

HOW TO CREATE A REVERSE SSH TUNNEL AND USE ENCASE ENTERPRISE TO SNAPSHOT/PREVIEW OR ACQUIRE A MACHINE THAT IS PROTECTED ON THE INSIDE OF A NETWORK

Lance Mueller, CISSP, GCIH, EnCE, GREM, CFCE, MCP
lance.mueller@guidancesoftware.com

A machine that is located inside a private business/corporation and is protected by a firewall cannot be connected to via the normal EnCase Enterprise techniques due to the firewall blocking any inbound connection.

In order to make a successful connection with FIM or EEE to a machine behind a firewall, the following is needed.

Target machine – located anywhere, protected by firewall or some other type of network filtering which prevents direct contact by the FIM/SAFE. The target machine must establish a SSH connection to the SSH server. The tools used in this example can fit on a floppy and can be inserted into the target machine and an outbound connection established from the command line.

****SSH Server** - Machine running SSH daemon. This can be default basic linux installation (the example shown here is a default RedHat 8.0 installation). Root access is not required, but preferable.

Examiner Machine (EEE or FIM)– The examiner machine located anywhere that can authenticate to it's SAFE and reach the SSH server. In the example described below, port 4445 is used to connect to the SSH server, so unobstructed access must be available to the SSH server on port 4445 from the examiner machine.

** The SSH server can not be on the same machine as your FIM/SAFE because of port conflicts, the SAFE must use TCP port 4445.

Putty is the SSH client used in the example below because it is small, compact and can fit on a floppy (364K). It can be obtained from:

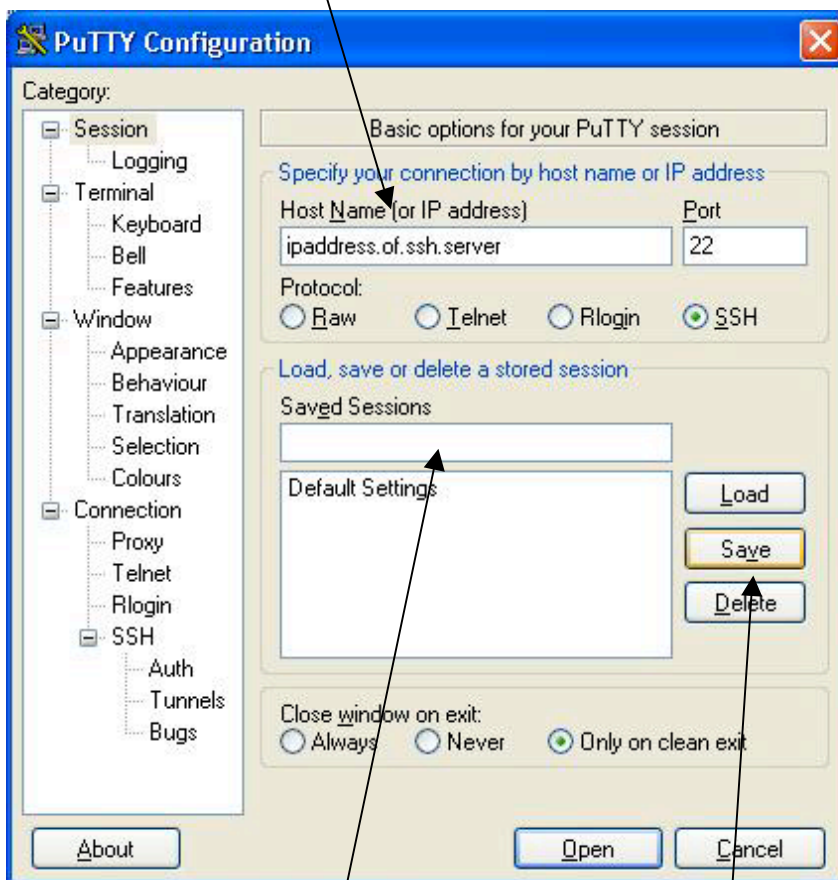
<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

Any other SSH client can be used (such as SSH Secure Shell, but it must be installed on target machine) as long as it can support port forwarding.

FROM THE TARGET MACHINE

Start PUTTY (from floppy or removable USB pen drive) and on the starting Screen, enter the IP address of the SSH server that you want the target machine to connect to. If you have previously set these parameters up, you can simply highlight the session name and click, load, and then open.

