Project 1: Firewall and Access Control
C. Project Report
CS 4371
Dr. Gu
03/05/2019
Group 5

Abebe Aryam
Droddy Richard
Geng Rebecca
Rakhsha Hanna
Vielma Oswaldo

Section I (Introduction)

Our report on this project centers around setting up a firewall and access control in an operating system environment of linux. The group members listed above, all collaborated interchangeably on different tasks as well as writing up this report. To break down more specifically, for task I, Aryam worked on internal computer D1, Hanna worked on external computer AD and Richard worked on the second internal computer D2. On task II a, b and c, Hanna and Aryam worked on the external computer A.D while Oswaldo, Rebecca and Richard worked on the internal computers D1 and D2. On task III a, Aryam and Rebecca created rough drafts of the access control matrix and configured the router along with the rest of the group. On task III, part b Aryam and Richard modified the firewall to model our access matrix created for part a and with help from the rest of the group entered the ip table commands on computer D1 to specify rules that will be enforced by the kernel's netfilter framework. On task IV, Aryam worked on computer G.1, Richard worked on computer G.2, and Hanna worked on computer AG. Oswaldo and Rebecca also helped work on task IV.

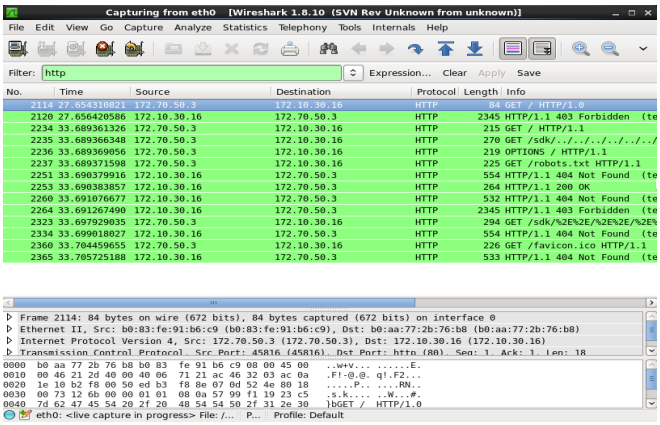
An objective for this project was to learn how networking, security devices, and tools operate by following procedures to set up and configure networking systems. Using resources within our group, course, and outside to implement security policies. Learning this material ultimately allowed us to analyze and check the security of the networking systems. For the paper, Aryam worked on the introduction, conclusion and explanations of task 2 part a, d, task 3 part b, d and e, task 4 part d. Rebecca worked on adding to task 3 part b, task 3 part c, the conclusion. Hanna worked on task 4 part b and c, as well as refined the other sections of the paper. Oswaldo added a part of task 2 part d regarding the cisco default firewall and a part of the conclusion. Richard worked on overall revisions, section 2 part b, c, and d, as well as making sure that all of the requirements from the rubric were met.

Section II (Task II)

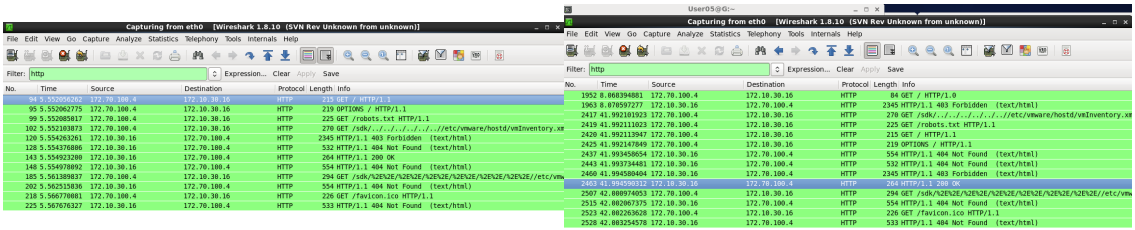
a) We used command "nmap -p- 10.0.4.1/16' to scan all the computers and service ports.

b) These Wireshark screenshots show us checking the web service between the computers. The web service between the computers was allowed. This is shown from the HTTP packets that were captured.

