Laboration report - firewalls

Emil Nielsen (emini352) Erik Lindström (erili440)

December 12, 2007

1 Discussion and results

In the original firewall configuration, all incoming, outgoing and forwarded traffic was allowed, providing minimal security and control over the information flow. This meant that anyone could access most services on our computer, including our internal and secret web servers. Our final firewall configuration can be found in section A.

This could mean confidential information ending up in the hands of anyone with access to our IP address, which could cause great harm to, for example, a large company which handled personal information about customers, or other forms of confidential information.

A firewall does not protect against attacks from the inside. It is a good way to control the access to, for instance, a web server. One good way to set this up would be to initially prevent all access to the service, by using a drop policy, and then gradually granting access to the users needing it. This ensures that only the correct people get access to the service. If the administrator forgets something, this only means that someone will complain, allowing the administrator to fix the problem quickly. If, on the other hand, a policy allowing access by default had been used, some vulnerabilities might have been forgotten, which could potentially result in serious damage or information leakage, if an attacker were to discover them.

A iptables configuration

```
-P INPUT DROP
-P FORWARD DROP
-P OUTPUT ACCEPT
-A INPUT -m state -state ESTABLISHED -j ACCEPT
-A INPUT -s 192.168.80.13 -p tcp -j ACCEPT
-A INPUT -p tcp -destination-port 80 -j ACCEPT
-A INPUT -s 192.168.80.10 -p tcp -destination-port 8080 -j ACCEPT
-A OUTPUT -p tcp -destination-port 80 -d 192.168.80.13 -j ACCEPT
-A OUTPUT -p tcp -destination-port 80 -d 192.168.80.10 -j ACCEPT
-A OUTPUT -p tcp -destination-port 80 -j DROP
```