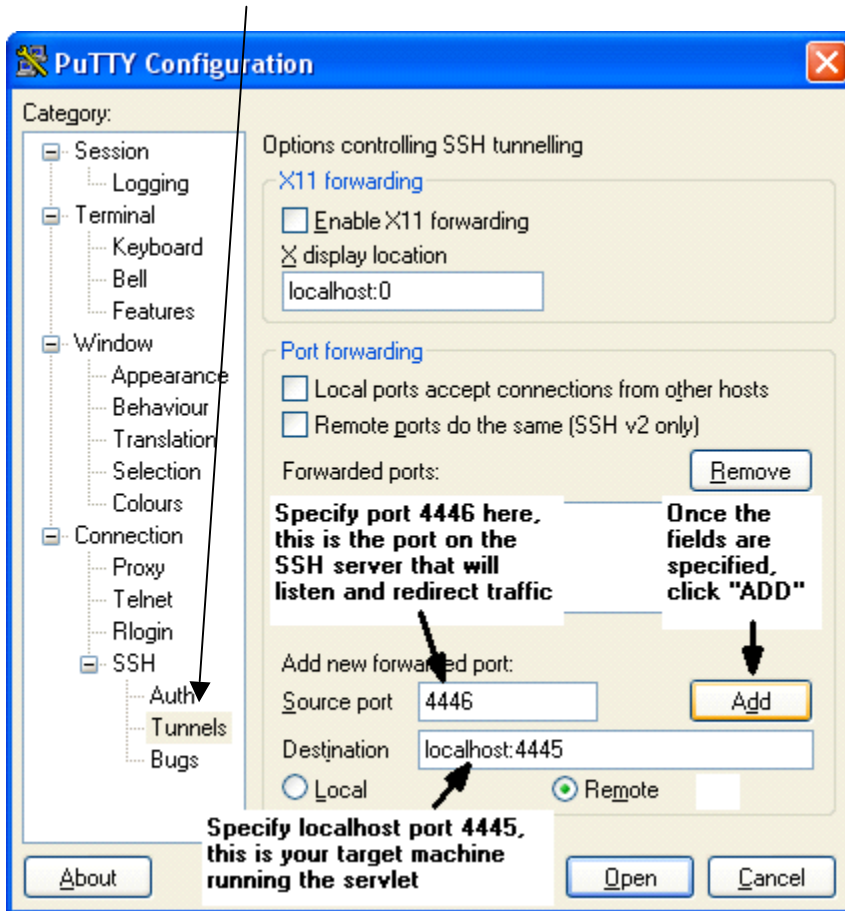
Specify the IP address



Put a session name so you can save these settings

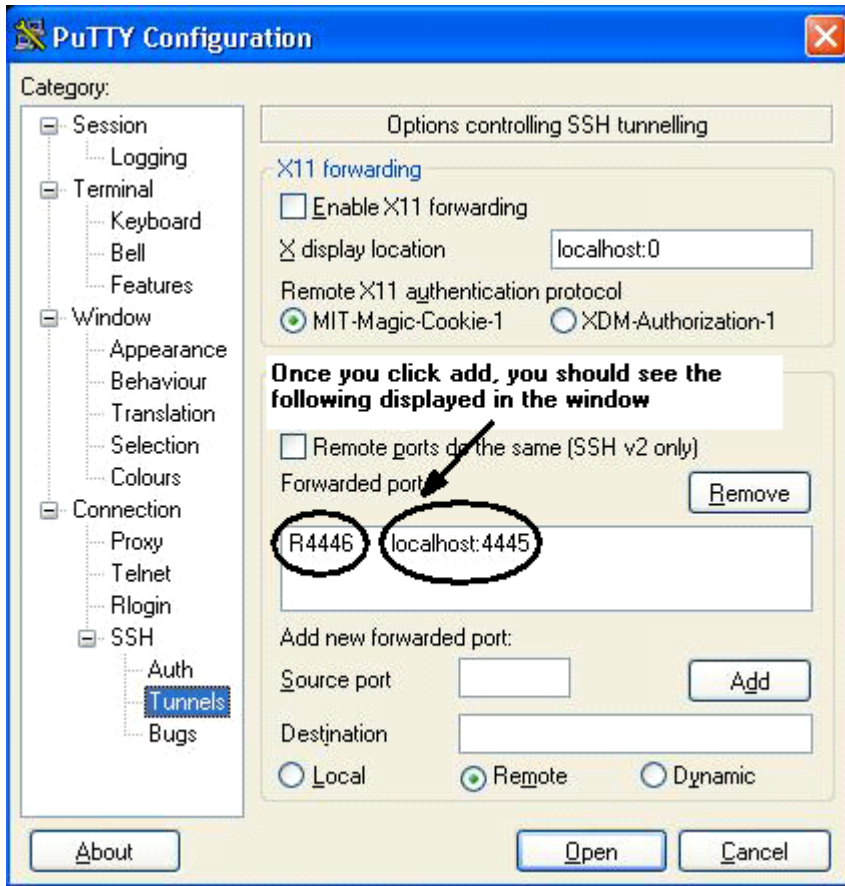
After entering a session name and IP address, Click “SAVE”

