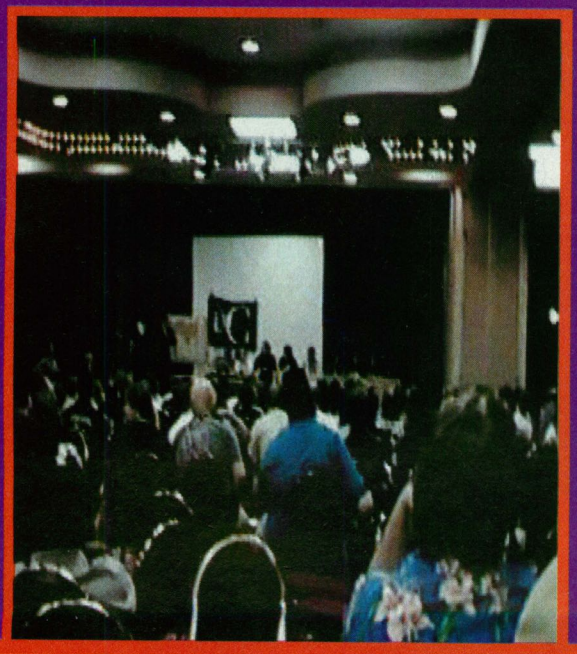
DEFCON V

GLI HACKER SI INCONTRANO

Non è un incontro goliardico: interessatissimi sono esperti di compagnie telefoniche, di aziende, polizia, agenti segreti e mafia

Nel mondo esistono circa 200 superconoscitori di kernel di sistemi operativi; intorno a loro altri 2.000 persone in grado di capire la documentazione prodotta dai primi. E' a questo livello che si trovano i migliori esperti di sicurezza informatica, i quali possono garantirla o creare seri danni ai computer di chiunque. Talvolta, alcuni di questi lavorano per servizi segreti o per mafie.

Come ogni estate, anche quest'anno Las Vegas è stato lo scenario dove ha avuto luogo la più grossa convention mondiale di hacker: il DefCon 5. La partecipazione è stata impressionante: migliaia di hacker, phreaker, cracker, cyberpunk, cypherpunk, hammy, virus koder, system administrator, programmatori... sono arrivati in Nevada da tutto il mondo per potersi confrontare, sfidare e fondamentalmente conoscere.



Sarà stato il gran parlare di sicurezza che si è fatto durante tutto l'anno o una maggior sensibilità da parte del grande pubblico a questo tipo di *cultura*, ma quest'anno non si poteva fare un passo a Las Vegas senza imbattersi in un gruppo di individui poco abbronzati che indossavano la maglietta del DC 5.

Lo stesso Dark Tangent - aka Jeff Moss - organizzatore della convention è rimasto spiazzato... si parla di circa 2000 partecipanti.

A questo raduno infatti non partecipano solo hacker, esperti di sicurezza di agenzie ed enti governativi americani, network administrator per grosse corporation... ma anche molti giornalisti, scrittori e semplici curiosi. Il raduno si svolge su due livelli: esiste un programma ufficiale, molto ricco, nel quale sono invitati a parlare importanti esponenti del mondo underground, esperti di sicurezza a livello mondiale, tutori dell'ordine (FBI, CIA, NSA), esperti tecnici delle compagnie telefoniche... queste sono conferenze pubbliche a cui tutti possono partecipare. Durante questi incontri i partecipanti hanno modo di conoscersi, di valutare il livello di competenza reciproco... è proprio durante queste conversazioni che vengono affrontati gli argomenti più interessanti. La grande disponibilità di computer, router e il collegamento ad internet consentono di testare subito praticamente ciò di cui si sta parlando.

Si tratta di vere e proprie sessioni parallele (che durano anche diverse ore) in cui vengono affrontati argomenti come denial of service, ip spoofing, packet sniffing sotto diversi sistemi operativi. A queste sessioni, tuttavia è possibile partecipare solo se si sa il fatto proprio e lo si puo' dimostrare! Quest'anno il programma ufficiale (per una serie di problemi tecnici e organizzativi) è stato un po' scarso ma le ses-

sioni private sono state *davvero* interessanti e la presenza di importanti personaggi quali Jericho, Acid Angel, Bronc Buster, Mudge, Wrangler... ha portato i discorsi ad un'alto livello tecnico! Con questo articolo *non* mi propongo di creare un manipolo di hacker insegnando loro le tecniche più potenti per penetrare in uno o più server, ma vorrei riuscire a spiegare ciò che ogni IT-manager dovrebbe conoscere riguardo la reale pericolosità e le metodologie usate dagli hacker in modo che possano predisporre adeguate difese per il proprio sistema informativo aziendale.

