

**Ethical Hacker's speech:
interventi tecnici e tavola rotonda**
24/01/2002, Fiera di Milano

ABSTRACT

Il convegno ha l'obiettivo di presentare i lati inesplorati della Sicurezza Informatica, le vulnerabilità tecnologiche che si nascondono dietro alle tecnologie informatiche. Si parlerà di vulnerabilità note e meno note e dei metodi "underground" utilizzabili per capirle e risolverle.

Capiremo quindi perché è importante che la cultura degli "hacker" si affianchi alla cd cultura ufficiale al fine di migliorare la ICT Security.

Gli interventi avranno un taglio estremamente tecnico, ove possibile saranno eseguite anche demo.

PROGRAMMA

1) INTRO

Ore (15 min) Presentazione e introduzione
Naif – Raptor - Nobody – Kobaiashi
Presentazione della giornata e dei relatori dei tre workshop e dibattito finale.

Ore (15 min) Hackers, chi sono ? Underground e Security Research

Gli hacker vengono spesso demonizzati dai media e associati a qualsiasi forma di criminalità commessa attraverso il computer: ma chi sono in realtà, e quali sono i reali legami fra il mondo dell'hacking e l'Information Security ?

2) INTERVENTO I

Ore (45 min) Sovversioni del protocollo TCP, attacchi e contromisure
Fusys

3) INTERVENTO II

Ore (60 min) Buffer Overflow e dintorni
Awgn

3) INTERVENTO II

Ore (60 min) Smart Card (Java Card)
Kiai

4) TAVOLA ROTONDA

Ore (45 min) Tavola rotonda e dibattito finale
Chiusura della giornata
Presentazione futura Blackhats Conference
Nobody – Naif

Scaletta dei singoli interventi

✓ Hackers, chi sono ?

Relatori: Raptor, Naif, Kobaiashi, Nobody

Target: generico: *giornalisti, CEOs, operatori del settore*

Gli hacker vengono spesso demonizzati dai media e associati a qualsiasi forma di criminalità commessa attraverso il computer: ma chi sono in realtà, e quali sono i reali legami fra il mondo dell'hacking e l'Information Security ?

Scaletta:

- Un po' di storia
- Terminologie
- Nomi ed aneddoti, famosi o curiosi
- I legami tra il digital underground e la security research
- L'evoluzione e la crescita: The L0pht, Kevin Poulsen, Aleph1, CCC, Security Focus.

C.V. dei Relatori

- Naif

Fabio Pietrosanti aka naif

Security Manager della I.NET SpA (gruppo BT Ignite), appena ventunenne si occupa di security professionalmente dal '98 .

Il suo attuale lavoro è di ricerca e implementazione di soluzioni di security, Penetration Testing, Forensic Analysis, Network Planning.

Scriva articoli tecnici per la rivista WeekIT (Mondadori editore) e partecipa a numerosi eventi sulla sicurezza informatica sia ufficiali che underground, come relatore e spettatore.

Con il nome naif vive quotidianamente l'underground digitale italiano, da dove provengono tutti i suoi skill tecnici. Utilizza Linux, impegnandosi nella sua diffusione, implementazione e sviluppo definendosi un "OpenSource Evangelist" (www.perens.com).

- Raptor

Marco Ivaldi aka Raptor.

Security Manager presso la D.S.D. @ Mediaservice.net Srl. Tra i suoi interessi specifici vi sono le vecchie reti packet switched (X.25), la telefonia e la crittografia. Attualmente si occupa di security-related incidents, network security, pen-tests e progettazione di nuove soluzioni per l'area R&D.

Scriva regolarmente articoli tecnici per riviste del settore ed e' tra i fondatori di Linux&C, la prima rivista italiana interamente dedicata a Linux ed ai sistemi operativi open-source.

Utilizza OpenBSD, il sistema UNIX-like sicuro di default. Gestisce infine i mirrors ufficiali italiani di SSH, Nessus Security Scanner e Opensource.Org su Antifork.Org, gruppo di ricerca no-profit di cui e' membro fondatore.

