InternsElite

"Rule the world with elite"

InternsElite

PROJECT

Cyber Security program

Name:- Dharmendra Kumar
Program Name:-CYBER SECURITY PROGRAM
Roll no:- 24/CS/J1456
Submission Date:- 21/07/2024

BY:- Dharmendra kumar

1. What is Cyber security? Why it is Essential for Us?
   Cybersecurity involves safeguarding internet-connected systems, encompassing hardware, software, and data, against theft, damage, unauthorized access, and digital attacks. It employs technologies, processes, and practices to protect network devices and electronic information from cyber threats.

2. Explain The various types of Hacking. And Consequences of Hacking in Corporate sector.
   There are five types of hacking.
   - Ethical hacking (White Hat)
   - Malicious hacking (Black Hat)
   - Grey Hat Hacker
   - Hacktivism
   - State Sponsored hacking:
   - Phishing and social Engineering

     - What is Ethical Hacking (White hat)?
       Ethical Hackers are authorized professionals who attempt to penetrate system to identify vulnerabilities. Their goal is improve security by fixing theses weakness before malicious hackers exploit them. It is known as White hat hacker.
     - What is Malicious Hacking (Black hat)?
       Malicious hackers break into systems for prosonal gain ,disruption ,or to cause harm. They exploit vulnerabilities for financial gain, stealing sensitive information, or simply to weak havoc. it is known as black hat hacker.

     - What is Grey Hat hacker?
       Gray hat hackers operate in a middle ground between black hat hackers, who have malicious intent, and ethical hackers. They typically access systems without permission but do not intend harm. When they discover vulnerabilities like zero-day exploits, they often disclose them to the affected parties. However, they might request payment for providing detailed information about the vulnerabilities they uncover.

     - What is Hacktivism?
       Hacktivists hack systems to promote political agendas, social change, or to protest against organizations or governments.

- What is State Sponsored hacking?
  State-sponsored hacking involves government or state-affiliated entities conducting or supporting cyber attacks political military or economic goals. They use advanced methods to infiltrate and compromise targets, including other governments military installations, critical infrastructure, and private sector organizations.

- What is Phishing and Social Engineering?
  Phishing is a cyber attacks where attackers impersonate legitimate entities to deceive individuals into divulging sensitive information such as passwords or financial details through emails. Messages, or websites.

- Social Engineering ia a static where attackers manipulates individuals to gain access to confidential information or systems by exploiting psychological traits trust or ignorance through methods like ipmpersonation, pretexting, or baiting.

Consequences of hacking in the corporate Sector:

1. Financial losses
2. Reputational Damage
3. Legal and Regulatory penalties
4. Operational Disruption
5. Intellectual property Theft
6. Compliances Issues

Consequences of Hacking in the Corporate Sector:

Financial Losses: Hacking incidents can result in direct financial losses through theft of funds, intellectual property, or disruptions in business operations.

Reputational Damage: Data breaches and hacking incidents can erode customer trust and damage the reputation of a company, impacting customer retention and brand value.

Legal and Regulatory Penalties: Organizations may face legal consequences, fines, or lawsuits for failing to protect sensitive information or for violating data protection regulations.

Operational Disruption: Successful hacking attempts can disrupt business operations, leading to downtime, loss of productivity, and additional costs to recover and restore systems.

Intellectual Property Theft: Hackers targeting research and development departments can steal proprietary information, compromising competitive advantage and future innovations.

Compliance Issues: Failure to secure sensitive data can lead to non-compliance with industry regulations and standards, resulting in further penalties and loss of business opportunities

3. Explain the below terms.
   a. Scanning
      Scanning involves a detailed exploration of a system to identify valuable data and services within a specified IP address range. By pinpointing potential entry points, scanning techniques help ethical hackers safeguard organizations against potential attacks.

   b. Footprinting
      Footprinting involves gathering extensive information about a targeted network, victim, or system, which aids hackers in planning intrusions. This technique also assesses the security posture of the target. Footprinting can be either passive, where data is collected covertly without the owner's knowledge (also known as pseudonymous footprinting), or active, where data is obtained through intentional release or direct contact with the owner.
   c. Reconnaissance
      Reconnaissance is the covert practice of discovering and gathering information about a system. It is frequently employed in ethical hacking or penetration testing scenarios.
   d. Vulnerability
      A weakness or flaw in a system or software that could be exploited by a threat actor to gain unauthorized access or cause harm.

4. What is Proxy Server & V.P.N. With Detailed Explanation.
   A proxy server is a system or router that provides a gateway between users and the internet. It helps prevent cyber attackers from entring a private network.
   - Access to blocked content.
   - Firewall System
   - Filter Content
   - Speed are stabilized

   What is VPN?

VPN full form is Virtual private Network.

Security Technology that allows secure encrypted connections over public networks.

Useful for remote workers or organizations with multiple locations.

Enable Secure Communication between devices network even when Separated by large distances.

5. What are the Different types of Malware. Explain it with Detail.

There are various type of malware .

- Viruses
- Worms
- Trojans
- Ransomware
- Spyware
- Adware
- Keyloggers
- Bot and botnets
  - What is viruses?
    A Computer Virus is a form of computer program that replicates itself on execution they after different computer program by attaching its own code.

  - What is Worms?
    A worm is a type of malware that can self-replicate and spread independently across computer networks, exploiting vulnerabilities in operating systems or network protocols to infect other devices without requiring user interaction or a host file.

  - What is Trojans horse?
    Trojans looks like certified software but harms the system on installation. They create a backdoor in the system and through this the hacker steals our information.

  - What is Ransomware?
    Ransomware is a type of malicious Software malware that threatens to publish or block access to data or a computer systems, usually by encrypting it. Until the victim pays a ransom free to the attacker.

