Armaan Shamsaasef

Deception and Disruption

Notes: Deception and Disruption (SY0-701 - 1.2)

Core Concept: These are proactive security techniques designed to confuse, delay, and misdirect attackers, making it more difficult and time-consuming for them to succeed. They move beyond pure defense and aim to actively interfere with an attacker's process.

Key Techniques

1. Deception

The goal is to trick attackers into wasting time and resources on fake assets, revealing their presence and methods in the process.

- Honeypots:
    - Definition: A decoy system designed to attract and lure attackers.
    - Purpose: To study an attacker's techniques, gather intelligence on their tools, and distract them from real production systems.
    - Example: Setting up a server that looks like a company's database server but contains only fake, non-sensitive data. When an attacker interacts with it, security teams are alerted and can monitor their every move.
- Honeynets:
    - Definition: An entire decoy network, often containing multiple honeypots, designed to simulate a real production environment.
    - Purpose: To observe how an attacker moves laterally through a network and interacts with different systems.
- Honeyfiles:
    - Definition: Fake files designed to attract an attacker's attention.
    - Purpose: To act as "canaries in a coal mine." When a honeyfile is accessed, it triggers an immediate alert.
    - Example: A file named "passwords.xlsx" or "Q4_earnings_report.pdf" placed on a server. Any access to this file is considered malicious.

- DNS Sinkhole:
    - Definition: A DNS server that provides false or controlled results for specific domain names, redirecting malicious traffic away from its intended target.
    - Purpose:
        1. Disruption: To prevent malware from communicating with its command-and-control (C&C) server by redirecting it to a safe, controlled server.
        2. Analysis: To track and identify infected machines on a network that are attempting to call home.

2. Disruption

The goal is to actively block or hinder an attacker's communication and control over compromised systems.

- Port Security (on Network Switches):
    - Definition: A set of features that controls which devices can connect to a physical switch port.
    - Common Methods:
        - MAC Address Filtering: Only allowing a specific, pre-configured MAC address to use a port.
        - Violation Modes: If an unauthorized device connects, the switch port can be shut down (disabled), put in a restricted mode, or simply block traffic from the new MAC address.
    - Purpose: To prevent an attacker from simply plugging a rogue device (like a laptop) into a network jack and gaining network access.

Key Takeaway

Deception and disruption techniques shift the balance of power from the attacker to the defender. Instead of just building walls, these strategies involve laying traps (deception) and actively interfering with an attacker's operational capabilities (disruption). This increases the attacker's cost and time, giving defenders a greater chance to detect and respond to an incident.