



Attacco a Router Alice Gate 2 Plus

Data: Sabato, 20 giugno @ 22:49:30 CEST

Argomento: 8 - Sicurezza

Sniffing in Lan su rete ethernet gestita da router
Alice Gate 2 Plus?

Con la diffusione delle reti wireless le attività di sniffing, cioè di intercettazione dati, si sono incredibilmente diffuse, indipendentemente dalle chiavi di crittazione usate (wep-wpa). Con l'ausilio di programmini adatti lo sniffer di reti wifi è così facile che è diventata roba da ragazzini.

Ma sniffing di dati su cavi ethernet con router dotato di bridge, come Alice Gate Plus 2?

Questa è la domanda che mi sono fatto, e se siete curiosi leggete questa incredibile guida...(Continua)



Introduzione

Per i meno esperti di reti consiglio caldamente di

leggere [il nostro tutorial principi basei internet e Lan \(clikka qui\)](#), giusto per avere un'idea dell'argomento.

Adesso un piccolo riepilogo di termini tecnici:

Router: E' letteralmente l'instradatore, un dispositivo di rete che permette lo smistamento e l'invio di pacchetti dati. I router domestici sono quasi sempre dotati di modem integrato per permettere la creazione di una lan (local area network), dove diversi computer (client) usano un unico dispositivo di rete (router-server) per accedere a internet o comunicare tra loro. Il router può essere collegato direttamente o separato dai client (pc ad esso collegati) da uno switch, o avere integrato al suo interno un bridge. Il router è quasi sempre configurabile via browser, con immissione user e password, ed essere dotato o meno di un firewall proprio.

Bridge: E' un dispositivo di rete che effettua la mappatura dei pc collegati alla lan con le relative porte e smista selettivamente il traffico dati (forwarding table). Spesso è integrato nei router. Non permette la creazione di lan con numerosi pc.

Switch: E' un dispositivo di rete che inoltra selettivamente i dati ricevuti e inviati dal router

verso il singolo client (pc della lan) interessato alla comunicazione. Permette la creazione di lan con numerosi pc.

Cavo incrociato ethernet o crossover: E' un tipo di cavo di rete usato per connettere assieme dei dispositivi di computer direttamente dove invece vengono normalmente connessi mediante uno switch di rete, hub o router.

Scheda di rete : Interfaccia digitale costituita da una scheda pci o integrata a cui si collegano uno o più cavi ethernet per consentire l'accesso a una rete informatica.

Indirizzo Ip : Un Indirizzo IP è un numero che identifica univocamente un dispositivo collegato a una rete informatica che comunica utilizzando lo standard Internet Protocol.

MAC address: L'indirizzo MAC (in inglese MAC address, dove MAC sta per Media Access Control), detto anche indirizzo fisico, indirizzo ethernet o indirizzo LAN, è un codice di 48 bit (6 byte) assegnato in modo univoco ad ogni scheda di rete ethernet prodotta al mondo.

Sniffing: Si definisce sniffing l'attività di intercettazione passiva dei dati che transitano in

una rete telematica. Tale attività può essere svolta sia per scopi legittimi (ad esempio l'individuazione di problemi di comunicazione o di tentativi di intrusione) sia per scopi illeciti (intercettazione fraudolenta di password o altre informazioni sensibili).

Promiscue Mode : Impostazione dell'interfaccia di rete nella cosiddetta modalità promiscua, che disattiva il relativo filtro hardware permettendo al sistema l'ascolto di tutto il traffico generato dal server che passa dal cavo ethernet o via etere per il wifi.

