CSCI 530 - Lab-6

Rishit Saiya (rsaiya@usc.edu)

1. Optimistic stance by definition states that it allows data that is not perspicuously prohibited. By default configurations, the firewall is open and applies only certain closures based on rule sets (policies that might be set). However, in a Pessimistic stance, by default configurations, most of the settings are blocked to data unless explicitly mentioned to allow in accordance with the policy. For the asked statement, Windows XP's incoming stance is Pessimistic in nature because by default it doesn't allow anything in. In addition, it doesn't possess the capability to block outbound connections.

2.

a. In this script, firstly existing rules and tables have been discarded. A new table is created with three different chains for the purpose of incoming, outgoing and forwarding with a pessimistic stance. Additionally, other rules have been added to allow HTTP (web traffic) and DNS for internal nodes of a network. The details for the same are below:

First Section:

```
nft flush ruleset
```

This rule is set to flush/discard existing chains/rules/tables.

Second Section: (Related to nft add table ip mytable)

A table is created and is populated with three chains as mentioned above. The first one is for input (incoming), second one is for output (outgoing) and third one is for forwarding. All these chains represent Pessimistic stance where everything is blocked by default until explicitly is permitted.

Third Section: (First Service)

Rules have been added to communicate with the DNS traffic. The first rule allows DNS traffic which is destined to all nodes in a network with destination port 53 (UDP protocol is used) and the second rule permits incoming DNS traffic from all nodes in a network with source port 53 (UDP protocol is used).

Fourth Section: (Second service)

Rules have been added to communicate with web traffic (HTTP traffic). First rule allows http traffic which is destined to all nodes in a network with destination port 80 (TCP protocol is used) and second rule permits incoming http traffic from all nodes in a network with source port 80 (TCP protocol is used).

b. Lines 10 and 11 are related to DNS traffic. Whenever a user wants to access any domain/website, the request first goes to the DNS server for fetching the corresponding IP address of the website. Thereafter, that request goes to the web server to fetch the particular website and finally the response from that website & communication takes place. So if line 10

and 11 are removed, which essentially are in place for enabling communication with the DNS server, the user's request will not reach a server to translate the website into the corresponding IP address and hence no communication will take place with websites.

c. Lines 15 and 16 are apropos of HTTP traffic (web traffic). If a user wants to access a website, Port 80 (HTTP) must be opened, else the communication does not take place. If these rules get removed, users would not be able to access the website. Traffic to and from the website and user machine will be blocked.

3.

a. The object is to run a web server on our XP box. It will require internet connection. If any user from the outside world wants to access the web server, traffic should be allowed to pass through the router. In the router (Netgear WGR614), by default, those on an outside network (internet network) can send nothing into systems inside the internal network. But the router can create firewall rules that will allow systems from outside the network to Windows XP, web server (that is inside the network). Through the technique of Port Forwarding, routers can enable systems from outside the network to reach the web server on our Windows XP box (provided Windows XP box doesn't block the connection).
Windows XP also has a firewall that has an input chain. It deals with incoming requests. So once a router allows traffic to reach Windows XP, it will have an option to accept it or discard it through firewall rules. Windows XP has to adjust rules for accepting the traffic. Hence firewall adjustment should be done on both Router as well as Windows XP.

b. By default Windows XP can send anything out to an outside network. To enforce restriction, rule sets need to be implemented on the router through menu option security and submenu option Filter. That will disable insiders reaching the outside world. So firewall changes will be required on the Router. Windows XP box can prohibit/allow incoming connection from different systems however it will not be useful to prevent outgoing connection that stems from Windows XP machine. So if we want to prevent the XP box from conversing with the internet using certain protocols, either (Router or Windows XP) will do the job (From incoming connection perspective). If we talk from the perspective of outbound connection, then changes need to be done on Router as windows XP doesn't have capability to block outbound connection.

4. If all connections from ports/interface (1 WAN and 4 LAN) are considered, the total computer connections will be like as below:

WAN to LAN1, WAN to LAN2, WAN to LAN 3 and WAN to LAN4
LAN 1 to LAN2, LAN 2 to LAN3, LAN 3 to LAN 4 and likewise so on:

So mathematically, this can be easily calculated as $5C2/2 = 5!/(2! * 3!)*2 = 5$. Therefore, $n = 5$.