Tor&Privoxy: traffico in chiaro VS. traffico criptato.

PROTEZIONE PRIVACY: ANALISI E SOLUZIONE PROBLEMI

Questa mini guida è volta alla comprensione ed alla soluzione del problema della privacy e della sicurezza su internet. Come molti di voi sapranno, quando si naviga su internet, tutto il traffico dei dati in passaggio dal vostro pc verso l'esterno (internet) e viceversa, è "in chiaro". Questa espressione, "in chiaro", trae origine dal fatto che ogni pagina che visitiamo, ogni mail che scarichiamo, etc., etc., può essere tranquillamente "letta" da qualcuno in ascolto.
Il problema diventa ancora maggiore se le nostre attività su internet vengono svolte su una rete wireless senza protezione o con protezioni agevolmente superabili come la crittografia dei dati con chiave wep.

Vedremo un esempio di sniffing di una rete wireless senza alcuna protezione ed un esempio con una protezione un po' particolare. Questa protezione non è nè una chiave wep, nè una chiave wpa ma uno strumento che può essere utilizzato indipendentemente dalla protezione della rete e semplicemente installando due piccole applicazioni sul pc che intendiamo usare per navigare: tor & privoxy. Questi strumentini da ultimo citati possono essere utilizzati con straordinari risultati ad esempio quando si naviga attraverso un HotSpot pubblico... infatti, chi ci assicura che "attaccato" a quell'hotspot non ci sia qualche giocherellone che legga le nostre password di accesso alla webmail o le pagine dei siti web che stiamo navigando?
Bene, provocazioni a parte, vediamo cosa ci serve per analizzare la nostra rete casalinga.

Ingredienti:

PC1 --> Pc con accesso ad internet tramite router/gateway (vittima)
PC2 --> Router/gateway che fornisce l'accesso ad internet (vittima)
PC3 --> Pc in ascolto (attaccante)

Partiamo subito dall'analisi del flusso di dati che girano sulla nostra rete e, precisamente, dall'analisi del traffico generato tra un pc dotato di connessione wireless ed un router/gateway che dà accesso ad internet. Per fare ciò utilizzeremo un programma che sniffa i pacchetti in transito sulla rete attraverso un attacco man-in-the-middle tra i due pc vittime: ettercap.