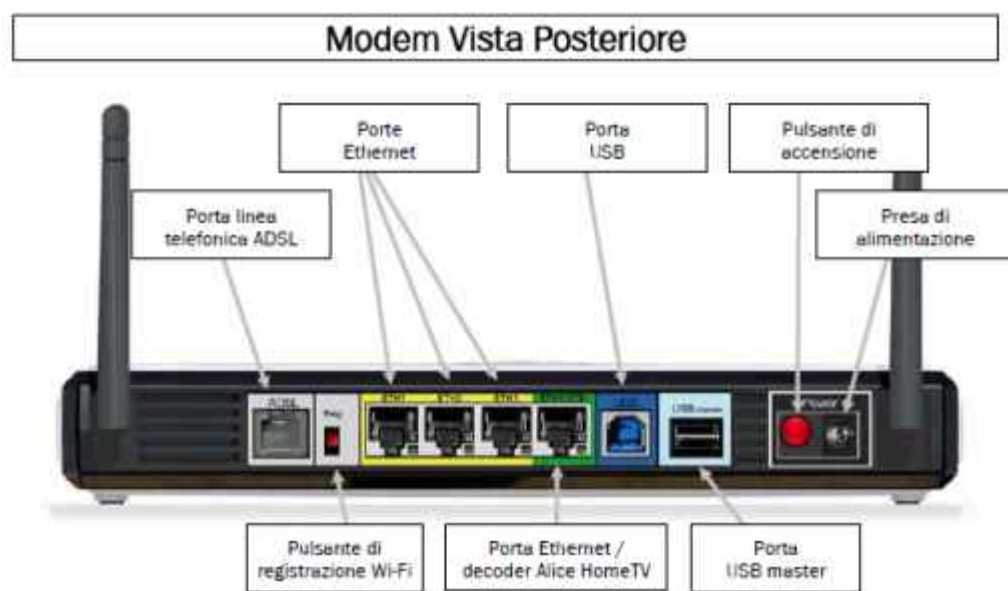
ARP poisoning: In ambito informatico, l'ARP poisoning (detto anche ARP spoofing) è una tecnica di hacking che consente ad un attacker, in una switched lan, di concretizzare un attacco di tipo man in the middle verso tutte le macchine che si trovano nello stesso segmento di rete. L'ARP poisoning è oggi la principale tecnica di attacco alle lan commutate. Consiste nell'inviare intenzionalmente e in modo forzato risposte ARP contenenti dati inesatti o, meglio, non corrispondenti a quelli reali. In questo modo la tabella ARP (ARP entry cache) di un host conterrà dati alterati (da qui i termini poisoning, letteralmente avvelenamento e spoofing, raggio). Molto spesso lo scopo di questo tipo di attacco è

quello di reindirizzare, in una rete commutata, i pacchetti destinati ad un host verso un altro al fine di leggere il contenuto di questi per catturare le password che in alcuni protocolli viaggiano in chiaro.

Dettagli tecnici Router Alice Gate 2 Plus
Vediamo qualche informazione sul router oggetto del nostro test:

- > Standard ADSL:
 - > ITU G.992.1/2/3/5 Annex A
 - > ANSI T1.413
 - > Protocolli Supportati:
 - > RFC 2516 (PPP over Ethernet)
 - > RFC 2684 / formerly RFC 1483 e RFC 2364
 - > Supporto ATM UNI3.1, UNI4.0
 - > OAM F4/F5 Loop-back
 - > Interfaccia ADSL, connettore RJ11
 - > Interfaccia USB full speed (12 Mbps), connettore tipo B ("device"), compatibile con lo standard "Universal Serial Bus Specification" rev.1.1
 - > Interfaccia USB high speed (480 Mbps), connettore tipo A ("host"), compatibile con lo standard "Universal Serial Bus Specification" rev.2.0
 - > Interfacce Ethernet, connettore RJ45, compatibile con lo standard IEEE 802.3 10/100 Base-T auto sensing

- > Interfaccia Ethernet/SetTopBox, connettore RJ45, compatibile con lo standard IEEE 802.3 10/100 Base-T auto sensing
 - > Interfaccia Wi-Fi IEEE 802.11b/g2
 - > Velocità di trasmissione 11/54 Mbps
- > Cifratura WPA-PSK con chiave di 24 caratteri ASCII (256 bit)
 - > Cifratura WEP con chiave di 128 bit (13 caratteri ASCII)
 - > Supporto procedura di registrazione semplificata Telecom Italia
 - > DHCP server
 - > Funzionalità di routing (NAT, NAPT,...)
 - > Virtual Server
- > Configurazione e gestione locale mediante interfaccia locale web based
- > Configurazione e gestione remota mediante protocollo CWMP (DSL Forum TR-069)
 - > Firmware aggiornabile da remoto
 - > Alimentazione 15Vdc 1.2A
- > Alimentatore esterno tipo switching 230Vac 50Hz 0.12A - 15Vdc 1.2A

