Scheme of Valuation
(Scoring Indicators)

Revision: 2015 **Code: TED (15) 5135**

Course: ETHICAL HACKING

Q.No	Scoring Indicator	Split up score	Total score
I	**PART A**		
1	It refers to the act of locating weaknesses and vulnerabilities of computer systems or in computer networks by duplicating the intent and actions of malicious hackers.	2	2
2	Footprinting means to gather maximum amount of information about a computer system or a network and about the devices that are attached to the network.	2	2
3	Interprocess communication mechanism. Allows a program running on one host to run code on a remote host	2 x 1	2
4	WEPCrack, AirSnort, NetStumbler	2 x 1	2
5	An access point (AP) is a radio transceiver that connects to a network. It bridges the wireless network with a wired network	2 x 1	2
II	**PART B**		
1	• This type of attack takes advantage of a program that is waiting on a user's input. • In a buffer overflow attack, a programmer finds a vulnerability in poorly written code that does not check for a defined amount of memory space use. • The attacker writes code that overflows the buffer, which is possible because the buffer capacity may not be correctly defined in the program. • The trick is to not fill the overflow buffer with meaningless data, but fill it with executable program code. • That way, the OS runs the code, and the attacker's program does something harmful. • Usually the code elevates the attacker's permission to an administrator's level or gives the attacker the same privileges as the program's owner or creator.	6 x 1	6

2	1) Spyware Sends information from the infected computer to the attacker Confidential financial data Passwords PINs Any other stored data Can register each keystroke entered (keylogger) Prevalent technology Educate users about spyware 2) Adware Similar to spyware, Can be installed without the user being aware Sometimes displays a banner Main goals Determine user's online purchasing habits Tailored advertisement Main problem: Slows down computers	2 x 3	6
3	1. Cyberkit : graphical tool which let do whois, single ping and ping sweep, traceroute, portscanning. It is best used for single ping, whois and traceroute while it is not as fast as other tools for ping sweep and portscanning. 2. Samspade : graphical tool similar to Cyberkit which does whois, traceroute, finger and dnslookup. The key features of Samspade are: Advanced DNS, zone transfer, scan addresses, crawl website, search IP block etc. 3. WUPS (Windows UDP portscanner): allows to check UDP ports, hosts with active ports. WUPS can only do one host at a time, but can also select what ports to look for. 4. Pinger : it is a very fast ping sweeper. Once the IP block of the target organization is obtained, pinger can be used to see what hosts are active. 5. SuperScan : it allows to scan a range of IP addresses and do TCP port scanning. It is a very fast and powerful tool which can check all the ports or the one selected. 6. ActivePorts : tool that enables to monitor all open TCP and UDP ports on the local computer. *Any 3*	Listing – 3 Explanation - 3	6
4	Packet crafting is the art of creating a packet according to various requirements to carry out attacks and to exploit vulnerabilities in a network. It's mainly used to penetrate into a network's structure. Steps Involved in Packet Crafting • Packet Assembly: This is the first step involved in packet crafting. In this process, the attacker selects the network to be cracked,	Definition – 2 Steps - 4	6

	collects the possible vulnerability information and creates the packet. • Packet Editing: In this step, the packets are tested before sending. The packets are edited in such a way that maximum information could be retrieved by injecting a minimum number of packets. • Packet Playing: When the packets are ready, packet playing sends them to the targeted machine and collects the resultant packets for further analysis • Packet Analysis: The sent packets are received by the attacker and they are analyzed to extract the information. Various sniffing tools like Wireshark, tcpdump, dsniff, etc. are used for this purpose.		
5	Null sessions Anonymous connection established without credentials Used to display information about users, groups, shares, and password policies Necessary only if networks need to support older Windows versions To enumerate NetBIOS vulnerabilities use:Nbtstat, Net view, Netstat, Ping, Pathping, and Telnet commands Server Message Block(SMB) Used to share files Usually runs on top of:NetBIOS, NetBEUI, orTCP/IP Several hacking tools target SMB. L0phtcrack's SMB Packet Capture utility and SMBRelay. Microsoft took seven years to patch the vulnerability these hacking tools exploited. SMB2 - Introduced in Windows Vista. Several new features. Faster and more efficient	2 x 3	6
6	Comprehensive password policy is critical Should include: 1) Change passwords regularly 2) Require at least six characters Require complex passwords Passwords can't be common words, dictionary words, slang, jargon, or dialect 3) Passwords must not be identified with a user Never write it down or store it online or in a file Do not reveal it to anyone 4) Use caution when logging on and limit reuse 5) Configure domain controllers Enforce password age, length, and complexity 6) Password policy aspects that can be enforced: Account lockout threshold Set number of failed attempts before account is disabled temporarily Account lockout duration Set period of time account is locked out after failed logon attempts	6 x 1	6

