

CERTIFIED NETWORK SECURITY MANAGER

CORE SKILLS

MILANO

Starhotel Splendido

30 GIUGNO 4 LUGLIO 2003

1-5 DICEMBRE 2003

**GARANTIRE
UN ELEVATO
LIVELLO DI
SICUREZZA E
RIDURRE AL
MINIMO LA
VULNERABILITÀ
DELLA RETE
AZIENDALE**



**REALIZZARE UNA RETE AZIENDALE
SICURA E PROTETTA**



**UTILIZZARE EFFICACEMENTE I TOOLS
DI SICUREZZA**



**VERIFICARE L'INTEGRITÀ DELLA RETE
ATTRAVERSO UN CONTINUO
MONITORAGGIO DEI SISTEMI**



**EVITARE ATTACCHI ED INTRUSIONI
NEL SISTEMA INFORMATICO**



**CONOSCERE GLI ASPETTI
GIURIDICO-LEGALI DELLA SICUREZZA**

TEL.	02.83847.627
FAX	02.83847.262
E-MAIL	corsi@iir-italy.it
WEB	www.iir-italy.it

NOVITÀ ESCLUSIVA

SCONTO 20% sui servizi di Security Scan
e Auditing di Infosec
(valido fino al 31-12-2003)



CERTIFIED NETWORK SECURITY MANAGER

A CHI È RIVOLTO

- Security Manager
- Responsabile Sistemi Informativi
- Responsabile Sicurezza
- Amministratore di Rete
- Responsabile C.E.D.

AGENDA

- 08.45 Registrazione (1° giorno)
- 09.00 Inizio lavori
- 11.00 Coffee break
- 13.00 Pranzo
- 15.45 Tea break
- 17.00 Conclusione lavori

PROGRAMMA FORMATIVO

1° GIORNATA

SIGUREZZA E SUE PROBLEMATICHE

Perché esiste il problema della sicurezza informatica

- Quali sono i rischi reali, dove sono le vulnerabilità maggiori
- Quali sono le corrette modalità di approccio al problema

Perché i rischi legati alle reti informatiche sono attuali ed in continuo aumento

- Statistiche e percentuali
- La sicurezza informatica e le violazioni nel mondo
- Perché in Italia le statistiche sono diverse

Problemi dovuti ad attacchi e problemi di configurazione

- Identificare gli attaccanti: chi sono, cosa cercano, come agiscono
- Identificare i bersagli: perché attaccano noi
- Distinguere gli attacchi reali dagli errori di configurazione

Punti vulnerabili in una tipologia di rete, nei servizi e nelle soluzioni

- Vulnerabilità Software e Hardware
- Esempi di vulnerabilità in reti eterogenee
- Analisi dei singoli punti di vulnerabilità e motivazioni

Panoramica sui protocolli di rete

- Introduzione pratica al protocollo TCP/IP (TCP, UDP, ICMP)
- Vulnerabilità e metodologie di attacco legate al protocollo TCP/IP

2° GIORNATA

LE BASI PER LA COSTRUZIONE DI UNA RETE SICURA

“Secure way of it”, come fare le cose, come usarle ed in che ottica

- Avere una rete operativa non vuol dire lavorare in sicurezza: differenza tra “funziona” ed “è sicuro”
- Come valutare il giusto equilibrio tra efficienza e sicurezza
- Politiche di sicurezza e “best practices”
- Come scegliere i protocolli e le metodologie più adatte in base alle diverse esigenze

Tecniche utilizzate durante l'attacco

- Buffer overflow
- Cattiva validazione dell'input
- Denial of Service
- Backdoor e Trojan

Problematiche relative alle reti wireless

- Antivirus
 - A cosa servono e dove servono
 - Quali sono i vantaggi e quali i limiti
 - Differenze tra i principali software antivirus

Attività pratiche: esempi di attacchi e relative contromisure, problematiche nella gestione dei sistemi antivirus.

