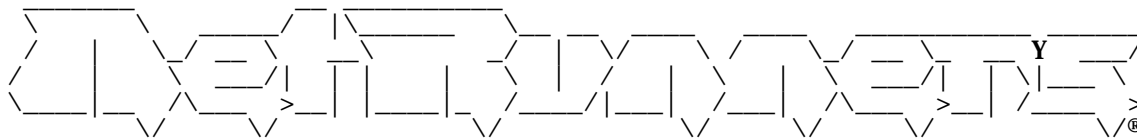


NtRun0. txt



NumEro Zero

Sommario:

Giusto per conoscersi	By ChRoMe
Cosa e' Netrunners	By ChRoMe
Chi sono gli SpiPPoLaToRi e che hanno in mente	By Conte Stefy Reiner
Qualcosa sullo spoofing Cenni generali sull'ip spoofing	By Brigante
Tutorial per il redirecting tramite Back Orifice	By ChRoMe
Traduzione di remailer-help remailer@replay.com	By Adam

Giusto per conoscersi.

Ok ragazzi.....come dice il titolo di queste due righe...giusto per conoscersi. Io sono ChRoMe, mi interesso al mondo dei personal da qualche anno... di ciamo dai primi 8080, in su'.

Sono un autodidatta, non ho avuto la possibilita' di fare studi informatici, quello che ho imparato, e' frutto di innumerevoli nottate davanti al monitor e sacrifici economici per comprare i libri da cui apprendere le varie tecniche... per poi metterle in atto, spippolando come un pazzo.

Adesso faccio parte di un gruppo di simpatiche persone, tutte con la stessa passione per i pc, la rete ed in particolare la sete di informazione.

Lungi da me' definirmi hacker, magari lo fossi veramente, come dicevo prima, mi piace cercare di capire come funzionano le cose, e' una passione, c' e' chi va' a pesca, chi colleziona francobolli....io SPIPPOLO.....

OK, mi sembra che puo' bastare....ed ora altri ragguagli....hehehehehe

ChRoMe SPP meMber

#

Cosa e' NetRunners.

Bella domanda... forse sarebbe stato meglio dire, che cosa sara' NetRunners.

L'idea di base e' semplice... NetRunners sara' un contenitore di informazioni, le piu' svariate, che di volta in volta ci porteranno a cercare di capire, migliorare, ridere, riflettere... insomma, se la storia andra' avanti, con la collaborazione di tutti, e per tutti non intendo solo gli SpiPPoLaToRi, ma anche di chi leggera' questa (newsletter?MailingList?Immune cazzata?... non so' come definirla... fate voi), ci potremmo scambiare un sacco di cose che andranno dai siti di un certo interesse, a l'uso di programmi, alle giude su determinati argomenti.... chi piu' ne ha, piu' ne metta.....

Certamente, l'indirizzo degli argomenti trattati, avra' una preferenza verso l'hacking, la sicurezza della rete, lo sviluppo di nuove tecniche di

Difesa\Attacco di un sistema..... ma non necessariamente, potremmo parlare di tutto... basta sia interessante per chi segue (dai, in qualche modo bisogna chiamarla)... questa E-Zine....

I primi numeri (sempre se la cosa avra' un seguito) saranno di assestamento, di

NtRun0. txt

pianificazione, cercheremo di vedere cosa realmente ci interessa fare.....
Sikke' potrebbero risultare noiosi, come questa, oramai gia' troppo
lunga, introduzione... ma se la collaborazione parte, credo che la cosa potrebbe
anche diventare interessante.....

Ok Boyz... ora passo la patata al nostro Coordinatore. hehehehe che
parolona... che vi illustrera' la filosofia del nostro gruppo...
A dopo... hehehehehe

ChRoMe SPP member

#

Chi sono gli SpiPPoLaToRi
e che hanno in mente

Filosofia del gruppo redatta da quel brav' uomo del Conte Stefy Reiner

Gli

04-07-98
ASCII
by
/Ri goR MorteM

Presentano:

Titolo: SpiPPoLaTorI Philosophy

By Conte Stefy Reiner
tradotto da:
note:

