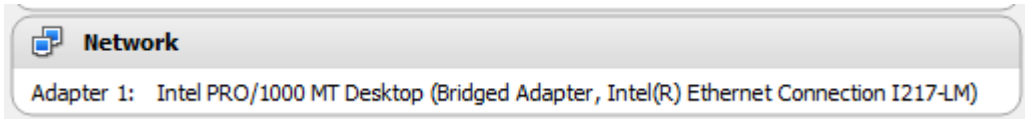
Lab7 – Honeypot

Document your commands or take screenshots. Answer questions in english or finnish.

The labs use bridged Honeypot Virtual Machine. Username & password kippo/kippo

Start Honeypot (1p)

Retrieve the pre-installed VM image for Honeypot from \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\ . Import it to Virtualbox. Set interface for bridged.



Find what your Honeypot's IP address is, try to wget www.iltasanomat.fi from it, so we know connections are ok.

```
kippo@ubuntu:~/kippo-0.5$ wget www.iltasanomat.fi
--2017-03-15 11:36:26--  http://www.iltasanomat.fi/
Resolving www.iltasanomat.fi (www.iltasanomat.fi)... 54.192.129.46, 54.192.129.35, 54.192.129.43, ..
.
Connecting to www.iltasanomat.fi (www.iltasanomat.fi)|54.192.129.46|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.is.fi/ [following]
--2017-03-15 11:36:26--  http://www.is.fi/
Resolving www.is.fi (www.is.fi)... 54.192.129.69, 54.192.129.24, 54.192.129.71, ...
Reusing existing connection to www.iltasanomat.fi:80.
HTTP request sent, awaiting response... 200 OK
Length: 601112 (587K) [text/html]
Saving to: 'index.html'

100%[======================================================>] 601,112     3.40MB/s   in 0.2s

2017-03-15 11:36:26 (3.40 MB/s) - 'index.html' saved [601112/601112]
```

Run these commands:

cd kippo-0.5/

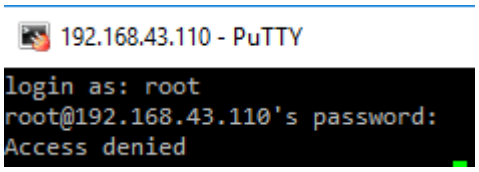
./start.sh

```
kippo@ubuntu:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=12.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=13.1 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 12.908/13.053/13.199/0.184 ms
kippo@ubuntu:~$ cd kippo-0.5/
kippo@ubuntu:~/kippo-0.5$ ./start.sh
Starting kippo in background...kippo@ubuntu:~/kippo-0.5$
```

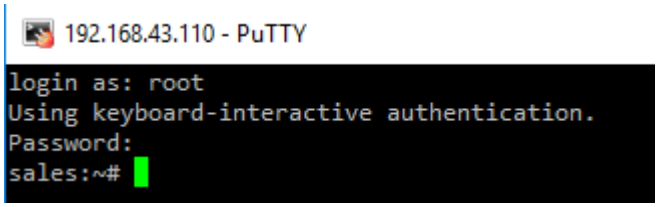
- **Connect Virtual Machine with Host computer (1p)**

Use your Putty or other SSH-client to take ssh connection to Kippo machine port 2222. Use username root, password 123456

Access denied to port 22:



Succesful connection to port 2222:



When you get connection, leave a mark that you were inside machine: touch YourName.txt where your name is your name. Then wget some www site, try to ping google.com.

```
sales:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:4c:a8:ab:32:f4
          inet addr:10.98.55.4  Bcast:10.98.55.255  Mask:255.255.255.0
          inet6 addr: fe80::21f:c6ac:fd44:24d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

