Armaan Shamsaasef

Impersonation

Impersonation - SY0-701 - 2.2

Definition: A social engineering attack where a threat actor pretends to be someone else to gain unauthorized access, information, or privileges.

1. Pretexting

- Description: Creating a fabricated scenario (or "pretext") to engage a target and extract information.
- How it Works: The attacker invents a false identity and situation that justifies why they need the information. It often involves building a false sense of trust over a short conversation.
- Example:
    - An attacker calls an employee, pretending to be from the IT Help Desk. They say, "We're running a security test on the VPN and need you to read the one-time password from your authenticator app to verify it's working."
    - The pretext (testing the VPN) creates a plausible reason for the request.

2. Identity Fraud

- Description: The actual theft and use of someone's personal or financial information for deceptive gain.
- How it Works: The attacker uses real, stolen details (e.g., name, Social Security Number, credit card) to impersonate the victim for financial transactions or to create accounts.
- Example: Using a stolen credit card number to make an online purchase. The attacker is fraudulently using the victim's financial identity.

3. Impersonation (Physical)

- Description: An attacker physically poses as someone who should have access to a restricted area.
- Common Tactics:
    - Dressing the Part: Wearing a uniform (e.g., delivery person, technician) to appear legitimate.
    - Tailgating/Piggybacking: Following an authorized person through a secure door without using their own credentials.
    - Forged Credentials: Using a fake ID badge.
- Example: An attacker, dressed as a cable technician with a tool belt and clipboard, waits outside a secure office door. An employee holds the door open for them, allowing them to bypass physical access controls.

Key Differences & Relationships

- Pretexting vs. Identity Fraud:
    - Pretexting is about creating a false story and role. The attacker might use a fake name and department.
    - Identity Fraud is about using real, stolen details of a specific person.
    - They can be combined: An attacker might use pretexting to steal information and then use that information for identity fraud.
- Digital vs. Physical Impersonation:
    - The core principle is the same: "I am someone I am not."
    - It can happen digitally (pretexting over the phone, phishing emails) or physically (tailgating, wearing a uniform).

Summary

- Impersonation is a broad category of attacks based on deception.
- Pretexting is building a fabricated scenario to manipulate a target into giving up information.
- Identity Fraud is the criminal use of stolen personal information.
- Physical Impersonation involves bypassing physical security by appearing to be an authorized person.