

LA TECHNOLOGY TRANSFER PRESENTA

JIMMY DONOHUE

**INTERNET SECURITY:
MINACCE E
CONTROMISURE**

ROMA 6-7 OTTOBRE 2003

**WIRELESS NETWORK
SECURITY**

ROMA 8-10 OTTOBRE 2003

RESIDENZA DI RIPETTA - VIA DI RIPETTA, 231



info@technologytransfer.it
www.technologytransfer.it

INTERNET SECURITY: MINACCE E CONTROMISURE

Firewalls, IDS, crittografia e politiche di sicurezza non sono sufficienti a prevenire gli attacchi degli hackers, le aziende non hanno bisogno solo di tecnologia ma di professionisti preparati in grado di prevenire o mitigare questi attacchi.

Questo seminario spiega in dettaglio quali minacce possono arrivare alle aziende da Internet e quali contromisure le aziende devono prendere per difendersi da questi attacchi. I partecipanti impareranno come difendersi dalle vulnerabilità di OS, le Best Practices di design per la salvaguardia delle implementazioni DNS e DHCP, capiranno dove crittografia e PKI sono strumenti necessari per la sicurezza dei networks e delle infrastrutture, saranno in grado inoltre attraverso workshops, di costruire templates di strategie di difesa per migliorare la loro attuale politica di sicurezza e i loro requisiti sulla sicurezza fisica.

I partecipanti impareranno:

- A identificare le minacce alla sicurezza
- A irrobustire i servizi e i sistemi interni
- A irrobustire i devices e i servizi di Internetwork
- Secure network communications
- A capire una PKI
- A capire i certificati digitali
- A implementare e monitorare la sicurezza sui network

PARTECIPANTI

Professionisti di IT che si interessano di networking e di sicurezza.

DESCRIZIONE

WIRELESS NETWORK SECURITY

Più aumenta la popolarità e le implementazioni di LANs wireless più cresce la necessità di rendere sicuri questi networks. La sicurezza per soluzioni wireless non può venire da un singolo protocollo software o da una soluzione hardware, ma deve essere costruita da professionisti di wireless networking attraverso l'implementazione di salvaguardie multiple.

Questo seminario esaminerà le tecnologie wireless, le architetture, la complicata matrice di protocolli, l'hardware, la matematica di RF, il comportamento di RF, la loro operatività, gli aspetti chiave della sicurezza, il troubleshooting. Attraverso presentazioni e dimostrazioni il seminario mostra le varie soluzioni wireless, spiega gli attacchi a cui i wireless sono sottoposti e fornisce le contromisure necessarie per difendere il Vostro wireless network sia da minacce esterne che interne. Esamina le tecnologie di sicurezza WEP e 802.1x, sviluppa politiche di sicurezza per wireless e fornisce tutto quello che è necessario per la gestione dei rischi della Wireless Security.

Alla fine del seminario i partecipanti saranno in grado di:

- Distrarci fra le tecnologie wireless emergenti
- Conoscere l'anatomia di un attacco al wireless e le tecniche di difesa
- Discutere soluzioni sui rischi alla sicurezza
- Capire come evolve la tecnologia wireless
- Distrarci e capire gli standards e i protocolli wireless
- Conoscenza della tecnologia di wireless encryption

PARTECIPANTI

- Managers responsabili di sicurezza e network operations
- Network Administrators
- Architetti di Information Security
- Auditors
- Consulenti e tutti i professionisti che pianificano, implementano e gestiscono wireless networks

INTERNET SECURITY: MINACCE E CONTROMISURE

1. Concetti generali di sicurezza

- Autenticazione
 - Kerberos
 - CHAP
 - Certificati
 - Username/Password
 - Tokens
 - Multi-factor
 - Mutual Authentication
 - Biometrics
- Servizi e Protocolli non essenziali
- Disabilitare i sistemi e i processi non necessari
- Attacchi
 - DOS/DDOS
 - Back Door
 - Spoofing
 - Man in the Middle
 - Replay
 - TCP/IP Hijacking
 - Weak keys
- Codice malizioso
 - Virus
 - Troiani
 - Logic Bombs
 - Worms
- Social Engineering
- Auditing – Logging, system scanning

