

Assignment Policies:

- 1) No collaboration allowed
- 2) No extension allowed
- 3) Solutions should be submitted online in the Blackboard
 - a. Will not be accepted through email or any other form.

Due On:

10/20/09 5 PM

Questions (100 Points Total, 25 Points Each):

1. Using Fermat's theorem find the multiplicative inverse of 7 in the field of integers mod 53.
2. Show that in DES, if K is key, X is the input, and Y is the output and X' is X complement then,
 - a. $E(K,X) = Y \Rightarrow E(K',X') = Y'$
3. Perform Differential cryptanalysis of the first Sbox of DES (S_1)
 - a. Show the differential table
 - b. Find the differential pair that has the highest probability
4. Write IP table firewall rules for a server (example1.syslab.unt.edu) which conforms to the following 4 rules:
You should be able to connect to the server over SSH (which uses TCP port 22) only when,
 1. You connect from a specific IP address (example2.syslab.unt.edu).
 2. You connect as the system administrator (when you log in as root)
 3. Any outgoing traffic from the server should work
 4. Anything other than the above traffic is not allowed

This means that:

- You should NOT be able to SSH to the server if you are connecting from example2.syslab.unt.priv with any other user id other than root.
- You should NOT be able to SSH to the server if you are connecting from any other machine in the internet.

You can use "iptables" (the standard Linux firewall) on the firewall machine (desk1.syslab.unt.edu) in order to set firewall rules, and you need to be logged in as root in order to access and change firewall settings.

First, check to make sure you are starting with a clean firewall configuration using the command "iptables -L -n". You should see output that looks something like this:

```
[root@desk1 ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

Notice that all policies are set to "ACCEPT" and there are no rules. If this is not what the iptables command says, you can clear it to this state with the command "service iptables stop" (when logged in as root).

A firewall "chain" is basically a set of conditions that are matched against packets, and when a match is found the rule says what action to take, e.g. accept the packet, drop the packet, log the packet, etc. If none of the rules match the packet, then the chain's policy is applied. The previous example showed no rules and a policy of "ACCEPT" on each chain, so basically everything was allowed. In this assignment you are to set up the "FORWARD" chain, which applies to all packets that are being forwarded from one subnet to another

("INPUT" and "OUTPUT" refer to packets sent to or from this machine, respectively). Since our network policy will be to drop all packets that aren't specifically allowed, the FORWARD policy should be set to DROP with the following command:

```
iptables -P FORWARD DROP
```

IMPORTANT!!: You need to save your firewall configuration settings so as to submit them and in case you need to restore them. You can dump the current firewall configuration to a file using the command `iptables-save`, and redirecting the output to a file. Since all of you will be using the same firewall machine, all logged in a root, you need save your files as such: "**username-rules.txt**". You may use this command to save your firewall configuration:

```
iptables-save >yourusername-rules.txt
```

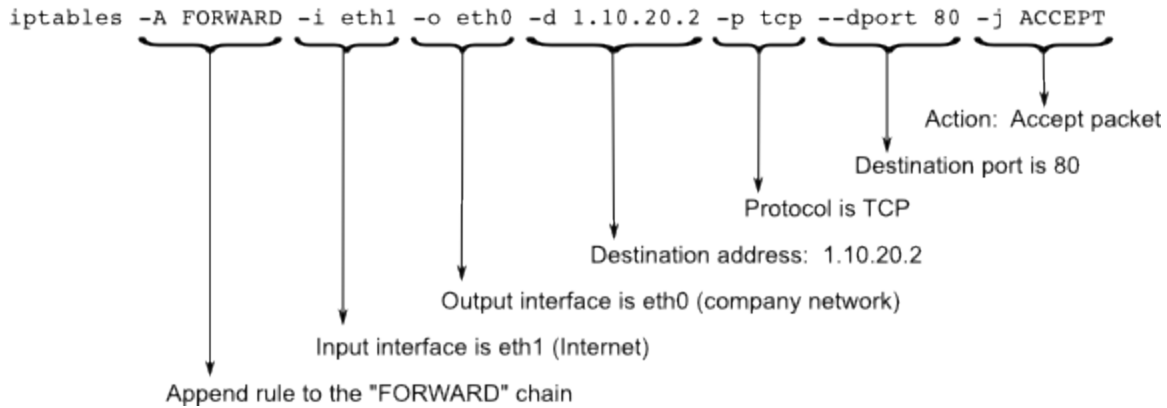
Naming your configuration files correctly is very important. This is the only way that we can differentiate your works. So, please pay extra attention to that.

In case needed, you can restore your settings using the command:

```
iptables-restore <yourusername-rules.txt
```

Remember to save your settings and then do "service iptables stop" when you finish using the machine so that you've saved your settings and left the machine in a clean state for the next person. You should also try to remember to copy your firewall rules to your own personal account (you can use `scp`) and delete the file from the root account. You should also ignore any files that others may have forgotten and left in the root account. Please be honest to yourself and do not attempt to check other students' rules.

You add rules using the `iptables` command, just like you used to set the policy -- you tell `iptables` what chain to add your rule to, what needs to match for this rule, and then what to do with the packet. Below is a firewall rule with its explanation:



Note that this rule only allows web traffic to enter the business network (the IP address also needs to be changed). To learn more about options to rules, look in the iptables man page, please pay particular attention to the "--state" rule. This (in addition to some other things) is what makes iptables a stateful firewall, rather than a simple packet filter (which is what its predecessor, called ipchains, was).

Using iptables, you define correct rules to implement the business policy rules 1 through 4 described at the beginning of this assignment.

Now you need to verify your configuration. Configuring a firewall is sometimes fairly subtle, and a main goal of this assignment is to make you aware of these issues -- while the assignment looks straightforward enough, don't expect it to work the first time. Also note that when you do "iptables -L -n -v" it will give you counts of how many times each rule has matched -- that way you can see what rules are actually "firing" and which aren't.

Do an nmap scan (TCP) of the server from any of the other machines (please save the results to turn in). Then try to use ssh to log in to each machine from any of the other machines.

Finally, check the configuration from inside the network.