Il club SpiPPoLaTorI ha lo scopo, forse un po' presuntuoso, di accrescere
le conoscenze dei facenti parte in vari campi tecnologici.
E' un gruppo di persone che non hanno nulla da nascondere ma preferiscono
l'anonimato e la discrezione, non vogliono sottrarsi alle norme vigenti
nel proprio paese e intendono rispettarle in quanto sono animali socievoli.
Ognuno si assume le sue responsabilità, ogni SpiPPoLaRorE non è vincolato
in nessun modo da altri... ma spippola solo per propria scelta...
Le responsabilità del singolo non dovranno in alcun modo ricadere sul resto
del gruppo.
Il club pubblicherà il proprio resoconto nel sito ufficiale...
Sempre attraverso il sito ufficiale sarà possibile fare richieste o reclami
per il contenuto o per aggiornamenti vari...
Tutto il materiale raccolto e pubblicato, è per semplice scopo educativo
e non ci si assume alcuna responsabilità sul suo uso, o sue eventuali modifiche
o eventuali utilizzi impropri...
Il club non ha scopi bellici o anarchici... ma da solo la possibilità di
accedere informazioni per il semplice scopo di conoscerle e quindi cautelarsi
di conseguenza.
La forza del club sta nella sola voglia di conoscere...
La curiosità è il nostro carburante, e il rispetto per gli altri la nostra
bandiera.
Termino esordendo come disse Napoleone ai suoi soldati:
"non avete i cannoni? be, cosa aspettate, prendeteli all'avversario"

e concludo col dire " Fate buon uso di quello che avete a disposizione "

-----> by
SpiPPoLaTorI

Dopo questo documento ufficiale, vi allego uno stralcio di un reply, sempre di
Stefy, apparso su icsv.
E' un pezzo di risposta di Stefy a Maurizio Codogno, non mi addentro in inutili
descrizioni del soggetto, ma ho ritenuto simpatico farvi conoscere, tramite la
risposta intelligente di Stefy, un'altro pezzo del pensiero degli Spp.

____snip-----

Inoltre aggiungo.. che siamo molto burloni.. non ci formalizziamo per i termini... cerchiamo di aiutare chi ce lo chiede .. senza scopi di lucro... e capita anche a noi qualche volta di scoprire qualche cosa di interessante... non solo nuke e backdoor...

Ricordo che molti di voi ci campano con i nuke e le back door e coi virus ... non dimenticatevelo... se ci sono gli amministratori di rete addetti alla sicurezza è solo grazie a qualcuno che cerca di hackerare il vostro orto telematico :)))))) non per questo c'è da fargli un monumeto a questi tizi anzi... ma ogni tanto capita che anche l'hacker ci capisca qualche cosa... di quello che sta facendo

Se ci volete dare dei lamer solo per il nostro nome (che non è altro che una nostra presa in giro) fai pure... ma non si capisce come mai tante persone, invece, in questo breve periodo, ci stanno ringraziando per aver imparato tante cose... o per aver avuto tante delucidazioni...

----snip_____

#

Qualcosa sullo spoofing

Cenni generali sulla tecnica dell'ip spoofing
By Brigante

IP Spoofing

Lasciatemi cominciare col dire che in generale c'è una certa confusione tra lo spoofing e l'hacking, in particolare per i novizi. Bisogna essere attenti a non mischiare i 2 termini, altrimenti si rischia di fare confusione.

Prima di cominciare la spiegazione, lasciatemi dire che ci sono degli ottimi documenti nell'URL riportato alla fine. Andate all'indirizzo e cercate qualcosa del tipo tcpspoof.txt, oppure sequence_attacks.txt o shimomur.txt.

Se siete mai stati sui Newsgoup alt.hacker o alt.hacking, avrete visto molti messaggi del tipo Ho un computer con Win 95.. come posso fare un IP spoofing?. Ma per capire perché bisogna farlo, sono necessarie prima alcune nozioni basilari sul protocollo TCP/IP e sul routing.

Se notate, nei pacchetti che viaggiano attraverso Internet, sono contenute le informazioni sull' IP di partenza e sull'IP di destinazione. In particolare dette informazioni sono contenute negli header, ossia delle vere e proprie intestazioni che si trovano in capo ad ogni pacchetto. I pacchetti devono sapere dove vanno ed il computer remoto a cui inviare le risposte.

Ora, il termine spoofing è usato per indicare il mutamento del proprio indirizzo IP, o dell'indirizzo IP di partenza del pacchetto, così da far sembrare che ci sia qualcun altro dall'altra parte.

Bene, ci sono attacchi che usano questa tecnica, ma sono molto, molto sofisticati.

