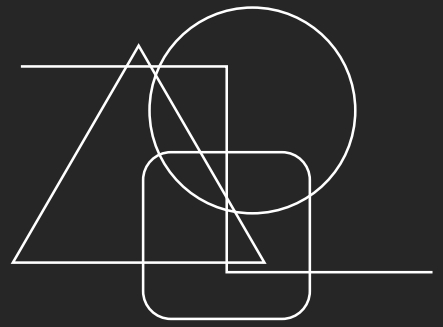
COSC 734
Lab Introduction

Instructor: Dr. Wei Yu
Lab Assistant: Weichao Gao
wgao3@students.towson.edu

Towson University



OUTLINE

- **Pre-built VMs**
- **Lab Instruction**
- **Lab Tasks**

Pre-Built VM

- The provided DVD contains pre-built Virtual Machine that can be copied to the host PC.
- Open the Virtual Machine:
  - Windows:

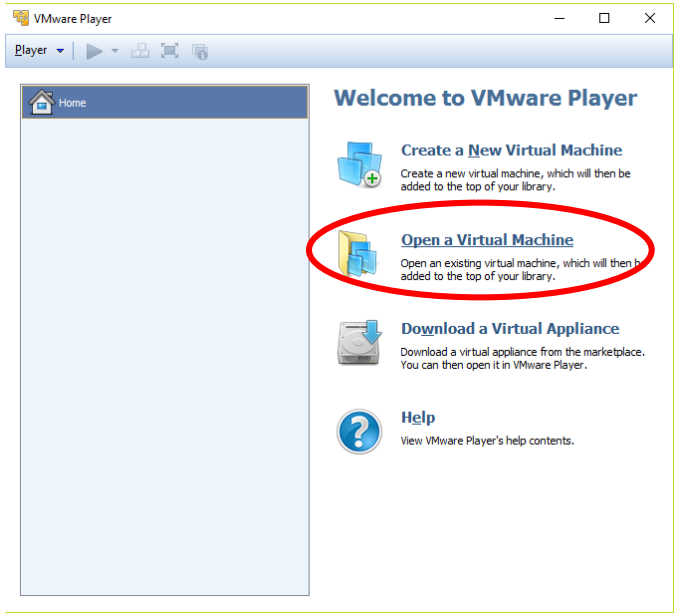
    VMware player

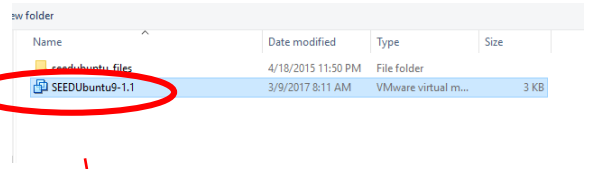
    http://www.vmware.com/products/player/
  - Mac, Linux:

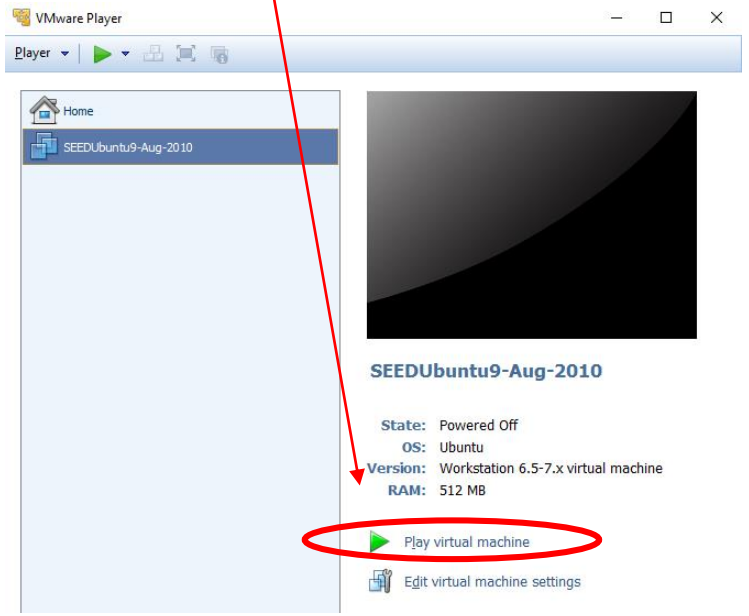
    Virtual box

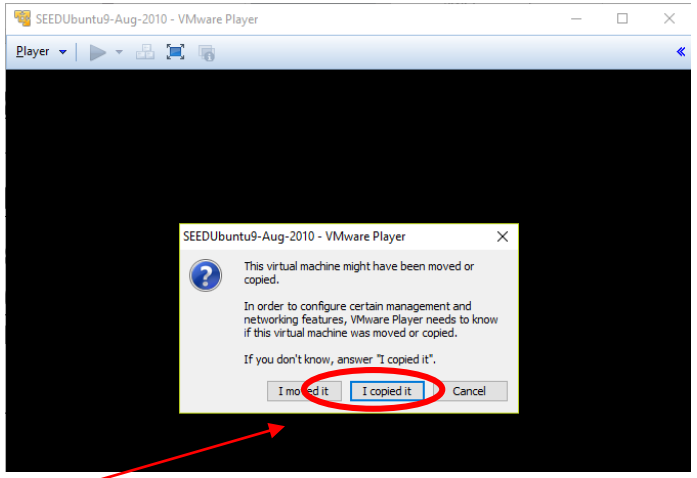
    https://www.virtualbox.org/wiki/Downloads

Pre-Built VM


VMware Player
Player
Home
Welcome to VMware Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Download a Virtual Appliance
Download a virtual appliance from the marketplace. You can then open it in VMware Player.
Help
View VMware Player's help contents.