Click on the "Tunnels" menu to display tunnel configuration information

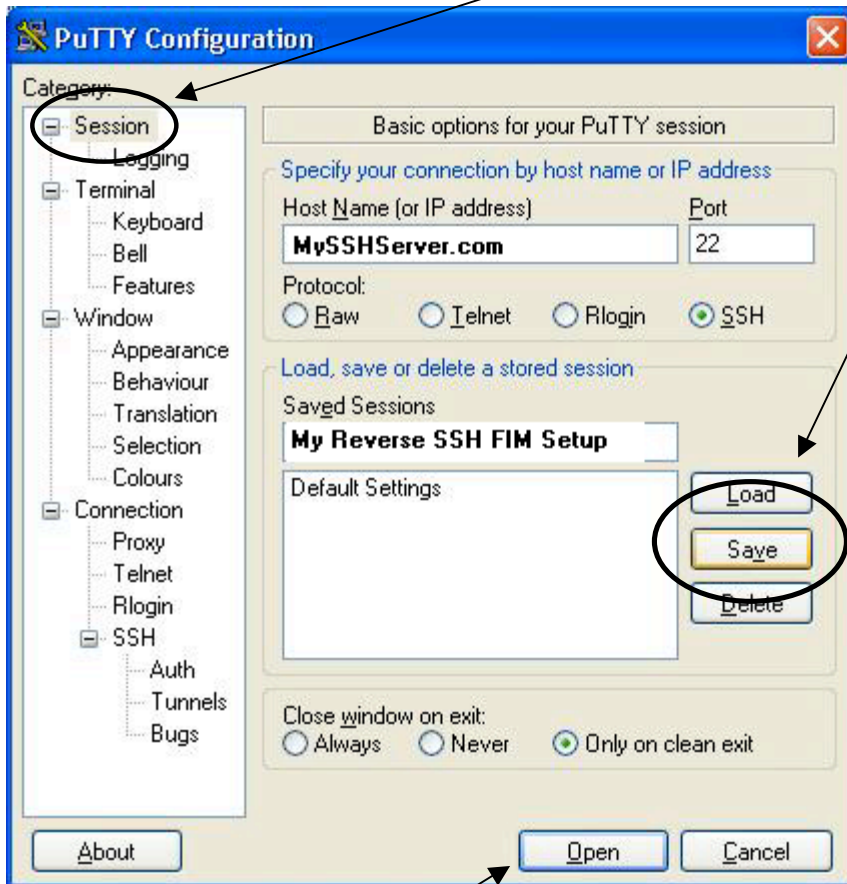


Here you need to enter the information to create a reverse tunnel. Essentially what you are doing here is creating a "ssh tunnel" to an SSH server somewhere on the publicly accessible Internet. Once connected to the SSH server, any traffic arriving at the SSH server on port 4446 will be redirected down the SSH tunnel to the target machine on port 4445, where the servlet is listening.

Once you have entered the port forwarding information, the dialog window should appear like the one below.

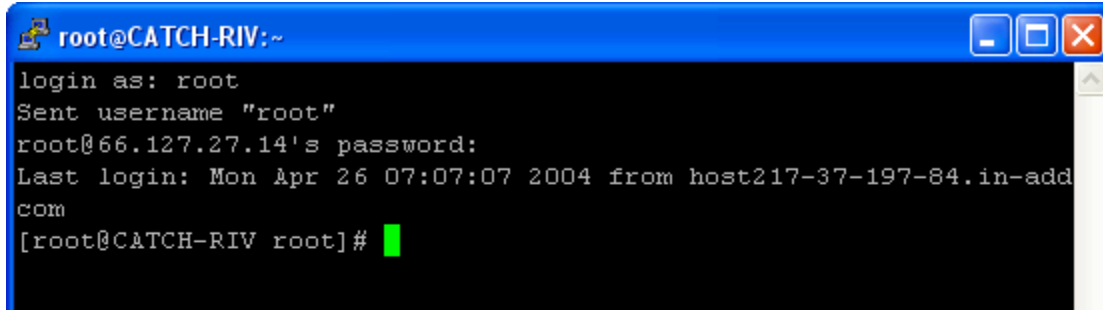


Once you have entered this information, go back to the “SESSION” tab and again select “save”.



