Assignment 2: Firewalls

Deadline: Fri 11/10 17:00

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

Name1: _____Anna Furugård, annfu090_____

Name2: _____

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?**

   Answer:

   - Packet filter firewalls have an access control list. The list dictates if what packets that will be looked and what action that should be applied.

   - The arriving packets are examined one at a time. This means that it misses attacks, packet filtering firewall have a low level of security.

2. **How do stateful firewalls work for TCP?**

   Answer: The TCP keeps track of its connection's usage of destination- and source address, IP flags and port numbers. The TCP is a connection-oriented protocol, and sessions starts with a three-way handshake, which makes keeping track of the state of a connection easier.

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

   Answer: Yes, they can. The protocols can record connections similar as with TCP but with less security. They are less secure because they are not bidirectional connections, this makes them more vulnerable for attacks.

4. **How does a NAT firewall work?**

   Answer:

   - The NAT firewall allows only internet traffic to pass through if a device on the private network has requested it. All other unsolicited requests or data packets are discarded.

   - The NAT firewall also changes the outgoing IP address and port, which hides the machine for possible attacks.

5. Explain application firewall operation.

Answer: An application firewall controls input, output or system calls for an application. It works by controlling the packets arriving and ascending from applications.

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

Answer: A separate proxy program is needed for each separate application filtered on the firewall. This means that we need four proxy programs.

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

Answer: The last rule should be **Permit All** because the screening firewall is only a layer of defense and checks for simpler 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?

Answer: ACL is applied in order top-down, this could lead to rules being overridden by another 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.

Answer:

1. The top prioritized rule says that all incoming connections is allowed on port 25, which we want.
2. We allow all outgoing tcp from the internal LiU-IP address, which we want.
3. I would change line 2: *"drop tcp 130.236.136.96:* → *:*"* to: *"drop * *:* → *:*"* since we want to allow only incoming connections to port 25. This makes the ACL follow our wished security policy.