CSCI-3403 Cyber Security

Name: Chen Hao Cheng

Review Question Chapter 9

9.11) What is a DMZ network and what types of systems would you expect to find on such networks?

Demilitarized zone (DMZ) is a computer network or host between the internal and external firewall and prevents the direct access from external users to server.

Externally accessible systems are located in DMZ networks and also those systems need some security or protections. The systems in DMZ network encourages the external connectivity like

1. Corporate website
2. Email server
3. Domain name system server

9.13) How does an IPS differ from a firewall?

Intrusion prevention system (IPS) can detect or block the traffic by discarding the packet. It also monitors the ports and sends the commands to firewall to block the traffic. Besides, IPS offers an additional Intrusion Detection System (IDS) algorithm into IPS to block the traffic.

Problems Chapter 9

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 change

Rule A:

“remote host receiving the incoming email from external server from source port of more than 1023 to destination port of 25”, so rule A permits the inbound SMTP connection

Rule B:

“external server receiving the incoming email from remote host from source port of 25 to destination port of more than 1023”, so rule B permits the outbound SMTP connection

Rule C:

“external server transmits the outgoing email to remote host from source port of more than 1023 to destination port of 25”, so rule C permits the outbound SMTP connection

Rule D:

“remote host transmit the outgoing email to external server from source port of 25 to destination port of more than 1023”, so rule D permits the outbound SMTP connection

Rule E:

Since the direction is “In or Out” from any source address to any destination address from any source port to any destination port, so this rule doesn’t do any action. Its default rule is denied

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.

* Based on Rule A: Packet1 allows the “remote host receiving the incoming email from external host from source port of 1234 to destination port of 25”, so rule A permits inbound SMTP connection for packet1
* Based on Rule B: Packet2 allows the “external host receiving the incoming email from remote host from source port of 25 to destination port of 1234”, so rule B permits outbound SMTP connection for packet2
* Based on Rule C: Packet3 allows “external host transmit the outgoing email to remote host from source port of 1234 to destination port of 25”, so rule C permits outbound SMTP connection for packet3
* Based on Rule D: Packet4 allows “remote host transmit the outgoing email to external host from source port of 25 to destination port of 1234”, so rule D permits inbound SMTP connection for packet4
* Based on Rule E: Packet5 rejects “remote host transmit the outgoing email to external host from source port of 5150 to destination port of 8080”, so rule E is default rule to set the action is denied for packet5
* Based on Rule E: Packet5 rejects “remote host transmit the outgoing email to external host from source port of 8080 to destination port of 5150”, so Rule E is default rule to set the action is denied for packet6

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Packet | Direction | Src Addr | Dest Addr | Protocol | Src port | Dest port | Action |
| 1 | In | 192.168.3.4 | 172.16.1.1 | TCP | 1234 | 24 | Permit rule A |
| 2 | Out | 172.16.1.1 | 192.168.3.4 | TCP | 25 | 1234 | Permit rule B |
| 3 | Out | 172.16.1.1 | 192.168.3.4 | TCP | 1234 | 25 | Permit rule C |
| 4 | In | 192.168.3.4 | 172.16.1.1 | TCP | 25 | 1234 | Permit rule D |
| 5 | In | 10.1.2.3 | 172.16.3.4 | TCP | 5150 | 8080 | Permit rule E |
| 6 | Out | 172.16.3.4 | 10.1.2.3 | TCP | 8080 | 5150 | Deny rule E |

9.11)

Simple Mail Transfer Protocol (SMTP)

Demilitarized Zone (DMZ)

Domain Name Server (DNS)

Post Office Protocol (POP)

Hyper Text Transfer Protocol (HTTP)

Transmission Control Protocol (TCP)

User Datagram Protocol (UDP)

Simple Network Management Protocol (SNMP)

Secure Shell (SSH)

