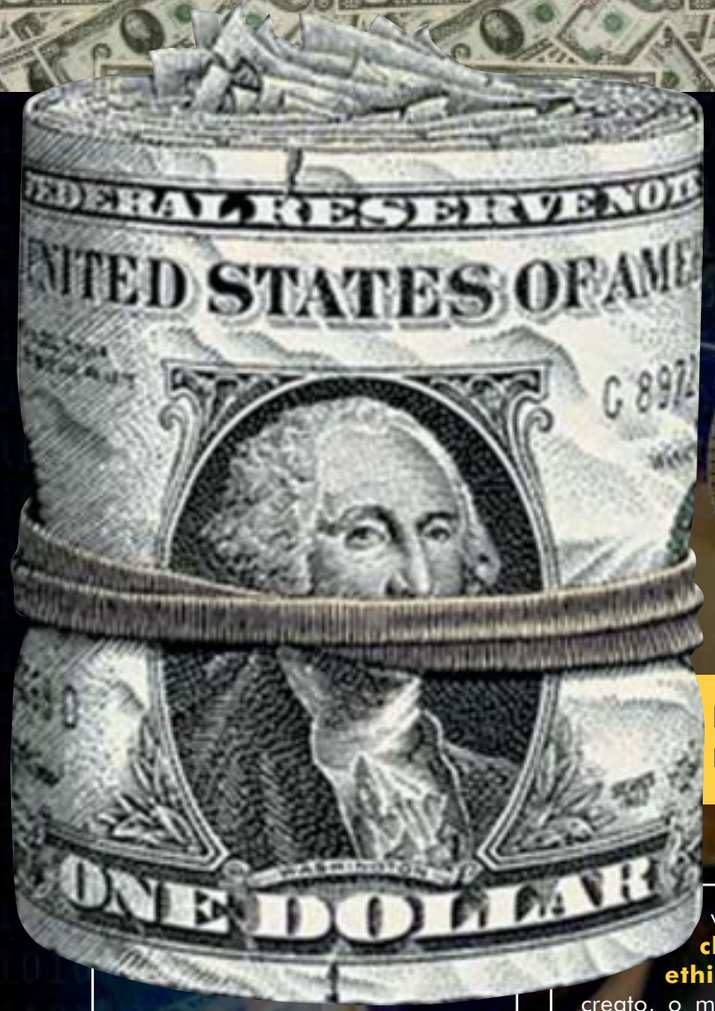
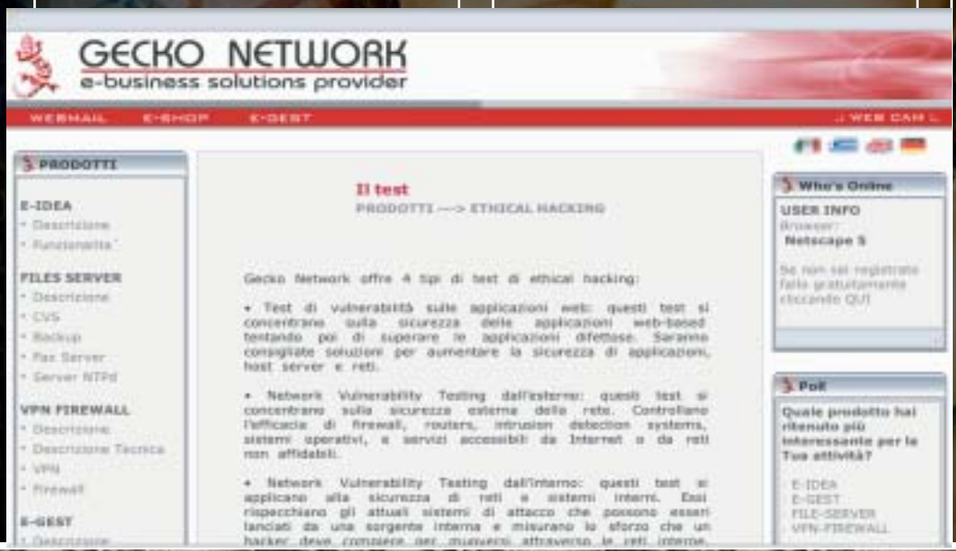


E c'è chi con

Attenzione! Lo chiamano Ethical Hacking, ma non c'entra nulla con l'etica hacker!