7	1. Hackers use wardriving to find insecure access points using a laptop or palmtop computer. 2. Wardriving is not illegal. 3. But using the resources of these networks is illegal. 4. An attacker or security tester simply drives around with the following equipment - Laptop computer, Wireless NIC, An antenna and Software that scans the area for SSIDs. 5. Not all wireless NICs are compatible with scanning programs. 6. Antenna prices vary depending on the quality and the range they can cover.	6 x 1	6
	PART C		
III a	1) Virus Virus attaches itself to an executable file Can replicate itself through an executable program Needs a host program to replicate No foolproof method of preventing them Eg : Gumblar, Luckyploit, Zlob, Gpcode Macro virus: Virus encoded as a macro, Lists of commands, Can be used in destructive ways. Virus creation kits available for download 2) Worms Replicates and propagates without a host, often through email Can infect every computer in the world in a short time Examples : Code Red, Nimda, conflicker, slammer 3) Trojan Programs Insidious attack against networks. Disguise themselves as useful programs Hide malicious content in program i. Backdoors ii. Rootkits Allow attackers remote access	3 x 3	9
III b	1.Educating Users 2.Avoiding fear tactics 3.Make sure PC is updated and secure 4.Be very sceptical of random pop-up windows, error messages and attachments 5.Remove spam 6.Think well before installing any new software 7.Behave online as you would in real life *Any 6*	Listing -3 Explanation -3	6
IV a	1) Session hijacking enables an attacker to join a TCP session and make both parties think he or she is the other party. This attack occurs when a session token is sent from the web server to a client browser following the successful authentication of a client log on. A session hijacking attack works when it compromises the token by	4 x 2	8

	either confiscating or guessing what an authenticated session will be, thus acquiring unauthorized access to the web server. This can result in session sniffing, man-in-the-middle attack, Trojans etc. The http cookies that are used to sustain a web session can be bootlegged by an attacker. Session hijacking of web sites can be avoided by including encryption methods, using long, random numbers for the session keys, change cookie value requests and implement session regeneration after logins. 2) Replay Attack An attack on a security protocol using replay of messages from a different context into the intended or original or honest context, thereby fooling the honest participants into thinking that they have successfully completed the protocol run. During replay attacks, the intruder may send to the victim the same message which he had already been used in his communication previously. The message is correctly encrypted, so the receiver may treat it as a correct request and take actions desired by the intruder. The attacker must 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 secret key and be used for providing authentication. Replay attacks can be avoided by some methods. Before communication sides may negotiate, create a random session key, valid only for a specified time and process. It is also reasonable to use timestamps in all messages and accept messages that have not been sent too long ago. In banking operations, the popular technique is to use one-time passwords for each request.		
IV b	Denial of service (DoS) A DoS attack prevents legitimate users from accessing services or information. Attacker overloads a server with more requests than the server can process. Target of DoS attack can be networks or the network of sites the computer is trying to use. Online banking, email and commercial websites are often targeted. The purpose of DoS is to disrupt an organization's network operations by denying access to its users. Also, the attacker can take control of the target computer or terminal and use it to infect thousands of other computers, referred to as zombies. Zombies are computers that are infected and taken over by the attacker. Distributed Denial of Service (DDoS) A distributed denial of service attack is launched against a host from multiple servers or workstations. In a DDoS attack, a network could be flooded with literally billions of packets; typically, each participant in the attack sends only a few of the total number of packets. The participants are often not aware that their computers are taking part	DoS – 3 DDoS - 4	7