Ma andiamo con ordine: cerchiamo di capire come è strutturata la comunità degli hacker a livello mondiale.

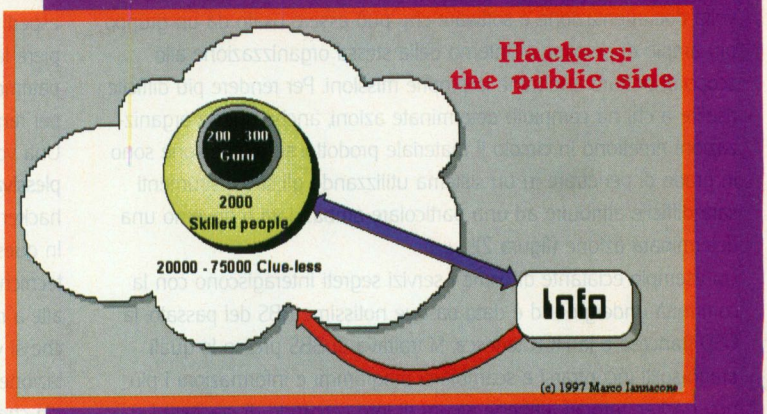
Durante il DefCon 5 Ira Winkler (direttore del NCSA) ha fatto una descrizione molto realistica dell'universo underground.

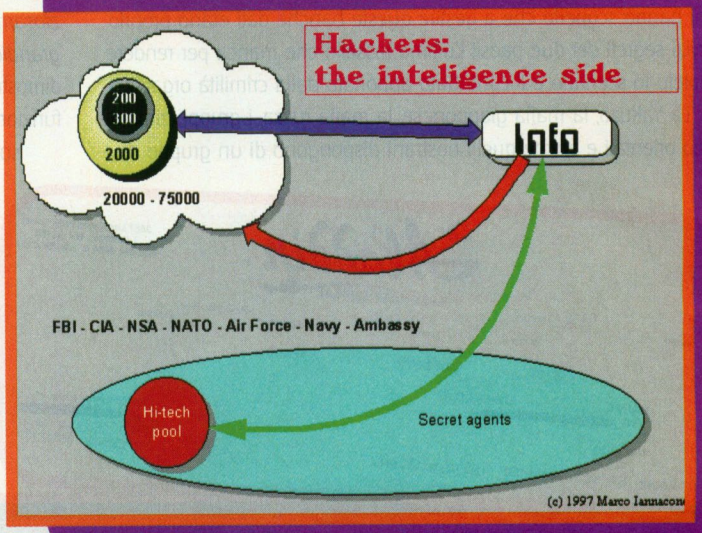
Si stima che a livello mondiale esistano all'incirca 200/300 individui che conoscono a fondo il funzionamento dei kernel dei principali sistemi operativi, dello stack TCP/IP, dei router e dei firewall, e che vi lavorano attivamente sviluppando programmi in C in grado di testare eventuali problemi di sicurezza e di creare le opportune patch per superare questi limiti. Questi programmatori sono in continuo contatto tra loro, si scambiano informazioni, comunicano le loro scoperte ad istituzioni quali il CERT (=Computer Emergency Responce Team) e producono documentazione molto tecnica, che contiene le informazioni essenziali.

Attorno a questi 200 guru gravitano circa 2000 programmatori e system administrator (skilled people) che sono in grado di capire ciò che dicono i 200. Questo secondo livello di skilled people analizza la documentazione prodotta dai 200, prova i programmi da loro sviluppati su altri sistemi operativi, li migliora, scrive a sua volta altri programmi più semplici da usare e produce della documentazione decisamente più articolata che spiega in dettaglio il problema preesistente, dimostra come sfruttare il bug a proprio vantaggio e fornisce una soluzione oppure indica la direzione nella quale lavorare per poterlo risolvere. Generalmente i programmi sviluppati a questo e al precedente livello sono distribuiti gratuitamente (nel miglior spirito hacker) e possono essere usati sia per testare i propri sistemi e migliorarli, che per penetrare in sistemi altrui.

