185 D April-24 Page No-8

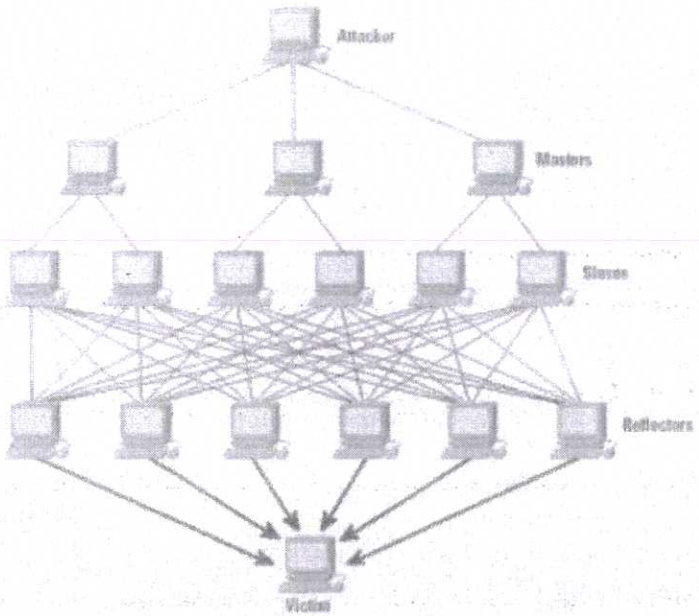
Scoring Indicators

COURSE NAME: ETHICAL HACKING

COURSE CODE:5133B **QID:** 2109230299- B

Q. No.		Scoring Indicators	Split Score	Sub Total	Total Score
		PART A			9
I	1	Keylogger is a program to records everything you type on your PC such as log-in names, passwords, and other sensitive information, and send it on to the source.	1	1	
I	2	A virus is a contagious program or code that attaches itself to another piece of software, and then reproduces itself when that software is run.	1	1	
I	3	Any two Spyware Adware	½ + ½	1	
I	4	A type of attack carried out by e-mail is called phishing.	1	1	
I	5	Port scanning is the process of examining a range of IP addresses to determine what services are running on a system or network.	1	1	
I	6	Windows file system is used to store and manage information.	1	1	
I	7	Any two Open VAS chkrootkit ,Tripwire	1	1	
I	8	Web server stored valuable information and are accessible to the public domain.	1	1	
I	9	An attacker can embed malicious code and run a program on the database server or send malicious code in an HTTP request		1	
		PART B			24
II	1	**Spyware** Software installed on users' computers without their knowledge that records personal information from the source computer and sends it to a destination computer. **Adware** Adware, however, sometimes displays a banner that notifies users of its presence. Adware's main purpose is to determine a user's purchasing habits so that Web browsers can display Advertisements.	1.5 1.5	3	
II	2	-Educate users: conducting structured training of all employees and management. -Update antivirus software periodically -Use spyware /adware removal programs -Install firewalls to protect a network	3	3	
II	3	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.	3	3	

II	4	Zone transfer is a way of gather information when footprinting a network is through Domain Name System (DNS). DNS is the network component responsible for resolving hostnames to IP addresses and vice versa.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. This process, called a zone transfer, can be done with the Dig command.	3	3	
II	5	Packets contain source and destination IP addresses as well as information about the flags SYN, ACK, FIN, and so on. Create a packet with a specific flag set. Hping and Fping are helpful tools for crafting IP packets	3	3	
II	6	**Remote procedure call (RPC)** 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.	3	3	
II	7	**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.	1 1 1	3	
II	8	-Apache– This is the commonly used web server on the internet. It is installed on Linux. Most PHP websites are hosted on Apache servers. - Internet Information Services (IIS)– It is developed by Microsoft. It runs on Windows. Most asp and aspx websites are hosted on IIS servers. -Apache Tomcat – Most Java server pages (JSP) websites are hosted on this type of web server.	1 1 1	3	
II	9	**Metasploit and Neosplit.** **Metasploit**– this is an open source tool for developing, testing and using exploit code. It can be used to discover vulnerabilities in web servers and write exploits that can be used to compromise the server. **Neosplit** – this tool can be used to install programs, delete programs, replicating it, etc.	1.5 1.5	3	
II	10	**Service Set Identifiers** A service set identifier (SSID) is the name used to identify a WLAN, much the same way a workgroup is used on a Windows network. An SSID is configured on the AP as a unique, 1 - to 32 character, case-sensitive alphanumeric name. For wireless-enabled computers to access the WLAN the AP connects to, they must be configured with the same SSID as the AP. The SSID name, or code is attached to each packet to identify it as belonging to that wireless network	3	3	
		PART C			42
III		**VIRUS** A virus is a program that attaches itself to a file or another program, often sent via e-mail. A virus doesn't stand on its own, so it can't replicate itself or operate without the		7	

		presence of a host. A virus attaches itself to a host file or program just attaches itself to a host organism, and then performs whatever the creator designed it to do. Viruses may be classified into the following categories: o Boot sector infector: o File infector: o Macro virus: o Encrypted virus **WORMS** A worm is a program that replicates and propagates itself without having to attach itself to a host . Network worm programs use network connections to spread from system to system. To replicate itself, a network worm uses some sort of network vehicle such as E-mail, remote execution capability,remote login capability.	3.5 3.5		
IV		**Distributed Denial of Service Attack** In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of our computer. Then force computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is distributed because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.  There are basically three types of DDOS attacks: 1. Application layer DDOS attack 2. Protocol DDOS attack 3. Volume-based DDOS attack	3 2 1	7	
V		Footprinting tools(Any 3 tools) Footprinting is the process of gathering network information with web tools and utilities. 1. Whois: Gather ip and domain information.	1 2	7	

