Hacker

e Haching

Chi è e cosa fa

BY

LINOX

Avvertenze

La violazione di un computer o rete altrui è un reato perseguibile penalmente dalla legge italiana (art. 615 ter del Codice Penale).
Alcune delle procedure descritte sono da ritenersi a titolo scolastico/ illustrativo/ informativo e messe in pratica solo su dispositivi in nostro possesso o in ambienti di test controllati.
L'hacking di per sé non è illegale, tutto dipende dalle intenzioni. Se si lancia un sasso con l'intenzione di ferire qualcuno, questo costituisce reato. Se l'intenzione non è quella di ferire qualcuno, ma l'azione porta comunque al ferimento, probabilmente questo non costituisce reato, ma sarete comunque tenuti a pagare per risarcire i danni.
Potrebbe essere considerato illegale fare hacking su qualcosa che avete regolarmente acquistato e che vi appartiene. Ci sono hacker che sono stati puniti perché hanno hackerato i propri dispositivi e computer. Ci sono hacker che hanno fatto hacking su software, musica e film che hanno acquistato e che sono stati citati in giudizio per questo. Nello specifico potreste non essere autorizzati a compiere azioni di hacking su ciò che acquistate, anche se lo fate semplicemente per testare la sicurezza del prodotto. Questo avviene perché molte delle cose che acquistate sono protette da un contratto EULA. Tali contratti esplicitano chiaramente che non è possibile farlo.

Significato del termine

L’hacker del terzo millennio è di fatto quella persona che possedendo capacità e nozioni maggiori della norma riesce a sfruttare la rete per eseguire scorribande all’interno di sistemi a cui normalmente l’accesso risulta essere vietato.
Spesso si pensa all’hacker come a quella persona che si inserisce dentro ai sistemi di banche per accreditarsi sul proprio conto cifre cospicue o che magari, come ci hanno fatto vedere in alcuni film, entra in qualche computer di società di viaggio per prenotarsi viaggi in posti caratteristici del nostro mondo.
Un hacker è uno “smanettone”, uno sperimentatore, sebbene il termine “scienziato pazzo” appaia più adeguato in quanto differentemente dagli scienziati tradizionali, gli hacker seguono l'istinto piuttosto che un'ipotesi formale.

Significato del termine

Questa non è una caratteristica necessariamente negativa. Molti oggetti interessanti sono state realizzati o inventati da persone che non hanno seguito le convenzioni standard di quanto era noto e certo ai tempi.

Gli hacker possono intrufolarsi nei computer degli altri e prendere possesso dei loro account. Possono leggere le vostre e-mail senza che lo sappiate. Possono usare la vostra web-cam senza permesso e possono guardarvi ed ascoltarvi violando la presunta privacy di casa vostra.

Alcuni hacker vedono la sicurezza delle reti come una ulteriore sfida da superare e quindi pensano ai metodi per poter aggirare o fregare il sistema. Il loro obiettivo è quello di superare l'ingegno di chi ha progettato o installato la rete.

Hacher and craker

L'hacher è un buono che vuole arricchire la sua conoscenza. Lavora anche per testare la sicurezza dei sistemi informatici.
Un hacker non è qualcuno che scrive un post da un account di un altro che lascia il proprio social network aperto ed incustodito guarda le password ed accede in seguito ai vostri account . Questo non è un hacker. Un hacker non è nemmeno chi scarica dalla rete uno strumento da script kiddie per violare l'e-mail di altri utenti.

Hacher and craker

Un studio sugli hacker ha fatto emergere che i danni maggiori dovuti ad azioni di hacking sono causati da hacker giovani ed inesperti che danneggiano i sistemi altrui per sbaglio.
Sfortunatamente a volte l'attività di hacking è fatta da criminali ed i loro obiettivi sono illegali, invasivi e distruttivi, questi sono i soli hacker che fanno notizia. Per questi casi è stato coniato il termine di **cracker.**

Se volete fare delle prove di haching limitatevi ad hackerare quello che è di vostra proprietà

I vari tipi di Hacker

Quando l'hacking viene utilizzato contro un governo straniero per compiere azioni criminali di effrazione, intrusione, furto e distruzione per ottenere informazioni politiche o militari, si parla di spionaggio. Invece, quando queste azioni sono realizzate da entità commerciali di governi diversi per impossessarsi di informazioni economiche, si parla di spionaggio economico.
Quando le informazioni pubblicamente accessibili sono sviscerate allo scopo di attaccare una persona o una società, ma nessun crimine è stato compiuto per ottenere le informazioni stesse, allora si parla di document grinding o di OSIntelligence (Open Source Intelligence).

