

Sikring af trådløse netværk

Varighed:
2 dage workshop

Målgruppe:
Alle med interesse for netværk vil have glæde af denne workshop

Formål:
Introduktion til wireless teknologier baseret på IEEE 802.11 og sikkerhed, herunder penetrationstest og forberedelse til test af egne trådløse netværk.

Indhold:

På kurset gennemgås de nødvendige tiltag for at sikre dit netværk mod de nye trusler fra wireless hacking, aflytning af trådløse netværk m.m.

Kurset i Wireless sikkerhed dækker begreber, teknikker og metoder i forbindelse med sikring af trådløse netværk. På kurset gennemgås bl.a.

- Introduktion til 802.11 trådløse netværk
- Trusler og risici ved trådløse netværk
- Protokoller og standarder 802.11
- Information om netværksnavn og SSID
- Kryptering, Wired Equivalent Privacy (WEP) og Wi-Fi Protected Access WPA
- Access points
- Sikkerhedsteknologier i enterprise netværk: 802.1x, VPN, IPsec og firewalls
- SSH/SSL
- WEP og WPA-PSK cracking, forudsætninger og muligheder
- aircrack-ng, airodump-ng, aireplay, airpwn og lignende hackerværktøjer

Workshop arbejdsformen betyder at vi konfigurerer udstyr og udfører angreb mod sårbare trådløse netværk i praksis med de tilgængelige værktøjer og platforme - på samme måde som en hacker ville gøre det.

Forudsætninger:

Kurset kræver ingen forudsætninger, men det største udbytte opnås med

Wireless sikkerhed

forudgående kendskab til TCP/IP.

Materialer:

Der udleveres på kurset:

- Kursusmateriale bestående af præsentation og øvelseshæfte - udleveres gerne elektronisk som PDF
- Boot CD med programmer
- Kursusevaluering