SniffJoke eviscerated

http://www.delirandom.net/sniffjoke

SniffJoke eviscerated

Come funziona uno sniffer,
Come ricostruisce i flussi TCP
Quindi si basa su delle assunzioni
E se noi le facciam crollare ?

Le intercettazioni nell'immaginario della massa
la verità sulla sicurezza,
e sull'insicurezza

Effetto di SniffJoke

vecna@delirandom.net http://www.delirandom.net
progetto winston smith - http://winstonsmith.info

Come funziona uno sniffer ?

Un pacchetto transita in una rete,
  In questa rete una macchina alla quale il pacchetto non è destinato, la scheda di rete è in **promisc** e legge il pacchetto.
  il gateway, legittimo o illegittimo, riceve il pacchetto perché a lui è destinato.

```
struct packet
{
    struct ether_header ethhdr;
    struct iphdr ip;
    struct tcphdr tcp;
    unsigned char data[1442];
};
```

Come si ricostruiscono i flussi ?

```
IP remote:1025 > localweb:80: S 2653389673:2653389673(0) win 65535 <mss
16344,nop,wscale 3,nop,nop,timestamp 237170260 0,sackOK,eol>
IP localweb:80 > remote:1025: S 224414191:224414191(0) ack 2653389674 win
65535 <mss 16344,nop,wscale 3,nop,nop,timestamp 237170260
237170260,sackOK,eol>
IP remote:1025 > localweb:80: . ack 1 win 65535
<nop,nop,timestamp 237170260 237170260>
IP localweb:80 > remote:1025: . ack 1 win 65535
<nop,nop,timestamp 237170260 237170260>
IP remote:1025 > localweb:80: P 1:18(17) ack 1 win 65535
<nop,nop,timestamp 237170355 237170260>
IP localweb:80 > remote:1025: . ack 18 win 65535
<nop,nop,timestamp 237170355 237170355>
IP remote:1025 > localweb:80: P 18:20(2) ack 1 win 65535
<nop,nop,timestamp 237170362 237170355>
IP localweb:80 > remote:1025: . ack 20 win 65535
<nop,nop,timestamp 237170362 237170362>
IP localweb:80 > remote:1025: P 1:155(154) ack 20 win 65535
<nop,nop,timestamp 237170362 237170362>
IP remote:1025 > localweb:80: . ack 155 win 65535
<nop,nop,timestamp 237170362 237170362>
IP localweb:80 > remote:1025: F 155:155(0) ack 20 win 65535
<nop,nop,timestamp 237170362 237170362>
IP remote:1025 > localweb:80: . ack 156 win 65535
<nop,nop,timestamp 237170362 237170362>
IP remote:1025 > localweb:80: F 20:20(0) ack 156 win 65535
<nop,nop,timestamp 237170362 237170362>
IP localweb:80 > remote:1025: . ack 21 win 65535
<nop,nop,timestamp 237170362 237170362>
```

Come si ricostruiscono i flussi ?

```
SYN
                                        SYN ACK
ACK
GET / HTTP 1.1/
                        ACK (del dato CLIENT)

                      HTTP/1.0 403 Forbidden
Date: Thu, 18 Jun 2009 19:39:09 GMT
                          Server: BProxy 0.1
                          Content-Length: 25
          Content-Type: application/json

                   {"error":"403 Forbidden"}

ACK (del dato SERVER)
                                          FIN
ACK (del FIN)
FIN
                                          ACK
```

Come si ricostruiscono i flussi ?

Si legge il pacchetto

Si verificano la coerenza delle dimensioni del pacchetto

Si verifica la tupla **ipsrc:portasrc – ipdst:portadst**

Si legge lo stato della tupla e si associa il flag del pacchetto

Se ci sono dati, si appende alla sessione.

Ma, se ci fossero pacchetti inaspettati ?

Fanno tutti i check necessari ?
  Se non li fanno, possono:
  accettare pacchetti che il server scarta.

Così facendo gli sniffer possono credere a pacchetti che non influiscono sulla connessione, e legge informazioni invalide.
  Puo' chiudere la sessione,
  Cancellarne delle parti,
  Accettare dati fasulli,
  Crashare!

Ma, se ci fossero pacchetti inaspettati ?

