225

12

Scoring Indicators

COURSE NAME : ETHICAL HACKING
COURSE CODE : 5133B (21)

QID : 2109230298

PART A

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

(9 x 1 = 9 Marks)
Max. marks

Q.No	Scoring Indicators	Split score	Sub Total	Total score
	PART A			9
I.1	An ethical hacker is a person who performs most of the same activities a hacker does but with the owner or company's permission.		1	
I.2	White box model, Black box model, Grey box model (Any one).		1	
I.3	Confidentiality, Integrity, and Availability.		1	
I.4	The process of finding information on a company's network is called footprinting.		1	
I.5	Domain Name System.		1	
I.6	Common Internet File System.		1	
I.7	New Technology File System.		1	
I.8	Open Web Application Security Project.		1	
I.9	Service Set Identifier.		1	
	PART B			24
II.1	Virus, Macro Virus, Worms, Trojan Programs, Spyware, Adware. (Any three).	3 x 1	3	
II.2	An ethical hacker is a person who performs most of the same activities a hacker does but with the owner or company's permission. A cracker accesses a computer system or network without the authorization of the system's owner. A cracker will be charged with a crime but an ethical hacker will not be charged. Ethical hackers are usually contracted to perform penetration tests or security tests.	2 1	3	
II.3	Black hats, White hats, and Grey hats. Black hat hackers access systems illegally, with malicious intent, and often for personal gain. White hat hackers work with companies to identify weaknesses in their systems and make corresponding updates.	1 1 1	3	

	Grey hat hackers are somewhere in the middle. These may sometimes violate laws or typical ethical standards, but usually does not have the malicious intent typical of a black hat hacker. There are many different types of hackers, but the most common are black hat, white hat, and grey hat hackers.			
II.4	Antivirus programs can detect many malware programs. Educating users about the types of attacks is also important. A network can be protected by installing a firewall with Intrusion Detection System. Protecting an organization from malware attacks is difficult because new viruses, worms, and Trojan programs appear daily.	1 1 1	3	
II.5	Whois, Nmap, NSlookup, Sam Spade, SuperScan, Nessus. Whois utility is a commonly used Web tool for gathering IP address and domain information. The Whois utility gives you information on a company's IP addresses and any other domains the company might be part of. Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities. Nslookup is an application that lets users enter a host name and find out the corresponding IP address or domain name system (DNS) record. Users can also enter a command in nslookup to do a reverse DNS lookup and find the host name for a specified IP address.	1 1 1	3	
II.6	DNS is the network component responsible for resolving host names to IP addresses and vice versa. DNS uses name servers to resolve names. After determining what name server a company is using, one 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. To determine a company's primary DNS server, one 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 determining the primary DNS server, one can perform another zone transfer to see all host computers on the company network. Thus the zone transfer gives an organization's network diagram. This is how DNS is a major area of potential vulnerability for network attacks.	3	3	

II.7	Null session is an unauthenticated connection to a Windows computer that uses no logon and password values. It is an anonymous connection established without credentials, such as a username and password. This is also called an anonymous logon. A null session can be used to display information about users, groups, shares, and password policies. Null sessions are necessary only if networks need to support older Windows versions. Null session is one of the biggest vulnerabilities of NetBIOS systems.		3	
II.8	Common Gateway Interface (CGI) is a standard that handles moving data from a Web server to a Web browser. It enables Web designers to create dynamic HTML Web applications. Many dynamic Web pages are created with CGI and scripting languages. CGI is the interface that determines how a Web server passes data to a Web browser. CGI's main role is passing data between a Web server and Web browser.	3	3	
II.9	A network needs components like communication devices to transmit and receive signals, protocols, and a medium for transmitting data. A wireless network has the following three major components: 1. Wireless network interface cards (WNICs), which transmit and receive wireless signals, and access points (APs), which are the bridge between wired and wireless networks. 2. Wireless networking protocols, such as Wi-Fi Protected Access (WPA). 3. A portion of the RF spectrum, which replaces wire as the connection medium.	1 1 1	3	
II.10	Driving around with inexpensive hardware and software that enables one to detect access points that haven't been secured is known as wardriving. Wardriving has now been expanded to include warflying, which is done by using an airplane wired with an antenna and uses the same software used in wardriving. To conduct wardriving, 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.	3	3	
	PART C			42
III	Malicious software are softwares used to destroy or corrupt data or to shut down a network or computer system. Virus : A virus is a program that attaches itself to a file or another program, often sent via e-mail. The key word is "attaches." A virus doesn't stand on its own, so it can't	1	7	