I vari tipi di Hacker

Quando si utilizza l'hacking per comprendere il funzionamento della rete di un'azienda, dei suoi sistemi, applicazioni e apparati al fine di renderli oggetto di un attacco, ma senza introdursi nei sistemi stessi, allora si parla di network surveying.
Quando l'hacking è utilizzato per studiare a fondo un concorrente, senza violare nessuna legge (anche se potrebbe essere considerato comunque meschino e scortese), allora si parla di competitive intelligence.
Ad esempio pensate alla possibilità di stressare una persona o di farla preoccupare per ottenere informazioni.

Esempio di document grinding

Ammettiamo che un hacker voglia sapere dove un'azienda sta per costruire una nuova fabbrica. Userà il document grinding per capire quali sono le persone responsabili di questa decisione. In seguito l'hacker chiamerà i loro uffici per scoprire quali città e fabbriche hanno visitato di recente. Ovviamente queste informazioni sono riservate e nessuno le comunicherà senza allarmarsi. Pertanto l'hacker ha bisogno di trovare un modo per ottenerle in modo “ingannevole”. Non è difficile immaginare l'ipotetica sequenza degli eventi.

Esempio di document grinding

Hacker: Salve, sono il Dottor Luca. Chiamo dalla scuola per parlarle di sua figlia Maria.
Target: Davvero? Cosa ha combinato questa volta?
Hacker: Guardi, le sanguina il naso e non riusciamo a bloccare l'emorragia.
Vorrei chiederle se è stata di recente esposta a qualche agente chimico, sostanze chimiche od altro. Questi sintomi sono rari tranne che in persone che sono state esposte a tali sostanze. Può dirmi qualcosa in merito?
Target: (“vuota il sacco”)
Fare questo non è illegale in molti posti. Sicuramente è causa di stress aggiuntivo.
Senza parlare del fatto che è davvero meschino far preoccupare in questo modo un genitore.

Generalmente si usa Windows o al suo posto Linux.
Chiaramente l'ambiente Linux è quello ideale in quanto tutto è già incluso comprese diverse librerie legate alla programmazione di rete le quali si supportano su determinate estensioni del kernel stesso.

Obiettivi

Quando pensi ad un hacker, questo sta lavorando alla riga di comando. Puoi fare cose complesse e potenti nell'interfaccia a riga di comando (CLI).
Una volta che avrai imparato i fondamenti della riga di comando, potrai iniziare ad usare questi comandi in file di testo (chiamati script); è la più semplice programmazione che ci sia.

Sistema operativo – Obbiettivi

Parleremo di comandi e strumenti elementari per il sistemi operativo Linux. Avrai bisogno di conoscerli per avere familiarità con:

- Comandi generali di Linux
- Comandi di base e strumenti di rete, che includono

Ping – traceroute – netstat – ipconfig/ifconfig -Route

Non effettuare MAI prove verso computer dei quali non sei proprietario!

Comandi

date	Mostra o imposta la data
time	Mostra o imposta l'ora
fsck	Esegue il controllo del filesystem e fornisce un report
cat file	Mostra il contenuto di uno o più file di testo
pwd	Mostra il nome della directory in uso
hostname	Mostra il nome del computer che stai usando
finger user	Mostra informazioni su un utente
ls	Elenca il contenuto della directory corrente
cd directory	Passa dalla directory corrente a directory. Se nessun nome di directory viene specificato, passa alla directory home
cp source dest	Copia il file sorgente nel file destinazione
rm file	Cancella i file. Solo gli utenti con adeguati permessi di accesso (o root) possono cancellare specifici file

Comandi

mv source dest	Sposta o rinomina file e directory
Mkdir directory	Crea una directory con il nome directory
Rmdir directory	Cancella la directory con il nome directory ma solo se è vuota
find / -name file	Cerca i file che iniziano da / con il nome file
echo string	Scrive una stringa a video
Command > file	Redirige il normale output video di un comando verso un file. Se questo file esiste già, esso verrà sovrascritto
Command >> file	Redirige il normale output video di un comando verso un file. Se il file esiste già, esso aggiunge l'output alla fine del file
man command	Mostra le pagine del manuale online relative al comando