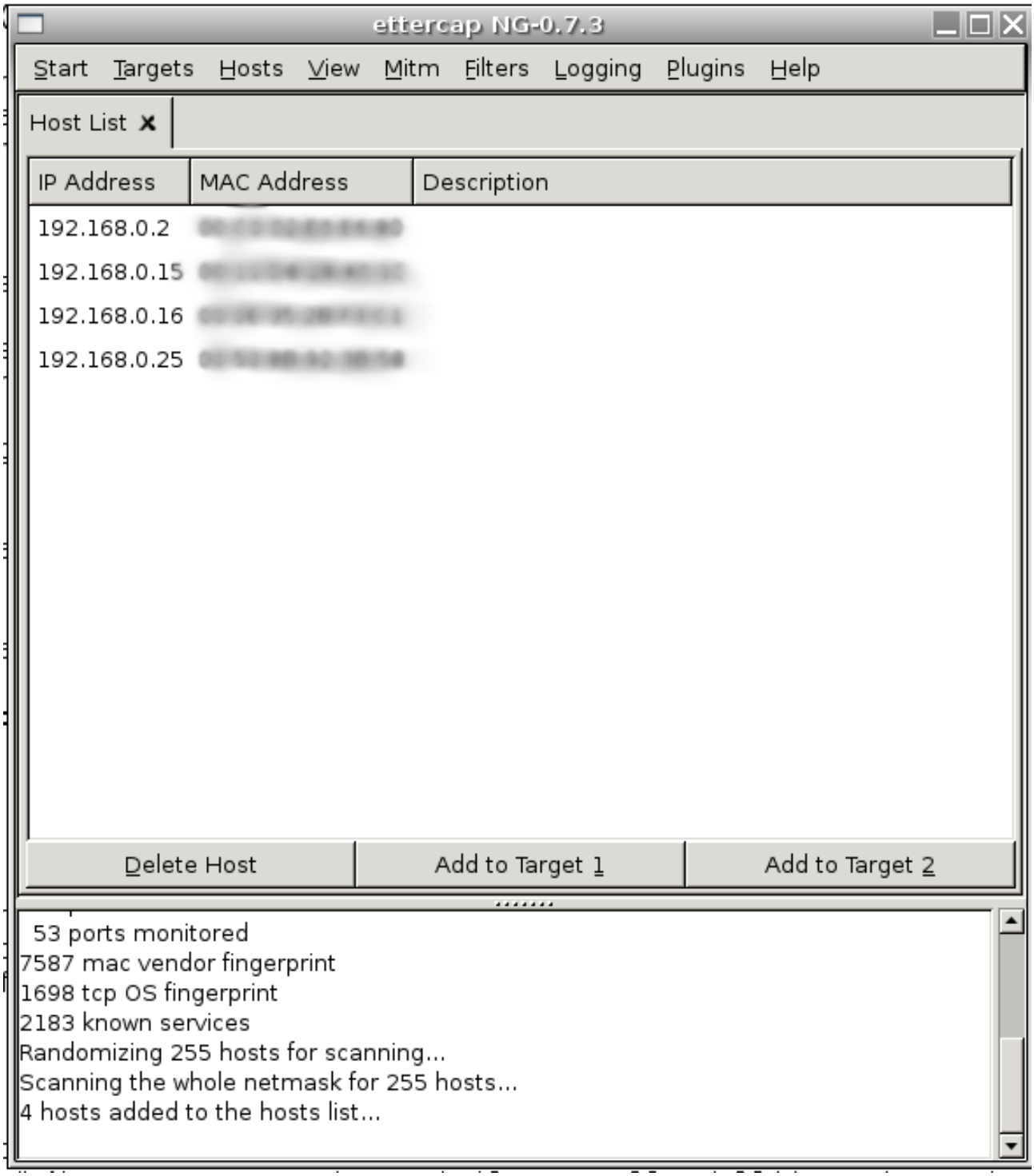
Una parentesi-premessa prima di iniziare sul serio...
Ho deciso di utilizzare ettercap (nonostante sia considerato uno strumento "pappapronta" che non insegna nulla e non sempre è ben visto dai puristi delle reti!) perchè è un programma che permette di analizzare il nostro problema specifico dei "dati in chiaro" senza avere un'ampia conoscenza di come funzioni tecnicamente un attacco man-in-the-middle nè di come si legga il contenuto dei pacchetti che girano tra le due macchine vittime. Per questo motivo chiunque potrà ripetere l'esperimento sulla propria rete casalinga senza dover essere un esperto, salva poi la possibilità per chiunque di approfondire gli argomenti. E' ovvio che questo esperimento può essere ripetuto con gli stessi mezzi anche su una rete wired.

