

TECNICHE E METODOLOGIE PER AFFRONTARE LA WIRELESS (IN)SECURITY

COD: **BBFSW3**

Un corso utilissimo per acquisire le informazioni e le tecniche necessarie per controllare tutti i rischi legati all'utilizzo delle reti non cablate

La diffusione delle reti senza fili, grazie anche ai più recenti sviluppi della tecnologia, avviene a ritmi sempre più alti e in tutti gli ambiti applicativi, dalle piccole realtà domestiche alle vaste infrastrutture industriali. Ma se l'integrazione delle reti wireless con le LAN cablate moltiplica l'utilità, la versatilità e la flessibilità della rete, nello stesso tempo può esporre l'intero network a una serie di rischi di nuova natura.

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 BBFSW3

Il corso SPRING BBFSW3 nasce per rispondere a questo tipo di esigenze: nell'arco di 18 ore distribuite in 3 giornate, analizza le tecnologie e le architetture WLAN più recenti con particolare riferimento alle caratteristiche e ai protocolli per la sicurezza, per poi passare in rassegna tutte le principali tecniche note di intrusione, attacco o comunque di interazione malevola con la rete wireless; infine descrive e spiega accuratamente le procedure da mettere in atto per implementare un elevato grado di sicurezza in una rete wireless. Il corso ha un taglio teorico-pratico e contempla una serie di esercitazioni di in aula nel corso delle quali, fra l'altro, verranno replicate le fasi di implementazione della rete e verranno simulate diverse situazioni di attacco e di difesa.

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.



Durata

18 ore su 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.

Costo

1.200,00 €+ I.V.A.

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

WIRELESS SECURITY

Programma del corso SPRING BBFSW3

1° GIORNO	2° GIORNO	3° GIORNO
<p>9.00 Wireless LAN: architetture e protocolli</p> <ul style="list-style-type: none"> • 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 <p>I problemi di sicurezza delle wireless LAN</p> <ul style="list-style-type: none"> • I punti deboli dello standard 802.11 <ul style="list-style-type: none"> - 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 <p>13.00 Colazione di lavoro</p> <p>14.00 Sicurezza dell'accesso: l'autenticazione</p> <ul style="list-style-type: none"> • Metodi di Autenticazione <ul style="list-style-type: none"> - 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) 	<p>9.00 Riservatezza e integrità delle comunicazioni</p> <ul style="list-style-type: none"> • La riservatezza dei dati • Principi base della crittografia • Certificati e Autorità di certificazione • Virtual Private Networks (VPN) <ul style="list-style-type: none"> - Implementazione di IPsec nelle Wireless LAN - Session security: il protocollo SSL/TLS • Gli algoritmi di cifratura nelle reti 802.11 <ul style="list-style-type: none"> - Il protocollo Wired Equivalent Privacy (WEP) - Limiti e vulnerabilità della crittografia WEP - Centralized Encryption Key Server - Wi-Fi Protected Access (WPA) - Temporary Key Integrity Protocol (TKIP) - WPA2 - Advanced Encryption Standard (AES) - Counter Mode with CBC-MAC Protocol (CCMP) - WPA/WPA2 <p>12.00 Colazione di lavoro</p> <p>13.00 RSN – Robust Security Network</p> <ul style="list-style-type: none"> • Introduzione a IEEE 802.11i • Architettura di RSN • Gerarchia e generazione delle chiavi • Distribuzione e aggiornamento delle chiavi • Coesistenza dei protocolli di cifratura • Tecniche di Fast BSS Transition <p>Introduzione al Wireless Hacking</p> <ul style="list-style-type: none"> • Attacchi noti: review tecnica <ul style="list-style-type: none"> - 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" • H/W e S/W per il wireless hacking 	<p>9.00 Progetto, implementazione e verifica della sicurezza nelle WLAN</p> <ul style="list-style-type: none"> • L'approccio "Tiered Protection" nel progettare la sicurezza delle WLAN <ul style="list-style-type: none"> - 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 <p>12.00 Colazione di lavoro</p> <p>13.00 Esempi di Wireless Hacking</p> <ul style="list-style-type: none"> • Anatomia di un Attacco <ul style="list-style-type: none"> - 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 <p>Metodologie e standard per il Wireless Security Test.</p>

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