Analiza vulnerabilităţilor reteţelor WLAN pe baza atacului asupra acestora

DUMITRU ALEXANDRU-FLORENTIN

DUMITRU ALEXANDRU-FLORENTIN

Cu o experienţă de peste 5 ani în domeniul bancar din care în ultimii 3 ani am administrat infrastructura IT, în echipele de Helpdesk IT şi Admin IT, îmi place să afirm despre mine că sunt o persoană atrasă de inovaţie preferând proiectele îndrăzneţe dar ancorate în realitate în detrimentul task-urilor repetitive.

- **Masterand în anul 2 în cadrul Universităţii "Titu Maiorescu" – Securitatea sistemelor informatice şi a reţelelor informaţionale**
- **IT Systems Administrator – BRD Finance**

Introducere

Un atac comun asupra unei rețele WLAN implică interceptarea pachetelor de date pentru a decripta parolele de acces. Un exemplu de astfel de atac este atacul de tip „Handshake Capture”, unde voi intercepta procesul de autentificare între un client și router, capturând „handshake”-ul. Ulterior, folosind tehnici de forță brută sau dicționare de parole, urmând să obţin parola rețelei.

PROTOCOALE DE SECURITATE

WEP

WPA\WPA2

WPA3

WEP (Wired Equivalent Privacy)

La început, se credea că WEP oferă o rezistență impenetrabilă împotriva hackerilor. Cu toate acestea, pe măsură ce rețelele wireless au început să devină populare, mulți criptoanaliști și cercetători au descoperit probleme în designul original al WEP

Chiar și cu slăbiciunile sale cunoscute, WEP este încă mai eficient decât lipsa totală de securitate.

Algoritmul WEP folosește cifrul RC4 pentru a cripta datele între punctul de acces și dispozitivul wireless.

Este vulnerabil la atacul de tipul "man in the middle"

WPA (Wi-Fi Protected Access) şi WPA2

Wi-Fi Protected Access (WPA) și Wi-Fi Protected Access 2 (WPA2) reprezintă două protocoale de securitate dezvoltate ca răspuns la vulnerabilitățile grave ale protocolului anterior, WEP (Wired Equivalent Privacy). Acestea au fost create pentru a oferi o protecție mai eficientă și mai sigură pentru rețelele wireless, întrucât WEP a devenit rapid învechit și vulnerabil la atacuri cibernetice.

WPA a prezentat o criptare mai puternică prin intermediul TKIP (Temporal Key Integrity Protocol)

WPA2 utilizează criptarea AES exclusivă și nu mai include suport pentru TKIP

WPA3

Pentru a ţine pasul cu dezvoltarea tehnologică, la nivelul protocoalelor de securitate pentru rețelele wireless a fost introdus protocolul WPA3. Scopul acestuia este de a simplifica securitatea, de a permite autentificare robustă și de a crește puterea criptografică

În WPA3-Personal, Pre-shared Key (PSK) nu mai este folosit fiind preferat Simultaneous Authentication of Equals (SAE).

Odată cu WPA3 este pentru prima dată prezentat şi protocolul Wi-Fi Enhanced Open, care reprezintă un răspuns la problema rețelelor deschise

Atacul asupra reţelei wireless

În videoclipul următor, atacul prezentat în introducere va fi efectuat step by step.

Pentru acest atac am utilizat un adaptor de reţea Archer T3U Plus Adaptor USB Dual-Band Wireless High-Gain AC1300 şi un VM unde este instalat Kali Linux.