Guida ai Newbies
by Sbirilindo (alexmessomalex staff)

Thanks to: alexmessomalex.com; #alexmessomalex; Mimi (ti amo!!);
Gau; Tao; Prinzi; Monte; Soffie; Già; Taba; Rice;
a tutto l'alexmessomalex staff.
Fuck to: compiti delle vacanze; Biologia; è Pasqua quindi risparmio gli altri... :D

//
Grande Guida ai Newbies di Sbirilindo
//

Salve a Tutti.
Allora ho deciso di scrivere questa guida per far si ke i membri "alle prime armi" della nostra community (e non solo) possano inkominciare a vedere con altri occhi internet e quello ke gli sta attorno.
Questa guida non vi farà diventare Hacker (anke perche non esiste nessuna guida in grado di farlo).

Incominciamo con un po' di nomi....

INDIRIZZO IP: è un indirizzo numerico che identifica il vostro PC sulla rete. tutte le macchine connesse ad internet hanno un indirizzo IP con il relativo HOST NAME.
Un esempio di indirizzo IP è questo 62.149.130.78

PORTE: Le porte di connessione sono quei dispositivi che servono a far comunicare il vostro computer con il mondo di Internet.
Esse Sono numerosissime ed ognuna ha una sua funzione e un compito ben stabilito.
Vediamo le porte + usate:
PORTA 80 [HTTP]= E' la porta che contiene un indirizzo internet http (no ftp e altro), e viene usata ad ogni connessioni ad un sito, se chiudete questa porta non potrete più navigare in internet.
PORTA 110 [pop3]= Porta dedicata alla posta in ingresso.
Ha il compito di collegarsi al server e scaricare le e-mail. E' fatto obbligo tenerla aperta se si usano e-mail sul PC.
PORTA 53 [dns]= E' una porta che esegue il comando di DNS: trasformare un indirizzo web in un indirizzo IP reale.
PORTA 23 [Telnet]=
Porta dedicata al telnet, programma che serve per la comunicazione tra computer in rete. Il telnet ha il compito di collegarsi ai server di ogni sito che visitate e scaricare le pagine per visualizzarle.

HOST NAME: per fare un esempio di host name basta un sito.
www.alexmessomalex.com è un host name, ovviamente anke www.alexmessomalex.com ha un indirizzo IP ke è appunto 62.149.130.78
Adesso vi chiederete come ho fatto a scoprire l'IP da un semplice HOST.
Facile col DNS!

DNS (Domanin Name Server): è praticamente una funzione svolta da un Server situato sulla rete che si occupa di risalire ad un IP tramite un host name e viceversa. Senza questo computer la nostra navigazione in internet non potrebbe esistere. infatti per collegarsi ad un sito, Internet non riconosce gli host ma ha bisogno del relativo IP.
inutile dire che tutti i browser svolgono questa funzione automaticamente.

BROWSER: è un programma che vi permette di vedere e di navigare nei siti internet. Internet Explorer ne è un esempio.

CLIENT: un client è un programma che richiede ad un server un certo tipo di servizio.
Internet explorer è un client che serve per collegarsi ad un servizio web
Microsoft Outlook è un client di posta elettronica, e serve per collegarsi al servizio e-mail.

SERVER: Un computer che risponde alle richieste dei client che vi si collegano, ad esempio, quando vi collegate ad internet, il vostro modem si connette ad un ISP (internet service provider) che instrada la connessione ad internet. Di solito l'ISP è quello con il quale avete un contratto telefonico, a meno che non usiate altri numeri per connettervi.

PROTOCOLLI:

HTTP: è il protocollo web che vi permette di navigare/visitare i siti WEB.
SMTP: è il protocollo di posta in uscita
POP3: è il protocollo posta in entrata

bhe avete visto vi ho citato un po' di protocolli, ma ke sono?
Un PROTOCOLLO è un insieme di regole per la gestione di un servizio internet.

[][][][][][][TELNET][][][][][][]

Allora il telnet è lo strumento principale dell'hacker, è un'applicazione standard di internet, è possibile trovarla in tutti i sistemi operativi. Permette ad un utente di stabilire una comunicazione client-server. la porta utilizzata è la 23.
Inoltre telnet gestisce le operazioni di collegamento ai server di ogni sito che visitate e quelle di scaricare le pagine per visualizzarle.
Tutto questo in automatico, senza che voi lo vediate, o almeno, voi lo vedete nel vostro browser solo in modo grafico.
Quindi usando telnet noi ci sostituiamo al nostro computer, inviando dati ad altri server.