- Kobaiashi

Igor Falcomatà aka Kobaiashi

Ideatore e moderatore delle mailing list su sikurezza.org, da oltre 2 anni IT Security Manager di INFOSEC, società specializzata in servizi e consulenze per la sicurezza informatica in ambito sia pubblico che privato.

- Nobody

Raoul Chiesa aka Nobody

E' uno tra i primi ethical hacker italiani; fondatore della Divisione Sicurezza Dati alla @ Mediaservice.net e Membro del Comitato Direttivo del CLUSIT (Associazione Italia per la Sicurezza Informatica), si occupa oramai da anni di sicurezza informatica ad alto livello, insieme ad un selezionato team di tecnici ed esperti, con collaborazioni internazionali.

Scrivo articoli sul controllo e lo sviluppo di Internet e cura rubriche on ed off line. In quest'ottica viene spesso chiamato come relatore in svariati convegni e corsi di specializzazione universitaria, convinto dell'importanza di diffondere cultura **in** e **sulla** Rete, tramite una continua e sempre maggiore informazione su tutto quello che gravita intorno ad essa, con un occhio di riguardo alla vulnerabilità dei sistemi informatici ed alle continue evoluzioni tecnologiche, anche segno di cambiamento dei tempi.

✓ **Sovversioni del protocollo TCP, attacchi e contromisure**

Relatore: Fusys

Target: *Responsabili Sistemi Informativi, Responsabili Sicurezza, Responsabili Reti, CTO*

Scaletta:

- ❑ descrizione teorica del protocollo TCP: header, connessioni, algoritmi base
- ❑ punti deboli di TCP: numeri di sequenza (RFC1948, analisi statistica), mancanza di autenticazione reale
- ❑ sovrersione attiva: basi dello sniffing, predizione dell'ISN, socket RAW
- ❑ attacchi al protocollo: TCP spoofing, TCP hijacking, Man-In-The-Middle

C.V. Fusys aka Matteo Falsetti

Ricercatore indipendente di sicurezza e figura conosciuta nell'underground digitale per i suoi technical paper, e' membro attivo del gruppo di security research S0ftPj: i suoi maggiori interessi sono le reti, la suite di protocolli TCP/IP ed i covert channels, l'implementazione, la gestione ed il reversing della sicurezza. Programmatore in ambiente UNIX/Linux, studia attivamente il kernel Linux per la creazione di LKM inerenti la sicurezza ed ha prodotto svariato codice opensource.

✓ **Buffer overflow e dintorni**

Relatore: awgn

Target: *Responsabili Telecomunicazioni, Responsabili Reti, Responsabili Web, Responsabili Sistemi Informativi, Responsabili Sicurezza, CTO.*

Scaletta:

- ❑ Introduzione agli attacchi: exploits.
- ❑ Code injection: una delle tecniche usate dai crackers.
 - cosa e' un exploit
 - cosa e' un exploit code injection based
- ❑ Panoramica di attacchi remoti e locali.
- ❑ Esecuzione di codice iniettato dall'attacker in un processo.
- ❑ Target: ottenere un accesso shell privilegiato.
- ❑ Obiettivi sensibili:
 - setuid root binary
 - demoni in ascolto tcp o udp.
 - nota chroot escape.
- ❑ Codice da iniettare: cosa e', come funziona, e come si realizza uno shellcode.
 - registro EIP nei processori intel.
 - OPCODE, operandi e allineamento.
 - shellcode locale dimostrativa execve
 - shellcode locale suid(0) + execve
 - shellcode x attacco remoto: dup2() + suid() + chrootescape() + execve
 - shellcode e filtri regexp [A-Za-z0-9] (nota del compilatore di phrack)
- ❑ Il primo caso "banale".
 - Il caso "CIAO", introduzione al concetto di buffer overflow.