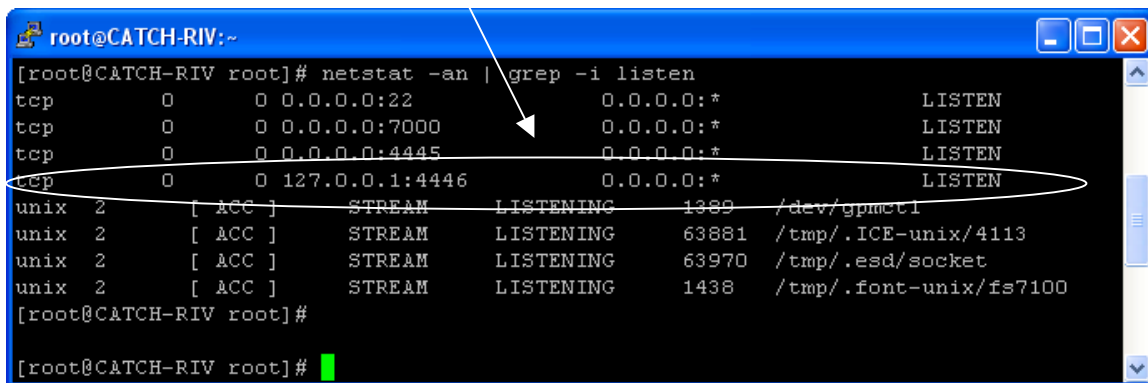
Now click “OPEN” and you will be prompted for your username and password on the SSH server.

Once established you will have a terminal window on the SSH server.



```
root@CATCH-RIV:~
login as: root
Sent username "root"
root@66.127.27.14's password:
Last login: Mon Apr 26 07:07:07 2004 from host217-37-197-84.in-add
com
[root@CATCH-RIV root]#
```

You can issue a “netstat -an | grep -i listening” so make sure the reverse tunnel you just created is listening on port 4446.



```
root@CATCH-RIV:~
[root@CATCH-RIV root]# netstat -an | grep -i listen
tcp        0      0 0.0.0.0:22          0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:7000       0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:4445       0.0.0.0:*           LISTEN
tcp        0      0 127.0.0.1:4446     0.0.0.0:*           LISTEN
unix 2      [ ACC ]     STREAM  LISTENING   1389    /dev/gpmctl
unix 2      [ ACC ]     STREAM  LISTENING   63881  /tmp/.ICE-unix/4113
unix 2      [ ACC ]     STREAM  LISTENING   63970  /tmp/.esd/socket
unix 2      [ ACC ]     STREAM  LISTENING   1438   /tmp/.font-unix/fs7100
[root@CATCH-RIV root]#
[root@CATCH-RIV root]#
```

A reverse tunnel creates a port on the remote SSH server that listens for incoming connections and then sends them down the tunnel to your target machine. Unfortunately, the reverse tunnel only listen to traffic coming from 127.0.0.1, so you must create one more tunnel that creates another listening port on port 4445, that redirects to port 4446 and then send the traffic down the SSH tunnel. To create this additional tunnel, the following command is used on the SSH server:

```
ssh -L 4445:localhost:4446 -f -N -g root@localhost
```

This will prompt you again for the root user’s password. Once entered you will have created a second tunnel (shown above listening on 0.0.0.0:4445) that can now be connected to by a FIM or EEE installation. When the FIM connects to port 4445 on the SSH server, it is redirected to port 4446 and then down the tunnel to the target machine.

Once the two tunnels are created, enter the IP address of the SSH server into the network tab of EnCase.