Questo tipo di attacchi sono in genere fattibili da macchine UNIX o LINUX, perché questi sistemi operativi consentono di avere un controllo dettagliato sulla creazione dei pacchetti IP.. se si sa come fare.

Così lavora ad esempio il SYN Flood Attack. L'attaccante manda migliaia di pacchetti TCP SYN al server in pochi secondi. Questi pacchetti provano a iniziare una sessione con il server così che il server deve allocare alcune risorse alle richieste, e quindi prova a rispondere alla stazione di partenza.

Ma non può trovare questa stazione, perché l'indirizzo IP di destinazione è stato mutato.. così le richieste arrivano, il server alloca sempre più risorse (memoria, ecc.), finché il sistema non collassa per mancanza di risorse.

Ora, supponiamo che voi possiate mutare il vostro indirizzo IP, vediamo cosa accade.

Volete hackerare una macchina remota e volete nascondere chi siete. Okay, giusto. Per fare questo create un pacchetto, ma l'indirizzo IP di destinazione non sarà lo stesso di quello del vostro computer. Così, quando la macchina remota riceve la risposta, cerca di replicare all'indirizzo IP di destinazione. ma anche se trova l'indirizzo, comunque non è il VOSTRO indirizzo. Così voi potete mandare pacchetti, ma non avere niente che ritorna verso il vostro IP.

Ora parliamo della mascherazione dell'indirizzo IP. che non è lo stesso che

NtRun0.txt

cambiarlo. Mascherare il proprio indirizzo è semplice usando un altro sistema, come utilizzare un proxy o uno shell account, per far pensare alla macchina di destinazione che stiamo provenendo dal proxy. Ecco come lavora: avete un browser WEB configurato per accedere ad un server proxy. Inviare una richiesta per una pagina WEB, e il proxy service manda la richiesta al computer di destinazione. Ora, la richiesta avrà come indirizzo di risposta l'indirizzo del proxy, che è diverso dal vostro. Il proxy quindi girerà la risposta a voi.

Primo passaggio: Invio della richiesta

```
[u. u. u. u] [p. p. p. p]
  Voi           Proxy
```

Secondo passaggio: Il proxy gira la richiesta

```
[p. p. p. p] [t. t. t. t]
  Proxy       Computer di destinazione
```

**Per il target, la richiesta sta provenendo dall'IP del proxy

Terzo passaggio: La risposta è inviata al proxy

```
[p. p. p. p] [t. t. t. t]
  Proxy       Computer di destinazione
```

Quarto passaggio: Ricevete la risposta dal proxy

```
[u. u. u. u] [p. p. p. p]
  Voi           Proxy
```

Ora, lo stesso accade quando usate telnet ed uno shell account o due. Voi mascherate l'indirizzo IP del vostro computer telnettando verso uno o più shell account e quindi telnettando verso il computer di destinazione. Questa tecnica usa lo stesso principio sopra descritto.

Brigante

#

Tutorial per il redirecting
tramite Back Orifice

By ChRoMe

1. Introduzione

Questo tutorial e' stato scritto, xche' trovo sempre molte richieste di come poter reinstradare il proprio ip, tramite l'ip di un boservizzato. Questa tecnica non ha nulla a che fare con l'ip spoofing, e non e' neanche sicuro al 100% ma e' sempre meglio di nulla..... Il tutorial e' stato scitto in base alle mie conoscenze del client dos di Bo, xche' non uso gran che' la gui dello stesso... ma i comandi sono li stessi.. piu' o meno. Vi consiglio di leggervi il file bo.txt, che trovate in ogni release del Bo, troverete molti esempi e comandi non trattati in questo tutorial

E non fara' altro che accrescere la vostra conoscenza sul programma.

2. La reindirizzazione

Per questo esempio, useremo un ip del tutto casuale
Mettiamo che il vostro host (l'ip del pc ospite.. che avrete
gia' infettato con
il Bo) sia 152.170.135.133
Mi pare ovvio che voi dovrete mettere l'ip vero, del vostro pc
ospite, altrimenti
non avete capito nulla..hehehehehe
Dicevo, mettiamo che l'ip sia quello di cui sopra, e voi
vogliate usarlo per
reindirizzarvi su un server irc di efnet (se non sapete
cosa e' irc...
documentatevi, ma state tranquilli, vi spieghero' altri usi del
redirect piu'
avanti)
Il server di efnet che useremo per questo esempio
sara' irc.mo.net
che risponde all'ip 209.16.213.131