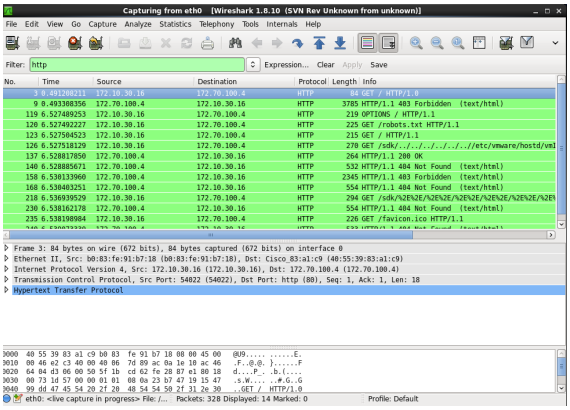
G.1



G.2

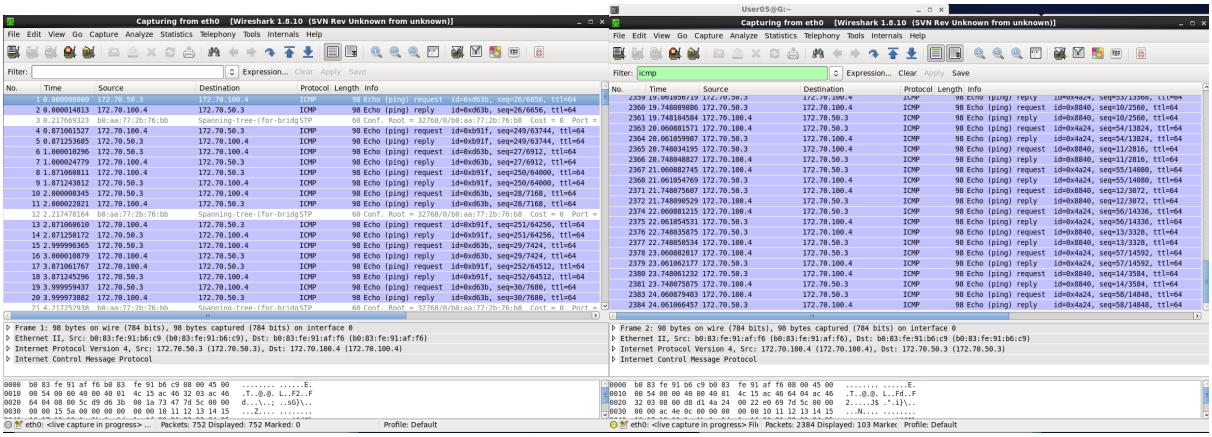


AG

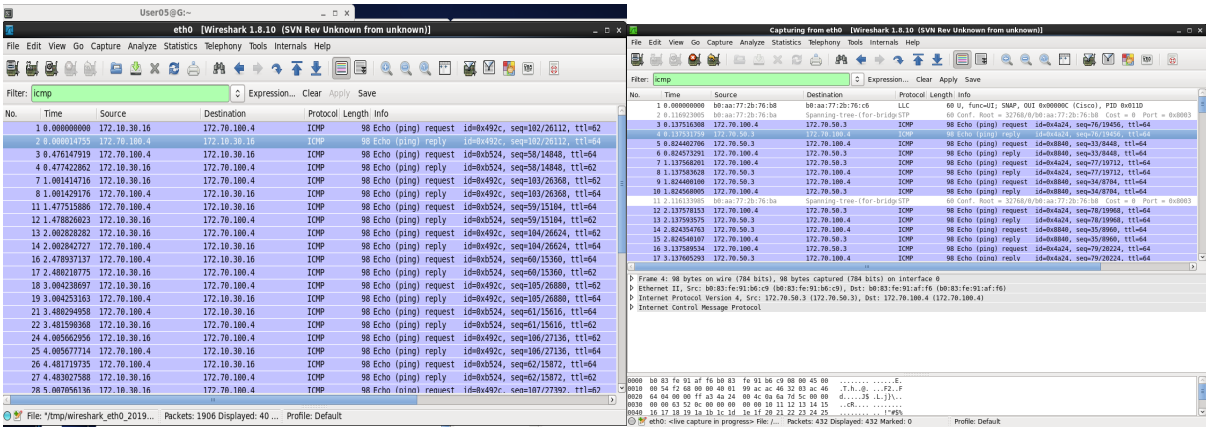


c) These Wireshark screenshots show us checking the ping service between computers. The computers were able to ping each other and this can be seen from the ICMP packets.

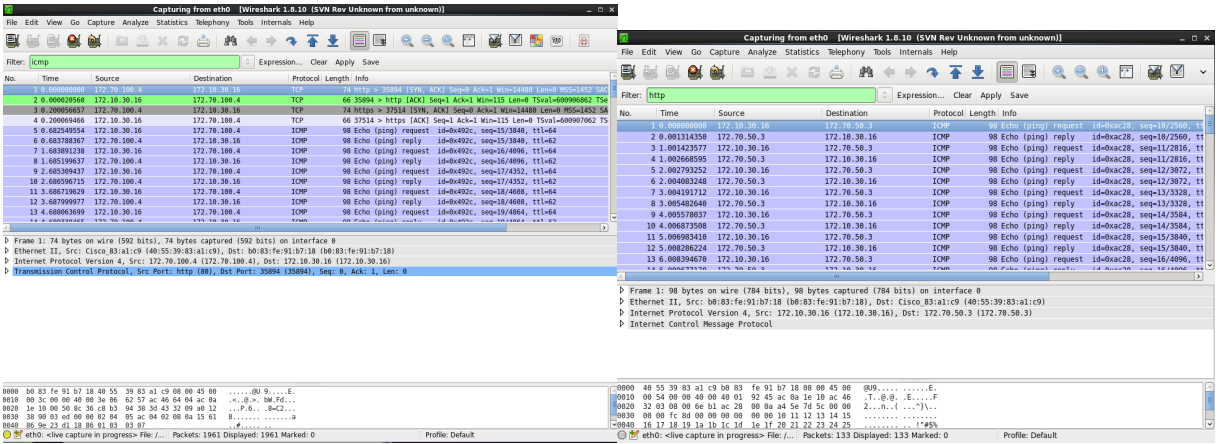
G.1



G.2



AG



d) Cisco firewall policy accepts communication between the internal and external computers automatically when using the “http” and “icmp” commands. By default, the Cisco firewall applies a list of default access, such as allowing DNS and HTTP traffic, and denying the private

IP address space. It was important to be mindful that there are also some configuration settings that may compromise router and network security enabled by default because they offer useful services (CDP for example, enables an administrator to easily view information about neighboring routers on the network).

