



DOCENTE
Professionista esperto di
IT Security

La sicurezza delle Applicazioni Web

Verificare la sicurezza delle applicazioni web, apprendendo le principali minacce incombenti ed acquisendo le nozioni per le opportune contromisure

(cod. corso IT03SAW)

Destinatari

IT Manager
Responsabile Sicurezza
Informatica
Tecnico di Sicurezza
Informatica
Analista e Sviluppatore di
Applicazioni Web

Obiettivi

Utilizzare gli opportuni strumenti per verificare la sicurezza delle applicazioni web, degli application server e dei sistemi operativi

Ottimizzare il livello di sicurezza dei propri sistemi e delle applicazioni ed evitare il superamento delle barriere di protezione

Considerare i bug dei sistemi operativi, dei dispositivi di rete, ed i difetti di programmazione delle applicazioni web

Esercitarsi concretamente nelle verifiche sulla sicurezza e nell'allestimento delle opportune misure correttive.

Prerequisiti: conoscenze base di sistemi operativi e di networking;

Prima giornata

8.45 Registrazione dei partecipanti

9.00 Introduzione

- Cosa occorre proteggere?
- La normativa internazionale ISO/IEC 27001
- Le vulnerabilità più comuni
- Risk Analysis
- Statistiche sui Security Incidents

10.00 Elementi costitutivi di un'applicazione web

- Stratificazione fisica di un sistema web
- Il protocollo HTTP

10.45 Coffee break

11.00 I rischi inerenti i servizi web

- SQL Injection
- Buffer overflow
- Cross-Site Scripting
- Cookie poisoning

12.00 ESERCITAZIONE PRATICA: simulare alcune casistiche di vulnerabilità di applicazioni web tra quelle illustrate.

I partecipanti, con la guida del docente, simuleranno alcuni esempi di vulnerabilità tra quelle illustrate mettendo in luce ed attuando le strategie per prevenirle

13.00 Colazione di lavoro

14.00 Il Firewall di rete nella protezione dell'applicazione Http

- Caratteristiche generali
- Metodologie di funzionamento
- Soluzioni architetturali
- Tipologie di firewall esistenti

15.00 ESERCITAZIONE PRATICA: configurazione di un Firewall Open Source: IPTables per Linux

15.45 Tea break

16.00 Il Firewall Applicativo o Proxy Server

- Il proxying
- Metodologie di funzionamento
- Soluzioni Architetture
- Tipologie di proxy esistenti

17.00 ESERCITAZIONE PRATICA: configurazione di un Proxy Open Source: Squid per Linux

17.45 Conclusione della prima giornata

Seconda giornata

8.45 Registrazione dei partecipanti

9.00 La riservatezza delle informazioni

- Confidenzialità e riservatezza delle informazioni
- Tecniche crittografiche
- Crittografie a chiave simmetrica e asimmetrica

10.00 ESERCITAZIONE PRATICA: applicazioni di tecniche crittografiche per la riservatezza dei dati

10.45 Coffee break

11.00 ESERCITAZIONE PRATICA: installazione di un Web Server Apache su Linux

12.00 **CASE STUDY: implementazione del protocollo SSL su Linux/Apache con OpenSSL**
Verrà illustrata la procedura per allestire un'infrastruttura per una web application basata su protocollo Secure Socket Layer

13.00 Colazione di lavoro

14.00 ESERCITAZIONE PRATICA: creazione di un tunneling SSH per un trasferimento sicuro di dati

Verrà utilizzato Putty come client SSH realizzando un canale attraverso cui far viaggiare dati sicuri crittografati a livello applicativo con SSH verso un SSH Server

15.00 Configurazione del sistema e del software

- La configurazione predefinita, il rischio maggiore
- L'aggiornamento del sw una necessità assoluta

15.45 Tea break

16.00 Messa in sicurezza di un sistema Windows

- Service Pack ed Hot Fixes
- Meccanismi di sicurezza per gli utenti

17.00 Messa in sicurezza di un sistema Linux

- Installazione delle patch correttive
- Gestione delle utenze

17.45 Conclusione della seconda giornata

Terza giornata

8.45 Registrazione dei partecipanti

9.00 I Vulnerability Detection Systems (VDS)

- Loro utilizzo per il monitoring della sicurezza delle applicazioni web
- Panoramica degli strumenti freeware
- Panoramica degli strumenti commerciali
- I Web Server Vulnerability Scanner (WSVS)
- Esempi di WSVS

10.45 Coffee break

11.00 CASE STUDY: le principali vulnerabilità dei sistemi

Momento di riflessione riguardante i casi proposti dai partecipanti: verranno prese in considerazione le vulnerabilità principali solitamente riscontrate con i Vulnerability Detection Systems e le possibili contromisure da adottare

12.00 **ESERCITAZIONE PRATICA:** Utilizzo di uno strumento di Vulnerability Detection per l'analisi delle vulnerabilità di un sistema su cui risiede una web application

13.00 Colazione di lavoro

14.00 Principio dello sviluppo protetto

- Sicurezza di sviluppo, quale budget occorre prevedere?
- Quando integrare la sicurezza nel ciclo di sviluppo?
- Quali regole rispettare nello sviluppo?
- Il controllo dei dati inviati dall'utente, la base della protezione

15.00 L'autenticazione degli utenti

- Connessione anonima e autenticazione applicativa
- Digest Access Authentication Scheme
- Gli attacchi alle password
- RSA Secure ID, un alternativa alle password
- L'Identity & Access Management (IAM)

15.45 Tea break

16.00 Gli IDS Intrusion Detection Systems

- Loro utilizzo per la prevenzione di attacchi alle web application
- Tipologie e soluzioni architetturali
- Panoramica sugli IDS commerciali e freeware

17.00 **ESERCITAZIONE PRATICA:** Utilizzo dell' IDS Snort nel monitoraggio di una DMZ con un web server

17.45 Conclusione del corso e consegna degli attestati