Project 1: Firewall and Access Control

Due Date: 10/2

A. Project Objectives

Security policy is critical to protect a computer system. In this project, you will
a) Learn to use networking and security devices and tools.
b) Learn to set up and configure networking systems.
c) Learn to implement security policy for networking systems.
d) Learn to analyze and verify the security of networking systems.

B. Project Tasks

The networking devices are assigned to fix groups.
Group B manages Computer A.B and the devices in Network B.
Group C manages Computer A.C and the devices in Network C.
Group D manages Computer A.D and the devices in Network D.
Group E manages Computer A.E and the devices in Network E.
Group F manages Computer A.F and the devices in Network F.
Group G manages Computer A.G and the devices in Network G.

The following project description applies to Group B. The project description for the other groups is similar to Group B's, except that their configurations are different.
Feel free to install any software, if needed. But, **before install any software, check if it is already in the computers.**

Please DO NOT change any settings in Router A, Z, and Switch A, Z.

Task I: Setup networks

Please check before setup. If the following step was completed by the other groups, you don't need to do again.

1) Check that the NICs of Computer A.B, B.1, and B.2 are configured according to Figure 1.
2) Check that the **web** services (Apache) in Computer B.2 and Computer A.B are started.
3) Check that the **ssh** services in Computer B.2 and Computer A.B are started.
4) Check that the firewalls (iptables) in all computers are stopped.

ifconfig

service sshd ... status
httpd ... stop
iptables ... start

5) Check that Wireshark and NMap are installed in B.1 and A.B.

Task II: Default Cisco firewall policy and exploit testing

Let Network B be the **internal network (172.20.*.*/16).**
Let Network A be the **external network (172.10.*.*/16).**

1) Open the Cisco Configuration Professional in WinXP VM in B.1 to configure the firewall in Router B.
2) Remove all removable firewall policy in the firewall. If the configuration tool prompts that a policy item cannot be removed, then leave the item as is.
3) Run NMap in Computer A.B to scan all computers and services in Network B. Record the identified computers and services.
4) Design experiments to check the default security configuration of the firewall. Record the results with Wireshark.
No credit will be given to the tests that were not conducted with Wireshark.

a) Check whether Computer B.1 can access the web service in Computer B.2.
b) Check whether Computer A can access the web service in Computer B.2.
c) Check whether Computer B.1 and B.2 can access the web service in Computer A.
d) Do the same check on the firewall regarding ICMP (ping) between the internal network and the outside network.

Task III: Implement security policy

Assume the internal network is owned by a company and is organized as follows.
a) The computers with the IP **172.20.100.*/24** are **internal servers** to provide services.
b) The other computers in the internal network **172.20.*.*/16** are **internal workstations** that are used by employees for working.

Every computer represents many computers

The company plans to deploy the following security policy.
a) Internal servers provide only web service to external computers.
b) Internal servers provide only SSH and web service to internal workstations.
c) Internal servers shall not access any service provided by any external computer.
d) Internal workstations shall not provide any service.
e) Internal workstations can access the services hosted by internal servers.
f) Internal workstations can access only the web service provided by external computers.
g) Internal computers can use ping to test the aliveness of any other computer.
h) External computers cannot ping to any internal computers.

As a network and security administrator, configure the Cisco firewall to enforce the security policy.
1) Make an access control matrix to represent the security policy. **The AC matrix shall not use single IP as a subject or an object.**
2) Configure the Cisco firewall according to your access control matrix to enforce the security policy. (Note that some items of the policy cannot or can only be partially enforced by the Cisco firewall.)

Task IV: Test the implementation of the security policy

Design experiments to verify whether the firewall configuration can enforce the security policy.
1) Run NMap in A.B to find all services and IPs of the internal network that are exposed to the external network.
2) Use Wireshark to illustrate your testing and analysis.

C. Project Report

How to Deliver

A group report is needed to show what you did in the project. Please clearly state your results of this project. You are expected to submit a report in the following formats:
a) Hard copies only.
b) A cover page with names of your group members with font size 12.
c) Single space and single column.
d) 5-15 pages (not including the cover page).

What to Deliver

Section I (Introduction):

Summarize what you have done in the project and clearly state the responsibility of each group member, e.g. who did which task, who wrote which part of the report, how your group was coordinated, etc.

purpose is to demonstrate responsibilities

Section II (Task II):

a) Show the NMap commands to scan the computers and the service ports.
b) Show the Wireshark results (screen shots) of checking the web service between computers.

State if web service is allowed between computers.
c) Show the Wireshark results (screen shots) of checking the ping between computers. State if ping is allowed between computers.
d) Summarize the default Cisco firewall policy.

Section III (Task III):

a) Copy and paste the access control matrix.
b) Find and explain which policy cannot be enforced by the Cisco firewall and which policy can only partially be enforced by the Cisco firewall.
c) Copy and paste a screen shot of your Cisco firewall configuration.
d) Discuss how to use iptables to enforce the security policy that is not implemented in the Cisco firewall.
e) Show the iptables commands in the internal server that enforce the security policy that is not implemented in the Cisco firewall.

Section IV (Task IV):

For the results, do not enable iptables. Only show the results with configured Cisco firewall.
a) Show the NMap results (screen shots) of the exposed computers and ports.
b) Show the Wireshark results (screen shots) of checking the web service between computers. State if web service is allowed between computers.
c) Show the Wireshark results (screen shots) of checking the ping between computers. State if ping is allowed between computers.
d) Assume the company only stores classified business data in Computer B.1, and does not allow anyone to carry a device to transfer data. Discuss whether or not the security policy can ensure that the classified data will not be disclosed to external computers through network. Be as specific as possible in your discussion. For example, if you do not think the security policy is secure, you shall show which item of the policy has problem or what policy is missing.

D. Grading Rubrics

If you do not contribute to the project, you get 0.

Group credits (70%).
1) Section I: Introduction (10%)
2) Section II: Task II (20%)
3) Section III: Task III (20%)
4) Section IV: Task IV (20%)

Individual credits (30%)

any, even subtasks

1) If you did some part of the tasks, you get 15. If you did nothing for the tasks, you get 0.
2) If you wrote some part of the report, you get 15. If you wrote nothing for the report, you get 0.
3) **If you only wrote some part of the report, you get 0.**

any part, one paragraph

Network Diagram