

Buffer overflow og exploitprogrammer

Varighed:
2 dage workshop

Målgruppe:
Det forventes at deltagerne har en interesse i og gerne kendskab til basale principper som assemblerprogrammering og ikke er bange for en debugger. Kodning af exploits vil tillige tage udgangspunkt i skabeloner med Perl kode.

Formål:
Introduktion til buffer overflows og dybere forståelse for problematikkerne i forbindelse med beskyttelse imod disse.

Indhold:

Dette kursus vil gennemgå shellcode og buffer overflows i detaljer med udgangspunkt i basale stakbaserede buffer overflow på UNIX systemer - samt beskyttelse imod disse. Kurset fortsættes med Windows overflows.

På workshoppen vil vi gennemgå teknikkerne bagved buffer overflows og metoderne til struktureret analyse af programmer og systemer. Workshop arbejdsformen betyder at vi udfører angreb mod sårbare systemer i praksis med de tilgængelige værktøjer og platforme - på samme måde som en hacker ville gøre det.