Sicurezza rete TCP/IP

Obiettivo:	Introduzione alla sicurezza di rete
Figure interessate	Amministratore di Rete, Sistemisti, Responsabili di area, Analisti Programmatori
Requisiti	Conoscenza minima dei servizi offerti da TCP/IP
Durata	16 ore
Durata Lezione	Da 4 a 8ore

Sommario

ALEF-0 di Carlo Donà e Silvia Simone
Tel Cellulare 348/2209748
Tel 041/5210439
Email formazione@alef-0.com
Web http://corsi.alef-0.com

Unità didattica 1: Scansione della rete (6 ore)

Tipologia di attacco: scansione tramite ICMP

Porte TCP e porte UDP
Scansione con Linux: nmap, netcat icmpquery
Scansione con Windows: Look@Host, superscan, scanline

Contromisure

Configurazione Firewall per bloccare ICMP
Chiudere le porte inutili
I sistemi IDS (Intrusion Detection System), SNORT in Linux.

Tipologia di attacco: identificazione della struttura di rete

Rilevamento geografico in base all'IP
Rilevazione del Sistema Operativo con nmap
Identificazione dei servizi con nmap

Contromisure

Configurazione corretta del DNS
Hardening dei servizi
Raffinazione regole Firewall

ALEF-0 di Carlo Donà e Silvia Simone
Tel Cellulare 348/2209748
Tel 041/5210439
Email formazione@alef-0.com
Web http://corsi.alef-0.com

Unità didattica 2: Servizi di rete (6 ore)

Enumerazione dei servizi di rete comuni ad utilizzo applicativo

Enumerazione tramite finger
Enumerazione mediante Netbios
Enumerazione tramite SNMP
Enumerazione geografica tramite WHOIS
Enumerazione tramite SQL
Regole di attribuzione di un indirizzo IP

Contromisure

Hardening Active Directory
Hardening motori DB
Limitazione ai trasferimenti di zona DNS
Rilevazione degli accessi tramite SNORT
Spunti sull'hiding di un nodo applicativo in un rete

ALEF-0 di Carlo Donà e Silvia Simone
Tel Cellulare 348/2209748
Tel 041/5210439
Email formazione@alef-0.com
Web http://corsi.alef-0.com

Unità didattica 3: Hacking dei Sistemi Operativi (4 ore)

Hacking di Linux

Debolezza delle password
Buffer overflow
Utilizzo di SUDO

Hacking di Windows 2000, 2003

Diventare amministratori
Controllo remoto
Elenco Chiavi di registro sensibili

ALEF-0 di Carlo Donà e Silvia Simone
Tel Cellulare 348/2209748
Tel 041/5210439
Email formazione@alef-0.com
Web http://corsi.alef-0.com