Durata: 2 giorni (16 ore)
Luogo: Milano
Orario: dalle 9:00 alle 13:00 e dalle 14:00 alle 18:00

Sommario del contenuto del programma:

Modulo 1: Misure di sicurezza

Terminologia WiFi; Sicurezza debole (Protezione MAC;SSIDs); Sicurezza intermedia (WEP, EAP); Sicurezza avanzata (WPA; VPNs)

Modulo 2: Metodi di attacco

Accesso alle reti con protezione debole (trovando IPs;MACs;trovando SSIDs); Rottura WEP (attacchi primitivi ed avanzati; accellareazione degli attacchi); attacchi non lineari (Denial of Service; falsi APs); Integrazione con altri metodi

Modulo 3: Strumenti di attacco

Scoprire a mappare le reti (Netstumbler, Kismet);Sniffing; Rottura WEP (WEPcrack, Airsnort, Aircrack); Faking e man-in-the-middle;antenne ed altro hardware

Modulo 4: Rafforzare la sicurezza WiFi

Sicurezza dell reti; sicurezza dei clienti; Sistemi AAA; combinazione di altre tecnologie (IDS,PKI), Counter-attack tecnico; relazioni con altre tecnologie wireless

Destinatari:

Questo corso e' indirizzato ad amministratori di rete, auditor, consulenti di sicurezza e direttori tecnici.

Metodologia:

Unire sessioni di teoria e di pratica, con descrizione degli argomenti da parte degli istruttori e sperimentazioni sul personal computer. Saranno effettuati esercizi e simulzioni di risoluzioni pratiche con individualizzazioni.

Istruttori:

Questo corso e' coordinato e diretto dal sig. Antonio Sousa, Direttore Tecnico di Marketware Europa (rappresentante e partner di Symantec SSL, Qualys, N-Stalker e Keynote, tra gli altri).

Per registrazione ed informazioni
Telefono: (02) 479 565 41
E-mail: formazione@marketware.eu
Indirizzo: Marketware, Largo Augusto, 3, 20 122 Milano

Modulo di registrazione