Dopo l'associazione hacker-criminale, insieme all'associazione cracker-criminale-pirata informatico sembra che si stia diffondendo quella di **hacker-esperto in sicurezza**. Tale associazione ha portato all'affermazione di una nuova **elite di specialisti che si definiscono ethical hacker** ed ha creato, o meglio, istituzionalizzato una nuova forma di hacking, nota appunto come ethical hacking, che consiste più o meno nel **farsi pagare per fare quello per cui gli hacker e i cracker sono arrestati o condannati**: penetrare nei sistemi informatici e aggirarne le protezioni. Non ha però nulla ha a che fare con l'"etica hacker" dei programmatori del MIT, e tanto meno con l'"etica hacker del lavoro" che, come spiega molto chiaramente Pekka Himanen, è qualcosa che **va ben al di là del "mi porto a casa la pagnotta programmando"**. Vediamo di che si tratta.



>> C'è anche l'hackeretico

Un articolo di Affari&Finanza del 3 febbraio 2003, dal titolo "C'è anche l'hackeretico...", spiega: "Rappresentano la filosofia "buona" della cosiddetta pirateria informatica. Sono al servizio delle aziende e testano la sicurezza dei computer". "L'approccio e l'insuperabile conoscenza dei sistemi informatici sono gli stessi degli hacker tradizionali: **adesso si guarda però al business** della gestione delle reti e della tutela della privacy. L'hacker etico o hacker eretico o hacker convertito, "in giacca e cravatta (sia pure metaforicamente)", o in qualunque modo lo si voglia definire, rimane però ancora fedele, così si dice, alla filosofia e allo spiri-

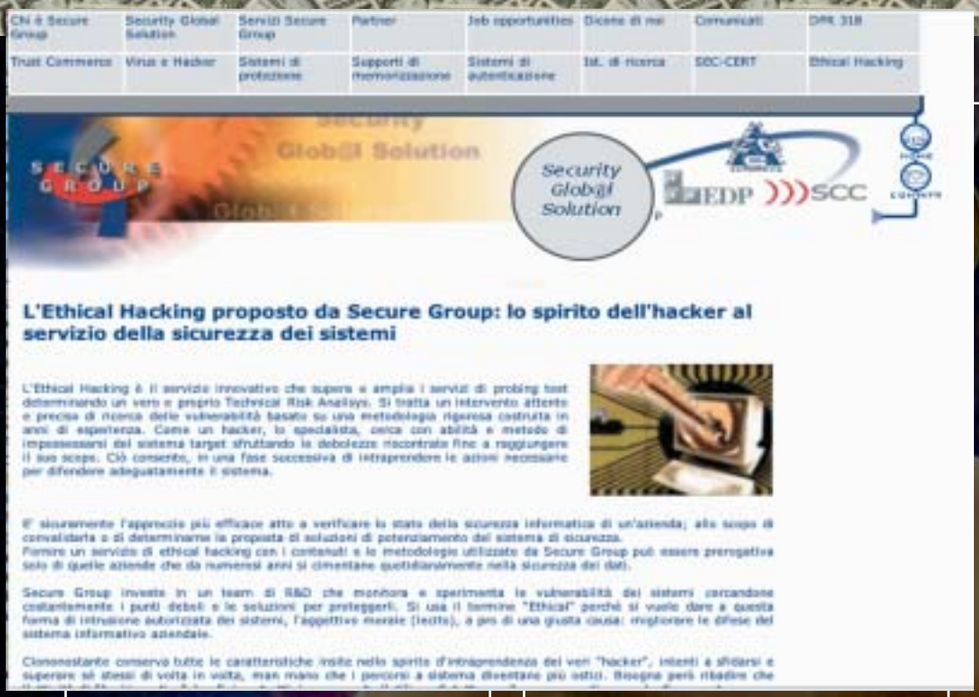
L'HACKING si è fatto i soldi...