- ❑ Introduzione al gcc nei sistemi Intel IA-32.
 - utilizzo dello stack come suggerito dal vendor.
 - indirizzi di stack e sistema operativo: paginazione.
 - prologo epilogo (enter/leave) per programmazione strutturata...
 - uso dei registri EIP, EBP, ESP.
 - ret e fp.
- ❑ Attacco reale, dettagli tecnici.
 - Problematiche:
 - indirizzo del buffer.
 - La base dello stack pointer per l'istanza di primo livello (main).
 - Compilazione condizionale che puo' modificare la struttura delle istanze.
 - Nop padding.
- ❑ Dallo stack all'heap/bss.
 - Concetto di buffer dinamici.
 - variabili con visibilita' a livello di file e varibili statiche.
 - Struttura completa
- ❑ ATTACCO 1: forzatura del ret nello stack per l'esecuzione di codice iniettato dall'esterno.
- ❑ ATTACCO 2: frame pointer, utilizzo da parte del processore per le nested function: 1 byte overflow.
- ❑ ATTACCO 3: heap overflow.
- ❑ ATTACCO 4: format bug.

C.V.

Nicola Bonelli aka awgn.

Laureando in ingegneria telecomunicazioni presso l'Universita' degli studi di Pisa. Esperto di programmazione C sicura in sistemi operativi Posix e BSD.

Founder di antifork.org research, movimento italiano rivolto alla ricerca nel settore informatico e della sicurezza di sistemi operativi opensource.

✓ Smart Card e Java Card

Relatrice: Kiai

Target: *Ricercatori, Responsabili Telecomunicazioni, Responsabili Reti, Responsabili Web, Responsabili Sicurezza.*

Scaletta:

- ❑ Che cosa è una smart-card (intro)
 - Struttura fisica
 - Struttura logica (black box)
 - Perchè smart-card
 - ISO 7816, Open Platform, EMV, ETSI
 - Utilizzi comuni
- ❑ Meccanismo di comunicazione
 - Protocolli (PC/SC)
 - APDU
- ❑ Strumenti per lo sviluppo: Javacard Development Kit
 - JCRE/JCVM
 - package javacard.framework
 - Sviluppo e caricamento di una cardlet
- ❑ Attacchi (tampering)
 - Software
 - intromissioni e modifiche sull'interfaccia di comunicazione
 - Hardware (breve accenno)

- Fault Generation
(bombardamenti alla carta per generare errori)
- Eavesdropping
(studiate le caratteristiche analogiche della carta)
- ❑ Costruiamo insieme una semplicissima cardlet commerciale (purse)
 - Tecniche di "programmazione sicura"

C.V.

Francesca Fiorenza aka Kiai

E' ricercatrice presso una delle più note aziende di Card Systems e lavora nella sede di Parigi, dove si occupa di sistemi di personalizzazioni di smart-card, per applicazioni bancarie e bytecode verifier, PKI, GSM cardlet.

Laureata in Scienze dell'Informazione, lavora inoltre sulla verifica di protocolli crittografici per i quali ha sviluppato un programma per la simulazione e l'analisi automatiche.

1) Dibattito finale

Relatori: Naif – Raptor – Kobaiashi – Nobody – Fusys – Kiai – Awgn – Nail – Vecna – Gigi Sullivan

Target: Tutti

Scaletta:

- ❑ Q & A con i relatori
- ❑ Chiusura lavori

BlackHats.it: Who is Who

Blackhats.it è una comunità di ricerca sorta spontaneamente, formata da un gruppo di nove persone: hackers, esperti di security, alcuni che lavorano nel mondo dell'I.T., altri impegnati come ricercatori. Professionisti della sicurezza informatica, con forti legami al mondo underground ed alla filosofia hacker, che si dedicano a migliorare la sicurezza della rete Internet. Lo fanno per proprio conto e con risorse proprie, dedicando il tempo personale a questa passione.

Altre figure si aggiungeranno nel tempo, in quanto Blackhats.it è una comunità aperta a tutti coloro i quali vedono l'I.T. Security da punti di vista differenti dai canoni standard, lontano dai legami e dagli obblighi commerciali e vicino alla filosofia Open Source.

Al momento i Black Hats italiani sono :

naif@blackhats.it
nail@blackhats.it
nobody@blackhats.it
raptor@blackhats.it
fusys@blackhats.it
sullivan@blackhats.it
awgn@blackhats.it
kiai@blackhats.it
claudio@blackhats.it
koba@blackhats.it