Kippo Installation on Debian

May 26, 2011 at 6:31 pm (Kippo)

This is by far the easiest distribution to install kippo on. I used Debian 6 in a VM just to run kippo. Im not sure if there are ways to break out of the fake SSH session but I thought it would be better safe then sorry to use a VM.

1. Download kippo from here http://code.google.com/p/kippo/downloads/list
2. Get the one needed extra file by running: aptitude install python-twisted
3. kippo can not be run as root so install it somewhere where your regular user will have access to it
4. tar xvzf the file, there is no installation and where ever you unzip it will be where the program lives
5. Edit the file kippo.cfg to set the port and IP address mainly
6. Theres a trick to this though I found. Regular users are not allowed to use port 22 (default SSH port) but root cant run kippo. This puts you in a strange position
7. You can use port forwarding to get around this. I used my router for this. I had the incoming port 22 forwarded to the port set in kippo.cfg. People think they are SSHing into port 22 but they are actually being routed to a different port. They will not know the difference.

Thats pretty much it for the basic setup. Just run ./startsh as a regular user and it should return you back to prompt. Test that its running by SSHing to the port on your localhost.

The log files are located in the /log/tty directory. I found the best way was to move the utility playlog.py from the utils directory into the log directory. The best playback format for the command is: python playlog.py filename 0

```
mward@herman:~/kippo-0.8/log$ cat /etc/network/iptables
# Generated by iptables-save v1.4.12 on Tue Apr 16 16:03:29 2013
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -i eth0 -p tcp -m tcp --dport 22 -j REDIRECT --to-ports 2222
COMMIT
# Completed on Tue Apr 16 16:03:29 2013
# Generated by iptables-save v1.4.12 on Tue Apr 16 16:03:29 2013
*mangle
:PREROUTING ACCEPT [474:30672]
:INPUT ACCEPT [474:30672]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [293:22808]
:POSTROUTING ACCEPT [293:22808]
COMMIT
# Completed on Tue Apr 16 16:03:29 2013
# Generated by iptables-save v1.4.12 on Tue Apr 16 16:03:29 2013
```

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [146:12016]
-A INPUT -i eth0 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 2222 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 1222 -j ACCEPT
-A INPUT -i eth0 -p tcp -m tcp --dport 25 -j ACCEPT
COMMIT
# Completed on Tue Apr 16 16:03:29 2013
```