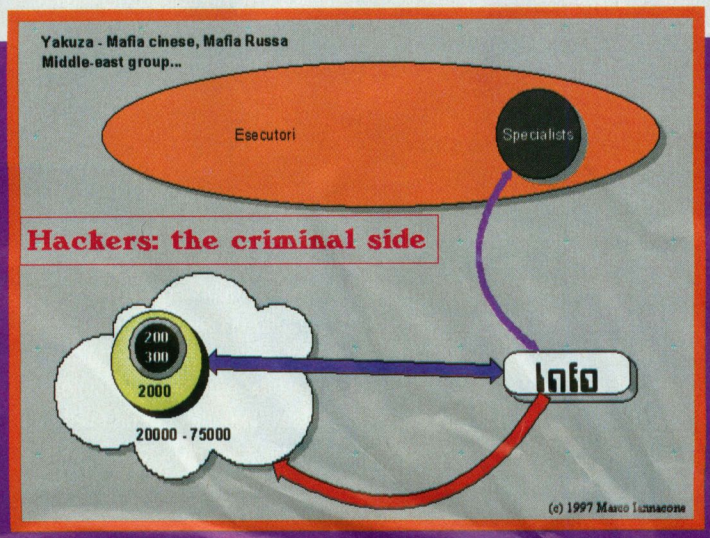
L'uso che verrà fatto del programma dipende dallo spirito e dall'etica del singolo individuo. In generale (a qualsiasi livello) l'unica legge universalmente accettata da tutti gli hacker è il diritto alla libera circolazione delle idee. L'hacker è alla continua ricerca della conoscenza... per questo motivo, egli prova, scrive codice, raccoglie e scambia diligentemente informazioni al fine di conoscere tutto ciò che è possibile sapere.

Attorno a questi 2000 programmatori esiste un vasto gruppo (tra i 20 e i 75 mila) che Winkler definisce clue-less (letterlamente incapaci) che sfruttano le informazioni e i prodotti diffusi dall'anello precedente per propri fini personali. Si tratta di persone con discrete conoscenze dei sistemi operativi ma con scarse doti di programmazione. **La figura 1 (fig1.gif)** illustra graficamente la struttura appena descritta.





Lo scenario però, afferma Winkler, è un po' più complicato. Fino ad ora abbiamo descritto ciò che è presente sullo scenario *pubblico*. La sicurezza informatica, la penetrazione in sistemi informativi aziendali e/o governativi, tuttavia, interessa anche ad altre realtà: le agenzie governative, i servizi sergreti, l'esercito e le ambasciate (FBI, CIA, NSA, NATO, NASA, i servizi segreti israeliani, il Japanese immigration plan...) hanno anche loro un pool di super esperti in grado di indagare, risolvere e sfruttare a loro piacimento i bug dei sistemi informativi. Questo staff attinge al materiale di pubblico dominio e produce a sua

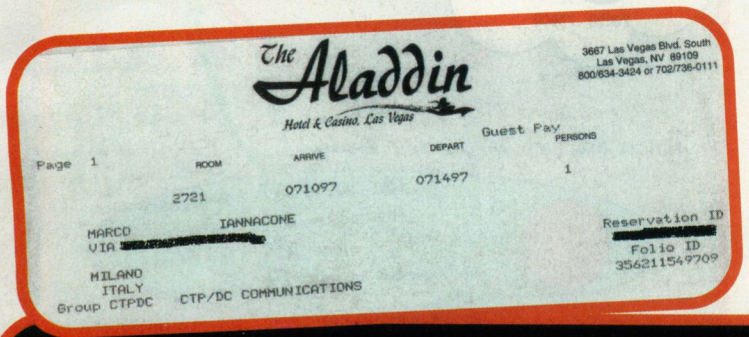


volta documentazione e software che può essere usato da un gruppo più ampio di persone all'interno della stessa organizzazione allo scopo di portare a termine le proprie missioni. Per rendere più difficile risalire a chi ha compiuto determinate azioni, anche queste organizzazioni rimettono in circolo il materiale prodotto: se più persone sono in grado di penetrare in un sistema utilizzando gli stessi strumenti sarà difficile attribuire ad una particolare ambasciata o governo una determinata azione **(figura 2)**!

