Firewall Simulation

COMP620

Hands-On Activity

- On Friday, February 26, we will be meeting in the Graham 212 lab to participate in a firewall configuration simulation.
- This simulator was written by Dr. Williams with help from several A&T students for an NSF funded workshop

Firewall Simulation

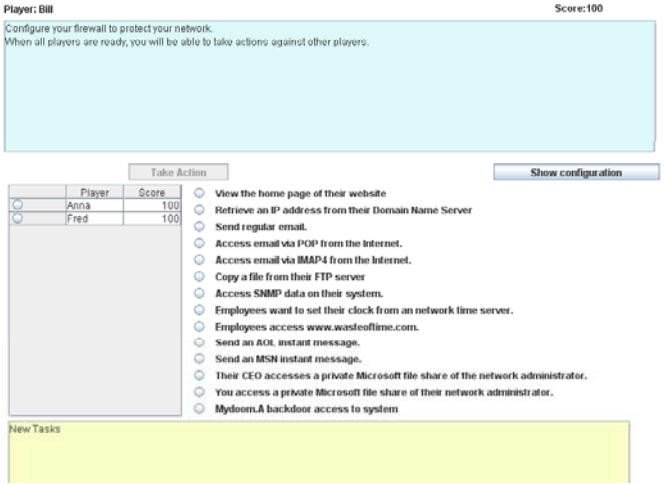
- The simulation allows participants to configure their own simulated firewalls using Cisco-like syntax.
- Participants can take benign or malicious actions against other players to score points.
- The interactive and competitive nature of the simulation helps students learn about firewalls while having fun.

Simulated Network

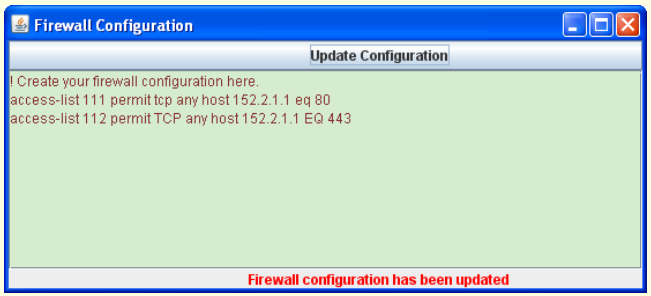
- During the simulation you assume the role of network administrator and are required to configure your firewall to protect your network
- You can also "*attack*" the simulated networks of other students. If you are successful, you will earn points and the other student will lose points.
- During the simulation the security requirements will change requiring you to change your firewall's configuration.

Real World Security

- The firewall simulator is a Java applet that runs in a browser and communicates with a server program
- The applet is signed using a self generated certificate. Your browser will warn you about the evil “Ken Williams”.
- The Windows firewall may complain about using UDP port 49,876 although it seems to work.



Firewall Configuration Window



Simulation Process

- When you first start, you must enter your name to identify yourself to other participants.
- Configure your firewall to allow needed services while preventing attacks.
- Once the actions are enabled, you can take actions against other players.
- Reconfigure your firewall whenever necessary to correct problems.
- New tasks will appear that may require you to reconfigure your firewall.

Cisco-Like Configuration Syntax

access-list number {**permit** | **deny**}
[protocol]
{**any** | ipaddr mask | **host** ipaddr}
{**any** | ipaddr mask | **host** ipaddr}
[operator port | **established**] [**log**]

- *The entire access-list command must be written on one line.*

Address Formats

- You can specify a source or destination IP address in three different formats:
  - **any** – all addresses match
  - **host** *12.34.56.78* – This address matches one specific computer with the given address
  - *IPaddress mask* – This address is compared to the given IP address ignoring the bits that are one in the mask.

Example

- This permits any computer on the Internet to connect to the computer whose IP address is 152.8.1.1 using the TCP protocol and port 443.

```
access-list 111 permit tcp any host 152.8.1.1 eq 443
```

Example

- This prevents any UDP traffic from reaching computers in 152.8.100.X subdomain

```
access-list 112 deny udp any
        152.8.100.0  0.0.0.255
```

- *Note: access-list statements must be written on one line.*

Order is Important

- When a packet arrives at your firewall, it will be compared with each access-list statement in the order they appear.
- The first statement that applies to that packet determines if it is permitted or denied.
- For incoming traffic, there is an implicit deny everything at the end of the access-lists.
- For outgoing traffic, there is an implicit permit everything at the end of the access-lists.

Try It

- Write an access statement to allow all users in your network to use the computer at 123.45.67.8

Restricting a Port

- Port numbers are used to identify specific applications
- The access-list statement must end with an operator and a port number
- The operators are:
  - **eq** equal
  - **lt** less than
  - **gt** greater than
  - **neq** not equal
  - **range** a range of ports; you must specify two different port numbers

Useful Port Numbers

- 21 FTP
- 23 Telnet
- 25 Simple Mail Transport Protocol
- 53 Domain Name Servers
- 80 HTTP
- 110 POP3 client email
- 123 Network Time Protocol
- 137-139 Microsoft NETBIOS
- 143 IMAP4 client email
- 161 Simple Network Maintenance Protocol
- 443 HTTPS
- 445 Windows File Sharing
- 1863 MSN Instant messaging
- 3389 Windows Remote Desktop Protocol
- 5190 AOL instant messenger

Example

- This allows FTP traffic to your local server at 152.8.110.47

```
access-list 113 allow tcp any
        host 152.8.100.0 eq 21
```

- *Note: access-list statements must be written on one line.*

Firewall Configuration

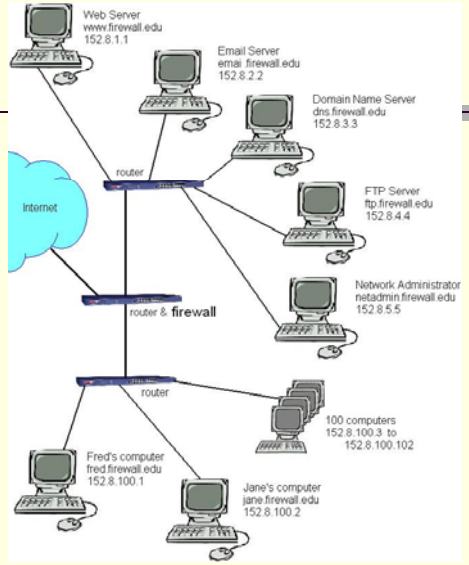
- The firewall configuration window should contain all of your **`access-list`** commands.
- Some real firewalls allow you to input only one line at a time or upload a file of commands
- The simulator assumes the file upload concept

Try It

- Write a firewall configuration statement to allow everyone in your network to receive POP3 email from the server at 211.72.229.163

Your Simulated Network

- There is a link on the webpage to a diagram of the simulated network showing the computers and their IP addresses.
- Your domain has the Internet address of 152.8.0.0/16



Coming and Going

- The access-list commands specify source and destination addresses.
- If the source address starts with 152.8, then the traffic is going out from your network to the Internet.
- If the source is any other address, then the traffic is coming into your network.

Initial Needed Services

- Access by the public to your web site
- Email from other email servers using SMTP
- Domain Name Server access

Fairness

- Once you have successfully attacked another student, you may not initiate the same attack against the same student for 45 seconds
- When a configuration change is specified, you have 45 seconds before anyone can be attacked related to that change

Simulator System Requirements

- The simulation is designed to run on regular PCs with no special networking restrictions.
- Participants need a Java enabled browser.
- Runs on Windows, Linux, etc.
- Safe to run in a public environment.
- The web server has to run the central monitor program.
- UDP port 49876 has to be open on real firewalls.