Server Checklist

A bare minimum for any public facing Linux server.
These tests should be ran immediately or the host powered down until it's secured.

First Login

On a fresh Linux server, you'll first access your host as the root user. This user should only be used for administrative purposes, and not for running or installing local applications, packages, or services. Update your packages, and change /set the password for root.

```
sudo apt -y update && sudo apt -y upgrade


#Assuming this is a fresh system and first boot -
#Update your ROOT password
sudo passwd
New password:
Retype new password:
passwd: password updated successfully
```

Follow the instructions to Create New SSH Users carefully, and be sure to back up your keys appropriately in the process. You should be careful when distributing or granting access to your servers, as these keys grant access to whoever obtains them - However, we will configure passwords and 2FA to prevent this being an issue.

SSH Authentication Setup

Its important to be very specific about how you plan to authenticate over SSH. Check out the guides below for details on different forms of authentication, or choose your own. They are generally configured very much the same, once you have done it a few times you will be able to navigate the documentation to get the answers you need. Things to configure or look into for SSH -

- PAM
  - Check out different ways to authenticate, there are lots of modules available
- SSHD
  - Custom Port
- Fail2Ban
  - Setup Fail2Ban so users will be locked out upon repeated failed authentication attempts.
- UFW / IPTables / Firewall

- Specify what ports serve what types of packets, and in which direction they should be going.

Important Settings

SSH Configuration

- Creating New Users
- Enabling Google Two-Factor Authentication
- YubiKey Authentication

Basic FTP Configuration

- *You probably don't need it, and shouldn't use it.*

Hostname Configuration

- If you didn't already specify, have a look here.

OpenSCAP

These are automated tests that can be easily downloaded and ran on any Linux system. Check out their website for more information on what tests are available and how to run them. They provide a full user guide explaining the process for RHEL systems.

DevSec

These are some more automated tests that can be easily downloaded and ran on any Linux system. Be sure to check out the page on DevSec Linux Server Hardening, where we go into how you can install and use DevSec. There is a long list of tests available, just be sure to at the least run the tests covered in the guide linked above.

Revision #4
Created 2019-07-06 01:42:54 UTC by Shaun Reed
Updated 2020-05-27 08:02:33 UTC by Shaun Reed