to del vero hacker. Tra coloro che praticano questa nuova forma di hacking si menzionano **Secure Group**, **Gecko Network** insieme ai **Black Hats**. Questi ultimi sono i primi ad aver parlato di ethical hacking, ma in maniera molto diversa dagli altri. Li considereremo quindi come un caso a parte.

Come gli hacker, gli specialisti di Secure Group e di Gecko Network, sfruttano dei bug dei sistemi per lanciare degli attacchi, sia dall'esterno tramite la rete internet sia dall'interno. Ma sottolineano: **"non intendono né danneggiare i sistemi né sottrarre informazioni riservate"**. Si tratta infatti di semplici simulazioni: viene riprodotto "il modus operandi di un hacker/cracker" e "l'attacco effettuato da persone con un accesso o una conoscenza delle risorse interne dell'azienda". In questo modo si può valutare la sicurezza dei sistemi, redigere dei report da consegnare ai proprietari in cui vengono descritte le vulnerabilità e intervenire per difendere adeguatamente il sistema. Non si limitano a identificare i problemi, **"ma aiutia-**

Raoul Chiesa

Dei Black Hats ha fatto parte anche Raoul Chiesa aka Nobody, un hacker o ex hacker che oggi pratica quello che egli definisce l"hacking del lavoro": si occupa di sicurezza informatica, protegge i sistemi e crea prodotti I.T. Security. "Hacking, nel senso più puro del termine", spiega Chiesa, "significa ricercare i difetti, gli errori. Scoprirli, renderli noti, risolverli. La Security, nel significato più pratico del termine, significa fare attenzione ai difetti ed agli errori. Scoprirli, renderli noti, risolverli. Hacker e Security Researcher vivono dunque tra bug, exploits, security advisory, testing, reverse engineering". Chiesa è convinto che la sicurezza non possa fare a meno della ricerca e della sperimentazione underground e che l'unico modo per saggiarne la robustezza sia provare a forzare i sistemi. Parla dell'hacker come di un "amico della sicurezza" e descrive l'ethical hacker come: "colui che hackera il vostro sistema, lo esplora velocemente e ve lo fa persino sapere, inviandovi mail di report o suggerimenti". E' quello che fa anche Chiesa, ma per lavoro. Tra i servizi offerti dalla sua azienda (Mediaservice) vi è il Security Probe, o Penetration Test: "il cliente ci richiede di violare, con tutti gli strumenti possibili, la propria rete aziendale, sfruttando tutte quelle dimenticanze, errate configurazioni o bug lasciate dai fornitori abituali". A chi lo accusa di essere passato dall'altra parte, spiega: "Quando mi sono avvicinato all'hacking per la prima volta vedevo questo mondo come un luogo sacro, una religione, uno stile di vita, un modo di pensare e agire. La penso ancora così. Ho rifiutato spesso di procedere o partecipare all'identificazione di hacker responsabili di violazioni di sistemi, ma non di danni. Perchè hacking, per me, continua a voler dire libertà, sfida, essere più bravi...Non credo di condividere le idee comuni dei responsabili o esperti di sicurezza informatica. Continuo a sentirmi hacker". Chiesa è un hacker ma non è la sua attuale professione ad averlo reso tale. Lo status e la fama di hacker, già "vasta nella cominità hacker europea", gli è stata "riconosciuta e suggellata" dalle autorità internazionali "dopo una serie di eclatanti intrusioni in grossi Enti e Istituzioni - tra le quali Bankitalia, IBM e AT&T".