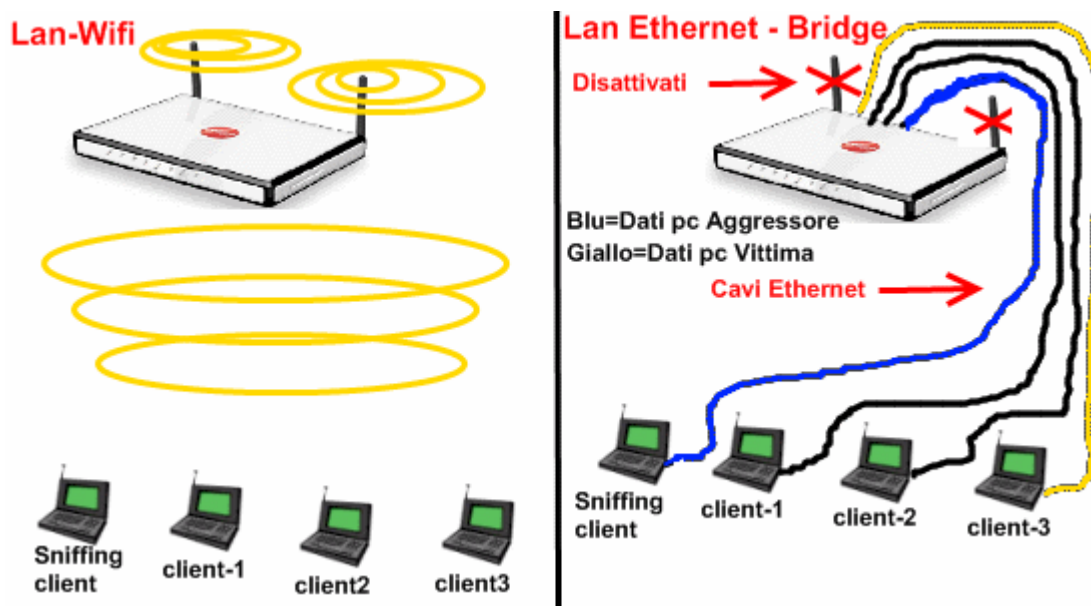


Come potete notare il nostro **Router Alice Gate 2 Plus** è dotato di un ingresso per la linea Adsl costituito dalla prima porta a sinistra grigia, ben 4 porte ethernet di cui tre gialle e una verde che svolge funzione aggiuntiva per il servizio Alice Home Tv, e alle quali è possibile collegare quattro computer per la creazione di una lan domestica, e infine 2 porte usb per l'utilizzo del solo modem integrato. Al Pannello di Amministrazione del router si accede digitando nell barra degli indirizzi del browser (Explorer o firefox o altri...) l'indirizzo ip **192.168.1.1**, o in altri router all'indirizzo **10.0.0.1**, che comunque è di default nel modello specifico e non modificabile. Nei Router con software telecom le impostazioni di configurazione sono minimali, mentre nei router Telecom sbloccati o con firmware pirelli le impostazioni possibili sono quelle di un router professionale. Non si può non notare i due

simpatici antennini usati per la trasmissione wifi. Da notare che tale router usa il sistema **Bridge** per smistare i pacchetti tra i vari pc collegati in lan via ethernet!

La storia...

Per ragioni di sicurezza non ho mai attivato il trasmettitore radio del mio router alicegate, disabilitandolo dal pannello di amministrazione, anche perchè tengo tutti i miei computer in una stessa stanza, e tutti collegati in lan con cavi ethernet. Questo perchè possiedo dati abbastanza importanti nei miei computer e attaccare le reti wifi, come detto in precedenza, è diventata roba per ragazzini vivaci. Una Lan via cavo invece è senz'altro più sicura, soprattutto se provvista di un Bridge integrato, come nel nostro caso. Perchè? Cercherò di spiegarlo nel modo più semplice che posso:



Nella figura di sinistra è rappresentata una rete lan-wifi e a destra una rete lan ethernet con bridge, entrambe con 4 computer presenti:

Client-1, client-2 e client-3 autorizzati, e Sniffing client il pc abusivo dell'attacco.

Client-1 e Client-2 stanno lavorando in locale, quindi non negoziano connessioni di rete, mentre client-3 si collega e inizia una navigazione web generando traffico dati, indicato con il colore giallo.

Nel primo caso, nella lan wifi, i dati vengono trasmessi a tutti i client, compreso quello dell'attaccante Sniffer, alla ricerca del Client-3 che si autenticherà per ricevere i dati. I dati saranno comunque accessibili a tutti, cripati e non, impostando la modalità promiscua della scheda di rete, perchè viaggiano su un cavo comune: l'aria!

La stessa cosa avviene nelle reti lan ethernet che non hanno un Bridge o uno Switch, in quanto il traffico dati viene inviato a tutti i pc anche se la negoziazione è partita da un un singolo pc, che poi è comunque l'unico che accetta la ricezione a meno che un altro client non è in modalità promiscua. Questo sistema però ha dei grossi difetti, sia di efficienza che di sicurezza: di efficienza perchè viene generato traffico oltre il necessario con perdita di pacchetti, rallentamenti e possibili conflitti; e di sicurezza per la facilità di eventuali attacchi di sniffing.

Con il Bridge o lo Switch questi problemi vengono ovviati in quanto entrambi, in modalità e quantità differenti, provvedono a veicolare i dati solo al computer interessato.