I pacchetti possono essere:

non accettati dal server, accettati dallo sniffer.

non accettati dallo sniffer, accettati dal server.

essere ricevuti dallo sniffer, e non raggiungere mai il server.

Si configurano 3 attacchi:

- checksum errato,
- TTL basso,
- TCP/IP options

E cosa gli facciamo credere ?

Il bypass si ha con:
- Checksum sbagliato,
- TTL che expire,
- IP Options

Si danneggia la ricostruzione con:
- dati falsi, in anticipo o posticipo,
- sequence number differenti,
- RST, FIN

La cosa bella...

E' che questi attacchi esistono da 11 anni!

Phrack 54-10
Defeating Sniffers and Intrusion Detection Systems

Thomas H. Ptacek, Timothy N. Newsham:
Insertion, evasion, and denial of service, Eluding network intrusion detection

SniffJoke 0.1/0.2

Si ispirava ad innova,

era un plugin per ulogd,

poteva solo mandare pacchetti in ritardo rispetto alla sessione reale.

Superava ethereal, non wireshark, non libnids.

SniffJoke 0.3

Si ispirava al MOCA :)

Un client VPN è anche il software che manipola il traffico dopo che è transitato per il gateway.

SniffJoke 0.3 fa la stessa cosa, e poi inoltra al default gateway.

Puo' bloccare i pacchetti, e quindi le opzioni di attacco aumentano...

SniffJoke 0.3

Bruteforce del TTL per ogni host,

Utilizzo randomico della sequenza di attacchi,

Utilizzo randomico delle variabili nei singoli hack,

Iniezionie di IP options sui pacchetti legittimi (anche se il risultato non è testato! le implementazioni degli stack TCP/IP differiscono tra tutti gli OS!)

SniffJoke 0.3

Perché ?

A QUALCUNO VA CHE GLI FACCIA DA DENTISTA ?

Supponiamo nessuno :)

A qualcuno va che “le soluzioni di sicurezza” vengano da giornalisti o politici ?

La tendenza drammatica é che il non esperto-di-sicurezza, ha come unico riferimento hollywood...

E anche alcuni esperti ;)

Perché ?

La rete Internet funziona con meccanismi totalmente diversi da quelli ai quali, la maggioranza della cittadinanza, è abituata (a immaginare).

Dove tutti erano utenti allo stesso modo...
  Qui chiunque puo' installare software

Dove solo lo stato aveva la possibilità
  Ora i privati concedono questa possibilità

Dove le leggi erano statali, e bastavano
  La rete è globale

securiry-enforcement, lawful-interception,

Devono di conseguenza funzionare diversamente !

1) Il controllo totale serve solo per gli sprovveduti

1 bis) crea uno squilibrio di potere

2) non risolve problemi, ne crea di nuovi

3) non è possibile

4) molti civili lo vorrebbero!!!!11!one

e SniffJoke ?

Dovrebbe impattare poco!

Chi fa analisi manuali, su un obiettivo specifico, puo' riconoscere che c'e' del traffico fasullo (plausible! ma plausibilmente pure fasullo :)

Chi fa un'indagine ha uno spettro di visione molto piu' ampio che gli stream TCP

Serve, per lo più, per proteggersi da trojan e da sniffer di massa che girano in rete (locale, ISP, o remota)

SniffJoke e effetti

Consente l'occultamento, l'offuscamento, della connessione.

