

SICUREZZA DELLE RETI WIRELESS ED ETHICAL HACKING

UNA TRATTAZIONE SISTEMATICA ED APPROFONDIRITA DI STRUMENTI E TECNICHE PER IMPLEMENTARE WLAN SICURE

COD: SPSW3

Un corso avanzatissimo per acquisire una volta per tutte solide basi con cui affrontare e vincere i rischi legati alle reti non cablate

In un contesto come quello odierno in cui la diffusione delle reti senza fili avviene sempre più rapidamente ed il loro impiego riguarda tutte le tipologie di utilizzatori, dalle piccole realtà domestiche alle vaste infrastrutture multinazionali, il ruolo delle WLAN è al tempo stesso strategico e cruciale. L'integrazione delle reti wireless con le LAN cablate e con Internet da un lato ne moltiplica l'utilità, mentre dall'altro espone l'intero network a tutti i potenziali rischi di attacchi malevoli.

Risulta evidente l'importanza di saper riconoscere il grado di esposizione di una rete, essere in grado di valutarne tutti i punti deboli ed avere competenze sufficienti per predisporre le adeguate contromisure, sfruttando le tecnologie già disponibili ed implementando i protocolli standard per la gestione di sicurezza e riservatezza.

Il corso SPRING SPSW3

Il corso SPRING SPSW3 nasce per rispondere a questo tipo di esigenze: nell'arco delle tre intensive giornate, analizza nel dettaglio dapprima le tecnologie e le architetture WLAN allo stato dell'arte per poi passare in rassegna tutte le principali tecniche di intrusione, attacco o comunque di interazione malevola con la rete wireless; infine descrive e spiega accuratamente le tecniche per implementare la sicurezza in una rete wireless. Il corso ha un taglio teorico-pratico e contempla una serie di esercitazioni di laboratorio nel corso delle quali, fra l'altro, verranno replicate fedelmente le fasi di un attacco: si procederà partendo dalla implementazione di una rete WiFi, alla descrizione dell'hardware/software impiegato negli attacchi, alle attività di mappatura/discovery e site-surveying e, infine, all'analisi delle vulnerabilità sfruttate durante l'attacco.

Note per i laboratori:

- Verrà realizzata una rete wireless 802.11, si implementeranno i principali concetti visti durante le lezioni teoriche e si realizzeranno alcuni attacchi noti in letteratura.
- Ad ogni partecipante verrà distribuito un Live CD contenente una versione di Linux creata ad hoc con i principali tools impiegati da un hacker.
- Ogni partecipante dovrà essere dotato di notebook con lettore CDROM e scheda di rete wireless (preferibilmente con chipset Atheros o Intel).



Durata

3 giorni

A chi è rivolto

Questo corso è rivolto agli IT manager, ai security manager, agli amministratori di WLAN nonché ai responsabili di CED ed al personale IT che devono fronteggiare problematiche relative alla sicurezza dei sistemi wireless. Può essere inoltre un prezioso ausilio per i progettisti di reti, System Integrator, e per tutti i tecnici specialistici che vogliono acquisire competenze solide ed aggiornate per integrare la sicurezza nelle proprie realizzazioni.

Prerequisiti

Non sono indispensabili prerequisiti specifici per accedere al corso, tuttavia una conoscenza di base dei protocolli e delle architetture di reti Wi-Fi e dei concetti fondamentali di crittografia e network security costituiscono il presupposto per una più profonda comprensione degli argomenti trattati, soprattutto in funzione della loro applicazione nella realtà concreta.

Costo

1.500,00 €+ I.V.A.

Per saperne di più

Per maggiori informazioni, e per conoscere il calendario delle prossime sessioni di questo come di altri corsi, visitate il sito: www.spring-italy.it

Programma del corso SPRING SPSW3

1° GIORNO

9.00 Wireless LAN: architetture e protocolli

- Componenti dell'architettura di una rete wireless
- Analisi dei protocolli 802.11a, 802.11b, 802.11g, 802.11n
- Caratteristiche tecniche degli Access Point per una rete sicura
- Caratteristiche tecniche dei client wireless per una rete sicura
- Concetti sulle Antenne
- Localizzazione di una Wireless LAN
- Le reti chiuse
- Frequenze e regolamentazioni
- Hot spot pubblici e obbligo delle misure minime di sicurezza

I problemi di sicurezza delle wireless LAN

- I pilastri della sicurezza informatica
- I punti deboli dello standard 802.11
 - L'intercettazione delle comunicazioni
 - L'interruzione del servizio
 - L'accesso non autorizzato alle reti
 - Autenticazione
 - Algoritmi di crittografia
- Il fenomeno del wardriving e del warchalking
- Le principali tecniche di difesa
- Le infrastrutture di rete sicura: Firewall, IDS, IPS
- Le policy di sicurezza

13.00 Colazione di lavoro

14.30 Sicurezza dell'accesso: l'autenticazione

- Metodi di Autenticazione
 - Open System Authentication
 - Shared Key Authentication
 - Il Captive Portal
- Architettura IEEE 802.1x
- La famiglia di protocolli Extensible Authentication Protocol (EAP)
- 802.1x applicato alle Wireless LAN
- Il ruolo del Server Radius nell'autenticazione basata su EAP e 802.1x
- Autenticazione tramite: LEAP, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS
- Analisi del TLS su EAP
- Analisi del CISCO Light EAP (LEAP)

