NSWSEC - 2giorni

CORSI

La Sicurezza nelle Reti Wireless

Introduzione

Il tema della sicurezza è oggi sentito in modo prioritario dai responsabili dell'IT delle imprese e da tutte le figure chiave all'interno dell'azienda ormai consapevoli dell'importanza di una sua corretta politica di gestione.
Le wireless LAN sono ormai diventate parte integrante e a volte strategica di qualsiasi istallazione di reti locali e di campus. La velocità di installazione, i costi contenuti e, ora, le prestazioni non più penalizzanti, aprono a questa tecnologia prospettive sempre più interessanti, ma al contempo si amplifica l'esposizione dell'intera infrastruttura a tutti i potenziali rischi di attacchi malevoli tipici delle reti senza fili.
Risulta evidente l'importanza di saper valutare il grado di esposizione di una rete wireless, essere in grado di valutarne i punti deboli ed avere competenze sufficienti per predisporre gli adeguati rimedi per una efficace azione di prevenzione e/o mitigazione.

Agenda

Introduzione alle Wireless Networks

- IEEE 802.11: principi generali, standard e protocolli
- Caratteristiche delle realizzazioni "Ad hoc mode"
- Aspetti specifici delle reti "Infrastucture mode"
- Sistemi Wireless Distribution System (WDS)
- Impiego del Monitor mode (RFMON - Radio Frequency MONitor)

La sicurezza nelle reti wireless

- I temi della sicurezza informatica
- Punti deboli nello standard 802.11
- Intercettazione delle comunicazioni
- Interruzione del servizio
- Accesso non autorizzato e tecniche di autenticazione
- Lo standard 802.11x
- Algoritmi di cifratura
- Gli algoritmi WEP/WPA/WPA2
- I fenomeni del wardriving e warchalking
- Tecniche di difesa, policy di sicurezza e best practice

Principali tipologie di attacco

- Scanning attivo e passivo
- Man-in-the-middle
- MAC Address spoofing
- ARP poisoning
- Denial of service
- Jamming
- AP overloading
- Tecniche di flooding
- Rogue e Fake AP

AIRCRACK-NG

- Piattaforme supportate
- Download e istallazione
- Determinazione del chipset nella scheda wireless
- Utilizzo dello strumento
- Verifica di funzionamento
- Prove pratiche con esempi di crack

Attacco e difesa

- Attaccare reti WEP clientless
- Attaccare reti WEP
- Attaccare reti WPA/WPA2
- Shared Key Authentication (SKA) bypass
- Attaccare Wi-Fi Protected Setup (WPS)
- Cosa sono le Rainbow Tables e come usarle
- Concetto di Rogue AP: esempio pratico
- Come velocizzare gli attacchi alle reti WiFi
- Tecniche di difesa
- Policy di buon senso per SSID broadcasting
- Impiego oculato dei filtri
- Utilizzare una Wireless DMZ
- Controllo della rete con Firewall, IDS e IPS
- Implementare autenticazione e controllo dell'accesso sicuri
- Cifratura robusta delle comunicazioni
- Controllo della copertura e del segnale radio
- Utilizzo dei WLAN Controller
- Vulnerability Assessment e Penetration Test
- Wireless security auditing e standard di riferimento

Metodologie didattiche

Il corso integra alla teoria una serie di esempi architetturali, casi di studio, esercitazioni. Il laboratorio permetterà agli utenti di sperimentare le **tecniche d'attacco utilizzate *in the wild***. I partecipanti dotati di PC portatile potranno partecipare direttamente e attivamente alle dimostrazioni realizzate scaricando, istallando e utilizzando **AIRCRACK-NG un potentissimo *tool* per il wireless cracking**.
Il materiale didattico comprende l'intera collezione delle diapositive mostrate in classe ed è integrato da esempi e casi di studio. Ulteriori documentazione di protocolli e programmi sono inoltre forniti a corredo del programma teorico.
Ad ogni partecipante sarà rilasciato un attestato di partecipazione certificato da NCP.

Obiettivi

Il corso mira ad evidenziare le problematiche di sicurezza delle reti WIFI suggerendo le migliori soluzioni da attuare al fine di proteggersi da accessi e utilizzi indesiderati e/o malevoli.

Destinatari

Il corso è rivolto agli IT manager, ai security manager, agli amministratori di WLAN e ai responsabili di CED. In generale a tutti i tecnici IT che devono fronteggiare aspetti relative alla sicurezza dei sistemi wireless. Può essere inoltre di interesse per i network design, i system integrator e chiunque altro senta il bisogno di acquisire valide competenze nel settore della sicurezza finalizzato alla realizzazione di soluzioni wireless.

Prerequisiti

Non sono richiesti prerequisiti specifici, anche se un minimo di cultura dei principi di base delle reti WiFi e di Networking sarebbe ideale per poter beneficiare appieno del corso.