Per ora solo per i CLIENT
I server dovrebbe essere dalla 0.4

Gli hack non so neppure quando fanno effetto :P

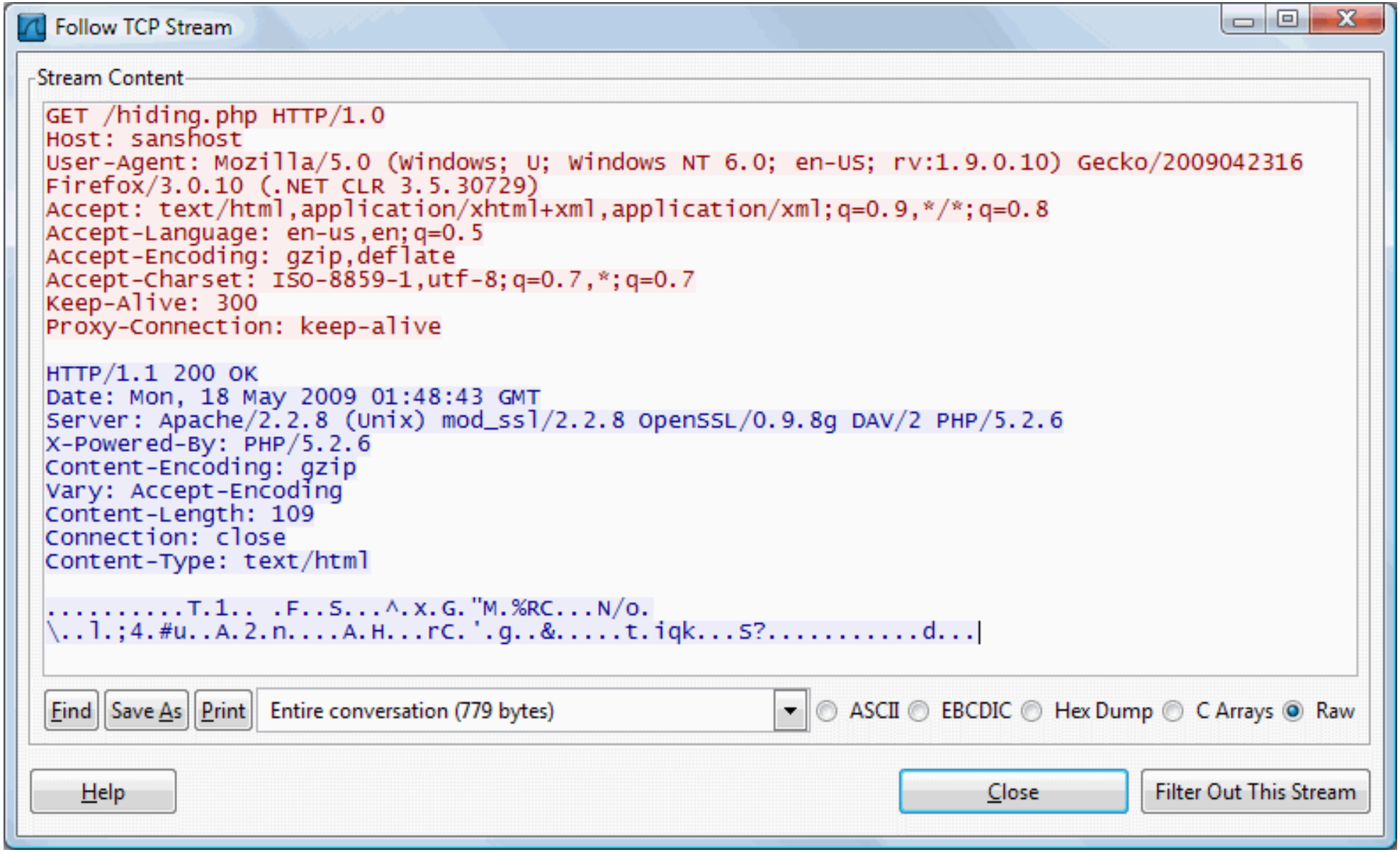
Si basano sull'immaginare quali parti di codice possono essere state eliminate per ottimizzare l'analisi del traffico.

Sul formare connessioni che siano “plausibili”, ma che tocchino quelle parti di RFC non definite con esattezza.