Passo1: Configurazione ettercap su PC3-Attaccante

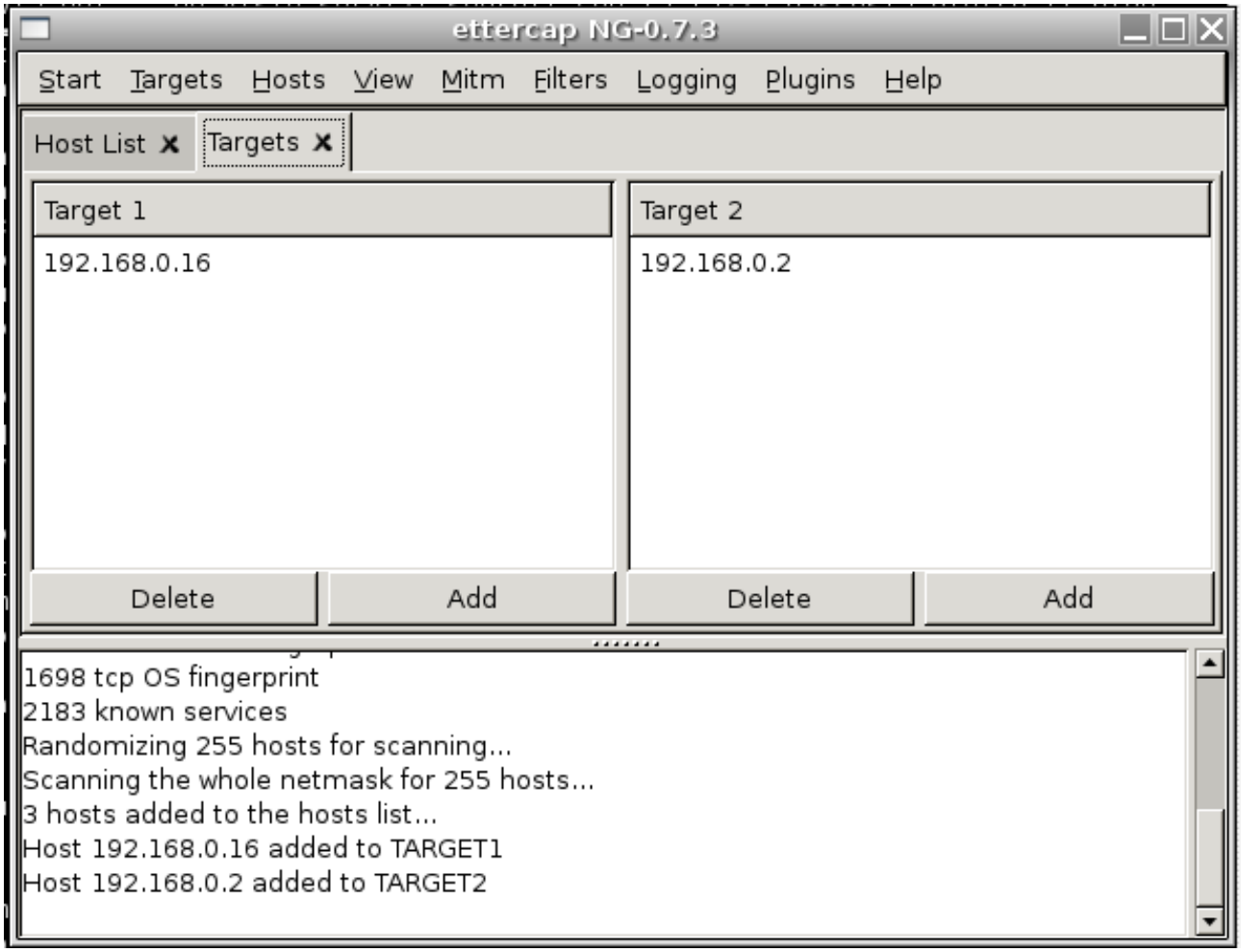
Tutto ciò che ci serve è installare ettercap, magari con l'interfaccia grafica (ettercap-gtk).
Una volta installato, apriamo un terminale di shell e digitiamo da root "ettercap -G" per far partire il programma con la GUI.
Ci troveremo di fronte a questo:

A questo punto selezioniamo nei menu "Sniff-->Unified sniffing". Ci apparirà una finestra dove ci viene chiesto con che interfaccia ethernet vogliamo effettuare lo sniffing. Nel mio caso ho scelto "eth0".
Ci apparirà, poi, una nuova finestra di ettercap...

E' giunto il momento di scegliere le vittime del nostro attacco. Effettuiamo la scelta degli host attraverso il menu "Hosts-->Scan for hosts"
Se adesso aprite la tab degli hosts ("Hosts-->hosts list") scoprirete quanti pc ha trovato ettercap.



Ne scegliamo volutamente 2 (le 2 vittime) e li aggiungiamo ai target attraverso gli appositi pulsanti (Add to target 1 e Add to Target 2), facendo attenzione a che il PC1 sia messo nel Target 1 ed il router (PC2) sia messo nel Target 2.

