CMPUT 333, Assignment 2, Winter 2021

(non-sliding part - 75%)

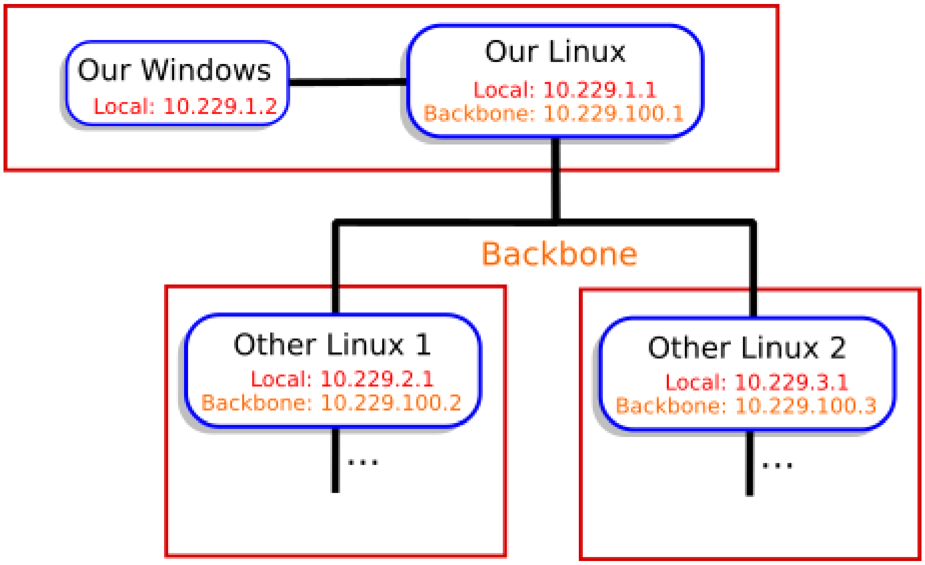
University of Alberta / Department of Computing Science

Instructor: Ioanis Nikolaidis (nikolaidis@ualberta.ca)

(firewalls, network services)

Network Layout

You will be given a set of virtual machines (VMs) that run in VirtualBox and have been configured to represent the following (networked) environment. *Supplemental installation documents for setting the VMs will be available in eclass and during lab sessions.*



Introduction

For this assignment we will be using the VMs to simulate a real network. You will be given access to two host VMs. One is running Windows Server 2016 and the other is running Arch Linux. We will refer to these two machines as the `Windows host` and `Linux host` (shown in the network layout above as `Our Windows` and `Our Linux`). Additionally, two "black box" VMs will also be provided. You can see these in the network layout above. They are named `Other Linux 1` and `Other Linux 2`. You will not be given credentials to log on to these two VMs but you must run them in order to test your firewall rules (see Part 3 below). They are self-sufficient and will periodically send requests to the various services you will be firewalling against in part 3.

All four of the VMs are connected together through two separate networks. One is the "local" network `10.229.1.0/24` and the other is the "backbone" network `10.229.100.0/24`. The former connects your two hosts, while the latter connects the Linux host with the two 'black box' machines.

Of note is that the Linux host needs to be behaving as a router for the Windows host to the rest of the network (the two black box machines). Instructions on how to connect to the Internet will be provided separately in subsequent VM-setup documentation. All of the VMs have been initialized with proper routing tables to allow communication with each other. You must not manipulate these tables directly.

Part 1 (10%)

Your first step to completing this assignment is to choose non-trivial root password for your `OurLinux` firewall host and non-trivial Administrator passwords for your `OurWindows` host. Use your experience from the previous assignment and the readings of this course to choose strong passwords.

Create one regular user account for each (Linux, Windows) system and associate it with a correspondingly difficult-to-guess password.

Your chosen passwords and the reasons you chose them are to be included in the deliverables of this assignment.

Default Passwords:

- Linux --> user: `root`, pass: `root`
- Windows --> user: `Administrator`, pass: `SomePassword9001`

Part 2 (25%)

In this task you will configure services from your two host VMs and make them available to each other and outsiders (the other two Linux VMs on the backbone network) in a manner which is controlled by your firewall host. In this part you may need to adjust your Windows firewall, e.g., to accommodate for general `http` and `ftp` traffic (client and server).