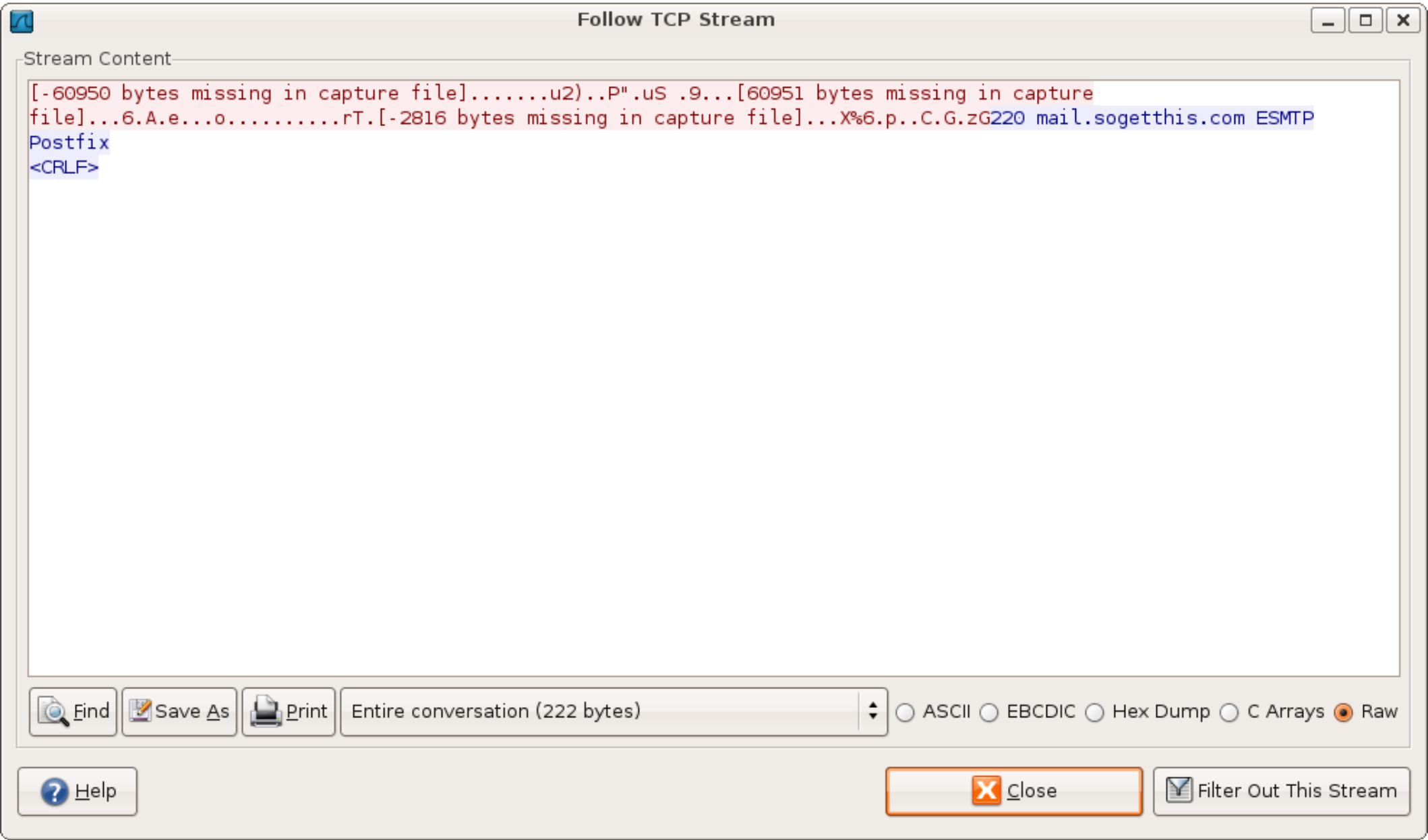
SniffJoke con #HACKSDEBUG

```
Session[0]: local:33103 -> 66.135.60.177:25 puppet 9711 TTL exp 0 wrk 255
** [fake data] (lo:33103 66.135.60.177:25 #2) id 32636 exp:16 wrk:17 len 52-113[77] data 25 {01000}
** [fake SEQ] (lo:33103 66.135.60.177:25 #2) id 32643 exp:16 wrk:17 len 52-111[75] data 23 {00000}
** [fake FIN/RST] (lo:33103 66.135.60.177:25 #2) id 32638 exp:16 wrk:17 len 52-88[52] data 0 {01001}
** [zero window] (lo:33103 66.135.60.177:25 #2) id 32634 exp:16 wrk:17 len 52-88[52] data 0 {10011}
** [valid RST bad SEQ] (lo:33103 66.135.60.177:25 #2) id 32636 exp:16 wrk:17 len 52-88[52] data 0 {01001}
** [fake SYN] (lo:25 66.135.60.177:33103 #2) id 32640 exp:16 wrk:17 len 52-88[52] data 0 {10000}
** [fake data] (lo:33103 66.135.60.177:25 #3) id 32639 exp:16 wrk:17 len 64-119[83] data 19 {01000}
** [fake SEQ] (lo:33103 66.135.60.177:25 #3) id 32644 exp:16 wrk:17 len 64-116[80] data 16 {00000}
** [fake FIN/RST] (lo:33103 66.135.60.177:25 #3) id 32640 exp:16 wrk:17 len 64-100[64] data 0 {01010}
** [zero window] (lo:33103 66.135.60.177:25 #3) id 32635 exp:16 wrk:17 len 64-100[64] data 0 {10011}
** [valid RST bad SEQ] (lo:33103 66.135.60.177:25 #3) id 32643 exp:16 wrk:17 len 64-100[64] data 0 {01001}
** [fake SYN] (lo:33103 66.135.60.177:25 #3) id 32640 exp:16 wrk:17 len 64-100[64] data 0 {10000}
```