2. Sicurezza della comunicazione

- Accesso Remoto
- E-mail
 - S/MIME
 - Vulnerabilità
 - PGP
 - Spam
 - Hoaxes
- Web
 - Minacce dalle applicazioni Web
 - SSL/TLS
 - HTTP/S
 - Privacy
 - Vulnerabilità
 - Java Script
 - ActiveX
 - Buffer Overflows
 - Cookies
 - CGI
 - SMTP Relay
 - Instant Messaging
 - NAT/Naming Conventions
 - Packet Sniffing
 - Invalid Parameters
- Directory Services
- File Transfer
- Wireless

3. Le 10 principali minacce per la sicurezza dell'applicazione

4. Sicurezza dell'infrastruttura

- Devices
- Media
- Topologie di sicurezza
- Intrusion Detection
 - Basata su network
 - Basata su host
 - Basata su anomalia
 - Incident Response
- Baselines di sicurezza
 - OS/NOS Hardening
 - File System
 - Aggiornamenti (Hotfixes, Packs, Patches)
 - Network hardening
 - Aggiornamenti (Firmware)
 - Configurazione
 - Enabling e Disabling
 - Servizi e Protocolli
 - Access control lists

5. Fondamenti di crittografia

- Algoritmi
 - Hashing
 - Simmetrici
 - Asimmetrici
- Concetti di uso della crittografia
 - Confidenzialità
 - Integrità
 - Disponibilità
- Firme digitali
 - Autenticazione
 - Non-Repudiation
 - Firme digitali
 - Controllo di accesso
 - PKI
 - Certificati (distinguere quali certificati sono usati e per quali scopi)
 - Politiche del certificato
 - Certificate Practice Statements
- Standards e Protocolli
- Aspetti chiave di gestione

6. Aspetti operativi e organizzativi della sicurezza

- Controllo di accesso per la sicurezza fisica
 - Barriere fisiche
 - Biometrics
 - Social Engineering
 - Ambiente
 - Wireless Cells
 - Location
 - Schermatura
- Disaster Recovery
 - Backups
 - Off Site Storage
 - Recovery sicuro
 - Siti alternati
 - Disaster Recovery Plan

- Continuità del Business
 - Utilities
 - Alta disponibilità/Fault Tolerance
 - Backups
- Politica e procedure
 - Politica della sicurezza
 - Uso accettabile
 - Due Care
 - Privacy
 - Separazione delle mansioni
 - Necessità di conoscere
- Gestione del privilegio
 - Gestione Utente/Gruppo/Ruolo
 - * Sign-on singolo
 - * Centralizzato verso decentralizzato
 - * Auditing (privilegio, uso, escalation)
 - * MAC/DAC/RBAC
- Forensics
 - Catena della custodia
 - Preservare la prova
 - Raccolta delle prove
- Identificazione del rischio
- Education

WIRELESS NETWORK SECURITY

1. Tecnologie wireless

- Fondamenti di Radio Frequency (RF)
- Tecnologie ad ampio spettro
- WPAN (Wireless Personal Area Network)
- WLAN (Wireless Local Area Network)
- WMAN (Wireless Metropolitan Area Network)
- WWAN (Wireless Wide Area Network)
- M-Commerce
- Selezione dell'antenna

2. Architettura Bluetooth™ e sicurezza

- Design e protocol stack di Bluetooth™
- Piconets e Scatternets
- Bluetooth™ Security Architecture
- Minacce alla sicurezza e tecniche di attenuazione

3. Architettura e sicurezza di 802.11 (b, a & g)

- Il design e il protocol stack di 802.11
- Networks ad hoc, bridged o shared
- Supporto per utenti roaming
- Configurazione del wireless access point
- Configurazione wireless del NIC
- Wired Equivalent Privacy (WEP): come lavora, i suoi principali punti di debolezza, attacchi conosciuti

4. Minacce e tecniche di attenuazione nei networks 802.11

- Proteggere l'interfaccia di Management
- Controllare e scoprire accessi non autorizzati al network
- Minacce al wireless network sniffing
- Wireless locators
- Wireless sniffers
- Combattere la fuga dell'informazione
- Attacchi di spoofings
- MAC address
- IP address
- ARP
- Access Point
- Rifiuto del servizio attraverso il jamming
- Non perdere di vista le vulnerabilità del firmware

