Penetration Testing

Was ist Pentesting?

- Aufdecken von Sicherheitslücken
- Mögliche Angriffszenarien durchgehen
- Sicherheitslücken aufzeigen
- Dokumentation **aller** durchgeführten Schritte und Ergebnisse, jedes kleine bisschen
  - Fließt in die Präsentation ein
- "Ethical hacking"
- Eindringen mit Zustimmung
- Simulation eines Cyber-Angriffs ohne Schaden anzurichten
- Nutzung von Werkzeugen eines Angreifers
- Standards: OWASP Testing Guide, OSSTMM3
- Kunde möchte am Ende die Dokumentation der Ergebnisse: Was wurde getestet? Wie wurde es getestet? Was ist das Ergebnis?

Definition

- Verbesserung der IT-Sicherheit eines Systems
- Erkennung Schwachstellen
- "Nachweis" der Sicherheit durch eine 3. Partei (gelegentlich)
- Verbesserung interner Sicherheitsprozesse

Rechtliches

- Straftat Computerbetrug §263 StGB
- Ausspähen von Daten §202a StGB
- Abfangen von Daten §202b StGB
- Vorbereiten des Ausspähens oder Abfangens (Hacker-Paragraph) §202c StGB
- Datenhehlerei §202d StGB

Beauftragung

- Beauftragungsdatum hier: 10.01.2025
- Klärung Ziel, Zeitplan und Aufwand
- Festlegung des Ablaufs (Projektplan)
- Vertraulichkeitsvereinbarung (NDA)
- Rollen und Verantwortlichkeiten auf Tester und Kundenseite
- Umfang und Arbeitsaufwand

- Kommerzielle Aspekte: Kosten, Zahlungsmodalitäten, Haftung/Haftungsausschluss (im Projekt hier nicht)

Briefing

- Definition zu testende Systeme u. Netzwerkadressen (Scope)
- Klärung, in welchem Maß Zugang bestehen:
  - Internet?
  - Aus authentisierter Nutzer einer Anwendung?
  - Physikalischer Zugriff auf Netze im Haus?
- Sollen Maßnahmen mit zerstörerischen Auswirkungen durchgeführt werden?
- Was sind Kriterien und Vorgehen für Abbruch des Tests?
- DoS, DDoS eingeschlossen?
- Ausschluss bestimmter Techniken (z.B. Social Engineering, Gold Tickets, ...)
- Keine personenbezogenen Daten und Passwörter in die Dokumentation schreiben

Black Box Test

- Keine Informationen über das zu testende System
  - Strukturen, Schwachstellen, ... müssen von außen erkannt werden
- Vorteile
  - Perspektive eines externen Angreifers
  - Realistische Angrifssimulation
- Nachteile
  - Hoher Zeitaufwand durch aufwändige Analyse

White Box Test

- Vollständiger Zugriff auf Dokumentation, Quellcode, ... (Position eines gut informierten Insiders)
- Vorteile
  - Gezieltes Angreifen von Komponenten
  - Verständnis für den Gesamtnetzzusammenhang
- ...

Gray Box Test

- Zugriff zu ausgewählter Dokumentation bestimmter Systemkomponenten
- Vorteil
  - Gezielt Komponenten angreifen
  - Angriffswege können vorab identifiziert und geplant werden
  - Test kann auch bei unvollständiger Dokumentation durchgeführt werden
- Nachteil
  - Auftraggeber muss die bereitgestellte Dokumentation auswählen

Umfang des Pentests

- Uneingeschränkt
  - Alle Systeme können angegriffen werden
  - Ausnahmen können definiert werden für besonders kritische Systeme
- Eingeschränkt (meistens)
  - Nur bestimmte Systeme und Netze angreifen z.B. Alle Systeme in der DMZ
- Fokussiert (häufig)
  - Es wird nur eine bestimmte Anwendung oder Komponente getestet
  - z.B. Test einer neuen Webanwendung vor der Inbetriebnahme

Pflichten Auftraggeber und Auftragnehmer

- Auftraggeber
  - Bereitstellung Briefing-Informationen
  - Information von potentiell betroffenen Dritten (Cloud/Hoster)
  - Vermeidung unnötiger Schäden durch den Test
- Auftragnehmer
  - Geheimhaltung der erhaltenen Informationen und Schwachstellen
  - Dokumentation Vorgehensweise und Ergebnisse (Nachvollziehbarkeit)
  - Allgemeine Sorgfaltspflicht zur Vermeidung unnötiger Schäden

