1.113.7 Set up secure shell (OpenSSH) Weight 4

Linux Professional Institute Certification — 102

Geoffrey Robertson ge@ffrey.com Nick Urbanik nicku@nicku.org

This document Licensed under GPL—see section 10

2005 July

1.113.7 Set up secure shell

(OpenSSH) Weight 4

Geoff Robertson

Context

Objective

....

Versions of S

SSH commands and

Advanced usage

Jser Keys

SSH from Windows

ther frontends

Outline

Context
Objectives
What is SSH?
Versions of SSH
SSH commands and utilities
ssh
scp
sftp
Advanced usage

Redirecting stdin and stdout
X forwarding
Port Forwarding
Authenticating with User Keys ssh-agent
SSH from Windows
Other frontends
License Of This Document

1.113.7 Set up secure shell (OpenSSH)

Weight 4

Geoff Robertson

Contex

Objective

What is SSH'

VC1310113 01 0011

utilities

ravariood doago

User Keys

SSH from Windows

Other frontends

Topic 113 Networking Services [24] Where we are up to

1.113.7 Set up secure shell (OpenSSH) Weight 4

Geoff Robertson

Context

Objectives

SSH commands and

Advanced usage

User Keys

SSH from Windows

Other frontends

- 1.113.1 Configure and manage inetd, xinetd, and related services [4]
- 1.113.2 Operate and perform basic configuration of sendmail [4]
- 1.113.3 Operate and perform basic configuration of Apache [4]
- 1.113.4 Properly manage the NFS, smb, and nmb daemons [4]
- 1.113.5 Setup and configure basic DNS services [4]
- 1.113.7 Set up secure shell (OpenSSH) [4]

Description of Objective

1.113.7 Set up secure shell (OpenSSH)

The candidate should be able to obtain and configure OpenSSH. This objective includes basic OpenSSH installation and troubleshooting, as well as configuring sshd to start at system boot.

1.113.7 Set up secure shell

(OpenSSH) Weight 4

Geoff Robertson

Context

Objectives

viiat is som:

CCI -------

utilities

Advanced usag

Jser Keys

55H from Windows

Other frontends

Key files, terms, and utilities include:

keys, user keys

```
/etc/hosts.allow — TCP Wrappers file: sshd is linked
            against TCP Wrappers
/etc/hosts.deny — TCP Wrappers file: sshd is linked
            against TCP Wrappers
/etc/nologin — if present, only root can log in; others
            shown content of this file
/etc/ssh/sshd config — sshd configuration
/etc/ssh known hosts — holds public host keys of hosts
            to verify their identity when connect to them
/etc/sshrc — global login script for SSH
      sshd — SSH server program
ssh-keygen — Generates public/provate key pairs for host
```

1.113.7

Set up secure shell (OpenSSH)

Geoff Robertson

Context

Objectives

hat is SSH?

0011

itilities

dvanced usage

User Keys

SSH from Windows

ther frontends

"Secure SHell"

A functional replacement of the ancient ${\tt rsh}$ command, except with encryption and authentication.

1.113.7

Set up secure shell (OpenSSH) Weight 4

Geoff Robertson

Context

Objective

What is SSH?

Versions of

utilities

dvanced usage

User Keys

SSH from Windows

ther frontends

Versions

Commercial SSH Finnish company. Original authors of SSH.

OpenSSH Split from last free version of commercial SSH.

Development led by OpenBSD team.

Draft "secsh" RFC.

Alternative implementations exist (Putty, Net::SSH::Perl, etc.)

.113.7

Set up secure shell (OpenSSH) Weight 4

Geoff Robertson

Context

Objective

Wilat is OOIT:

Versions of SSH

utilities

Advanced usage

User Keys

SSH from Windows

ther frontends

ssh Run a shell command on a remote host
sshd SSH server daemon
scp Copy files using SSH
sftp An ftp-like interface into scp
ssh-keygen Generate an SSH key pair
ssh-agent, ssh-add SSH key forwarding

1.113.7 Set up secure shell (OpenSSH)

Weight 4

Geoff Robertson

Conte

Objectiv

What is SSH?

Versions of

SSH commands and

ssh

S

sf

Advanced usage

Authenticating with

SSH from Windows

thar frontanda

icense Of This

ssh [options] host [command]

Run a shell command on a remote host.

Acts like a normal shell command. ie: STDIN, STDOUT work as normal.

Without a *command*, ssh runs an interactive login.

1.113.7 Set up secure shell (OpenSSH)

Weight 4

Geoff Robertson

Contex

Objective

What is SSH?

versions of 53

ISH commands a tilities

ssh

sft

Advanced usage

Authenticating with

SSH from Windows

Other frontends

scp user@host:path/file user2@host2:path/file2

Copy a file over ssh. user defaults to current login, user@host maybe omitted for local files, path is relative to \$HOME 1.113.7 Set up secure shell (OpenSSH)

Weight 4

Geoff Robertson

Contex

Objective

What is SSH?

Versions of

SSH commands and

sep

sf

Advance

Authoriticating with

Jser Keys

SSH from Windows

ther frontends

License Of This

sftp user@host:path

ftp-like command line interface to scp.
Only provided with more recent ssh versions.