Un esempio eclatante di come i servizi segreti interagiscono con la comunità underground è dato da due notissime BBS del passato: la QSD francese e la HCK tedesca. Si trattava di BBS presso le quali erano soliti incontrarsi e scambiarsi programmi e informazioni i più noti hacker europei.. ebbene alcuni di loro cercando di craccare i sistemi hanno scoperto che a gestire queste banche dati erano proprio i servizi segreti dei due paesi! L'ultimo tassello che manca per rendere completo lo scenario è il contributo apportato dalla crimilità organizzata. La Yakuza, la mafia giapponese, la mafia russa, i gruppi criminali medio orientali e anche quelli nostrani dispongono di un gruppo di esperti che elaborano le tecniche con cui gli esecutori possono compiere le loro azioni. Anche loro hanno tutto l'interesse ad attingere al patrimonio pubblico e a diffondere le tecniche da loro implementate per rendere difficile risalire ai veri esecutori **(figura 3)**.

Una volta chiaro lo scenario **(la figura 4 fornisce un'immagine complessiva)**, è importante capire alcune delle tecniche utilizzate dagli hacker nella fase che precede una loro incursione.

In questa fase di apprendimento, l'hacker mette in pratica una serie di tecniche (che sono raggruppate sotto il nome di Social Engineering) atte a raccogliere il maggior numero di informazioni relative alla società che si vuole colpire e alle persone che vi lavorano. Nella sua presentazione (*Le dinamiche del Social Engineering: una mappa per trovare ciò che vuoi sapere, lavorando sulle reti e facendo spionaggio silenziosamente; l'uso della paranoia, dell'immaginazione e della grandiosità per costruire la* ***Grande Immagine***) Richard Thieme dimostra come sia semplice ottenere delle informazioni quali nomi, funzioni ricoperte, indirizzi, numeri di telefono, nomi di familiari di persone che occupano posizioni chiave all'interno di un'azienda, semplicemente utilizzando un po' di astuzia e facendo alcune telefonate sotto una falsa identità. E' proprio questo infatti il metodo utilizzato dagli hacker: una volta noti i nomi chiave si tratta di scoprire la struttura informativa interna all'azienda. Sapendo quindi dove guardare e cosa cercare si tratta solo di riuscire a penetrare nel giusto computer, ma questo è la parte più facile per un hacker. Inoltre nelle aziende ci sono spesso grossi problemi di sicurezza... tanto per parlare dell'aspetto più evidente le password sono spes-


The Aladdin
Hotel & Casino, Las Vegas
3667 Las Vegas Blvd. South
Las Vegas, NV 89109
800/634-3424 or 702/736-0111
Page 1
ROOM
ARRIVE
DEPART
Guest Pay
PERSONS
2721
071097
071497
1
IANNACONE
MARCO
VIA [redacted]
MILANO
ITALY
Group CTPDC
CTP/DC COMMUNICATIONS
Reservation ID [redacted]
Folio ID
356211549709

Curiosità sul DEFCON V

1) Il DefCon non vuole essere una convention noiosa: per questo motivo vengono organizzate diverse attività a scopo puramente goliardico. I giochi più noti sono: *THE HACKER JEOPARDY, THE TCPIP DRINKING GAME, CAPTURE THE FLAG, SPOT THE FED* e la *QUAKE COMPETITION*.

The Hacker Jeopardy è la parodia di una nota trasmissione televisiva americana nella quale i concorrenti si affrontano rispondendo a delle domande su argomenti prefissati e guadagnano dei punti a seconda del tipo di domanda a cui decidono di rispondere. La versione del DefCon affronta argomenti tecnici o legati alla storia dell'informatica e del mondo Unix.

Capture the Flag - hackers style è forse il gioco più interessante che ha luogo al DefCon! Lo scopo del gioco è quello di rubare il file rootflag dal computer delle altre squadre cercando di impedire il furto dal proprio sistema. Al gioco partecipano 5 squadre ognuna delle quali possiede un proprio computer sul quale è stata fatta una installazione standard (cioè quella presente nell'80% dei server su internet) di uno tra i più noti sistemi operativi (le macchine possono avere sistemi operativi differenti). I computer sono collegati in rete tra loro attraverso un grosso router.