Wireshark – follow TCP stream



Wireshark mail + sniffjoke



(senza) SniffJoke, xplico

http://localhost:71/webs/resBody/30

Google

nature

Cerca immagini | Cerca nel Web | Ricerca avanzata | Preferenze

Protezione SafeSearch media attivata

Immagini Mostra: Immagini di tutte le dimensioni | Qualsiasi contenuto

Risultati **1** - **20** di circa **132.000.000** (0,03 secondi)

Natura
Scopri su Focus tutte le novità
su ambiente, **natura** e tanto altro!
www.Focus.it

Hot New Cars
2 Fast Cars
Good Gas Cars
www.mycomputer.com

Link sponsorizzati


in mezzo alla **natura**
1024 x 768 - 513k - jpg
blog.libero.it


Galleria
1024 x 768 - 176k - jpg
www.european-webzine.eu


Perche' anche la **natura** ha un suo ...
1600 x 1200 - 1302k - jpg
www.enature.it


potrei sembrare il calassico ragazzo ...
1024 x 768 - 153k - jpg
blog.libero.it


Nature
1024 x 768 - 369k - jpg
www.myspace.com
[Altre risultati da photobucket.com]


1024x768, centro, wallpaper
1024 x 768 - 127k - jpg


nature-orage-sydney.jpg
800 x 600 - 86k - jpg


Mother **Nature** ...
500 x 375 - 36k


... Earth **Nature**
500 x 375 - 123k - jpg


Nature
550 x 400 - 36k - jpg

Done

FoxyProxy: Disabled 127.0.0.1

(con) SniffJoke, xplico

Disservizi, considerazioni, ecc...

Crea un tunnel VPN in modo automatico (per ora funziona solo su Linux, forse per 0.4, o per la 1.0, MacOSX/BSD)

Cambia default gateway = le regole di iptables legate ad un'interfaccia cessano di funzionare.

Eventuali altri tunnel VPN non vengono considerati, perché trova il default gateway solo in ethernet (e fa packet forging ethernet)

Disservizi, considerazioni, ecc...

All'inizio di una sessione TCP, effettua l'equivalente di un tcptraceroute per conoscere la distanza in HOP con il server da contattare.

Tiene una cache per ogni avvio, versione 0.4/1.0, avrà il dump su file
  trivia: come fareste a supportare diverse network locations ?

Manca la configurazione per porte TCP
Manca l'injection a payload fake layer 5

GUI & distro

Siccome sono convinto che software per la privacy e la difesa online abbiano senso se vengono utilizzati da utenti non esperti, i due modi provati sono stati:

1) cercare di far qualcosa facilmente packettizabile, così godendo dei repository di riferimento per diffondersi.

2) una GUI e dei default il piu' possibile autonomi. la GUI è stata fatta con libswill, tramite un webserver locale che stampa HTML come fosse un vecchio CGI.

o'rly !?

Pagina del progetto
http://www.delirandom.net/sniffjoke

progetto su github:
http://github.com/vecna/sniffjoke/tree/master

software di Gianluca Costa, che ha analizzato gli effetti di SniffJoke su questo e altri sniffer
http://www.xplico.com

Defeating sniffer & IDS
http://www.phrack.org/issues.html?issue=54&id=10

anti anti sniffer patch, marginalmente correlato
http://www.s0ftpj.org/bfi/online/bfi9/BFi09-14

Discussione sulla mailing list WireShark riguardo a Sj
http://www.mail-archive.com/wireshark-dev@wireshark.org/msg13465.html