SSH: uso quotidiano

LinuxDay 2k12

mailto:johnnyrun@linuxvar.it

Cosa??

- intro supersonica su ssh
- non posso vivere senza....
- Troppi host e poca memoria (dell'op)
- networking e ssh
- il mio ambiente sull'host remoto
- comodità vs sicurezza
- velocità
- tool esterni

Intro

Storia

- In 1995, Tatu Ylönen, a researcher at Helsinki University of Technology, Finland
- 1998 - SSH Communications Security
- 1999 Björn Grönvall's torna alla 1.2.12 e sviluppa OSSH
- 1999 OpenBSD (2.6) forka OSSH in OpenSsh
- 2006 ssh-2 viene adottato come standard

Non posso vivere senza ...

Autocompletamento

- Bash completion
- zsh

CHIAVI SSH

- LATO CLIENT

  ssh-keygen

  ~/.ssh/id_rsa ~/.ssh/id_rsa.pub
- LATO SERVER

  mkdir ~/.ssh; chmod 600 ~/.ssh;

  cat id_rsa.pub >> ~/.ssh/authorized_keys2

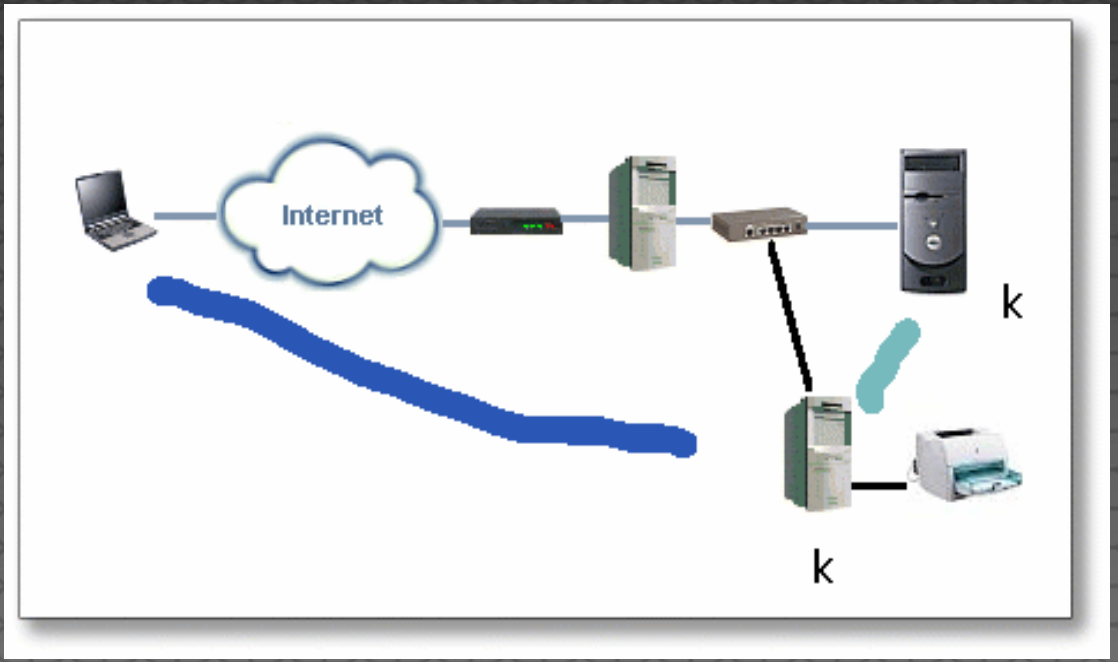
Anatomia di una chiave pubblica

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAvE4Q/QlWmQY
1z56U5i8jqvjZgCPEd+631rIfMKr91nx8Te4bXdC990jqXdzxNSXc
OzVkTtj/OAoYeXiUi39DxsIULc+Yjbk9jEuVv694Bxq7VwC6F7ofLE
9O5CaQFDaRlfDX7HhPms/29H/jbkBOgSyllE//oPuN2qxe2NRTKT
Dty5zcxo26J+nVV3DQGbtDU+Yzm6igcRdB41WjMYDAG623Z586
g6KhyrCG4Rsefspw64wNcxWYCSHe0lEFMl6SEC/jghosDiwfqjlin
FqFp2PZeY4cz4f3QKjkmsu3f/Z18gDARwLcbj0Ofj3XNNlu4McEd
AaDQrS0NYxmna/I0w== gianni@penombra