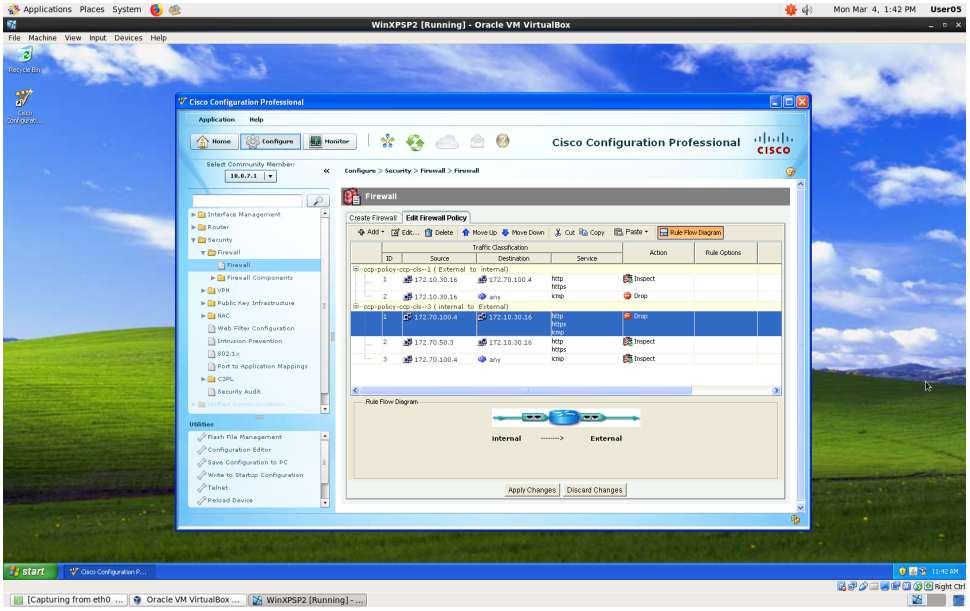
Section III (Task III):

a) Access Control Matrix

Subject, Object	Internal servers	Internal workstations	Internal computers	External Computers
Internal servers		d		c
Internal workstations	Ssh, http, b, e	d		http f
Internal computers	Ping g	d ping g	ping g	ping g
External Computers	http a	d	h	

b) Policies which cannot be enforced by the Cisco firewall are parts b, d, e and g. We used Cisco to enforce the policies for the router since the router connects the internal network and external network. These cannot be enforced because of the internal servers and workstations. The policy that can only partially be enforced by the Cisco firewall was part g and was produced by iptables. This policy permitted internal workstations to ping other computers as well as pinging internal/external computers in the firewall.

c) Below is the Cisco firewall configuration.



d) When using iptables, we noticed that partial policies are set by Cisco for internal and external while others were not. We had to change the default input chain from ‘ACCEPT’ to ‘DROP’ in

the workstation or internal server. This depends on what source and destination needed on varying policies. Following this, we use the iptable rules for varying policies and do this with commands.

Command one: ‘sudo iptables -P INPUT DROP’

Command two: ‘sudo iptables -A INPUT -p tcp -s 172.40.3/16 -d 172.40.100.4/24 -j e)

e.b) Internal servers giving only ssh and web service to internal workstations, iptable commands used in internal server D.2.

- sudo iptables -P INPUT DROP
- sudo iptables -A INPUT -p tcp -s 172.40.3/16 -d 172.40.100.4/24 -j ACCEPT

e.d) Internal workstations do not give any service. Iptable commands used in internal workstation D.1.

- sudo iptables -P INPUT DROP

e.e) Internal workstations can be granted serviced by internal servers. Iptable commands implements in internal workstation D.1.

- sudo iptables -A OUTPUT -p tcp -s 172.40.100.4/24 -d 172.40.50.3/16 -j ACCEPT

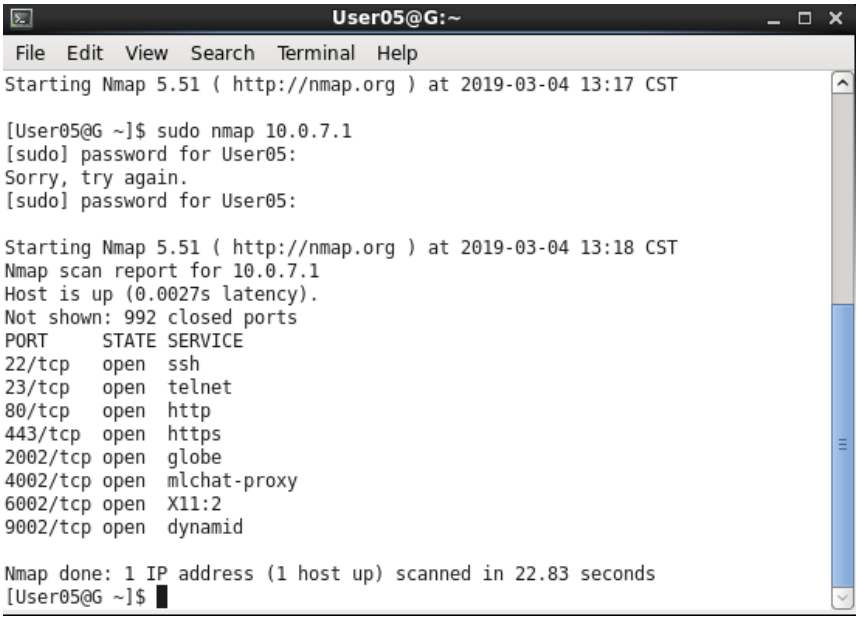
e.g) Internal computers can ping in order to test the active status of other computers. Iptable commands used in internal workstation.