"Permission to attack"

- Angriffe gegen IT-Systeme sind normalerweise strafbar (§202a StGB)
- Bestätigung des Auftrags zum Angriff sichert den Pentester rechtlich ab
- Dokumentation sollte schriftlich erfolgen als sog. "permission to attack"

Durchführung

- Start-/Ende-Meldungen (z.B. Security Monitoring Team + Incident Management)
- Kontaktdaten für ggfs. Abbruch
- 5 Phasen
  - Vorbereitung
    - Tools installieren (Kali Linux)
    - WLAN aufsetzen in dem man die Geräte einbringen kann, ...
  - Reconnaissance
    - Überblick über die Zielsysteme bekommen
    - Analyse des Angriffsziels mit dem Ziel möglichst umfassende Informationen zu sammeln
    - Identifikation der vorhandenen Systeme die Teil des Angriffsziels sind
    - Nutzung öffentlicher Informationsquellen ("OSINT") im Internet
    - Verbindungsaufbau zu den Zielsystemen (Websiten-Aufrufe, Ports, Scans, ...)
  - Auswertung
    - Analyse erkannter Systeme und Schwachstellen

        - Auswahl von Angriffszielen, Dokumentation der Auswahl für den Abschlussbericht
        - Recherche von Angriffsmustern und Schadcode/Exploits
    - Angriffsversuche
        - Erfolgreicher Einbruch in die Zielsysteme
        - Aktive Einbruchsversuche mit ausgewählten Werkzeugen
        - Prüfung, in wie weit die Schwachstellen ausnutzbar sind
        - Prüfung, welche Konsequenzen die Ausnutzung der Schwachstellen für die Zielsysteme hat
        - Je nach Beauftragung kann auf die Durchführung des Angriffs verzichtet werden (Doku der Möglichkeit reicht dann aus)
    - Abschließende Analyse
        - Aufstellung der erkannten und angegriffenen Systeme
        - Darstellung identifizierter Schwachstellen
        - Ableitung damit verbundener Risiken
        - Darstellung nach (nachvollziehbare) Dokumentation erfolgreicher Angriffsversuche
        - Empfehlungen von Maßnahmen zur Behebung der Schwachstellen

Abschlussbericht

- Erklären was das Ziel ist
- Was sind die Briefing Informationen?
- Vorstellung der Ergebnisse des Pentests beim Kunden
- Vorgehen und eingesetzte Werkzeuge
- Identifizierte Systeme und Schwachstellen
- Bewertung der Schwachstellen
- Handlungsempfehlungen und Gegenmaßnahmen
- In Präsi: Kein Protokoll erzählen "das haben wir gemacht, und das ..." sondern eine gute Story erzählen

Tools - Kali Linux

- Optimiert für die Durchführung von Pentests
- Basiert auf Debian
- Läuft auch auf Windows WSL

Ausgewählte Tools:

- Aircrack-ng (WLAN Credentials)
- Burp suite (Application Security Scanner)
    - Technisch gesehen Proxy Server
    - MITM Angriff gegen TLS
    - Bildungsregeln für Token und Cookies
    - Manipulation und Veränderung von Anfragen
    - Einfügen von Strings, SQL-Injection

- OWAP-ZAP (Web Application Scanner)
  - Scan nach Standardproblemen (x-site-scripting)
- Nmap, Wireshark (Netzwerk-Analyse)
- Nessus (Schwachstellenscanner)
  - OpenVAS - Fork von der letzten OS-Nessus-Version aber OpenSource
- spiderfoot - Crawlen von Websites und extrahieren von interessanten Informationen
- ARP cache poisoning
  - Manipulation Auflöstung von ARP-Adressen auf IP-Adressen
  - Daten kommen auf Gerät des Angreifers an statt auf dem Standard-Gateway
  - Angreifer kann in geswitchten Netzen Daten mitlesen
  - Tool: arpspoof
  - Schutz davor: TLS
- fuzzer - z.B. API-Pentest Tool (viele Fehlereingaben senden)

Revision #5
Created 10 January 2025 12:11:33 by Max
Updated 10 January 2025 14:53:34 by Max