Usually, HTML data goes as a name-value pair; if the attacker is able to modify the values of the parameter during transfer, it may lead to many other attacks.

Unvalidated inputs:

Web applications accept user inputs, queries are constructed based on dynamic user input. If these inputs are not properly sanitised they will open a way for the attacker to launch attacks like XSS, SQL injection attack, Directory traversal attack, etc., identity theft, data theft are dangerous outcomes of this attack.

Directory traversal Attack:

This is a type of vulnerability where an attacker is able to access beyond the web root directory, into the restricted directories on the web server. Then an attacker will be able to access system files, run OS commands, access configuration information, etc.

6. What are Web Services Attacks? (Remembering)

The vulnerabilities in the web service protocols like SOAP, WSDL, UDDI can be exploited to do various kinds of attacks like SQL injection, XML poisoning, etc.

File Uploads:

DNS Hijacking/Poisoning:

7.Define Web service attacks. (Remembering)

This attack happens wherein a user is able to upload all types of file extensions even though the upload is intended only for few extensions. This is due to improper validation against the type of files getting uploaded, an attacker will be able to upload malicious files.

8.What is DNS Hijacking/Poisoning?(Understanding)

If an attacker is able to get access to the DNS files, he can modify the contents of the DNS records so that he can redirect the victim to a malicious web page, though they are requesting for a legitimate web page. DNS Server does the domain to IP resolving; so when a DNS poisoning is executed to modify the IP corresponding to a domain to some other IP, the attacker can trick the victim into browsing the pages he intended them to instead of the original ones.

Poisoning can be done at cache/DNS server, or an attack can modify the IP on the fly by intercepting the traffic too.

9.List some Vulnerability scanners. (Remembering)

Scanners like Nikto, Nessus, URLscan, Acunetix can be used to find out vulnerabilities in a web application.

10.What is SQL injection and its types? (Remembering)

If the application doesn't sanitize the user input then the SQL injection happens. Thus a malicious hacker would inject SQL question to gain unauthorized access and execute administration operations on the database. SQL injections may be classified as follows:

Error-based SQL injection

Blind SQL injection

Time-based SQL injection

11.What are the advantages and disadvantages of WirelessNetworks?(Understanding)

Connectivity beyond walls, wireless connection, easy to access internet even in areas where laying cables is difficult, speed and sharing. But, wireless networks have a few disadvantages, the major issue being the security.

12.Give the standards of wireless networks. (Remembering)

WIRELESS STANDARDS			
Standard	**Data Rate**	**Frequency**	**Range**
802.11a	54 Mbps	5 GHz	50 feet
802.11b	11 Mbps	2.4 GHz	150 feet
802.11g	54 Mbps	2.4 GHz	50 feet
802.11n	300 Mbps	2.4 GHz and 5 GHz	175 feet

13.List out the Authentication types. (Understanding)

Open Authentication

Shared Key Authentication Process

Centralised Authentication:

14.What is open Authentication? (Remembering)

When a client wants to connect to an open access point he/she sends a probe request, and the AP sends a probe response; the client then sends an authentication request. Upon receiving a response, the client establishes an association with the AP.

15.Define Shared Key Authentication Process(Remembering)

Here, the client sends a probe request, and the access point sends the probe response; then, the client requests for an authentication request, the AP sends an authentication challenge to the client. The client needs to send the shared key as authentication challenge response. AP, then, verifies the client and authenticates him/her, who then establishes a connection with the access point.

16.What is Centralised Authentication? (Understanding)

In the corporate environment, instead of an Access point verifying client's authentication details, a centralised server does the job of verifying the client. RADIUS is a centralised authentication server which verifies clients who want to connect with the access point.

PART B

1.Briefly explain the web application vulnerabilities.(Understanding)

2.Briefly explain the tools of web attackers and security testers(Understanding)

3. Explain about Wireless hacking.(Remembering)

UNIT V(CRYPTOGRAPHY AND NETWORK PROTECTION)(CO5)
PART A(2 MARKS)

1.Define cryptography (Remembering)

Cryptography is the art of converting text into another form for secret transmission and reception. It works by converting plain text into cipher text using some encryption algorithm at the sender's side and converting ciphertext into plain text at the receiver's. Cryptography is used to provide confidentiality, integrity, authenticity and non-repudiation.