- sudo iptables -A INPUT -p icmp -s 172.40.50.3/16 -d 172.40.50.3/16 -j ACCEPT
- sudo iptables -A OUTPUT -p icmp -s 172.40.50.3/16 -d 172.40.50.3/16 -j ACCEPT

Section IV (Task IV):

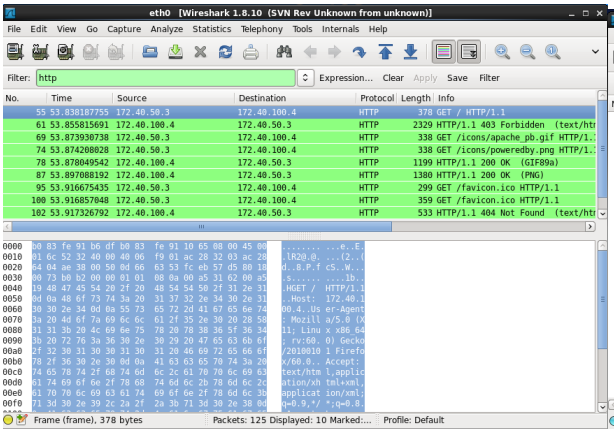
a) Below is the NMap results of the exposed computers and ports.

G.1

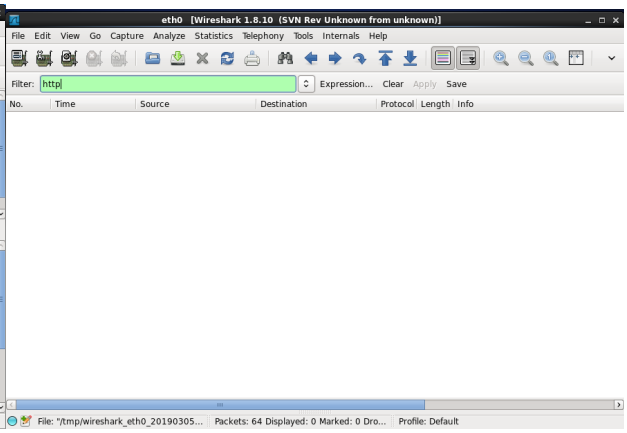


b) As seen below, in the Wireshark results, web service is allowed between computers D.1 and D.2. Web service is not allowed between A.D and D.1/D.2.

