What is SSH:

Secure Shell (SSH) is a way for people called system administrators to connect to and control servers like websites, online databases, and other devices over the internet. The login information must be protected well to keep these connections safe. Sometimes, administrators use passwords to log in, but passwords have many problems. People often pick easy-to-guess passwords, share them with others, or get tricked into typing them on fake websites.

It's better to use something called asymmetric or public-key systems to make SSH more secure. It's like having a unique digital key that only the right person can use to open the door. In this lab, you will learn how to use one of these special keys called RSA to log in to a server instead of using passwords. This skill is essential for system administrators because it helps them better protect their systems.

Examples:

Imagine you have a website, and you want to ensure that only authorized people can change it. You can use SSH with an RSA key to let only those authorized people in.

Let us say you have a network device (like a router) that you need to control from a distance. Using SSH with a unique key, you can securely manage that device without worrying about someone else sneaking in and causing problems.

SSH Instructions

From the landing page, connect to the server were indicated to access your lab desktop environment. From here, open a new terminal window, and verify you can login to the following server:

```
ssh cyberarena@10.1.1.51

Password: Let's workout !
```

 The password will *NOT* be shown as you are typing it into the terminal!

Oh, no! You can login through SSH with only a password! Let us fix that. Use the following commands and configuration files to ensure login only occurs through asymmetric key authentication.

You will need to explore the commands through a web search and figure out the precise commands to run. Once you have fully secured the login for the cyberarena user, then assessment will show complete.

1. ssh-keygen: Run on your lab desktop machine to generate RSA public and private keys.

2. ssh-copy-id: Use your lab desktop to remotely copy your public key over to the remote server 10.1.1.51.

3. /etc/ssh/sshd_config: Edit this file with nano or vim (e.g., nano /etc/ssh/sshd_config) to enforce asymmetric key authentication.