OpenSSH

Szwajcarski scyzoryk dla Internetu.

Dariusz Puchalak
Dariusz < at > Puchalak.net


joe-ks.com

History

SSH: Secure Shell
Created by Tatu Ylonen (1995)

- Secure loggin into remote computer
- Authentication, encryption, integrity

Why SSH?

- IP spoofing
- IP source routing
- DNS spoofing
- Password sniffing
- Manipulation of transfer data
- Atack on X11 (sniffing on authorization)

SSH replaces telnet

ssh host.domena.pl

ssh user@host.domena.pl

ssh -l user host.domena.pl

SSH replaces FTP

Podsystem SFTP

```
sftp host.domena.pl
sftp> dir
```

SSH replaces r-command

rexec
ssh host "cat /etc/passwd"

rlogin
ssh user@host

rcp:
scp file host.domena.pl:

Authentication

password
publickey (some patches to use X.509)
GSSAPI – Kerberos or NTLM
keyboard-interactive – skey or tokens

1000 and 1 passwords

```
bash$ ssh-keygen -b 2048 -t rsa -f test
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in test.
Your public key has been saved in test.pub.
The key fingerprint is:
c4:56:cb:dc:38:fd:91:bc:b3:e0:9f:04:e5:ea:e2:08
scorpius@debian
```

1000 and 1 passwords

ssh-agent

bash$ ssh-add
Enter passphrase for /home/scorpius/.ssh/id_rsa:
Identity added: /home/scorpius/.ssh/id_rsa
(/home/scorpius/.ssh/id_rsa)

bash$ ssh-add -l
1024 73:b9:ff:34:a7:fc:6e:3f:27:66:e6:cc:61:f9:ae:10
/home/scorpius/.ssh/id_rsa
(RSA)

skopiować test.pub do .ssh/authorized_keys na mszynie zdalnej

Remote command execution

Synchronization of remote files using rsync over SSH

rsync -avH -e ssh hosta:2BACKUP/ ../

Remote command execution

Filesystem backup over SSH

ssh "tar -cSzv --one-file-system -C / -f - ."
server1 | cat > serwer1-backup-root.tar.gz

Remote command execution

Moving files beetwen different filesystems:

```
ssh rootdp@hostA "tar -cSzv -C / -f -
/u02/_installs/9iAS/" | ssh rootdp@192.168
.1.44 "tar -xpSzv  -C / -f -"
```

NNTP over SSH?

LocalForward

LocalForward 1050 news.pwr.wroc.pl:119

bash$ NNTPSERVER=localhost
NNTPPORT=1050 tin -r

... over SSH

POP3 over SSH:
LocalForward 1110 news.pwr.wroc.pl:110

SMTP over SSH:
LocalForward 1025 news.pwr.wroc.pl:25

IMAP over SSH:
LocalForward 1143 news.pwr.wroc.pl:143

LocalForward 10.0.0.2:25 poczta.pl:25

Remote Forward

RemoteForward 65020 127.0.0.1:22

GatewayPorts

GatewayPorts yes

GatewayPorts no

GatewayPorts clientspecified

Your own proxy

DynamicForward 1080

Socks4/Socks5 proxy

Agent forwarding

Agent forwarding

```
ssh -A host1
user@host1:~$
user@host1:~$ ssh host2
....
user@host2:~$
```

Agent forwarding is it secure?

Agent forwarding from inside:

Need rights to read socket:
/tmp/ssh-.../agent.931

Exploit:
EXPORT SSH_AUTH_SOCK=/tmp/ssh-XX2aESOF/agent.931
ssh-add -l
ssh root@hostA rm -rf / tmp/plik

Better way

SSH - proxycommand

.ssh/config

```
...
Host hostB
        ProxyCommand ssh hostA nc %h %p
Host hostA
        HostName 172.16.48.10
...
```

```
bash$ ssh hostB
```

Proxy Command 2

Bypassing aplication firewalls:

ProxyCommand nc -X connect -x 192.168.1.1:8080 %h %p

X11 forwarding over SSH

ssh -X user@host netscape

Trusted X11 forwarding:
ssh -Y user@host

Host lefthand
    Hostname 192.168.1.99
    User lfmk
    ForwardX11 yes

OpenSSH VPN

```
Host sshgateway
    Tunnel yes
    TunnelDevice 0:any
    PermitLocalCommand yes
    LocalCommand sh /etc/netstart tun0
```

SSH i cron

command="cat /etc/passwd" ssh-rsa AAAA[.....]sagSH kluczyk123

from=”serverA.net”
idle-timeout=5m
no-agent-forwarding
no-port-forwarding
no-X11-forwarding
no-pty
permitopen=”hostB.domain:12345”
tunnel=”n”

SSHFS

Network filesystem using SSH
(Needs FUSE)

Dariusz@Puchalak.net

Reusing Control Connection

```
Host *
  ControlMaster auto
  ControlPath /tmp/%r@%h:%p
```

Summary

Types of tuneling:

- LocalForward
- RemoteForward
- DynamicForward
- ProxyCommand
- ForwardX11/ForwardX11Trusted
- Tunnel
- ControlMaster

Security

- ssh-agent
- X11
- GatewayPorts
- MITM
- SSH-1.99
- SSH timing attack

Questions?

Dariusz@Puchalak.net

Thank you.

http://docs.probosit.pl/SSH

Dariusz@Puchalak.net