	replicate itself or operate without the presence of a host. A virus attaches itself to a host file or program. Macro virus : A macro virus is a virus encoded as a macro in programs that support a macro programming language, such as Visual Basic for Applications (VBA). Macro commands that open and close files, can be used in destructive ways. These commands can be set to run automatically as soon as a file is opened or clicked on, as in an e-mail attachment. Eg: Melissa. Worms : A worm is a program that replicates and propagates itself without having to attach itself to a host. Eg: Code Red. Trojan Programs : Trojan programs disguise themselves as useful programs and will install a backdoor or rootkit on a computer. Backdoors or rootkits are programs that give attackers a means of regaining access to the attacked computer later. A rootkit is created after an attack and usually hides itself in the OS tools, so it's almost impossible to detect. Spyware : A spyware program sends information from the infected computer to the person who initiated the spyware program on the target computer. This information could be confidential financial data, passwords, PINs or any data stored on infected computer. Adware : Adware and spyware can be installed without users being aware of their presence. Adware, 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 tailored to this user. The biggest problem with adware is that it slows down the computer it's running on.	Any 3 x 2		
IV	An attack is defined as any attempt by an unauthorized person to access, damage, or use network resources or computer systems. Network security is concerned with the security of computers or devices that are part of a network infrastructure. Denial-of-service (DoS): This attack prevents legitimate users from accessing network resources by flooding the network. Some forms of DoS attacks don't even involve computers. Distributed Denial-of-Service Attacks: A distributed denial-of-service (DDoS) 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.	Any 2 x 3.5	7	

	Buffer overflow attack: In this attack, a programmer finds a vulnerability in poorly written code that doesn't check for a defined amount of memory space use. Basically, the attacker writes code that overflows the buffer, which is possible because the buffer capacity hasn't been defined correctly 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 permissions to an administrator's level or gives the attacker the same privileges as the program's owner or creator. Ping of Death Attacks: The Ping of Death attack is a type of DoS attack. It is not as common as it was during the late 1990s. Here, the attacker simply creates an ICMP packet that is larger than the maximum allowed 65,535 bytes. The large packet is fragmented into smaller packets and reassembled at its destination. User's system at the destination point can't handle the reassembled oversized packet, thereby causing the system to crash or freeze. Session Hijacking: Session hijacking enables an attacker to join a TCP session and make both parties think he or she is the other party. Keyloggers: Key loggers are hardware devices or software that can be used to capture keystrokes on a computer. Software keyloggers behave like Trojan programs and are loaded on a computer. A hardware keylogger is a small device, often smaller than an inch long.			
V	Social engineering means using knowledge of human nature to get information from people. In computer attacks, the information is usually a password to a network or other information an attacker could use to compromise a network. Social engineers use many different techniques in their attempts to gain information from unsuspecting people: Urgency—"I need the information now or the world will come to an end!" For example, a social engineer might tell a user he needs the information quickly or the network will be down for a long time, thus creating a false sense of urgency. Quid pro quo—"I can make your life better if you give me the information I need." The social engineer might promise the user faster Internet access, for example, if he or she helps by supplying information.	Any 2 x 3.5	7	

	Status quo—"Everyone else is doing it, so you should, too." By using the names of other employees, a social engineer can easily convince others to reveal their passwords. Position—Convincing an employee that you're in a position of authority in the company can be a powerful means of gaining information. This is especially true in the military, where rank has its privileges. Following methods are also used by social engineers : 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. Dumpster diving: In this method, useful information is collected by examining someone's trash. Sometimes network administrators write notes in manuals or even note down passwords. Company phone directories are another source of information. Piggybacking: In this method, a tester or an attacker trails closely behind an employee who has access to an area without the person realizing the attacker didn't use a PIN or a security badge to enter the area. Skilled piggy backers watch authorized personnel enter secure areas and wait for the apt time to join them quickly at the security entrance.			
VI	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. Features : Flexible: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more. Powerful: Nmap has been used to scan huge networks of literally hundreds of thousands of machines. Portable: Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more. Easy: While Nmap offers a rich set of advanced features	1 Any 2 x 3	7	

