COURSE: ETHICAL HACKING

Course Code: 5135

Revision: (2015)

Qn. No		Scoring Indicators	Split up Score	Sub Total	Total
I	1	Ethical hacking is the legal act of finding the possible entry points (weakness) that exist in a computer system or a computer network and usually enters into them for testing purpose	2	2	2
	2	Virus,Worms,Trojanhorse,Randsomeware,Adware,Spyware etc..(any two).	1+1	2	2
	3	The process of finding information on a company' s network is called foot printing.	2	2	2
	4	Shoulder surfing is a social engineering technique to obtain information by looking over the victims shoulder.	2	2	2
	5	War driving—driving around with inexpensive hardware and software that enables hackers to detect access points that haven't been secured. Most APS have no passwords or security measures, so ward riving can be quite rewarding for hackers.	2	2	2
II		**PART B**	1	6	6
II.1		How to prevent malware	1		
		Keep your computer and software updated.	1		
		Use a non-administrator account whenever possible.	1		
		Think twice before clicking links or downloading anything.			
		Be careful about opening email attachments or images.	1		
		Don't trust pop-up windows that ask you to download software.			
		Limit your file-sharing.	1		

II.2	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.	3	6	6
	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.	3		
II.3	IP crafting is the art of creating packet according to various requirements to carry out attacks and to exploit vulnerabilities in a network.	2	6	6
	Used to bypass firewall and intrusion detection system. Use fping to identify the active host Use hping to send crafted packet to the identified host Use tcpdump to watch the traffic enerated	4		
II.4	Microsoft Remote Procedure Call (RPC) defines a powerful technology for creating distributed client/server programs. The RPC run-time stubs and libraries manage most of the processes relating to network protocols and communication. This enables you to focus on the details of the application rather than the details of the network.	3	6	6
	RPC can be used in all client/server applications based on Windows operating systems. It can also be used to create client and server programs for heterogeneous network environments that include such operating systems as Unix and Apple.	3		

II.5	A null session is an anonymous connection to an inter-process communication network service on Windows-based computers. The service is designed to allow named pipe connections but may be used by attackers to remotely gather information about the system. A null session is an anonymous connection to an inter-process communication network service on Windows-based computers. The service is designed to allow named pipe connections but may be used by attackers to remotely gather information about the system.	3 3	6	6
II.6	1.Aircrack 2.AirSnort 3.Kismet 4. Cain & Able. 5. WireShark. 6. WiFi Wireless Cracker. 7. CoWPAtty. 8. Airjack. (any six)	Any six 6*1=6	6	6
II.7	Access Points An access point contains a radio card that communicates with individual user devices on the wireless LAN, as well as a wired NIC that interfaces to a distribution system, such as Ethernet. Routers By definition, a router transfers packets between networks. The router chooses the next best link to send packets on to get closer to the destination. Routers use Internet Protocol (IP) packet headers and routing tables, as well as internal protocols, to determine the best path for each packet. Repeaters-Access points, which require interconnecting cabling, generally play a dominant role for providing coverage in most wireless LAN deployments.	2 2 2	6	6

	PART C	Any five 5*3=15	15	15
III	1.Adware Software package that presents unwanted advertisements to the user of a computer — tracks our internet browsing habits — sends popups containing advertisements related to the sites we have visited.	3		
	2. Spyware — Malicious computer program that spies on us —scans our hard disk for personal information and internet browsing habits — record login usernames and passwords as well as sensitive banking and credit information.	3		
	3.Virus- spread from one computer to another — corrupt or delete data not try to spread itself — spread my means of email, network, copying files or installing illegal software.	3		
	4. Worms - Stand alone malware program — replicates itself without the help of human — hundreds or thousands of copies of itself.	3		
	5. Trojan- Computer worms have been replaced by Trojan malware programs as the weapon of choice for hackers. Trojans masquerade as legitimate programs, but they contain malicious instructions. They've been around forever, even longer than computer viruses, but have taken hold of current computers more than any other type of malware.	3		
	6. Ransomware-Malware programs that encrypt your data and hold it as hostage waiting for a cryptocurrency pay off has been a huge percentage of the malware for the last few years, and the percentage is still growing. Ransomware has often crippled companies, hospitals, police departments, and even entire cities.			
	7.Fileless malware-Fileless malware isn't really a different category of malware, but more of a description of how they exploit and persevere. Traditional malware travels and infects new systems using the file system.			
	(any five)			