1.113.7 Set up secure shell

et up secure she (OpenSSH) Weight 4

Geoff Robertson

Contex

Objectiv

What is SSH?

Versions of

SSH commands a

sc

sftp

Advanced usage

Authenticating with

SSH from Windows

SOLL HOLL ANDOW

Juler fronterias

Redirecting stdin and stdout Advanced Usage

Remember that STDIN and STDOUT still work as normal (unlike telnet):

ssh remote tar zcf - /remotepath > localfile.tar .gz vs

Set up secure shell (OpenSSH) Weight 4

Geoff Robertson

Redirecting stdin and stdout

Advanced Usage X Forwarding

ssh -X host.

Login to *host* and "forward" X11 connections back to the local Xserver.

A "fake" \$DISPLAY and xauth environment are created, and the X11 data is passed back over the same SSH connection.

Set up secure shell (OpenSSH) Weight 4

Geoff Robertson

X forwarding

Advanced Usage X Forwarding ctd...

 Forwarding X over SSH is secure and easy, but slower than not doing it.

 On a local LAN, the encryption is probably unnecessary—use normal X methods such as rstart instead (rstart can use ssh for authentication anyway).

- Specialised X11 caching methods (eg: LBX) can get better performance than ssh compression over slow links.
- ▶ There are concerns over connecting to a hostile remote machine and forwarding X back again, so don't forward X by default. A hostile remote site may forward damaging commands back down the link to your X server (ie your screen and keyboard).

Set up secure shell (OpenSSH) Weight 4

Geoff Robertson

X forwarding

Advanced Usage

Arbitrary ports can also be forwarded over the SSH connection, to add security to other protocols (or bypass poor firewall policies...)

```
# .fetchmailrc example
poll localhost protocol pop3 port 11110:
    preconnect "ssh -C -f user@host.com \
        -L 11110:host.com:110 sleep 10"
```

1.113.7 Set up secure shell

et up secure she (OpenSSH) Weight 4

Geoff Robertson

Conte

Objectiv

What is SSH'

versions of 55m

SSH commands and utilities

Advanced usage
Redirecting stdin and stdout

Port Forwarding

Authenticating wit

SSH from Windows

Other frontends

Other frontends

Advanced Usage SSH Kevs

- Public key authentication. More secure alternative to password login.
- ▶ Generate a public/private "key pair" with ssh-keygen.
- Keep the private key secret.
- Append the public key into your (remote)
 - ~/.ssh/authorized keys to allow access.
 - \$ cat identity.pub »
 - \sim /.ssh/authorized keys \hookleftarrow
- More powerful automation (scripting) possibilities.

Set up secure shell (OpenSSH) Weight 4

Geoff Robertson

Authenticating with User Keys

Advanced Usage SSH Authentication Agent

- ssh-agent allows key information to be "forwarded" between its child processes—even across nested ssh sessions.
- Start ssh-agent in your X-session or login scripts, and run ssh-add to add keys.
- ▶ ssh-askpass is (basically) an X11 version of ssh-add.

1.113./ Set up secure shell (OpenSSH)

Weight 4

Geoff Robertson

Conte

Objectiv

what is 55H

versions of a

SSH commands and utilities

Advanced usage

Authenticating with

ssh-agent

SSH from Windows

ner frontends

icense Of This

Advanced Usage SSH from win32

Putty Includes command line pscp.exe scp clone too.

http://www.chiark.greenend.org.uk/
~sgtatham/putty/

Winscp Graphical SCP client.

http://winscp.vse.cz/eng

1.113.7 Set up secure shell (OpenSSH)

Weight 4

Geoff Robertson

Conte

Objectiv

What is SSH

versions of

SSH commands and utilities

Advanced

uthenticating with Iser Keys

SSH from Windows

Other frontends

License Of This

Advanced Usage Other "frontends"

KDE kio fish Provides ssh://konquerer paths. tramp.el Transparent access to remote files for emacs. rsh-compatible Anything that can use rsh (eg: CVS)

Set up secure shell (OpenSSH) Weight 4

Geoff Robertson

Other frontends

Topics Covered

Context

Objectives

What is SSH?

Versions of SSH

SSH commands and utilities

ssh

scp

sftp

Advanced usage

Redirecting stdin and stdout

X forwarding

Port Forwarding

Authenticating with User Keys

ssh-agent

SSH from Windows

Other frontends

License Of This Document

.113.7

Set up secure shell (OpenSSH) Weight 4

Geoff Robertson

Context

Nhipotivos

Mhat is SSH

SSH commands

duanced uses

henticating wi

I L former AAGeneraters

Other frontends

Amer frontends

License Of This Document

Set up secure shell (OpenSSH) Weight 4

Geoff Robertson

Context

Objectives

Wildt is Son!

SSH commands and

ıtilities

Advanced usage

User Keys

SSH from Windows

Other frontend

License Of This Document

Copyright © 2005, 2003 Geoffrey Robertson <ge@ffrey.com> and Nick Urbanik <nicku@nicku.org>.

Permission is granted to make and distribute verbatim copies or modified versions of this document provided that this copyright notice and this permission notice are preserved on all copies under the terms of the GNU General Public License as published by the Free Software Foundation—either version 2 of the License or (at your option) any later version.