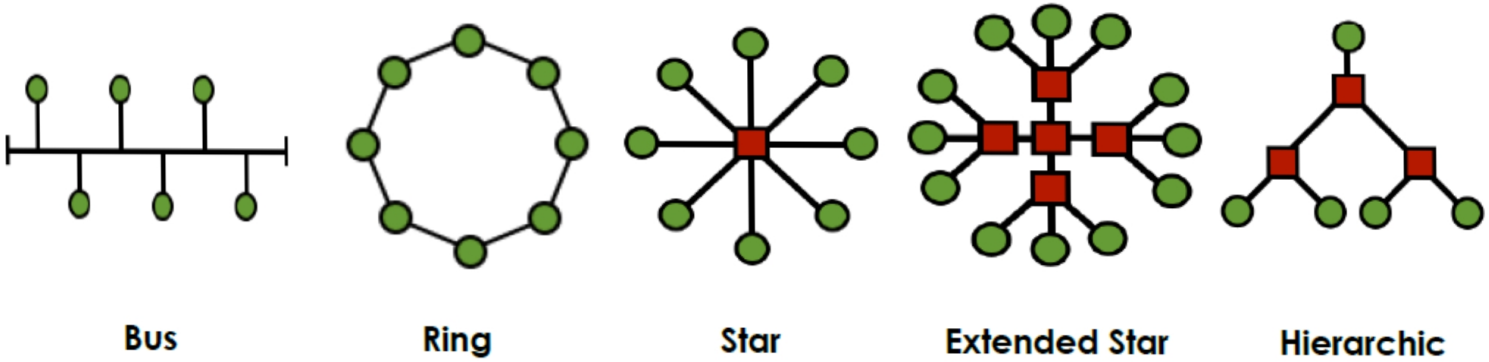
Strumenti

ping host	Verifica la connessione con il computer host
traceroute host	Mostra il percorso che i pacchetti seguono per raggiungere il computer host:
ifconfig	Mostra le informazioni sulle interfacce di rete attive (ethernet, ppp, etc.).
route	Mostra la tabella di routing
netstat	Mostra le informazioni sulle tue connessioni di rete

DISPOSITIVI

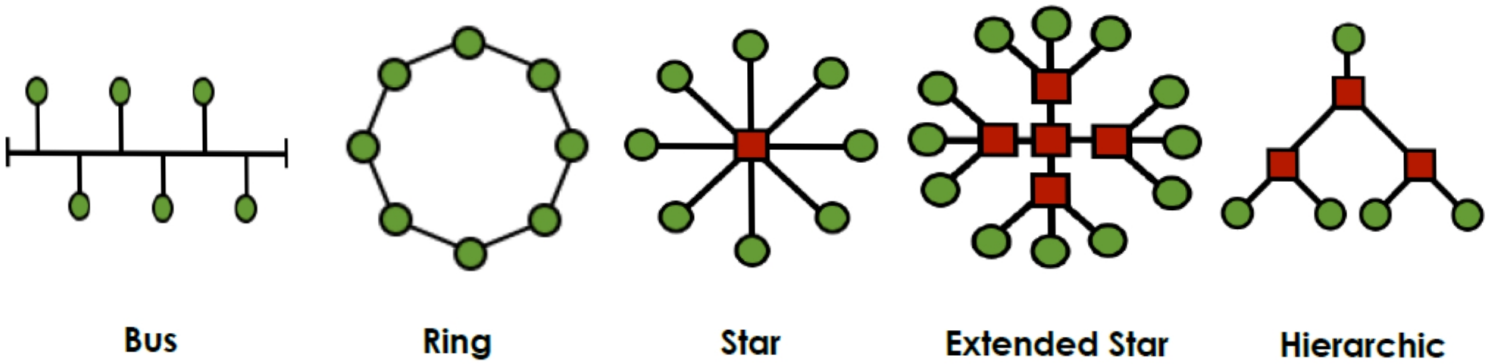
- Un **hub** è come un vecchio centralino: tutti sono sul medesimo filo e possono ascoltare le conversazioni degli altri. Questo può rendere una LAN “rumorosa ma veloce”.
- Uno **switch** filtra il traffico così che solo i due computer che parlano fra di loro possano ascoltare la conversazione. Ma come un hub, si usa solo su una LAN.
- Un **router** si posiziona fra LAN; viene usato per accedere ad altre reti e ad Internet ed inoltre usa indirizzi IP. Controlla i pacchetti che vengono mandati e decide a quale rete appartengano. Se il pacchetto appartiene all'altra rete, indirizza il pacchetto dove deve andare, come farebbe un vigile.

