Create SSH Server

To: All IT Personnel and System Administrators
From: Safin Singh, CEO
Date: 2/9/2024
Subject: Instructions for Setting Up an SSH Server on "earth" Machine

---

Purpose

This document provides detailed instructions for configuring an SSH server on the machine named "earth" within Earth, Inc.'s network infrastructure. The goal is to enable secure remote access for the user "goat" using public key authentication. The SSH server must listen on port 2022.

Requirements

- Machine Name: earth
- User: goat
- SSH Port: 2022
- Authentication Method: Public Key Authentication
- Public Key File: goat.pub

Pre-Installation Checklist

1. Ensure you have root or sudo privileges on the "earth" machine.
2. Verify that the SSH server software (OpenSSH) is installed. If not, install it using your system's package manager.
3. Locate the "goat.pub" file provided by the network security team.

Installation and Configuration Steps

Step 1: Configure SSH Server

1. Open the SSH server configuration file in a text editor. This file is usually located at `/etc/ssh/sshd_config`.

```
sudo nano /etc/ssh/sshd_config
```

2. Find the line that specifies the port number. Change it to listen on port 2022. If the line does not exist, add it.

```
Port 2022
```

3. Ensure that public key authentication is enabled by verifying the following line is uncommented and set to "yes":

```
PubkeyAuthentication yes
```

4. Save the changes and exit the text editor.

Step 2: Set Up User and Public Key

1. If the user "goat" does not already exist on the system, create it using the following command:

```
sudo adduser goat
```

2. Create a directory for SSH authorized keys for the "goat" user, if it doesn't already exist:

```
sudo mkdir -p /home/goat/.ssh
```

3. Copy the "goat.pub" file to the "goat" user's `.ssh` directory and rename it to `authorized_keys`:

```
sudo cp /path/to/goat.pub /home/goat/.ssh/authorized_keys
```

4. Adjust the permissions of the `.ssh` directory and the `authorized_keys` file:

```
sudo chown -R goat:goat /home/goat/.ssh
sudo chmod 700 /home/goat/.ssh
sudo chmod 600 /home/goat/.ssh/authorized_keys
```

Step 3: Restart and Verify SSH Service

1. Restart the SSH service to apply the changes:

```
sudo systemctl restart sshd
```

2. Verify that the SSH service is listening on port 2022:

```
sudo ss -tuln | grep 2022
```

You should see an entry indicating that SSH is listening on port 2022.

Post-Installation

- Ensure that the "goat" user can successfully authenticate using the provided public key. Test this by attempting to SSH into "earth" on port 2022 from a remote machine:

```
ssh -i /path/to/private/key -p 2022 goat@earth
```

- Document any issues encountered during the installation or testing phases and report them to the network security team for further assistance.

Conclusion

By following these instructions, you will secure remote access to the "earth" machine for the "goat" user using SSH on port 2022. This setup enhances our network security by employing public key authentication. For any questions or additional support, please contact the network security team.