IV	Any two network attacks such as session hijacking, ping of death, man-in-the middle, replay etc. Session hijacking - It involves the theft of another one's internet session thereby allowing the attacker to impersonate as the original user-2 types — Active and passive Pin of death — The attacker creates an ICMP packet larger than the maximum allowed 65535 bytes. The larger packet is fragmented into smaller packets and reassembled at its destination. The user's system at the destination point cannot handle oversized packets causing the system to crash or freeze. Replay — The attacker captures data and attempts to resubmit the captured data so that the device thinks that a legitimate connection is in effect. If the captured data is logon information, the attacker could gain access to a system and be authenticated. non replicating malicious program. Disguise as something normal and desirable which makes a victim to install it. Runs as a background process. Classified as back door Trojan, ransom Trojan, spy Trojan, mail finder Trojan. 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. If one server bombards an attacked server with hundreds or even thousands of packets, available network bandwidth could drop to the point that legitimate users notice a performance degradation or loss	3 3 3 4	15	15

	of speed. Now imagine 1000 servers or even 10,000 servers involved, with each server sending several thousand IP packets to the attacked server. There you have it: a DDoS attack. Keep in mind that participants in the attack often aren't aware their computers are taking part in the attack. 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.	2		
V	Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions	3	15	15

	that break security practices, such as revealing sensitive information or granting access to critical resources. Phishing Phishing is a technique of fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate business—a bank, or credit card company—requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN or a credit card number. For example, in 2003, there was a phishing scam in which users received emails supposedly from eBay claiming that the user's account was about to be suspended unless a link provided was clicked to update a credit card (information that the genuine eBay already had). **Shoulder surfing** -Shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder.[1] This attack can be performed either at close range (by directly looking over the victim's shoulder) or from a longer range, for example by using a pair of binoculars or similar hardware.[Dumpster diving-Dumpster diving involves searching through trash or garbage looking for something useful. This is often done to uncover useful information that may help an individual get access to a particular network. Piggy backing -In two-way communication, wherever a frame is received, the receiver waits and does not send the control frame (acknowledgement or ACK) back to the sender immediately. The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame.	4 3 2 3		

	This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as piggybacking.			
VI	SYN scan, Connect scan, NULL scan, PING scan, XMAS scan, ACK scan, FIN scan, UDP scan **SYN scanning** is also known as half-open **scanning**. In **SYN scanning**, the hostile client attempts to set up a TCP/IP connection with a server at every possible port. This is done by sending a **SYN** (synchronization) packet, as if to initiate a three-way handshake, to every port on the server. **TCP HALF-OPEN(SYN SCAN)** This is probably the most common type of port scan. This is a relatively quick scan that can potentially scan thousands of ports per second. It works this way because it does not complete the TCP handshake process. It simply sends a packet with the SYN flag set and waits for the SYN-ACK from the target and does not complete the connection. When you initiate a TCP connection you first send a packet with the SYN (synchronize) flag set to the destination. The destination then acknowledges this synchronize request with a packet with the SYN-ACK (synchronize-acknowledge) flag set. Finally, the sender acknowledges that it got the SYN-ACK response packet by sending the destination a packet with the ACK flag set. Now, a connection is established.	1 4	15	15

	By not sending the final ACK packet to the target after receiving a SYN-ACK, a connection is not established; however, you now know if the target/port is available and listening. If you receive a RST (reset) packet back from the target, then you know that the target is active; however, the port is closed. If no response is received and you know that the target is alive, then the port is considered filtered. **TCP CONNECT** This is essentially the same as the half-open scan above but instead, we finish the handshake process and establish a connection by sending the final ACK packet. This is a much slower means of port scanning as it takes more packets to finish. **UDP** UDP scans are most common to detect DNS, SNMP and DHCP services. UDP scans work by sending a packet, which is usually empty. This can be changed or even set to a random payload for each port. If the target responds with an ICMP unreachable error (type 3, code 3) packet, you know the port is considered closed. If it responds with an ICMP unreachable error packet with other codes, the packet is considered filtered. If no response is received at all, the port is considered open or filtered. The reason why it might be filtered is that packet filters might be in use that are blocking the communication. Version enumeration could very well help in knowing if packet filters are involved. The problem with using any communication with UDP is that it is unreliable – it has no way of creating an established connection or synchronizing the packets like TCP does. For this reason, UDP scans are typically slow. Because you are waiting for a packet that may never come, nor do you have any real way of telling if the packet even got there in the first place, you might have to send numerous packets then wait to make sure a port is considered open or filtered.	2 3		

