Rainer's Technical Tips

Installing OpenSSH Server on a linux-based Appliance

created bv: Rainer Bemsel – **Version** 1.0 – **Dated:** Nov/05/2003

The Purpose of this document is to provide you with instructions on "How to enable SSH Server on a Linux Based Security Appliance". This document will also help you to add SSH on any other Linux system as well.

NOTE: If your appliance is not SSH enabled by default, you may want to add SSH. To do this, you may overcome a previously hardened OS. So make sure to restrict access only to certain workstations and close down communication as tight as possible.

In this example I have used Redhat Linux 7.0 (Guiness) with SSH 2.1.1. In the case you are using a newer distribution, you may have to add OpenSSL and GLIBC as well. I've put the files into usr/src/

- openssh-2.1.1p4-1.i386.rpm
- openssh-server-2.1.1p4-1.i386.rpm

```
lnx-appliance:/usr/src/rpm -e openssh
lnx-appliance:/usr/src/rpm -i openssh-2.1.1p4-1.i386.rpm
lnx-appliance:/usr/src/rpm -i openssh-server-2.1.1p4-1.i386.rpm
```

Done with it, go to:

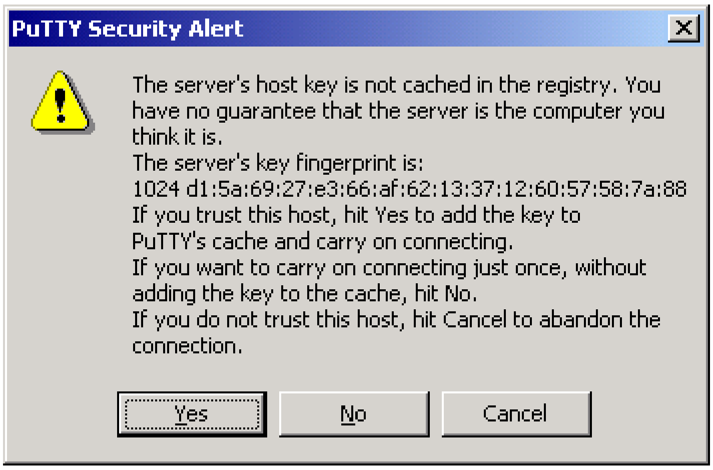
```
lnx-appliance:/usr/src/cd /etc/rc3.d
lnx-appliance:/etc/rc3.d/service sshd start
```

The OpenSSH daemon uses the configuration file /etc/ssh/sshd_config. The default configuration file installed with Red Hat Linux should be sufficient for most purposes. If you want to configure the daemon in ways not provided by the default sshd_config, read the sshd man page for a list of the keywords that can be defined in the configuration file.

To stop the OpenSSH server, use the command:

```
 lnx-appliance:/etc/rc3.d/service sshd stop
```

If you reinstall a Red Hat Linux system, and clients connected to it before the reinstall with any of the OpenSSH tools, after the reinstall, the client users will see the following message:


PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's key fingerprint is:
1024 d1:5a:69:27:e3:66:af:62:13:37:12:60:57:58:7a:88
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

Rainer's Technical Tips

DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consult each Vendor for further information or support.

Although I believe the information provided in this document to be accurate at the time of writing, I reserve the right to modify, update, retract or otherwise change the information contained within for any reason and without notice. This technote has been created after studying the material and / or practical evaluation by myself. All liability for use of the information presented here remains with the user

The reinstalled system creates a new set of identification keys for the system; hence, the warning about the RSA host key changing. If you want to keep the host keys generated for the system, backup the /etc/ssh/ssh_host*key* files and restore them after the reinstall

This process retains the system's identity, and when clients try to connect to the system after the reinstall, they will not receive the warning message.

That’s pretty much all to do with RedHat Linux 7.0. If you are running a newer version, the steps are similar, however, you may have to add some libraries before. But, this will be told, when trying to install OpenSSH 3.5p1 for example.

The man page of OpenSSH could be found here:

<http://www.openbsd.org/cgi-bin/man.cgi?query=ssh&sektion=1>

A couple of SSH Clients could be found here:

snailbook.com/software.html

There might be the case, that some rpms are missing on your system. A good source to find rpms is:

http://rpmfind.tux1000.org/Distribs.html

or

http://www.redhad.com/download