Configurazione reti



- In una topologia a bus, tutti i computer sono connessi ad un singolo cavo e tutti i computer comunicano tra loro. La rottura di una qualsiasi parte del bus comporta l'esclusione di tutti dalla rete. Le topologie a bus sono raramente usate oggigiorno.
- Nella configurazione ad anello, ciascun computer è connesso con il seguente e l'ultimo con il primo e ogni computer può comunicare direttamente con i due adiacenti. Le tecnologie ad anello sono spesso usate al livello inter statale, solitamente con due anelli contro rotanti che inviano il traffico in direzioni opposte per garantire affidabilità e resistenza ai guasti..

Configurazione reti



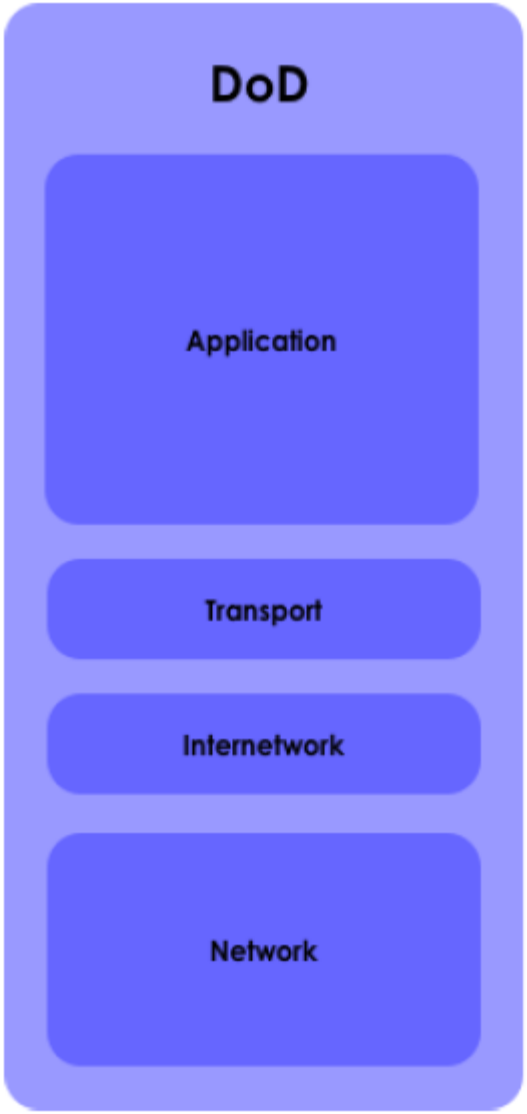
- Nella topologia a stella, nessuno dei computer è direttamente connesso con gli altri, sono connessi attraverso un hub o uno switch che rilancia le informazioni da un computer all'altro.
- Se diversi hub o switch sono connessi uno all'altro, si ottiene una topologia a stella estesa. Questa è la topologia LAN più comune oggigiorno.
- Connettendo insieme due reti a stella o stella estesa usando un punto centrale che controlla o limita il traffico fra le due reti, avrai una topologia di rete gerarchica. Questa è la topologia solitamente sviluppata nelle imprese più estese.

Modello TCP/IP

TCP/IP fu sviluppato negli anni '70 e fu creato per essere uno standard aperto che chiunque potesse usare per connettere insieme computer e scambiare informazioni fra di essi. Il TCP/IP è diventato la base per l'Internet.
Generalmente la più semplice forma del modello TCP/IP è chiamata il Modello DoD ed è ciò da dove inizieremo.