	in the attack. The flood of incoming messages, connection requests or malformed packets to the target system causes it to slow down or even crash and shut down, thereby denying service to legitimate users or systems. In a DDoS attack, the assailant begins by exploiting a vulnerability in one computer system and makes it a DDoS master. The attack master system identifies other vulnerable systems and gains control over them by either infecting the systems with malware or through bypassing the authentication controls. There are three types of DDoS attacks. Network-centric or volumetric attacks, Protocol attacks and Application layer attacks.		
V a	<u>Social Engineering</u> It is the art of manipulating users confidential information that can be used to gain unauthorized access to a computer system. Means using knowledge of human nature to get information from people. Targets the human component of a network It is the biggest security threat to network <u>Shoulder Surfing :</u> A shoulder surfer is skilled at reading what users enter on their keyboards, especially logon names and passwords. They also use this skill to read PINs entered at ATMs or to detect long distance authorization codes that callers dial. To help prevent this attack • Educate users not to type logon names and passwords when someone is standing directly behind them or standing nearby. • Caution users about typing passwords when someone nearby is talking on a cell phone. • Make sure all computer monitors face away from the door or cubicle entryway. <u>Dumpster Diving:</u> Dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering technique 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 <u>Piggy Backing:</u> Piggybacking, in a wireless communication context, is the unauthorized access of a wireless LAN. Piggybacking is sometimes referred to as "Wi-Fi squatting The usual purpose of piggybacking is simply to gain free access rather than any malicious intent, but it can slow down data transfer to legitimate users of network.	Definition – 2 Any 2 types – 3 x 2 (6)	8

	A network that is vulnerable is piggybacking for network access is equally vulnerable when the purpose is data theft dissemination of viruses, or some other illicit activity Phishing A phishing attack is a computer-based social engineering, where an attacker crafts an email that appears legitimate. Such emails have the same look and feel as those received from the original site, but they might contain links to fake websites. If the user is not smart enough, then he will type user ID and password and will try to login which will result in failure and by that time, the attacker will have his ID and password to attack his original account.		
V b	Port Scanning Tools Number of tools are available for both hackers and security testers o Commercial o Freeware o Open Source Nmap Originally written for Phrack magazine One of the most popular tools Add new features constantly OS detection Fast multiple –probe ping scanning GUI versions Front end called Zenmap and Ubuntu's NmapFE Open source tool; if bugs are found, users can offer suggestions for correcting them. Standard tool for security professionals Unicornscan Developed in 2004 for Linux & UNIX only Ideal for large networks Scans 65,535 ports in three to seven seconds Optimizes UDP scanning Alco can use TCP, ICMP, or IP OpenVAS The Open Vulnerability Assessment System (OpenVAS) is a vulnerability scanner maintained and distributed by Greenbone Networks. It is intended to be an all-in-one vulnerability scanner with a variety of built-in tests and a Web interface designed to make setting up and running vulnerability scans fast and easy while providing a high level of user configurability. The OpenVAS vulnerability scanner is a free appliance designed to allow users to quickly and easily perform targeted scans of their computer systems. It is free, updated daily, and easy to use, making it an ideal choice for the independent penetration tester or small business sysadmin who needs an inexpensive and intuitive option for identifying potential security holes.	Listing – 3 Explanation - 4	7

VI a	Port Scanning The process of examining a range of IP addresses to determine what services are running on a network. Finds open ports on a computer and the services running on it. SYN Port Scan Client SYN → Server Client ← SYN/ACK Server Client RST → Server Three states – 1) Closed - RST response from server 2) Open - SYN,ACK response from server. Client then sends RST 3) Filtered - No response from server Connect scan Similar to SYN scan Completes the three-way handshake Not stealthy--appears in log files Can be detected easily Three states – 1) Closed - RST response from server 2) Open - SYN,ACK response from server. Client sends ACK. Client sends RST 3) Filtered - No response from server NULL scan The packet is sent without any flag set All the packet flags are turned off creating a lack of TCP flags that should never occur in the real world Two results: 1) Closed ports responds to a NULL scan with RST packet 2) Open or filtered ports give no response XMAS scan FIN, PSH and URG flags are set Works like a NULL scan – a closed port responds with an RST packet Determine which ports are open ACK scan Used to get information about a firewall or other filtering devices To determine whether the host is protected by some kind of filtering system The attacker sends an ACK packet with a random sequence number where no response means that the port is filtered If an RST response comes back, this means the port is closed. i.e, no filtering device. Stateful firewalls track connection and block unsolicited ACK packets Stateless firewalls just block incoming SYN packets, so you get a RST response FIN scan Only FIN flag is set Closed port responds with an RST packet When a three-way handshake ends, both parties send a FIN packet to end the connection UDP scan A UDP packet is sent to the target computer. Closed port responds with ICMP "Port Unreachable" message If the message is not getting, the port is open Rarely used	Listing – 3 Explanation - 5	8

