CSCI 530: Security Systems
Lab 6: Firewalls; Submission Due: November 8th, 2024
Name: Anne Sai Venkata Naga Saketh
USC Email: annes@usc.edu
USC ID: 3725520208

Question 1:
Windows XP's firewall by default lets nothing in and everything out. Comment on whether we should consider this an "optimistic" or "pessimistic" stance?
Answer: The Windows XP's firewall rules may be treated as a pessimistic stance for incoming traffic, as it blocks all unwanted traffic by default. This "default deny" method aligns with the security idea of restricting any exposure to outside threats. This pessimistic coverage assumes that any incoming traffic/connections will be a threat, prioritizing protection by way of refusing access to probably dangerous traffic instead of assuming it is honest.

On the other hand, the firewall adopts an optimistic stance for outgoing traffic, allowing all internal programs to connect freely to external servers. This policy assumes that all internal processes are secure, which may additionally result in vulnerabilities if malware applications are already on the system that have a free hand at transmitting data. Therefore, whilst the firewall is "pessimistic" regarding incoming traffic, it's far greater "optimistic" about internal programs in terms of outbound connections.

Question 2:
Here is a script that sets up a firewall.

```
1 # flush existing rules and tables
2 nft flush ruleset
3
4 nft add table ip mytable
5 nft 'add chain ip mytable myinputchain { type filter hook input priority 1; policy drop; }'
6 nft 'add chain ip mytable myoutputchain { type filter hook output priority 1; policy drop; }'
7 nft 'add chain ip mytable myforwardchain { type filter hook forward priority 1; policy drop;
}'
8
9 ########## first service ##########
10 nft add rule mytable myoutputchain udp dport 53 ip daddr 0.0.0.0/0 accept
11 nft add rule mytable myinputchain udp sport 53 ip saddr 0.0.0.0/0 accept
12
13
14 ########## second service ##########
15 nft add rule mytable myoutputchain tcp dport 80 ip daddr 0.0.0.0/0 accept
16 nft add rule mytable myinputchain tcp sport 80 ip saddr 0.0.0.0/0 accept
```

a. briefly state in declarative English what the script above expresses in nftables syntax. Include mention of the effects of each of its four main sections, in terms of resulting behavior. For example, the first main section discards existing tables/chains/rules. (Look up the port numbers found in the script if you don't recognize them.)

Answer:

In Lines 1-2, it Flushes all existing firewall tables, chains, and rules. Basically, it clears any previous configurations that were set.

In Lines 4–7, table named mytable is created in nftables under IPv4 address family. Line 5 creates a chain called myinputchain commands in mytable that is set up to deny all unwanted incoming traffic by dropping all incoming packets by default. In line 6, myoutputchain triggers a chain of commands in mytable blocking all outgoing traffic that isn't specifically permitted by other rules. Line 7 creates a chain of myforwardchain commands to restrict any forwarding traffic through the system.

In Lines 10–11, on executing Line 10 permits outbound DNS requests (UDP on port 53) to any destination in myoutputchain. While Line 11 permits receiving DNS responses (UDP on port 53) from any source in myinputchain.

In Lines 15–16, on executing Line 15 it configures myoutputchain to allow outgoing HTTP requests (TCP traffic on port 80) to any destination in myoutputchain, and Line 16 permits incoming HTTP responses (TCP traffic on port 80) from any source in myinputchain.

b. for different reasons, removal of either lines 10 and 11, or else lines 15 and 16, will obstruct the primary behavior otherwise possible under this firewall. What's the reason when lines 10 and 11 are removed?

Answer: In the firewall rules, removing Lines 10 and 11 will stop DNS Traffic (UDP traffic on port 53) from entering and leaving the system. Blocking this traffic will prevent the system from using domain names to access the internet because DNS is necessary for translating domain names to IP addresses. The server/computer will therefore be unable to access websites or other resources by their domain names in the absence of DNS resolution, significantly limiting internet reach.

c. what's the reason when lines 15 and 16 are removed?

Answer: In the firewall rules, removing Lines 15 and 16 will stop HTTP Traffic (TCP traffic on port 80) from entering and leaving the system. Blocking this traffic will prevent the system from transmitting web pages. Removing these lines will lead the system unable to access web pages.

Question 3:

You have a home LAN containing 2 computers. The first computer is a general purpose PC running Windows XP. The second computer is a typical commercial router, perhaps a Netgear WGR614. The router, in addition to being on the LAN, is on the internet (it has 2 NICs).

a. You want to run a web server on your XP box. To enable, do you need to make the firewall adjustment on the router, XP, or both?

Answer: Both the router and the XP system must have their firewalls adjusted to run a web server on the XP box. For the web server to react to requests, we must set up the XP firewall to let incoming HTTP traffic, which is normally on port 80. To enable external HTTP traffic from the internet to reach the XP computer on the LAN, changes must also be made to the router's firewall. This can entail configuring port forwarding on the router to forward inbound port 80 traffic to the IP address of the Windows XP computer on the LAN.

b. You want to prevent the XP box from conversing with the internet using certain protocols. To do it, do you need to make the corresponding firewall adjustment on the router, XP, or both?

Answer: Only the XP system needs to be modified to stop the XP box from using certain protocols to communicate with the internet. This is because the restriction is only meant for the XP box and is not necessary for other devices in the network. By setting up the firewall on Windows XP, we can restrict specific protocols (like FTP or SMTP) without compromising the internet access.