Version B

137
13/11/23

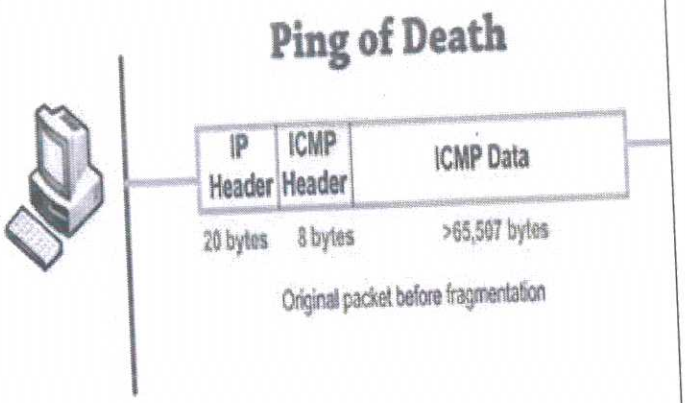
13
NOV-23

Scoring Indicators

COURSE NAME : ETHICAL HACKING

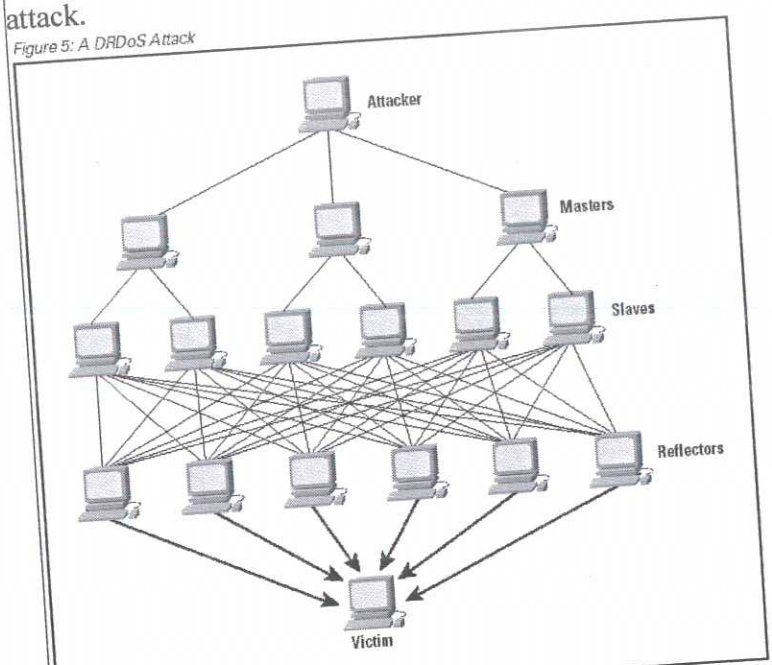
COURSECODE: 5133B **QID:2109230297**

Q No	Scoring Indicators	Split score	Sub Total	Total score
	PART A			9
I. 1	Norton, McAfee, AVG,AVIRA etc.	½+½	1	
I. 2	A penetration test (pen test) is an authorized simulated attack performed on a computer system to evaluate its security. Penetration testers use the same tools, techniques, and processes as attackers to find and demonstrate the business impacts of weaknesses in a system.		1	
I. 3	Whois,nslookup	½+½	1	
I. 4	ACK		1	
I. 5	Port scanning tool		1	
I. 6	Ext2,ext3,ext4 etc.		1	
I. 7	Null session is an anonymous connection established **without credentials**, such as a username and password. Also called an anonymous logon.		1	
I. 8	Apache,IIS	½+½	1	
I. 9	A service set identifier (SSID) is the name used to identify aWLAN, much the same way a workgroup is used on a Windows network. An SSID is configuredon the AP as a unique, 1- to 32-character, case-sensitive alphanumeric name.		1	
	PART B			24
II. 1	**Availability**: Availability ensures that information and resources are accessible and usable when needed by authorized users. This principle aims to prevent disruptions, denial of service, or other attacks that could render the system or data inaccessible, leading to potential business downtime or loss of productivity.		3	
II. 2	A Worm is a form of malware that replicates itself and can spread to different computers via Network. It doesn't need a host to replicate from one computer to another. A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data. It requires a host is needed for spreading.		3	
II. 3	**Ping of Death**		3	