2° GIORNO

9.00 Riservatezza e integrità delle comunicazioni

- La riservatezza dei dati

- Algoritmi a chiavi simmetriche
- Algoritmi a chiavi asimmetriche
- Principi base della crittografia
- Certificati e Autorità di certificazione
- Virtual Private Networks (VPN)
 - Implementazione di IPsec nelle Wireless LAN
 - Session security: il protocollo SSL/TLS
- Gli algoritmi di cifratura nelle reti 802.11
 - Il protocollo Wired Equivalent Privacy (WEP)
 - Chiavi WEP statiche e dinamiche
 - Limiti e vulnerabilità della crittografia WEP
 - Centralized Encryption Key Server
 - Evoluzione del WEP: Wi-Fi Protected Access (WPA)
 - Temporary Key Integrity Protocol (TKIP)
 - Differenze con il WEP
 - Vulnerabilità del TKIP
 - Il WPA2
 - Advanced Encryption Standard (AES)
 - Counter Mode with CBC-MAC Protocol (CCMP)
 - WPA/WPA2 Personal - implementazione e configurazione

13.00 Colazione di lavoro

14.30 RSN – Robust Security Network

- Introduzione a IEEE 802.11i
- Architettura di RSN
- Gerarchia e generazione delle chiavi
 - Pair wise Keys e Group Keys
- Distribuzione e aggiornamento delle chiavi
 - 4-Way Handshake
 - Group Key Handshake
- Coesistenza dei protocolli di cifratura
- Tecniche di Fast BSS Transition (FT)

Introduzione al Wireless Hacking

- Ethical Hacking
- Social Engineering
- Attacchi noti: review tecnica
 - Scanning Attivo e Passivo
 - Man-in-the-middle
 - MAC Address spoofing
 - ARP poisoning
 - Denial of service
 - Jamming
 - AP overloading (Association Flooding, Authent. Flooding)
 - Rogue e Fake AP

- WEP cracking
- Attacchi "Brute Force"
- Hardware per il wireless hacking
- Software per il wireless hacking

3° GIORNO

9.00 Progetto, implementazione e verifica della sicurezza nelle WLAN

- L'approccio "Tiered Protection" nel progettare la sicurezza delle WLAN
 - Progettare una Wireless DMZ
 - Implementare autenticazione e controllo dell'accesso
 - Cifrare le comunicazioni
 - Implementare i filtri
 - Controllo della copertura radio e verifica dell'intensità del segnale
 - Analisi della rete e network mapping
- Configurazione di Access Point e client con chiavi WEP
- Configurazione di Access Point e Client con WPA Preshared Key
- Configurazione di un Server Freeradius con autenticazione basata su EAP-TLS

Esempi di Wireless Hacking

- Anatomia di un Attacco
 - Sniffing
 - Acquisizione del SSID
 - Acquisizione degli indirizzi IP
 - Port Scanning
 - MAC spoofing
 - Cracking delle chiavi WEP/WPA
 - Attacco DoS
 - Jamming: uso dei generatori di segnale
- Wireless Intrusion Detection
- WLAN controller
- RF Watermarking
- HoneyNet

13.00 Colazione di lavoro

14.30 Metodologie e standard per il Wireless Security Testing

- Vulnerability Assessment e Penetration Test
- Il wireless security auditing
- Gli standard di riferimento
 - ISO 17799
 - SSE-CMM
 - OSSTMM
- Errori comuni nel Wireless Security Testing
- Il report di un Wireless Security Testing
- Redigere le Wireless Security Policy

WIRELESS SECURITY

SPRING S.a.s.

Via C. Finocchiaro Aprile, 14 - 20124 Milano
tel. +39 02 620 227 218 Fax +39 02 659 5913

www.spring-italy.it - info@spring-italy.it

Per iscriversi al Corso SPRING SPSW3 stampare e compilare il modulo presente ed inviarlo al **FAX: 02 659 5913**

Desidero partecipare al Corso SPRING SPSW3 sulla Sicurezza delle Reti Wireless

Nome

Cognome

Società Settore di attività

Via N°

CAP Città Prov.

Tel Fax e-mail

Codice Corso: **SPSW3** Sede: Data:

Fatturare a:

Azienda (se diversa dall'intestazione)

Indirizzo
.....

C.F. /P. IVA

Il pagamento dell'importo totale di € 1.800,00 (€ 1.500,00 + IVA 20%) sarà effettuato a ricevimento fattura tramite Bonifico Bancario su:

Banca Intesa Filiale di Rho (MI) CIN C ABI 03069 CAB 20502 C/C n° 612005655981
Intestato a: SPRING S.a.s.

La quota di partecipazione comprende quanto indicato nella descrizione del corso, la colazione di lavoro ed i coffee break.
Le iscrizioni ed il pagamento devono pervenire, in ogni caso, almeno quindici giorni lavorativi prima della data d'inizio del corso; le iscrizioni eseguite oltre tale data limite sono accettate salvo disponibilità di posti e devono essere accompagnate dalla fotocopia del bonifico bancario.
SPRING S.a.s. si riserva il diritto di annullamento dei corsi programmati. In caso di annullamento si impegna a rimborsare integralmente la quota versata per la partecipazione al corso annullato. L'esercizio del diritto di recesso unilaterale da parte del Cliente almeno dieci giorni lavorativi prima della data di inizio del corso non determina a suo carico alcuna penale. Trascorso tale termine il Cliente dovrà corrispondere a SPRING, a titolo di penale, salvo il maggior danno, un importo equivalente al 60% del corrispettivo concordato per la partecipazione al corso; nel caso la quota sia stata già versata, sarà trattenuta su quanto ricevuto.

Ai Sensi della legge 675/96 autorizzo SPRING S.a.s. a trattare i dati sopra riportati per la realizzazione delle proprie attività istituzionali, compresa la comunicazione, l'informazione e la promozione.

.....
Data

.....
Firma