Infatti nella seconda figura, notiamo che i dati generati dal traffico di rete del client-3 e marchiatati di colore giallo sono trasmessi esclusivamente allo stesso computer e non agli altri tre!

La mia Lan è rappresentata quindi dalla figura di destra. Adesso, penso che uno dei pochi vantaggi di avere uno come me in famiglia è non avere in generale quasi mai problemi con i computer (eccezion fatta per eventuali irruzioni della Polizia Postale), e quindi ogni componente dell'albero

genealogico stretto può godere di un suo pc personalizzato secondo le esigenze, hardware sistema operativo e software incluso, e c'è anche un pc per gli ospiti. Dovrei essere relativamente tranquillo, e invece no! E se qualcuno usa uno dei miei pc per far danni? O lo usa per spiarmi? E io, a mia volta, potrei usare uno dei miei pc per tenere sotto controllo gli altri o spiarli dalla mia postazione senza che se ne accorgano? E tutto ciò all'interno di una lan con bridge?

Queste sono le domande che mi sono fatto, e la risposta è stata: assolutamente sì!

Gli attrezzi

Se sei arrivato fino a qui, leggendo attentamente e senza saltare nulla, vuol dire che non sei uno stupido lamer, e che la tua è semplice voglia di imparare, scoprire e sperimentare. Ma comunque, anche tu che leggi, per evitare di metterti nei guai, leggi attentamente anche questo:

Il Codice penale al cap.2 ("dei delitti in particolare") dedica un'apposita sezione a tale tema: "Dei delitti contro la inviolabilità del domicilio" (sez. IV). Gli artt. 615 bis e ter specificano le pene per accesso abusivo ad un sistema informatico o telematico, o interferenze illecite nella vita privata.

L'uso improprio e illegale di tale guida

costituisce reato, e l'autore declina qualsivoglia responsabilità in merito.

Bene, allora, si dicevamo degli attrezzi, eccoli:

1) Un computer con Windows Xp o Vista

2) [Advanced IP Scanner v1.5](#)

3) [WireShark win32-1.2.0](#)

Naturalmente questa tecnica risulta efficace anche con sistemi operativi diversi, come Debian o Ubuntu, anzi è molto più facile reperire altri tool alternativi per la scansione della lan, mentre wireshark è tra i migliori anche in versione open source. Scaricate adesso Advanced IP Scanner v1.5 e WireShark win32-1.2.0 sul vostro Desktop cliccando nei links qui sopra.

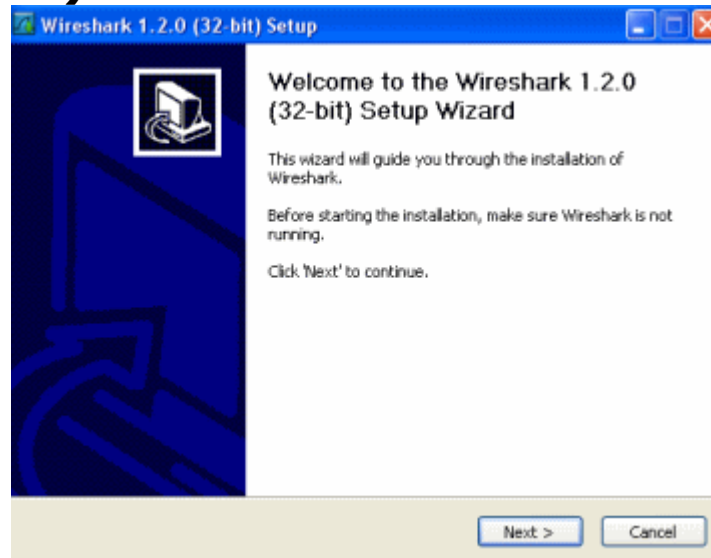
La Tecnica in teoria

Con Advanced ip scanner faremo la scansione completa della lan alla ricerca dell'ipotetico computer vittima, e avremo il rapporto di tutti i pc accesi e collegati alla rete con le relative informazioni: indirizzo ip, mac adress, nome computer e altro ancora. Useremo Wireshark per intercettare tutti i pacchetti che arriveranno alla nostra scheda di rete, anche quelli che eventualmente non abbiamo richiesto, e

avveleneremo il bridge del router mediante un attacco di **ARP spoofing**, per mandarlo in confusione in modo che invii il traffico della vittima anche al nostro pc.

