Autore: Raoul Chiesa - *Giugno 1999*

Who is Who: Hackers, chi sono?

"Si sente spesso dire che ci sono differenti tipi di hackers in giro: ma chi sono veramente ?"

Questa la domanda che, con maggior frequenza, mi viene posta dai Clienti, dai system manager, dagli amministratori delle società per le quali effettuo consulenze di security-check o after-attack recovery. Possiamo dire, rispondendo a questa domanda, che ce ne sono nove: nove tipi di hacker. Possiamo persino dividerli in ***categorie.***
Userò un po' di terminologia ***underground,*** per aggiungere un po' di "colore" e rendere le cose più divertenti.

Wannabe Lamer - ***Vorrei essere...Lamer!***

E' la categoria più "divertente". Si possono trovare in Rete hacker di questo tipo praticamente ovunque, in quanto gli stessi chiedono continuamente, ed in pubblico, aiuti di vario tipo. La loro domanda classica, riportata in puro "slang" hacker, è "Yo man! Whaz di b3st way t0 hack www.nasa.gov ???? Ehy c'mon, explain me man!!!" Che, tradotta, significa "Qual è il modo migliore per bucarmi www.nasa.gov ? Daiiiiiii amico, dimmelo!!!". Potete vedere alcune "chicche" postate da elementi di questo tipo su http://www.insecure.org/nmap/index.html (parte bassa). E' l'home page del creatore di NMAP, un'utility di port scanning. Ha fatto un elenco delle e-.mail "migliori"...ed è tutta da ridere.

Script Kiddie - ***Il ragazzo degli script***

Diciamo che sono "culturalmente avanzati", ma non li vorreste per proteggere il vostro sistema. In genere chiamano ogni giorno http://www.rootshell.com , o seguono i mailing-list su BugTraq (maggiori informazioni su http://www.geek-girl.com/bugtraq/about.html), da dove prelevano gli ultimi exploit e tool.
A volte sono persino capaci di entrare nei sistemi ed urlarlo per mari e monti.

The "37337 K-rAd iRC #hack 0-day exploitz" guy - ***Il ragazzo "cool" che va sul canale #hack di IRC e dice di avere gli exploit in tempo zero (cosi' come il trader si vanta di essere uno "0 day" courier)***

Sono, in genere, i tipi che darebbero qualunque cosa per divenire "famosi".
Farebbero veramente di tutto per avere il loro alias (nickname) pubblicato ovunque, per finire sui giornali, per far sì che si parli di loro. Sono pronti ad utilizzare "mezzi brutali" per arrivare dove vogliono.
Non è il genere di hacker che esplora, ma piuttosto che utilizza quanto è già disponibile.

Cracker

Innanzitutto chiariamo un'incomprensione: il termine "Cracker", in origine, era inteso nei confronti di quella persona che rimuoveva le protezioni dai programmi (software) commerciali. Recentemente la definizione ha iniziato ad apparire su giornali e mailing-list, ed è attualmente utilizzata per descrivere gli hacker "violenti", quegli hacker che sono ben felici di divenire un incubo nella vita dei system administrator, cancellando file e creando danni permanenti ed irreparabile al sistema.
Questa categoria è anche più avanzata dei ragazzini del "37337 K-rAd iRC #hack 0-dayz exploitz", ed ha anche il know-how necessario.
Cercheranno di rimanere sul vostro sistema il più a lungo possibile. Quando sospetteranno di stare per perderne il controllo, lo "annulleranno", cancellando file, log, ogni tipo di traccia, importante o meno.
E' una categoria di hacker abbastanza pericolosa.

Ethical Hacker - ***L'Hacker "Etico"***

Potrebbero persino piacervi. Sì, entrano, hackerano il vostro sistema. Sì, sono cattivelli, impertinenti, curiosi...ma molto spesso (una moltitudine di report sono presenti a tal proposito) entreranno nel vostro sistema, lo esploreranno velocemente (se si tratta di un grosso computer o di una rete molto vasta, molto probabilmente curioseranno in giro un pochino "oltre" il limite della normale "educazione") e ve lo faranno persino sapere, inviandovi mail di report o suggerimenti, quando avranno terminato la loro esplorazione.
Hanno una conoscenza estremamente ampia e a 360 gradi dei sistemi operativi, mentre normalmente la gente dà per scontato che gli hacker smanettino solo con UNIX: falso ed errato. Non lo fanno per trarne un profitto o per cercare fama: nulla di simile. La passione li guida, come dice uno spot...
A volte sono ingenui, e parlano pubblicamente delle loro azioni, dando per scontato il fatto di non aver fatto nulla di male.
Se vi capita la "fortuna" di averne uno nel vostro sistema..non cacciatelo via: approfittatene per apprendere i buchi della vostra rete aziendale o i bug della vostra Sun Workstation da dieci milioni di lire....

Quiet, paranoid, skilled hacker - ***L'hacker taciturno, paranoico, specializzato***

Abbiatene paura. E' il tipo di hacker più pericoloso. Ciò non significa che vi cancellerà file o cose del genere, ma è paranoico, e quindi sarà molto difficile rilevare la sua presenza o, peggio, trovarlo. Rimarrà sui vostri sistemi per un periodo di tempo lunghissimo, senza fare nulla di grave o spiacevole. Lo esplorerà con calma, ma sarà attirato solo da quanto può rappresentare un qualche interesse per lui (non leggerà le vostre e-mail private, ma controllerà uno per uno i syslog e file similari..); non è interessato alla fama. Non "lo fa" per soldi. Lo fa per se stesso, per la sua esperienza ed il suo know-how.
E' altamente capace e competente su più tipi di sistemi operativi: esplorerà, ma non perderà tempo ad impressionare nessuno.
Se rileverete la sua presenza - cosa molto improbabile -, sparirà immediatamente.

Cyber-Warrior - ***Il cyber-guerriero***

E' un mercenario. Ha acquisito capacità elevate negli anni. Probabilmente arriva da una delle categorie sopra elencate, ed ha scelto la sua strada. Si vende al migliore. Ma rifiuta alcune richieste. E' utilizzato come basso profilo, i suoi target sono bassi, difficilmente attaccherà la multinazionale, molto più probabilmente il vostro Internet Service Provider, l'università locale o l'anagrafe. Non gli interessa chi buca e perché, entro certi limiti. Lo fa per i soldi. Non lascia quasi mai tracce. E' intelligente. Ma non convintissimo di quello che fa: si sente "sporco".

Industrial Spy - ***La spia industriale (Spionaggio industriale)***

Soldi. "Lo fa" per soldi. Altamente capace, con moltissima esperienza. Pericoloso, se è alla ricerca di materiale confidenziale. In questa categoria rientrano sfortunatamente molti "insider", vale a dire le persone che accedono illegalmente ad informazioni sensibili, all'interno della loro stessa azienda, per utile personale.

Government agent - ***L'agente governativo***

Politica e soldi. La combinazione peggiore in questi casi. In genere sono persone con un buon background hacker. Non c'è bisogno di aggiungere altro. Politica e soldi.