2. What is the difference between Asymmetric and Symmetric encryption? (Analyzing)

Asymmetric encryption	Symmetric encryption
Asymmetric encryption uses different keys for encryption and decryption.	Symmetric encryption uses the same key for both encryption and decryption.
Asymmetric on the other hand is more secure but slow. Hence, a hybrid approach should be preferred.	Symmetric is usually much faster but the key needs to be transferred over an unencrypted channel.

3. What is data leakage? How will you detect and prevent it?(Analyzing)

Data leak is nothing but data knowledge getting out of the organization in an unauthorized manner. Data will get leaked through numerous ways in which – emails, prints, laptops obtaining lost, unauthorized transfer of data to public portals, removable drives, pictures etc. There are varied controls which may be placed to make sure that the info doesn't get leaked, many controls will be limiting upload on web websites, following an internal encryption answer, limiting the emails to the interior network, restriction on printing confidential data etc.

4.What is the importance of Public Key Infrastructure? (Understanding)

PKI is a set of roles, policies and procedures needed to create, manage, distribute, use, store, and revoke digital certificates, and manage public-key encryption. Here the binding of the public key to respective identities, like people or organisation is done. In public environment, where third-party verifications are required, this PKI is used.

5.What are three parties involved in PKI?(Remembering)

There are three parties involved here-

- Registration authority
- Validation Authority
- Certification authority

6. What is a firewall? (Remembering)

A firewall could be a device that allows/blocks traffic as per outlined set of rules. These are placed on the boundary of trusted and untrusted networks.

It is a wall of separation between the insecure internet and secure internal network. Firewall monitors incoming and outgoing connections, for various rules and patterns, and filters the connections passing through them.

7.List out Types of firewall (Remembering)

Packet Filtering Firewall

Circuit level Firewall

Application Firewall

Stateful Firewall

Evading Firewall

8.What is Packet Filtering Firewall? (Understanding)

This type of firewall monitors the TCP packet header at TCP level and looks for the source address, destination address, source port, destination port and the protocol used. Depending on these details they either allow or disallow the packets according to the rules written.

Any Any Any 80 Allow – This rule tells the firewall to allow any packet coming from any source going to any source to the port 80 to be allowed.

9.Give the importance of Circuit level Firewall.(Analyzing)

They operate at the session layer and filter at the connections. Even before the packets are transmitted they look for trusted connections and filter based on those trusted connections.

10.What do you mean by Application Firewall? (Understanding)

Otherwise called as Proxy firewall; they act at the application layer, filtering the application level packets. At the proxy, different rules can be given to filter the data. The web servers which are usually accessed by the internet users are placed outside the internal network as proxy servers and all connections can be directed to the proxy; thus, protecting the internal network from outside connections.

11.Give the importance of Stateful Firewall(Understanding)

This is the combination of all three firewalls. It operates at the Network Layer, filtering transport level packets, session level connections and application data as well. This has a state table which maintains the status of various connections and a rules table. It also keeps track of sequence numbers to protect against related attacks.

12.What is Evading Firewall? (Understanding)

Using Fragmented Packets.

Using Firewalking to scan beyond the firewall for open ports.

Using Source routing, avoiding the route of Firewall.

HTTP-tunnelling and ICMP-tunnelling.

13.Define Intrusion Detection System (Remembering)

IDS' are the security systems which monitor the traffic and alert or notify the administrator on traffic of concern. They do not prevent the attack but they just alert the administrator.

14.List the types Types of IDS(Understanding)

Network-Based IDS

Host-based IDS

15.What is the importance of Honey bot? (Understanding)

It’s a trap to research and understand the attacker’s behaviour on the network. Either the honey bot can be designed as high interaction one, allowing the attacker to completely compromise all services; thus, studying the pattern and attack methods, or designing a low interaction one, where only limited services are opened for attackers to compromise. The basic need is to study the attack pattern and update the signature database for new signatures and patterns.

PART B

1.Briefly explain the Symmetric and asymmetric algorithms.(Understanding)

2.Briefly explain Firewalls and IDS.(Understanding)

3. Explain about Protecting networks with security devices.(Remembering)