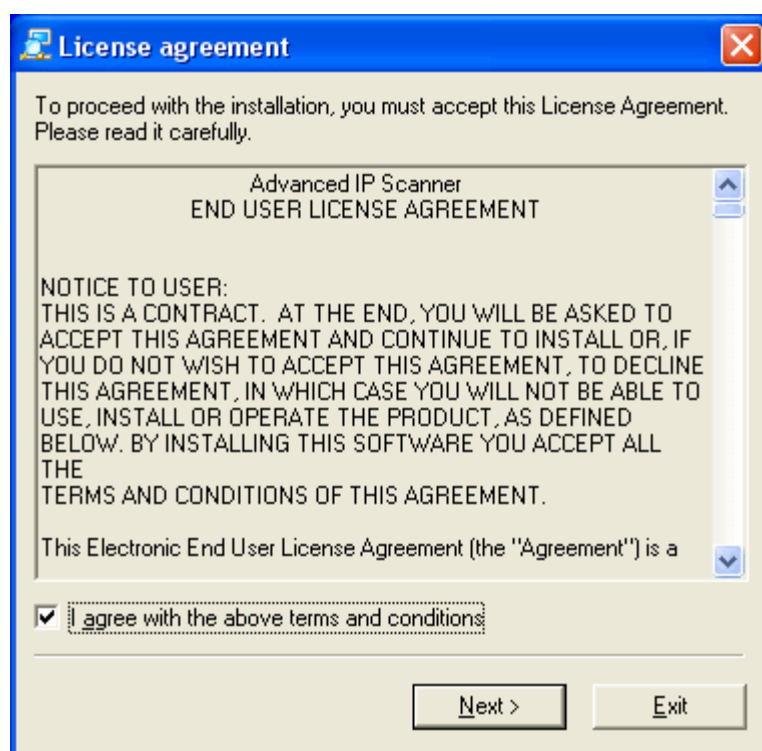
Prepariamo gli attrezzi per l'attacco Sniffer

a) Installiamo Wireshark



Clicchiamo sull'eseguibile di WireShark ed avviamo la fase di installazione, lasciate le impostazioni di default, e cliccate sempre su next. A metà fase di installazione vi verrà chiesto se installare anche i driver e le librerie di **Win Cap**: è un programmino che permetterà l'ascolto dei dati da parte della vostra scheda di rete in *modalità promiscua*, accettate e installate naturalmente!

b) Advanced Ip Scanner 5.1

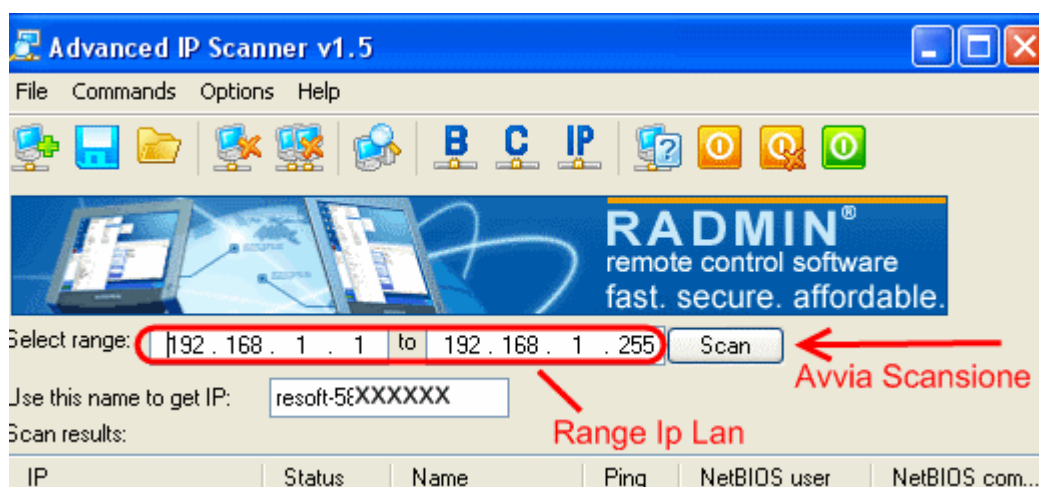


Avviamo l'eseguibile di Advanced Ip Scanner 5.1, accettiamo i termini di licenza, e completiamo l'installazione. Fatto!

Importante: riavviate il Computer dopo aver installato i 2 programmi!

Iniziamo la simulazione dell'attacco di intercettazione dati

La prima operazione sarà data dalla scansione della rete lan, per averne una mappa precisa, e soprattutto per vedere quali sono i computer attivi ad essa collegati ed ottenere le relative informazioni che ci serviranno per portare avanti l'attacco. Avviamo quindi l'Ip Scanner cliccando sull'icona del Desktop.