		2. Nslookup Nslookup is an another useful command to find the information about DNS server including IP addresses of Computers and MX records etc. 3. Traceroute Traceroute(Linux) or Tracert(Windows) is one the important command that would help you to determine the path and the way by which your computer send the packet to the desire(victim) computer.	2 2		
VI		**Nmap** Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running and what type of packet filters/firewalls are in use. **Nessus** Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. Nessus employs the Nessus Attack Scripting Language (NASL), a simple language that describes individual threats and potential attacks. Nessus has a modular architecture consisting of centralized servers that conduct scanning Significant capabilities of Nessus include: Compatibility with computers and servers of all sizes. Detection of security holes in local or remote hosts. Detection of missing security updates and patches. Simulated attacks to pinpoint vulnerabilities. Execution of security tests in a contained environment. Scheduled security audits.	3.5 3.5	7	
VII		Competitive intelligence Competitive intelligence is the process of gathering information about the competitors through observation and web tools. **Conducting competitive intelligence** Analyzing a company's web site Network attacks often begin by gathering information from a company's Web site because Web pages are an easy way for attackers to discover critical information about an organization. Using other footprinting tools The Whois utility is a commonly used Web tool for gathering IP address and domain information. With just a company's Web address, you can discover a tremendous amount of information. Using Email addresses Based on an e-mail account listed in DNS output, you might discover that the company's e-mail address format is first	2 5	7	

		name initial, followed by last name and the @companyname.com sequence. Using HTTP basics A security tester can pull information from a Web server by using HTTP commands. You've probably seen HTTP client error codes before, such as 404 Not Found. Detecting cookies and web bugs			
VIII		The attacking techniques used for Social Engineering Social engineering is the ability to use an understanding of human nature to get information from unsuspecting people. **Attacking techniques used for Social Engineering** Shoulder surfing Dumpster diving Piggybacking Phishing SHOULDER SURFING Shoulder surfing refers to the act of obtaining personal or private information through direct observation. Shoulder surfing involves looking over a person's shoulder to gather information. 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. 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 employee. PHISHING 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.	1 2 4	7	
IX		**Windows password and authentication policies(Any seven points)** 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,	1*7	7	

		jargon, or dialect. • Passwords must not be identified with a particular user, such as birthdays, names, or companyrelated 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 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.			
X		**Counter measures against Linux OS** □ 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. **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 a penetration testing tool	3 4	7	
XI		**Common Internet file system.** CIFS is a remote file system protocol that enables computers to share network resources over the Internet. To share files and folders, CIFS relies on SMB, but it offers many enhancements, including the following:	1		
		• Locking features that enable multiple users to access and update a file simultaneously without conflicts • Caching and read-ahead/write-behind capability • Support for fault tolerance • Capability to run more efficiently over slow dial-up lines • Support for anonymous and authenticated access to files to improve security To prevent unauthorized access to these files, CIFS relies on SMB's security model. An administrator can select two methods for server security: Share-level security—A folder on a disk is made available to users for sharing. A password can be configured for the share but isn't required. User-level security—The resource is made available to network users; however, a username and password are required to access the resource.	3 3	7	
XII		**Hardening of Windows systems** Methods of hardening are: -Patching systems		7	

		-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.	7		
XIII		**Components of web application** Web application is supported by a Web server that runs on a general-purpose or embedded OS. Each component (application, server, and OS) has its own set of vulnerabilities. Web application components are: Web forms Common Gateway Interface (CGI) Active Server pages (ASP) Web servers PHP Cold Fusion VB script, Javascript OLE DB(Object Linking and Embedding database), ODBC Active x Data objects	2 5	7	
XIV		**War Driving and the tools used for War Driving.** To conduct war driving, an attacker or a security tester simply drives around with a laptop computer containing a WNIC, an antenna, and software that scans the area for SSIDs. Not all WNICs are compatible with scanning software, so you might want to look at the software requirements first before purchasing the hardware. Antenna prices vary, depending on their quality and the range they can cover. Most scanning software detects the company's SSID, the type of security enabled, and the signal strength, indicating how close the AP is to the attacker. **Tools for war driving** WLANs can be attacked with many of the same tools used for hacking wired LANs. Wireshark(sniffer) can also be used to scan WLANs. NetStumbler – is a freeware tool for windows to detect WLANs. iwScanner Kismet – can detect hidden network SSIDs. It is a passive scanner.	3.5 3.5	7	