PERCHÈ PARTECIPARE

Le nuove opportunità di business legate a Internet e la progressiva diffusione dei servizi offerti in rete espongono inevitabilmente le aziende ad un crescente rischio di minacce ai propri sistemi informativi. Ecco perché la sicurezza delle reti informatiche è un tema sempre più sentito da tutte le realtà aziendali. In questo contesto diventa cruciale, per le aziende, essere sempre in grado di valutare le aree di vulnerabilità della propria rete, conoscere le molteplici tipologie di attacco possibili ed adottare le contromisure più adeguate. Il corso “Network Security Manager”, costantemente aggiornato alla luce delle più recenti novità tecnologiche e normative, affronta tutti gli aspetti relativi alla gestione del rischio informatico, da quelli tecnologici a quelli metodologici e legali, e ha l'obiettivo di trasferire le competenze specifiche necessarie per monitorare costantemente le minacce ai propri sistemi informativi, fronteggiare i possibili attacchi dall'esterno e applicare una politica di sicurezza veramente efficace.

LA DOGENZA

Igor Falcomatà IT Security Manager e Matteo Falsetti Research & Development Manager presso Infosec



società specializzata nella fornitura di servizi e consulenze per la sicurezza informatica. Infosec (<http://www.infosec.it>) si rivolge a tutte le realtà del settore pubblico e privato che abbiano l'esigenza di realizzare e gestire infrastrutture di rete con elevati livelli di sicurezza, proponendosi come partner flessibile capace di operare come auditor esterno, come sviluppatore di sistemi ad hoc, come collaboratore in progetti complessi, in relazione alle specifiche necessità della clientela.

Infosec è socio CLUSIT (<http://www.clusit.it>), Associazione Italiana per la Sicurezza Informatica

Avv. Luca M. de Grazia

Patrocinante in Cassazione, editorialista di Radio 24 e del Sole 24 Ore, ha pubblicato numerosi scritti su internet e diritto e ha partecipato in qualità di relatore a numerosi convegni. Oltre alla libera professione, svolge abitualmente attività di formazione nel settore della sicurezza informatica.



TEL.	02.83847.627
FAX	02.83847.262
E-MAIL	corsi@iir-italy.it
WEB	www.iir-italy.it

FORMAZIONE PERSONALIZZATA

L'obiettivo è quello di creare interventi formativi su misura adattati alle specifiche esigenze delle aziende clienti ed erogabili pertanto nella modalità "in-house".

Per ulteriori informazioni o per concordare un'analisi delle vostre necessità formative, non esiti a contattarci telefonicamente al numero 02.83847.281 o inviarci una mail all'indirizzo: info_inhouse@iir-italy.it



3° GIORNATA

STRUMENTI PER LA DIFESA DELLA RETE

Firewall

- Cos'è e come funziona
- A cosa serve e con quali applicazioni posso usarlo, quali sono i limiti
- Politiche di sicurezza applicate: come decidere le regole e in base a cosa
- Come proteggere i servizi più comuni su server web, mail, proxy e dns
- Esempi di regole per alcuni dei firewall più comuni

La sicurezza dei dati da e verso l'esterno

- Perché un firewall non è sufficiente: metodologie di attacco a reti protette;
- Esempi di traffico "malicious" incapsulato in traffico "legittimo"
- Problematrice tecniche relative al traffico in transito: come discriminarlo e limitarlo, relativamente ai vari punti della rete

Intrusion Detection Systems

- Cosa sono e come funzionano
- Il problema dei falsi positivi e falsi negativi
- Principali soluzioni commerciali ed Open Source

Attività pratiche: esempi di configurazione di snort, esempi di firewalling con linux iptables, elusione dei sistemi firewall e IDS e relative contromisure.