VI b	1)Domain Name System (DNS) is the network component responsible for resolving hostnames to IP address and vice versa. 2)DNS uses name servers to resolve names. After determining what nameserver a company is using, an attempt can be made to transfer all the records the DNS server is responsible. This process is called a zone transfer and can be done with the Dig command. 3)DNS zone transfer, also sometimes known by the including DNS query type AXFR, is a type of DNS transaction. 4)It is one of the many mechanisms available for administrators to replicate DNS databases across a set of DNS servers. 5)A zone transfer uses the Transmission control Protocol (TCP) for transport and takes the form of a client-server transaction. The client requesting a zone transfer may be a slave server or secondary server requesting data from a master server, sometimes called a primary server. The portion of the database that is replicated is a zone. 6)Zone transfer comprises a preamble followed by the actual data transfer. A company's primary DNS server is the one containing a Start of Authority (SOA) record. An SOA record shows for which zones or IP addresses the DNS server is responsible. 7)After determining a company's primary DNS server, performing another zone transfer help to see all host computers on the company network, ie the zone transfer give an organization's network diagram.	7 x 1	7
VII a	<u>Best Practices for Hardening Windows Systems</u> 1) Patching Systems Options for small networks Accessing Windows Update manually Configure Automatic Updates Options for large networks Systems Management Server (SMS) Windows Software Update Service (WSUS) Third-party patch management solutions 2) Antivirus Solutions Small networks Desktop antivirus tool with automatic updates Large networks Require corporate-level solution 3) Enable Logging and Review Logs Regularly 4) Important step for monitoring critical areas a. Performance b. Traffic patterns c. Possible security breaches Logging is configured carefully 5) Disable Unused Services and Filtering Ports Disable unneeded services Delete unnecessary applications or scripts Unused applications are invitations for attacks Reducing the attack surface Open only what needs to be open, and close everything else	Listing -4 Explanation - 4	8

	6) Other Security Best Practices a. Rename (or disable) default Administrator account b. Make sure there are no accounts with blank passwords c. Use Windows group policies d. Develop a comprehensive security awareness program e. Keep up with emerging threats f. Be careful of default permissions g. Use appropriate packet-filtering techniques h. Use available tools to assess system security i. Disable Guest account		
VII b	**NetBios** 1) Software loaded into memory 2) It enables computer program to interact with network resource or device 3) NetBIOS isn't a protocol 4) Interface to a network protocol 5) NetBios Extended User Interface (NetBEUI) Fast, efficient network protocol Allows NetBIOS packets to be transmitted over TCP/IP NetBIOS over TCP/IP is called NBT . 6) Systems running newer Windows OSs Vista, Server 2008, Windows 7, and later versions Share files and resources without using NetBIOS 7) NetBIOS is still used for backward compatibility Companies use old machines	7 x 1	7
VIII a	File system stores and manages information-User created, OS files needed to boot Windows File Systems 1) File Allocation Table(FAT) Original Microsoft file system Supported by nearly all desktop and server OS's Standard file system for most removable media Other than CDs and DVDs Later versions provide for larger file and disk sizes (FAT 12, FAT16, FAT32) In FAT32 single file can only up to 4GB and disk vol. upto 8TB Doesn't support file-level access control lists (ACLs) which is necessary for setting permissions on files Using FAT in a Multiuser environment use results in vulnerability 2) NTFS(New Technology File System) First released as high-end file system Added support for larger files, disk volumes, and ACL file security Subsequent Windows versions Included upgrades for compression, journaling, file-level encryption, and self-healing Alternate data streams (ADSs) Can "stream" (hide) information behind existing files Without affecting function, size, or other information Intruders can use this feature for hacking	2 x 4	8