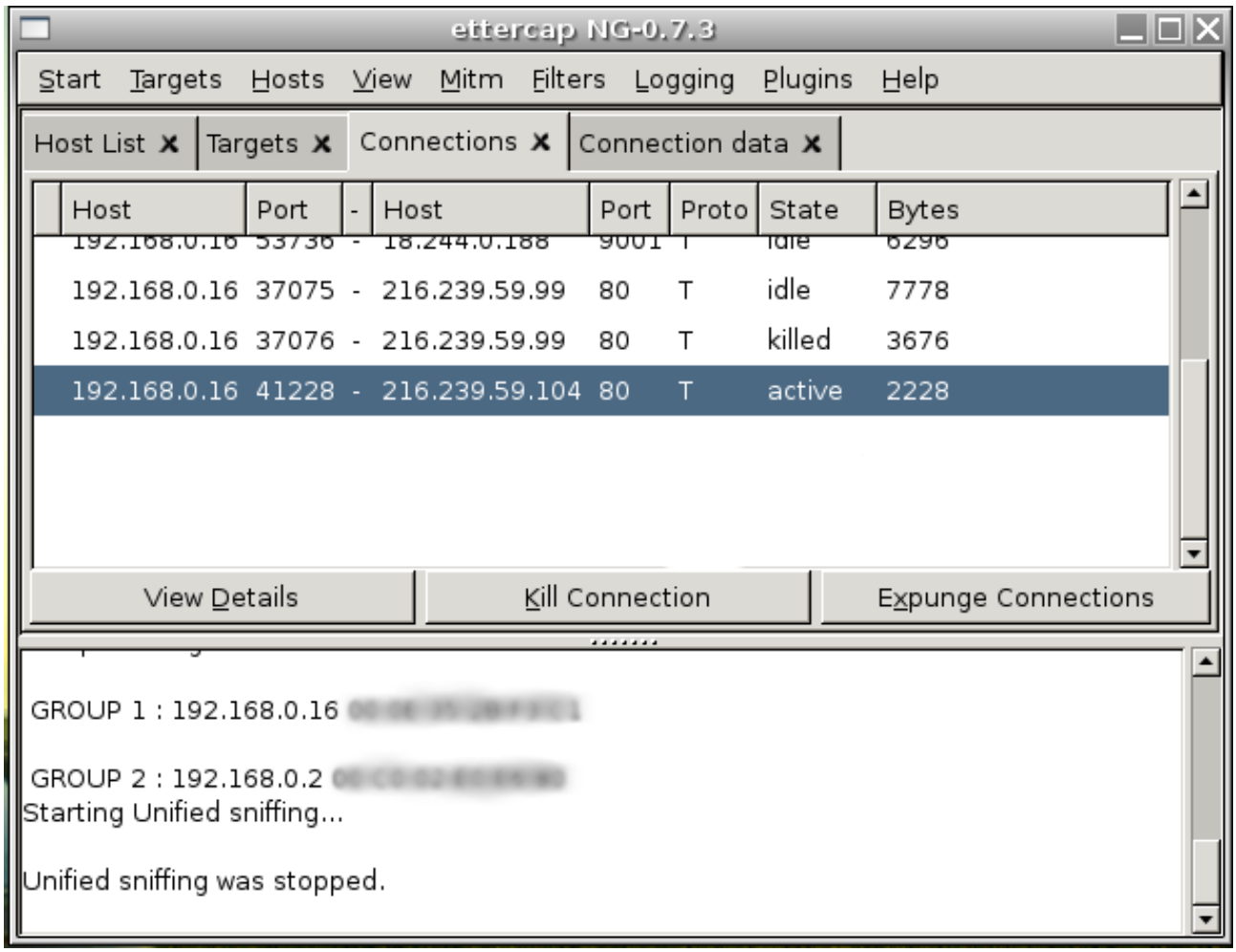


A questo punto manca qualche altro piccolo passaggio ed il gioco inizia.
Selezioniamo il tipo di man-in-the-middle che vogliamo utilizzare tramite il menu MITM.
Sceglieremo l'arp poisoning.
Adesso non ci resta altro che far partire Ettercap: Start-->Start sniffing.

