MEIC / MERC – IST Tagus
Network and Computer Security
2011/2012

Assignment 1
Implement and analyse a virtual computer network

Goals

- Implement and test a virtual computer network;
- Perform a TCP/IP packet analysis.

1 Introduction

Throughout this course, lab assignments make use of a computer network connecting several virtual machines. Virtualization is done through Microsoft's Virtual PC, while the virtual machines run Linux CaixaMágica.

This first assignment requires you to recall some basic networking concepts. The goal is to install the aforementioned computer network and monitor its TCP/IP activity.

2 Installing a virtual machine

The folder `C:\VM Magic Box SIRS` of each physical machine in the lab contains a virtual disk image, named `vm200708-base.vhd`, which is preconfigured with a Linux CaixaMágica operating system. This sections details the required steps to instantiate a virtual machine based on the given virtual hard disk image.

2.1 The host system

The host is the physical machine running the Virtual PC software. Every PC in the lab runs Windows XP and has Virtual PC already installed. All PC's are interconnected through a local network, with dynamically assigned ip addresses (172.20.34.**X**).

2.2 Creating a virtual machine

Create a virtual machine named **trab1-vm1** by executing the following steps:

1. Create a virtual disk:
    - Windows: **Start** → **All Programs** → **Microsoft Virtual PC**.
    - Virtual PC: **File** → **Virtual Disk Wizard**.
    - Disk Options: Select **create a new virtual disk**;
    - Virtual Disk Type: Select **A virtual hard disk**;

- Virtual hard disk location: Choose a name and location for your new virtual hard disk (ex. `My Virtual Machines\vm1\trab1-vm1.vhd`);
- Virtual Hard Disk Options: Since you will use a pre-existing image select the option **Differencing**;
- Differencing Virtual Hard Disk: Browse to and select the file **`C:\VM\vm200708-base.vhd.`**

2. Create a virtual machine:
   - Windows: **Start → All Programs → Microsoft Virtual PC**;
   - Virtual PC: **File → New Virtual Machine Wizard**;
   - Options: Select **Create a virtual machine**;
   - Virtual Machine Name and Location: Assign a name and location to your new virtual machine (ex. `My Virtual Machines\vm1\trab1-vm1.vmc`);
   - Operating System: Select **Other**;
   - Memory: Adjust the memory value to 64 MB;
   - Virtual Disk Options: Select **An existing virtual hard disk**;
   - Virtual Hard Disk Location: Browse to and select the VHD file created in step 2.2.1.

2.3 Configuring the virtual machine

The following steps will allow you to connect your virtual machine to the lab's local network:

1. *Hardware* configuration:
   - Virtual PC: Select the virtual machine created in step 2.2.2 and click on the **Settings** button;
   - Networking: Select the Intel network adapter in the drop-down menu from Adapter 1;
   - Notice that it is possible to add more network adapters to your virtual machine and close the settings panel by clicking **OK**.
2. Launch your virtual machine by clicking **Start**. Log in with the user *root* and the password *inseguro*;
3. Network configuration:
   a. *ip* configuration: the *ip* address for the virtual machine must be set to 172.20.34.(100+**X**), where **X** is the host's *ip* rightmost octet. For instance, if the host machine has the *ip* address 172.20.34.**4**, then the virtual machine will have an *ip* address of 172.20.34.10**4**. The *netmask* is 255.255.255.0;
      - Create a network interface configuration file named `/etc/sysconfig/network/ifcfg-eth0` and set the *ip* and *netmask* values. Delete any unnecessary files in that folder;

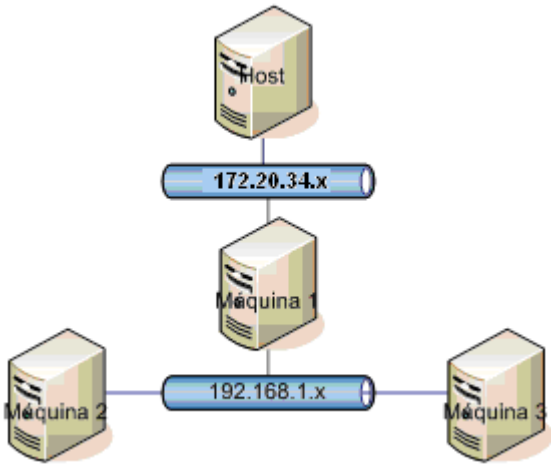
   b. *Gateway* configuration: Set the host's *ip* address as the *gateway*.
      - Update the file `/etc/sysconfig/network/routes` with a default gateway address for interface *eth*0 (**man route**). Delete the line with the *ip* address 192.168.0.0 since it is automatically added as the default network address for the interface *eth*0.

   - Execute **`/etc/init.d/network force-reload`** to reload the network interfaces;
   - Check the *ip* and routing table using the **ifconfig** and **route** commands.
4. Test the network configuration:
   - Use the **ping** command (man ping) to test the connection with the host machine;
   - Use the ping command in the host machine to test the connection with the virtual machine.

- Confirm that it is possible for the virtual machine to ping other PC's in the lab.

3 Create a virtual network

Implement the following virtual network by creating two additional virtual machines, as specified in step 2.2.



This network has two subnets:

- The subnet 172.20.34.X is the lab's local network, connecting the first virtual machine to all PC's in the lab;
- The subnet 192.168.1.X connects the three virtual machines. This second subnet requires the use of a loopback Network Adapter (e.g., Local).

3.1 Configuring machine 1

Notice that machine 1 has two network interfaces, one connected to the subnet 172.20.34.X and another one connected to the subnet 192.168.1.X. You will need to shut down this virtual machine in order to add a second Network Adapter through the Settings panel in Virtual PC.

Since machine 1 will be the default gateway for machines 2 and 3, *ip* forwarding must be enabled. This will allow machine 2 and 3 to communicate with machines outside the subnet 192.168.1.X.

- Open the file `/etc/sysconfig/sysctl` and set the `IP_FORWARD` value to `yes`;
- Load the configurations into the *kernel*:
  ```
  /etc/init.d/boot.ipconfig restart
  ```
- Confirm that the flag value was updated to **1**:
  ```
  sysctl net.ipv4.conf.all.forwarding
  ```

3.2 Configuring machines 2 and 3

Set machine 1 as the default gateway for both machines 2 and 3. Use the ping command to test the connectivity between **all virtual machines**, as well as **with the host system**.

3.3 Configuring machine 1 (NAT)

During the previous step, the connectivity test between machines 2 or 3 with the host system failed. Since NAT was not enabled in machine 1, the host sent the reply to its gateway, which eventually dropped the packet. Use the **iptables** command (man **iptables)** in machine 1 to correct this behaviour.

```
iptables –P FORWARD ACCEPT
iptables –F FORWARD

iptables –t nat -F
iptables –t nat –A POSTROUTING  –o eth0 –j MASQUERADE
```

4 Monitor network traffic

Use machine 3 to run **tcpdump** and capture all network traffic. Make sure you can detect ICMP packets originating at machine 1 and destined to machine 2 (using ping). Use tcpdump with options –X and –XX and identify the ip addresses, mac addresses and protocol in a given packet.

While still running tcpdump, open a telnet connection between machines 1 and 2 using user *fireman* and password "*inseguro*". Verify that you can capture both the username and password with tcpdump.