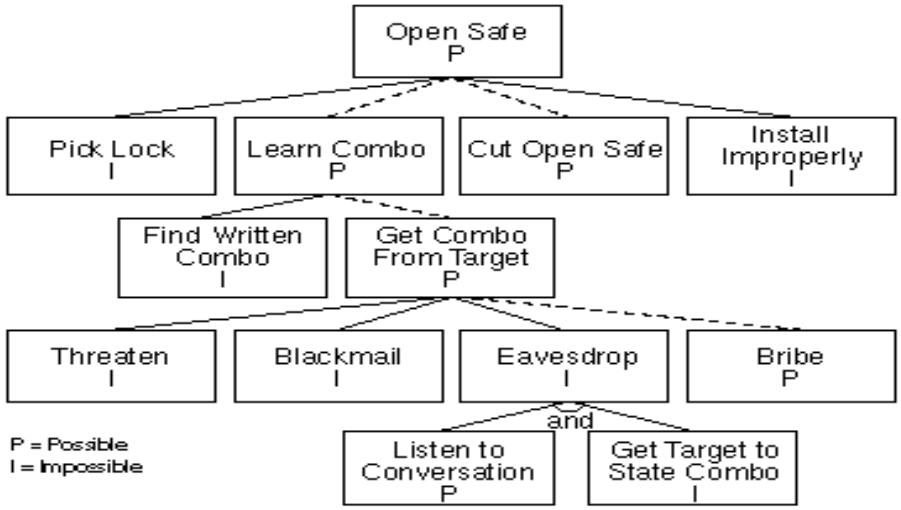
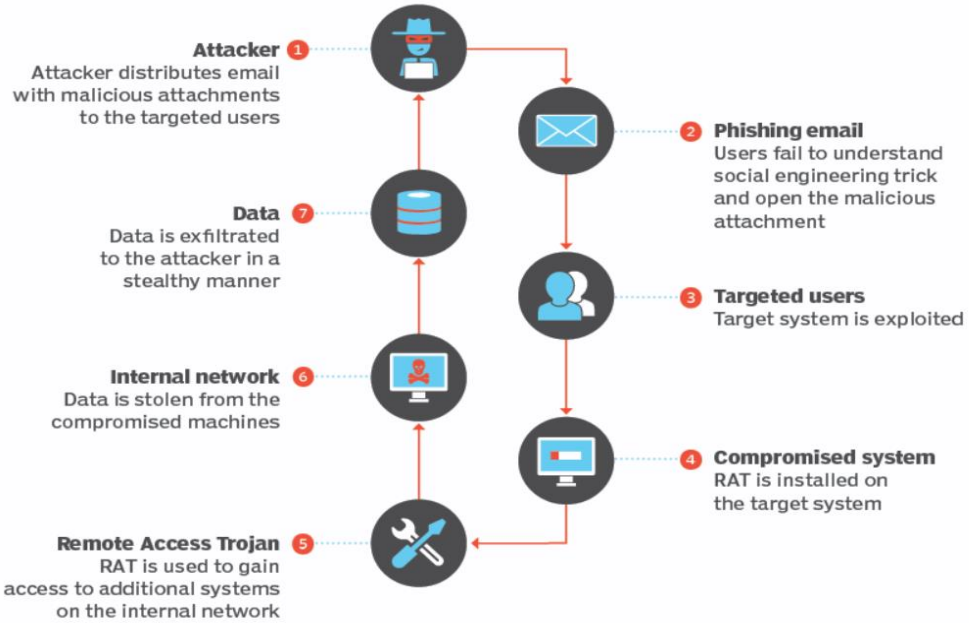
VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering
Fall Semester 2024-25
CAT-1

Programme Name & Branch: B.TECH & CSE **SLOT: F2+TF2**
Course Name & Code: CYBER SECURITY & BCSE410L
Exam Duration: 90 Min. **Maximum Marks: 50**

Q. No.	Answer All the Questions
1.	In a top software company ABC software's, there are several departments available. The finance section requires higher level network traffic filtering device. Propose different solutions which can be implemented for restricting the unwanted traffic accessing the finance department. **Firewalls 5 marks** **Packet Filters** **Proxy Firewall** **Intrusion Detection Systems 5 marks** **Signature-based** **Anomaly-based** **Host-based** **Network-based**
2.	a) You are working as a security expert in a company with more than 10000 employees and 1200 devices connected to the company network. You are responsible for the company's security. Using penetration testing asses the company's network security. (5 Marks) **Steps to a successful penetration test include:** 1. Determine how the attacker is most likely to go about attacking a network or an application 2. Locate areas of weakness in network or application defenses 3. Determine how an attacker could exploit weaknesses 4. Locate assets that could be accessed, altered, or destroyed 5. Determine whether the attack was detected 6. Determine what the attack footprint looks like 7. Make recommendations b) Differentiate TCP full connect scan and Half-Open Scan in computer networks. (5 Marks) TCP Full Connect Scan • Utilizes the three-way handshake • Completed handshake indicates open port • Incomplete handshake indicates closed • Scan gives most accurate picture of port status • Drawback is scan can be easily logged • nmap –sT–v <target IP address> Half Open Scans • Starts like full connect scan • Scan does not complete the final step of the handshake • Benefit is scan has lower chance of being logged • Scan tends to be faster than full connect • nmap –sS –v <target IP address>
3.	Develop a simple attack tree for picking a physical safe in bank. The goal is opening the safe. Note that there are AND nodes and OR nodes. OR nodes are alternatives (the different

