CSCI 3403 **Brennon Lee**
Homework 12 **Fall 2018, CU-Boulder**

1. **Review Question 9.11** What is a DMZ network and what types of systems would you expect to find on such networks?

   DMZ (demilitarized zone) network is just inside of the external firewall, but outside of the internal firewall. It is a subnet that separates an internal local area network from the outside sources like the internet. The systems in the DMZ normally require access to external connections such as a web server, e-mail server, or a DNS server.

2. **Review Question 9.13** How does an IPS differ from a firewall?

   Intrusion Prevention Systems can block traffic like a firewall does but also makes use of types of algorithms developed for IDSs to determine when to do so.

3. **Problem 9.1** As was mentioned in Section 9.3, one approach to defeating the tiny fragment attack is to enforce a minimum length of the transport header that must be contained in the first fragment of an IP packet. If the first fragment is rejected, all subsequent fragments can be rejected. However, the nature of IP is such that fragments may arrive out of order. THus, an intermediate fragment may pass through the filter before the initial fragment is rejected. How can this situation be handled?

   answer

4. **Problem 9.5** SMTP is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following rule set:

Rule	Direction	Src. Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	> 1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	> 1023	Permit
E	Either	Any	Any	Any	Any	Deny

(a) Describe the effect of each rule.
Rule A - is allowing inbound mail from an external source (since port 25 is for SMTP incoming).
Rule B - is allowing responses to an inbound SMTP connection (like what rule A permits).
Rule C - allows outbound mail to an external source.
Rule D - allows responses to an outbound SMTP connection.
Rule E - Default last policy to reject any other connections since we don't want to allow anything else to occur.

(b) Your host in this example has IP address 172.16.11. Somone tries to send you e-mail from a remote host with IP address 192.168.3.4. If successful, this generates an SMTP dialogue between the remote user and the SMTP server on your host consisting of SMTP commands and mail. Additionally, assume a user on your host tries to send e-mail to the SMTP server on the remote system. Four typical packets for this scanario are as shown:

Packet	Direction	Src. Addr	Dest Addr	Protocol	Dest Port	Action
1	In	192.168.3.4	172.16.11	TCP	25	?
2	Out	172.16.11	192.168.3.4	TCP	1234	?
3	Out	172.16.11	192.168.3.4	TCP	25	?
4	In	192.168.3.4	172.16.11	TCP	1357	?

Indicate which packets are permitted or denied and which rule is used in each case.

Rule A will permit Packet 1 since this is inbound mail from an external source.
Rule B will permit Packet 2 since this is a response to an inbound SMTP connection.
Rule C will permit Packet 3 since this matches with outbound mail.

Rule D will permit Packet 4 since this matches with a response to outbound sent mail.

(c) Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.34) in order to carry out an attack. Typical packets are as follows:

Packet	Direction	Src. Addr	Dest Addr	Protocol	Dest Port	Action
5	In	10.1.2.3	172.16.34	TCP	8080	?
6	Out	172.16.34	10.1.2.3	TCP	5150	?

Will the attacks succeed? Give details.

Yes, the attacks will be permitted and succeed. Packet 5 will be permitted due to matching with Rule D (which allows responses from outbound sent mail). And Packet 6 will also be permitted to due Rule B (which allows responses from our server to the sender's SMTP connection).

5. **Problem 9.6** To provide more protection the rule set from the preceding problem is modified as follows:

Rule	Direction	Src. Addr	Dest Addr	Protocol	Src Port	Dest Port	Action
A	In	External	Internal	TCP	> 1023	25	Permit
B	Out	Internal	External	TCP	25	> 1023	Permit
C	Out	Internal	External	TCP	> 1023	25	Permit
D	In	External	Internal	TCP	25	> 1023	Permit
E	Either	Any	Any	Any	Any	Any	Deny

(a) Describe the changes.

The rule set has been modified to include a column of Source Ports to match against packets.

(b) Apply this new rule set to the same six packets of the preceding problem. Indicate which packets are permitted or denied and which rule is used in each case.

Packet 1 will be permitted due to rule A (source port $1234 > 1023$ **and Destination Port is** 25**).**

Packet 2 will be permitted due to rule B (source port 25 **and Destination Port is** $1234 > 1023$**).**

Packet 3 will be permitted due to rule C (source port $1357 > 1023$ **and Destination Port is** 25**).**

Packet 4 will be permitted due to rule D (source port 25 **and Destination Port is** $1357 > 1023$**).**

Packet 5 will be denied due to rule E. It does not match any of the rules in the table where a source port is 5150 **and a destination port is** 8080**.**

Packet 6 will be denied due to rule E as well. It does not match any of the rules in the table where a source port is 8080 **and a destination port is** 5150**.**

6. **Problem 9.11** You are given the following "informal firewall policy" details to be implemented using a firewall such as that in Figure 9.2:

(a) E-mail may be sent using SMTP in both directions through the firewall, but it must be relayed via the DMZ mail gateway that provides header sanitization and content filtering. External e-mail must be destined for the DMZ mail server.

(b) Users inside may retrieve their e-mail from the DMZ mail gateway, but only if they use the secure POP3 protocol and authenticate themselves.

(c) Users outside may retrieve their e-mail from the DMZ mail gateway, but only if they use the secure POP3 protocol and authenticate themselves.

(d) Web requests (both insecure and secure) are allowed from any internal user out through the firewall but must be relayed via the DMZ Web proxy, which provides content filtering (noting this is not possible for secure requests), and users must authenticate with the proxy for logging.

(e) Web requests (both insecure and secure) are allowed from anywhere on the Internet to the DMZ Web server.

(f) DNS lookup requests by internal users are allowed via the DMZ DNS server, which queries to the Internet.

(g) External DNS requests are provided by the DMZ DNS server.

(h) Management and update of information on the DMZ serveres is allowed using secure shell connections from relevant authorized internal users (may have different sets of users on each system as appropirate).

(i) SNMP management requests are permitted from the internal management hosts to the frewalls, with the firewalls also allowed to send management traps (i.e., notification of some event occurring) to the management hosts.

Design a suitable packet filter rule sets (similar to those shown in Table 9.1) to be implemented on the "External Firewall" and the "Internal Firewall" to satisfy the aftorementioned policy requirements.

answer