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?

IPSs inspect the *content* of the request, and perform actions based on that. Firewalls inspect request header information like IP, port, and protocol, and perform actions based on that.

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.

```
sudo iptables -A INPUT -p tcp –syn -m limit --limit 2/s --limit-burst 3 -j DROP
```

This command matches all incoming tcp packets with only the ‘syn’ bit set, meaning it’s looking to start a connection. The command then imposes a limit on these packets of 2/second, and a burst of 3. If these criteria are met, the packet is dropped.

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 inbound traffic of type TCP to port 25
B. Allow outbound traffic of type TCP to port >1023
C. Allow outbound traffic of type TCP to port 25
D. Allow inbound traffic of type TCP to port >1023
E. Disallow all 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	?
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	?

1. Permitted using rule A
2. Permitted using rule B
3. Permitted using rule C
4. Permitted 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:

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	?
6	Out	172.16.3.4	10.1.2.3	TCP	5150	?

The attack will succeed, as both of those transactions are allowed through rules D and B respectively.

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

The addition of a src port check constrains the allowed packets to those that interact with port 12 in some way

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.

1. Permitted using rule A
2. Permitted using rule B
3. Permitted using rule C
4. Permitted using rule D
5. Denied using rule D (port 5150 -> 8080)
6. Denied using rule B (port 8080 -> 5150)