	ways to open a safe, for example). AND nodes represent different steps toward achieving the same goal. 
4.	a) You have developed a fake link for the website www.hdfc.com. Explain the steps to perform a targeted spear phishing attack on a group of people. (5 Marks)  b) In June 2017, the NotPetya (also known as ExPetr) malware, believed to have originated in Ukraine, compromised a Ukrainian government website. The attack vector was from users of the site downloading it. The malware erases the contents of victims' hard drives. What type of attack is used in the above scenario? Explain the steps involved in the attack. (5 Marks) Watering hole • So-called watering hole (a.k.a. "water holing") attacks are probably the most economical of online exploits. • Instead of identifying and tracking down individual targets one-by-one, the threat actors first research and identify a vulnerable website frequently sought out by key professionals in the targeted industry or organization. • In the second step, they install an exploit kit that may allow the attackers to target that site's users even more selectively, for instance based on their IP number. Like lions hidden in the savannah grass, they then lay and lurk. • Once their prey shows up at the "water hole", the victim's locally installed browser takes care of the rest. Because the browser is designed to indiscriminately fetch and execute

	code from the web on the local machine, it will silently download the malware from the infected site. • This then allows the attackers to steal the visitor's corporate network credentials and stage a lateral attack within the victim's organization, for instance by following up with a pinpointed phishing emails to employees reporting to the victim.
5.	The Social Engineering Toolkit (SEToolkit) is a robust open-source tool for performing social engineering attacks, penetration testing, and credential harvesting. Explain the features of SEToolkit and explain in steps how you can use SEToolkit for harvesting the credentials. **(i). The Social Engineering Toolkit (SET) has many features, including: (3 Marks)** • Attack vectors: A wide range of pre-configured attack vectors, including phishing emails, spear phishing, website cloning, and credential harvesting • Customization: The ability to customize attacks and generate custom payloads to target specific systems • Phishing attack options: The ability to create convincing emails and malicious websites that look like legitimate services • Credential harvesting: The ability to create fake login screens for popular online services • Website cloning: The ability to create cloned websites that look like legitimate ones • Infectious media generator: The ability to embed malicious code in commonly used file formats, like PDF documents or Office files • Multi-platform: The ability to run on Linux, Unix, and Windows • Integration with third-party modules: The ability to integrate with third-party modules • Configuration menu: The ability to make multiple tweaks from the configuration menu **(ii). Steps using SEToolkit for harvesting the credentials (7 Marks)** How to Perform Credential Harvester Attack Using SEToolkit? **Step 1:** Launch the Social-Engineer Toolkit (SEToolkit) to begin your adventure towards ethical hacking. Simply type the following command on your Kali Linux terminal: setoolkit **Step 2**: Select Social-Engineering Attacks. When the SEToolkit is launched, you will be provided with a menu. Select "1" for "Social-Engineering Attacks." **Step 3**: Choose Website Attack Vectors. Select "2" from the next selection for "Website Attack Vectors." **Step 4:** Select the Credential Harvester Attack. Now, press "3" to activate "Credential Harvester Attack." **Step 5**: Choose Web Templates. You will be shown a list of pre-defined site templates. These themes are based on famous websites. Choose "1" from the list, and the SEToolkit will clone it. **Step 6:** Configure the IP Address for the POST Back. The SEToolkit will prompt you to launch the Apache server and Metasploit listener. Type "1" and click Enter to confirm. **Step 7**: Select a Template for Credential Harvester. The SEToolkit will generate a phishing link for you, choose "3″ from the list, and the SEToolkit will clone the site "Twitter" as shown in the list. **Step 8**: Create a Phishing Link and obtain Credentials. The SEToolkit will create a phishing link for you. This URL should be shared with your targets. When the cloning procedure is finished, you'll get information and progress updates in the terminal below. Prepare to actively watch this information, since it will include critical data regarding the attack's progress and outcomes. **Step 9**: Collect the Credentials. The SEToolkit will record the user's credentials when they click the phishing link and input them. The credentials will be presented on your SEToolkit terminal.