CN è Secure Group | Security Global Solution | Servizi Secure Group | Partner | Job opportunities | Dicono di noi | Comunicati | DPR 318
Trust Commerce | Virus e Hacker | Sistemi di protezione | Supporti di memorizzazione | Sistemi di autenticazione | Int. di ricerca | SEC-CERT | Ethical Hacking

Security Global Solution

EDP SCC

L'Ethical Hacking proposto da Secure Group: lo spirito dell'hacker al servizio della sicurezza dei sistemi

L'Ethical Hacking è il servizio innovativo che supera e amplia i servizi di probing test determinando un vero e proprio Technical Risk Analisys. Si tratta un intervento attento e precisa di ricerca delle vulnerabilità basato su una metodologia rigorosa costruita in anni di esperienza. Come un hacker, lo specialista, cerca con abilità e metodo di impossessarsi del sistema target sfruttando le debolezze riscontrate fino a raggiungere il suo scopo. Ciò consente, in una fase successiva di intraprendere le azioni necessarie per difendere adeguatamente il sistema.

E' sicuramente l'approccio più efficace atto a verificare lo stato della sicurezza informatica di un'azienda; allo scopo di convalidarla o di determinarne la proposta di soluzioni di potenziamento del sistema di sicurezza.
Fornire un servizio di ethical hacking con i contenuti e la metodologia utilizzate da Secure Group può essere prerogativa solo di quelle aziende che da numerosi anni si cimentano quotidianamente nella sicurezza dei dati.

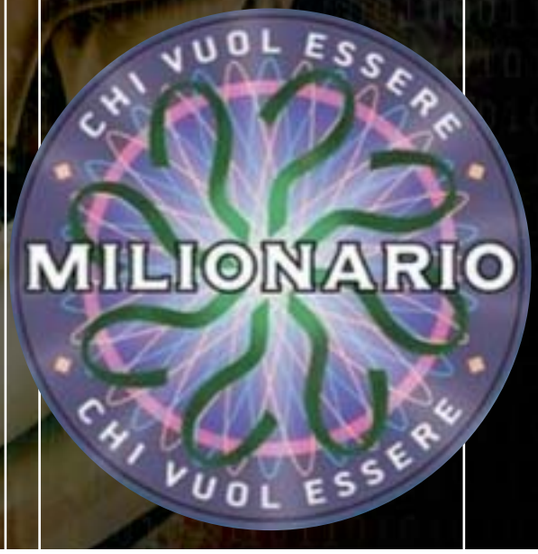
Secure Group investe in un team di R&D che monitora e sperimenta le vulnerabilità dei sistemi cercandone costantemente i punti deboli e le soluzioni per proteggerli. Si usa il termine "Ethical" perché si vuole dare a questa forma di intrusione autorizzata dei sistemi, l'aggettivo morale (lecito), a pro di una giusta causa: migliorare le difese del sistema informativo aziendale.

Ciononostante conserva tutte le caratteristiche insite nello spirito d'intraprendenza dei veri "hacker", intenti a sfidarsi e superare sé stessi di volta in volta, man mano che i percorsi a sistema diventano più ostici. Bisogna però ribadire che