	PING SCAN Ping Scans are used to sweep a whole network block or a single target to check to see if the target is alive. It sends an ICMP echo request to the target – if the response is an ICMP reply, then you know the target is alive. However, it is increasingly becoming more common that ICMP pings are being blocked by firewalls and routers that you will likely have to resort to other methods to accurately tell if the target is alive. **STEALTH SCANNING – NULL, FIN, X-MAS** These scan types are known as stealth scanning because you are crafting the packets flags in such a way that you are trying to induce some type of response from the target without actually going through the handshaking process and establishing a connection. The FIN scan sends a packet that would never occur in the real world. It sends a packet with the FIN flag set without first establishing a connection with the target. If a RST (reset) packet is received back from the target due to the way the RFC is written, the port is considered closed. If no packet is received at all, the port is considered open. The X-MAS tree scan gets its name because it "lights up the packet light a Christmas tree." It sets a TCP packet with URG, PUSH, FIN flags and fires it at the target. Again, if no packet is received, the port is considered open and if a RST packet is received, the port is considered closed. NULL scans also send a packet that should never occur in the real world. It does not set any flags on the TCP packet and fires it at the target. Like above, a RST packet response means it's a closed port – no response is considered an open port.	2 3		

VII	Vulnerability scanning of a network needs to be done from both within the network as well as without (from both "sides" of the firewall). **Wireshark**-The very first step in vulnerability assessment is to have a clear picture of what is happening on the network. Wireshark (previously named Ethereal) works in promiscuous mode to capture all traffic of a TCP broadcast domain. Typically, the tester is looking for stray IP addresses, spoofed packets, unnecessary packet drops, and suspicious packet generation from a single IP address. Wireshark gives a broad and clear picture of what is happening on the network. **Nmap**-This is probably the only tool to remain popular for almost a decade. This scanner is capable of crafting packets and performing scans to a granular TCP level, such as SYN scan, ACK scan, etc. It has built-in signature-checking algorithms to guess the OS and version, based on network responses such as a TCP handshake. Nmap is effective enough to detect remote devices, and in most cases correctly identifies firewalls, routers, and their make and model. Network administrators can use Nmap to check which ports are open, and also if those ports can be exploited further in simulated attacks. The output is plain text and verbose; hence, this tool can be scripted to automate routine tasks and to grab evidence for an audit report. **Metasploit**-Once sniffing and scanning is done using the above tools, it's time to go to the OS and application level. Metasploit is a fantastic, powerful open source framework that performs rigorous scans against a set of IP addresses. **OpenVAS**-The Nessus scanner is a famous commercial utility, from which OpenVAS branched out a few years back to remain open	1 2 2 2 2	15	15

	source. Though Metasploit and OpenVAS are very similar, there is still a distinct difference. OpenVAS is split into two major components — a scanner and a manager. A scanner may reside on the target to be scanned and feed vulnerability findings to the manager. The manager collects inputs from multiple scanners and applies its own intelligence to create a report. In the security world, OpenVAS is believed to be very stable and reliable for detecting the latest security loopholes, and for providing reports and inputs to fix them. A built-in Greenbone security assistant provides a GUI dashboard to list all vulnerabilities and the impacted machines on the network. **Aircrack**-The list of network scanners would be incomplete without wireless security scanners. Aircrack is a suite of software utilities that acts as a sniffer, packet crafter and packet decoder. A targeted wireless network is subjected to packet traffic to capture vital details about the underlying encryption. A decryptor is then used to brute-force the captured file, and find out passwords. Aircrack is capable of working on most Linux distros, but the one in BackTrack Linux is highly preferred.	3 3		
VIII a)	The Windows File System (WinFS) is Microsoft's new storage system for its upcoming SQL Server release. Along with serving as a database for structured, semi-structured and unstructured data, WinFS serves as a programming model that lets developers exchange data across applications and organize data in more constructive ways. According to Microsoft, it is not intended to replace NTFS, or the New Technology File System, which is used in Windows NT, but will serve as a link between NTFS and Vista's layer.	2	8	15

	A file system consists of two or three layers. Sometimes the layers are explicitly separated, and sometimes the functions are combined. The *logical file system* is responsible for interaction with the user application. It provides the application program interface (API) for file operations — OPEN, CLOSE, READ, etc., and passes the requested operation to the layer below it for processing. The logical file system "manage[s] open file table entries and per-process file descriptors." This layer provides "file access, directory operations, [and] security and protection." The second optional layer is the *virtual file system*. "This interface allows support for multiple concurrent instances of physical file systems, each of which is called a file system implementation."[8] The third layer is the *physical file system*. This layer is concerned with the physical operation of the storage device (e.g. disk). It processes physical blocks being read or written. It handles buffering and memory management and is responsible for the physical placement of blocks in specific locations on the storage medium. The physical file system interacts with the device drivers or with the channel to drive the storage device.[7]	2 2 2		