	In a Ping of Death attack, the attacker crafts an ICMP packet to be larger than the maximum 65,535 bytes, which causes the recipient system to crash or freeze. Most systems today aren't affected by this exploit.  The size of a correctly-formed IPv4 packet including the IP header is 65,535 bytes, including a total payload size of 84 bytes. Many historical computer systems simply could not handle larger packets, and would crash if they received one. This bug was easily exploited in early TCP/IP implementations in a wide range of operating systems including Windows, Mac, Unix, Linux, as well as network devices like printers and routers. Since sending a ping packet larger than 65,535 bytes violates the Internet Protocol, attackers would generally send malformed packets in fragments. When the target system attempts to reassemble the fragments and ends up with an oversized packet, memory overflow could occur and lead to various system problems including crash.			
II. 4	Have a documented equipment decommissioning process Use the appropriate secure storage media deletion process Have data retention policy Educate employees	3x1 mark	3	
II. 5	**DNS Zone transfer** 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. People would much rather memorize a URL than an IP address. DNS is a major area of potential vulnerability for network attacks. DNS uses name servers to resolve names. 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	

	To determine a company's primary DNS server, you 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 you determine the primary DNS server, you can perform another zone transfer to see all host computers on the company network. In other words, the zone transfer give you an organization's network diagram. You can use this information to attack other servers or computers that are part of the network infrastructure.			
II. 6	❖ **Patching systems** ❖ **Antivirus solutions** ❖ **Enable logging and review logs regularly** ❖ **Disable unused services and filtering ports** ❖ **Other security practices**	3x1 mark	3	
II. 7	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 foradministrative 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, jargon, or dialect. • Passwords must not be identified with a particular user, such as birthdays, names, orcompany-related 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.	3x1 mark	3	
II. 8	▪ Web forms ▪ Common Gateway Interface (CGI)	3x1 mark	3	

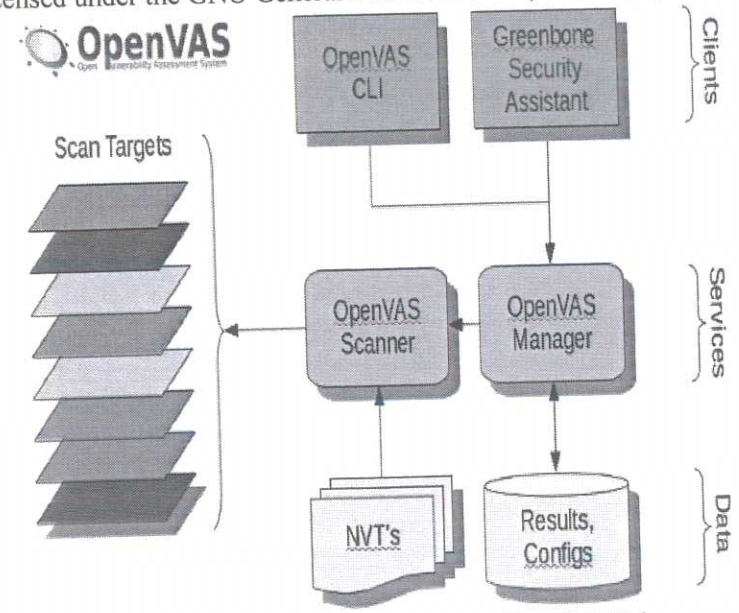
	▪ Active Server pages (ASP) ▪ Web servers ▪ PHP ▪ Cold Fusion ▪ VB script, Javascript ▪ OLE DB(Object Linking and Embedding database), ODBC ▪ Active x Data objects			
II.9	1. **Cross-site request forgery (CSRF)**—This vulnerability is also known as a one-click or session-riding attack. To send malicious code to a Web application, the attacker exploits a Web browser that has already been authenticated and is, therefore, trusted. Becausethe malicious code is coming from a trusted Web browser, it's normally executed withoutbeing checked or validated. This vulnerability can be extremely dangerous.		3	

