SSH

Sumner Evans
February 16, 2017
Mines Linux Users Group
Getting Started
What is SSH?

- SSH stands for Secure SHell.
- SSH is a cryptographic network protocol for operating network services securely over an unsecured network.
- SSH clients allow you to access any SSH server remotely and securely.
- SSH uses public-key cryptography for authentication.
- You can do other things with SSH as well.
What is SSH?

- SSH stands for Secure SHEll.
- SSH is a cryptographic network protocol for operating network services securely over an unsecured network.
  - SSH clients allow you to access any SSH server remotely and securely.
  - SSH uses public-key cryptography for authentication.
  - You can do other things with SSH as well.
What is SSH?

- SSH stands for Secure SHell.
- SSH is a cryptographic network protocol for operating network services securely over an unsecured network.
- SSH clients allow you to access any SSH server remotely and securely.
  - SSH uses public-key cryptography for authentication.
  - You can do other things with SSH as well.
What is SSH?

- SSH stands for Secure SHell.
- SSH is a cryptographic network protocol for operating network services securely over an unsecured network.
- SSH clients allow you to access any SSH server remotely and securely.
- SSH uses public-key cryptography for authentication.
- You can do other things with SSH as well.
What is SSH?

- SSH stands for Secure SHell.
- SSH is a cryptographic network protocol for operating network services securely over an unsecured network.
- SSH clients allow you to access any SSH server remotely and securely.
- SSH uses public-key cryptography for authentication.
- You can do other things with SSH as well.
How do I get an SSH client?

- **Linux**: openssh (or similar) package in your package manager (it’s probably already already installed).
- **macOS**: SSH is already installed, but it may be an old version. Use Homebrew if you want the latest version.
- **Windows**: You can use PuTTY (http://www.putty.org/).
- **Your web browser**: there’s an SSH plugin for all the modern browsers.
- **Your phone**: there’s an app for that.
How do I install an SSH server?

- Arch Linux: `openssh` package.
- Other Linux: you may need to install `openssh-server` or similar.
- macOS: You can enable Remote Login\(^1\) in System Settings.
- Windows: Read this ServerFault article and good luck.
  
  [http://serverfault.com/questions/8411/what-is-a-good-ssh-server-to-use-on-windows](http://serverfault.com/questions/8411/what-is-a-good-ssh-server-to-use-on-windows)
Using an SSH client
The basics

- `ssh [user@]server[:port]`
  - `user` is defaulted to your local username
  - `port` is defaulted to 22
- Enable X-Forwarding: use `-X` flag
- Exiting an SSH session: Ctrl + D or type `logout` or `exit` if your remote session is still running
- If you want to just run one command on the remote server: `ssh [flags] user@server[:port] command`
The basics

- `ssh [user@]server[:port]`
  - user is defaulted to your local username
  - port is defaulted to 22
- Enable X-Forwarding: use `-X` flag
- Exiting an SSH session: Ctrl + D or type `logout` or `exit` if your remote session is still running
- If you want to just run one command on the remote server: `ssh [flags] user@server[:port] command`
The basics

- `ssh [user@]server[:port]`
  user is defaulted to your local username
  port is defaulted to 22

- Enable X-Forwarding: use `-X` flag

- Exiting an SSH session: `Ctrl + D` or type `logout` or `exit` if your remote session is still running

- If you want to just run one command on the remote server: `ssh [flags] user@server[:port] command`
The basics

- `ssh [user@]server[:port]`
  user is defaulted to your local username
  port is defaulted to 22

- Enable X-Forwarding: use `-X` flag

- Exiting an SSH session: Ctrl + D or type `logout` or `exit` if your remote session is still running

- If you want to just run one command on the remote server: `ssh [flags] user@server[:port] command`
When logging into a server, you can authenticate using your password, or you can set up an SSH key to authenticate you without entering your password. How to configure this?

1. `ssh-keygen` and follow the steps - definitely set a password
2. `ssh-copy-id server` and enter your password on the server
3. `ssh server` should now authenticate you without having to use a password
But now I have to enter my SSH Key password all the time.

If you don’t like entering your SSH key password all the time, you can use `ssh-agent` and `ssh-add`.

I have the following in my `~/.zshrc` to set this up automatically.

```bash
if [ ! -S ~/.ssh/ssh_auth_sock ]; then
eval `ssh-agent`
    ln -sf "$SSH_AUTH_SOCK" ~/.ssh/ssh_auth_sock
fi
export SSH_AUTH_SOCK=~/.ssh/ssh_auth_sock
ssh-add -l | grep "The agent has no identities" && ssh-add
```
Configuring your SSH client

One thing that is annoying is when you have to type out your full username and full hostname when connecting to a server. You can add aliases to `~/.ssh/config` so you don’t have to do this.

```plaintext
Host isengard
  HostName isengard.mines.edu
  User jonathanevans
  Port 42
  ...
```
Setting up an SSH Server
Enabling SSH to your computer

On Arch, just start an enable sshd via systemctl.

You can configure your SSH daemon via the
/etc/ssh/sshd_config file (note the d).

Here are some of the things you can configure:

- **AllowUsers** - allows you to set which users can log in
- **PermitRootLogin** - if yes, you can SSH into the computer as root
- **AllowGroups** - allows you to set which groups can log in
- **PasswordAuthentication** - set to no if you want to force authentication using SSH key
References

- The Arch Wiki: https://wiki.archlinux.org/index.php/Secure_Shell
- The SSH manpage
- This Medium Post: https://medium.com/@shazow/ssh-how-does-it-even-9e43586e4ffc#.uwmcu64az
- https://lani78.com/2008/08/08/generate-a-ssh-key-and-disable-password-authentication-on-ubuntu/

Thanks to Kieth Hellman for inspiring this talk
Questions?
This presentation was from the **Mines Linux Users Group**. A mostly-complete archive of our presentations can be found online at [https://lug.mines.edu](https://lug.mines.edu).

Individual authors may have certain copyright or licensing restrictions on their presentations. Please be certain to contact the original author to obtain permission to reuse or distribute these slides.