Wasfi Momen

Assignment 4

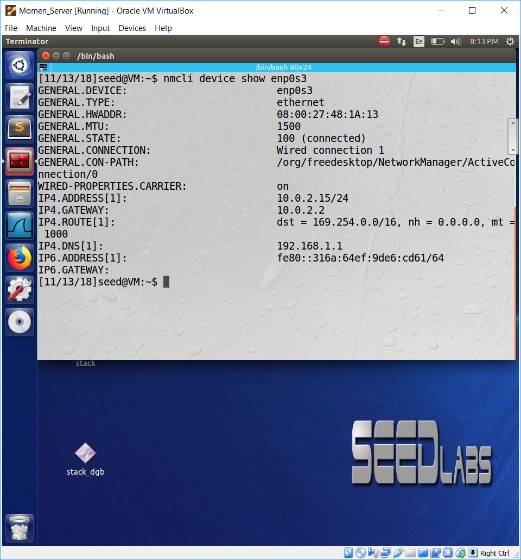
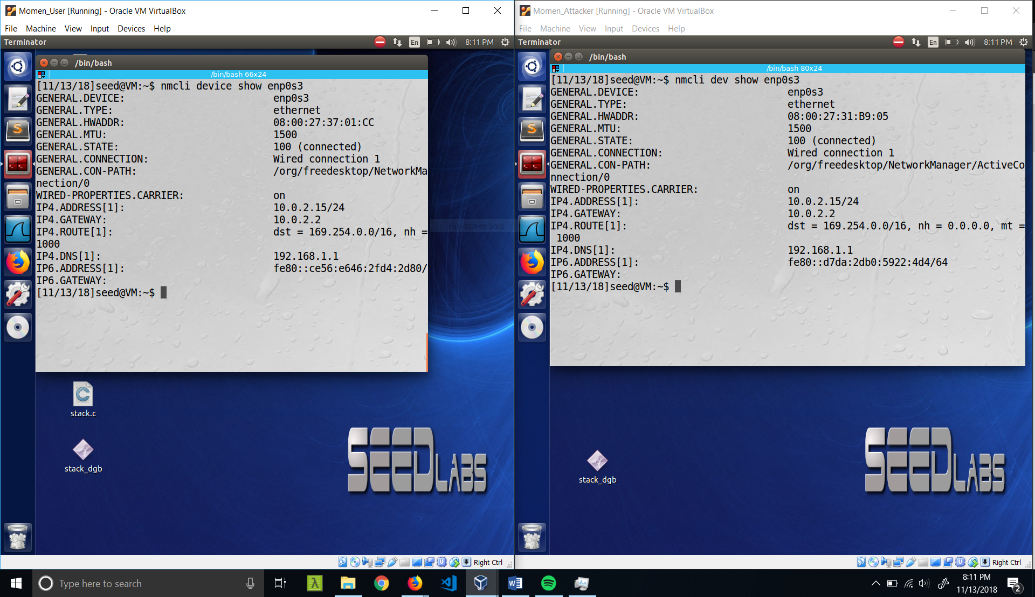
1. Allowing access to her Wifi opens Jill to many attacks. Her neighbors could use her Internet for illegal activities which she would be responsible for and use her IP address to make it seem like it came from her computer. Her neighbors could packet sniff all of the information Jill sends and receives.
2. An Ethernet frame has 22 bytes in the header and 4 bytes in the footer. The IPv4 packet within the Ethernet payload 20 bytes header. Inside the Ipv4 payload, the TCP packet will have 20 bytes header. If there was a UDP packet instead, the UDP packet will have 8 bytes header.
3. The adversary can use a botnet or just spoof his address repeatedly to get a lot of connections with the web server. Since the spoofed addresses don’t exist, the adversary will have to listen to the web server and send back spoofed ACKs to complete the TCP 3-way handshake. The web server will have created thousands of connections and will reject new ones until timeout. Even though SYN cookies were used, these connections were all valid and still resulted in a DOS attack.
5. Sequence = 156955004