Livelli

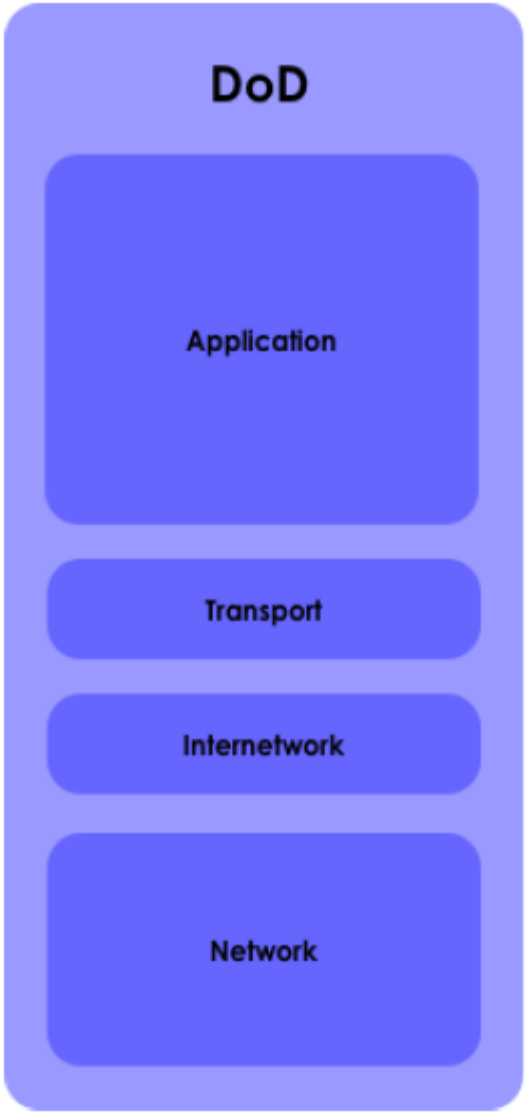
Il semplice modello DoD definisce 4 livelli totalmente indipendenti, fra i quali si divide il processo di comunicazione fra due dispositivi. I livelli attraverso cui passa l'informazione.



Modello TCP/IP

Sono:

- Applicazione. Il livello applicazione è quello dove lavorano le applicazioni
- Trasporto. Il livello trasporto imposta le connessioni di rete internet
- Internetwork. Questo livello aggiunge informazioni circa gli indirizzi di origine e di destinazione e dove il pacchetto inizia e finisce.
- Accesso alla rete. Questo è il più basso livello del network fisico che usi per connetterti all'internet. connessione PPP, se hai una DSL allora starai usando ATM, Ethernet connessione internet via cavo.



Protocolli e porte

- FTP o File Transfer Protocol è usato per la trasmissione di file fra due dispositivi. Usa una porta per inviare i dati e un'altra porta per mandare segnali di controllo (“Ho ricevuto il file! Grazie!”). Le porte più comunemente usate sono la 20 e la 21 (TCP).
- HTTP o Hyper-Text Transfer Protocol è usato per le pagine web. Questo traffico solitamente usa la porta 80. HTTPS è una variante sicura che cifra il traffico di rete, solitamente su TCP porta 443.
- SMTP o Simple Mail Transfer Protocol è il protocollo che invia le e-mail. La sua porta TCP è la 25.

DNS o Domain Name Service è il modo in cui un dominio del tipo google.it viene associato a un indirizzo IP come 216.92.116.13. Usa la porta 53 (UDP).

Protocolli del livello Trasporto

TCP e UDP sono i due protocolli principali usati dal livello trasporto per trasferire dati.

TCP o Transmission Control Protocol stabilisce una connessione logica (una sessione) fra due computer su una rete. Attiva questa connessione usando l'handshake a tre vie.

1.Quando il mio computer vuole collegarsi al tuo, manda un pacchetto SYN per sincronizzarsi.

2.Il tuo computer (se accetterà la connessione) risponde con un pacchetto di riconoscimento SYN/ACK.

3.Il mio computer chiude la procedura con un pacchetto ACK e noi siamo connessi.

Ma questo accade solo con il TCP. L'UDP (User Datagram Protocol) invece è un protocollo di trasporto che non si cura se hai una connessione. Questo rende l'UDP molto veloce, così è utile per molte cose come lo streaming vocale e video.

Preliminari di un hacher

- Identificare il Proprietario di un Dominio. Il primo passo quando si vuole identificare un sistema remoto è osservare il nome dell'host, il nome di dominio o il suo indirizzo IP. Una ricerca whois relativa ad un nome di dominio restituisce molte informazioni.
- Identificare l'indirizzo IP di un Dominio. Puoi recuperare l'indirizzo IP di un dominio con il comando whois, o puoi fare una ricerca DNS (DNS lookup) con il comando ping. La prima cosa che vedrai sarà l'indirizzo IP del dominio.
- Ping e Traceroute. Devi essere sicuro che siano macchine realmente attive, ping è un tuo amico. Usa traceroute per mettere insieme tutte le informazioni che puoi trovare sui computer e i router tra il tuo computer e l'obiettivo,

Preliminari di un hacher

- Nmap. Esegui il comando nmap con un nome host o un indirizzo IP, e lui scandirà quell'host. usa un insieme di attribuiti per fare cose molto complicate. Se fai la domanda giusta, cercherà di dirti il sistema operativo del tuo obiettivo e le porte in uso.
- Netstat, Il comando netstat visualizza lo stato della rete. Netstat può darvi informazioni su quali porte sono aperte e sugli indirizzi IP che vi stanno accedendo, su quali protocolli stanno usando tali porte, lo stato delle porte e informazioni sul processo o programma che le utilizza
- Sniffing. Uno sniffer memorizza il traffico di rete sul vostro computer, consentendovi di esaminare i dati.

