

HANDS ON HACKING 2



CORSO DI ETHICAL HACKING: LE APPLICAZIONI WEB



Argomenti

Zone-H presenta **Hands-on Hacking 2**, il corso di **ethical hacking** destinato ai **security manager** e **professionisti IT** dedicato agli **aspetti fondamentali della Internet security** e alle **nuove frontiere dell'hacking: le web application**.

Le statistiche dimostrano che....

Da anni si registra un incremento costante degli attacchi alle architetture web-based tanto da costituire oggi la modalità privilegiata. Dagli inizi del 2003 la maggior parte degli attacchi viene messa a segno utilizzando vulnerabilità legate a errori di configurazione delle applicazioni o a fattori intrinseci. La diversificazione e combinazioni possibili rendono gli attacchi ad una architettura web tipica sempre più efficaci e diffusi.

Hands on Hacking 2 nasce con l'intento di mostrare chiaramente come un attacco si possa risolvere nella compromissione di una qualsiasi delle componenti di una architettura web, firewall di protezione perimetrale, webserver, middleware, applicativi, database... Gli scopi? Diversificati, molto spesso il furto di identità...

Live hacking!

Il corso è composto di un parte teorica e di vari laboratori pratici: inserite all'interno di una vera e propria hacking challenge, 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.

Esclusivo materiale a corredo

Al termine del corso verrà fornito a tutti i partecipanti l'aggiornatissimo cd-rom "Security Repository", una vasta collezione di strumenti di sicurezza per Windows e Linux corredata da un'ampia e aggiornata raccolta di exploit specifici.

A chi è rivolto

Security manager, IT manager, amministratori di rete, responsabili CED, sviluppatori, personale IT.

Come

Ogni partecipante avrà a disposizione un computer 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 di frequenza.

Prerequisiti

Nozioni di programmazione di base.

Durata

2 giornate.

Dove

Presso le sedi NEST2 di Milano e Padova

Iscrizione e informazioni

Per maggiori informazioni telefonare allo 049 7386000

Dall'osservatorio
più autorevole
del crimine
informatico i corsi
di hacking etico
più esaustivi
e aggiornati



HANDS ON HACKING 2



CORSO DI ETHICAL HACKING: LE APPLICAZIONI WEB



Contenuti

Introduzione: statistiche sugli attacchi lato server

Il protocollo HTTP

La struttura di un web server

Attacchi alle applicazioni web: classificazione

Autenticazione
Autorizzazione
Esecuzione di comandi
Attacchi lato client
Information disclosure
Attacchi logici

Raccolta informazioni sul bersaglio

Gli strumenti offerti dai motori di ricerca

Live session

Cross Site Scripting in Depth

La spiegazione dettagliata di come una tecnica ritenuta banale come XSS consenta in realtà di ottenere risultati eccezionali
Come evitare questo tipo di attacchi

Live Session

Cookie Manipulation (cURL e Mozilla Firefox)

Live session

Backdoors with Javascript

Come installare backdoor utilizzando Javascript

Remote Files Reading/Inclusion I più comuni errori delle applicazioni PHP

Esecuzione di codice arbitrario
Esecuzione di comandi
File disclosure

Live session

SQL Injection (simple, blind, advanced)

Attaccare un sistema utilizzando vulnerabilità di SQL: Form bypassing, Database dump, altri

Live Session

Attacchi CSRF/XSRF (Cross Site Request Forgery)

Encoding Attacks

Bypassing IDS; filtering

Altre vulnerabilità

AJAX
XPath Injection
LDAP Injection

HTTP Response Splitting

Come modificare pacchetti HTTP

Miniguia alla programmazione sicura: 20 errori da evitare



HANDS ON HACKING 2



CORSO DI ETHICAL HACKING: LE APPLICAZIONI WEB



Team Docenti

Luigi D'Amato (SecurityWireless) – Italia

“The wireless expert”... Fondatore e admin del primo portale web di tecnologie wireless www.securitywireless.info, nonché membro di Zone-h. Certificato CWNA, Cisco CCNA e WLAN FE. L'uomo giusto al quale fare tutte le domande sulla sicurezza delle reti wireless.

