First Exercise: Boot Security - Break into Your Kali Virtual Machine

Your Kali virtual machine is ready to go, but we haven't given you a root password.

If you've turned it on, please turn it off at this time. Now turn it on and wait for it to show the blue Kali boot screen.

At this boot screen, **hit the e key** to edit the running boot configuration.

Hit the down arrow 14 times to reach the line that begins "linux" and ends with "ro quiet".

Hit Ctrl-e to move to the end of this line of text.

Replace the text that reads "ro quiet splash" with this text:

```
      rw quiet init=/bin/bash
```

Hit Ctrl-X to boot this configuration.

Once you reach a root shell, change the root password by running:

```
passwd root
```

Now enter the same password twice. To make things easy on yourself, choose `lockthisdown`.

Now, we want to remount the root filesystem as read-only. We need to determine the device file that the machine has mounted as its root partition. Try this:

```
mount | grep ext4
```

Your output might look like this:

```
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro)
```

The first field of this line (here: `/dev/sda1`) is providing the root (/) of the filesystem. Whatever that first device on the line is, insert it below in place of "/dev/sda1". This will remount the root partition as read-only.

```
mount -o ro,remount /dev/sda1 /
```

Now turn the system off, turn it back on again and allow it to boot to a graphical login screen. Login as root, then **hit Alt-F2** to run a program and type `lxterminal` to get a useful terminal.

Please read both sides of this sheet of paper

Welcome to “A Purple Team View – Attacking and Defending Linux, Docker and Kubernetes!”

We’re very excited to work with you!

Please, check your e-mail for a “Note from the Instructor.” If you haven’t received it, please e-mail the course creator and main instructor, Jay Beale, via jbeale@inguardians.com.

Please do the first exercise (on the other side of this page) at least a day before the class – it will give you access to the laptop. Then, please connect the laptop to the Internet. It uses “Resilio Sync” to download updated virtual machines, handouts and tools. It would be most helpful if the laptop was connected to the Internet and turned on for several hours during the day before our class.

We’ll be using Slack during the class. We have installed it on the laptop. We’ll help you join the Slack channel during the class.

Thank you for registering – you’re going to have a great time and learn quite a bit!

Please read both sides of this sheet of paper