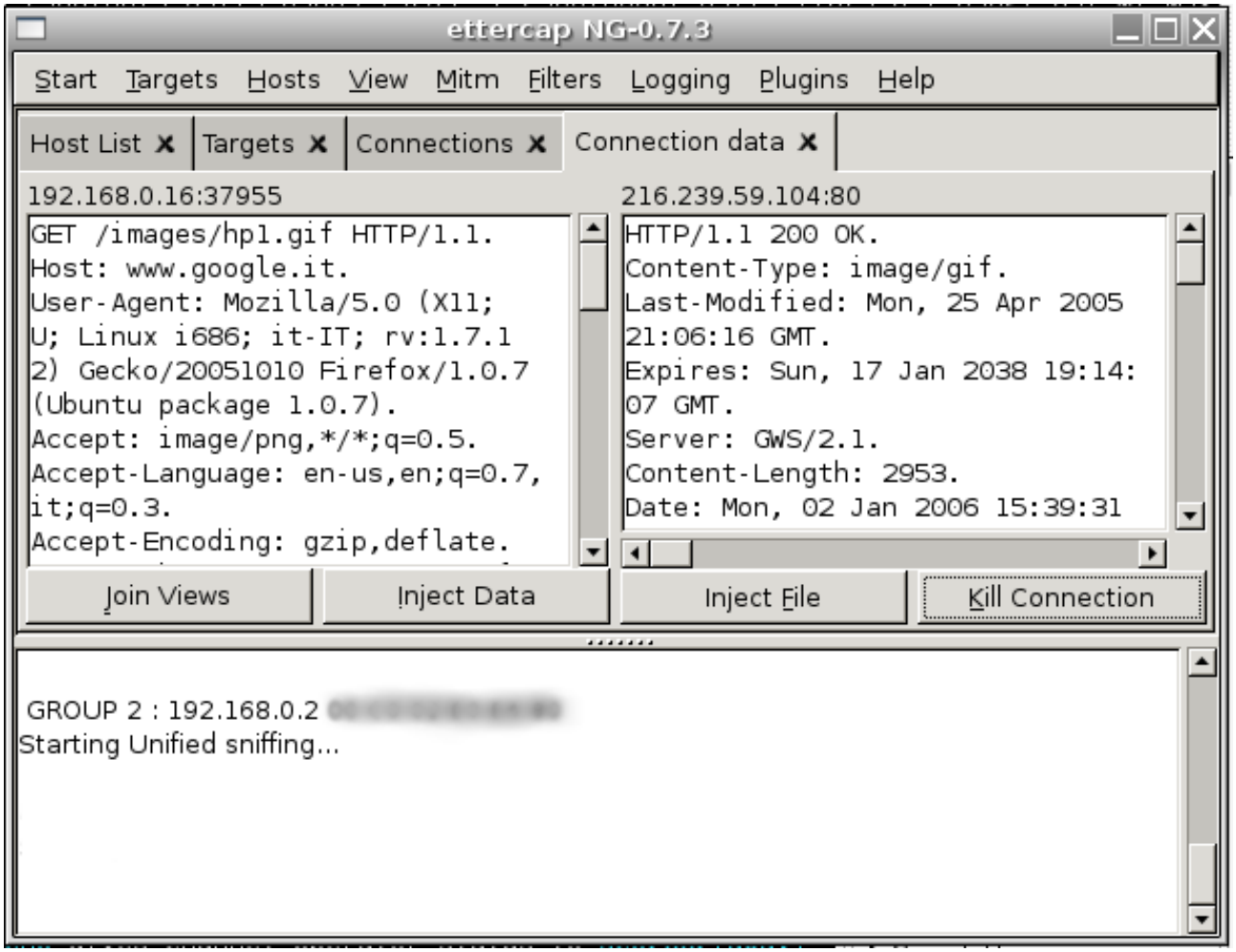
Passo2: Navighiamo dal PC1-Vittima

Bene bene. Rechiamoci sul Pc vittima che si collega ad internet tramite il router/gateway e proviamo ad aprire una pagina web con Firefox (vanno bene anche altri browser, of course). Proviamo a digitare "www.google.it"...

Risultato? Per conoscerlo torniamo sulla macchina attaccante e leggiamo in ettercap cosa è successo... Se apriamo la tab delle connessioni scopriamo qualcosa di sconcertante. L'attività della visita di google è visibile!



Non solo... addirittura possiamo leggere il contenuto della pagina visitata (doppio clic sulla connessione):



Ma non è finita qui. Se ci portiamo di nuovo sulla macchina vittima dove abbiamo digitato l'url di google e proviamo a scaricare la posta elettronica, noteremo che ettercap, addirittura, logga direttamente le nostre user e pass! Il tutto perchè le nostre connessioni sono state effettuate "in chiaro"!

