**MIS 6330: Cybersecurity Fundamentals**

**Individual Homework 7**

1. SMTP is the standard protocol for transferring mails over a TCP connection. The server listens to TCP port 25 and the user typically uses a port above 1023. Suppose you wish to build a packet filter ruleset allowing certain inbound and outbound SMTP traffic. All other traffic is thus blocked. You generate the following ruleset:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Rule | Direction | Source | Destination | 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 |

* 1. Your host has the IP address 172.16.1.1. A benign outside source tries to send an e-mail to your host, using SMTP, from a remote host with the IP address 192.168.3.4. Four typical packets for this scenario are as follows:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Packet | Direction | Source | Destination | 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 | ? |

Determine the action for each packet, i.e., which ones will be permitted and which ones will be denied.

* 1. Someone from the outside world (10.1.2.3) attempts to open a connection from local port 5150 on a remote host to the Web proxy server on on port 8080 on one of your local hosts (172.16.3.4) in order to carry out an attack. The packets involved are as follows:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Packet | Direction | Source | Destination | Protocol | Dest Port | Action |
| 1 | In | 10.1.2.3 | 172.16.3.4 | TCP | 8080 | ? |
| 2 | Out | 172.16.3.4 | 10.1.2.3 | TCP | 5150 | ? |

Will this attack succeed? Explain.

1. Explain why *stateful filters* are more secure vis-à-vis other *packet filters*.
2. Compare the following firewall topologies: *Double Bastion T* vs. *Double Bastion Inline*. What are their main differences from a security manager’s perspective? Which one is more secure in your opinion?