Name
Date modified
Type
Size
SEEDUbuntu9-1.1
4/18/2015 11:50 PM
File folder
3/9/2017 8:11 AM
VMware virtual m...
3 KB


VMware Player
Player
Home
SEEDUbuntu9-Aug-2010
SEEDUbuntu9-Aug-2010
State: Powered Off
OS: Ubuntu
Version: Workstation 6.5-7.x virtual machine
RAM: 512 MB
Play virtual machine
Edit virtual machine settings


SEEDUbuntu9-Aug-2010 - VMware Player
Player
SEEDUbuntu9-Aug-2010 - VMware Player
This virtual machine might have been moved or copied.
In order to configure certain management and networking features, VMware Player needs to know if this virtual machine was moved or copied.
If you don't know, answer "I copied it".
I moved it
I copied it
Cancel

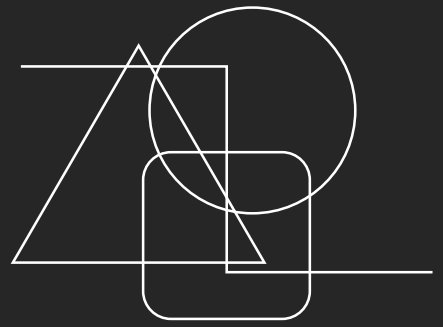
Login to the VM

Username: **seed**

Password: **dees**

Operating System for Labs

- Any version of Linux will be OK
  - I recommend **NOT** to apply the labs on your current daily use system.
- Ubuntu 9 has been installed in the pre-built VM



OUTLINE

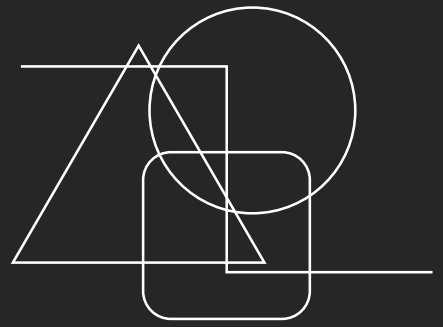
- Pre-built VMs
- Lab Instruction
- Lab Tasks

Tools

- Most of the network attack labs (including DNS attack, TCP/IP attack) need some special tools, so you can construct arbitrary packets.
- Here are the manuals of NETWOX, NETWIB, and NETWAG.
- Netwag is already installed in our pre-built Ubuntu VM image.

Knowledge needed

- Basic Linux Commands:
  cd, ls, cp, rm, mkdir, ssh, ping, etc.
- http://infohost.nmt.edu/tcc/help/unix/unix_cmd.html
- C Programming
- Basic Network knowledge



OUTLINE

- Pre-built VMs
- Lab Instruction
- **Lab Tasks**

Task1 : Packet Sniffing

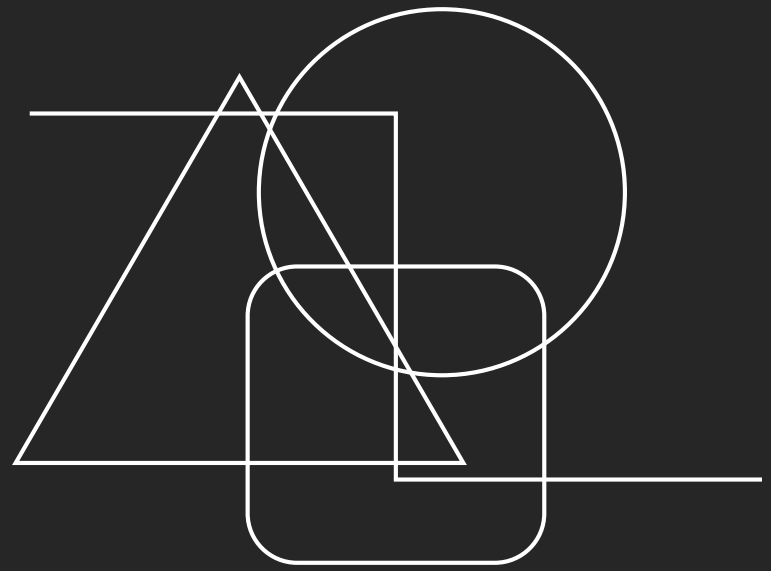
- Sniffer programs can be easily written using the pcap library. Tim Carstens has written a tutorial on how to use pcap library to write a sniffer program.
  - The tutorial is available at http://www.tcpdump.org/pcap.htm.
- In this task, you need to read the tutorial, play with the program sniffex included in the tutorial, read the source code sniffex.c, and solve several problems.
  - Understand the code
  - Make changes based on requirements

Task2:ARP cache poisoning

- Lab requirements:
  - Show the ARP table before attack
  - Show the ARP table after attack
  - Try the DoS attack if interesting (not required)

Hints

- The ARP cache poisoning is only successful when the IP entry already exists in victim's ARP catch. Otherwise the attack will not going to succeed.
- Attack tool to use: netwag 33
- If you want to conduct the DoS attack, you can use this tool: netwag 72
- To conduct this lab, you need to have at least 2 machines
  - Attacker
  - Victim
  - (You can make another copy of the pre-built VM and open 2 VMs)



THANK YOU