II.10	• Wireless network interface cards (WNICs), which transmit and receive wireless signals,and access points (APs), which are the bridge between wired and wireless networks • Wireless networking protocols, such as Wi-Fi Protected Access (WPA) • A portion of the RF spectrum, which replaces wire as the connection medium	3x1 mark	3	
				42
	PART C			
III.	**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 your computer. He or she could then force your 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. *Figure 5: A DRDoS Attack*  There are basically three types of DDOS attacks: **1. Application layer DDOS attack** Application-layer DDOS attacks are attacks that target Windows, Apache, OpenBSD, or other software vulnerabilities to perform the attack and crash the server.	Explanation 4 marks + counter measures 3 marks	7	7

	2. Protocol DDOS attack A protocol DDOS attacks is a DOS attack on the protocol level. This category includes Synflood, Ping of Death, and more. **3. Volume-based DDOS attack** This type of attack includes ICMP floods, UDP floods, and other kind of floods performed via spoofed packets. There are many tools available for free that can be used to flood a server and perform an attack. A few tools also support a zombie network to perform DDOS attacks. **Countermeasures** Reduce Attack surface area Know what is normal and abnormal traffic Deploy firewalls for sophisticated application attacks			
IV	1. **Adware:**. The least dangerous and most lucrative Malware. Adware displays ads on your computer. 2. **Spyware**:. Spyware is software that spies on you, tracking your internet activities in order to send advertising (Adware) back to your system. 3. **Virus:** 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. Most often this is spread by sharing software or files between computers. 4. **Worm:** A program that replicates itself and destroys data and files on the computer. Worms work to "eat" the system operating files and data files until the drive is empty. 5. **Trojan:** The most dangerous Malware. Trojans are written with the purpose of discovering your financial information, taking over your computer's system resources, and in larger systems creating a "denial-of-service attack " Denial-of-service attack: an attempt to make a machine or network resource unavailable to those attempting to reach it. Example: AOL, Yahoo or your business network becoming unavailable.	List 3 marks+explanation 4 marks	7	7
V.	• **SYN scan**—In a normal TCP session, a packet is sent to another computer with theSYN 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 theACK flag set. If the port the SYN packet is sent to is closed, the computer respondswith an RST/ACK (reset/acknowledgment) packet. If an attacker's computer receivesa SYN/ACK packet, it responds quickly with an RST/ACK packet, closing the session. This is done so that a full TCP connection is never made and logged		7	7

	as a transaction.In this sense, it's "stealthy." After all, attackers don't want a transaction logged showingtheir connection to the attacked computer and listing their IP addresses. • **Connect scan**—This type of scan relies on the attacked computer's OS, so it's a littlemore risky to use. A connect scan is similar to a SYN scan, except that it does completethe three-way handshake. This means the attacked computer most likely logs thetransaction or connection, indicating that a session took place. Therefore, unlike aSYN scan, a connect scan isn't stealthy and can be detected easily.			
VI	**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 pertinent information while the victim is oblivious. 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. **Countermeasures** Educate users not to type logon namesand passwords when someone is standing directly behind them—or even standing nearby. Caution users about typing passwords when someone nearby is talking on acell phone because of the wide availability of camera phones. Make sure all computer monitors face away from the door or the cubicleentryway. Warn your users to change their passwords immediately if they suspect someonemight have observed them entering their passwords.	Explanation 4 marks + counter measures 3 marks	7	7
VII	Footprinting is a first step that a penetration tester used to evaluate the security of any IT infrastructure. Footprinting is then process of gathering network information with web tools and utilities. Footprinting is a first and the important step because after this a penetration tester know how the hacker sees this network. To measure the security of a computer system, it is good to know more and more as you can because after this you will able to determine the path that a hacker will use to exploit this network. the systematic and methodical footprinting of an organization enables attackers to create a near complete profile of an organization's security posture. Footprinting tools Whois,nslookup Search engines Social networking sites	Definition 3 marks+explanation 4 marks	7	7
VIII	**Ping sweep** Port scanners can also be used to conduct a ping sweep of a large network to identify which IP addresses belong to active hosts. In other words, to find out which	Definition 4 marks+ tools 3 marks	7	7