Passo3: installazione e configurazione Tor&privoxy

Come si può fare ad evitare tutto ciò, soprattutto se ci troviamo su una rete wireless pubblica e senza protezione?
Gli strumenti che abbiamo a disposizione si chiamano, come già vi ho detto, Tor e Privoxy.
Per avere informazioni su come funzionano questi strumenti andate qui:
http://tor.eff.org
http://www.privoxy.org

Per ora basta dirvi che tor è un sistema rivoluzionario di server proxy che cripta le nostre connessioni e le fa viaggiare attraverso più proxy. Privoxy è un altro strumento che, interfacciandosi a Tor, fa in modo che il nostro pc devii le sue connessioni http verso la rete di server tor (ha anche altre funzioni come il blocco dello spam pubblicitario sui siti internet, ma per ora nn ci interessano).

Procuriamoci tor e privoxy ed installiamoli con le solite procedure sulla macchina PC1-Vittima.
La configurazione è davvero semplicissima, se vogliamo usare da subito gli strumentini.
L'unica accortezza che dobbiamo avere è quella di modificare una riga nel file /etc/privoxy/config

Precisamente ci rechiamo nella sezione "5.2. forward-socks4 and forward-socks4a" ed inseriamo questa riga:

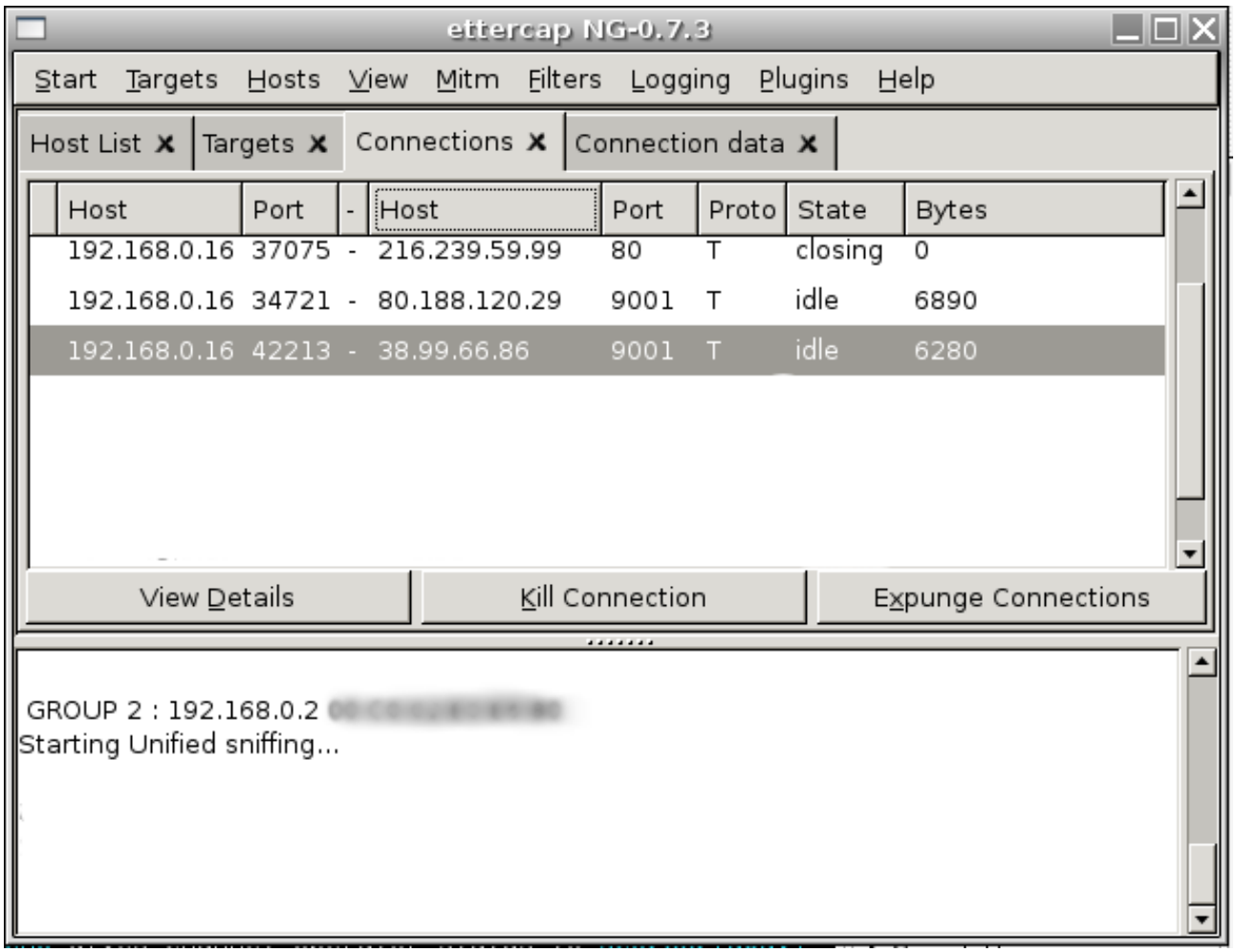
forward-socks4a / localhost:9050 .