SSH AGENT

- Compreso in openssh-client
- Versioni grafiche (gnome-keyring / kde??)
- Ssh-agent
- opzione -t TEMPOinSecondi
- Forward dell'agent

  ssh -A user@host



Confusione del gnome keyring

$ ssh-add -D

All identities removed.

$ ssh-add -l

2048 84:62:12:4c:a3:33:a2:c8:1f:22:3a:63:3b:ab:b3:f4 gianni@gianni-laptop (RSA)

- WTF!!

WTF!!

From: "C. Scott Ananian" <cscott@xxx>

To: 472477@bugs.debian.org

Subject: Bug still present

Date: Fri, 27 Jan 2012 11:41:02 -0500

Ping? It's been almost **four** years now, and this bug is still present.

It's causing me troubles with github ssh.

--scott

Ma io volevo usare..

- ssh-add -D (delete all)
- ssh-add -x (lock!!)
- ssh-add -d

Sinonimi

- Ssh user@host
- Ssh -l user host

  opzione
- Ssh -o User=user host

  opzione in formato config file

Sinonimi

-C	Compression=yes
-p 2222	Port=2222
-l username	User=username
-D 4128	DynamicForward=4128
-X	ForwardX11=yes
-A	ForwardAgent=yes
-N	
	VerifyHostKeyDNS=yes

Troppi host e poca memoria (dell'op)

~/.ssh/known_hosts

- HashKnownHosts=yes ## DEFAULT
- HASHED:

  o|1|QKgw7OseDqXWKGkk5eqxOLF5w10=|+puenNkNRnqlOXZRK8HvlzcKiEI= ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA1HwEZNDh6fHqx+Q4I1Rw/u0dOxqzhVvupYHUfHBA1zz5ArWM4iSRcRkETAyjc5tmgXYNll7U2bXskiyNIerzhHtGK01UOv/ct30s7TaASbuAg+Kl9h24xXCkmacPEtWKIBsz8eClPvm+adVoO8nVOZzt7DzaElpCoP3I1xHhXt2WPt/Yxd0W0tQobR2RRYJHBYyzEqgnGSvM2pV9HpU8czMXIqpXvCXB4ZC8vmmQ7cXqSozblkOPFII7V30QCDzOa6h/qVdRl7mYiSHqKFhH1tzhdZrunn/vv5QQQGv1Ne7h89TK6EAiPrrgVgP+aBG+ss8cirxOWeBDo5sj9nVAwQ==

- HashKnownHosts=no ## autocomplete :D

  127.0.0.1 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA1HwEZNDh6fHqx+Q4I1Rw/u0dOxqzhVvupYHUfHBA1zz5ArWM4iSRcRkETAyjc5tmgXYNll7U2bXskiyNIerzhHtGK01UOv/ct30s7TaASbuAg+Kl9h24xXCkmacPEtWKIBsz8eClPvm+adVoO8nVOZzt7DzaElpCoP3I1xHhXt2WPt/Yxd0W0tQobR2RRYJHBYyzEqgnGSvM2pV9HpU8czMXIqpXvCXB4ZC8vmmQ7cXqSozblkOPFII7V30QCDzOa6h/qVdRl7mYiSHqKFhH1tzhdZrunn/vv5QQQGv1Ne7h89TK6EAiPrrgVgP+aBG+ss8cirxOWeBDo5sj9nVAwQ==

~/.ssh/config

```
Host IlMioAliasPerLaMacchina
    Hostname 192.168.8.2
    User johnnyrun
    ForwardAgent=yes
Host *linuxvar.it
    User johnnyrun
Host *
    User root
```

my2c

- Convenzione nella nomenclatura degli host
- Dividere gli host per cliente
  - Non si può fare

    include “config_miocliente”
  - Ma posso fare:

    cat ~/.ssh/config_* >~/.ssh/config

Velocità
(e sicurezza?)