First, you need to install and/or configure adequate software to provide `http` services and anonymous `ftp` services from both your virtual Linux host and from your virtual Windows host. In doing so, make sure you satisfy the following requirements:

- Each `ftp` service should allow only "anonymous" access.
- Each `ftp` server should have at least one file of content available called `ftpcontent.pdf` at the top directory of the space accessed by `anonymous`.
- Each `http` server should allow content access only to the regular user account you introduced in Part 1 on the corresponding host. It should authenticate to `http` using the exact same password as the user's login.
- Each `http` server should have at least a single web page accessible as `webcontent.html` at the top level once the user is successfully authenticated.

Describe in your report how you performed the above steps. Steps should be described by listing, in the proper order, the commands you used (if you used a command line interface) and/or by providing screenshot sequences. Describe the differences between Linux and Windows on how you achieved the ability to authenticate the user account to allow `http` content access.

- Answer how do you ensure that if the user account changes their password, this change is automatically (without any additional manual overhead) reflected also in the password expected from the user when accessing the `http` service. What are similarities/differences in the two systems?

Part 3 (40%)

Your task is to introduce `iptables` firewall rules on your Linux host to enforce the following policies.

Inbound restrictions:

- Allow any host from the network `10.229.2.0/24` to access the `http` and `ftp` service of your Windows host EXCEPT for hosts from the network `10.229.3.0/24`.
- Allow any host from the network `10.229.3.0/24` to access the `http` and `ftp` service of your Linux host EXCEPT for hosts from the network `10.229.2.0/24`.
- Allow any host from any network to connect to the `ssh` service port on any of your group's hosts as well as allow `ICMP` echo messages (pings) from any host from any network.
- All hosts of your own group's internal network (`10.229.1.0/24`) should be allowed complete access to your group's hosts services.
- If none of the above rules apply, the default is to refuse all other inbound traffic (that is, unless the inbound traffic is caused by your own group's permitted outbound traffic).
- Add rules to log violations of the above rules.

Outbound restrictions:

- Prohibit your Windows host from accessing any services provided by the hosts on `10.229.2.0/24`. Note that we only want to block Windows from initiating a service on this network, but still allow machines on this network to use services on our Windows.
- Add rules to log any violations of the above restriction.

Deliverables are the `iptables` rules you used for the implementation of the above policies. You must put all of your rules in a shell script named "**create_iptables.sh**". I will run this script on my own VM in order to test your rules. Please provide comments (either in the shell script or in your report) that explain the rules you used and why you needed each rule.

Important: Your rules will be marked for their effectiveness, i.e., the least number of rules to achieve the exact desired effect. Rule correctness includes, for example, the ability to allow inbound traffic (as the reverse flow) for a connection that was allowed in the outbound direction, i.e., do not forget that TCP connections are bidirectional and also that some protocols like `ftp` can operate in either, so called, *passive* as well as in *active* mode. Describe the advantages and disadvantages of both ftp modes. Try to write rules to accommodate for both ftp modes, if possible.

Even though we do not talk about UDP services, they should be treated in a manner compatible with the spirit of the above rules. In presenting the rules you decided to use for UDP explain why you thought they are compatible with the provided policy.

Part 4 (25%)

Sliding component (due with Assignment 3) will be posted separately.

Deliverables

Only one of the group members need to submit on behalf of the entire group (in the event of more than one submission, the last one will be considered). Your report (in plaintext, markdown, or pdf format) should include answers to the questions posed in the specification and should cite any resources that you used to answer the questions. Your report should be accompanied by all relevant files, e.g., script for building your `iptables` rules. The solution you provide will be tested in the same VM environment that you have been provided for development. If there is a need to add/install software on the VMs to make your solution work, you need to provide the exact information so we can recreate your setup. By default it is assumed that all group members equally contribute to the assignment. If you need to deviate from this model of cooperation, explain why and indicate who was responsible for what.

(The sliding part (and the sliding part only) will be submitted separately by the deadline of Assignment 3. It is *not* due on the deadline of Assignment 2.)

Thursday, February 11, 2021