

HANDS ON HACKING UNLIMITED

Corso di ethical hacking

"La volpe sa molte cose ma il porcospino ne sa una importantissima."

Zone-h presenta Hands on Hacking Unlimited, il nuovo corso di ethical hacking destinato a security manager, responsabili IT, amministratori di rete e responsabili CED ed a tutti i professionisti che si occupano di sicurezza logica.

Nuova edizione Unlimited!

Questa nuova edizione del corso abbina i fondamentali dell'hacking con approfondimenti nelle aree di maggior criticità, fornendo un approccio completo alla problematica della sicurezza logica attraverso i percorsi del pensiero laterale proprio degli hacker. Il corso è dedicato a chi ha già acquisito i principi base dell'hacking ma anche a tutti coloro che avvicinandosi per la prima volta alla problematica desiderano disporre di un quadro di riferimento solido e di conoscenze pratiche approfondite.

Live hacking!

Punto focale del corso è la parte pratica, una serie di sessioni di live hacking dove, mediante l'esercitazione su casi reali, sarà possibile apprendere insight preziosissimi per la predisposizione di contromisure efficaci.

Hacking challenge

Al termine delle sessioni live hacking (effettuate su target proprietari) verrà assegnato un premio al partecipante più abile.

Esclusivo materiale a corredo!

Al termine del corso verranno forniti a tutti i partecipanti due utilissimi cd-rom: **The Ultimate Toolbox**: 450 strumenti di sicurezza per ambienti Windows e Linux e Exploit Yellow Pages, una vasta ed aggiornatissima collezione di exploit.



Durata

2 giornate

Quando

29/30 Settembre 2005

Dove

A Roma, in via Stanislao Cannizzaro 51

Come

Ogni partecipante avrà a disposizione un computer con doppio sistema operativo (Windows/Linux) connesso in rete ed a Internet.

Il corso verrà tenuto in lingua italiana; per gli interventi di docenti stranieri è prevista la traduzione contestuale. Alla fine del corso verrà rilasciato un attestato a tutti i partecipanti.

Iscrizione

Per partecipare al seminario compila il form che troverai a fondo pagina e riceverai tutto il materiale informativo.

Per maggiori informazioni

Telefono +39 06 40900256

Fax +39 06 40801892

E-mail corsict@didagroup.it



Prima giornata:

Introduzione generale alle problematiche relative all'hacking.

Strumenti per la raccolta di informazioni sul bersaglio (target)

- locali: scanners, fingerprints, etc.
- web-based: google, netcraft, visualroute, etc.

Extendend Network Mapping

Approfondimento:
analisi dettagliata delle tecniche da utilizzare per eseguire una accurata operazione di mappatura della rete da attaccare:

- Network mapping attivo e passivo
- DNS bruteforcing
- Zone Transfer

Raccolta informazioni su vecchie e nuove vulnerabilità

Proteggere la propria anonimità durante attività di hacking (shell, proxy)

Seconda giornata:

Introduzione all'utilizzo delle più note vulnerabilità in ambiente Windows

- Frontpage extension
- Il sempre presente Unicode
- Internet Explorer

Approfondimento: le più devastanti vulnerabilità in Internet Explorer. Come prendere possesso di un computer attraverso le vulnerabilità di IE. Tre esempi pratici su come utilizzare 3 diverse vulnerabilità per eseguire codice arbitrario su una macchina.

- Altri
- **Sessione live**

Attacchi al database

- SQL injection
- URL poisoning
- **Sessione live**

Black box hacking session

- Hacking an unknow Windows system
- Hacking an unknow Linux system
- Hacking an unknow OS system
- **Sessione live**

Attacco alla Wireless LAN: rischi e conseguenze

Wireless LAN

- Standard 802.11a/b/g

Danial of service

- RF Jamming
- Data flooding
- Hijacking

Unauthorized access

- Rogue Device
- Wlan Discovery
- Wep Setting
- SSID Setting
- MAC Filters

Encryption

- WEP/RC4
- Cracking WEP (Tutti i modi per crackare una chiave WEP)
- WPA
- WPA - PSK (Vulnerabilità & Cracking tool)
- 802.11i(WPA2/AES)

Rootkit

Trojan

Raccolta di informazioni sui vari target

- [Sessione live](#)

Struttura tipica di un sito web

- Analisi dei singoli componenti e dei possibili punti vulnerabili

Vulnerabilità

- Linee di comunicazione criptate
- Firewall e Router
- Webservice (Apache/IIS)
- Applicativi
- Database

Cross Site Scripting

Cos'è un exploit

Introduzione all'utilizzo delle più note vulnerabilità in ambiente Linux

- SSH
- SSL
- Apache
- Altri

- [Sessione live](#)

Aspetti teorici dei buffer overflow

System patching

Social engineering, tecniche e trappole psicologiche

In collaborazione con:



Tool utilizzati

- [Sessione live](#)

Profilo docenti

next2001 (Stefano Pisati)

The teacher...Membro di zone-h, seminarista e relatore universitario di lungo corso. Autore di numerosi articoli pubblicati su riviste di settore. Fondatore, partner e Chief Architect di una società operante nel settore della progettazione e realizzazione di soluzioni tecnologiche in ambito security per la media e grande azienda.

SecurityWireless (Luigi D'Amato)

Membro di zone-h, nonché fondatore del noto portale web di tecnologie wireless www.securitywireless.info. Il suo lateral thinking Vi mostrerà quanti modi ci sono per entrare nei sistemi. L'uomo giusto al quale fare tutte le domande sulla sicurezza delle reti wired e wireless.

