

Pragmatic Security: Attacks and Defense

Obiettivi del Corso

IMPARARE A GESTIRE ED ATTUALE LA SICUREZZA

Il corso mira alla sistematizzazione delle competenze di personale già avvezzo all'utilizzo ed alla gestione di asset tecnologici aziendali. Obiettivo della formazione è la sensibilizzazione alle dinamiche ed alle tecnologie alla base della gestione, della implementazione e del controllo della sicurezza in ambito della PMI.

Vengono affrontate con scenari reali ed addestramento "hands-on" tutte le principali tecniche intrusive, in modo da poter efficacemente esemplificare le strategie di protezione ed aiutare nella stesura ed implementazione di policy e infrastrutture atte al controllo ed alla mitigazione.

Il destinatario ideale del corso è il sistemista aziendale, il direttore della sicurezza aziendale, chi sia stato segnalato per ricoprire posizioni in cui sia necessaria una approfondita conoscenza delle dinamiche intrusive e cautelative.

COMPETENZE NECESSARIE

Per comprendere efficacemente i temi trattati è necessaria una esperienza diretta della gestione ed implementazione di infrastrutture di utilizzo comune negli ambienti della PMI. In particolar modo è necessaria una conoscenza di medio livello nelle dinamiche di installazione, gestione, e configurazione di apparecchiature di rete, di sistemi operativi e di eventuali appliance dedicate.

La conoscenza dei sistemi Unix/Linux, sebbene non sia considerata un prerequisito, è fortemente consigliata.

I Docenti

ING. YVETTE AGOSTINI

Laureata in ingegneria ha collaborato con grandi aziende del settore energetico e dei servizi, prima di dedicarsi alla consulenza nel campo della sicurezza delle informazioni. In questa veste si è occupata di incident handling, IT forensics, biometria, penetration testing, certificazioni BS7799-2 (ora ISO27001) presso aziende di telecomunicazioni e bancarie.

L'esperienza tecnica e la capacità di analisi dell'organizzazione e dei suoi processi le conferiscono una visione olistica della sicurezza delle informazioni.

Collabora saltuariamente con riviste del settore, e partecipa come relatrice ad eventi di formazione e didattica.

MATTEO G.P. FLORA

Svolge l'attività di Security Auditor. Perito Forense e Consulente Tecnico delle autorità di Polizia Giudiziaria come Freelance ed è Presidente Provinciale per Milano e Lodi di AIP. Dal Maggio 2006 Direttore Tecnico e Scientifico dell'Osservatorio Italiano Permanente Privacy e Sicurezza Informatica di AIP e coordinatore dell'Osservatorio Permanente sull'Accessibilità di AIP.

Ha tenuto seminari di Crittografia a Chiave Pubblica e Privata presso l'Università di Milano e i Master di Comunicazione d'Impresa di Publitalia '80. E' stato inoltre ideatore, coordinatore e docente del primo Corso italiano su Virus e Sicurezza Informatica, oltre che di importanti edizioni di corsi e seminari di Computer Forensics per professionisti e forze dell'ordine.

Insieme al M.llo Gerardo Costabile e altri importanti esperti ha scritto il volume "Sicurezza e Privacy: dalla carta ai bit" in stampa presso l'editrice Experta (Forlì). E' stato ospite di programmi radiofonici e di diverse puntate del Maurizio Costanzo Show, oltre che del TG3, della trasmissione RAI Scenari e di varie edizioni del TG5.

FABIO PIETROSANTI

E' stato Network Security Manager presso I.NET, gruppo BT Ignite ed attualmente riviste l'incarico di Security Evangelist presso Khamsa. Segue professionalmente i temi della sicurezza dal '98.

Si occupa da anni di ricerca e implementazione di soluzioni di security, Penetration Testing, Forensic Analysis e Network Planning.

Si interessa di sicurezza delle tecnologie wireless negli aspetti di attacco e difesa delle infrastrutture, intervenendo spesso su questi temi presso convegni e università. Ha realizzato assieme a Yvette Agostini, ha realizzato una "storica" indagine sulla sicurezza delle reti WLAN a Milano.

Scriva articoli tecnici per diverse riviste di settore e partecipa come relatore a numerosi eventi, ufficiali e underground, sui temi della sicurezza informatica.

Giornata 1: Teoria

ELEMENTI DI TEORIA DELLA SICUREZZA INFORMATICA

- **Elementi basilari di analisi del rischio**
- **Elementi basilari di minacce IT**
 - Scalata di privilegi
 - Social Engineering
 - Attacchi alle Password
 - Web Application Attacks
 - VoIP Attacks
 - DDos
 - Abuso di risorse di rete
 - Mitm
 - Wifi Attacks
 - Clientside attacks

Giornata 2: Pragmatical Attacks

DIMOSTRAZIONI HANDS-ON SU WIFI E WEB

- **Testing WiFi**
- **Webapplication Testing**

Giornata 3: Pragmatical Attacks

DIMOSTRAZIONI HANDS-ON

- **DoS**
- **Attacchi alle Password**
- **Mitm**
- **Clientside Attack**

Giornata 4: Pragmatical Defense TECNOLOGIE, METODOLOGIE E BEST-PRACTICE

- **Tools di scansione automatizzata**
- **Tecnologie di difesa**
 - Prevenzione
 - Perimetro (*firewall, ids, antivirus, vpn, ecc*)
 - Audit degli applicativi
 - Politiche di Sicurezza (*gestione password, accessi internet, risorse*)
 - Tools di Integrità
 - Hardening
 - Controllo
 - Log: architetture e monitoraggio
 - Verifiche periodiche
 - Enforcing password
 - Pentest e vulnerability assessment
 - Patching
 - Misure di Contenimento
- **Incident handling**
 - **Individuazione**
 - Analisi delle Segnalazioni (*automatica, manuale, su richiesta*)
 - **Mitigazione**
 - **Follow up**
 - Chi contattare
 - Gestione delle evidenze