Sichere Informationssysteme

Netzwerk- und Kryptopraktikum (NKP4)

Challenge 01 – Wargames

Markus Zeilinger

SoSe 2024

Ausgangslage

Im Umfeld des SESAM Labors (FH Gebäude 2, Ebene 4, FH2.436) wird ein WLAN mit der SSID `wargames`[1] im WPA2 Personal Mode betrieben.

1 Ziel

Dein Ziel ist es, das WPA2-Passwort dieses WLANs zu knacken und in weiterer Folge ein "Geheimnis" zu entwenden.

Teilaufgabe 1 – Einarbeitung

Lies dich in die Grundlagen für einen solchen Angriff ein und recherchiere, welche verschiedenen Möglichkeiten es für einen solchen Angriff gibt. Folgende Fragen könnten dabei maßgeblich sein:

- Welche Möglichkeiten gibt es, Angriffe auf WPA2 Personal Mode WLANs durchzuführen, um das verwendete WPA2-Passwort zu bestimmen?
- Wie funktionieren dabei Angriffe unter Verwendung des Vier-Wege-Handshakes und warum sind sie möglich?
- Wie funktionieren dabei s. g. PMKID Angriffe und warum sind sie möglich?
- Welche "unterstützenden" Angriffe gibt es, die dem*der Angreifer*in seine*ihre Arbeit dabei erleichtern?
- Welche Software/Tools gibt es, um Angriffe auf WPA2-Passwörter/Schlüssel durchzuführen?

Teilaufgabe 2 – Knacken des Passworts

Versuche nun mit dem gesammelten Wissen das WPA2-Passwort zu knacken! Du wirst dafür WLAN-Hardware (z. B. WLAN-Adapter deines Laptops) und ein geeignetes Betriebssystem (z. B. Kali Live System gebootet von einem USB Stick) brauchen. Zudem solltest du dir ein im Kontext des Themas der Aufgabe sinnvolles Wörterbuch an möglichen Passwörtern zusammenstellen. Verwende die während deiner Recherche gefundenen Tools, um das WPA2-Passwort zu knacken!

Teilaufgabe 3 – Ermitteln des "Geheimnisses"

Jetzt wo du das WPA2-Passwort des WLANs kennst, kannst du im WLAN stattfindende Kommunikation entschlüsseln und analysieren. Nutze das dabei erlangte Wissen, um das gesuchte "Geheimnis" zu entwenden!

[1] Der Film "Wargames - Kriegsspiele" kann über z. B. Amazon Prime Video bezogen aber auch in unserer Bibliothek auf DVD entlehnt werden.