

Forum:[Hack Forums](#)

Thread: [Create a SSH key?](#)

Lorenzon - June 22, 2015, 11:32 pm

I'm asked to create a SSH key to access a server. My question is, is it just as easy as running the ssh-keygen and save the keys or should I do something special like specifying the user and the domain?

I mean should I create a key that is in this format: root@192.168.1.1 or is admin@admin.local okay that's created when I just run the ssh-keygen?

Don't really know how these keys work I've searched a bit but I haven't found anything that's relevant too my situation.

I'm running Mac btw but that shouldn't matter.

Benign - June 22, 2015, 11:41 pm

Yes it is as simple as using ssh-keygen as the user that you want to authenticate remotely as, then copying the public key that gets created (for example for RSA it's id_rsa.pub) to ~/.ssh/authorized_keys on the client.

Then you can seamlessly authenticate to the server from the client using ssh, with the user that you created the key as.

Lorenzon - June 23, 2015, 12:22 am

(Jun 22, 2015 11:41 PM)Benign Wrote: [\[CITE\]](#) Yes it is as simple as using ssh-keygen as the user that you want to authenticate remotely as, then copying the public key that gets created (for example for RSA it's id_rsa.pub) to ~/.ssh/authorized_keys on the client.

Then you can seamlessly authenticate to the server from the client using ssh, with the user that you created the key as.

Yeah but I think I'll be authenticating as the root user, should I create a key that's like root@192.168.1.1 or will the certificate that's created if I just run the ssh-keygen okay?

Betty Blue - June 23, 2015, 11:52 am

(Jun 23, 2015 12:22 AM)Lorenzon Wrote: [\[CITE\]](#) Yeah but I think I'll be authenticating as the root user, should I create a key that's like root@192.168.1.1 or will the certificate that's created if I just run the ssh-keygen okay?Don't do that. Don't authenticate as root even with keys.

If you insist on doing that. You just need to use ssh-keygen. Then use scp to copy it to the remote server. Then change ssh_config so it says

PHP Code

```
<?php
```

PasswordAuthentication no

There is already an entry for it. Just change yes to no.

xkox - June 25, 2015, 10:21 am

```
ssh-add /home/user/.ssh/id_dsa
```

```
ssh USER@HOST_NAME -p
```

And you're ready to go.