Uso sicuro della posta

Le vostre e-mail possono essere usate contro di voi. Le e-mail dovrebbero essere considerate come cartoline, chiunque le vede può leggerne il contenuto. Non dovreste mai inserire in una mail ordinaria qualcosa che non volete venga letta. Detto questo, esistono strategie per rendere sicure le mail. Vediamo qualche consiglio..

Uso sicuro della posta

- Phising e Frodi. Si ricevono mail da persone mai sentite che vi chiedono di comprare software, medicine e beni immobili, senza menzionare chi chiede aiuto per far uscire dalla Nigeria 24 milioni di dollari. Questo tipo di pubblicità viene chiamata spam. Sorprende molte persone il fatto che le mail che ricevono possono fornire una gran quantità di informazioni ad un mittente, come quando la mail è stata aperta e quante volte è stata letta, se è stata inoltrata, ecc. Questo tipo di tecnologia – chiamata web bug – è usata sia dagli spammers che dai mittenti legittimi. Inoltre, la risposta ad una e-mail o la selezione di un link può indicare al mittente che è stato raggiunto un indirizzo attivo.
- Phishing. Avete mai ricevuto una mail che vi chiede di effettuare un login e verificare le informazioni relative al vostro account bancario? State in guardia perché è un tentativo di rubarvi le informazioni di accesso.

Per proteggervi da questo tipo di attacchi esistono semplici strategie.

Uso sicuro della posta

- E-Mail HTML. La sicurezza relativa alle mail basate su HTML è l'uso dei web bugs. I web bugs sono immagini nascoste nelle vostre e-mail che si collegano al server del mittente e che forniscono la notifica del fatto che voi avete ricevuto o letto la mail. Come regola, si dovrebbe usare un cliente di posta che consenta di disabilitare il download automatico delle immagini allegate o inserite nella mail. Un altro problema è associato agli script nella mail che possono lanciare un'applicazione se al browser non è stato aggiornato per coprire le falle di sicurezza. Se dovete usare mail HTML, fate attenzione!

Uso sicuro della posta

- Sicurezza degli allegati. Un altro problema legato alla sicurezza della posta ricevuta è quello degli allegati. Gli allegati sono un veicolo per malware, virus, cavalli di Troia. La miglior difesa contro tutto questo è non aprire gli allegati provenienti da chi non si conosce.

SICUREZZA DELLA POSTA ELETTRONICA

Non aprite mai un file con estensione .exe o .scr, poiché si tratta di file eseguibili che possono infettare il computer con un virus. Fate attenzione a file che assomigliano a tipi conosciuti, come i file zip. Viene cambiata l'icona e nascosta l'estensione in modo tale da non far capire che si tratta di un eseguibile.

- Intestazioni contraffatte. Occasionalmente potreste ricevere mail che sembrano essere state inviate da qualcuno che voi conoscete. Il problema è che contraffare un indirizzo di mail non richiede particolari conoscenze tecniche. Per fare questo, fate una semplice modifica alle impostazioni nel vostro software cliente di posta. Dove vi viene chiesto di inserire il proprio indirizzo e-mail (Opzioni, Impostazioni o Preferenze) inserite qualcos'altro. Da qui in uscita tutti i vostri messaggi avranno un indirizzo di ritorno falso. Questo significa che siete sicuri di non essere identificati? No, non esattamente.

La maggior parte degli ISP autenticano i mittenti e evitano l'inoltro, ciò significa che dovete essere chi dite di essere inviando una mail tramite il loro server SMTP. Gli hacker e gli spammer spesso agiscono su un server SMTP sul loro PC e quindi non devono autenticarsi per inviare una mail e possono simulare di essere chi vogliono. L'unico modo sicuro per sapere se una mail sospetta è legittima, è conoscere il mittente e chiamarlo. Non rispondete mai ad un messaggio che sospettate sia stato contraffatto, poiché questo fa sapere al mittente che ha raggiunto un indirizzo attivo.

Thank You !