Nel caso del **Router Alice Gate Plus 2** il range di ip da scansionare sarà da **192.168.1.1** a **192.168.1.255**, se tale range non è stato rilevato automaticamente impostatelo manualmente come descritto in figura e cliccate su **Scan!**

Advanced Ip Scanner effettuerà un ping veloce su tutti gli host attivi, e vi ritroverete in pochi minuti un risultato simile a questo.

IP	Status	Name	NetBIOS user	NetBIOS com...
192.168.1.1	alive 1)	homegate.homenet.telecomitalia.it		00
192.168.1.2	dead	N/A		00
192.168.1.3	dead	N/A		00
192.168.1.4	alive 2)	PC-XXX.homenet.Vista		00
192.168.1.5	alive 3)	resoft-58l Pc-Attacker	telecomital.a.it	00
192.168.1.6	dead	N/A	N/A	00-00-00-00
192.168.1.255	alive 4)	C/R	0	00-00-00-00

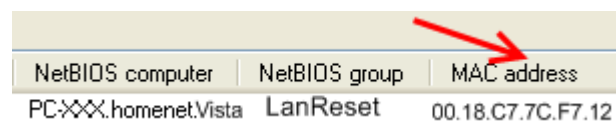
Spiegazione dei risultati: Le icone colorate dei computerini rappresentano i computer accesi e collegati mentre quelle in grigio i computerini spenti o ip non attivi, e sono la rappresentazione di dead (morto) e alive (vivo) come troviamo scritto nella

seconda colonna, e il nome del computer.
La mappatura della Lan da noi scansionata è la seguente, come rappresentata in figura:

- 1) **192.168.1.1** - Il nostro router
- 2) **192.168.1.4** - Il Pc Vittima con Windows Vista
- 3) **192.168.1.5** - Il nostro Pc usato per l'attacco
- 4) **192.168.1.255** - Un altro Pc collegato con S.O. Linux-debian

Come potete notare, nel pc 4, quello con linux, il nome del computer non viene rilevato...eh va bè, questa è un'altra storia, poi dici perchè il pinguino!

Quello che a noi interessa è il Mac-Adress del computer della vittima, quindi cliccate con il tasto destro sulla riga del computer **3**, e scegliete dal menù che apparirà **Get NetBios Info**, e verranno visualizzate le seguenti informazioni aggiuntive:



NetBIOS computer	NetBIOS group	MAC address
PC-XXX.homenet.Vista	LanReset	00.18.C7.7C.F7.12

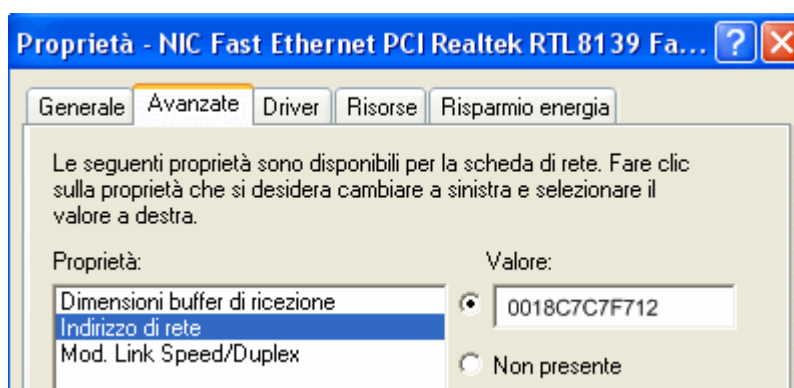
In sequenza avremo il nome del computer, il nome della rete Lan, e infine il **Mac Address** della scheda rete del computer vittima dell'attacco. Copiate su un fogliettino di carta il Mac Address, e attenzione a non fare errori! Oppure, per non fare errori, cliccate sempre sulla riga del pc vittima con il tasto destro del mouse e scegliete l'ultima riga **Proprietà**, e

copiate con il mouse l'indirizzo mac che da lì sarà accessibile selezionandolo.

Adesso dobbiamo modificare il Mac Address del nostro computer, andate in:

**Pannello di controllo-->Connessioni di Rete-->Connessione alla Rete locale
Con il tasto destro del mouse
Proprietà-->Configura-->Avanzate-->Indirizzo di Rete--> Valore**

Qui inserirete senza trattini o puntini il Mac Address del Computer della vittima, come rappresentato nella figura sottostante.