	hosts are "live," pingsweeps simply ping a range of IP addresses and see what type of response is returned. Theproblem with relying on ping sweeps to identify live hosts is that a computer might be shut down at the time of the sweep and indicate that the IP address doesn't belong to a live host. Another problem with ping sweeps is that many network administrators configure nodes tonot respond to an ICMP Echo Request (type 8) with an ICMP Echo Reply (type 0). Thisresponse doesn't mean the computer isn't running; it just means it isn't replying to the attackcomputer. Another problem is that a firewall filtering out ICMP traffic, and you have many reasons for using caution when running ping sweeps. Many tools can be used to conduct a pingsweep of a network: Fping,Hping,nmap			
IX	**Tools for identifying vulnerabilities in windows** **Popular OS vulnerability scanners** ❖ eEye Retina, Tenable Nessus, QualysGuard, GFI Languard, OpenVAS (These are used for both windows and Linux scanner) ❖ Microsoft baseline Security Analyser (MBSA) is a built in windows tool. MBSA performs the following actions during a scan: ▪ Checks for available updates to the operating system, Microsoft Data Access Components (MDAC), MSXML (Microsoft XML Parser), .NET Framework, and SQL Server. ▪ Scans a computer for insecure configuration settings. When MBSA checks for Windows service packs and patches, it includes in its scan Windows components, such as Internet Information Services (IIS) and COM+. ▪ Uses Microsoft Update and Windows Server Update Services (WSUS) technologies to determine what updates are needed. **OpenVAS** OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability	3 ½ + 3 ½	7	7

	management solution. The framework is part of Greenbone Networks' commercial vulnerability management solution from which developments are contributed to the Open Source community since 2009. All OpenVAS products are Free Software. Most components are licensed under the GNU General Public License (GNU GPL).  The Open Vulnerability Assessment System (OpenVAS) is a framework of several services and tools. The core of this SSL-secured service-oriented architecture is the **OpenVAS Scanner**. The scanner very efficiently executes the actual Network Vulnerability Tests (NVTs) which are served via the OpenVAS NVT Feed or via a commercial feed service.			
X	**Server Message Block (SMB)** The Server Message Block protocol is a client-server communication protocol used for sharing access to files, ports and other resources on a network. 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 password hashes.		7	7

From cve website:

The SMBv1 protocol is not safe to use. By using this old protocol, you lose protections such as pre-authentication integrity, encryption, disabling insecure guest logins, and improved message signing.
Vulnerabilities
SMB signing weakness
Brute force attacks
Man in the middle attacks
Null sessions

Common Internet File System (CIFS)

Common Internet File System (CIFS) is a standardized protocol that replaced SMB inWindows 2000 Server and later, but to allow backward compatibility, the original SMB isstill used. CIFS is a remote file system protocol that enables computers to share network resources over the Internet. In other words, files, folders, printers, and other resources can bemade available to users throughout a network. For sharing to occur, there must be an infrastructurethat allows placing these resources on the network and a method to control accessto resources. CIFS relies on other protocols to handle service announcements notifying userswhat resources are available on the network and to handle authentication and authorizationfor accessing these resources. CIFS is also available for many *nix systems.

