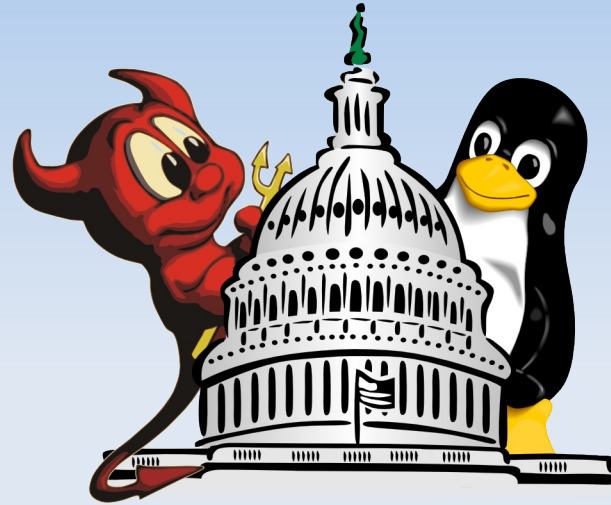


Networking and Security



GLLUG

**Greater Lansing
Linux Users Group**

Introduction

Introduction

- Summary: I'm boring

About this Class

- A brief (and boy do I mean *brief*) intro to networking and basic security concepts
- Meant as a starting point
- Follows the Ubuntu Server Guide:
<https://help.ubuntu.com/9.04/serverguide/C/index.html>
- For more info, RTFM

How the Internet Works

- Each computer has its own unique address
- Each computer talks directly to another
- Benefits:
 - Attack/Fault/Censorship Resistant
 - No central control (almost)
- Drawbacks:
 - Anyone can launch an attack against you
 - At least some knowledge necessary

TCP, UDP, and Ports

TCP vs UDP

- TCP: Connection-oriented
- UDP: Is not

Ports

- < 1024 : Privileged (root can open)
- ≥ 1024 Non-privileged (any user can open)

Addressing

- Public vs. Private Addressing
- Private Ranges:
 - 192.168.0.0 - 192.198.0.0 (65,536 addresses)
 - 172.16.0.0 - 172.31.255.255 (1,048,576 addresses)
 - 10.0.0.0 - 10.255.255.255 (16,777,216 addresses)
- Public Ranges:
 - (almost everything else)

Assignment

Static vs Dynamic

- Static IPs are configured manually
- Dynamic IPs are assigned automatically via DHCP

DNS

(the briefest primer you'll ever see)

- Send domain name, receive IP
 - Question: "Here's a hostname, what's the IP?"
 - Answer: (The IP)
- Cue cheesy phone book analogy

Ubuntu Network Configuration

- Dynamic (DHCP) configuration by default
- Set static IPs, netmask, gateway, nameservers

Network Time Protocol (NTP)

- Keep your server time accurate
- Easy to install and configure
- Helps with security analyses
- North American NTP Pool:
 - `server 0.north-america.pool.ntp.org`
 - `server 1.north-america.pool.ntp.org`
 - `server 2.north-america.pool.ntp.org`
 - `server 3.north-america.pool.ntp.org`

Network Security

(and other amusing oxymorons)

- Principles:
 - Constant balance between convenience and security
 - Expose only what you need to
 - Security is like an onion

Rule #1: Use the Firewall, Luke

- Cheap broadband router (w/ 3rd-party firmware)
- DIY:
 - pfSense
 - m0n0wall
 - IPCop
 - (other)
- A software firewall is better than nothing

Rule #2: Disable unnecessary services

- "sudo /etc/init.d/<service> stop"
- Make permanent: sysv-rc-conf
 - (or just uninstall)
- List open ports: "netstat -luntp"

Rule #3: Use Secure Passwords

- No empty passwords
- No dictionary words
- No patterns
- Nothing easily guessable
- Use different passwords for different accounts

Rule #4: Stay Patched

- "apt-get update && apt-get upgrade"
- Add a root alias to /etc/aliases
- Subscribe to ubuntu-security-announce
 - <https://lists.ubuntu.com/mailman/listinfo/ubuntu-security-announce>

Rule #5: Keep an Eye on Things

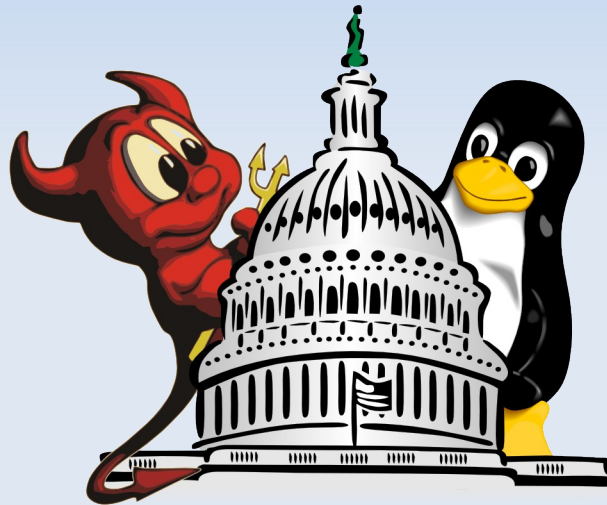
- Check logs
- Pay attention to last login
- System monitoring
 - logwatch
 - Nagios

Q&A

- What, you're still awake?

Join us!

- <http://www.gllug.org>



GLLUG

**Greater Lansing
Linux Users Group**