VIII b)	Common Internet File System (CIFS) is a file-sharing protocol that provides an open and cross-platform mechanism for requesting network server files and services. CIFS is based on the enhanced version of Microsoft's Server Message Block (SMB) protocol for Internet and intranet file sharing. CIFS - a key file sharing protocol because of its broad feature range - includes enhancements suited for Internet authoring and file sharing. CIFS is typically used in workstation and server OSs and was a native file-sharing protocol in Windows 2000. CIFS is also used in embedded and appliance systems. Recent storage products, like Storage Area Network (SAN) and Network Access Server (NAS), are based on CIFS. Supported CIFS protocol features include: • File access: Supports basic file operations like open, close, read, write and seek. • File and record locking: Supports unlocked file access and features like file and record locking. • Safe caching, read-ahead and write-behind: Facilitates caching, read-ahead and write-behind for safe files and even facilitates these operations for unlocked safe files.	4 3	7	15

IX	1. Aircrack-ng-Aircrack-ng is one of the most popular suites of tools that can be used to monitor, attack, test and crack WiFi networks. It is compatible with Windows, Linux, OS X and is a command line tool. It can be used for attacking and cracking WPA and WEP. The attaching mechanism is simple. It monitors and collects packets, once enough packets are captured; it tries to recover the password.	2	15	15
	2.AirSnort-AirSnort is free WiFi hacking software that captures the packets and tries to decrypt the keys. The monitoring is done in promiscuous mode and records enough packets to reliably decrypt the key. It is a simple tool and supports both Windows and Linux platforms	2		
	3. Kismet-Kismet is a free software written in C++ that can be used to sniff TCP, UDP, DHCP and ARP packets. It is a passive tool and does not interact with the network. It has the ability to find hidden networks and is used in wardriving kind of activities. The captured packets can be exported to WireShark and can be further analyzed. It is available for Linux, Windows and a few other platforms.	3		
	4. Cain and Abel-Cain & Abel is one of the most popular tools that is used for password cracking. The tool is able to sniff the network, crack encrypted passwords using various password cracking techniques and perform cryptanalysis attacks. It can also discover wireless keys by analyzing the wireless protocols	2		
	5.WireShark-WireShark is a very popular tool in networking. It is the network protocol analyzer tool which lets you check different things in your office or home network. You can live capture packets and	2		

	analyze packets to find various things related to network by checking the data at the micro-level. This tool is available for Windows, Linux, OS X, Solaris, FreeBSD and other platforms. WireShark requires good knowledge of network protocols to analyze the data obtained with the tool. If you do not have good knowledge of that, you may not find this tool interesting. So, try only if you are sure about your protocol knowledge. Wireshark does is one of the most popular tool in networking and this is why it was included in this list in higher position. 6.CoWPAtty-CoWPAtty is another nice wireless password cracking tool. It is an automated dictionary attack tool for WPA-PSK to crack the passwords. It runs on Linux OS and offers a less interesting command line interface to work with. It runs on a word-list containing thousands of password to use in the attack. If the password is in the password's word-list, this tool will surely crack the password. But this tool is slow and speed depends on the word list and password's strength. Another reason for slow process is that the hash uses SHA1 with a seed of SSID. It means the same password will have a different SSIM. So, you cannot simply use the rainbow table against all access points. So, the tool uses the password dictionary and generates the hash for each word contained in the dictionary by using the SSID. This tool is simple to use with available commands. 7.Airjack-Airjack is a Wi-Fi 802.11 packet injection tool. It is used to perform DOS attack and MIM attack. This wireless cracking tool is very useful in injecting forged packets and making a network down by denial of service attack. This tool can also be used for a man in the middle attack in the network. This tool is popular and powerful both.	2 2		

X a)	A **web application** or **web app** is a client–server computer program that the client (including the user interface and client-side logic) runs in a web browser. Common web applications include webmail, online retail sales, online banking, and online auction. Web Application Components When we say web application components, we can mean any of the following two: • **UI/UX Web Application Components** – This includes activity logs, dashboards, notifications, settings, statistics, etc. These components have nothing to do with the operation of a web application architecture. Instead, they are part of the interface layout plan of a web app. • **Structural Components** – The two major structural components of a web app are client and server sides. • **Client Component** - The client component is developed in CSS, HTML, and JS. As it exists within the user's web browser, there is no need for operating system or device-related adjustments. The client component is a representation of a web application's functionality that the end-user interacts with. • **Server Component** - The server component can be build using one or a combination of several programming languages and frameworks, including Java, .Net, NodeJS, PHP, Python, and Ruby on Rails. The server component has at least two parts; app logic and database. The former is the main control center of the web application while the latter is where all the persistent data is stored.	2 1.5 1.5 1.5 1.5	8	15

X b)	The associated countermeasures help protect your network from these vulnerabilities as well as from the malicious attacks previously mentioned. When testing your WLAN security, look out for the following weaknesses: • Unencrypted wireless traffic • Weak WEP and WPA pre-shared keys • Crackable Wi-Fi Protected Setup (WPS) PINs • Unauthorized APs • Easily circumvented MAC address controls • Wireless equipment that's physically accessible	1 1 1 1 1 1 1 1	7	15