EnCase Enterprise Training Edition

File Edit View Tools Help

New Open Save Print Add Device Edit New Delete Update Search Logoff Refresh

Table Timeline Report

Network

- Folder 1
 - Classroom
 - UK

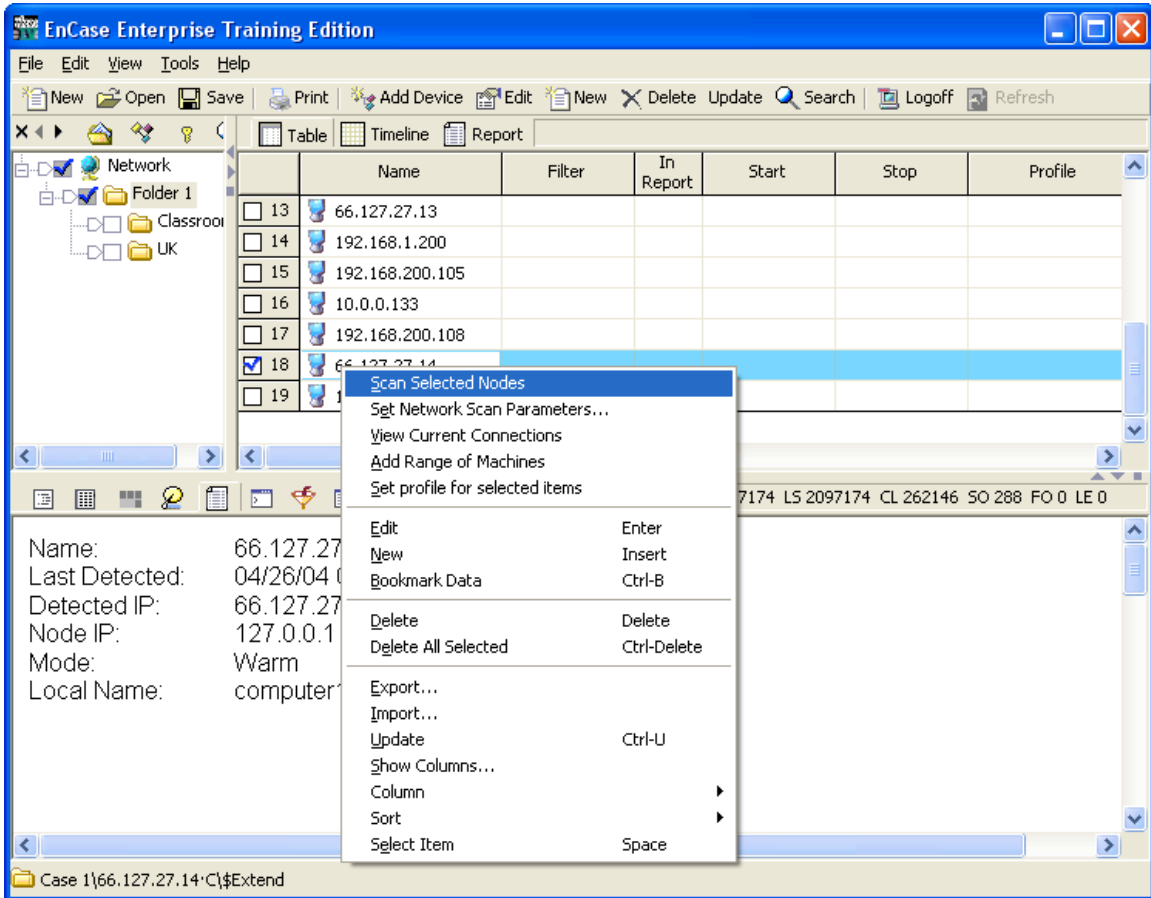
	Name	Filter	In Report	Start	Stop	Profile
<input type="checkbox"/>	13 66.127.27.13					
<input type="checkbox"/>	14 192.168.1.200					
<input type="checkbox"/>	15 192.168.200.105					
<input type="checkbox"/>	16 10.0.0.133					
<input type="checkbox"/>	17 192.168.200.108					
<input type="checkbox"/>	18 66.127.27.14					
<input type="checkbox"/>	19 192.168.100.26					

0/18448 66.127.27.14·C: P5 2097174 LS 2097174 CL 262146 SO 288 FO 0 LE 0

Name: 66.127.27.14
Last Detected: 04/26/04 06:23:27 AM
Detected IP: 66.127.27.14
Node IP: 127.0.0.1
Mode: Warm
Local Name: computer18

Case 1\66.127.27.14·C\Extend

Once entered, you should be able to blue check that IP address and select “Scan Selected Nodes”.



Once complete the “mode” column should show “WARM”.

	Detected IP	Node IP	Mode
<input type="checkbox"/> 16	10.0.0.159	10.0.0.159	Warm
<input type="checkbox"/> 17			New
<input checked="" type="checkbox"/> 18	66.127.27.14	127.0.0.1	Warm
<input type="checkbox"/> 19			New

Even though the IP address is of the SSH server, you are actually connecting to the target machine behind the firewall. From here you can do a snapshot, preview or acquisition of the target machine like any other acquisition. Note that this will be a little slower than a normal network acquisition or preview because to you are tunneling the normal EnCase TCP connection on top of an SSH connection, both of which are encrypted.