NSIP6S - 2giorni

CORSI

La Sicurezza nei sistemi IPv6

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.
I nuovi sistemi basati sul protocollo IPv6 sono sempre più diffusi. Il tempo in cui Ipv4 andrà definitivamente in pensione è ancora lontano ma già adesso si pongono i primi problemi di sicurezza e di esposizione a nuovi rischi di attacchi malevoli tipici del protocollo IPv6.
Risulta evidente l'importanza di saper valutare il grado di esposizione di una rete IPv6, di essere in grado di evidenziare i punti deboli ed avere competenze sufficienti per predisporre gli adeguati rimedi per una efficace azione di prevenzione e/o mitigazione.

Agenda

- Terminologia IPv6
- Novità rispetto a IPv4
- Analisi dell'Header Ipv6
- Il concetto di Daisy Chain
- Tipologie e formato degli indirizzi e le novità rispetto a Ipv4
- Metodologie di analisi del rischio
- Vulnerability assessment
- Penetration test. Cosa sono?
- Analisi degli scenari di esposizione al rischio in sistemi IPv4
- La problematica del host tracking in IPv6
- GTSM, Generalized TTL Security Mechanism
- Utilizzo del tool NMAP
- IPV6 Address host scanning
- Mitigazione host scanning
- Host tracking attack
- Mitigazione Host tracking
- ICMPv6 come veicolo per attacchi di tipo reset
- Path MTU Discovery: performance degrading e fragmentation attack
- Il protocollo Neighbor Discovery in IPv6
- Attacchi MITM e DDoS
- Neighbor Discovery message forging
- Utlizzo del tool "na6"
- Forwarding loop Router
- Overflowing neighbor cache attack
- Address sniffing attack
- SLAAC Attack
- DHCPv6 Attack
- Utilizzo del tool "Radvd"
- Attacchi di reti IPv4 mediante Ipv6: utilizzo di NATPT
- Implementare correttamente SEcure Neighbor Discovery (SEND)
- Monitorare il traffic con NDPMon
- Utilizzo di Router Advertisement Guard (RA-Guard)

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 **tool di hacking specifici di IPv6**.
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 IPv6 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 rete e ai responsabili di CED. In generale a tutti i tecnici IT che devono fronteggiare aspetti relative alla sicurezza dei sistemi Ipv6. 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 IPv6.

Prerequisiti

Una buona cultura dei principi di base delle reti TCP/IP e di Networking sarebbe ideale per poter beneficiare appieno del corso.