Effettuare il Penetration Test di reti LAN e WLAN

CORSO – (15 e 22 giugno 2016)

APERTURA ISCRIZIONI DAL 16/05/2016 ore 9.30

La scheda di preiscrizione dovrà essere compilata esclusivamente dal seguente link:
http://www.ordineingegneri.fi.it/contents/evento_2016-06-15_22_CorsoPenetrationReti.php

Per l'iscrizione on.line sono richiesti i seguenti dati:

Cognome e Nome
Titolo (Ing. Arch…)
Sezione (A o B)
iscritto all'Ordine della Provincia di
N. Iscrizione
cellulare
C.F. (personale)
Indirizzo e-mail
Intestazione per fatturazione - Indirizzo per fatturazione
P.IVA e C.F.

Quota di partecipazione: € 160,00 + IVA 22% (totale € 195,20)

Ai sensi dell'art.10 della D.Lgs. 196/03 La informiamo che il trattamento dei dati personali qui indicati, effettuabile anche con l'ausilio di mezzi elettronici esterni, è diretto solo all'attività in questione. I dati indicati per l'iscrizione verranno trasmessi allo sponsor salvo espresso diniego formulato all'atto dell'iscrizione

Segreteria Organizzativa: Ordine degli Ingegneri della Provincia di Firenze
Viale Milton 65 - 50129 Firenze - e-mail: info@ordineingegneri.fi.it

L'iscrizione verrà confermata con il pagamento della quota di partecipazione che dovrà essere effettuato entro 48 ore dalla registrazione a mezzo versamento **bonifico presso Banca Passadore intestato a Ordine Ingegneri Firenze: IBAN IT70 H 03332 02800 000002210920, nella causale "Corso 15 e 22/06/16" La ricevuta del bonifico dovrà essere inviata a: info@ordineingegneri.fi.it**
In caso di rinuncia alla partecipazione l'iscritto ha l'obbligo di darne comunicazione **almeno 4 giorni prima** dello svolgimento dell'evento. In mancanza di tale comunicazione non verrà restituita la quota di partecipazione e alla successiva iscrizione ad un evento formativo il partecipante verrà inserito in coda ed ammesso all'evento solo se rimangono posti disponibili.
L'Ordine degli Ingegneri valuterà, pochi giorni prima dell'evento, nel caso non si raggiunga il numero minimo di partecipanti, di annullare l'evento stesso, rimborsando la quota di iscrizione

Il corso sarà svolto al raggiungimento di minimo 12 partecipanti e le iscrizioni verranno chiuse al raggiungimento massimo di 40 partecipanti.

Agli ingegneri partecipanti saranno riconosciuti n° 16 CFP

ORDINE DEGLI INGEGNERI
DELLA PROVINCIA DI FIRENZE

organizza

Effettuare il Penetration Test di reti LAN e WLAN

CORSO

presso:

Ordine degli Ingegneri
Viale Milton 65 - Firenze

15 e 22 giugno 2016

NON SARANNO RICONOSCIUTI CFP NE' RILASCIATI ATTESTATI A CHI FIRMERA' IL REGISTRO D'INGRESSO DOPO L'ORARIO DI INIZIO DEGLI INTERVENTI PROGRAMMATI E QUELLO DI USCITA PRIMA DELL'ORARIO DI CONCLUSIONE INDICATO NEL PROGRAMMA E CHE NON SARA' PRESENTE PER TUTTA LA DURATA DEL CORSO
SARANNO RICONOSCIUTI CFP SOLO A COLORO CHE AVRANNO EFFETTUATO LA REGISTRAZIONE CON LE MODALITA' INDICATE

c.f.v.

Presentazione

DOCENTE
Ing. Gianluca Golinelli

Ingegnere elettronico, membro del C3I (Comitato Italiano Ingegneria dell'Informazione), board member di A3I (Associazione Italiana Ingegneri dell'Informazione), Coordinatore del Gruppo di lavoro di Informatica dell'Ordine degli Ingegneri della Provincia di Parma. Si occupa da anni di sicurezza informatica come consulente per aziende ed enti della Pubblica Amministrazione, per cui ha svolto attività di formazione e consulenza. Svolge inoltre attività di informatica forense in qualità di Consulente Tecnico di Parte e Consulente Tecnico d'Ufficio del Tribunale di Parma.