VIII b	Most critical tasks: 1) User awareness training Inform users a. No information should be given to outsiders i. Knowing OS makes attacks easier b. Be suspicious of people asking questions i. Verify who they are talking to ii. Call them back 2) Keeping current As soon as a vulnerability is discovered and posted, OS vendors notify customers about upgrades and patches Installing fixes promptly is essential Linux distributions most have warning methods 3) Configuring systems to improve security Many methods to help prevent intrusion Vulnerability scanners Built-in Linux tools Free benchmark tools - Center for Internet Security Security Blanket - To tighten system security by using Templates - Trusted Computer Solutions	Listing - 3 Explanation - 4	7
IX a	Web applications are the most important ways for an organization to publish information. Static Web pages – same information at any time. Created using HTML Dynamic Web pages – vary the information depends onvariables. <u>Web Server</u> The primary function of a web server is to deliver web pages on the request to clients using the Hypertext Transfer Protocol (HTTP). The two main Web servers are Apache (Open source) IIS (Microsoft) <u>Web forms</u> Use the <form> element or tag in an HTML document Allows customer to submit information to the Web server Web servers process information from a Web form by using a Web application <u>Common Gateway Interface (CGI) scripts</u> It handles moving data from a Web server to a Web browser Majority of dynamic Web pages are created with CGI and scripting languages It describes how a Web server passes data to a Web browser CGI programs can be written in different programming and scripting languages C or C++, Perl, Unix shell scripting, Visual Basic, FORTRAN <u>Active Server Pages (ASP)</u> It is a technology that enables developers to create dynamic, interactive web pages using scripting language. They are not static It uses languages such as JScript or VBScript	Listing – 4 Explanation - 4	8

	Using Scripting Languages PHP ColdFusion JavaScript Connecting to Databases Web pages can display information stored on databases There are several technologies used to connect databases with Web applications Technology depends on the OS used ODBC(Open Database connector) OLE DB - Object Linking and Embedding Database ADO - ActiveX Data Objects		
IX b	1. Anti-wardriving software makes it more difficult for attackers to discover your wireless LAN Honeypots, Black Alchemy Fake AP 2. Use special paint to stop radio from escaping your building 3. Allow only predetermined MAC addresses and IP addresses to have access to the wireless LAN 4. Use an authentication server instead of relying on a wireless device to authenticate users 5. Use an EAP(Entensible authentication protocol) 6. If you use WEP, use 104-bit encryption rather than 40-bit encryption 7. Assign static IP addresses to wireless clients instead of using DHCP 8. Don't broadcast the SSID 9. Place the AP in the demilitarized zone (DMZ). *Any 7*	Listing – 3 Explanation - 4	7

X a	Any network needs some components to work - communication devices to transmit and receive signals, protocols and a medium 1) Wireless network interface cards (WNIC) To transmit and receive wireless signals 2) Access points(AP) Bridge between wired and wireless N/W 3) A portion of the RF spectrum, replaces wire 4) Wireless networking Protocols such as WEP, WPA An access point (AP) is a radio transceiver that connects to a network. It bridges the wireless network with a wired network. The RF channels are configured in the AP. An AP enables users to connect to a LAN using wireless technology. Service Set IDentifier is used to identify a WLAN. An SSID is configured on the AP. The computers to access the WLAN, they must be configured with same SSID name within the AP. SSID is transmitted with each packet. Identifies which network the packet belongs. The AP usually broadcasts the SSID. A wireless router includes an access point, a router, and a switch. For wireless technology to work, each node or computer must have a wireless NIC. NIC's main function is to convert the radio waves it receives into digital signals the computer understands.	Listing – 4 Explanation - 4	8
X b	1) Cgiscan.c: CGI(Common Gateway Interface) scanning tool Written in C in 1999 by Bronc Buster search web sites for CGI scripts that can be exploited One of the best tools for systems with CGI vulnerabilities 2) Wapiti : Web application vulnerability scanner/ security auditor. It operates on a black box basis. Scans the web pages of the deployed app, looking for scripts and apps where it can inject data Once it gets this list, it acts like a fuzzer, injecting payloads to see if a script is vulnerable. 3) Wfetch: GUI tool from Microsoft It enables security testers to query a web server's status. Displays information that is not normally shown in a browser, such as HTTP headers Features are:1)Multiple HTTP methods 2) Configuration of host name & TCP port3)HTTP 1.0 and HTTP 1.1 support 4) Multiple connection types5)Proxy support6) Client-certificate support etc.	Listing – 3 Explanation - 4	7