	for power users, you can start out as simply as "nmap -v -A targethost". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source. Free: The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license. Well Documented: Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages here. Supported: While Nmap comes with no warranty, it is well supported by a vibrant community of developers and users. Popular: Thousands of people download Nmap every day, and it is included with many operating systems (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc).			
VII	1. 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. Many tools are available for this type of information gathering. Eg: Paros is a powerful tool for UNIX and Windows. 2. Using HTTP Basics: HTTP operates on port 80. A security tester can pull information from a Web server by using HTTP commands. A basic understanding of HTTP can be beneficial to security testers. If the return codes generated by a Web server is known, one can determine what OS is used on the computer where the security test is being conducted. 3. Detecting Cookies and Web Bugs: A cookie is a text file generated by a Web server and stored on a user's browser. The information in this file is sent back to the Web server when the user returns to the Web site. Some cookies can cause security issues because crooked people might store personal information in cookies that can be used to attack a computer or server. 4. Using E-mail Addresses: Knowing a user's e-mail address can help one to dig even further. Based on an e-mail account listed in DNS output, one can discover the	2 2 2 1	7	

	company's e-mail address format.			
VIII	1. SYN scan—In a normal TCP session, a packet is sent to another computer with the SYN flag set. The receiving computer sends back a packet with the SYN/ACK flag set, indicating an acknowledgment. The sending computer then sends a packet with the ACK flag set. If the port the SYN packet is sent to is closed, the computer responds with an RST/ACK (reset/acknowledgment) packet. If an attacker's computer receives a SYN/ACK packet, it responds quickly with an RST/ACK packet, closing the session. 2. Connect scan—This type of scan relies on the attacked computer's OS, so it's a little more risky to use. A connect scan is similar to a SYN scan, except that it does complete the three-way handshake. This means the attacked computer most likely logs the transaction or connection, indicating that a session took place. Therefore, unlike a SYN scan, a connect scan isn't stealthy and can be detected easily. 3. NULL scan—In a NULL scan, all packet flags are turned off. A closed port responds to a NULL scan with an RST packet, so if no packet is received, the best guess is that the port is open. 4. XMAS scan—In this type of scan, the FIN, PSH, and URG flags are set. Closed ports respond to this type of packet with an RST packet. This scan can be used to determine which ports are open. 5. ACK scan—Attackers typically use ACK scans to get past a firewall or other filtering device. A filtering device looks for the SYN packet, the first packet in the three-way handshake, that the ACK packet was part of. Remember this packet order: SYN, SYN/ACK, and ACK. If the attacked port returns an RST packet, the packet filter was fooled, or there's no packet-filtering device. In either case, the attacked port is considered to be "unfiltered." 6. FIN scan—In this type of scan, a FIN packet is sent to the target computer. If the port is closed, it sends back an RST packet. When a three-way handshake ends, both parties send a FIN packet to end the connection. 7. UDP scan—In this type of scan, a UDP packet is sent to the target computer. If the port sends back an ICMP "Port Unreachable" message, the port is closed. Again, not getting that message might imply the port is open, but this isn't always true. A firewall or packet-filtering device could undermine this assumptions.	Any 2 x 3.5	7	
IX	A password policy should include the following:	Any 7 x	7	

	1. Change passwords regularly on system-level accounts (every 60 days at minimum). 2. Require users to change their passwords regularly (at least quarterly). 3. Require a minimum password length of at least eight characters (and 15 characters for administrative accounts). 4. Require complex passwords; in other words, passwords must include letters, numbers, symbols, punctuation characters, and preferably both uppercase and lowercase letters. 5. Passwords can't be common words, words found in the dictionary (in any language), or slang, jargon, or dialect. 6. Passwords must not be identified with a particular user, such as birthdays, names, or company-related words. 7. Never write a password down or store it online or in a file on the user's computer. 8. Don't hint at or reveal a password to anyone over the phone, in e-mail, or in person. 9. Use caution when logging on to make sure no one sees you entering your password. 10. Limit reuse of old passwords. In addition to these guidelines, administrators can configure domain controllers to enforce password age, length, and complexity.	1		
X	1. Patching Systems : The best way to keep systems secure, operating at peak performance, and using the newest features is to keep systems under care up to date. Many attacks have taken advantage of a known vulnerability that has a patch available. There are several methods for obtaining service packs, hotfixes, and patches. Depending on the Windows version, Automatic Updates can be configured on each machine. This option is usually better because it helps ensure that machines are always up to date without the administrator or user's intervention. The downside is that some patches can cause problems, so testing a patch before applying it to a production system is preferable, particularly in large networks. 2. Antivirus Solutions: An antivirus solution is essential for small or large organisations. For small networks, desktop antivirus tools with automatic updating might be enough, but in a large network, a corporate-level solution is needed. Several excellent products are available, and selecting the right one requires some research. An	Any 2 x 3.5	7	