Destinatari
IT Manager
Responsabile Sicurezza Informatica
Tecnico di Sicurezza Informatica

Obiettivi
Difendersi adeguatamente dagli attacchi, comprendendo le tecniche di hacking utilizzate per penetrare nelle reti informatiche.
Ottimizzare il proprio livello di sicurezza ed evitare il superamento delle barriere di protezione
Considerare i bug dei sistemi operativi e dei dispositivi di rete per i quali esistono exploit che consento di ottenere accesso alle reti
Esercitarsi concretamente grazie alle simulazioni pratiche di Penetration Test

PROGRAMMA

Lezione del 15 giugno 2016
orario 9,00-13,00 14,00-18,00

Definire le fasi di un Penetration Test
- Introduzione: tipologie di Penetration Test
- Metodologie e standard, aspetti normativi
- La Suite Kali Linux

Individuare gli strumenti utilizzati dagli hacker per il footprinting della rete Target
- Analizzare alcuni tra i molteplici strumenti (ricerche Whois, Maltego, etc.):
  - per recuperare informazioni sull'organizzazione
  - per indagare sui domini
  - per recuperare informazioni sulla rete (indirizzi IP)
  - per la perlustrazione della rete

Interrogazione dei DNS
- Imparare ad utilizzare gli strumenti per interrogazione dei DNS: Nslookuo, Dig,etc
- Capire le vulnerabilità dovute ai trasferimenti di zona
- Analizzare i record A, MX, SRV, PTR
- Quali contromisure impiegare in questa fase

Identificazione dell'architettura della rete target
- Strumenti di tracerouting
- Tracert, e Traceroute
- Tracerouting con geolocalizzazione

Tecniche di Footprinting mediante motori di ricerca
- Footprinting con Google: utilizzo di campi chiave di ricerca
- Utilizzo di strumenti frontend per ricerche su motori: Sitedigger
- Footprinting su gruppi di discussione

ESERCITAZIONE PRATICA: simulare la fase di footprinting di una rete target
I partecipanti, con la guida del docente, simuleranno la fase di footprinting per esaminare quali informazioni è possibile reperire sulla rete target.

Introduzione alla fase di scansionamento delle reti
- Tipologie di scansionamento
- Aspetti legali inerenti lo scansionamento di porte
- TCP, UDP, SNMP scanners
- Strumenti Pinger
- Information Retrieval Tools
- Attuare contromisureagli scansionamenti

ESERCITAZIONE PRATICA: simulare la fase di scansionamento di una rete target

Introduzione alla fase di Enumerazione. Capire il funzionamento degli strumenti perl'enumerazione delle reti
- Enumerazione di servizi "comuni": FTP, TELNET, SSH, SMTP, NETBIOS, etc
- Enumerazione SNMP
- Ricercare le condivisioni di rete
- Ricerca di account di rete
- Conoscere le contromisure più efficaci per l'enumerazione

Lezione del 22 giugno 2016
orario 9,00-13,00 14,00-18,00

Conoscere l'Hacking dei sistemi per rendere sicure le reti
- Conoscere le principali tecniche di attacco ai sistemi
- Quali sono le principali tipologie di vulnerabilità Sfruttabili
- Ricerca di vulnerabilità inerenti i servizi rilevati nella fase di enumerazione:
  - Ricerca "Manuale"
  - I Vulnerability Scanner

ESERCITAZIONE PRATICA: Ricerca di Vulnerabilità in modo manuale e mediante Vulnerability Scanner

Comprendere l'Hacking dei sistemi operativi Microsoft Windows
- Hacking di Windows: le vulnerabilità più recenti
- Attacchi senza autenticazione
- Attacchi con autenticazione: scalata di privilegi (tecniche e tools)

ESERCITAZIONE PRATICA: effettuare la simulazione dell'hacking di un sistema Windows con Metasploit

Attacchi di tipo Man-In-The-Middle
- Dirottamento di sessioni
- Attacchi di tipo ARP Poisoning
- Tools per attacchi MitM: Cain&Abel

Comprendere l'Hacking del Web: hacking dei server web ed hacking delle applicazioni
- Identificare la tipologia del server web target
- Verificare le vulnerabilità di IIS e Apache
- Individuare vulnerabilità in applicazioni ASP, PHP, JSP
- Hacking mediante SQL Injection, Cross-Site Scripting, Cross-Site Request Forgery, etc
- Predisporre efficaci contromisure

ESERCITAZIONE PRATICA: effettuare l'hacking di un web server
Verrà simulato un tentativo di violazione di un sito web per verificarne la corretta configurazione in termini di sicurezza

Hacking di reti Wireless: le principali vulnerabilità
- Strumenti per effettuare la scansione delle reti wireless
- Packet Sniffer wireless, hacking di WEP, WPA e WPA2
- Strumenti di hacking delle WLAN inclusi in Kali Linux

Conclusione del corso