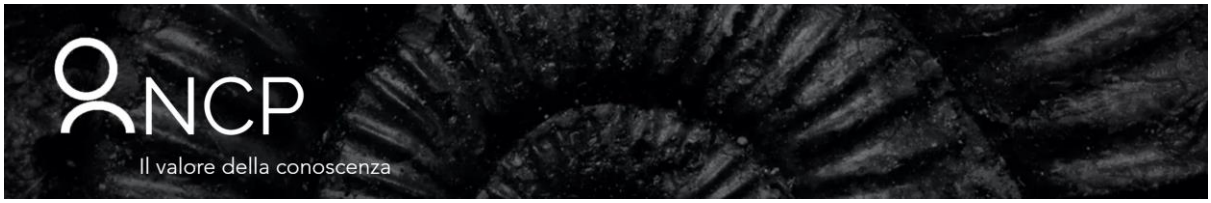
Corso specialistico di 2 giorni



VoIP Communication Security

Introduzione

Le tecnologie di trasporto della voce su infrastrutture IP sono ormai più che consolidate. Un enorme fermento anima l'intero settore in cui vecchie nuovi attori si impegnano per offrire nuovi prodotti e soluzioni. Unified & Instant Messaging, Presence, Collaboration, Mobility, Office Virtualization, sono tra le applicazioni più diffuse.
Ma quali problematiche si aprono dal punto di vista della sicurezza ? I sistemi VoIP sono sicuri ? A quali rischi sono esposti? Come si esegue un processo di vulnerability assessment ? Quali sono i rimedi ? Come si mette in sicurezza un sistema VoiP ?

Agenda

- I termini della sicurezza informatica applicati al VoIP
- Le dinamiche del VoIP
- Soluzioni architetturali ed elementi costitutivi di un sistema VoIP
- Principali vulnerabilità del VoIP e attacchi tipici
- Metodologie di analisi del rischio in sistemi VoIP
- Security Policies e Best Practices per i sistemi VoIP
- Vulnerability assessment e Penetration test in contesti VoIP
- Differenza tra infrastrutture Wireless e Wired nelle comunicazioni VoIP
- Interazione telefono switch
- Interazione telefono centrale telefonica
- Tecniche di protezione delle comunicazioni VoIP: cifratura, autenticazione, firma digitale
- Gestione dei certificati e PKI
- Accesso autenticato ai sistemi telefonici (IP-PBX)
- Cifratura dei flussi di segnalazione SIP mediante il protocollo TLS (Transport Layer Security)
- Cifratura del media attraverso il protocollo SRTP (Secure Real-time Transport Protocol)
- Utilizzo di programmi di "Sniffing" e intercettazione di chiamate VoIP con relativi tracciati
- Protezione dei sistemi medianti Firewall
- Il problema del NAT Traversal: soluzioni con STUN/TURN, ICE e ALG
- Separazione dei traffici mediante VLAN
- Esempi di attacchi tipici dei sistemi VoIP
- Dinamiche di provisioning dei telefoni VoIP e possibili vulnerabilità (Cisco, Polycom, Siemens, Snom)
- Hardening dei dispositivi VoIP contro accessi non autorizzati e attacchi.
- Rilevamento delle frodi: identificare e prevenire frodi che coinvolgono il servizio VoIP.
- Il problema dello SPIT - Spam over Internet Telephony
- SIP trunk: come cautelarsi dai "vampiri" di traffico telefonico
- Gestione degli incidenti di sicurezza in contesti VoIP.

Metodologie didattiche

Il corso integra alla teoria esempi architetturali, casi di studio e laboratori che prevedono l'emulazione di scenari tipici. I partecipanti dotati di PC portatile potranno partecipare direttamente e attivamente alle dimostrazioni realizzate nei laboratori.
Il materiale didattico comprende l'intera collezione delle diapositive mostrate in classe ed è integrato da numerosi esempi e casi di studio. Ulteriore documentazione di protocolli e programmi è inoltre fornita a corredo del programma teorico.
Ad ogni partecipante sarà consegnato un attestato di partecipazione rilasciato da NCP.

Obiettivi

Fornire un percorso esaustivo sulle tematiche della sicurezza legata alla implementazione di sistemi VoIP. Definire i termini della sicurezza, evidenziare i principali rischi, mostrare i rimedi, proporre best practices.
Il corso integra alla teoria esempi architetturali, casi di studio e laboratori che prevedono l'emulazione di scenari tipici. I partecipanti dotati di PC portatile potranno partecipare direttamente e attivamente alle dimostrazioni realizzate nei laboratori.

Destinatari

Il corso è rivolto ai manager di rete, agli installatori, ai system integrator, agli operatori telefonici che si stanno movendo verso l'integrazione Voce/Dati e al personale tecnico di qualsiasi fascia che opera nel mondo delle reti.

Prerequisiti

E' richiesta una cultura di base sui principi della telefonia e di Networking per poter beneficiare appieno del corso.