Ciphers=arcfour

#connessioni brevi, performance ottime : siamo over VPN?? siamo in LAN?

Multiplexing TCP

- Perfetto per l'autocompletamento scp

  ControlMaster auto

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

  ControlPersist=yes #permani alla chiusura

  # muori quando riceverai un:

  $ ssh -O exit penombra

(in)Sicurezza

- cambiamenti di ip o identità molto frequenti?

  UserKnownHostsFile /dev/null

  StrictHostKeyChecking no

Il mio ambiente

Workaround

- Lato server ci sarebbe
  AcceptEnv='EDITOR MIAVAR2 MIAVAR3'
  ma di default accetta solo LC_*

- ssh host 'EDITOR=vim bash'

- Nel config:
  Command='EDITOR=vim bash'

Networking, rimbalzi, portForward

Rimbalzi

ssh root@hostuno -t ssh fuffa@192.168.0.1

- Più “evoluto”:

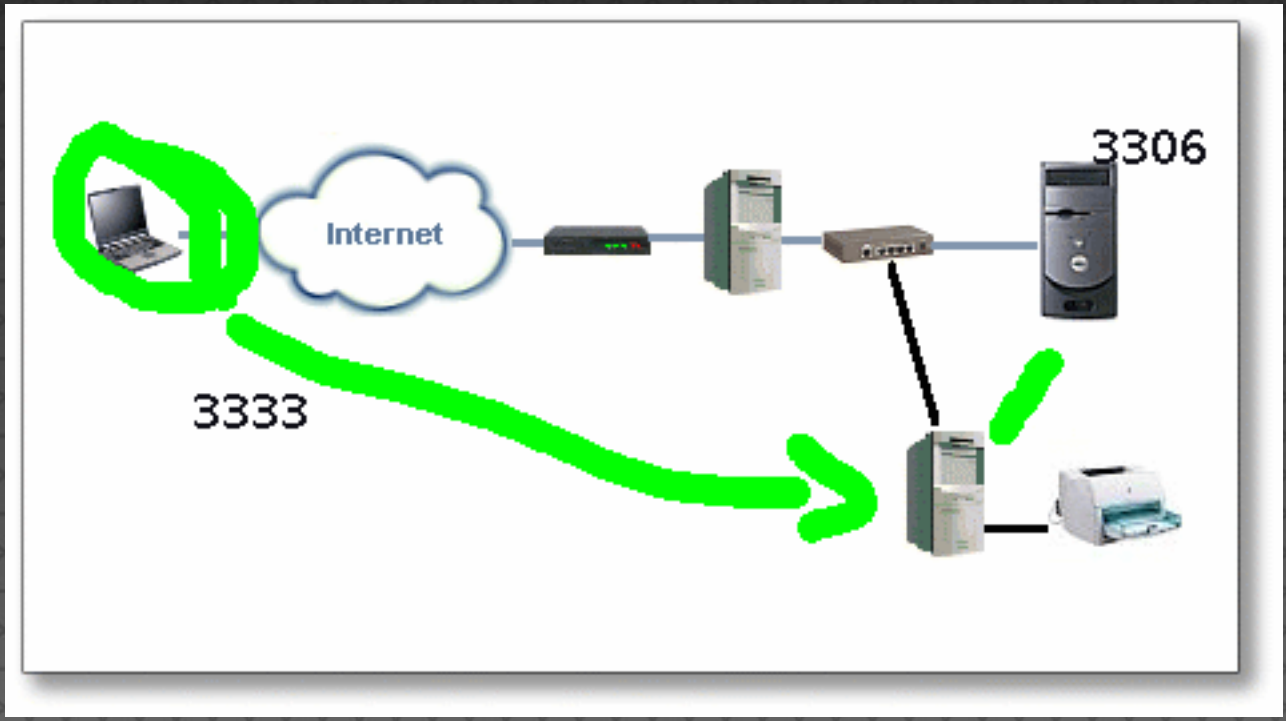
  Host due

  Hostname 192.168.0.1

  ProxyCommand ssh -q hostuno nc -q0 %h 22

Foward porte locali

- ssh -L 3333:192.168.0.12:3306 usename@host
- Abilitato di default in sshd

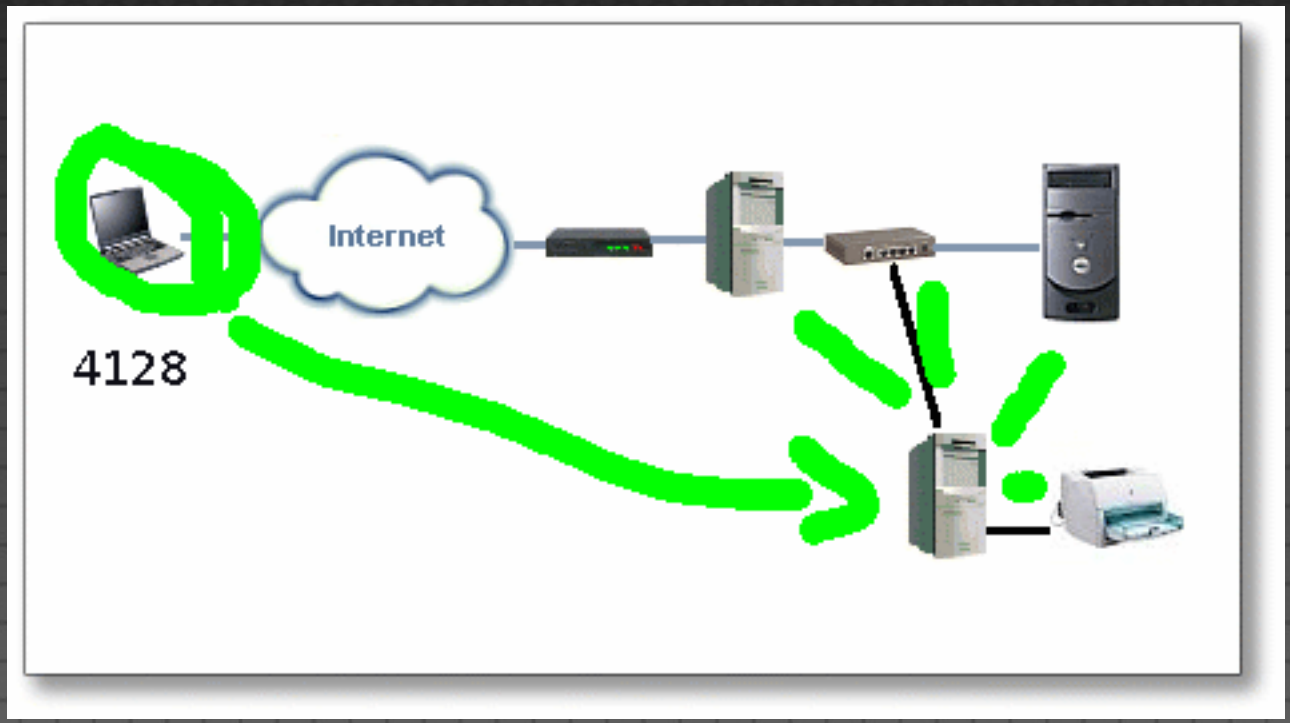


Nel config

- Host nome
  - Hostname 192.168.0.10
  - LocalForward 3333:192.168.0.12:3306
  - User root