{FAKE MAIL}
Con telnet possiamo mandare messaggi di posta elettronica, lo sapevate?
adesso mi direte: "ma scusa, perkè mi devo complicare la vita col telnet quando avendo Outlook mi basta schiacciare 2 pulsanti e la mia e-mail p già spedita?"
Semplice, con telnet si possono manomettere i dati dell'e-mail, facendo apparire al destinatario un e-mail non vostra.
Vi faccio un esempio irreale (magari mi fosse successo!) ma ke rende l'idea:
In classe è entrato il preside e mentre tutti si fanno i cazzi loro, voi riuscite a sentire ke il preside sussurra al prof di biologia "stasera mi mandi i risultati degli alunni nella sua materia per e-mail".
NOOO, in biologia ho 4!!! come faccio????
Bhe le E-mail del prof e del preside siamo riusciti ad averle a scuola, tramite un bidello un po' stupido... come agiamo?
Verso le 5 mandiamo un FAKE MAIL al prof con mittente l'indirizzo del preside, dicendo: "non si disturbi, non mi mandi i voti della sua classe, li ho già in archivio.
Il prof riceve l'e-mail e ovviamente, insegnando biologia, non capisce un cazzo di PC e non manda l'e-mail al preside...
UHHHH Pericolo scampato direte voi, invece no, il preside stasera si aspetta i risultati della classe.
Stesso metodo, mandiamo al preside l'e-mail con mittente l'indirizzo del prof, allegando un file di testo preparato da voi (ovviamente con un bel 7 al posto del vostro 4!) e dicendo: ecco i voti signor preside, cordiali saluti.
il gioko è fatto, il preside non vi manderà la lettera a casa e il prof non sospetterà niente, e anke se qualcosa venisse fuori non risalirebbero mai a voi.
Come fare tutto Questo??? A dirlo sembrerebbe una cosa da nulla.. infatti è proprio così!!!

P.S. il seguente testo è tratto dalla guida di Lord Shinva, ho modificato alcune parti rendendole + chiare.

Iniziamo dunque imparando ad usare Telnet.

Usandolo per collegarvi a un sito semplicemente inserendo un host name, vi collegherete al servizio Telnet. Ma abbiamo detto che non e` questo il nostro obiettivo. A noi interessa il servizio SMTP. Dunque, come fare per accedervi?

Bisognera` inserire, oltre all'indirizzo del server a cui vogliamo collegarci, anche un numero di "porta".
Vogliamo collegarci a SMTP? Basta utilizzare la porta 25.
Adesso dobbiamo scegliere un server al quale collegarci per inviare l'e-mail, di server ne troviamo tanti: uno è "mail.katamail.com", un'altro può essere "mx5.libero.it".
-NOTA BENE: se vogliamo spedire l'e-mail ad un utente che usa libero come casella di posta, dobbiamo connetterci al server di libero, se vogliamo spedire l'e-mail ad uno ke usa katamail, dobbiamo connetterci al relativo server.
-PROGRAMMA UTILE: un programma utile x trovare i server SMTP è SMTP Finder (vedrò di farlo aggiungere nei programmi d alexmessomalex)
torniamo a noi...
Dunque, una volta connessi a prova.it:25 avremo un messaggio di questo tipo:

220 prova.it Sendmail x.x/x.x 11/11/97 ready at Mon, 30 Oct 97 06:22:19 -0200

e niente altro. Il server sta ora aspettando comandi da parte nostra.
La prima cosa da fare e` identificarsi, e cio` va fatto con il comando HELO in questo modo:

HELO nomeprovider.it

sostituendo nomeprovider.it con il nome del nostro provider.

NOTA: usando Telnet *NON* e` possibile cancellare. Quindi digitate senza fretta, e se proprio sbagliate riavviate la connessione e ripetete tutto, oppure - in alcuni casi - puo` essere sufficiente premere invio e riscrivere la riga da zero. Non cancellate, anche se sembra funzionare. I risultati possono essere imprevedibili e potreste rivelare la vostra identita`.

