Spoofing

2. Ein Angreifer “sitzt” (lauscht) auf einem zufälligen Port oder Socket, den der server üblicher- weise nutzt.

3. Ein Angreifer kann alle möglichen Credentials der Reihe nach durchprobieren (online oder offline) und es gibt keinen Mechanismus, der ihn ausbremst.

4. Ein Angreifer kann sich anonym verbinden, weil Sie davon aus- gehen, dass Authentisierung auf einer höheren Schicht stattfindet.

5. Ein Angreifer kann einen Client verwirren, weil es zu viele Wege gibt, einen Server zu identifizieren.

6. Ein Angreifer kann einen Server spoofen, weil auf dem Client keinerlei Identifizierungsmerk- male gespeichert sind, die bei erneuter Verbindung überprüft würden (es gibt keine Key- persistence).

7. Ein Angreifer kann sich zu einem Server oder Peer über einen nicht authentisierten unverschlüsselten Kanal verbinden.

Fortsetzung umseitig

Spoofing cont.

8. Ein Angreifer kann auf einem Server gespeicherte Credentials stehlen und wieder verwenden (z.B. Schlüssel in einer für andere lesbaren Datei).

9. Ein Angreifer, der Zugang zu einem Passwort bekommt, kann es wieder verwenden (nutzen Sie stärkere Authenti- sierungsmethoden).

10. Ein Angreifer kann wählen, dass eine schwächere oder gar keine Authentisierung genutzt wird.

J. Ein Angreifer kann die auf einem Client gespeicherten Credentials stehlen und wieder verwenden.

Q. Ein Angreifer kann den Mechanismus angreifen, mit dem Passwörter zurückge- setzt oder aktualisiert werden (Account Recovery erfordert nicht die Eingabe des alten Passworts).

K. Ihr System wird mit einem Default Adminpasswort ausgeliefert und erzwingt nicht die Änderung dieses Passworts.doesn’t force a change.

A. Sie haben einen neuen Spoofing Angriff erfunden.