4° GIORNATA

SICUREZZA DEI DATI IN TRANSITO E MONITORAGGIO DELLA RETE

Ragioni, principi ed utilizzo della crittografia

Public Key Infrastructure

- Identificazione degli utenti
- Certificati digitali
- Certification/Registration Authority
- Firma digitale
- Applicazioni pratiche

Protocolli di sicurezza (VPN, SSL, SSH, IPSEC)

- Quali sono i protocolli "sicuri"
- Perché sono "sicuri"
- Definizioni, differenze ed applicazioni pratiche

I sistemi di pagamento (esempi, problemi, vulnerabilità)

- Le vulnerabilità di sicurezza più comuni legate ai sistemi di e-commerce ed alle tecniche di pagamento on-line

- Dove sono i rischi reali: problematiche della tecnologia, problematiche nella transazione, problematiche "pre" e "post"

Monitoraggio della rete

- Come controllare le attività di reti, sistemi e utenti
- Come identificare le violazioni o tentate violazioni
- Come accorgersi di un'intrusione
- Controllare l'integrità del sistema

Cosa fare se si è verificata un'intrusione

- Cosa fare se c'è stata una compromissione del sistema e dei dati
- Gestione e risoluzione degli incidenti

Strumenti di verifica

- Come verificare la sicurezza della propria rete

Esempi di simulazioni di attacco

- A cosa serve una simulazione
- Come funziona?
- Come scegliere?
- Limiti dei tool automatizzati
- Auditing delle applicazioni

Attività pratiche: sniffing e contromisure, ricerca di backdoor nel sistema, analisi dei log.

5° GIORNATA

ASPETTI LEGALI E RISORSE PER GLI AMMINISTRATORI

Aspetti legali della sicurezza informatica

- Introduzione ai concetti di Diritto e Sicurezza
- Come organizzare la sicurezza
- Security ed obblighi giuridici
- Legge 675/96
- DPR 318/99
- Vigilanza ed investigazioni

Risorse per amministratori

- Upgrade
- Aggiornamento
- Approfondimenti

Aggiornamento, fonti e risorse

- Identificare ed utilizzare le fonti di informazione "security related"
- Full disclosure, no disclosure, responsible disclosure
- Open e closed source, vantaggi e svantaggi

CERTIFIED NETWORK SECURITY MANAGER CORE SKILLS

SEDE	Milano - Starhotel Splendido
	Via A. Doria 4 - Tel. 02.6789

Sì desidero partecipare alla seguente edizione:

<input type="radio"/>	MILANO, 30 GIUGNO 4 LUGLIO 2003	T1212
<input type="radio"/>	MILANO, 1-5 DICEMBRE 2003	T1213

Quota d'iscrizione: Euro 2.050 + 20% I.V.A. per partecipante

10% di sconto Per ogni singolo evento, dal 3° iscritto pervenuto dalla medesima Azienda verrà applicato uno sconto del 10%

Non saranno ammesse in sala le persone la cui quota d'iscrizione non sarà pervenuta prima del corso. La quota d'iscrizione comprende la documentazione didattica, i pranzi e i coffee break. Per circostanze imprevedibili, l'Istituto di Ricerca Internazionale si riserva il diritto di modificare il programma, i relatori, le modalità didattiche e/o la sede del corso.

Modalità di pagamento

La quota deve essere versata secondo le modalità di seguito indicate. Copia della fattura/contratto di adesione al corso verrà spedita a stretto giro di posta.

- Versamento effettuato sul ns. c/c postale n.16834202
- Assegno bancario - assegno circolare
- Bonifico bancario (Banca Popolare di Sondrio - Milano, Agenzia 10, Via Solari, 15) c/c 2805/07 intestato a Istituto di Ricerca Internazionale Srl ABI 5696 CAB 01609 indicando il codice del corso prescelto
- Carta di credito: Eurocard/Mastercard American Express
 Diners Club Visa CartaSi

N°

Scadenza Titolare

Modalità di disdetta

L'eventuale disdetta di partecipazione all'intervento formativo dovrà essere comunicata in forma scritta all'Istituto di Ricerca Internazionale entro e non oltre il 10° giorno lavorativo precedente la data d'inizio del corso. Trascorso tale termine, sarà inevitabile l'addebito dell'intera quota d'iscrizione. Saremo comunque lieti di accettare un Suo collega in sostituzione purchè il nominativo venga comunicato via fax almeno un giorno prima della data corso.

