NSVOSEC - 2 giorni

CORSI

La Sicurezza nei Sistemi VoIP

Proteggere le risorse telefoniche dagli attacchi dei pirati informatici

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
- Le dinamiche del VoIP
- Soluzioni architetturali ed elementi costitutivi di un sistema VoIP
- Attacchi possibili: Hijacking, Mac flooding, Arp poisoning, DoS, …
- Metodologie di analisi del rischio
- Definire una politica di sicurezza per il VoIP
- Vulnerability assessment
- Penetration test. Cosa sono?
- Best Practices
- Differenza tra infrastrutture Wireless e Wired
- Interazione telefono switch
- Interazione telefono centrale telefonica
- Tecniche di protezione: cifratura, autenticazione, firma digitale
- Cifratura simmetrica e asimmetrica
- Gestione dei certificati e PKI
- Autenticazione del sistema telefonico (centrale IP)
- Cifratura dei flussi di segnalazione
- Cifratura dei flussi RTP
- Utilizzo di programmi di "Sniffing" e intercettazione di chiamate VoIP
- Protezione dei sistemi medianti firewall
- Separazione dei traffici mediante VLAN
- Esempi di attacchi tipici dei sistemi VoIP con relativi tracciati
- Intercettazione delle chiamate vocali in ambienti wireless e wired
- Endpoint e vulnerabilità (Cisco, Polycom, Siemens, Snom)
- Strumenti di attacco e di difesa

NCP – Networking Competence Provider Srl
Sede legale: Via di Porta Pertusa, 4 - 00165 Roma
Segreteria corsi : Tel: 06-88816735, Fax: 02-93660960
segreteria@ncp-italy.com

- Il problema dello SPIT - Spam over Internet Telephony
- SIP trunk: come cautelarsi dai “vampiri” di traffico telefonico
- Il problema del NAT Traversal
- Soluzioni con STUN/TURN, ICE e ALG
- Tunneling con GRE e IPsec

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. Ulteriori documentazione di protocolli e programmi sono inoltre forniti a corredo del programma teorico.
Ad ogni partecipante sarà rilasciato un attestato di partecipazione.

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

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