Acknowledge = 883790340

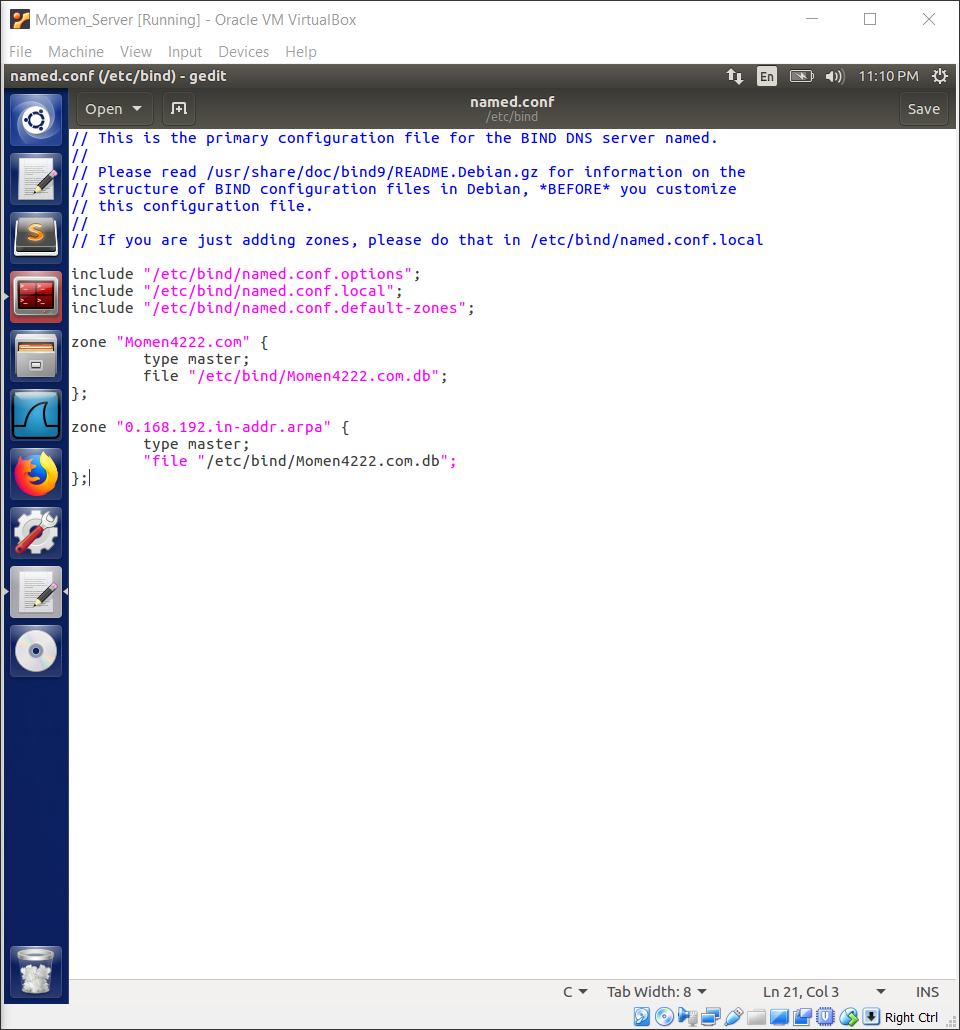
1. The adversary will have to send a packet with the spoofed IP of the target with the RST bit set to 1 and use the next sequence number. If the adversary cannot sniff packets, he cannot gain enough information to implement the attack.
2. A firewall rule should check each source IP address of the packet and see if it is in the network. If it is not, then drop the packet.
3. You could reject any packet that had a broadcast address as the destination IP address.

