CPRE 431

M06 HW

Assignments will be submitted in PDF format via Canvas.

Please submit your homework online through Canvas. Late homework will not be accepted.
Important: Your submission must be in .pdf format ONLY!
Please ensure that you support all your answers with the correct screenshots showing your solutions.

1. Explain what is the differences between an IPS and a Firewall?

IPS inspects the content of a request over the network and if the content is a malicious, the IPS can clean, alert, or drop the request.

Firewall monitors the IP address, port, and protocols on the network and can block traffic based on the network information.

2. A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system. This is a well-known type of attack and is generally not effective against modern networks. It works if a server allocates resources after receiving a SYN, but before it has received the ACK. If Half-open connections bind resources on the server, it may be possible to take up all these resources by flooding the server with SYN messages. Syn flood is a common attack and it can be blocked with Linux/Unix iptables rules. Can you craft iptables rules that can block SYN flooding attacks? Explain your work and rationale.

```
iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 5 -j RETURN
```

So we created a rule that take in all inputs that have the flag syn and set a limit on the maximum average matching rate to 1 second (to limit the number of syn packets coming in to 1 per second) and setting a limit-burst that limits the number of packets the server can match at a time to 5.

3. 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 rule set:

Rule	**Direction**	**Scr Addr**	**Dst Addr**	**Protocol**	**Dst 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.

A: Allow external package to reach the server’s TCP port 25

B: Allow the server’s packets to leave to connect the client’s TCP port if the port is higher than 1023

C: Allow the server’s packets to leave to connect the client’s TCP port if the port is 25

D: Allow External packets to reach the server TCP port if the port is higher than 1023

E: Default deny rule for all in/out traffic

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:

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

Packet	Direction	Scr Addr	Dst Addr	Protocol	Dst Port	Action
1	In	192.168.3.4	172.16.1.1	TCP	25	Permit
2	Out	172.16.1.1	192.168.3.4	TCP	1234	Permit
3	Out	172.16.1.1	192.168.3.4	TCP	25	Permit
4	In	192.168.3.4	172.16.1.1	TCP	1357	Permit

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:

   i. Will the attack succeed? Give details.

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

d. To provide more protection, the rule set from the preceding problem is modified as follows:

   i. Describe the change.

Rule	Direction	Src Addr	Dst Addr	Protocol	Src Port	Dst 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: External packets are allow reach the server's TCP port 25 if they have a source port greater than 1023

B: All internal packets can leave if the source port is 25 and trying to connect to an external port greater than 1023

C: All internal packets can leave if the source port is greater than 1023 and trying to connect to an external port that is 25

D: External packets are allow reach the server's TCP port greater than 1023 if they have a source port is 25

E: Default Deny Rule for any in or out traffic

e. 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	Direction	Scr Addr	Dst Addr	Protocol	Dst Port	Action
1	In	192.168.3.4	172.16.1.1	TCP	25	Permit, A
2	Out	172.16.1.1	192.168.3.4	TCP	1234	Permit, B
3	Out	172.16.1.1	192.168.3.4	TCP	25	Permit, C
4	In	192.168.3.4	172.16.1.1	TCP	1357	Permit, D

Packet	Direction	Src Addr	Dst Addr	Protocol	Dst Port	Action
5	In	10.1.2.3	172.16.3.4	TCP	8080	Permit, D
6	Out	172.16.3.4	10.1.2.3	TCP	5150	PERMIT, B