PENETRAČNÝ TEST BEZDRÔTOVÝCH SIETÍ (WIFI)

Mnoho firiem používa bezdrôtové (Wifi) siete, ktoré bývajú častým cieľom útokov nakoľko úspešný zrealizovaný útok na WiFi zariadenia môže znamenať priamy prístup do vnútornej siete.

Zatiaľ čo tieto siete prinášajú mnohé výhody, nechránená alebo zle nakonfigurovaná sieť môže viesť k neoprávnenému použitiu a možným bezpečnostným rizikám, ako napríklad získanie citlivých informácií.

VŠEOBECNÝ PREHĽAD SLUŽBY

Cieľom penetračného testu/auditu bezdrôtových sietí (Wifi) je zhodnotenie bezpečnosti Vašej bezdrôtovej siete, ktorá môže byť ohrozená v dôsledku nesprávnej konfigurácie, alebo implementácie.

Výsledkom penetračného testu je report, ktorý obsahuje nájdené zraniteľnosti, pridelené riziká a odporúčania ako ich odstrániť.

Penetračný test môže byt vykonaný pomocou metódy BLACK BOX (žiadne informácie o testovacom prostredí), GREY BOX (čiastočné informácie o testovacom prostredí), alebo WHITE BOX (úplne informácie o testovanom prostredí, vrátane konfiguračných súborov zariadení/popis nastavení).

Cena penetračného testu záleží od hĺbky testov, veľkosti a komplexnosti testovanej infraštruktúry. Táto cena je určená po konzultácii so zákazníkom, v ktorom sa určí rozsah, typ testov a ďalšie požiadavky od zákazníka.

DETAILNÝ PREHĽAD SLUŽBY A METODOLÓGIA

Na penetračný test používame metodológie ako Open Source Security Testing Methodology Manual (OSSTMM), NIST800-115, Information Systems Security Assessment Framework (ISSAF), ale hlavne našu interne vyvinutú metodológiu, ktorá simuluje útok tak, ako by postupoval skutočný útočník. Naši experti sú držiteľmi certifikácie Offensive Security Wireless Professional (OSWP).

Stručný prehľad preberaných tém:

- Identifikácia všetkých wifi prístupových bodov v celom objekte
  - Schované SSID
  - Rogue wifi access points
  - Neoprávnené/neschválené bezdrôtové siete s prístupom do podnikovej siete
- WEP/WPA/WPA2 Preshared Key brute force attacks
- Útok na WPA/WPA2 enterprise
- Útok na Wi-Fi Protected Setup (WPS)
- Identifikácia slabej autentifikácie (napríklad MAC filtering)

- Identifikácia a exploitácia zraniteľných služieb (HTTP, SNMP, Telnet, SSH, ...) wifi routerov
- Útok typu "Man in the middle" (MitM) na koncových používateľov pripojených vo wifi sieti
- Obídenie captive portálu
- Pokus o prekonanie segmentácie wifi siete guest a corporate
- Analýza sieťového toku
- Vytvorenie rogue wifi access point/Evil twin attack
- Exfiltrácia dát do internetu pomocou wifi siete (prekonanie firewallu)
- Zhodnotenie konfigurácie wifi routerov
- KRACK útok
- Zhodnotenie fyzického prístupu k wifi routerom