

LA TECHNOLOGY TRANSFER PRESENTA

KEN
VAN WYK

IDS/IPS

Intrusion Detection

using Snort

ROMA 15-17 NOVEMBRE 2010
VISCONTI PALACE HOTEL - VIA FEDERICO CESI, 37



info@technologytransfer.it
www.technologytransfer.it

DESCRIZIONE

Oggi nelle aziende gli ambienti di Data Processing sono grandi, distribuiti e altamente complessi. Monitorare e mantenere la sicurezza in questi ambienti eterogenei è un job molto complesso. Inoltre ad esasperare il problema ci pensano i vendors di prodotti di sicurezza che bombardano gli IT Managers con i propri slogan promettendo prodotti miracolosi.

Questo workshop esaminerà, con sguardo neutrale, le tecnologie esistenti e le loro reali capacità. Verranno comparate molte tipologie di IDS (Intrusion Detection Systems) e di IPS (Intrusion Prevention Systems) fornendo un apprezzamento realistico su cosa ci si possa aspettare da questi prodotti negli ambienti di produzione. Vi verrà spiegato con precisione cosa questi prodotti fanno e come lo fanno. Verranno esaminati i tipi di attacchi che questi prodotti fronteggiano e perché alcuni prodotti sono più indicati per fronteggiare particolari categorie di attacchi.

In particolare il seminario:

- Definisce chiaramente come le tecnologie e i prodotti IDS/IPS lavorano
- Descrive in maniera esaustiva i tipi di sfida che verosimilmente si incontrano quando si impiegano i prodotti IDS/IPS
- Esamina le architetture distribuite IDS/IPS e spiega come operano
- Descrive in maniera realistica i tipici attacchi alla sicurezza, come operano e come potrebbero (o non potrebbero) essere individuati dalle tecnologie IDS/IPS
- Spiega come IDS/IPS possano essere importanti nel fornire un valido input ad un programma di Incident Response

PARTECIPANTI

Il seminario si rivolge a tutti i Professionisti di Sicurezza IT che hanno la necessità di capire sino in fondo i sistemi IDS/IPS senza essere influenzati dai vendors.

PREREQUISITI

- Conoscenza dei fondamentali di TCP/IP
- Conoscenza dei sistemi di data processing e delle architetture di network

Si ricorda ai partecipanti di portare il laptop. Configurazioni raccomandate:

- Windows, Linux o Mac OS X
- 2 Gb RAM
- Privilegi amministrativi per installare e configurare software
- Circa 10 gigabytes di spazio sul disco
- Un ambiente virtual machine (ad esempio: VMware, Parallels, Virtual Box)

1. Comprensione del problema

- Panoramica degli attacchi e dei metodi più comuni
- Capire la necessità per IDS e IPS
- Come IDS/IPS si sono evoluti
 - Gli algoritmi usati per la detection
 - Soluzioni basate su network
 - Soluzioni basate su host
 - Punti di forza e di debolezza
- Uno sguardo alle architetture distribuite ed altamente eterogenee IDS/IPS di oggi

2. Survey dei prodotti di oggi

- Riflettori sui prodotti più popolari
- Soluzioni di monitoring distribuite ed eterogenee

3. Attacchi ed esercitazioni sui tools di attacco a livello sistema e network

- Discussione, dimostrazione ed esercizi sulle più comuni debolezze dei sistemi e i corrispondenti attacchi
- I partecipanti installeranno e proveranno molti tools di attacco (free e Open Source)
- Discussione sulla fattibilità e sfide associate all'individuazione di ciascun tipo di attacco

4. Attacchi ed esercitazioni sui tools di attacco a livello applicazione

- Discussione, dimostrazione ed esercizi sulle più comuni debolezze dei sistemi e i corrispondenti attacchi

- I partecipanti attaccheranno una applicazione difettosa in un ambiente sicuro sui propri laptops
- Discussione sulla fattibilità e sfide associate all'individuazione di ciascun tipo di attacco

