Kieren Ng

Homework 11

9.11

DMZ networks are demilitarized networks that exist within the external firewall and outside the internal firewall. The systems in the DMZ could be web servers, email servers, and DNS servers.

9.13

Firewalls analyze packet headers, whereas IPS analyzes the entire packets looking for specific events.

9.6

a. There is a src port now added to the dest port. Now with this, rules a-d confirm that the connections are smtp connections- in the previous question just any port above 1023 would be allowed.

b. Packet 1 permit, rule A, Packet 2 Permit rule B, Packet 3 Permit rule c, Packet 4 Permit rule d, packet 5 deny rule e, packet 6 deny rule e

9.11

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Src | Src port | Dest | Dest Port | Flags | Action |
| DMZ Mail | Any (>1023 works too) | Any | 25 aka smtp |  | Permit |
| Any | Any | DMZ mail | 995 (apparently is pop3s) |  | Permit |
| DMZ DNS | 53 | Any | 53 |  | Permit |
| Any | Any | Any | Any | Established | Permit |
| Any | Any | Any | Any |  | Deny |

22.4

DKIM is domainkeys identified mail, “a specification for cryptographically signing email messages, permitting a signing domain to claim responsibility for a message in the mail stream.”

22.5

The handshake protocol, the change cipher spec protocol, and the alert protocol

22.2

a. SSL authenticates both sides with certificates

b. Passwords should be encrypted, not plaintext, so it should be relatively useless.

c. IP isn’t used to authenticate, certificates are used.

d. The hijacker needs to know a secret key, so unless he already knows it…

e. I think you’re fucked for syn flooding, bc I think you can’t tell between legit connection requests and hostile ones.