Allora, assumendo che abbiate gia' la connessione con il vostro
host attivata
se non l'avete..attivatela con il comando
HOST <vostro ip> seguito da return.....
dovrete digitare la seguente riga di comando

```
rediradd 6667 209.16.213.131
```

Il prompt di risposta che vi apparira' sara'... piu' o meno... questo

```
B0:152.170.135.133>rediradd 6667 209.16.213.131
```

ok, spiego la sintassi della riga:
rediradd inputport outputip:port,u
Nota: se non viene specificata nessuna porta di output, verra'
usata quella di input
Nota: Se non viene specificato UDP (usando il parametro u),
il valore di default
sara' TCP (nel nostro esempio noi lasceremo di default il protocollo TCP)

Analizziamo meglio l'esempio:

```
B0:152.170.135.133>rediradd 6667 209.16.213.131
```

6667: e' la porta di input(e, se non si specifica nessun'altra porta di output,
sara' anche quella di output.....
209.16.213.131 e' l'indirizzo ip di output (il server di irc.mo.net)

Ok allora voi avete appena detto al pc ospite di dirottare
qualsiasi connessione
in arrivo sulla sua porta 6667, al server irc.mo.net sulla porta
6667 del
server stesso
Ricordate che le porte sono tutte e due uguali, xche' non abbiamo
specificato
nessun'altra porta di output.

Ok, fatto questo, proviamo a vedere cosa succede sul server.
Aprite il vostro client irc (io uso Mirc...ma credo che anche con
altri client
irc non dovrete avere problemi)

Digitate:

```
/server 152.170.135.133:6667
```

NOTA come sopra....qui' ci va' il vero ip..non questo

NtRun0. txt

dell'esempio.....

Questo ti consentira' di conneterti al server tramite il pc ospite
Quando sarai connesso....prova a dare il comando /DNS su te' stesso
e vedrai

che la risposta che otterrai..non sara' il tuo vero ip,ma quello
del povero

host

Questo e' comodo se ti hanno bannato da qualche canale...

cosi' puoi rientrarci

quando vuoi....

Mi raccomando.non ci fate le teste di cazzo.tipo offese..flames war....

Ricordate che bene o male.se vi vogliono beccare..

..prima o poi...vi beccano

3 Redirecting sul web

Se si puo' fare su irc..figuriamoci sul web.....

Questo metodo puo' essere utile per svariati motivi....

Uno di questi e' il Carding, allora io vorrei aprire una piccola parentesi.

Credo che tutti sappiano che il crading

(uso di carte di credito..non prorio vostre)

e' illegale,e quindi perseguibile ai fini di legge.

**IO CONSIGLIO VIVAMENTE DI NON USARE QUESTO METODO PER FARE CARDING, E NON MI
ASSUMO NESSUN TIPO DI RESPONSABILITA' SU LE AZIONI DI CHI LEGGERA' QUESTO TXT**

Non e' per fare il moralista.vi avverto solamente che puo' essere pericoloso
e non vorrei che poi mi si venisse a cercare me'.....hehehehehe

OK,dopo questa parentesi,tirniamo al redirecting sul web.

Come dicevo prima,i motivi per reindirizzarsi sul web...

sono molteplici,e voi

ne avrete certamente qaulcuno che non sia il famigerato carding...

..allora

provate a fare cosi....

NOTA questo e' sempre un ip di fantasia.

ma adesso dovrete averlo capito....

Al prompt di Bo digitate:

```
rediradd 80 204.71.200.72
```

Come al solito

80 sara' la porta di input(e output)

204.71.200.72 l'ip a cui volete connettervi tramite l'host

Fatto questo aprite il vostro browser e scrivete l'ip del pc ospite

nella finestra dell'url

Carino vero?.hhehehehehe

Vi consiglio di fare attenzione con questo giochino,ricordate che se

state facendo qualche cosa d'illegale,e' bene che monitoriate

le vostre connessioni con netstat,per assicurarsi di non avere connessioni

dirette con il sito che state....visitando

Queste sono alcune situazioni per cui puo' essere comodo,mascherare il proprio
ip, tramite una reinstradazione,ma la vostra fantasia...sicuramente ve ne fara'
scoprire di nuovi.....ora avete un minimo di base..lavorateci

Vi Butto li'..una cosa su cui lavorare.

