COURSE: SECURITY+ SY0-401

MODULE 3: THREATS AND VULNERABILITIES

Overview

- Summarize social engineering attacks and the associated effectiveness with each attack
- Explain types of wireless attacks
- Explain types of application attacks
- Analyze a scenario and select the appropriate type of mitigation and deterrent techniques

Social Engineering

One area of security planning that is often considered the most difficult to adequately secure is the legitimate user. Social engineering is a process by which an attacker might extract useful information from users who are often just tricked into helping the attacker. It is extremely successful because it relies on human emotions.

Social Engineering

Dumpster Diving: *As humans, we naturally seek the path of least resistance. Instead of shredding documents or walking them to the recycle bin, they are often thrown in the wastebasket. Equipment sometimes is put in the garbage because city laws do not require special disposal.*

Tailgating: *Tailgating is a simple yet effective form of social engineering. It involves piggybacking or following closely behind someone who has authorized physical access within an environment. Tailgating often involves giving off the appearance of being with or part of an authorized group or capitalizing upon people's desire to be polite.*

Social Engineering

- Principles (reasons for effectiveness)
- Authority
- Intimidation
- Consensus/Social proof
- Scarcity
- Urgency
- Familiarity/liking
- Trust

Wireless Attacks

Rogue Access Points: Rogue access points refers to situations in which an unauthorized wireless access point has been set up. In organizations, well-meaning insiders might use rouge access points with the best of intentions.

War Driving: A popular pastime involves driving around with a laptop system configured to listen for open 802.1x APs announcing their SSID broadcasts, which is known as *war driving*. Many websites provide central repositories for identified networks to be collected, graphed, and even generated against city maps for the convenience of others looking for open access links to the Internet.

Wireless Attacks

Bluejacking/ Bluesnarfing

Mobile devices equipped for Bluetooth short-range wireless connectivity, such as laptops, cell phones, and PDAs, are subject to receiving text and message broadcast spam sent from a nearby Bluetooth-enabled transmitting device in an attack referred to as *bluejacking*. Although typically benign, attackers can use this form of attack to generate messages that appear to be from the device itself, leading users to follow obvious prompts and establish an open

Bluetooth connection to the attacker's device. Once paired with the attacker's device, the user's data becomes available for unauthorized access, modification, or deletion, which is a more aggressive attack referred to as *bluesnarfing*.

Wireless Attacks

IV Attack: An *initialization vector* (*IV*) attack is best exemplified by the cracking of Wireless Equivalent Privacy (WEP) encryption. WEP was the original algorithm used to protect wireless networks. An IV is an input to a cryptographic algorithm, which is essentially a random number. Ideally, an IV should be unique and unpredictable. An IV attack can occur when the IV is too short, predictable, or not unique.

War chalking

Packet sniffing

Near field communication

Replay attacks

WEP/WPA attacks

WPS attacks

Application Attacks

Browser Threats

The evolution of web network applications, Web 2.0 interactive interfaces, and other browser-based secure and anonymous-access resources available via the HTTP and HTTPS protocols presents an “anytime/anywhere” approach to enterprise network resource availability. As more applications are migrated into the browser, attackers have an increasingly large attack surface area for interception and interaction with user input and for directed attacks against web-based resources. The global nature of the Internet enables attackers to place web-based traps in countries of convenience, where law enforcement efforts are complicated by international legal variance.

Application Attacks

Buffer Overflow: *Like desktop- and system-based applications, many web browser applications offer an attacker a mechanism for providing input in the form of a crafted uniform resource locator (URL) value.*

Session Hijacking: *Because browsers access resources on a remote server using a predefined port (80 for HTTP or 443 for HTTPS), browser traffic is easily identifiable by an attacker who may elect to hijack legitimate user credentials and session data for unauthorized access to secured resources.*

Application Attacks

Code Injections

Cross-Site scripting (XSS): *By placing malicious client-side script on a website, an attacker can cause an unknowing browser user to conduct unauthorized access activities, expose confidential data, and provide logging of successful attacks back to the attacker without the user being aware of her participation.*

SQL injection: Inserts malicious code into strings, which are later passed to a database server. The SQL server then parses and executes this code.

Application Attacks

Code Injections

LDAP Injection: Some websites perform LDAP queries based upon data provided by the end user. LDAP injection involves changing the LDAP input so that the web app runs with escalated privileges.

XML injection: Uses malicious code to compromise XML applications, typically web services. XML injection attempts to insert malicious content into the structure of an XML message to alter the logic of the targeted application.

OWASP Top 10

A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

https://www.owasp.org/index.php/Top_10_2013-Top_10

Mitigation Strategies

- Monitoring system logs
- Event logs
- Audit logs
- Security logs
- Access logs
- Hardening
- Disabling unnecessary services
- Protecting management interfaces and applications
- Password protection
- Disabling unnecessary accounts

Mitigation Strategies

- Network security
  - MAC limiting and filtering
  - 802.1x
  - Disabling unused interfaces and unused application service ports
  - Rogue machine detection
- Security posture
  - Initial baseline configuration
  - Continuous security monitoring
  - Remediation

Mitigation Strategies

- Reporting
  - Alarms
  - Alerts
  - Trends
- Detection controls vs. prevention controls
  - IDS vs. IPS
  - Camera vs. guard

THANK YOU