Netzwerkerkundung

Nachdem wir nun mit dem "fremden" WLan verbunden sind, müssen wir uns zunächst einen Überblick über die dort vorhandenen Geräte verschaffen, um weitere Ziele für unsere kleine Hackingreise auszumachen.

Das Werkzeug der Wahl hierfür ist `nmap`. Mit `nmap` kann man sowohl ganze Netzwerke nach vorhandenen Rechners "scannen" als auch einzelne Rechner untersuchen, um herauszufinden, welche Dienste diese im Netz anbieten.

Übersichtsscan

Um das Netzwerk auf aktive Geäte zu untersuchen, kannst du den Behfehl

```
nmap -sP {Netzwerkadresse/Subnetzmaske}
```

verwenden. Finde also Netzwerk und Subnetzmaske heraus und untersuche das Netzwerk. Du erhältst eine Liste mit aktiven Hosts als Ergebnis.

Inspektion der einzelnen Hosts

Untersuche die Geräte im Netz mit dem Befehl

```
nmap -sS -T4 {IP-Adresse}
```

Was bedeuten die Argumente des Befehls? (`-sS`, `-T4`) Mit `man nmap` kannst du die Manual-Page aufrufen, dort kannst du mit dem `/` suchen.

Unser nächstes Ziel ist der Server, bei dem die Ports 443 und 80 geöffnet sind. Finde heraus welche Dienste sich gewöhnlich hinter diesen Ports verbergen und versuche mit geeigneten Werkzeugen weitere Informationen zu gewinnen.

++++ Hilfe | Die Ports 80 und 443 werden üblicherweise für http und https verwendet - Erste Informationen kann man sich mit einem Web-Browser verschaffen, indem man die Adresse http://ip-adresse/ öffnet.