Le pagine web degli utenti di AOL (una fucina di lamers americani.un po' la tin
di oltre

oceano..)non richiedono ne' il login ne' la password,per editare

le stesse,se il server di Aol riconosce che siete collegati dall'ip del

proprietario della home page in questione

Il segreto e' fare un bel rediradd su la porta 21 (FTP)

quindi usare un client ftp (Cute,Ws_Ftp...o uno dei mille....)

per connettervi al pc host.....

Questa connessione sara' reindirizzata verso members.aol.com

e voi avrete l'accesso alla home del pc ospite.....

ConsiglioUna volta dentro l'ospite.segnatevi il nome dell'user

dove il tipo avra' salvato i documenti,le immagini..e tutto quello che e'

NtRun0.txt

inerente
alla sua HP...generalmente e' in nome della directory
L'url della pagina della vostra vittima sara':
<http://members.aol.com/~username>

Testo Tradotto e ampliato
da ChRoMe SPP MemBER
Testo Originale
By M1loch

._#_

Traduzione di remler-help di remler@replay.com

Tradotto da Adam
Suggerito e mandato da RigoR MorteM

Questo messaggio ti è stato mandato automaticamente in reply al messaggio che
hai
mandato a remler@replay.com col il subject "remler-help".

C'è un programma, che tratta in automatico le mail, installato su questo account
che
prenderà qualsiasi messaggio con i giusti headers e automaticamente te lo
spedirà
anonimamente.

E' capace di assicurare un altissimo livello di sicurezza se tu usi il software
Mixmaster per produrre i messaggi. Puoi scaricare il client Mixmaster da
<http://www.thur.de/ulf/mix/> (Germania). Per favore leggi il manuale e il file
README
per le istruzioni d'uso.

Più informazioni sui remlers anonimi sono disponibili a
<http://www.stack.nl/~galactus/remlers/> .

Per una lista aggiornata di remlers anonimi con statistiche, vedi
<http://anon.efga.org/anon/rlist.html> . Puoi anche prendere la lista facendo
finger
su rlist@anon.efga.org o rlist@anon.lcs.mit.edu.

Puoi usare il remler per mandare le e-mail a remler@replay.com, con l'header
"Anon-To: address", l'indirizzo a cui mandarla anonimamente. Se non puoi
aggiungere
headers alla tua mail, puoi mettere due "due punti" nella prima riga del
messaggio,
seguiti dalla riga "Anon-To:". A seguito un rigo vuoto e l'inizio del tuo
messaggio.
Per esempio:

=====
From: joe@site.com
To: remler@replay.com
Subject: Anonymous Mail

::
Anon-To: beth@univ.edu

This is some anonymous mail.
=====

Il suddetto messaggio sarà spedito a beth@univ.edu anonimamente. Tutti gli
headers
nel messaggio originale sono rimossi. Beth non saprà che il messaggio viene da

Joe e non sarà neanche capace di fare il reply al messaggio. Comunque, ci sono un paio di modi per trovare la vera identità del mittente. Primo, se molti messaggi anonimi sono stati spediti, qualcuno potrebbe comparare gli orari in cui i messaggi sono stati mandati con gli orari di entrata in cui Joe è stato registrato. Comunque, questo può essere prevenuto istruendo il remailer a ritardare il messaggio, usando l'header "Latent-Time: "

```
=====  
From: joe@site.com  
To: remailer@replay.com  
Subject: Anonymous Mail
```

```
::  
Anon-To: beth@univ.edu  
Latent-Time: +1:00
```

This is some anonymous mail.

```
=====  
Il messaggio dovrebbe essere ritardato di un'ora da quando è stato mandato. E' anche possibile creare un tempo casuale aggiungendo una "r" al tempo (+1:00r), che dovrebbe mandare il messaggio in un tempo casuale, ma non più di un'ora. Per esempio, "Latent-Time: 0:00" senza il "+" dovrebbe ritardare il messaggio fino a mezzanotte (orario del sito remailer). L'orario dovrebbe essere nel formato delle 24 ore.
```

NOTA: Questo remailer raggruppa insieme automaticamente i messaggi, per produrre l'effetto sopra descritto.

Un altro problema è che qualche programma di posta inserisce automaticamente la firma. Naturalmente, questa di solito contiene l'indirizzo di e-mail del mittente, e così rivelerebbe l'identità. Il software remailer può essere istruito a rimuovere un file con la firma con l'header "Cutmarks:". Qualche linea contenente solo il carattere che marca il taglio (cutmark character), e qualche linea seguente saranno rimosse.

```
=====  
From: sender@origin.com  
To: remailer@replay.com
```

```
::  
Anon-To: recipient@destination.com  
Cutmarks: --
```

This line of text will be in the anonymous message.