Web service D.1 to D.2

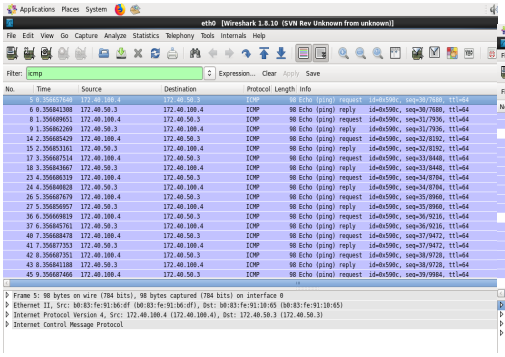


No web service A.D to D.1

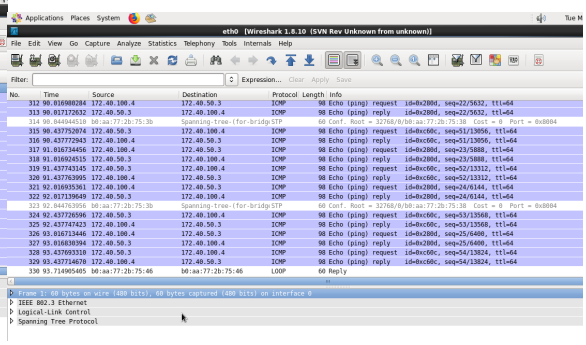


c) As seen below, in the Wireshark results, ping service is allowed between computers D.1 to A.D as well as D.2 to A.D, but not allowed between A.D to D.1 and A.D to D.2. Ping service is also allowed between D.1 and D.2.

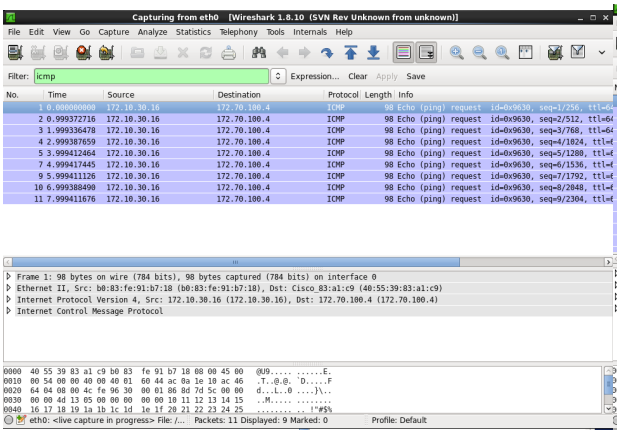
Ping D.2 to A.D



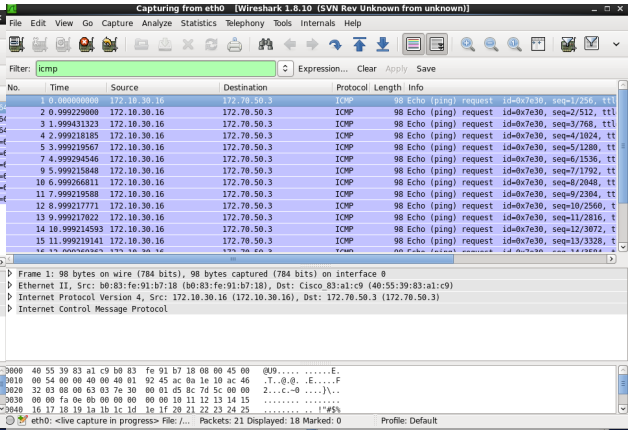
Ping D.2 to D.1



Ping not allowed AD to D2



Ping not allowed AD to D1



d) The business data would be secure in this policy. The data stored on internal workstations cannot be accessed since the internal workstation doesn't allow for any services for hosting, and anyone at the company with access to a workstation can only access web services by using an external computer. If anyone would want to transfer data, they would need to transfer using ssh.

Conclusion

In this project, we were able to learn how to manipulate and practice access control and how to configure the Cisco Configuration Professional in the Windows XP virtual machine. In task one, we learned how to check NICs of the three computers, web and ssh services. We learned how to check for connection of the internal servers and external servers by using the "ping" command. Task two, allowed us to work with Wireshark and NMap on a larger scale by scanning open ports and specifying the services running on those ports. In task three, we created an access control matrix and learned how to implement our ACM by configuring the Cisco firewall as well as determining which policies were not enforceable, using iptables to implement those policies. Finally, task four allowed us to test the security policies and verify whether they were successfully enforced.