Talvolta e` possibile inserire un nome falso, ma i nuovi server conoscono gia` il vostro IP Address quando vi collegate, quindi tanto vale inserire il vero nome.

La risposta sara`:

250 prova.it Hello NOMEPROVIDER.IT, pleased to meet you

A questo punto dovremo dire al server qual'e` il nostro indirizzo di e-mail.
Usiamo allo scopo il comando "MAIL FROM" e digitiamo:

MAIL FROM: (attenzione quando si inserisce l'indirizzo, si inserisce con i 2 <>, esempio: <indirizzofalso@ci6cascato.it>)

...ovviamente l'indirizzo da inserire e` quello falso =)
Il server rispondera` con un messaggio. Se avremo sbagliato qualcosa, sara` un messaggio d'errore, e dovremo ripetere l'immissione.

A questo punto dobbiamo scegliere la nostra "vittima", che supponiamo essere <vittima@lamer.it> Usiamo il comando "RCPT TO" e scriviamo:

RCPT TO:

Il server rispondera` con un altro messaggio.

Ed ora che abbiamo definito sorgente e destinazione passiamo all'invio delle intestazioni e del corpo del messaggio.
Avvisiamo il server che siamo pronti, scrivendo:

DATA

e il server ci dira` di scrivere il messaggio e di concludere con un punto su una riga vuota.

Fermiamoci un attimo. In ogni e-mail esistono delle intestazioni (headers) che si trovano prima del corpo del messaggio vero e proprio. Il loro scopo e` elencare tutti i computer attraverso i quali e` passato il messaggio, nonche` il nostro IP Address! Cio` potrebbe rivelare la nostra identita` a un hacker o a un SysAdmin esperto. Per evitarlo, digitiamo:

Received: by nomeprovider.it id AA11212 with SMTP; Sun, 12 Oct 97 13:40:58

dove nomeprovider.it e` il nome del vostro provider (quello che avete usato con HELO) e l'ultima parte (Sun, 12 Oct...) e` la data in formato standard.
ID AA11212 va cambiato. Potete mettere un numero qualsiasi (possibilmente che inizi con AA1 piu` altre 4 cifre, per farlo sembrare piu` reale).
Si tratta solo di un numero di serie del server, niente di importante.

Ora dobbiamo digitare:

Message-ID:

Cio` serve a far credere che il messaggio sia partito effettivamente dal server "microsoft.com" con l'ID AA11345 (puo` essere un numero qualsiasi, purche` NON uguale a quello inserito prima con l'intestazione "Received:").

Inseriamo ora di nuovo il destinatario, la data e il soggetto della e-mail:

To:
Date: Sun, 12 Oct 97 11:30:27
Subject: questa e` una prova...

Lasciamo uno spazio e scriviamo il messaggio che vogliamo inviare (lungo quanto vogliamo). Per concludere il messaggio lasciamo due righe vuote, digitiamo un punto, premiamo invio, scriviamo QUIT e invio.
La FakeMail verra` inviata automaticamente dal server, e noi possiamo anche chiudere Telnet.

E` importante inviare a se stessi dei messaggi di prova per vedere se il server scelto ha ricevuto i dati correttamente, se non sono stati commessi errori e, soprattutto, per vedere se il proprio IP Address si trova in mezzo alle intestazioni "Received:", oppure (sbagliato) alla fine.
Spero ke la guida e le mie implementazioni siano state di facile comprensione.

Passiamo ad altro...

[][][][][][][SGRADEVOLI CONOSCENZE DI INTERNET: Virus, Trojan Horse e Dialer][][][][][][]

Quante volte vi è capitato di andare su un sito "hacker" (perchè così si fanno chiamare, ma in realtà solo sono una bacheca di programmi inutili), e trovare una lista di programmi da scaricare tra quali virus e trojan horse.
I virus credo che sappiate cosa sono.... ok meglio rinfrescarci la memoria.

VIRUS: i virus informatici, sono dei codici, scritti in diversi linguaggi di programmazione, che sfruttano dei bug del sistema operativo, per fare danni, duplicarsi ed infine rispedirsi.
Esistono tantissimi tipi di virus, e possiamo ritrovarceli nel nostro sistema in svariati modi, il più usato adesso è per e-mail.
Per proteggerci dobbiamo adottare poche e semplici regole:
1) non aprire mai allegati provenienti da indirizzi e-mail sconosciuti.
2) avere un antivirus, aggiornato costantemente.