--
This line of text will not be in the anonymous message.

```
=====  
NOTA: Il carattere che marca il taglio (cutmark character) nell'esempio è "--", l'usuale separatore della firma delle e-mail. Se dimentichi di lasciare una riga bianca dopo il "--" nella direttiva "Cutmarks:", la tua firma non sarà tagliata via.
```

A volte vuoi una linea di subject o altri headers nel tuo messaggio anonimo. Headers addizionali possono esseri scritti nel messaggio emesso precedendoli con una linea di "##". Sono permessi headers su più linee con linee di continuazione indentate (rientrate).

NtRun0.txt

=====
From: chris@nifty.org
To: remailer@replay.com

::
Anon-To: andrew@where-ever.org

Reply-To: chris@nifty.org
Subject: A message with user-supplied headers: the subject extends
over two lines

Hi there!

=====
Il remailer può essere anche usato per fare post anonimi su Usenet. Per fare
ciò, manda un messaggio con l'header "Anon-Post-To: newsgroups", al newsgroup a cui
vuoi postare. Per cortesia nota che i nomi del gruppo devono essere separati dalle
virgole (ma non dagli spazi).

=====
From: poster@origin.com
To: remailer@replay.com

::
Anon-Post-To: alt.test, misc.test

Subject: Anonymous Post

This is an anonymous message.

=====
Quando posti messaggi test, usa i gruppi appropriati (alt.test, misc.test). Il
newsgroup a supporto del remailer alt.privacy.anon-server non è un gruppo di
test.

Occorre un subject per i post su Usenet. Il remailer scrive un header "Subject:
none" al messaggio emesso se non aggiungi il subject proprio.

Per citare e rispondere a un articolo (follow-up) e vederlo apparire in un
thread,
devi settare correttamente gli headers "Subject:" e "References:" del tuo
messaggio.

La seguente spiegazione è stata adattata dal file di help di nym.alias.net
(mailto:help@nym.alias.net).

Il subject del messaggio dovrebbe essere lo stesso dell'articolo al quale vuoi
replicare, a meno che non stai replicando al primo messaggio del thread, nel
qual
caso devi far precedere il messaggio originale da "Re: ".

Per costruire un header references, copia l'header references dell'articolo al
quale
stai replicando, e appendi il Message-ID dell'articolo. Se stai replicando al
primo
articolo del thread, non avrai un header di references. In questo caso usa il
Message-ID dell'articolo come header di references. Accertati di lasciare uno
spazio
tra i Message-ID nel tuo header di references. Per esempio, se stai replicando
al
messaggio che include questi headers:

=====
Newsgroups: alt.privacy.anon-server
Subject: Re: anonymous remailers
References: <5dfqlm\$m50@basement.replay.com>

NtRun0.txt

Message-ID: <5dko56\$11v\$1@news02.deltanet.com>

=====
il tuo messaggio anonimo di citazione dovrebbe essere con queste linee:

=====
::
Anon-Post-To: alt.privacy.anon-server

Subject: Re: anonymous remailers
References: <5dfqlm\$m50@basement.replay.com>
<5dko56\$11v\$1@news02.deltanet.com>

=====
[Nota che una linea rientrata in un header del messaggio indica una
continuazione
della precedente linea.] Se stai replicando al primo messaggio in un thread,
con questi headers:

=====
Newsgroups: alt.privacy.anon-server
Subject: Help with PGP
Message-ID: <5e96gi\$opv@job.acay.com.au>

=====
il tuo reply dovrebbe cominciare con queste linee:

=====
::
Anon-Post-To: alt.privacy.anon-server

Subject: Re: Help with PGP
References: <5e96gi\$opv@job.acay.com.au>

=====
L'header "References:" può essere sistemato per includere solo
gli ID dei messaggi che tu stai quotando o a cui stai rispondendo.

Separando i messaggi con dei marcatori del taglio (cutmarks), puoi mandare più
di un messaggio alla volta:

=====
From: me@mysite.org
To: remailer@replay.com
Subject: whatever

::
Anon-To: recipient1@site1.org
Cutmarks: --

Subject: message 1

Message one.