	antivirus tool must be planned, installed, and configured correctly to ensure the best protection. An antivirus tool is almost useless if it isn't updated regularly. Ideally, an antivirus tool should automatically download and install updates daily. 3. Enable Logging and Review Logs Regularly: Logging is an important step for monitoring many crucial areas, including performance, traffic patterns, and possible security breaches. It must be configured carefully to record only useful statistics because logging can have a negative impact on performance. Review logs regularly for signs of intrusion or other problems on the network. Scanning through thousands of log entries is time consuming, and missing important entries is likely. A log-monitoring tool is best for this task. 4. Disable Unused Services and Filtering Ports: Disabling unneeded services and deleting unnecessary applications or scripts is important because they give intruders a potential point of entry into a network. The idea is simple: Open only what needs to be open, and close everything else: also known as reducing the attack surface. 5. Closing ports: Filtering out unnecessary ports can protect systems from attack.			
XI	a) NetBIOS: NetBIOS is software loaded into memory that enables a program to interact with a network resource or device. Network resources are identified with 16-byte NetBIOS names. NetBIOS is the interface to a network protocol that enables a program to access a network resource. NetBIOS does not have built-in authentication mechanisms, making it susceptible to unauthorized access, spoofing attacks, and man-in-the-middle attacks. An attacker could potentially gain access to network resources or impersonate a legitimate device on the network. b) 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. The Conficker worm took advantage of a vulnerability in RPC to run arbitrary code on susceptible hosts.	3.5 3.5	7	
XII	1. User Awareness Training: Train users so that no information is given to outsiders, no matter how harmless the information might seem. Make users aware that many exploits can be downloaded from Web sites, and emphasize that knowing which OS is running makes it easier for attackers to select an exploit. 2. Keeping Current: As soon as a bug or vulnerability is	Any 2 x 3.5	7	

	discovered and posted on the Internet, OS vendors usually notify customers of upgrades or patches. Installing these fixes promptly is essential to protect the system. 3. Secure Configuration: Many methods and tools can be used to configure a Linux system to help prevent intrusions. Vulnerability scanners not only detect missing patches, but also help identify when a system is configured poorly.			
XIII	1.Cross-site scripting (XSS) flaws—In this vulnerability, a Web browser might carry out code sent from a Web site. Attackers can use a Web application to run a script on the Web browser of the system they're attacking. XSS is one of the easiest types of attacks to perform, which also makes it one of the most common. 2.Injection flaws—Many Web applications pass parameters when accessing an external system. An attacker can embed malicious code and run a program on the database server or send malicious code in an HTTP request. 3.Malicious file execution—Some Web applications allow users to reference or upload files containing malware. If these references or files aren't checked before the Web application executes them, they can give attackers complete control of the system. 4. Unsecured direct object reference—This vulnerability occurs when information returned via the URL to a user's Web browser contains information about files, directories, or database records. By simply changing the information in the URL, attackers can gain unauthorized access to information. 5. Cross-site request forgery (CSRF)—This vulnerability is also known as a one-click or session-riding attack. To send malicious code to a Web application, the attacker exploits a Web browser that has already been authenticated and is, therefore, trusted. Because the malicious code is coming from a trusted Web browser, it's normally executed without being checked or validated. This vulnerability can be extremely dangerous. 6. Information leakage and incorrect error handling—If an error occurs during normal operations and isn't handled correctly, information sent to users might reveal information attackers can use. 7. Broken authentication and session management—These vulnerabilities enable attackers to compromise passwords or session cookies to gain access to accounts. 8. Unsecured cryptographic storage—Storing keys,	Any 2 x 3.5		

	certificates, and passwords on a Web server can be dangerous. If an attacker can gain access to these mechanisms, the server is vulnerable to attack. 9. Unsecured communication—Connections between the Web browser and the Web application should be encrypted to protect information as it travels across the Internet. 10. Failure to restrict URL access—This vulnerability occurs when developers don't use adequate access controls for URLs.			
XIV	1. Infrared—Infrared light can't be seen by the human eye. Infrared (IR) technology is restricted to a single room or line of sight because IR light can't penetrate walls, ceilings, or floors. This technology is used for most remote controls and for syncing PDAs. 2. Narrowband—Narrowband technology uses microwave radio band frequencies to transmit data. The most common uses of this technology are cordless phones and garage door openers. 3. Spread spectrum—For data to be moved over radio waves, it must be modulated on the carrier signal or channel. Modulation defines how data is placed on a carrier signal. Spread spectrum uses the following 3 methods : a. Frequency-hopping spread spectrum (FHSS). b. Direct sequence spread spectrum (DSSS). c. Orthogonal frequency division multiplexing (OFDM).	2 2 3	7	