mo anche a definire soluzioni su misura degli obiettivi di business", sostiene Gecko Network. Sempre come un hacker, lo specialista Secure Group, svolge la sua attività con creatività e il suo scopo è innanzitutto sfidarsi e superare se stesso. Il vero spirito hacker è messo al servizio della sicurezza dei sistemi. Anche lo specialista di Gecko Network si preoccupa della sicurezza informatica delle aziende e il suo scopo è quello di salvaguardare "le molte cose buone che ha portato la crescita esplosiva di Internet", tra cui il commercio elettronico, un accesso facile a una quantità immensa di informazioni, il collaborative computing, l'e-mail, nuove strade per la pubblicità e la distribuzione di informazioni. Da notare come la distribuzione di informazioni venga menzionata accanto alla pubblicità, considerata altrettanto positiva!! (?) Secure Group usa il termine **"ethical"** perché "vuole dare a questa forma di intrusione autorizzata dei sistemi, l'aggettivo morale (lecito), a pro di una giusta causa: migliorare le difese del sistema informativo aziendale". Benché lo spirito d'intraprendenza sia quello di un hacker, Secure Group ribadisce che l'attività di "hacking etico" è a fini costruttivi e **"in totale contrasto con l'attacco di un cracker mirato alla distruzione di un obiettivo o comunque alla sua compromissione per secondi fini"**. Anche Gecko Network fornisce una descrizione dell'ethical hacking, ma nell'area "prodotti": "I governi, le aziende, i privati cittadini di tutto il mondo sono ansiosi di essere parte di questa rivoluzione, ma temono che qualche hacker entri nei propri web server e rimpiazzi il logo aziendale con immagini pornografiche, che possa leggere le e-mail, che possa intercettare il numero di carta di credito da un sito di shopping on-line, o installare qualche software che rende pubblici i segreti della propria azienda. Con queste ed altre preoccupazioni, l'hacker etico può essere d'aiuto". Ma **nel frattempo, il vero hacker si è parecchio incavolato nel vedersi associato persino alla pornografia!**

>> Black Hats e Raoul Chiesa

I Black Hats sono stati promotori dell'ethical hacking, ma **hanno chiuso i battenti il 6 marzo 2003**, perchè lo scopo che si erano proposti era ormai stato raggiunto: **"portare alla luce le conoscenze nascoste nell'underground tecnico italiano"**. Però chiariscono: si è conclusa solo questa esperienza, non il loro compito, ed è per questo che ne parleremo al presente. I Black Hats **mettono le proprie capacità a disposizione del prossimo** per rendere più sicura la digital life. Formano un'**associazione senza scopo di lucro**, non legano il loro nome a prodotti commerciali di alcun genere, in quanto vedono nella "filosofia Vendor Independent **l'unico modo per assicurare l'imparzialità e l'oggettività** nel campo dell'ICT Security". Molti di loro lavorano nel campo della sicurezza informatica per altre aziende, ma quella dei Balck Hats non è un'attività lavorativa, non ci guadagnano nulla e non effettuano penetration test, security assessment o product testing. La loro funzione primaria è quella di **divulgare la cultura nel campo della sicurezza**, attraverso speech tecnici e attività di ricerca, diffondere informazione



seria, corretta e veritiera sull'hacking che essi considerano "a state of mind", uno stile di ricerca e di vita, "affinchè i mass-media non commettano più i tipici errori nel comunicare informazioni sull'hacking, ricadendo in luoghi comuni con termini diffamatori e falsi come "pericolose bande di hacker" o "anarco-hacker" o "tecnobanditi" o ancora "pirati informatici" e "terroristi del web". I Black Hats cercano di fare cultura, così affermano, non solo sul piano tecnico ma anche filosofico/storico.