Emanuele Mornini (matador) - Italia

IT Security analyst and researcher, conosciuto come “the buffer overflow expert”. Esperto di sicurezza e di penetration testing, ad oggi lavora presso una società estera di sicurezza informatica. Membro del team internazionale di docenza; ha una conoscenza profonda delle tecniche di Hacking e delle loro contromisure.

Gerardo Di Giacomo (Astarot) – Italia

Tra i cofondatori di Zone-H, si e' occupato dapprima dello sviluppo dello stesso per poi entrare nel gruppo di docenti dei corsi di sicurezza informatica che ha tenuto per conto di Zone-H sia a livello nazionale che internazionale. Dal 2005 e' a capo del team di sicurezza della release di Linux Ubuntu. Ad oggi è senior analyst presso una società multinazionale di sicurezza informatica.

Tonu Samuel - Estonia

Senior security analyst e ricercatore. L'attività quotidiana lo vede impegnato come consulente security nelle aree risk analysis, auditing, penetration testing, hardening infrastrutture. Autore di svariati advisory. Relatore Zone-H di lungo corso. Un esperto dal paradiso tecnologico d'Europa: l'Estonia.

Agris Krusts - Lettonia

Senior security consultant alla guida di società di consulenza lettone, punto di riferimento per la grande impresa e PA locali. Agris è forte di una esperienza decennale nel settore IT; l'attività svolta per Zone-H lo vede impegnato nel team di docenza internazionale. Parla fluentemente inglese e russo, oltre al lettone, la sua lingua madre.

Uldis Mikelsons - Lettonia

Docente Zone-H in ambito internazionale. L'attività quotidiana come internet security specialist gli garantisce una prospettiva ampia sulle tematiche di sicurezza della Rete. Profondo conoscitore ambienti Windows e *nix. Uldis parla correntemente inglese e russo, oltre al lettone, la sua lingua madre.

Boris Mutina - Slovacchia

Docente Zone-H in ambito internazionale, editor e supervisore del mirror Zone-H in slovacco. L'attività quotidiana lo vede impegnato come consulente security nelle aree risk analysis, auditing, penetration testing, hardening infrastrutture. Boris parla correttamente inglese e tedesco, oltre allo slovacco, la sua lingua madre.

Zone-H

Zone-H, osservatorio digitale indipendente ed open-source, è oggi la voce più autorevole in Internet in materia di crimine informatico. La home page di www.zone-h.org registra 35.000 singoli accessi al giorno per un totale di circa 800.000 click.

I siti Zone-H sono attualmente disponibili in 16 lingue diverse: inglese, italiano, francese, russo, portoghese, slovacco, spagnolo, giapponese, sloveno, turco, tedesco, lettone, croato, polacco arabo e indonesiano. Avvalendosi della collaborazione di oltre 50 esperti in tutto il mondo, tra cui figurano professionisti, giornalisti, studenti ed accademici, Zone-H propone una prospettiva realistica e “no-hat” dei flussi che coinvolgono il web.

Informazione ed analisi in tema di cyber terrorismo e cyber crime, servizi per l'implementazione della security e programmi educativi vengono elaborati e messi a disposizione della comunità IT che ogni giorno può contare su advisory, statistiche, aggiornamenti e informazioni, frutto di un costante monitoraggio della rete da parte dello staff Zone-H. I dati prodotti da questa analisi costante del web confluiscono in uno dei più grandi archivi di attacchi digitali al mondo che comprende, ad oggi, più di 2.200.000 di attacchi di cui sono registrati profilo, motivazioni e metodologie.

Il programma educativo è frutto del know-how e dell'esperienza di Zone-H che organizza corsi e seminari in tutto il mondo trattando gli aspetti fondamentali della Internet Security, con lo scopo di promuovere la diffusione della filosofia dell'osservatorio di prevenzione e costante aggiornamento dei sistemi di difesa informatici tra i professionisti IT italiani.