By Talal Shafei 30/05/2024

Firewall Lab

1. Table 11.3 shows a sample of a packet filter firewall ruleset for an imaginary network of IP address that range from 192.168.1.0 to 192.168.1.254. Describe the effect of each rule.

    1) This rule allows any packet coming from any source and any port to be sent to the destination address 192.168.1.0 with port greater than 1023.
    2) This rule will reject and discard any packet that contains source address 192.168.1.1 with any of its ports, so in short 192.168.1.1 is not allowed to send packets.
    3) This rule will discard any packet going to 192.168.1.1
    4) This rule will allow 192.168.1.0 to send packets to anywhere (except 192.168.1.1 because technically the previous rule will be checked first).
    5) Allows 192.168.1.2 to receive SMTP packets from anywhere to the SMTP default port.
    6) Allows 192.168.1.3 to receive HTTP packets from anywhere to the HTTP default port.
    7) Discard all other packets that didn't meet the previous rules.

2. SMTP (Simple Mail Transfer Protocol) 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 ruleset (table in the pdf manual).

    a. Describe the effect of each rule.

        A) This rule will allow all incoming (inbound) packets to port 25 using TCP.
        B) Will allow all outgoing (outbound) packets to go to any port greater than 1023 using TCP.
        C) Will allow all outgoing packets to go to port 25 using TCP.
        D) Will allow all incoming packets to any port greater than 1023 using TCP.
        E) Safety rule that will discard any packet from using any port using any protocol if it does not meet any of the above rules.

    b. Your host in this example has IP address 172.16.1.1. Someone tries to send 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 that a user on your host tries to send e-mail to the SMTP server on the remote system. Four typical packets for this scenario are as shown, Indicate which packets are permitted or denied and which rule is used in each case.

1) Permit using rule A.
2) Permit using rule B.
3) Permit using rule C.
4) Permit using rule D.

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 (172.16.3.4), in order to carry out an attack. Typical packets are as follows. Will the attack succeed? Give details.

   Packet 5 will be permitted using rule D because it's params match the rule, and similarly packet 6 will be allowed using rule B, therefore the attack will succeed.

3. To provide more protection, the ruleset from the preceding problem is modified.

   a. Describe the change.

   Added the Source Port column to restrict more the flow for packets in the network.

   A) Now external packet must be from source port greater than 1023.
   B) Internal packet must be from port 25.
   C) Internal packet must be from source port greater than 1023.
   D) External packet must be from source port 25.

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

   Even though the packets mentioned in the pdf doesn't explicitly show their source port the table, we still can see it from Q2 that it mentions the server is listening to port 25 so it will always reply to requests from there, which means source port of the server is 25, for user it says he is using a port greater than 1023 to send and listen to responses.

   1) Permit with rule A.
   2) Permit with rule B.
   3) Denied with rule E, because source port is 25 and destination port is 25 and E is the only rule that match that.
   4) Denied with rule E, because source port is greater than 1023 and destination port is also greater than 1023, and no rule match that except rule E.

   Now for 5, and 6 the source port for the attacker is 5150 and the Web proxy server will respond back using the port that it's listening to which is 8080.

   5) Denied with rule E, since now rule D now only allows packets incoming from port 25, so the only matching rule is E.

6) Denied with rule E, since the web proxy server will reply with port 5150 but now rule B only allows reply from port 25, so the only matching rule is E.

   Attacker failed because he couldn’t send packet 5, or see the reply from packet 6 if any.

4. A hacker uses port 25 as the client port on his or her end to attempt to open a connection to your Web proxy server.
   a. The following packets might be generated. Explain why this attack will succeed, using the ruleset of the preceding problem.

      Packet 7 will easily slip through and get permitted with rule D, and packet 8 will get permitted to bypass the firewall with rule C, and by this the attacker sent a request and received his response utilizing firewall for an email server to hack through the Web proxy server, therefore the attack is completed.

   b. When a TCP connection is initiated, the ACK bit in the TCP header is not set. Subsequently, all TCP headers sent over the TCP connection have the ACK bit set. Use this information to modify the ruleset of the preceding problem to prevent the attack just described.

      From the question we can understand that the first TCP packet have ACK bit as 0, and after it a connection is initiated so ACK bit will be set to 1.

      So, the following rules were modified to include the ACK bit, if it was 0 that indicates the establishment of a connection, otherwise it’s 1.

      Rule A allow for an external user to connect to the internal email server.
      Rule C allow for internal user to connect to an external email server (port 25)
      Thus A, C have ACK as 0.
      Other rules B, and C are just reply back from servers so their ACK must be 1.

Rule	Direction	Src Addr	Dest Addr	Protocol	Src Port	Dest Port	ACK	Action
A	In	External	Internal	TCP	> 1023	25	0	Permit
B	Out	Internal	External	TCP	25	> 1023	1	Permit
C	Out	Internal	External	TCP	> 1023	25	0	Permit
D	In	External	Internal	TCP	25	> 1023	1	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny

The attacker was exploiting the vulnerability that an internal user or service can connect to an external machine on port 25, so he used his port 25 to establish a connection, but this new modification restricts this flow, and ensure there is a connection from within, before receiving packets with source port 25 and this was enforced by checking ACK of the packet.

So now packet 7 has ACK as 0 because, and when it tries to connect using TCP, it will no longer pass on rule D, because rule D is expecting an already established connection, so 7 only matches on rule E and gets denied.

Even though the attacker already failed we can see that even packet 8, won't be matched with rule C, because packet 8 has ACK as 1, since it's a reply from Web proxy server, and C expect an internal user or service to start a connection which means it expect 0 in ACK, so only E matches and 8 fails.

Therefore, we stopped the attack by restricting the rules even more using our knowledge of which one can be used to start connection and which not.

Finally, all the packets that were sent from the user in Q2.b still get permitted because they follow correct TCP connection flow.