5. IDS tools in azione

- Discussione, dimostrazione ed esercizi sull'installazione e il funzionamento di un popolare prodotto IDS Open Source
- I partecipanti installeranno e useranno un semplice sistema Open Source di network Intrusion Detection sui propri laptops
- Discussione di caratteristiche, punti di forza e di debolezza

6. Considerazioni a livello applicativo

- Il ruolo che le applicazioni possono e dovrebbero giocare in una strategia IDS/IPS
- Web Application Firewalls e come lavorano
 - Pro e contro di queste tecnologie

7. Trabocchetti nel mondo reale da capire e evitare

- Uno sguardo realistico alle complessità di un data center che possono mettere in difficoltà IDS/IPS
- Gli errori più comuni e il modo di evitarli (quando è possibile)

8. Considerazioni sull'Incident Response

- Come un sistema IDS/IPS si dovrebbe interfacciare con il processo di Incident Response

- Diagnostica di sicurezza o Forensics
- Problematiche di gestione delle prove
- Usare un IDS in una operazione di Incident Response

9. Mettere tutto insieme

- Prossimi passi da fare nel costruire un programma aziendale IDS/IPS

INFORMAZIONI

<p>QUOTA DI PARTECIPAZIONE</p> <p>€ 1500 (+iva)</p> <p>La quota di partecipazione comprende documentazione, colazioni di lavoro e coffee breaks.</p> <p>LUOGO</p> <p>Roma, Visconti Palace Hotel Via Federico Cesi, 37</p> <p>DURATA ED ORARIO</p> <p>3 giorni: 9.30-13.00 14.00-17.00</p> <p>È previsto il servizio di traduzione simultanea</p>	<p>MODALITÀ D'ISCRIZIONE</p> <p>Il pagamento della quota, IVA inclusa, dovrà essere effettuato tramite bonifico, codice Iban: IT 34 Y 03069 05039 048890270110 Banca Intesa Sanpaolo S.p.A. Ag. 6787 di Roma intestato alla Technology Transfer S.r.l. e la ricevuta di versamento inviata insieme alla scheda di iscrizione a:</p> <p>TECHNOLOGY TRANSFER S.r.l. Piazza Cavour, 3 00193 ROMA (Tel. 06-6832227 Fax 06-6871102)</p> <p>entro il 2 Novembre 2010</p> <p>Vi consigliamo di far precedere la scheda d'iscrizione da una prenotazione telefonica.</p>	<p>CONDIZIONI GENERALI</p> <p>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.</p> <p>SCONTI DI GRUPPO</p> <p>Se un'azienda iscrive allo stesso evento 5 partecipanti, pagherà solo 4 partecipazioni. Chi usufruisce di questa agevolazione non ha diritto ad altri sconti per lo stesso evento.</p> <p>ISCRIZIONI IN ANTICIPO</p> <p>I partecipanti che si iscriveranno al seminario 30 giorni prima avranno uno sconto del 5%.</p>	<p>TUTELA DATI PERSONALI</p> <p>Ai sensi dell'art. 13 della legge n. 196/2003, 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. 196/2003.</p>
---	--	---	---

KEN VAN WYK
IDS/IPS
INTRUSION DETECTION
USING SNORT

Roma 15-17 Novembre 2010
Visconti Palace Hotel
Via Federico Cesi, 37

Quota di iscrizione:
€ 1500 (+iva)

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

È previsto il servizio di traduzione simultanea

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



DOCENTE

Ken Van Wyk è un riconosciuto esperto di Information Security di fama internazionale con oltre 20 anni di esperienza, autore del libro “**Incident Response and Secure Coding**”. È columnist di eSecurityPlanet e Visiting Scientist al Software Engineering Institute della Carnegie Mellon University. Ha più di 20 anni di esperienza nel settore dell'IT Security, ha operato a livello accademico, militare e nei settori commerciali. Ha occupato posizioni tecniche prestigiose alla Tekmark, Para-Protect, SAIC oltre che al Dipartimento della Difesa e alle Università di Carnegie Mellon e Lehigh. È stato membro e chairman del comitato esecutivo di FIRST (Forum of Incident Response and Security Teams) ed è stato uno dei fondatori di CERT® (Computer Emergency Response Team).