```
sales:~# touch k1521.txt
sales:~# ls -l
drwxr-xr-x 1 root root 4096 2017-03-15 11:42 .
drwxr-xr-x 1 root root 4096 2017-03-15 11:42 ..
drwxr-xr-x 1 root root 4096 2009-11-06 13:16 .debtags
-rw------- 1 root root 5515 2009-11-20 11:08 .viminfo
drwx------ 1 root root 4096 2009-11-06 13:13 .aptitude
-rw-r--r-- 1 root root  140 2009-11-06 13:09 .profile
-rw-r--r-- 1 root root  412 2009-11-06 13:09 .bashrc
-rw-r--r-- 1 root root    0 2017-03-15 11:42 k1521.txt
```

```
sales:~# ping google.com
PING google.com (29.89.32.244) 56(84) bytes of data.
64 bytes from google.com (29.89.32.244): icmp_seq=1 ttl=50 time=46.3 ms
64 bytes from google.com (29.89.32.244): icmp_seq=2 ttl=50 time=42.4 ms
```

```
sales:~# wget www.google.com
--2017-03-15 11:44:25--  http://www.google.com
Connecting to www.google.com:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html; charset=ISO-8859-1]
Saving to: `index.html

100%[======================================>] 0           73K/s  eta 0s

2017-03-15 11:44:26 (73 KB/s) - `index.html' saved [11180/0]
```

Try to create new user (maybe with adduser or useadd) can you?

```
sales:~# adduser k1521
Adding user `k1521' ...
Adding new group `k1521' (1001) ...
Adding new user `k1521' (1001) with group `k1521' ...
Creating home directory `/home/k1521' ...
Copying files from `/etc/skel' ...
Password:
Password again:

Changing the user information for k1521
Enter the new value, or press ENTER for the default
        Username []:
```

```
Is the information correct? [Y/n] y
ERROR: Some of the information you entered is invalid
Deleting user `k1521' ...
Deleting group `k1521' (1001) ...
Deleting home directory `/home/k1521' ...
Try again? [Y/n] n
```

then exit

Are you now back to hosts cmd? (Try to do something there)

```
localhost:~# touch nakki.txt
localhost:~# ls -l
drwxr-xr-x 1 root root 4096 2017-03-15 11:50 .
drwxr-xr-x 1 root root 4096 2017-03-15 11:50 ..
drwxr-xr-x 1 root root 4096 2009-11-06 13:16 .debtags
-rw------- 1 root root 5515 2009-11-20 11:08 .viminfo
drwx------ 1 root root 4096 2009-11-06 13:13 .aptitude
-rw-r--r-- 1 root root  140 2009-11-06 13:09 .profile
-rw-r--r-- 1 root root  412 2009-11-06 13:09 .bashrc
-rw-r--r-- 1 root root    0 2017-03-15 11:42 k1521.txt
-rw-r--r-- 1 root root    0 2017-03-15 11:44 index.html
-rw-r--r-- 1 root root    0 2017-03-15 11:50 nakki.txt
```

- **Exploring logs (1p)**

Open Kippo machine (not from ssh, use virtualbox). Navigate to /home/kippo/kippo-master/log/

What information does these logs have?

```
kippo@ubuntu:~/kippo-0.5/log$ pwd
/home/kippo/kippo-0.5/log
```

Find the info who has tried to log to kippo before and with which passwords, find atleast 4 attempts and write them down.

```
kippo@ubuntu:~/kippo-0.5/log$ cat kippo.log | grep "login" | cut -d" " -f9
[jarmo/salasana]

[jarmo/nomikas]

[jarmo/seSittenOn]

[jarmo/APUVA!]

[jarmo/enKeksi]

[jarmo/luovutan]

[uuno/silakka]

[uuno/spede]

[uuno/ruoka]

[uuno/elisabeth]

[root/ubuntu]

[root/kippo]

