Firewalls (IPTABLES)

Objectives

1. Understand the technical essentials of firewalls.
2. Realize the limitations and capabilities of firewalls.
3. To be familiar with iptables firewall.

Introduction:

In the context of buildings, a firewall is a fireproof wall intended to prevent the spread of fire from one room or area of a building to another. It has acquired a related but an outside-to-inside attack prevention meaning in the context of the Internet. A typical intranet these days is not connected to the Internet directly. Instead, we connect it to a firewall, and channel all transmissions through the firewall.

Firewall Characteristics and goals

- All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.
- The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

General techniques that firewalls use to control access:

- **Service control:** Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address and TCP port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.
- **Direction control:** Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
- **User control:** Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as is provided in IPSec (lab 9).

- **Behavior control:** Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

**Limitation and capabilities of firewall:**

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network.
2. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.
3. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator (NAT), which maps local addresses to Internet addresses.
4. A firewall can serve as the platform for IPSec.

**Firewalls have their limitations, including the following:**

1. The firewall cannot protect against attacks that bypass the firewall.
2. The firewall does not protect against internal threats, such as a disgruntled employee or a employee who unwittingly cooperates with an external attacker.
3. The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.
**Types of Firewalls**

1- **Packet-Filtering Router**

A packet-filtering router shown in figure 1-a applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. The router is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet: **Source IP address, Destination IP address, Source and destination transport-level address**
port number (which defines applications such as SNMP or TELNET), IP protocol field, Interface.

One advantage of a packet-filtering router is its simplicity. One advantage of a packet-filtering router is its simplicity. Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions. Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited. Most packet filter firewalls do not support advanced user authentication schemes.

Here are some examples for packet filtering:

1. Block all incoming connections from systems outside the internal network, except for incoming SMTP connections (so that you can receive email).
2. Block all connections to or from certain systems you distrust.
3. Allow email and FTP services, but block dangerous services like TFTP, the X Window System, RPC, and the "r" services (rlogin, rsh, rcp, etc.).

2- **Application-Level Gateway**

An application-level gateway, also called a proxy server, acts as a relay of application-level traffic (Figure 1-b). The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall. Further, the gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denying all other features.

3- **Circuit-Level Gateway**

A third type of firewall is the circuit-level gateway (Figure 1-c). This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications. A circuit-level gateway does not permit an end-to-end TCP connection;
rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.

**Whether a connection is valid may be based on:**
- destination IP address and/or port
- source IP address and/or port
- time of day
- protocol
- user
- password

A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections. In this configuration, the gateway can incur the processing overhead of examining incoming application data for forbidden functions but does not incur that overhead on outgoing data.
Lab Experiment

Requirements:
We need two PCs for this experiment, one Linux machine (this lab applied for backtrack Linux and small changes may needed for other Linux distributions), and the other that runs Windows XP.

1. First let us know about common switches used with ip tables, use `iptables -h`.
2. To list the rules in all chains use `iptables -L`. Figure 3 shows chain contents before adding any rule.
3. Now we want to add rule to input chain, type `iptables -A INPUT -i lo -j ACCEPT`.
   This rule add accept rule to all packets come through loopback interface; to test this rule let us ping localhost.
   
   *Remember that ping is echo request (output from my PC) and echo replay (input to my PC). So we can test our input and output rule using ping command for simplicity.*

4. Try to ping localhost, then type `iptables -L -v` to view the statistics of each rule in each chain. Figure 4 shows the statistics related to the rule we add in input cahin.

5. Now add accept rule for all packets to output chain `iptables -A OUTPUT -o lo -j ACCEPT`.

6. Try to ping localhost then the result is shown in figure, notice that packets is pass through input and output chains so statistics of the two chains will increase. As shown in figure 5.
7. Now, to test drop action, add the following line
   
   `iptables -A INPUT -i lo -j DROP` and try ping command.
   
   This line will drop all packets that want to input from loopback interface.

   **Note that**: after this dropping rule added each thing is still as default; browse input chain rules, you will find two rules one that allow everything and the second to drop everything; the first match rule is applied so only accept rule will matched here. So we must first delete accept rule that come before drop rule in the chain.

8. To delete the old rule type the same rule but with `-D` switch, as follows

   `iptables -D INPUT -i lo -j ACCEPT`

9. ping to localhost and check the statistics using `iptables -L -v` the counter for the drop packet counts up and ping is still working why?
   
   Because our rule only drop incoming packets through loopback that only echo reply will dropped.
   
   The result illustrated in figure 6.

10. Now delete the accept rule from OUTPUT rule use

    `iptables -D OUTPUT -o lo -j ACCEPT` and add

    `iptables -A OUTPUT -o lo -j DROP`

    now try ping command , the result no packet send (echo request packets will dropped ). As shown by figure 7 the result is denying output packets and drop it.
11. Now the same command we can use with any interface, the following line will drop all packets that come to any interface from the source address 192.168.1.3:

```
iptables -A INPUT -s 192.168.1.3 -j DROP
```

Figures 8 and 9 shows pinging process from this ip and it will faced by Request time out because of its packet dropped and no returned result, other figure shows statistics that matches this dropping rule.

12. Another example that figure 10 show its result, that specify the denied traffic for that come from eth0 from TCP protocol and specific port 80.

To test this rule open any website, there is no response.

```
iptables -A OUTPUT -o eth0 -p TCP --dport 80 -j DROP
```
13. If no matching rule exists in iptable rules iptables, policy of the chain will be applied to all unmatched; it is by default ACCEPT, type to change this policy to DROP everything:

```
Iptables --policy INPUT DROP
```

For more about iptables review the powerpoint slides on the site.
Exercise:

1. Test iptables firewall using backtrack, do three different simple scenarios in your report.

2. Demilitarized Zone (DMZ) is a neutral zone between the private LAN and the public Internet. FTP servers, Web servers and the like are located in DMZ. How to design our network with DMZ? Provide simple figure for your answer.