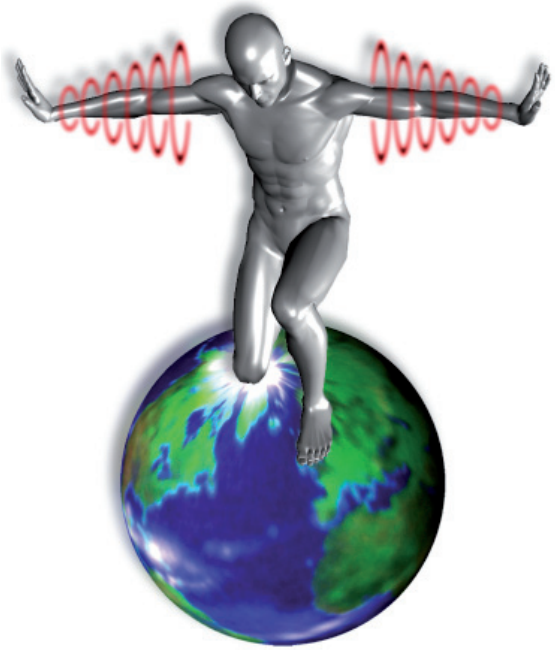
WIRELESS HACKING



SICUREZZA E (IN)SICUREZZA DELLE RETI WIRELESS

zone-h
unrestricted information

Argomenti

Zone-H presenta Wireless Hacking, l'innovativo corso hands-on sulla sicurezza delle wireless LAN destinato ai professionisti IT e a tutti coloro che vogliano comprendere a fondo gli aspetti fondamentali della sicurezza e (in)sicurezza delle reti senza fili.
Il corso nasce dalla collaborazione Securitywireless.info, il primo portale in Italia interamente dedicato alla sicurezza delle reti wireless.

Sicurezza e (in)sicurezza delle reti wireless

Il corso è rivolto a tutti coloro che vogliano scoprire il mondo wireless, le potenzialità offerte dalla nuova tecnologia ed approfondire le proprie conoscenze in questo ambito volte ad aumentare la sicurezza delle reti senza fili. Wireless Hacking ti aiuterà a migliorare la sicurezza della rete wireless attraverso l'analisi delle metodologie d'attacco in uso. Scoprirai che alcuni dei concetti e dei casi pratici esposti risulteranno fondamentali per la costruzione di reti wireless sicure.

Analisi dell'attacco e wardriving!

Il corso analizza nel dettaglio tutte le fasi di attacco ed è idealmente suddiviso in tre parti: si procederà alla descrizione dell'hardware impiegato negli attacchi, alle attività di mappatura e site-surveying e, infine, all'analisi delle vulnerabilità sfruttate durante l'attacco. Una vera e propria sessione di wardriving ti guiderà attraverso le fasi di mappatura e site-surveying.

Hardware administration

Ampio spazio viene dedicato alle best practice nella hardware administration.

Stile del corso: live hacking!

Come per tutti i corsi Zone-H, punto focale 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.

I benefici del corso

Wireless Hacking ti consentirà di:
- adottare il punto di vista di un hacker per proteggere al meglio la tua rete wireless
- conoscere a fondo le vulnerabilità delle reti wireless
- scoprire le tecniche di attacco comunemente utilizzate
- conoscere più approfonditamente gli standard e protocolli in uso per sfruttarne le potenzialità riducendone i limiti
- mettere a prova la tua rete wireless

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

A chi è rivolto

IT manager, security manager, amministratori WLAN, responsabili CED, personale IT.

Come

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

Prerequisiti

Background sulle reti wireless.

Durata

2 giornate.

Quando

23-24 Febbraio 2010
Orario corso: 9.00 - 17.00.
Alla colazione parteciperanno tutti i docenti.