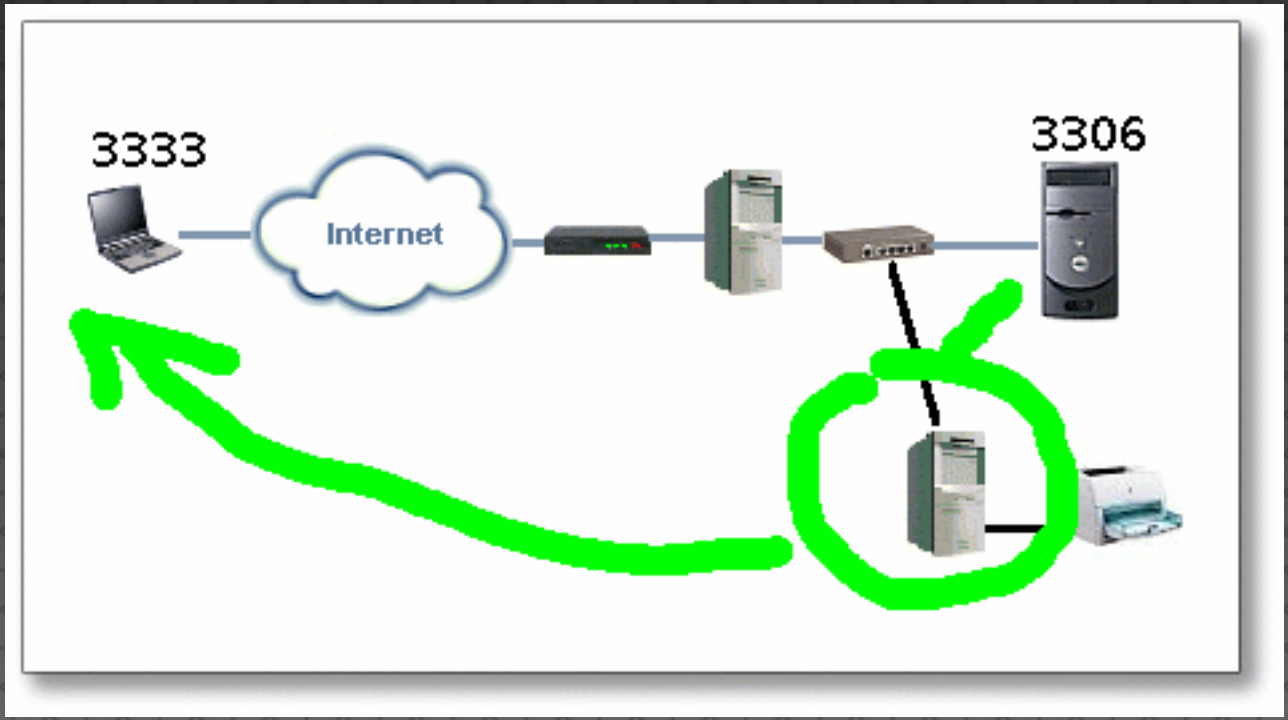
Socks server

Ssh -D 4128 -N root@host



Foward porte remote

- ssh -R 3333:192.168.0.12:3306 usename@host
- Abilitato di default in sshd



VPN oneline

#ssh -w 0:1 root@HOST

- LOCALE

  ifconfig tun4 10.0.0.1 up

  route add -net 10.0.0.0/24 tun4

- REMOTO

  ifconfig tun4 10.0.0.2 up

  route add -net 10.0.0.0/24 tun4

Tool esterni

sshfs

- sshfs user@host:/var/www ./mountpoint

- fusermount -u ./mountpoint

Cluster ssh

- cssh host1 host2 host3

Cssh: my2c

mcssh lvwww

mcssh www

mcssh '.*www[1-5]'

- #!/bin/bash

  STR=$1

  cssh $(cat ~/.ssh/config |awk '/Host\ .*'$STR'/ {print $2}'|sort|uniq);