CompTIA Security+

Personal Notes Exam Objectives

Author:
Scott *Skrobel*

May 19, 2024

Table of Contents

1 Threats, Attacks and Vulnerabilities

1.1 Compare and contrast types of attacks

Phishing : Social engineering tactic to acquire personal information from a fake email with a clickable link.
Smishing : (SMS phishing) The use of deceptive text messages into divulging sensitive information.
Vishing : (Voice Phishing) Impersonates a trusted entity, such as a bank to trick into giving information.
Spam : Unsolicited inappropriate messages sent with the purpose of spreading malware, advertising, phishing.
Spear phishing : Targeted type of phishing attack to make the scam convincing, often with insider information.
Dumpster diving : Searching through an organization's or individual's trash to find sensitive information.
Shoulder surfing : Observing a victim's screen or keyboard to obtain sensitive information.
Pharming : Manipulating the DNS system to resolve fake domain names, to lead them to a fake website.
Tailgating : Physical security breach by following authorized person to get access to secure areas.
Eliciting information : Psychological tactics to encourage individuals to share their knowledge willingly.
Whaling : Spear phishing for high-profile executives in an organization.
Prepending : Organizing, manipulating, and structuring data in various applications.
Identity fraud : An individual wrongfully obtains and uses someone else's personal data in a deceptive manner.
Invoice scams : Impersonation of a legit business to deceive individuals into paying fraudulent invoices.
Credential harvesting : Tricking someone into disclosing login credentials to access sensitive info.
Reconnaissance : Initial phase to gather intelligence via passive and active techniques.
Hoax : Fabrication intended to deceive or trick individuals into believing false information or events.
Impersonation : Masquerading as a legitimate user or entity to gain unauthorized access to information.
Watering hole attack : Infecting a commonly visited website of a targeted specific group.
Typosquatting : URL hijacking or domain squatting of fake domains which resemble a legit website.
Pretexting : Fabricated scenario involving direct interaction to obtain sensitive information.
Influence campaigns : Coordinated effort to shape public opinion, influence perceptions, and manipulate.
    Hybrid warfare: Blends conventional warfare tactics with unconventional method
Principles (reasons for effectiveness)

- **Authority**: The actor acts as an individual of authority
- **Intimidation**: Frightening or threatening the victim.
- **Consensus**: Convince based on what's normally expected.
- **Scarcity**: Limited resources and time to act.
- **Familiarity**: The victim is well known.
- **Trust**: Gain their confidence, be their friend.
- **Urgency**: Limited time to act, rush the victim.

1.2 Given a scenario, analyze indicators of compromise

Malware

Ransomware : Denies access to a computer system or data until a ransom is paid.
Trojan : A form of malware that pretends to be a harmless application.
Worm : A self-contained infection that can spread itself through networks, emails, and messages.
PUP's : Potentially Unwanted Programs software applications that may exhibit undesirable characteristics.
Memory-resident malware : Operates primarily in a computer's volatile memory (RAM) rather than with files
Command and control : (C2) Centralized server used by attackers to manager compromised devices.
Bots : AI inside an infected machine performs specific actions as a part of a larger entity known as a botnet.
Cryptomalware : A malicious program that encrypts programs and files on the computer to extort money.
Logic Bomb : A malicious program that lies dormant until a specific date or event occurs.
Spyware : Software that installs itself to spy and sends stolen info back to the host machine.
Keyloggers : A malicious program that saves all of the keystrokes of the infected machine.
Remote Access Trojan : (RAT) A remotely operated Trojan.
Rootkit : A backdoor program that allows full remote access to a system.
Backdoor : Allows for full access to a system remotely.

Password Attacks

Sprying a

Physical attacks

Sprying a

2 Architecture and Design