To share files and folders, CIFS relies on SMB, but it offersmany enhancements, including the following:

- Locking features that enable multiple users to access and update a file simultaneouslywithout 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. Anadministrator 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

<table>
<tr><td></td><td>network users; however, a username and password are required to access the resource. The SMB server maintains an encrypted version of users' passwords to enhance security.
Cifs is unsecure implementation of SMB
Cifs lack of encryption made it vulnerable- Ransomware attacks</td><td></td><td></td><td></td></tr>
<tr><td>X1</td><td><table>
<tr><th></th><th>NTFS</th><th>FAT32</th></tr>
<tr><td>Full-Form</td><td>New Technology File System</td><td>File Allocation Table</td></tr>
<tr><td>Structure</td><td>Complex</td><td>Simple</td></tr>
<tr><td>Maximum file size</td><td>16 TB</td><td>4 GB</td></tr>
<tr><td>Encryption</td><td>Encrypted with Encrypting File System (EFS)</td><td>Not encrypted</td></tr>
<tr><td>Fault tolerance</td><td>Automatic troubleshooting is present</td><td>No provision for fault tolerance</td></tr>
<tr><td>Compression</td><td>Supports file compression</td><td>No compression is allowed</td></tr>
<tr><td>User-level disk space</td><td>Present</td><td>Not present</td></tr>
</table></td><td>Name file system 1mark+ Any 3 points x2 marks</td><td>7</td><td>7</td></tr>
<tr><td>XII</td><td>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. In addition, free benchmark tools are available from the Center for Internet Security, and commercial tools with templates can be used to tighten security configurations quickly and easily.

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 apenetration testing tool</td><td>Counter measures 4 marks+tools 3 marks</td><td>7</td><td>7</td></tr>
<tr><td>XIII</td><td><u>Countermeasures against wireless attack</u></td><td></td><td>7</td><td>7</td></tr>
</table>

	Protecting a wireless network is a challenge for security professionals because of the inherent design flaws of wireless technology and because, to some extent, engineers are attempting toplace a band-aid over a gaping chest wound. Some countermeasure techniques discussed inthis section, such as using certificates on all wireless devices, are time consuming and costly.If you approach securing a wireless LAN as you would a wired LAN, you'll have a betterchance of protecting corporate data and network resources. Would you allow users to haveaccess to network resources simply because they plugged their NICs into the company'sswitch or hub? Of course not. Then why would you allow users to have access to a wirelessLAN simply because they have WNICs and know the company's SSID? If a company must use wireless technology, your job is to make it as secure as possible. Be sure wireless users are authenticated before being able to access any network resources. Hereare some additional guidelines to help secure a wireless network: • Consider using anti-wardriving software to make it more difficult for attackers to discoveryour WLAN. honeypots, which are hosts ornetworks available to the public that entice hackers to attack them instead of a company'sreal network. IT personnel can study how an attack is made on the honeypot,which can be useful in securing the company's actual network. To make it more difficultfor wardrivers to discover your WLAN, you can use Black Alchemy Fake AP(available free at www.blackalchemy.to/project/fakeap/). As its name implies, this programcreates fake APs, which keeps wardrivers so busy trying to connect to nonexistentwireless networks that they don't have time to discover your legitimate AP. • There are measures for preventing radio waves from leaving or entering a building sothat wireless technology can be used only by people in the facility. One is using a certaintype of paint on the walls,			

	but this method isn't foolproof because some radiowaves can leak out if the paint isn't applied correctly. • Use a router to filter unauthorized MAC and IP addresses and prevent them from having network access. Unfortunately, some exploits enable attackers to spoof authorized addresses, but this measure makes exploits more difficult for typical attackers.			
XIV	**WAR DRIVING** 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. Notall WNICs are compatible with scanning software, so you might want to look at the softwarerequirements first before purchasing the hardware. Antenna prices vary, depending on theirquality and the range they can cover. Some are as small as a cell phone's antenna, and someare as large as a bazooka, which you might have seen in old war films. The larger ones cansometimes return results on networks miles away from the attacker. The smaller ones mightrequire being in close proximity to the AP.Most scanning software detects the company's SSID, the type of security enabled, and thesignal strength, indicating how close the AP is to the attacker. Because attacks against WEPare simple and attacks against WPA are possible, any 802.11 connection not using WPA2should be considered inadequately secured. **Tools for war driving** • NetStumbler • iwScanner • Kismet	Explanation 5 marks+tools 2 marks	7	7