quick qanda

1. What is meant by a *half-open* scan?
2. What is the significance of a port number?
3. Is there anything stopping you from running SSH on something other than port 22?
4. How could a firewall easily detect a port scan?
5. In what ways could an attacker make a port scan stealthier?

qanda

- What is the IP address of the node1 NUC?
    - 10.100.100.141
- What is the IP address of the main NUC?
    - 10.100.100.140

- Book Questions
    A. What was the path through the TCP connection management finite state machine that the listening socket took to reach ESTABLISHED?
        a. CLOSED, LISTEN, SYN RCVD, ESTABLISHED
    B. What was the path through the TCP connection management finite state machine that the connecting socket took to reach ESTABLISHED?
        a. CLOSED, SYN SENT, ESTABLISHED

qanda

- Wireshark Questions
- Describe the established socket from both the listening and connection NUC, what changed? What remained the same?
    - The sockets on each machine are the same except the local address and peer addresses and ports are swapped.
- What was the sequence of FINs/ACKs from the listening side's perspective?
    - SYN -> SYN, ACK -> ACK -> FIN, ACK -> FIN, ACK -> ACK
- What was the sequence of FINs/ACKs fromm the connecting side's perspective?

    - SYN -> SYN, ACK -> ACK -> FIN, ACK -> FIN, ACK -> ACK
- How did the sequence numbers for each side of the connection change throughout the closing process?
    - The sequence numbers of each side increased.

Book Questions

- What was the path through the TCP connection management FSM that the listening socket took to reach CLOSED?
    - ESTABLISHED, CLOSE WAIT, LAST ACK, CLOSED
- What was the path through the TCP connection management FSM that the connecting socket took to reach CLOSED?
    - ESTABLISHED, FIN WAIT 1, CLOSING, TIME WAIT, CLOSED

qanda

Wireshark Questions

- Find a data transfer packet within the connection (there are two of them, pick one)
- How many total bytes was sent over the network for this frame?
    - 90
- How many of those bytes were the message you sent?
    - 24
- What was the sequence number on the first data packet sent? (the first of the two)
    - 0xEB2021DC (relative 1)
- What was the sequence number on the second data packet sent?
    - 0xEB2021F4 (relative 25)
- How are they related to each other and the acknowledgement numbers?
    - The second one is 24 more than the previous one. This is because the message is 24 bytes.

qanda

Wireshark Questions

- How many SYN packets did your machine send before giving up?
    - 7
- What is the time delta between each packet? (How much time has passed)
    - 1 second, then 2 seconds, then 4, then 8, then 16, then 32.
- Describe any patterns you observed.

    - Each delta is twice as large as the previous one,
- Linux Question
    - Run the command sudo sysctl -a | egrep 'tcp.*retries'
    - Do any of the numbers match your answer from above?
        - net.ipv4.tcp_syn_retries=6 matches our first answer. Because if you retry 6 times 7 packets will be sent.