THE PERFECT NGINX SERVER

CENTOS 8

INITIAL SERVER HARDENING

INITIAL SERVER HARDENING

We are finally going to login to your server and start the process of hardening the server.

This is the process of enhancing server security through a variety of means which results in a much more secure server operating environment.

Before you can login to your server, please ensure the following:

You have created a server instance as per the lecture "Web Hosts and Creating a Server Instance"

LINUX USERS:

You are good to go, no software installation or configuration is required.

MAC USERS:

Please ensure you have configured terminal as per the lecture.

WINDOWS USERS:

Please ensure that you have downloaded and configured CMDER as per the lectures. Ensure you have completed the entire lecture and configured the settings correctly.

FIRST LOGIN AS ROOT

You can open your terminal emulator and type the following command:

```
ssh root@ip_address
```

To change the root user's password, we make use of the command passwd

```
passwd
```

CONFIRM SELINUX STATUS

Type the command:

```
sestatus
```

Check the output for two directives: status and mode

REMOVE COCKPIT WEB SERVICE

```
dnf remove cockpit-ws
```

CHANGE THE PROMPT

We need to change the prompt to display our full location path rather than just the current location.

Find the line:

```
[ "$PS1" = "\\s-\\v\\\$ " ] && PS1="[\u@\h \W]\\$ "
```

Comment the line and add the following underneath:

```
PS1='\u@\H:\w \$ '
```

Save the file, the logout of the server to enable the change.

ADD A NEW NON-ROOT USER

You need to add a new user. This user is a non-root user, but you will give that user the ability to invoke root privileges when needed. A home directory for the user will also be created by the adduser command.

```
adduser username

passwd username
```

To delete a user:

```
userdel -r username
```

GIVE NON ROOT USER ROOT PRIVILEGES

The "wheel" group is a system group that is created by default. Any user that is part of the wheel group, can execute commands with elevated "root" privileges.

```
usermod -aG wheel username
```

PREVENT ROOT LOGIN

To prevent root login, you need to change to `/etc/ssh/` directory, open the sshd_config file and make the configuration changes.

```
cd /etc/ssh/

nano sshd_config
```

Find the line `PermitRootLogin`, you need to change `yes` to `no`.

We will use the systemctl command to restart various services on the server. Systemctl is the services manager utility on the server.

```
systemctl restart sshd
```

You are done working as the root user, you can logout of the server by typing exit.

```
exit
```

FIRST LOGIN AS A NON ROOT USER

You cannot login as the root user, root user login has been blocked on the server. You need to login as the non root user your created in the previous section.

As the non root user, you need to continue hardening the server process.

SSH KEY AUTHENTICATION

SSH keys are generated locally on your PC or MAC, **not** on the server

GENERATE KEY PAIR

Please ensure you are in your home directory and ensure you have a directory called .ssh/. Use the ls -a command and check the .ssh/ directory exists. If not, create the directory using the mkdir command:

```
cd

mkdir .ssh/
```

The key pair is generated locally on your pc or mac. Please ensure you are in the home directory of your PC or MAC.

The command is as follows:

```
cd

ssh-keygen -t rsa -b 4096
```

COPY THE PUBLIC KEY TO THE SERVER

The next step is to copy your public key to your server. The private key remains stored on your pc or mac and is not copied to the server.

```
scp .ssh/public_key.pub user@ip:/path/

scp .ssh/public_key.pub andrew@ip:/home/andrew/
```

SERVER CONFIGURATION

Login to your server:

The `ls` command will display the public key that was copied to the server.

The public key needs to be renamed to authorized_keys and to rename or move files or directories, you use the `move` command: `mv`

```
mv public_key authorized_keys
```

The `authorized_keys` file needs to be located in a directory called `.ssh/`

```
cd
mkdir .ssh/
mv authorized_keys .ssh/
```

Both the public key and the .ssh directory need to be secured.

```
cd
cd .ssh/
chmod 600 authorized_keys
sudo chattr +i authorized_keys
```

The .ssh directory itself must also be secured by changing the permissions.

```
cd
chmod 700 .ssh/
```

At this stage we need to edit the sshd_config file:

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

Edit the folllowing directives as per the video lecture.

```
# PubkeyAuthentication yes
AuthorizedKeysFile      .ssh/authorized_keys
PasswordAuthentication yes
```

Close nano and restart the ssh service on the server.

```
sudo systemctl restart sshd
```

At this stage DO NOT logout of the server. I'm going to repeat that, DO NOT logout of the server.

