VULNERABILITY SCANNING

Discovery of weaknesses

Pretexting involves the use of telephone calls to either obtain information or convince the user to unintentionally perform a malicious action. This is one of the most commonly used forms of social engineering.

If not properly discarded, sensitive information may be discovered by hackers in waste receptacles and dumpsters.

- Printed emails, expense reports, credit card receipts, travel information, etc.
- Network or application diagrams, device inventory with IP addressing, etc.
- Contact lists, notebooks, binders, or other work papers containing sensitive information

Hackers may rely on a physical approach to complement their technical attacks.

- Piggy backing: A hacker’s method of entering a facility with a group of employees or maintenance workers
- Identifying unsecure areas: Hackers search for loading docks, maintenance entrances, designated smoking areas, or other locations that may not be well secured.

Phishing is the process of crafting emails that appear to be from a trusted source and typically invite the recipient to either supply confidential information or click on a malicious link or attachment.

Penetration testing is a proactive approach to discovering exploitable vulnerabilities in computer systems, networks, and web applications. Manual penetration testing goes beyond automated scanning and into complex security exploitation.

Gaining a thorough understanding of vulnerabilities and risks enables the remediation of issues before an attacker is able to interrupt business operations.

Wireless capabilities can provide opportunities for attackers to infiltrate an organization’s secured environment—regardless of certain access and physical security controls. Wireless pen testing provides a map of access points in the wireless landscape. After gaining access to the wireless network, penetration testers attempt to exploit weaknesses in the network to gain access to privileged areas and demonstrate the potential impact of a wireless network breach.

Penetration testers perform assessments, interpret the results, and provide reports for the tested organization.

Reports should function as a guide; providing valuable information that prompts action.