--
::
Anon-To: recipient2@site2.org
Cutmarks: --

Subject: message 2

Message two.

--
me@mysite.org

NtRun0.txt

I due messaggi saranno mandati separatamente, e la firma sarà rimossa. Solo un cutmark è usato nell'esempio, ma puoi usarne diversi in ogni parte del messaggio se necessario. Per maggiore sicurezza, puoi crittare il tuo messaggio col PGP. Il software di remailer critterà il messaggio e lo spedirà. Qui c'è la chiave pubblica del remailer:

```
Type Bits/KeyID      Date      User ID
pub 1000/E7AEC1E5 1995/05/23 Replay Remailer Service <remailer@replay.com>
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i
```

```
mQCKAy/Bo9QAAAED6NMBE5oNGLqUmZvUZTWBfL41B67EVtDHu5VmqrPLX6w0gk8U
lPUNlW/1wACNQAFs/hxKKdOB15d8R7Qk1X7H1KPsdF9AAp8DI Be3MN59Z8i 0IdYB
GW8YhPg2EXnNAZyVQb/CGhDZhm8naq3wsQynZZu4J7DmVD0VsrLnrsHl AAURtC1S
ZXBsYXkgUmVtYWI sZXI gU2VydmIj ZSA8cmVtYWI sZXJAcMVwbGF5LmVvbT6JAJID
BRAvzi nRPRWysueuweUBAVpyA+dmx166/op40+nr90Qj ahqWHdvLYkKi panaLNM4
u0/U8RrkySEj 5n/R0zaJSG4mutZ28DQUEhz7rBHRFRYl eENRti I9TxZZrJVWl nE9
No7VwSW9j Wl pta2rCfu97EWLdPVPLXmXpd90TONHMk8a7sf/Lz5JFWl IK5PSqI /Z
xQ==
=5+RC
-----END PGP PUBLIC KEY BLOCK-----
```

Per utilizzare questa caratteristica, crea un messaggio con due "due punti" nella prima linea, poi l'header "Anon-To:" o "Anon-Post-To:", poi ogni altro comando come "Cutmarks:" or "Latent-Time:", poi una linea bianca, poi la linea opzionale "##" e i tuoi headers addizionali, poi una linea bianca e poi il corpo del messaggio. Critta questo con la chiave pubblica del remailer. Poi spedisilo al remailer, aggiungendo l'header "Encrypted: PGP". Se lo dimentichi, il remailer non saprà che occorre per decifrarla. Inoltre assicuratevi dell'uso dell'opzione "-t" con PGP, o i linefeeds non saranno gestite propriamente.

```
=====
From: me@mysite.org
To: remailer@replay.com
```

```
::
Encrypted: PGP
```

```
-----BEGIN PGP MESSAGE-----
Version: 2.6.3in
```

```
hIwCJD7BWgsRsnUBA/9kVuVl hFcZjh I 5cYFLGEAQi v4fUUI Z+hgPp6SQysToVLTM
d00vWqEb4TJgMRef6pHv4022yRLV6Pb9xaE/Gb82SUZYNE6TvfpxyKbWtRStHPXx
0l sLD+IudqvBQus6DoY/9Cl bbXyi bP6mOCy7gwFZW0y60Mv202ZI 3ufc/i CpgKYA
AAoLD7rvsI+c/Bod/GKAffpHqN2fi msoXrdCEMhI fN+rSC7PnMmaX1c4w==
=afKM
-----END PGP MESSAGE-----
=====
```

Per confondere i possibili aggressori ancora di più, puoi generare del traffico di copertura mandando messaggi crittati con l'header speciale "Null:" piuttosto che l'usuale "Anon-To:" or "Anon-Post-To:". Il remailer cestinera questi messaggi.

Qualche testo dopo che hai crittato il messaggio al remailer è anche reindirizzato. Questo permette di spedire messaggi a qualcuno che è anonimo. Se crei un messaggio crittato con PGP a te stesso attraverso questo remailer, e poi lo dai a qualcuno, questi può spedirti un messaggio mandandoti il messaggio crittato al remailer.

NtRun0.txt

Il remailer poi lo decrittterà e te lo spedirà. Il messaggio rimane anonimo nel processo, così il mittente includerà un indirizzo di ritorno se vuole una replica.