To login using a key pair:

```
ssh -i .ssh/private_key andrew@ip
```

CONFIG FILE

To login to your server using ssh key authentication, the command is:

```
ssh -i .ssh/private andrew@ip
```

You can use nano to create a config file:

```
cd

nano .ssh/config
```

You need to specify the following variables in a config file:

Host | Alias for the server

HostName | IP address of your server

User | The username you use to login

IdentityFile | path to the private key

ServerAliveInterval | Sets a timeout value, in seconds, after which if no data is received from the server. ssh will send a message to the server, requesting a response

ServerAliveCountMax | Sets the number of ServerAlive messages that can be sent

SERVER UPDATES

In the Linux Essential Skills section we looked at package managers, now we are going to start using the CentOS package manager `dnf` or dandified yum

```
sudo dnf update
```

FIREWALLD

As creating iptable rules can become very complex and manually typing firewall rules is an extremely frustration experience we are going to make use of Firewalld.

INSTALLING FIREWALLD

```
sudo dnf install firewalld
```

After installing firewalld, you need to start the firewall service:

```
sudo systemctl start firewalld
```

You also to enable the firewalld service to start after a server reboot:

```
sudo systemctl enable firewalld
```

To check the status of firewalld

```
sudo systemctl status firewalld
```

The service is running, but you will notice a warning:

```
WARNING: AllowZoneDrifting is enabled.

This is considered an insecure configuration option.
```

To "disable" AllowZoneDrifting

Please follow the video lecture regarding AllowZoneDrifting

After editing the firewalld.conf file, you need to restart the firewalld service:

```
sudo systemctl restart firewalld
```

CONFIGURING FIREWALLD

Firewalld is easy to configure.

To view the list of default rules, you have two commands:

```
sudo firewall-cmd --list-all

sudo firewall-cmd --list-services
```

We need to open http and https, that is ports 80 and 443 and then reload firewalld to enable the change in rules.

```
sudo firewall-cmd --zone=public --add-service=http --permanent

sudo firewall-cmd --zone=public --add-service=https --permanent

sudo firewall-cmd --reload

sudo firewall-cmd --list-all
```

Cockpit provides an additional vector of attack, to block Cockpit access:

```
sudo firewall-cmd --remove-service=cockpit --permanent

sudo firewall-cmd --reload

sudo firewall-cmd --list-all
```

FAIL2BAN

INSTALL FAIL2BAN

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-
8.noarch.rpm
```

To install fail2ban,

```
sudo dnf install fail2ban
```

After installing fail2ban, you need to start the fail2ban service:

```
sudo systemctl start fail2ban
```

You also to to enable the fail2ban service to start after a server reboot:

```
sudo systemctl enable fail2ban
```

To check the status of fail2ban

```
sudo systemctl status fail2ban
```

CONFIGURING FAIL2BAN

Fail2ban's configuration files are found in the `/etc/fail2ban` directory.

```
cd /etc/fail2ban

ls

sudo cp jail.conf jail.local
```

Open the `jail.local` file using nano

We need to edit the bantime, findtime and maxretry

Modify as per the video lectures

Unban an ip: check fail2ban log for the ip:

```
sudo fail2ban-client set `jailname` unbanip `ip`
```

THE FAIL2BAN LOG FILE

Fail2ban has its own log file, located in the following directory: `/var/log/fail2ban.log`

You can view the contents of a log file by using the cat or less commands.

To view the contents of a log file, you can use any of the following commands, followed by the log file name.

```
sudo cat filename

sudo less filename
```

The cat command will display the entire file contents on the screen, that’s fine if the file contains very little information.

The less command is more useful, as each page will be paused for you to peruse. You can use the following keys: HOME, END, PgUp, PgDn and your cursor keys. Pressing q will quit less and return to the prompt.

CONCLUSION

In this section we continued the process of hardening the server as the non root user.