5. Politiche di sicurezza e tecniche di auditing per i networks 802.11

- Sviluppare politiche pratiche, procedure e standards di sicurezza per le tecnologie wireless

- Passare in rassegna i diagrammi dei networks
- Usare locators e analizzatori di pacchetto per verificare la conformità
- Usare caratteristiche avanzate dell'analisi del pacchetto per una verifica avanzata della politica e dell'intrusion detection
- Wired tools per la scoperta e l'auditing di wireless
- Tools di intrusion detection per wireless LAN (WID)

6. Nuovi standards e nuove tecniche per l'autenticazione e l'encryption su 802.11

- Il ruolo del sub-comitato 802.11i
- Far girare le tecnologie SSL e VPN sul wireless
- Soluzioni basate su 802.1X
- EAP
- EAP-TLS
- EAP-TTLS
- Soluzione LEAP di Cisco
- Esempio di architetture Enterprise usando RADIUS e PKI

7. Architetture cellulari e Modelli di sicurezza per WMAN e WWAN

- Panoramica del mercato del cellulare
- Prima generazione di tecnologie wireless (1G): solo voce
- Seconda generazione di tecnologie wireless (2G)
- Voce e dati a bassa larghezza di banda
- TDMA, GSM, CDMA, iDEN, PDC/iMode CDPD, Mobitex
- Terza generazione di tecnologie wireless (3G)
- Voce e dati con alta larghezza di banda
- GPRS, EDGE, CDMA 2000
- Quarta generazione di tecnologie wireless (4G)
- Voce con data networks ibridi
- Integrare WWAN di 2G/3G con WLAN e WPAN

8. M-Commerce sta superando la tecnologia WWAN: limitazioni per le transazioni sicure

- Vincoli di design per m-Commerce
- La soluzione WAP
- WAP protocol stack: WML, WMLScript, WSP, WTLS, WDP
- WAP security architecture
- Aspetti di sicurezza e di audit legati ai gateways WAP
- Punti di debolezza sulla sicurezza in WTLS
- Sfide di PKI per m-Commerce

Demo che saranno svolte durante il seminario:

Lab1: Costruire una Infrastructure Mode Wireless Lan

Questo Lab vi mostrerà come connettersi a un access point usando matching SSIDs e WEP settings. Imparerete il processo corretto per connettere diversi Clienti wireless all'access point e di cosa aspettarsi da una wireless LAN. L'efficacia e la copertura di RF è mostrata attraverso le utilities Client.

Lab2: Imparerete a dimensionare le celle wireless in un ambiente di infrastruttura e a implementare ARS (Automatic Rate Selection)

Imparerete come architettare una wireless LAN usando site surveys. I principali argomenti sono l'analisi e le predizioni del dimensionamento delle celle e ARS. Questo site survey includerà inoltre considerazioni sulla velocità potenziale, la sicurezza e l'affidabilità della wireless LAN basata sul numero di celle usate.

Lab3: Analisi dell'Infrastructure Mode Throughput

Questo Lab copre i possibili scenari di throughput ottenibili dalle LAN wireless. I partecipanti impareranno i limiti delle wireless LAN half-duplex nelle situazioni reali.

Lab4: Connettere in una configurazione ad hoc e analisi del throughput

In questo Lab i Clienti wireless saranno connessi in una configurazione ad hoc. I partecipanti impareranno come settare i canali e comparare il throughput degli ambienti ad hoc verso gli ambienti infrastructure.

Lab5: Tools base di sicurezza

In questo laboratorio gli studenti apprenderanno le basi dello standard wireless IEEE 802.11.

Lab7: Autenticazione in 802.1x, generazione di chiavi WEP statiche e dinamiche, Mutual Authentication usando 802.1x/EAP e RADIUS

In questo Lab si parlerà di WEP. L'istruttore Vi mostrerà il controllo di accesso port-based con autenticazione EAP e i nuovi standards wireless security di Cisco.