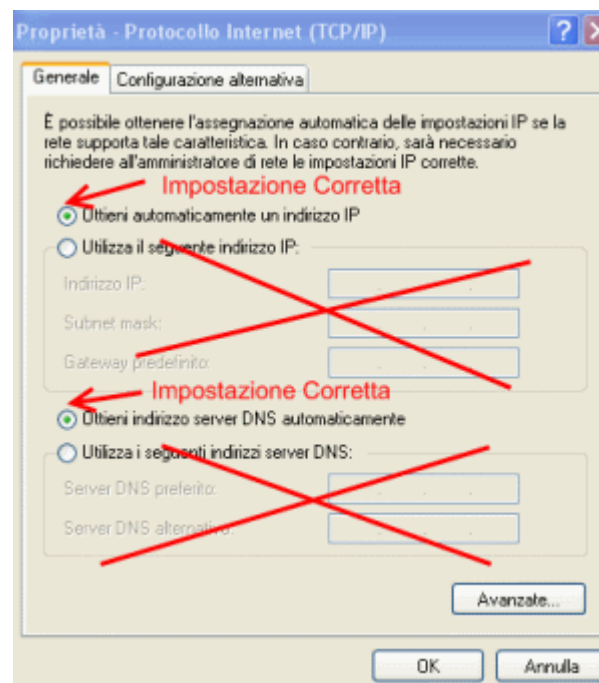


Se abbiamo impostato un indirizzo Ip Statico e dei Server Dsn Preferenziali, disabilitiamo entrambi per avere un Ip Dinamico e per i DSN costringere il router a un lavoro maggiore facendo usare al nostro pc gli stessi DSN del pc vittima. Quindi prima di chiudere la configurazione della scheda di rete

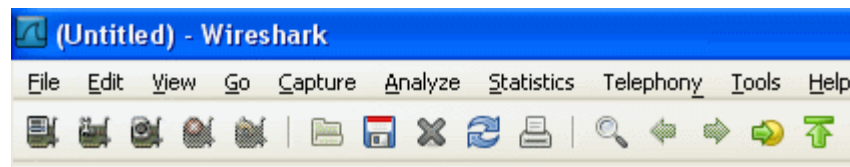
andate in:

Protocollo Internet (Tcp-Ip)-->Tasto destro del Mouse-->Proprietà

E assicuratevi che sia impostata come nell'immagine sottostante, date ok e la scheda di rete si autoconfigurerà con un nuovo indirizzo Ip che concorderà con il router e con lo stesso Mac Adress del computer vittima.



Siamo pronti. Adesso avviate **WireShark**. Ci troveremo il menù dell'immagine sottostante.



Andate in **Edit-->Preferences..**, e impostate così:

Capture

- Capture packets in promiscuous mode:
- Capture packets in pcap-ng format:
- Update list of packets in real time:
- Automatic scrolling in live capture:
- Hide capture info dialog:

Name Resolution

- Enable MAC name resolution:
- Enable network name resolution:
- Enable transport name resolution:
- Enable concurrent DNS name resolution:

Protocols-->HTTP

Hypertext Transfer Protocol

- Reassemble HTTP headers spanning multiple TCP segments:
- Reassemble HTTP bodies spanning multiple TCP segments:
- Reassemble chunked transfer-coded bodies:
- Uncompress entity bodies:

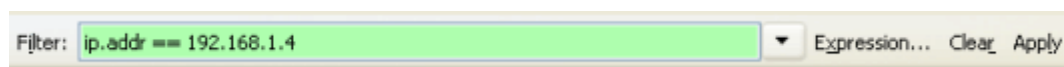
TCP Ports:

SSL/TLS Ports:

E' tutto pronto! Adesso in **Interface** selezioniamo la nostra scheda di rete (Non quella con driver generico), nel nostro caso Nic Fast Ethernet, e cliccando sulla terza icona del menù principale partendo da sinistra avviamo lo sniffing dei dati (Start New Live Capture). E' Fatta. Adesso mentre Wireshark è al lavoro voi effettuate delle query ai dsn, in modo da generare traffico dati. Difficile? Ma

no, dovete soltanto navigare con il vostro browser explorer o firefox in contemporanea con il pc della vittima, in modo che il bridge del router di Alice inizi a contrattare pacchetti tcp anche con noi. Quando dovrà smistare i frame però si troverà in difficoltà in quanto dovrà inviare i dati ma avrà due mac-adress identici, e nel dubbio li invierà anche a noi. Il pc vittima avrà degli impercettibili rallentamenti nella connessione e qualche conflitto, ma non si accorgerà di nulla, noi avremo le informazioni preziose sulla sua navigazione. Dopo 10 minuti fermiamo Wireshark, cliccando sulla 4 icona del menù principale partendo da sinistra verso destra, e noteremo subito che abbiamo una gran mole di dati.

Come estrapolare quelli che ci interessano? Nella barra dei filtri copiare e incollare il seguente comando **ip.addr == 192.168.1.4** e cliccare Apply.