>> Pubblicità e falsa Informazione

Il termine "hacker", si legge nel **Jargon File**, tende a connotare l'appartenenza ad una comunità globale. Implica anche che la persona in questione sottoscriva in qualche modo l'etica hacker. Per un hacker etico è una forma di cortesia spiegare al sysop, tramite e-mail o da un account di superuser, esattamente come si è fatto ad entrare nel sistema e come il buco possa essere tappato. Questo hacker si comporta come un **"tiger team"** che nel gergo dell'esercito USA sta appunto per un esperto che segnala delle falle nei sistemi (non informatici) di sicurezza, lasciando, per esempio, in una cassaforte che si pensa sia custodita e in realtà non lo è, un cartellino che dice "avremmo potuto rubare i vostri codici". Solo che **l'hacker etico non è pagato e il suo intervento non è neanche richiesto**. Secure Group e Gecko Network, invece, propongono l'hacker come **"una nuova figura professionale del complesso mondo della New Economy"**. I loro specialisti sono nuovi hacker o ex-hacker che, a differenza di molti altri che **vendono le proprie conoscenze alle multinazionali**, fanno spionaggio elettronico o lavorano per i governi, hanno deciso di mettersi in proprio e al servizio delle aziende e del business. **Ma non è questo che li rende etici!** Lo diventano nel momento in cui confrontano il fine della loro attività - ma **non lo spirito e neanche la tecnica** -, con quello degli hacker e dei cracker cosiddetti "criminali" o "pirati". L'Ethical Hacking, proposto da queste aziende, non è una filosofia e in realtà non è neanche un'etica. Viene, infatti, da essi stessi definito **una metodologia, un servizio, un prodotto**. Gecko Network offre quattro tipi di test di ethical hacking; Secure Group fornisce moltissimi servizi di ethical hacking.
Gli ethical hacker di Gecko Network e Secure Group salvaguardano la sicurezza dei sistemi informatici, **tutti gli altri hacker danneggiano, rubano informazioni riservate o entrano nei sistemi per secondi fini illeciti**. Un vero hacker o chi ha capito come la pensano, **non incorrerebbe in questo errore**, già abbondantemente perpetrato dai media. Nonostante l'opera di diffusione di una cultura dell'hacking anche da parte dei Black Hats, i primi a definirsi ethical hacker, c'è ancora chi, sventolando la bandiera di "una strana e non ben definita etica hacker", associa gli hacker a immagini pornografiche e i cracker e persino gli hacker a coloro che entrano nei sistemi informatici per far danno. Per un hacker etico l'informazione è tutto, soprattutto se "veritiera"! Ma questa non lo è! La diffusione della cultura informatica ha sicuramente aperto la strada a nuove forme di criminalità. Questa criminalità, però, è sempre solo e unicamente associata agli hacker, **persino dagli ethical hacker**. Gecko annovera "le molte strade della pubblicità" tra le molte cose buone che ci ha dato internet. Descrive l'hacker come colui che installa "qualche software che rende pubblici i segreti della propria azienda". La pubblicità però è una delle tante forme di intrusione non autorizzata, forse la più diffusa. Accade spesso che software cosiddetti legali contengano al loro interno degli **"Spyware"**, programmi che comunicano informazioni sul nostro conto. Queste informazioni vengono poi usate, senza che nessuno ce l'abbia chiesto, per fini statistici, ma più spesso per inviarci pubblicità indesiderata, il cosiddetto **"Spam"**. **Nessuno parla di queste intrusioni come di crimine o pirateria!** L'ethical hacking è a nostro parere un fenomeno che **trae i suoi frutti e i suoi vantaggi proprio dalla criminalizzazione degli hacker e dei cracker**. Più i media parlano di hacker e cracker criminali informatici, più questa nuova forma di hacking si alimenta e trae i suoi profitti. Come rileva Raoul Chiesa in un suo articolo dal titolo "Il difficile rapporto tra hacking e marketing" **l'associazione hacker-pubblicità** sta andando molto di moda. Si amplifica la portata degli attacchi hacker per invocare stati d'assedio fittizi. Si vende un servizio perché si genera paura e contro la paura alcune aziende hanno il rimedio. Nella strategia militare, simili tecniche, affatto corrette, si raggruppano sotto il nome di Propaganda e disinformazione.

DaMe`
www.dvara.net/HK

BIBLIOGRAFIA E SITOGRAFIA

Italian Black Hats:
http://www.blackhats.it

Gecko Network:
http://www.geckos.it

Secure Group:
www.securegroup.it

Affari&Finanza - Susanna Jacona Salaria: C'è anche l'hackeretico…:
http://www.securegroup.it/rs/feb_03_affariefinanza.pdf

Raoul Chiesa: Il difficile rapporto tra hacking e marketing:
http://www.internos.info/archivio/rc16.pdf

Biografia e molti articoli di Raoul Chiesa:
http://www.lamerone.net/raoul/00_whois.php