Scoring Indicators

COURSE NAME: Ethical Hacking

COURSE CODE: 5133B **QID: 2109230295**

Q. No.		Scoring Indicators	Split Score	Sub Total	Total Score
PART A					**9**
I	1	**Malware** is malicious software, such as a virus, worm, or Trojan program, introduced into a network to destroy or corrupt data or to shut down a network or computer system.	1	1	
I	2	White, Grey and Black Hackers.	-	1	
I	3	Ping Of Death is a denial of service network attack.	1	1	
I	4	Nmap, hping and fping (any two)	2*0.5	1	
I	5	**Piggy backing** is another method of gaining access to restricted area using an authorized person's help.	1	1	
I	6	Windows file system, Remote Procedure call, NetBIOS, Server Message Block, CIFS, Buffer overflow (any 2)	2*.05	1	
I	7	User awareness training, Keeping current(up to date), Secure configuration (any 2)	2*.05	1	
I	8	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.	1	1	
I	9	Wi-Fi Protected Access (WPA)	1	1	
PART B					**24**
II	1	A **virus** is a program(malware) 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 presence of a host.(rain drops, ransomeware etc) A **worm** is a program(malware) that replicates and propagates itself without having to attach itself to a host (unlike a virus, which needs to attach itself to a host). Eg. Code Red, Nimda, and Conficker	2*1.5	3	
II	2	In a **replay attack**, the attacker captures data and attempts to resubmit the captured data so that the device, which can be a computer or router, thinks a legitimate connection is in effect. If the captured data is logon information, the attacker could gain access to a system and be authenticated.	-	3	
II	3	In a **man-in- the-middle attack,** attackers place themselves between the victim computer and another host computer. They can then intercepts messages sent form the victim to the host and pretend to be the host computer. Here the malicious user impersonates both the parties (sender and receiver) and gain access to information that the two parties were trying to send each other.	-	3	

II	4	**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. Eg. dumpster diving, shoulder surfing, piggy backing etc (Definition -2 marks , example 1 mark)	2+1	3	
II	5	Nmap is a port scanning tool and it can also be used to identify the remote operating system.The example command with remote systems ip 192.168.5.54 is nmap –sV –allports 192.168.5.54 –o Nmap can be used to conduct ping sweep also nmap –sn 192.168.5.1/24 or nmap –sn 192.168.5.*	2*1.5	3	
II	6	In Windows, **Server Message Block** (SMB) is used to share files and usually runs on top of NetBIOS, NetBEUI, or TCP/IP. Several hacking tools that target SMB can still cause damage to Windows networks. Two well-known SMB hacking tools are L0phtcrack's SMB Packet Capture utility and SMBRelay, which intercept SMB traffic and collect usernames and pass- word hashes. Microsoft introduced SMB2 in Windows Vista, and this version has several new features and is faster and more efficient.	2*1.5	3	
II	7	**Remote Procedure Call (RPC)** is an inter process communication mechanism that allows a program running on one host to run code on a remote host.	-	3	
II	8	Web forms, Common Gateway Interface, Active Server Page, virtual directory, IIS , Apache web server, Scripting Languages-(PHP, Cold fusion Scripting Languages, VBscript, Java script, Python etc) database connectivity (ODBC, OLEDB) (Any 6)	6*0.5	3	
II	9	Wireless network includes- Wireless Network Interface Card(WNIC),a portion of Radio frequency spectrum as medium and Wi-Fi Protected Access (WPA) as protocol and an Access point(AP- an interface between wired and wireless network)	3*1	3	
II	10	**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; attackers simply save the form to their local computers and change the form field values.	-	3	