In pratica abbiamo detto al programma di visualizzare solo i dati catturati per il traffico di rete generato dall'indirizzo ip 192.168.1.4, che altro non è che il computer della vittima di Windows Vista! Nelle impostazioni iniziali Di WireShark, nella sezione Name Resolution, avevamo configurato il software per risolvere automaticamente gli

hostname dove possibile, ed ecco infatti che gli ip esterni sono risolti nel nome del sito web visitato. Ce l'abbiamo fatta! Ecco come dovrebbero apparirvi i dati dopo aver impostato il filtro.

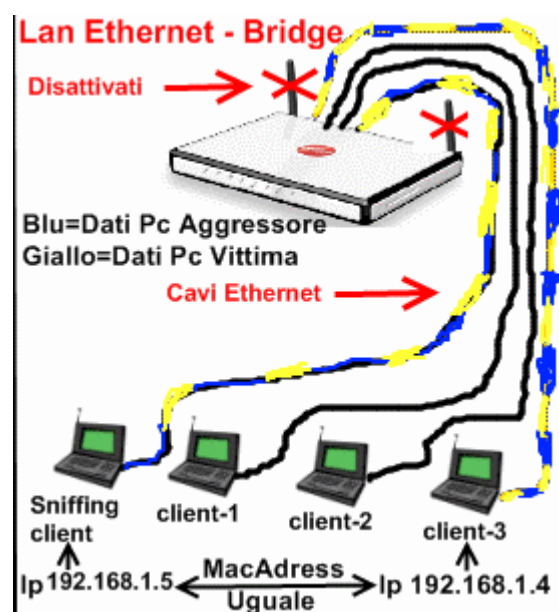
53	10.380	CENSURA	www.ciao.it	192.168.1.4
55	10.382		www.ciao.it	192.168.1.4
56	10.384		www.ciao.it	192.168.1.4
85	15.648		fg-in-f104.google.com	192.168.1.4
88	16.878		www.performix.it	192.168.1.4
90	16.908		www.ciao.it	192.168.1.4
93	71.128		static.corriere.it	192.168.1.4
94	71.129		static.corriere.it	192.168.1.4
95	71.130		static.gazzetta.it	192.168.1.4
96	71.130		static.corriere.it	192.168.1.4
97	71.130	static.corriere.it	192.168.1.4	

Naturalmente ho postato solo una parte dei dati, e censurato altri. Comunque potete facilmente vedere che il nostro amico dal computer vittima all'indirizzo ip 192.168.1.4 prima era su www.ciao.it, poi è andato su google.com, e da lì è andato a leggersi il corriere.it, e poi....Se cliccate su una riga con il tasto destro del mouse, e scegliete *Follow Tcp Stream*, se ci sono dati a sufficienza visualizzerete anche il codice html della pagina web visitata.

Consigli e Conclusioni

Questa non è una guida per principianti, ma ho cercato come sempre, di essere il più semplice e chiaro possibile, e quindi se leggete bene e attentamente tutto, e non vi arrendete al primo errore, riuscirete anche voi a testare la sicurezza della vostra rete lan. Ricordatevi di riavviare il pc dopo aver installato Wireshark. Una volta cambiato

il Mac-Adress del vostro pc non riavviate il computer. Più navigherete in contemporanea con il pc della ipotetica vittima, più pacchetti vi invierà il vostro bridge di router, più dati avrete a disposizione. Potete confrontare la figura in alto di destra, quella che descrive lo smistamento dei dati nella rete lan con bridge, con l'immagine della lan sniffata qui in basso dopo che ci abbiamo giocato. Questo sotto è il risultato della *connessione avvelenata* che abbiamo stabilito con il router e il suo bridge!



Questa guida serve solo a scopo di studio per testare la sicurezza della vostra lan domestica o aziendale. Se usate questa guida per spiare o intercettare dati altrui, senza averne il

diritto, o per mandare in tilt una rete, siate consapevoli che state commettendo un reato e siete penalmente perseguibili.

L'autore declina ogni qualsivoglia responsabilità dall'uso improprio delle informazioni contenute in questa pagina.

E' consentita la pubblicazione di questa guida sul web con obbligo di citazione della fonte e dell'autore (www.windowx.it-Reset74)

Per chiarimenti o domande non inviate emai e messaggi privati, ma usate il forum della community!

Enjoy!

Powered by



Con affetto
@(_°_°)@
RESET74

Questo Articolo proviene da WINDOWX.IT

<http://www.windowx.it>

L'URL per questa storia è:

<http://www.windowx.it/article87.html>