Ogni squadra - composta da una o più persone - può fare del suo meglio per proteggere il proprio sistema. Il gioco risulta molto interessante non solo per i diretti partecipanti, ma anche per chi assiste che ha modo di apprendere moltissimo.

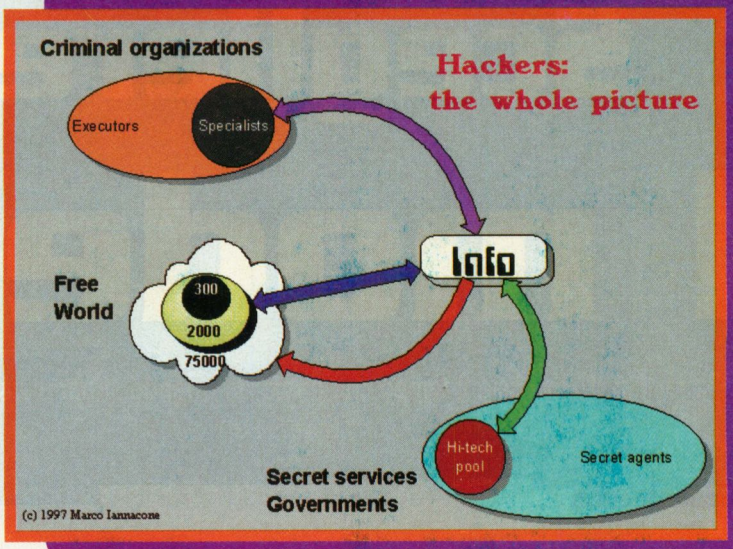
Spot the Fed - O meglio: chi è la persona che vi sta seduta accanto? Essenzialmente il gioco funziona in questo modo: se vedete un *una persona vestita di nero*, con auricolari, occhiali da sole che tiene d'occhio ogni vostro movimento e ogni singolo tasto premuto... avvertite gli altri che avete scoperto un federale (Spotted a Fed). A questo punto dovrete spiegare le motivazioni che vi hanno indotto a pensare che si tratti di un agente. Seguirà una votazione pubblica e se l'individuo viene giudicato un Federale voi vincete una maglietta.

2) Anche quest'anno un'altro ragazzino è scappato di casa per poter venire ad assistere al DefCon. Si tratta di una cosa che accade spesso...

3) Ogni anno il DefCon ha luogo in un albergo differente: a causa di ciò che hanno combinato i partecipanti durante le convention precedenti nessuno li vuole una seconda volta. Quest'anno il DefCon si è tenuto presso l'Alladin Hotel e sembra che anche l'anno prossimo debbano cercare un'altro posto! Alcuni partecipanti hanno fatto decine di telefonate intercontinentali gratuitamente, si sono introdotti nella rete dell'albergo, hanno tentato di frodare le slot-machine e per finire c'è stato perfino chi ha portato di fronte alla platea la portiera di una vettura della GTE (una delle principali compagnie telefoniche americane).

Fortunatamente DT aveva stipulato un'assicurazione da 1 milione di dollari per i danni eventualmente causati!

so facilissime da scoprire, soprattutto conoscendo qualcosa sulla persona che ne è proprietaria (spesso è il nome del figlio, della moglie, la data di nascita, il codice fiscale... oppure è identica alla user-id o è addirittura la parola *password*!). Il primo passo, quindi, che un buon amministratore di sistema dovrebbe fare è quello di verificare la bontà delle password scelte dagli utenti, invitarli a cambiarle spesso (o meglio ancora assegnarle lui stesso) ed evitare che vengano scritte su un post-it attaccato al monitor o chiuso nel primo cassetto!



L'ottanta per cento dei furti di informazioni e dei fenomeni di hackeraggio avviene infatti dall'interno dell'azienda stessa. Si dovrebbe quindi fare attenzione a che fine fanno le informazioni riservate una volta finite nel cestino... vengono eliminate? in quante mani passano prima di venire davvero distrutte? Che informazioni è possibile ottenere dalla centraliniste? e dalle segretarie? Riuscire a limitare la fuoriuscita di informazioni è una precauzione che non costa molto in termini di investimenti ma che può limitare notevolmente i danni che l'azienda potrebbe subire.

