Assignment 2: Firewalls

Deadline: Thursday 6/10 17:00

This assignment can be done by at most two persons. Email your solution to Elmira.

Name1: __Uma Eriksson umaer178____

Name2: __Hugo Dahl hugda958____

Firewalls

This section contains questions related to security issues of firewalls; how this technology works and the different types of firewalls.

1. What are the two characteristics of static packet filter firewalls?

   They require you to manually establish firewall rules, internal and external networks will also remain open or closed unless manually adjusted by an admin.

2. How do stateful firewalls work for TCP?

   It collects data regarding all connections made through it.

3. Can stateful firewalls maintain state information for connectionless protocols like UDP and ICMP ?

   Yes it can.

4. How does a NAT firewall work?

   It works by only allowing internet traffic to pass through if a device on the private network has specifically requested it. A NAT firewall also protects the identity of a network, and it won't show the internal IP addresses to the internet.

5. Explain application firewall operation.

   It uses a series of configuration policies to decide whether to allow or block communications to or from an app.

6. If you will proxy four applications, how many proxy programs will you need?

   Four, a separate proxy program is needed for each application filtered on the Firewall.

7. Should the last rule of a screening firewall be Deny All or Permit All? Explain.

   Last Rule is Permit All to let main firewall handle everything but simple attacks.

8. You have a rule in your ACL to block a particular type of traffic. However, when you do an audit, you find that the firewall is not blocking this traffic. What is the problem likely to be?

> You might have placed another allow rule for this type of traffic. ACL rules are placed in a top-down fashion, meaning this deny rule might have been placed before an allow rule.

9. Assume that LiU has decided to have the following security policy:

- to allow only incoming (inbound) connections to port 25 of LiU mail server (130.236.8.134)

- to allow all outbound connections, that is, to permit all connections initiated by LiU internal hosts.

The LiU technician Pier implements the following ACL:

```
allow  tcp   * : *  →  130.236.8.134 : 25

drop  tcp   * : *  →  130.236.8.134 : *

allow  tcp   130.236.136.96 : *  →  * : *

allow  tcp   130.236.136.97 : *  →  * : *

        . . .  //  plus one such a rule for every internal IP address

drop   *    * : *  →  * : *
```

Does this rule set enforce the LiU security policy? Explain.

This one is a tricky question, be careful.

> It should work, the first line allows all incoming connections to the liu mail server, the second drops suspicions packets that make no sense, the third and fourth allow all connections from internal LiU hosts, and the last denies all other packages.