Dove

Manno – Centro Galleria 2 – Sala PRIMAVERA

Offerta speciale

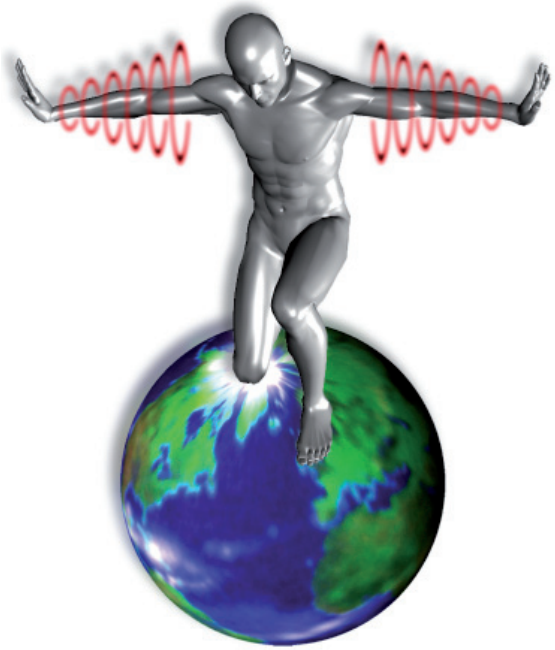
990 CHF SOCI ated – ICT Ticino
1200 CHF NON soci

Per la partecipazione al seminario è necessario iscriversi sul sito **www.ated.ch** entro il 30.01.2010. Il pagamento della quota, tramite fattura, vale come conferma d'iscrizione al corso.

ated ICT Ticino

securitylab

WIRELESS HACKING



SICUREZZA E (IN)SICUREZZA DELLE RETI WIRELESS

zone-h
unrestricted information

Contenuti

INTRODUZIONE AL WIRELESS HACKING
La tecnologia wireless nel mondo
Che cosa è una wlan
Perché analizzare una wlan
L'insicurezza nel wireless
Fare wardriving
Il fenomeno warchalking
Metodologia del wireless penetration testing

IL PROTOCOLLO 802.11
Analisi del protocollo (802.11a, 802.11b, 802.11g)
Architetture di protocollo
Tecnologie DSSS, FHSS, OFDM
Frame 802.11
Sessione live: analisi del traffico

ASSEMBLARE L'ARSENALE: HARDWARE 802.11
PDA e laptop a confronto
Tipi di adattatori wireless
Chipset: Prism, Cisco Aironet, Hermes, Symbol, Atheros

RF BEHAVIOR
Gain, loss, reflection, refraction e altri
Tipi di antenna: settoriali , omnidirezionali e direzionali
Connettori e cavi RF
Calcolo EIRP: esercitazioni pratiche
Sessione live: costruzione di una Antenna Pringles

802.11 drivers e utilities
Linux Wireless Extensions
Linux-wlan-ng utilities
Hostap
Soluzioni sotto Windows

NETWORK MAPPING E SITE SURVEYING: 'WARDRIVING'
Metodi di scansione nella identificazione di reti wireless
Rilevazione e analisi traffico in monitor mode
Kismet
Airtraf
Airfart
Netstumbler
Tools di monitoraggio del segnale RF
Sessione live: wardriving

METODI DI PROTEZIONE POSSIBILI
Algoritmo WEP
Hide SSID
MAC filtering
WEP
WPA
WPA2
802.11i
Sessione live

VULNERABILITA' ALGORITMI
Vulnerabilità WEP
Vulnerabilità WPA
Vulnerabilità WPA2
Sessione live

PIANIFICARE L'ATTACCO
Footprinting della rete
Site survey: considerazioni e pianificazione
Attacco: ottimizzazione timing e consumo batteria
Elementi nascosti nel wireless penetration testing

ASSEMBLARE L'ARSENALE: GLI ARNESI DEL MESTIERE
Tools di encryption cracking
WEP crackers
AirSnort
Wepattack
Aircrack
Tools per recuperare chiavi WEP da locale:
LucentRegCrypto
Tools di traffic injection utilizzati per accelerare il WEP cracking
Sessione live

DOS ATTACK
Airjack
File2air
void11
macflood
Sessione live

BREAKING THROUGH
bypassing closed ESSIDs, MAC and protocols filtering

WIRELESS FRAME GENERATING TOOLS
AirJack
File2air
FakeAP
Sessione live

VARI METODI DI KEY RECOVERY
WEP bruteforcing
The FMS Attack
Korek Attack
Sessione live