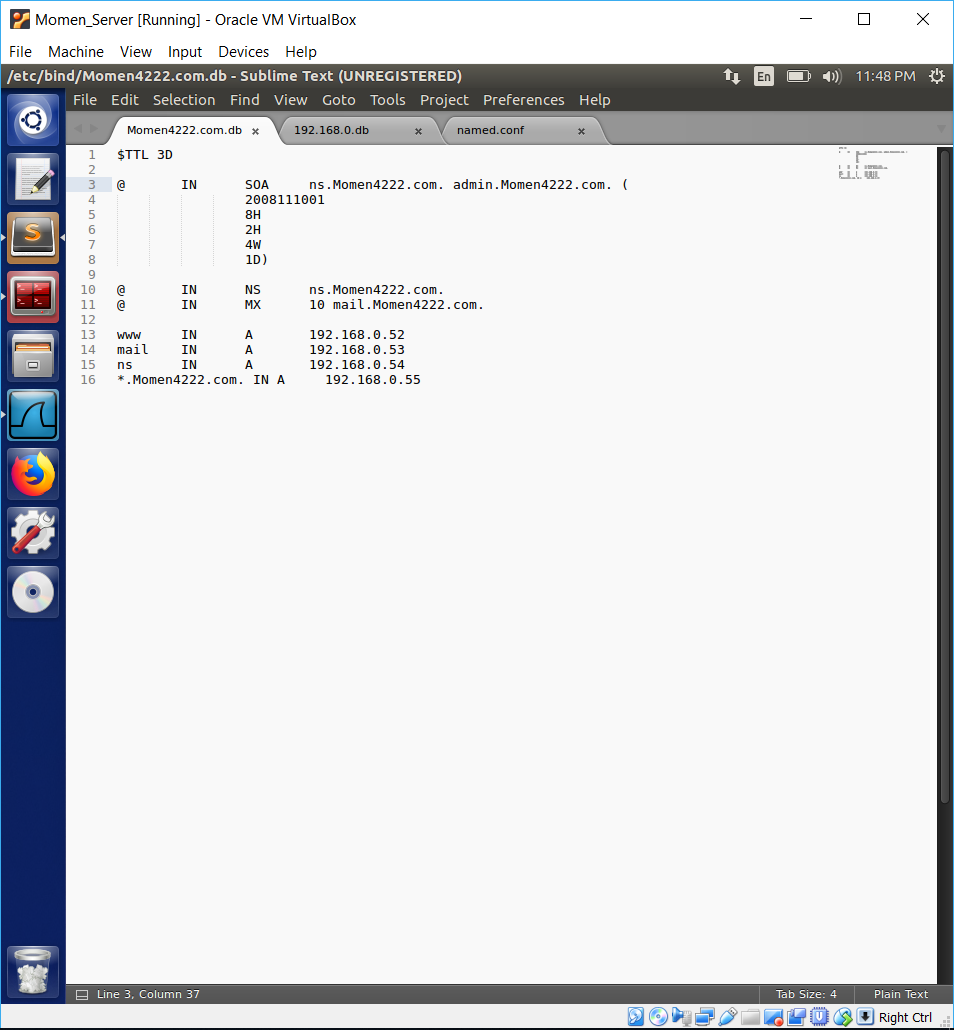
|  |  |  |  |
| --- | --- | --- | --- |
|  | User VM | Attacker VM | DNS Server VM |
| IP V4 Address | 10.0.2.15 | 10.0.2.15 | 10.0.2.15 |
| Network Mask | 24 | 24 | 24 |
| DNS Server | 192.168.1.1 | 192.168.1.1 | 192.168.1.1 |

We use “nmcli dev show enp0s3” to show the details of our wireless card.



|  |  |  |  |
| --- | --- | --- | --- |
|  | User VM | Attacker VM | DNS Server VM |
| IP V4 Address | 10.0.2.5 | 10.0.2.15 | 10.0.2.4 |
| Network Mask | 24 | 24 | 24 |
| DNS Server | 10.0.2.4 | 10.0.2.4 | 192.168.1.1 |



Last digits of my PantherID are 52.

