UFW - Special Cases

Purpose

This article is to help provide some basic knowledge and information on setting up ufw for the ubuntu based computers.

For the most part, most Linux flavor computers come with `iptables` as the firewall resource. `ufw` or Uncomplicated Firewall is the ubuntu equivalent, essentially it is `iptables` but simplified.

Ubuntu firewall by default is turned off and not configured

Requirements

You will need to have `sudo` or at least `root` privileges on the machine to execute `iptables`.

You should have console access to the machine in case you make a mistake with the firewall commands.

Special Cases

Ubuntu User Manual

Ubuntu: if you are installing it on mac hardware as well as a few other manufacturers, Ubuntu makes its user manual publicly available, and unfortunately world readable and writable at least in terms of some of the x frame options. that makes it vulnerable to click jacking. If you simply do not want to disable the Apache server or put a firewall rule in place to block off campus access, you will need to append the following line.

```bash
vim /etc/httpd/conf.d/security.conf

#append the following line:
Header always append X-Frame-Options DENY
```

Alternatively, there are a couple different ways to stop web servers, be aware that all commands do not work on all linux versions

```bash
sudo systemctl stop apache2.service
  or

sudo service apache2 stop
  or

sudo /etc/init.d/apache2 stop
  or

sudo update-rc.d apache2 disable
```
SSL enabled by installed software

Sometimes when you install software, said software turns on services for you, other times said software will try to communicate with the outside world, but not be programmed to use a specific protocol. We have had several cases where old software talks to the outside world, does not know which security protocol to use, and picks the first one on the available list, even if said protocol is normally unused due to being old and broken. Example: the Ubuntu user manual using the broken TLSV1.0 when it could be using the far more secure TLSv1.2. The below is adapted from https://www.digitalocean.com/community/tutorials/how-to-protect-your-server-against-the-poodle-sslv3-vulnerability

SSL protocols can appear in multiple config files, you will want to change each place it appears

in /etc/httpd/conf.d/ssl.conf (apache running the ubuntu user manual)

can also appear in

/etc/nginx/conf.d/ssfe.conf
/etc/nginx/nginx.conf
/etc/apache2/mods-available/ssl.conf

and several other location depending on what software you have on your computer

original version for ubuntu 14.04 LTS

SSLProtocol all -SSLv3

Edit it and change to:

SSLProtocol -all +TLSv1.1 +TLSv1.2

You may need to restart the computer, otherwise just restart the service

sudo service httpd restart

Related articles

Page: How to do X11 Forwarding on a Mac
Page: What is my College of Engineering Login?
Page: How to Password Protect a Web Page
Page: Security Checklist
Page: Securing Linux Computer