Opera nel settore dell'IT dal 1983 e fornisce servizi di consulenza e formazione dal 1993. Ha operato con una varietà di piattaforme e sistemi. Ha cominciato con Netware 2.01a e ha seguito tutte le versioni Windows dalla 2.0 fino al 2003. Negli ultimi quattro anni ha focalizzato il suo interesse sul networking e su Internet, facendo ottimizzazioni e design dell'infrastruttura di network con particolare attenzione alle tecnologie di sicurezza e wireless.

JIMMY DONOHUE

QUOTA DI PARTECIPAZIONE

Internet Security: Minacce e Contromisure

€ 1100 (+iva)

Wireless Network Security

€ 1300 (+iva)

La partecipazione a entrambi i seminari viene offerta a una speciale quota di € 2250 (+iva)

La quota comprende documentazione, colazioni di lavoro e coffee breaks.

CONDIZIONI GENERALI

In caso di rinuncia con preavviso inferiore a 15 giorni verrà addebitato il 50% della quota di partecipazione, in caso di rinuncia con preavviso inferiore ad una settimana verrà addebitata l'intera quota.

In caso di cancellazione del seminario, per qualsiasi causa, la responsabilità della Technology Transfer si intende limitata al rimborso delle quote di iscrizione già pervenute.

MODALITÀ DI ISCRIZIONE

Il pagamento della quota, IVA inclusa, dovrà essere effettuato tramite: bonifico sul c/c N. 4889027/01/10 della Banca Intesa S.p.A. - Ag. 3 di Roma CAB 05039 - ABI 03069 intestato alla Technology Transfer S.r.l. e la ricevuta di versamento inviata insieme alla scheda di iscrizione a:

TECHNOLOGY TRANSFER S.r.l.

Piazza Cavour, 3 - 00193 ROMA - Tel. 06-6832227 - Fax 06-6871102

entro il 22 Settembre 2003

Vi consigliamo di far precedere la scheda di iscrizione da una prenotazione telefonica.

LUOGO

Roma, Residenza di Ripetta - Via di Ripetta, 231

DURATA ED ORARIO

2 giorni/3 giorni: 9.30-13.00 14.30-17.30

È previsto il servizio di traduzione simultanea

TUTELA DATI PERSONALI

Ai sensi dell'art. 10 della legge n. 675/96, il partecipante è informato che i suoi dati personali acquisiti tramite la scheda di partecipazione al seminario saranno trattati da Technology Transfer anche con l'ausilio di mezzi elettronici, con finalità riguardanti l'esecuzione degli obblighi derivati dalla Sua partecipazione al seminario, per finalità statistiche e per l'invio di materiale promozionale dell'attività di Technology Transfer.

Il conferimento dei dati è facoltativo ma necessario per la partecipazione al seminario. Il titolare del trattamento dei dati è Technology Transfer, Piazza Cavour, 3 - 00193 Roma, nei cui confronti il partecipante può esercitare i diritti di cui all'art. 13 della legge n. 675/96.

JIMMY DONOHUE



@

- | | | |
|--------------------------|--|--|
| <input type="checkbox"/> | INTERNET SECURITY:
MINACCE E CONTROMISURE | <i>Roma 6-7 Ottobre 2003
Residenza di Ripetta
Via di Ripetta, 231
Quota di iscrizione
€ 1100 (+iva)</i> |
| <input type="checkbox"/> | WIRELESS NETWORK
SECURITY | <i>Roma 8-10 Ottobre 2003
Residenza di Ripetta
Via di Ripetta, 231
Quota di iscrizione
€ 1300 (+iva)</i> |
| <input type="checkbox"/> | ENTRAMBI I SEMINARI | <i>Quota di iscrizione per
entrambi i seminari
€ 2250 (+iva)</i> |

È previsto il servizio di traduzione simultanea

In caso di rinuncia o di cancellazione dei seminari valgono le condizioni generali riportate sopra.

nome

cognome

funzione aziendale

azienda

partita iva

codice fiscale

indirizzo

città

cap

provincia

telefono

fax

e-mail



Timbro e firma

Da restituire compilato a:
Technology Transfer S.r.l.
Piazza Cavour, 3 - 00193 Roma
Tel. 06-6832227 - Fax 06-6871102
info@technologytransfer.it
www.technologytransfer.it