TROJAN HORSE:

Tradotto letteralmente "cavallo di troia", bhe funziona letteralmente nello stesso modo.
La conoscete la storiella del cavallo di troia, no?
Allora, questo programma si divide in 2 parti: client e server.
Il client è la parte che risiede nel computer dell'attaccante (del LAMER), il server è il programma che l'attaccante dovrà installare sul computer della vittima per far si ke avvenga la connessione tra i 2 pc.
Il tutto si svolge così: una volta installato il server l'attaccante si connette ad internet ed aspetta che la vittima si colleghi alla grande rete. nel pc dell'attaccante arriva una notifica tramite ICQ, che segnala la vittima on-line e consegna all'attaccante l'IP della vittima.
L'attaccante apre il client, inserisce l'IP della vittima e si collega al pc del malcapitato.
Ricordo ke esistono tantissimi trojan che permettono le più svariate azioni da parte dell'attaccante.
[[Questo è il modo più semplice per entrare in un PC altrui, ma è un metodo da LAMER e BASTA.
Se volete diventare qualcosa di più, non usate trojan, al massimo sperimentateli tra 2 VOSTRI COMPUTER, solo per vedere il funzionamento.]]
- Come difendersi dai Trojan:
1) antivirus aggiornato
2) avere un firewall (ne parleremo dopo)
3) okkio alle e-mail

NOTA: ormai tutti gli antivirus riconoscono i trojan, questi programmi ormai hanno vita breve.

DIALER:

I dialer sono programmi che una volta scaricati, vi disconnettono dalla vostra connessione abituale e si connettono a numeri tipo 899, facendo levitare la vostra bolletta di molto.
Di solito questi programmi si scaricano da siti hard o siti ke offrono servizi per mandare le suonerie ai cellulari.
Ragazzi state attenti!
N.B. con l'adsl non c'è il rischio di essere disconnessi.

[][][][][][][Sicurezza][][][][][][]

Sicurezza, quando connetti il tuo pc alla rete non esiste la sicurezza al 100%, come dice anche il motto del sito, "un computer sicuro è un computer spento".
Eh si, sagge parole... Ma cosa dobbiamo fare per essere sicuri su internet. A dir la verità se non siamo amministratori di rete di grandi aziende (anche perke dubito ke questi stiano seduti davanti al loro pc leggendo queste righe!!), non dovremmo avere grossi problemi di sicurezza.

Ma fidarsi e bene e non fidarsi è meglio, quindi.... apriamo le danze!

FIREWALL:

Letteralmente traducibile come muro anti-incendio, il firewall si interpone tra internet ed il vostro computer, osservando tutto il traffico in entrata ed in uscita. Quando il firewall rileva qualcosa di anomalo, chiude la porta al quale quel "qualcosa di anomalo" che stava entrando nel nostro pc, domandando a noi il permesso di farlo entrare o sbatterlo fuori.
Facile come funzionamento, no?
Per noi utenti domestici sono stati pensati firewall di tipo software, cioè, programmi installabili sul nostro pc. Le grandi aziende hanno computer adibiti a firewall, ovviamente molto + efficaci del nostro (se configurati bene).
Vorrete sapere adesso dove reperire questi firewall. Andate su www.google.it, cercate "firewall", usciranno tantissimi risultati.
I migliori firewall domestici e gratuiti sono Zone Alarm e Black Ice.

ANTI-VIRUS:

Credo che sappiate che genere di programmi siano... bhe sono dei programmi che tengono sotto controllo tutto il contenuto del vostro pc, permettendovi di effettuare scansioni alla ricerca di virus, controllo delle e-mail in entrata ed in uscita.
Se avete un computer potente optate per il Norton Anti-virus, va anke a meraviglia AVG, e la nuova versione del Panda antivirus.
===IMPORTANTE=== ricordarsi di tenere sempre aggiornate le definizioni del proprio antivirus!!