On the external firewall:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Action** | **Src** | **Port** | **Destination** | **Port** | **Flags** | **Comment** |
| Permit | DMZ mail gateway | Any | Any | SMTP(25) | Not Established | Sanitizing the header |
| Permit | Any | Any | DMZ mail gateway | SMTP(25) | Not Established | Filtering the content |
| Permit | Any | Any | DMZ mail gateway | POP3S(995) | Not Established | User authentication |
| Permit | DMZ web proxy | Any | Any | HTTP(80)  HTTPS(443) | Not Established | Content filtered, user authentication |
| Permit | DMZ DNS server | DNS(53) | Any | DNS(53) | Not Established | TCP & UDP |
| Permit | Any | DNS(53) | DMZ DNS server | DNS(53) | Not Established | TCP & UDP |
| Permit | Any | Any | Any DMZ server | Any | Established | Return traffic flow |
| Permit | Any | Any | Any | Any | Not Established | Block all else |

On the internal firewall:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Action** | **Src** | **Port** | **Destination** | **Port** | **Flags** | **Comment** |
| Permit | Any internal | Any | DMZ mail gateway | SMTP(25) | Not Established | Sanitizing the header |
| Permit | Any internal | Any | DMZ mail gateway | POP3(110)  POP3S(995) | Not Established | Filtered content |
| Permit | Any internal | Any | DMZ mail proxy | HTTP(80)  HTTPS(443) | Not Established | User authentication |
| Permit | Any internal | DNS(53) | DMZ mail server | DNS(53) | Not Established | Content filtered,  user authentication |
| Permit | DMZ DNS server | DNS(53) | Any internal | DNS(53) | Not Established | TCP & UDP |
| Permit | Any | Any | Any DMZ server | SSH(22) | Not Established | TCP & UDP |
| Permit | Management user hosts | Any | Any DMZ server | SNMP(161) | Not Established | Return traffic flow |
| Permit | Permit | Any | Management user host | SNMP TRAP(162) | Not Established | Block all else |

Review Questions Chapter 22

22.4) What is DKIM?

* Domain Keys Identified Mail (DKIM) is an email validation system that is used to detect the e-mail spoofing by checking if the incoming mail from a domain is authorized by that domain administrator or not.
* Cryptographic sign of e-mail messages are specified in DKIM
* DKIM makes a possibility for the messages recipients to verify the signature by querying the signer’s domain directly

22.5) What protocols comprise SSL?

**Secure Sockets Layer (SSL)**

* Implemented in set of protocols rely on TCP
* Establishes an encrypted link between a server and client
* Offers a reliable end-to-end secure over a TCP
* It is a secure protocol used to describe the usage of algorithm
* Determines the encryption variables for both the link and transmitted data

**Protocols comprise SSL**

* SSL handshake protocol
  + 1. The handshake protocol is used to authenticate both the server and client by each other and it negotiates an encryption, MAC algorithm, and cryptographic keys to protect the data send in SSL record
* SSL change cipher spec protocol
  + 1. This protocol consists a single message, that message consists of a single byte with the value 1
    2. The main purpose of this message is to copy the pending state into current state, and it updates the cipher suits to be used on SSL connection
* SSL alert protocol
  + 1. Alert protocol is used to convey the SSL related alerts to the peer entity
* SSL record protocol
  + 1. It provides the confidentiality and message integrity services for SSL connections

Problem Chapter 22

22.2)

**Secure Sockets Layer (SSL)**

* Implemented in set of protocols rely on TCP
* Establishes an encrypted link between a server and client
* Offers a reliable end-to-end secure over a TCP
* It is a secure protocol used to describe the usage of algorithm
* Determines the encryption variables for both the link and transmitted data

1. Man-in-the-middle attack: An attacker interposes during key exchange, acting an the client to the server and as the server to the client

The SSL uses public-key certificate service to authenticate the correspondents between server and client to protect key exchange from man-in-the-middle attack

1. Password sniffing: Password in HTTP or other application traffic are eavesdropped

The SSL uses the encryption service to encrypt the user’s data to protect the password in HTTP or other application traffic from eavesdropping

1. IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data

If the IP spoofer does not have valid SSL public-key or SSL certificate, then they cannot communicate the server

1. IP hijacking: An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts

The SSL uses the encryption service to encrypt the data to prevent the system from the attack. A secret key is used between sender and receiver, the sender secret key is verified by the receiver in every communication

1. SYN flooding: An attack sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacked TCP module typically leaves the “half-open connection” around for a few minutes. Repeated SYN messages can clog the TCP module.

The SSL does not offer any service to protect SYN flooding