		PART C			**42**
III		**Brute force attack** is a trial and error method used to obtain information such as user password or personal identification number (PIN) or Encryption keys. In this automated software is used to generate the large number of consecutive guesses as to the value of the desired data. In a **dictionary attack**, after attackers have access to a password file, they can run a password- cracking program that uses a dictionary of known words or passwords as an input file. Most of these input files are available on the Internet and can be downloaded free. It can also used in an attempt to find the key necessary to decrypt an encrypted message or document.	2*3.5	7	
IV		**DoS** – Denial of service. –Prevents legitimate users from accessing network resources- Keeps the network or server busy by sending excessive messages-uses one computer and internet connection to flood a targeted system or resource. **DDoS** – Distributed denial of service – uses multiple computers and internet connections to flood the targeted resource-difficult to stop-systems are unaware that they are sending malicious packets to a victim.	2*3.5	7	
V		A method, social engineers use to gain access to information is **dumpster diving**. It is form of gathering information, by examining someone's trash. For example, discarded computer manuals can indicate what OS is being used. **Phishing** is a form of social engineering. It is a technique for attempting to acquire sensitive data such as bank account numbers, through a fraudulent solicitation in email or on a website , in which the perpetrator masquerades as a legitimate business or reputable person	2*3.5	7	
VI		SYN scan, Connect scan, NULL scan, XMAS scan, ACK scan, FIN scan, UDP scan.	7*1	7	
VII		Both are port scanning tools. Namp – Network mapper – allows finding out which TCP ports are open on the target host. Nmap [options] target Target is the IP address of the target host Many options for scanning, version detection etc Nessus – remote security scanning tool – discovers any vulnerability by running tests on a given computer. Contains nessus server and client.	2*3.5	7	
VIII		Port scanners can also be used to conduct a ping sweep			

		of a large network to identify which IP addresses belong to active hosts. With the Fping tool you can ping multiple IP addresses simultaneously. Ping can accept a range of IP addresses entered at a command prompt, or you can create a file containing multiple IP addresses and use it as input for the Fping command. For example, the fping -f ip_address.txt command uses ip_address.txt, which contains a list of IP addresses, as its input file. You can also use the Hping tool to perform ping sweeps. However,many security testers use it to bypass filtering devices by injecting crafted or otherwise modified IP packets. This tool offers a wealth of features.	2*3.5	7	
IX		Many tools are available for discovering Windows vulnerabilities. Using more than one tool for analysis is advisable. Popular OS vulnerability scanners include eEye, Retina, Tenable, Nessus, QualysGuard, GFI Languard, and IBM Internet Scanner as well as OpenVAS. In addition, several tools are built into Windows. **Built-in Windows Tools** - Microsoft Baseline Security Analyzer (MBSA). This tool is capable of checking for patches, security updates, configuration errors, blank or weak passwords, and more. (listing -2 marks: explanation -5 marks)	2+5	7	
X		Patching Systems, Antivirus solutions, Enable Logging and Review logs regularly, Disable unused services and Filtering ports, Other Security best practices. (Listing 2 marks Explanation of each point -5 marks)	2+5	7	
XI		Change system level password regularly, Request user to change their password regularly, maintain minimum password length, complex password, password cannot be common name, never write down the password, don't hint a password, avoid shoulder surfing of password, Limit reuse of password, Lock system after 2-3 password failure – 7 points(7 marks)	7*1	7	
XII		**User awareness training** – Train users for not giving information to outsiders and make them aware that many exploits are downloaded from websites. **Keeping current on kernel releases and security**– Update to protect the system and update security tools. **Secure configuration** – Security enhanced Linux contains mandatory access control that enforces access rules based on privileges. (listing 1mark, explanation 2marks each)	1+3*2	7	
XIII		**War driving**—driving around with inexpensive hardware and software that enables hackers to detect access points that haven't been secured. Most APs	4+3	7	

		have no passwords or security measures, so war driving can be quite rewarding for hackers. By this method attackers can directly get access to the wireless network. (4 marks). The attacker simply drives around with a laptop containing a WNIC, an antenna and software that scans the area for SSID. The testers used Kismet, and Netstumbler tools which identifies APs that attempt to "cloak" or hide their SSIDs. (3marks)			
XIV		Cross-site scripting (XSS) flaws, Injection flaws, Malicious file execution, Cross-site request forgery (CSRF), Information leakage and incorrect error handling, Broken authentication and session management, Unsecured cryptographic storage, Unsecured communication, Failure to restrict URL access (Any 7*1)	7*1	7	