AD-WARE:

Poko conosciuti, perche è un fenomeno che si è formato da poco tempo.
Esistono programmini chiamati SpYware, programmi che si insediano nel vostro pc, e, ogni volta che vi connettete ad internet comunicano al loro "padrone" i vostri dati personali, ad esempio:
quando vi connettete ad internet, i programmi usate maggiormente, cosa digitate sulla tastiera ecc..
Nel giro di 2 mesi se lo SpyWare non viene eliminato, queste persone avranno una "scheda" di tutte le vostre abitudini, e forse anke password o dati personali in qualche server sparso per il pianeta.
Non vi preoccupate, basta installare sul vostro pc un piccolo programma, AD-WARE 6.0 (oppure Spy-Bot searching & destroy) un programma che svolge le funzioni dell'antivirus, ma mirate agli Spyware.

[][][][][][][Anonimità][][][][][][]

Cosa permette agli hacker di non essere mai rintracciati?
Cos'è un proxy?
e Un socks?

Questo doveva essere uno tra i primi argomenti, ma ho voluto spiegarvi prima il significato di alcune parole e farvi fare pratica con telnet (in poke parole mi sono dimenticato di inserire questo argomento precedentemente [:D]).
Risposta alla prima domanda, semplice: le altre tre elencate sotto!
Un hacker prima di attaccare un server o una società deve essere il più anonimo possibile, così anke se rimane qualche traccia del suo passaggio, l'amministratore non riesce a risalire direttamente a lui.

PROXY:

Computer o software che ne simulano la presenza in grado di redirigere (reindirizzare) la tua connessione su altri server.
Così non sembra tanto semplice... facciamo un disegnino.

Questa è la connessione che avviene normalmente, ogni volta che ti connetti.

[TU] ----------> [Internet]

Questa è la connessione che avviene usando un proxy.

[TU] ------> [PROXY] -----> [Internet]

Capirete quindi che quando vado su un sito, il sito non loggherà il mio IP ma quello del proxy, quindi sarete anonimi.
Adesso vi do 2 siti da dove scaricare proxy sempre aggiornati.
http://www.atomintersoft.com/products/alive-proxy/socks4-list/
http://www.checker.freeproxy.ru/checker/last_checked_proxies.php

===Configurazione Proxy===

Come si configura il browser per utilizzare i proxy.

Per Internet Explorer

Dal menu Strumenti seleziona Opzioni Internet spostati poi sulla cartella Connessioni.
Qui apparirà un elenco di tutti i provider a cui siete abbonati,
selezionare quello che si vuole usare o si sta usando per la connessione
e clickare su Impostazioni quindi selezionare la casella Utilizza un server proxy
inserire Indirizzo e porta poi clickare su ok.

facile no?

===Programmi Utili===

In poche parole, lasciando attivi questi programmi mentre navigate, loro vi anonimizzeranno senza che voi configuriate il borwser come prima.
Uno, il più famoso, è il multi proxy, poi ne esistono altri come in nuovo JAP Anonimity.
Io sono rimasto alla tradizionale configurazione...

SOCKS:

I socks sono uguali ai proxy, la differenza fondamentale tra i socks e proxy sta ke utilizzando i socks, un computer collegato ad una rete lan protetta da firewall, per accedere a internet passerà attraverso il firewall senza richiedere una trasmissione diretta dell'IP.
Ah, i socks utilizzano di solito la porta 1080, ma li potete trovare anke con porte diverse.

===Programmi Utili===

In proposito, ho scritto una guida all'uso del Sockscap32, un programma che serve ad anonimizzare la navigazione in internet tramite socks.
La guida ed il Programma sono reperibili su www.alexmessomalex.com

[][][][][][][Pubblicazione Siti e piccola introduzione al Ftp][][][][][][]

FTP= (File Transfer Protocol) [con la gentile collaborazione di scherzzi6]

Il ftp è un protocollo usato per trasferire file su internet. Viene usato per permettere agli utenti di scaricare File dai server.
Con ftp si può gestire on-line un proprio sito, su un proprio spazio web, semplicemente trasferendolo (con un processo di up-load) su quest'ultimo.
Questo sitema ti permette di aggiornare 24 ore su 24 il tuo sito internet.
Tutto questo è possibile con programmi appositi come: Smartftp o CuteFtp.
Non è finita qui, si possono anke scambiare kon gli amici song e film tramtie ftp.
Un server ftp è http://www.pablovandermeer.nl/getfile.php?id=13, è pikkolissimo e molto semplice da configurare.

Per adesso ho finito, alla prossima!

By

Sbirilindo