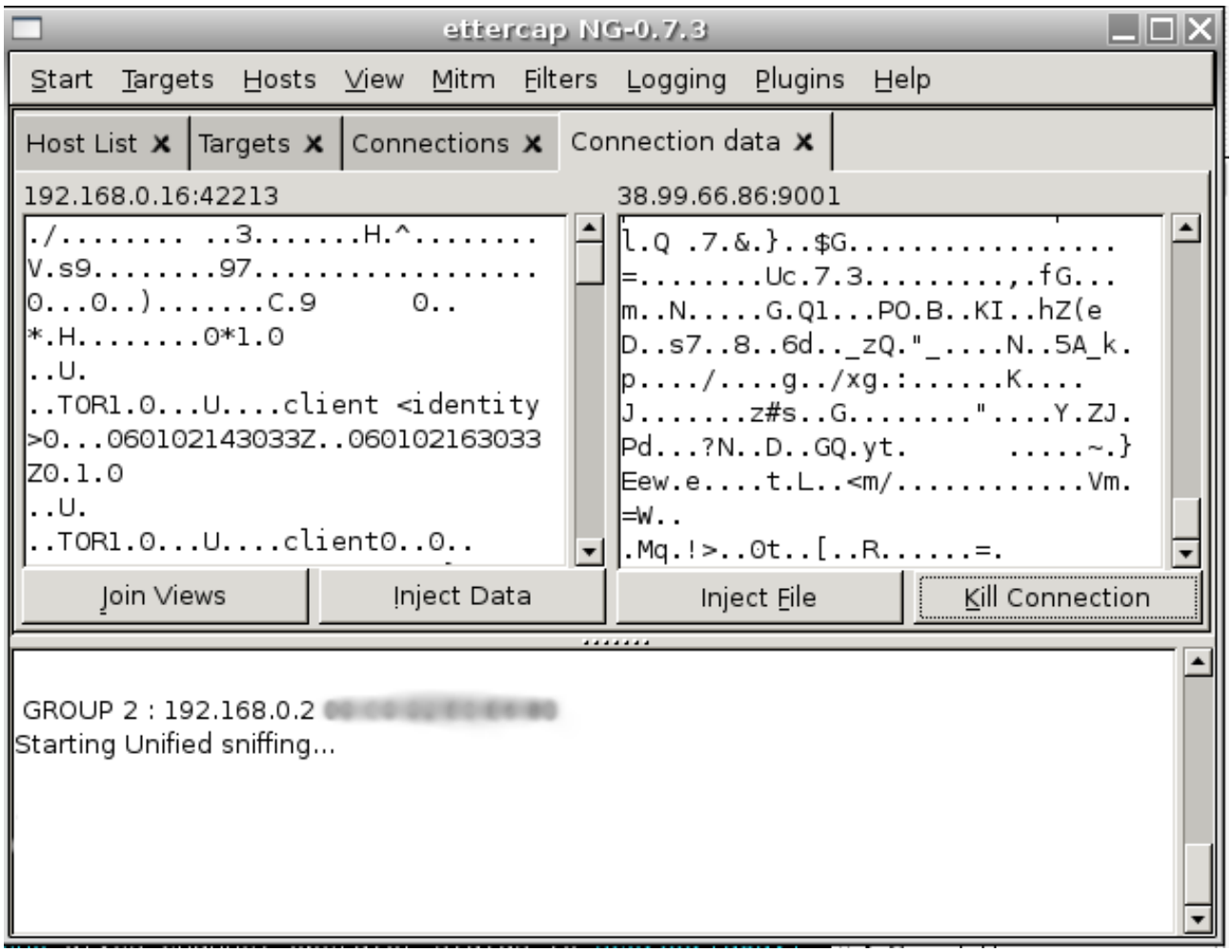
Mi raccomando al punto finale!

