WITHYOU
WITHME

Linux Fundamentals – Part 5

Snooping the Network

Objective of today's byte

To explore networks using Linux

Networks are not just a means to transfer files from one computer to another or find cat pics on the internet, they can be a way to breach a network. The use of firewalls, switches, vlans and port closing can help protect you form being breached. Though this is a bit in depth for this week, we will start you on the way by learning how to view the networks around you.

The Why

To understand the network, we have to explore it.

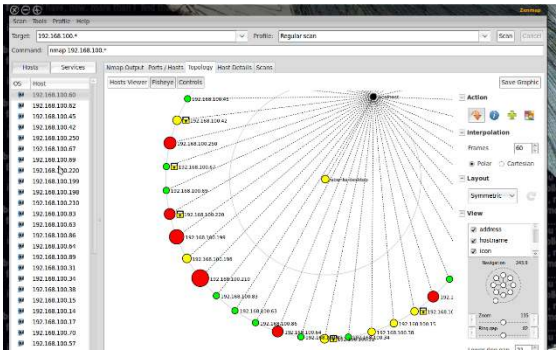
Basic commands

Network commands

Ifconfig	Short for "interface configuration", lets you know the configuration of your networking interfaces. Examples of this are your ethernet port, wireless dongle and and VPN tunnels you may have active
Ping x.x.x.x	A ping is a method used to receive a response from a specific ip address, It is used to determine whether the receiver is available or open to communication.
Ifup eth0 Ifdown eth0	This command enables or disables a network interface. Up to turn on, down to turn off
Nmap	Nmap is a powerful tool with many uses. For example determing if a computer is available and what ports are open or closed. It can also determine what services are in use. Use -h to see all available options In the example I used: Nmap -sn 192.168.1.0/24 • -sn – do not port scan • 192.168.1.0 – scan from 192.168.1.1 thru 192.168.1.255 • /24 only scan on port 24

Networking programs

Zenmap is a GUI version of nmap. It can be a little unstable, but as you see provides a great visualization of a network



Wireshark is a network information monitor. When a computer sends data on a network, it can sometimes be seen unencrypted. Wireshark can do many things, but if you are having network issues it can also be a great tool to help you diagnose faults.