[root/12345]
```

Go inside tty folder

```
kippo@ubuntu:~/kippo-0.5/log/tty$ ls -lah
total 736K
drwxr-xr-x 2 kippo sudo 4.0K Mar 15 11:52 .
drwxr-xr-x 3 kippo sudo 4.0K Feb 14 09:06 ..
-rw------- 1 kippo sudo  15K Aug  9  2016 20160809-120603-4484.log
-rw------- 1 kippo sudo  33K Aug  9  2016 20160809-124042-5741.log
-rw------- 1 kippo sudo 6.6K Oct  4 08:08 20161004-080801-115.log
-rw------- 1 kippo sudo 5.2K Feb 14 08:55 20170214-085428-8811.log
-rw------- 1 kippo sudo 609K Feb 14 09:00 20170214-085815-8152.log
-rw------- 1 kippo sudo  977 Feb 14 09:05 20170214-090533-3383.log
-rw------- 1 kippo sudo 8.7K Feb 14 09:12 20170214-091041-1857.log
-rw------- 1 kippo sudo  24K Mar 15 11:50 20170315-114146-7006.log
-rw------- 1 kippo sudo 3.5K Mar 15 11:53 20170315-115202-9985.log
```

Here run " ../../utils/playlog.py *NameOfLatest.logFile 0*"

```
kippo@ubuntu:~/kippo-0.5/log/tty$ ../../utils/playlog.py 20170315-114146-7006.log 0
sales:~# touch k1521.tx
```

What does it show?

It shows the ssh playlog, every command the user has done in normal speed.

- **Changing Kippo settings (2p)**

At this point kippo is running at port 2222, and normal ssh is still on default port 22.... Not good...

We want change things so that basic ssh connection goes to inside honeypot, and ssh connection to port 2222 is real ssh connection. Find a way to do that. Hint: Change default port of ssh-server and default port of Kippo. Or use iptables to change ports.

```
  GNU nano 2.2.6                File: /etc/ssh/sshd_config

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 2222
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
```

```
kippo@ubuntu:~/kippo-0.5$ sudo reload ssh
```

```
  GNU nano 2.2.6              File: /home/kippo/kippo-0.5/kippo.cfg

#
# Kippo configuration file (kippo.cfg)
#

[honeypot]

# IP addresses to listen for incoming SSH connections.
#
# (default: 0.0.0.0) = any address
#ssh_addr = 0.0.0.0

# Port to listen for incoming SSH connections.
#
# (default: 2222)
ssh_port = 22
```

```
kippo@ubuntu:~/kippo-0.5$ ./start.sh
Starting kippo in background...kippo@ubuntu:~/kippo-0.5$
```

Find out how to add “fake user” for Kippo, by fake meaning user that gets inside honeypot. Use these credentials for it: adminuser: adminuser. Prove that if you connect ssh with that user he goes inside honeypot.

```
kippo@ubuntu:~/kippo-0.5$ sudo adduser adminuser
Adding user `adminuser' ...
```

```
  GNU nano 2.2.6                File: /home/kippo/kippo-0.5/kippo.cfg

# behaviour).
#
# (default: not specified)
#fake_addr = 192.168.66.254

# MySQL logging module
#
# Database structure for this module is supplied in doc/sql/mysql.sql
#
# To enable this module, remove the comments below, including the
# [database_mysql] line.

#[database_mysql]
#host = localhost
#database = kippo
#username = kippo
#password = secret
username = adminuser
password = adminuser
```

Ls -

Proving that changes works as expected:

```
kippo@ubuntu:~$ sudo apt-get install sockstat
```

Take ssh connection with adminuser to port 22 and end up inside honeypot

Take ssh connection with kippo to port 2222, and get inside as real kippo user.

```
Mar 15 13:06:08 ubuntu sshd[1881]: Accepted password for kippo from 192.168.43.37 port 14168 ssh2
Mar 15 13:06:08 ubuntu sshd[1881]: pam_unix(sshd:session): session opened for user kippo by (uid=0)
Mar 15 13:06:08 ubuntu systemd-logind[450]: Removed session 1.
Mar 15 13:06:08 ubuntu systemd-logind[450]: New session 2 of user kippo.
Mar 15 13:06:12 ubuntu sudo:    kippo : TTY=tty1 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/tail
auth.log
Mar 15 13:06:12 ubuntu sudo: pam_unix(sudo:session): session opened for user root by kippo(uid=0)
kippo@ubuntu:/var/log$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:2222                  *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp6       0      0 [::]:2222               [::]:*                  LISTEN
```