

UNIX sikkerhed

Varighed:
3 dage workshop

Målgruppe:
Alle med interesse for Unix og Unix sikkerhed vil få udbytte af denne workshop

Formål:
Introduktion til Unix operativsystemernes sikkerhedsmekanismer og gængse programmer. Det overordnede mål er at ruste deltagerne til at genkende sikkerhedsproblemer som er relateret til Unix herunder applikationer, protokoller og netværk

Indhold:

På kurset gennemgås de nødvendige tiltag for at hærde og sikre netværk baseret på Unix systemer mod trusler fra netværk.

Kurset i Unix sikkerhed dækker alle de klassiske begreber, teknikker og metoder i forbindelse med sikring og der gennemgås bl.a.

- Secure Shell SSH
- Inetd services
- NFS sikkerhed og RPC
- Telnet, FTP, Rlogin og andre ældre protokoller som skal fjernes
- Buffer overflows og stack protection
- UNIX filrettigheder
- Almindelige services som BIND/named, anonym FTP og Apache webserveren
- Integritetscheckere som tripwire, mtree og AIDE

Workshop arbejdsformen betyder at vi konfigurerer udstyr og udfører angreb mod sårbare UNIX systemer 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 forudgående kendskab til Unix og TCP/IP på brugerniveau.

Unix sikkerhed

Materialer:

Der udleveres på kurset:

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