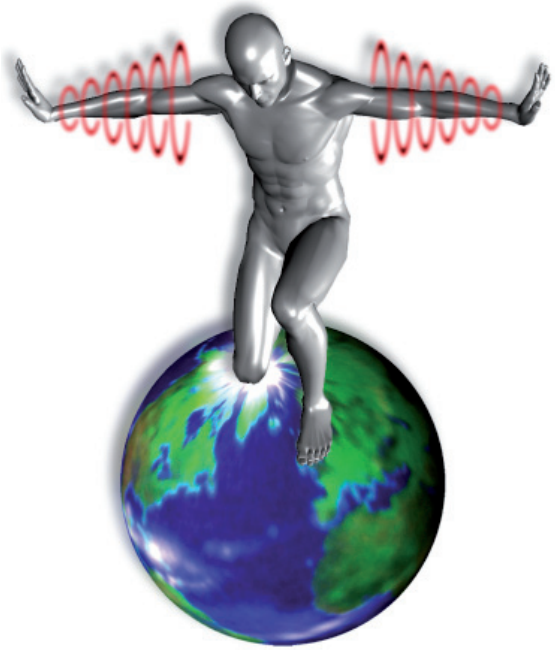
HARDWARE ADIMINISTRATON
Configurazione apparati
Pincipali parametri di configurazione
Best practice
Sessione live

TECNOLOGIA BLUETOOTH
Protocollo e stack
Vulnerablità
Possibili scenari

ated ICT Ticino

securitylab

WIRELESS HACKING



SICUREZZA E (IN)SICUREZZA DELLE RETI WIRELESS

zone-h
unrestricted information

Iscrizione

Per la partecipazione al seminario è necessario iscriversi sul sito **www.ated.ch** entro il 30.01.2010.

Sede dei corsi:
Manno – Centro Galleria 2 – Sala PRIMAVERA

Data
23-24 Febbraio 2010
Orario corso: 9.00 - 17.00.

Offerta Speciale
990 CHF SOCI ated – ICT Ticino
1200 CHF NON soci

Modalità di pagamento
Il pagamento della quota, tramite fattura, vale come conferma d'iscrizione al corso.

per informazioni:
Segretariato ated - ICT Ticino
Tel. +41 91 857 58 80
oppure 0041-91-9249590;
e-mail: segretariato@ated.ch
http://www.ated.ch/ - http://www.it-ti.ch/

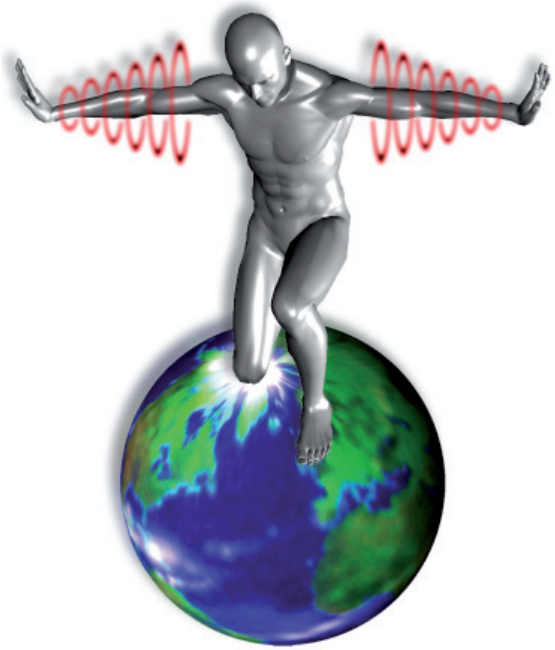
Condizioni commerciali
Per partecipare al corso è necessario iscriversi sul sito **www.ated.ch** entro il 30.01.2010. Le iscrizioni verranno accettate solo al ricevimento della contabile di avvenuto pagamento e secondo l'ordine cronologico di arrivo poiché il numero di posti è limitato.

Penali:
La penale in caso di annullamento è del 50% dal 31 Gennaio fino al 14 Febbraio 2010 ed in seguito del 100%.

ated ICT Ticino

securitylab

WIRELESS HACKING



SICUREZZA E (IN)SICUREZZA DELLE RETI WIRELESS

zone-h
unrestricted information

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 (Astharot) – 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 nazoinale che internazionale. Dal 2005 e' a capo del team di sicurizzazione della release di Linux Ubuntu. Ad oggi è senior analist 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 di Zone-H. 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 inglese, francese e portoghese.

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 educational 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 3.000.000 di attacchi di cui sono registrati profilo, motivazioni e metodologie.

Il programma educational 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.

www.zone-h.org