Tutti gli OS sono violabili, NT di più

Per quanto riguarda la sicurezza dei propri sistemi ci sono state diverse presentazioni relative a differenti OS; nelle sessioni private si poteva imparare come mandare in crash i principali sistemi operativi. Ciò che è emerso in maniera evidente è che non esiste il sistema inviolabile... non dovete sentirvi sicuri solo perchè avete comprato l'ultima versione di un sistema operativo! Esistono decine di patch che vanno applicate su ogni macchina per poter ridurre davvero i rischi di penetrazione... il problema è essere informati, sapere quali sono i problemi e dove trovare le soluzioni. A questo proposito la maggior parte degli hacker presenti al raduno lavorano in società che si occupano di testare, mantenere e migliorare il livello di sicurezza di altre aziende. Le relazioni più interessanti sono state, a mio avviso, quelle atte a dimostrare l'insicurezza di Windows NT. L'interesse del grande pubblico si sposta infatti generalmente verso le macchine UNIX quando si affronta il discorso della sicurezza... sono infatti i computer più potenti su cui girano gli applicativi mission critical e sui quali l'azienda fa affidamento. E ovviamente le società che si occupano di sicurezza dedicano gran parte del loro tempo a rendere sicuri questo tipo di sistema. Windows NT, attualmente, non è un sistema sicuro, anzi... contiene parecchi bug che consentono di mandarlo in crash da remoto, scoprire le password di amministratore e compiere ogni sorta di manomissione. Mudge - del L0pht Heavy Industries - ha presentato in maniera molto dettagliata come sia possibile costringere una macchina NT a trasmettere le password in chiaro (NT lo consente per garantire compatibilità con LAN Manager) e come ottenere i privilegi di Amministratore attraverso diverse tecniche, incluso un brute force attack. In diverse sessioni private, invece, è stato mostrato come realizzare un denial of service di una macchina NT utilizzando telnet, ping o un semplice 4GL come VB e poche righe di codice.
Questo tipo di problemi sono più difficili da risolvere e per questo il mio consiglio è quello di rivolgersi a società in grado di affrontare i problemi partendo dalla radice: con appositi strumenti (tra cui i più noti sono gli scanner) viene testato l'intero sistema informativo aziendale per poi risolvere i problemi presenti macchina per macchina. Tra le società più qualificate (composta da ex-hacker) per questo tipo di interventi vi è l'israeliana Xpert (www.xpert.com) che è presente in Italia con la sua consociata Netconfig (www.netconfig.com).

Crittografia e posta elettronica

Un'altra relazione molto interessante è stata quella di Bruce Schneier (autore di Aplied Cryptography e Blowfish algorithm) intitolata *Perchè la crittografia è più difficile di quello che sembra.*
Insieme a Sameer Parek (del c2.net) ha descritto i problemi di implementazione e produzione confrontandoli con il desiderio della gente e delle aziende di avere un potente sistema di crittografia distribuito. Un'importante notizia è che il brevetto Stanford sta per scadere per cui il suo codice del DES potrà essere utilizzato da un numero più ampio di persone, mentre l'algoritmo di crittografazione per eccellenza diverrà l'AES (Advanced Encription System). Un'altra importante notizia per noi europei (viste le norme restrittive sull'esportazione di codice dagli USA) è che sono stati sviluppati numerosi programmi e algoritmi indipendenti sia in Inghilterra che in Germania per cui la crittografia non è più confinata a chiavi di 40-bit. Per concludere il mio reportage sul DefCon vorrei elencare alcune tecnologie che devono essere seguite attentamente perchè saranno ciò su cui si baserà lo scambio di informazioni nei prossimi anni. Per quanto riguarda la crittografia, è importante seguire l'evoluzione di X.509, PGP Web of Trust, S/MIME e per finire la prossima versione di sendmail (v9) che verrà rilasciata per la fine dell'anno porrà una particolare attenzione alla sicurezza supportando l'autenticazione del mittente e la crittografia dei messaggi.

Marco Iannacone
ianna@iol.it

Marco Iannacone, si occupa di UNIX, networking e internet come sistemista e consulente. Lavora come System Administrator responsabile dei servizi internet presso la Dun & Bradstreet Kosmos e collabora frequentemente con la rivista *inter.net*