

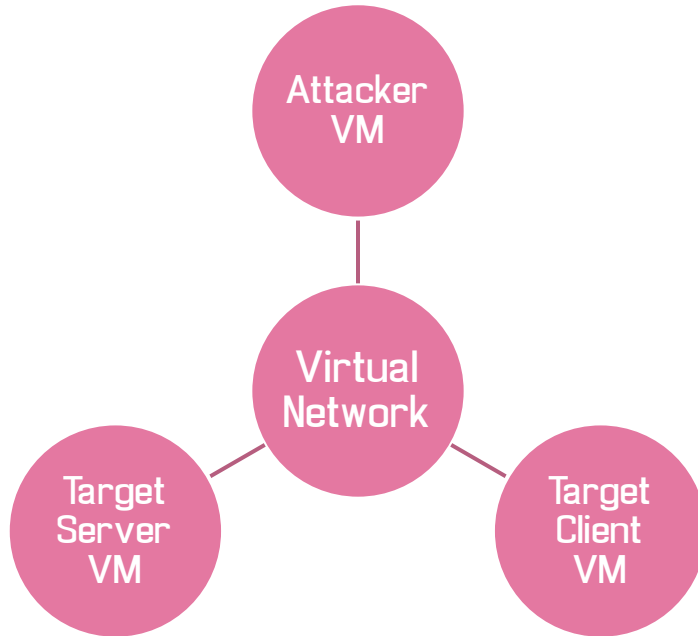
Setting up a PenTesting Environment

The aim

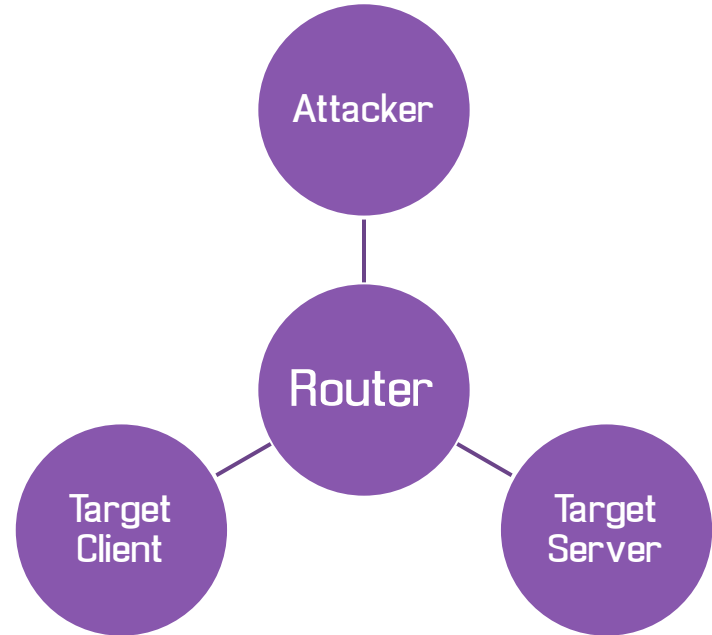
- ▶ To have an environment suitable to try out the skills you'll be learning
- ▶ To not have to perform any illegal activity
 - ▶ You'll only be hacking what you own
- ▶ To not interrupt anything else on your network
 - ▶ Whether accidentally or on purpose
 - ▶ Safety to try running exploits without HR tapping your shoulder.

What you'll need:

A computer with Virtual box



3 computers and your own router



The image features a white background with two large, solid pink triangles in the corners. One triangle is in the top-left corner, and the other is in the bottom-right corner. They are oriented such that their hypotenuses point towards the center of the slide.

The machines to create

The Offensive computer: Kali

- ▶ Will be our primary machine.
- ▶ Kali Linux is a specially maintained, debian based OS that comes pre-installed and configured with a bunch of security testing features
- ▶ Can be run in Live mode, but recommend a full install to store configs and scripts you create

The easy target: Metasploitable

- ▶ Will most often be the remote target.
- ▶ A pre-configured OS image
- ▶ Specifically built with a variety of vulnerable services and features enabled.
- ▶ Should ***NOT*** be put on any live network
 - ▶ It would be a serious weakness in any network, so we have it completely isolated from the internet

The desktop user: Ubuntu

- ▶ Used to demonstrate attacks on other user interfaces, such as XSS or MITM
- ▶ A fully patched, desktop installation of Ubuntu

The background features two solid pink triangles in the corners. One triangle is in the top-left corner, and the other is in the bottom-right corner. They are oriented such that their hypotenuses point towards the center of the slide.

Network Configuration

Setting up an isolated network in virtual box

- ▶ Virtual box's "Internal Network" interface will allow our VM's to communicate without any external ingress/egress
- ▶ Does not come with DHCP, so we will manually assign ourselves IP addresses on boot.
 - ▶ Also ensures IP consistency between boots
- ▶ We will also add some shortcut domains to `/etc/hosts` for ease
 - ▶ Those these will have to be disabled if we later want to test DNS poisoning

Network Config

- ▶ We'll use 192.168.64.0/8 for our network
 - ▶ 192.168.64.2 will be Metasploitable
 - ▶ 192.168.64.4 will be Ubuntu
 - ▶ 192.168.64.8 will be Kali

Setting IP on boot (Linux)

- ▶ `/etc/network/interfaces`
 - ▶ Or a file in:
`/etc/network/interfaces.d/`
- ▶ Configure the interface with a static IP address
- ▶ `ifup / ifdown` to turn an interface on or off
- ▶ ‘`man interfaces`’ for more information

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# eth0 static setup
auto eth0
iface eth0 inet static
    address 192.168.0.1
    network 192.168.0.0
    netmask 255.255.255.0
    broadcast 192.168.0.255

~
~
~
~
~
~
~
~
~
~
~
```

(END)

The background features a light gray gradient with two large, solid pink triangular shapes. One triangle is in the top-left corner, and the other is in the bottom-right corner, both pointing towards the center of the slide.

Other stuff you'll want

VirtualBox Guest Additions

- ▶ Resizable screen
- ▶ Shared folders
- ▶ Clipboard integration

- ▶ Don't bother installing on the metasploitable.



But I don't want to be a sysadmin...

I'm working on it

- ▶ A vagrant environment that will bring up all the required machines and configure them
- ▶ Ability to update and give you new demos with the 'git pull' of a repository
- ▶ Turns out trying to keep a VM isolated, but also updateable is hard