CIS 4367.01 **Brandon Thompson**
Prof. Elibol Due Date: 4/27/2020

Homework 20

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?

SOLUTION:
This is handled when the fragment is reassembled at the destination. Because the first fragment is discarded, it is impossible to reassemble the packet, after some time the packet will be rejected because it is not completed.

PROBLEM #9.4:

Table 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.

	Source Address	**Source Port**	**Dest Address**	**Dest Port**	**Action**
1	Any	Any	192.168.1.0	>1023	Allow
2	192.168.1.1	Any	Any	Any	Deny
3	Any	Any	192.168.1.1	Any	Deny
4	192.168.1.0	Any	Any	Any	Allow
5	Any	Any	192.168.1.2	SMTP	Allow
6	Any	Any	192.168.1.3	HTTP	Allow
7	Any	Any	Any	Any	Deny

SOLUTION:

1. Allows packets that are returned from TCP connections to internal subnet.
2. Deny the firewall from transmitting packets with the firewalls source address.
3. Deny external packets from from accessing the firewall.
4. Allow internal systems to connect to external systems using any external address and protocol.
5. Allow external packets to send email because it contains SMTP data.
6. Allow external packets to access World Wide Web server because it contains HTTP data.
7. Deny packets from outside sources

PROBLEM .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.

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 you 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 are shown:

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
1	In	192.168.3.4	172.16.1.1	TCP	25	?
2	Out	172.16.1.1	192.168.3.4	TCP 1234		?
3	Out	172.16.1.1	192.168.3.4	TCP	25	?
4	In	192.168.3.4	172.16.1.1	TCP	1357	?

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

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:

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
5	In	10.1.2.3	172.16.3.4	TCP	8080	?
6	Out	172.16.3.4	10.1.2.3	TCP	5150	?

Will the attack succeed? Give details.

SOLUTION:

a Description for each rule:

A Remote host receives email from external serer.

B External server receiving email from remote host.

C External server transmit the outgoing email to remote host.

D Remote host transmit the outgoing email to external server.

E Deny all other.

b Indicate each packet action:

Packet	**Direction**	**Src Addr**	**Dest Addr**	**Protocol**	**Dest Port**	**Action**
1	In	192.168.3.4	172.16.1.1	TCP	25	Permit (Rule A)
2	Out	172.16.1.1	192.168.3.4	TCP 1234		Permit (Rule B)
3	Out	172.16.1.1	192.168.3.4	TCP	25	Permit (Rule C)
4	In	192.168.3.4	172.16.1.1	TCP	1357	Permit (Rule D)

c The attack of packets 5 and 6 could succeed because the original filter set rule B and rule D permits all connections ends with transmission ports of above 1023.

Rule B will allow packet 5 and rule D will allow packet 6.

PROBLEM #9.7:

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:

Packet	**Direction**	**Src Addr**	**Dest** Addr	**Protocol**	**Src Port**	**Dest Port**	**Action**
7	In	10.1.2.3	172.16.3.4	TCP	25	8080	?
2	Out	172.16.3.4	10.1.2.3	TCP	8080	25	?

Explain why this attack will succeed, using the rule set of the preceding problem.

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 rule set of the preceding problem to prevent the attack just described.

SOLUTION:

a Reason this attack succeeds:

Rule D allows outbound SMTP connection for packet 7. Rule C allows outbound SMTP connection for packet 8.

b Prevent this attack:

Rule	**Direction**	**Src Addr**	**Dst Addr**	**Protocol**	**Src Port**	**Dst Port**	**ACK set**	**Action**
A	In	External	Internal	TCP	>1023	25	Yes	Permit
B	Out	Internal	External	TCP	25	>1023	Yes	Permit
C	Out	External	Internal	TCP	>1023	25	Any	Permit
D	In	Internal	External	TCP	25	>1023	Yes	Permit
E	In	Any	Any	TCP	Any	Any	Any	Deny

PROBLEM #9.8:

Section 9.6 lists five general methods used by a NIPS device to detect an attack. List some of the pros and cons of each method.

SOLUTION:

- Pattern matching
  - Advantages
    - Identifies the attacks.
    - Provides particular information for analysis and response of the attack.
  - Disadvantages
    - Produces false positive
    - Frequent signature table updates
    - Attacker can modify attack to avoid detection
- Stateful matching
  - Advantages
    - Identifies attacks
    - Detects signature of spread packets
    - Provides information for analysis and response
  - Disadvantages
    - Produces false positives
    - Frequent updates to signature table
    - Attacker can modify attack to avoid detection
- Protocol Anomaly
  - Advantages
    - Identifies attacks not including the signature
    - Shrinks false positive with good protocols.

  - Disadvantages
    * Produces false positives with complex protocols
    * Larger overhead.
- Traffic Anomaly
  - Advantages
    * Identifies unknown attacks and DoS floods
  - Disadvantages
    * Difficult to tune properly
    * Should understand normal traffic clearly
- Statistical Anomaly
  - Advantages
    *
  - Disadvantages
    * Takes time to gather the statistical data necessary

PROBLEM #9.13:

Explain the strengths and weaknesses of each of the following firewall deployment scenarios in defending servers, desktop machines, and laptops against network threats.

a A firewall at the network perimeter.

b Firewalls on every end host machine.

c A network perimeter firewall and firewalls on every host machine.

SOLUTION:

a A perimeter firewall provides access control and protection for DMZ systems that need external connectivity. Policy cannot be to strict or firewall will cut off access to necessary functions.

b Firewall can have more strict policies to better protect specific systems.

c This is the best option to ensure that systems are as protected as possible.