  - What is Spyware?
    Spyware malware is a type of malicious software designed to covertly gather sensitive information from a computer or device without the user's knowledge or consent. It monitors activities such as web browsing habits,

keystrokes, and personal information, which can be used for identity theft, financial fraud, or espionage purposes.

- What is Adware?
  Adware, short for 'advertising-supported software,' presents undesired and occasionally harmful advertisements on computer screens or mobile devices. It can redirect search results to advertising sites and gather user data for sale to advertisers without consent. While not all adware is malicious—some is legitimate and safe—users can influence its occurrence and the types of downloads permitted by adjusting pop-up controls and preferences in their web browsers or employing ad-blocking software.

- What is keyloggers?
  A keylogger is a type of spyware that monitors user activity. Keyloggers can be used for legitimate purposes – for example, families who use them to keep track of their children's online activity or organizations which use them to monitor employee activity. However, when installed for malicious purposes, keyloggers can be used to steal password data, banking information, and other sensitive information. Keyloggers can be inserted into a system through phishing, social engineering, or malicious downloads

- What is Bots and botnets?
  A bot is a computer that has been infected with malware so it can be controlled remotely by a hacker. The bot – sometimes called a zombie computer – can then be used to launch more attacks or become part of a collection of bots called a botnet. Botnets can include millions of devices as they spread undetected. Botnets help hackers with numerous malicious activities, including DDoS attacks, sending spam and phishing messages, and spreading other types of malware.

6. What is sniffing and their types?
   - What is Sniffing?

   Sniffing is a process of monitoring and capturing all data packets passing through given network. Sniffers are used by network/system administrator to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc. Sniffers can be hardware or software installed in the system. By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyze all of the network traffic.

   - There are two types:

- Active Sniffing:

Sniffing in the switch is active sniffing. A switch is a point to point network device. The switch regulates the flow of data between its ports by actively monitoring the MAC address on each port, which helps it pass data only to its intended target. In order to capture the traffic between target sniffers has to actively inject traffic into the LAN to enable sniffing of the traffic. This can be done in various ways.

- Passive Sniffing:

  This is the process of sniffing through the hub. Any traffic that is passing through the non-switched or unbridged network segment can be seen by all machines on that segment. Sniffers operate at the data link layer of the network. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. This is called passive since sniffers placed by the attackers passively wait for the data to be sent and capture them.

7. What is Dos & DDoS Attack?

   It is Stand for Denial of service & Distributed Denial of service .

   DDoS Attacks are getting more extreme with hackers getting easy access to botnet terms and compromised devices.
   Sending multiple requests from to a web-resources or machine.
   A hacker must create a network of zombie bots that can be used to attack the targeted victim when called upon , using malware infusion.

8. Explain the Password Attacks.

   Identifying the password of unauthorized device or network resources.
   Can be used to gain illegal access to resources .
   Tools used can be programs running locally or online web-based attacks.
   Usually involves breaking hash algorithm to retrieve stored password in plaintext.

- There are mainly four techniques of password Cracking
  - Phishing
  - Social Engineering
  - Dictionary Attack
  - Rainbow table

- Phishing

  A Phishing email directs the unwary reader to a counterfeit log-in-page linked with whatever services the hacker want to access, which later steals the credentials.

- Social Engineering

Social Engineering Influences the victim to get personal information such as bank account numbers or passwords

- Dictionary Attack
  Password dictionaries cover many themes and mixtures of topics as politics, movies and music groups. User's failures to create a strong password is why this approach efficiently cracks password.

- Rainbow Attacks
  A rainbow table is a set of pre-computed hashes of probable password combinations.

9. Explain about Kali Linux, Metasploit framework and it's usage.
   Kali Linux is a specialized Linux distribution for digital forensics and penetration testing, equipped with tools for assessing computer system and network security. It's used by cybersecurity professionals and ethical hackers to test vulnerabilities and conduct security assessments.

   Metasploit is an open-source framework used to develop, test, and execute exploits against remote targets. It's a platform where security researchers, penetration testers, and hackers can create and validate exploit code, automating different stages of penetration testing.

There are mainly uses of Metasploit includes:

- Reconnaissance: Gathering pertinent information about the target system or network.
- Vulnerability Scanning: Identifying potential weaknesses within target systems.
- Exploitation: Employing Metasploit modules to leverage identified vulnerabilities.
- Post-Exploitation: After gaining access, conducting additional actions such as privilege escalation or data retrieval.
- Reporting: Documenting findings and suggesting improvements to enhance security measures.

10. What is TOR Network and it's use. Explain about the Network and their types.

The TOR Network, or The Onion Router, enables anonymous internet browsing by encrypting and routing traffic through volunteer-operated servers called nodes. This hides both the origin and destination of data, bolstering user privacy and security.

Uses of the TOR Network:

- **Anonymous Browsing:** Users can access websites without revealing their IP addresses or physical locations.
- **Circumventing Censorship:** TOR helps bypass internet censorship, granting access to restricted content.

Whistleblowing: It provides a secure, anonymous platform for whistleblowers and journalists to communicate.

- **Avoiding Tracking:** TOR prevents tracking by advertisers and surveillance agencies.
- **Privacy:** Enhances online privacy by masking users' internet activities from ISPs and other entities.

Types of TOR Network Nodes:

- **Entry Nodes (Guard Nodes):** First nodes that receive encrypted traffic, unaware of the data's final destination.
- **Middle Nodes:** Receive traffic from entry nodes and pass it along without knowing its source or final destination.
- **Exit Nodes:** Final connection point that decrypts data before sending it to the destination server, aware of the destination but not the source of unencrypted data.