Linux Host Security

Understanding Chroot Jails

Eghbal aminejad
LINUX AUTHOR AND TRAINER
github: @eqba1

Understanding Chroot Jails

- Course Objectives

- **Securing environments using chroot**
- **Limiting resource access using chroot jails**

Weight

- A chroot jail limits access to files on your system
- The command /usr/sbin/chroot will create an environment with a false root directory
- Services or users within the jail have access to only the files added to the jail
- if your chroot directory was /var/chroot then to you the bash shell would be found in /var/chroot/bin/bash
- All needed libraries, executables and configuration files need to be added to the jail

Chrooting Services

بعضی سرویس ها مانند DNS، بهترین پیشنهاد برای پیاده سازی با استفاده از chroot است. اگر تنظیم شود تمام فایل های مورد نیاز سرویس را در یک دایرکتوری کپی کرده و مسیر روت را به آن مسیر تغییر میدهیم. و در صورتی که شخصی به سرور DNS دسترسی بگیرد به آن دایرکتوری و فایلهای که در مسیر به اصطلاح زندان مانند وارد شده و مجوز های بسیار محدودی دارد.

```
$ ldd /bin/bash /bin/ls
$ sudo mkdir -p /v ar/chroot/{bin,etc,lib64}
$ echo "PS!='JAIL $ '" | sudo tee /var/chroot/etc /bash.bashrc
```

Then copy executables and teh libraries listed by ldd to the correct directory

Create a Jail

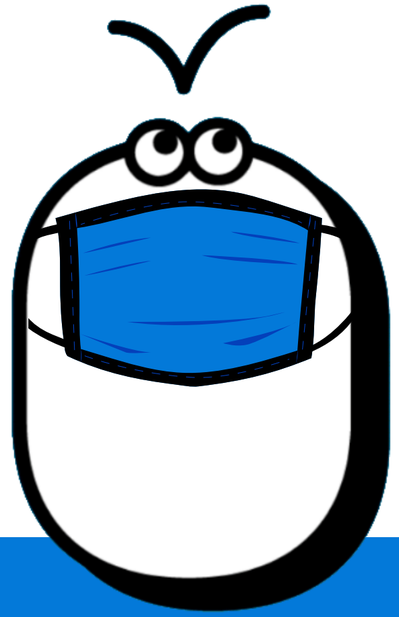
برای درک بهتر; یک محیط chroot برای یک کاربر ساخته، اجازه میدهیم که فقط بتواند دستوارت bash و ls را اجرا کند. قطعا نیاز داریم که برای اینکه این دستورات در یک محیط جدا اجرا شوند کتابخانه ها و پیکربندی های دو دستور را به مسیر جدید انتقال دهیم.

```
$ sudo chroot /var/chroot /bin/bash

JAIL $ ls -R /
```

Enter the Jail

در داخل این محیط به اصطلاح زندان، bash را در آن اجرا میکنیم. محیط کامند لاین که اجرا خواهد شد همان شلی است که در محیط مجازی در مسیر /var/chroot/bin/bash قرار دادیم. prompt نیز همانند پیکربندی تغییر خواهد کرد و تنها دستوری که میتوانیم اجرا کنیم دستور ls خواهد بود.

Now is your chance to build a jail



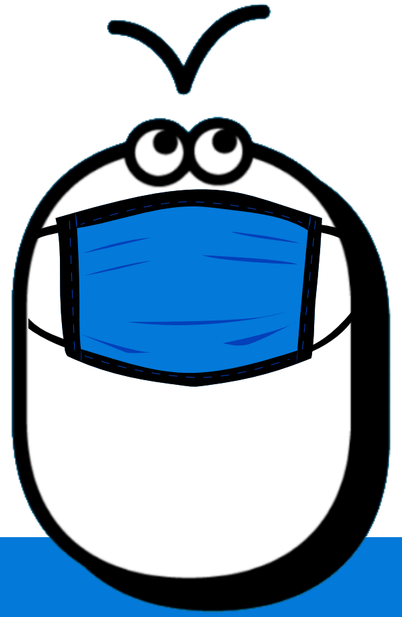
Demo

```
$ sudo useradd -s /bin/bash user1

$ sudo passwd user1

Match User user1
        ChrootDirectory /var/chroot
```

Chrooting Users

حالا کاربرها میتوانند با ssh وارد شوند. کسانی که با ssh وارد سیستم میشوند میتوانند دسترسی ریشه داشته باشند اما با این تفاوت که در دایرکتوری خاصی که ما برای انها تعیین کرده ایم نه کل سیستم. اگر میخواهیم که همه یوسرها به این دایرکتوری دسترسی نداشته باشند میتوانیم از Match User و Match Group استفاده کنیم.

Start chrooting users connecting to your ssh Server



Demo

summary

- By changing the root directory seen by a user or service you limit the files they can access to those within their jail
- We need to add executables, libraries and configuration files needed by the user or service
- The command ldd can display the libraries needed by commands
- Use your Linux skills to create a better list of libraries to copy:

```
ldd /bin/ls /bin/bash | cut -d " " -f3 | \
sed -e 's/://' -e '/^$/d' | sort | uniq
```

Weight

Next up

Limiting User Access to Resources

Eghbal aminejad

LINUX AUTHOR AND TRAINER

github: @eqba1