I messaggi inviati con questo modo possono essere crittati usando la caratteristica

"Encrypt-Key:". Qualunque testo seguente una linea che comincia con "***" sarà crittato con questa chiave. Per esempio, se inserisci nel testo semplice del tuo messaggio crittato con PGP:

=====

::
Anon-To: you@yourhost.org
Encrypt-Key: your_password

**

=====

Il messaggio appeso dopo "***" sarà crittato con la chiave "your_password", usando le opzioni convenzionali del PGP. E' molto semplice gestire questi "reply blocks", sia dalla prospettiva del mittente che dal destinatario, usando un nymserver. Per cortesia leggi <<http://www.publius.net/n.a.n.html> per maggiori informazioni (l'homepage per nym aliasnet, la casa del software nymserver).

Per una maggiore irrintracciabilità, il tuo reply block può essere diretto al news alt.anonymous.messages. Poichè devi usare una line di subject quando posti su Usenet, i messaggi spediti usando lo stesso reply block avranno lo stesso subject. Per evitare questo, puoi crittare un messaggio e usare nel subject la caretteristica "Ecrypt-Subject:". Per esempio, se inserisci all'interno del tuo reply block:

=====

::
Anon-Post-To: alt.anonymous.messages
Encrypt-Key: your_password
Encrypt-Subject: your_other_password

##

Subject: This subject is MD5 hashed and IDEA encrypted

**

=====

Il subject sarà convertito a 128 bit e crittato con IDEA usando il modo CFB con la chiave "your_other_password", e stampato in esadecimale (48 characters); e il messaggio sarà postato su alt.anonymous.messages. Il subject originale non può essere ritrovato, solo l'hash MD5 di quello, e poi solo se hai la password. Il subject risultante sarà differente ogni volta per l'uso del modo CFB, così questo aiuta a prevenire l'analisi del traffico basata sull'header del subject.

Codificare il subject (per verificare che il messaggio è diretto a te) richiede software speciale. Un piccolo programma in C che può farlo è parte della distribuzione del remailer, ma una più robusta applicazione dovrebbe essere apprezzata. Puoi ottenere il codice sorgente in ascii come archivio unix TGZ mandando una mail a remailer-source@squirrel.owl.de .

Abuso:

non usate il remailer anonimo per molestare, annoiare, fare spam (tanto meno commerciale), per attività illegali. Gli spammers saranno pubblicamente umiliati.

Se non vuoi ricevere e-mail anonime, manda un messaggio all'operatore, e il tuo

NtRun0.txt

indirizzo sarà aggiunto alla block list. Per maggiori informazioni sul filtrare la
posta indesiderata, vedi <http://www.abuse.net/> .

Puoi avere una lista delle statistiche sull'uso dei remailer mandando una mail
al
remailer con Subject: remailer-stats.

Per avere la chiave pubblica del remailer, manda una mail col subject:
remailer-key
o fai finger su rlist-keys@anon.efga.org o remailer-keys@anon.lcs.mit.edu per
ottenere le chiavi pubbliche di PGP di tutti i remailers Cypherpunk.

Per una copia di queste istruzioni, manda una mail con subject: remailer-help.

Per raggiungere l'operatore, indirizza la tua mail a abuse@replay.com.

~#~

This is the the end, my only friends, the end

By ChRoMe (ancora..e basta....)

Come Cantava il vecchio Jimbo, siamo arrivati alla fine del numero zero
Un numero di prova, di sperimentazione, forse il primo di una lunga serie,
forse..l'unico..mha'.chi vivra' vedra'.
I ringraziamenti di rito..per chi ha partecipato, e per chi vorra' farlo.
Aspetto nuove idee, proposte, adesioni, consigli, critiche, biglietti gratta e vinci,
il numero di telefono di Anna Falchi, il crack per il telnet.....
Facciamo un rubrica della posta?.... (Master...Harlock...e chi e' un risponditore
incallito..potremmo usare questo foglio per rendere pubbliche le innumerevoli
mail che vi (ci) arrivano....)
Facciamo un...SITARIO..proponendo qualche sito interessante?
Con due righe di spiegazione sul contenuto....

Bho.io il sasso l'ho gettato...ora aspetto.la sassaiola...

Se ne vogliamo parlare...facciamolo sul ng...credo che sarebbe un thread...non
meno
interessante di molti altri, che ultimamente, ci girano sopra.

Per qualsiasi, varia ed eventuale....
execrew@bigfoot.com

Ciao Ciao.e grazie dell'attenzione

Netrunners numero =0=
Dagli SPP Per La Rete

NtRun0. txt