PER ISCRIVERSI

TEL.	02.83847.627
FAX	02.83847.262
E-MAIL	corsi@iir-italy.it
WEB	www.iir-italy.it
POSTA	Istituto di Ricerca Internazionale Via Forcella, 3 - 20144 Milano

SCHEDA DI ISCRIZIONE

Non rimuovere l'etichetta. Grazie.

T1212 WWW - I124/VIII

Dati del partecipante:

NOME _____ COGNOME _____
FUNZIONE _____
INDIRIZZO _____
CAP _____ CITTÀ _____ PROV. _____
TEL. _____ FAX _____
E-MAIL _____
CONSENSO ALLA PARTECIPAZIONE DATO DA: FUNZIONE _____
NOME E COGNOME _____

Dati dell'Azienda:

RAZIONE SOCIALE _____
SETTORE MERCEOLOGICO _____
FATTURATO IN EURO 0-10 Mil 11-25 Mil 26-50 Mil 51-250 Mil 251-500 Mil +500 Mil
NUMERO DIPENDENTI **G** 1-10 **F** 11-50 **E** 51-100 **D** 101-200 **C** 201-500 **B** 501-1000 **A** +1000
PARTITA I.V.A. _____
INDIRIZZO DI FATTURAZIONE _____
CAP _____ CITTÀ _____ PROV. _____
TEL. _____ FAX _____
E-MAIL _____

Timbro e firma

TUTELA DATI PERSONALI - INFORMATIVA

Si informa il Partecipante ai sensi dell'art.10 della legge 31.12.1996 n.675: (1) che i propri dati personali riportati sulla scheda di iscrizione ("Dati") saranno trattati in forma automatizzata dall'Istituto di Ricerca Internazionale (I.R.I.) per l'adempimento di ogni onere relativo alla Sua partecipazione alla conferenza, per finalità statistiche e per l'invio di materiale promozionale di I.R.I.; (2) il conferimento dei Dati è facoltativo: in mancanza, tuttavia, non sarà possibile dar corso al servizio; (3) i Dati saranno comunicati, previo Suo consenso, a società controllate o altrimenti collegate, anche indirettamente, ad I.R.I., ovvero a soggetti terzi, in Italia e all'estero, per il compimento di ricerche di mercato e per la promozione dei servizi offerti dagli stessi soggetti, ovvero per la gestione dei Dati stessi ai fini indicati al punto 1. In relazione ai Dati, il Partecipante ha diritto di opporsi al trattamento sopra previsto.

TITOLARE E RESPONSABILE DEL TRATTAMENTO è l'Istituto di Ricerca Internazionale, via Forcella 3, Milano nei cui confronti il Partecipante potrà esercitare i diritti di cui all'art. 13 Legge 675/96 (accesso, correzione, cancellazione, opposizione al trattamento, indicazione delle finalità del trattamento).

La comunicazione potrà pervenire via:

e-mail **variazioni@iir-italy.it** - fax **02.83.847.262-224** - tel. **02.83.847.634**

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Il sottoscritto, preso atto dell'informativa sopraesposta, che dichiara di avere letto in ogni sua parte, per quanto riguarda il trattamento dei propri dati personali per finalità di informazione e promozione commerciale, di studi statistici di ricerche di mercato:

dà il proprio consenso non dà il proprio consenso

alla comunicazione degli stessi dati alle categorie di soggetti indicati al punto 3) della predetta informativa (società del gruppo di appartenenza - collegate o controllanti);

alla comunicazione degli stessi dati ai soggetti indicati al punto 3) della predetta informativa (società terze).

Il presente consenso è subordinato al rispetto, da parte del Titolare del trattamento, della vigente normativa.

data _____ firma del Partecipante _____



Istituto di Ricerca Internazionale
The World's Leading Business Information Company