



Know your tools

SSH

Dariusz Puchalak

Dariusz_Puchalak < at > ProbosIT.pl



History

SSH: Secure Shell
Created by Tatu Ylonen (1995)

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



Why SSH?

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



SSH replaces r-command

rexec

```
ssh host "cat /etc/passwd"
```

rlogin

```
ssh user@host
```

rftp:

```
scp file host.domena.pl:
```



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



Remote command execution

Moving files between different filesystems:

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



Remote network capturing

```
ssh root@10.0.0.254 "tcpdump -l -n -s 0 -w -  
not port 22" | wireshark -i -
```



File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... Clear Apply

No.	Time	Source	Destination	Protocol
3199	59.303589	10.0.0.254	10.0.0.120	ICMP
3200	60.303525	10.0.0.120	10.0.0.254	ICMP
3201	60.303565	10.0.0.254	10.0.0.120	ICMP
3202	61.303820	10.0.0.120	10.0.0.254	ICMP
3203	61.303857	10.0.0.254	10.0.0.120	ICMP
3204	62.303829	10.0.0.120	10.0.0.254	ICMP
3205	62.303876	10.0.0.254	10.0.0.120	ICMP
3206	63.304947	10.0.0.120	10.0.0.254	ICMP
3207	63.304989	10.0.0.254	10.0.0.120	ICMP

Frame 1 (74 bytes on wire. 74 bytes captured)

```
0000  00 40 ca df 13 0c 00 40  ca df 11 ba 08 00 45 00  .@.....@ .....
0010  00 3c ca 80 40 00 40 06  5b 10 0a 00 00 2e 0a 00  .<..@.@. [...
```

-: <live capture in progr... Packets: 3207 Displayed: 3207 ... Profile: Default



Remote

?



\$HOME/.ssh/config

Host router

Hostname 192.168.1.1

Port 2022

User root

Ciphers aes256-cbc

MACs hmac-sha1



\$HOME/.ssh/config

Host *

StrictHostKeyChecking ask

ForwardAgent no

ForwardX11 no

ForwardX11Trusted no

GatewayPorts no

Protocol 2

CheckHostIP yes

Ciphers aes256-ctr

MACs hmac-ripemd160



LocalForward

```
$HOME/.ssh/config
```

```
Host corp-remote
```

```
HostName XXX.corp.pl
```

```
LocalForward 1100 mail.int.corp:110
```

```
LocalForward 1025 mail.int.corp:25
```

```
LocalForward 1143 mail.int.corp:143
```

```
$ ssh corp-remote
```

```
mail client configured to used:
```

```
POP3 localhost:1100
```

```
IMAP localhost:1143
```

```
SMTP localhost:1025
```



Remote Forward

```
RemoteForward 65020 127.0.0.1:22
```



GatewayPorts

GatewayPorts yes

or

GatewayPorts clientspecified

...

RemoteForward przecieki.pl:2080 internal.corp.pl:80

...

GatewayPorts no

RemoteForward [localhost]:2080



Your own proxy

DynamicForward 1080

Socks4/Socks5 proxy



DynamicForward 1080

Web browser set to use proxy on localhost:1080

ssh remote.site.pl

Go to any site with „your address is” and
you are connected from:

remote.site.pl

:)



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 application firewalls:

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

```
netcat -X proxy_protocol
```

Supported protocols are ... “connect” (HTTPS proxy).



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 and 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)



SSHFS

```
sshfs my_comp:/ sshfs-da1/
```

```
Password:
```

```
df -m sshfs-da1/
```

Filesystem	1M-blocks	Used	Available	Use%	Mounted on
root@10.0.0.254:/	1024000	0	1024000	0%	/home/puchalakd/sshfs-da1



Reusing Control Connection

Host *

ControlMaster auto

ControlPath /tmp/%r@%h:%p



Encapsulate TCP connections in DNS

```
cat $HOME/.dns2tcprc
```

```
domain = your.domain.tld
```

```
ressources = ssh
```

```
local_port = 4430
```

```
server = 10.12.23.45
```

```
cat $HOME/.ssh/config
```

```
Host remote-via-dns
```

```
    HostName localhost
```

```
    DynamicForward 1080
```

```
    Port 4430
```



Encapsulate TCP connections in DNS

dns2tcpc -r ssh

Listening on port : 4430

ssh remote-via-dns

```
16:30:04.642528 IP 10.10.10.37.49062 > 10.12.23.45.53: 47518+ KEY?  
AACBgCTBA3NzaA==.your.domain.tld. (50)  
16:30:04.657650 IP 10.12.23.45.53 > 10.10.10.37.49062: 47518 1/0/0 (74)  
16:30:04.658668 IP 10.10.10.37.49062 > 10.12.23.45.53: 61644+ TXT?  
2vIAAAABBA==.your.domain.tld. (46)  
16:30:04.713632 IP 10.12.23.45.53 > 10.10.10.37.49062: 61644 1/0/0 (111)  
16:30:04.713952 IP 10.10.10.37.49062 > 10.12.23.45.53: 10728+ TXT?  
2vIAAQACBA==.your.domain.tld. (46)  
16:30:04.715062 IP 10.10.10.37.49062 > 10.12.23.45.53: 22382+[|domain]  
16:30:04.715115 IP 10.10.10.37.49062 > 10.12.23.45.53: 2755+ TXT?  
2vIAAAAEBA==.your.domain.tld. (46)  
16:30:04.716214 IP 10.10.10.37.49062 > 10.12.23.45.53: 12437+[|domain]  
16:30:04.716319 IP 10.10.10.37.49062 > 10.12.23.45.53: 61821+ TXT?  
2vIAAAAGBA==.your.domain.tld. (46)  
16:30:04.716370 IP 10.10.10.37.49062 > 10.12.23.45.53: 22220+[|domain]
```



Encapsulate TCP connections in ...

ICMP

...

and use ssh on top

and sshfs works :))

and portforwarding works :))

and all ssh stuff you know works :))



Summary

Types of tunneling:

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



Security

- ssh-agent
- X11
- GatewayPorts
- MITM
- SSH-1.99
- SSH timing attack
- Debian openssl
- SSH plaintext recovery vulnerability



Questions?



Thank you.

<http://docs.probosit.pl/SSH>