A questo punto, dopo esserci assicurati che i servizi Tor e privoxy siano attivi ("ps aux | grep tor" e "ps aux | grep privoxy" oppure ci colleghiamo col browser all'indirizzo 127.0.0.1:8118 e 127.0.0.1:9050), ci dobbiamo recare nelle Impostazioni di connessione del browser (in firefox: "modifica--> preferenze--> tab generale--> impostazioni connessione...") e lì dobbiamo scegliere "configurazione manuale proxy" inserendo in tutte le tab degli indirizzi dei server proxy il valore 127.0.0.1 e la porta 8118. Solo nell'ultima tab (quella relativa ai proxy socks) inseriremo 127.0.0.1 e porta 9050.
Ciò che abbiamo fatto è stato dire al nostro browser di navigare usando come proxy la coppia privoxy+tor che girano rispettivamente su porta 8118 e 9050. Privoxy dalla porta 8118 girerà le connessioni a Tor su porta 9050.
Per verificare che le connessioni passino effettivamente attraverso la rete Tor possiamo fare la prova del 9....
collegatevi sul sito "www.showmyip.com" e verificate se il vostro indirizzo IP attuale è lo stesso di quello assegnato dal vostro provider. Se così non fosse, vuol dire che tor e privoxy stanno funzionando correttamente!

Passo4: la svolta finale.

Fatto ciò, riproviamo il test di ettercap per vedere cosa cambia...
Dopo esserci assicurati che ettercap funzioni a dovere, andiamo sulla macchina vittima e digitiamo www.google.it. Torniamo sulla macchina attaccante e vediamo cosa ha scovato ettercap....


ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins Help
Host List
Targets
Connections
Connection data
Host Port - Host Port Proto State Bytes
192.168.0.16 37075 - 216.239.59.99 80 T closing 0
192.168.0.16 34721 - 80.188.120.29 9001 T idle 6890
192.168.0.16 42213 - 38.99.66.86 9001 T idle 6280
View Details
Kill Connection
Expunge Connections
GROUP 2 : 192.168.0.2
Starting Unified sniffing...



NON HA TROVATO NULLA! NE' PAGINE VISITATE, NE' INDIRIZZI VISITATI, NIENTE DI NIENTE!
L'unica cosa che noteremo è la presenza di collegamenti verso indirizzi ip che appartengono alla rete Tor! Ma il contenuto dei collegamenti e, quindi, l'indirizzo digitato (nel nostro caso www.google.it), la pagina visitata, etc. non sono più visibili ad occhi indiscreti. Stessa cosa se proviamo ad accedere alla nostra webmail!

Passo5: plugin di firefox per Tor&Privoxy, "switchproxy"

Prima ho parlato del browser firefox... c'è un motivo. Mi pare davvero assurdo dover modificare ogni volta le impostazioni del browser per navigare con Tor&Privoxy, anche perchè noterete che la connessione si rallenta e non sempre è utile utilizzare la rete Tor. Esiste un plugin di firefox che switcha con 2 clic la connessione da "tradizionale a proxata" e viceversa. Per sapere come usarlo andate qui:

http://tor.eff.org/cvs/tor/doc/tor-switchproxy.html

Spero di essere stato abbastanza chiaro e che la mini-guida vi sia utile.
Meditate gente, meditate.

Ciao,
Stefano alias zeno