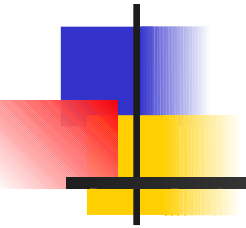
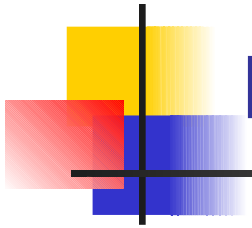


OPS235:

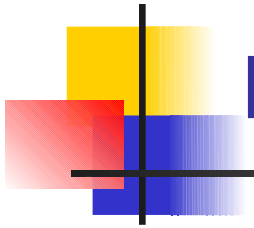
Configuring a Network Using Virtual Machines – Part 2



Lab 6 - Topics

Investigations 5 - 8

- Hostname Resolution
- Network Information Commands:
  - **Ifconfig**
  - **Route**
  - **arp**
  - **netstat**
- Securing Networks - **iptables**



Local Hostname Resolution

- As you may know, it is easier for humans to remember a series of words as opposed to an IP address.
- DNS (Domain Name System) uses a distributed data-base in order to act as translators of names to IP addresses to make it easier for Humans and computer processing.
- A similar technique can be used on a local-network basis. For example, accessing computer network by name as opposed to IP address.

Local Hostname Resolution

- List the steps to setup Local Hostname for all machines (including Vms) on your diskpack.
- What commands would be affected by the setup of Local Hostnames?

Networking Tools

Explain the purpose and uses for each of the following commands:

- **ifconfig**
- **route**
- **arp**
- **netstat**

Linux Firewall: iptables

There is an interesting connection between investigations 7 and 8 in lab6:

- *Investigation 7* teaches the **netstat** command to identify states and port information of running services.
- *Investigation 8* demonstrates the **control of services** (via a firewall). The netstat command can be used to prove how these services are affected.

Linux Firewall: iptables

- Various GUI applications can be used to manipulate the Linux system's, firewall policies, but we will learn how to perform this operation from using the command:

  iptables

- Therefore, we can learn the command to be proficient in both Graphical and Text-based Linux servers.

Linux Firewall: iptables

Iptables are a list of rules:

- These rules are placed into “chains” where data that is sent into, out of, or through the computer is compared against this chain (rules) to take action.

Linux Firewall: iptables

Ip chains consist of:

- **Filters** (*OUTPUT*, *INPUT*, *FORWARD*)
- **Conditions** (*ACCEPT*, *DROP*, *LOG*)
- **Options** (change policy, insert policy, list policies, reset to default, port number, protocols, etc)

Linux Firewall: iptables

Using iptables:

- How to display info? / reset to default?
- How to block incoming traffic?
- What is the standard port number for the World-Wide-Web?
- How to log outgoing traffic via the World Wide Web? Where to view logging information?