DFSC 1316: digital forensic and information assurance fundamentals I

6 Case study: the curious Mr. X

*Reference book: *TCP/IP Protocol Suite* by Behrouz A. Forouzan.

Objectives

- See how TCP/IP principles are used in real forensics analysis.

- Get hands-on experience on network forensics.

Case: the curious Mr. X

While a fugitive in Mexico, Mr. X remotely infiltrates the Arctic Nuclear Fusion Research Facility's (ANFRF) lab subnet over the Interwebs. Virtually inside the facility (pivoting through a compromised system), he conducts some noisy network reconnaissance. Sadly, Mr. X is not yet very stealthy.

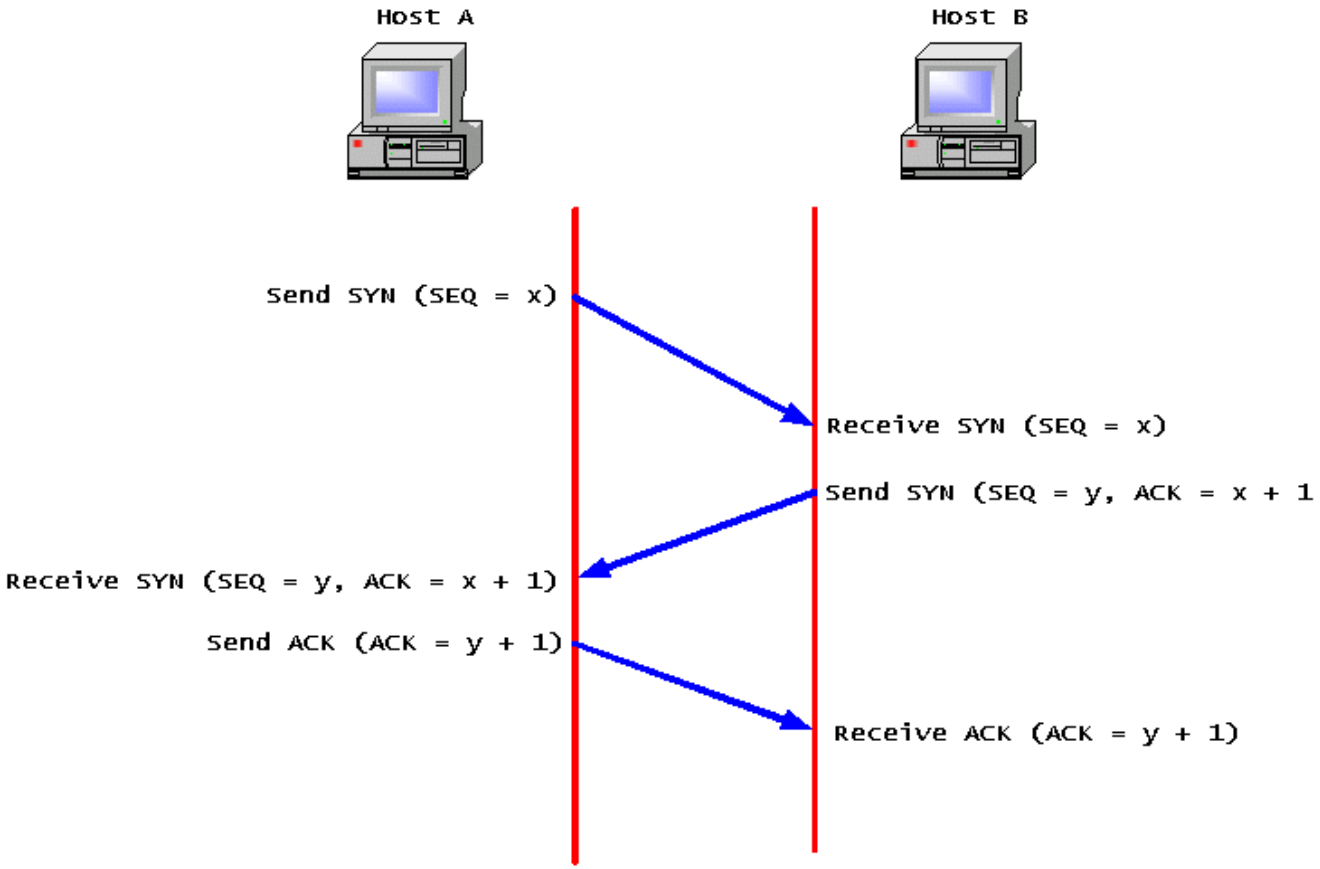
Unfortunately for Mr. X, the lab's network is instrumented to capture all traffic (with full content). His activities are discovered and analyzed… by you!

As the network forensic investigator, your mission is to answer the following questions:

1. * What was the IP address of Mr. X's scanner?
2. * For the FIRST port scan that Mr. X conducted, what type of port scan was it? (Note: the scan consisted of many thousands of packets.) Pick one:
   - TCP SYN, TCP ACK, UDP, TCP Connect, TCP XMAS, TCP RST
3. * What were the IP addresses of the targets Mr. X discovered?
4. * What was the MAC address of the Apple system he found?
5. * What was the IP address of the Windows system he found?
6. * What TCP ports were open on the Windows system?

Port Scanning

- The TCP 3-way handshake



TCP SYN Scan

- AKA, half-open scan.
  - Terminate the connection after SYN,ACK.

Below is a complete packet trace of a TCP SYN scan.

```
# Once again we are sending initial SYN to port 80 on google.com
0.695056  192.168.1.100  ->  72.14.207.99  TCP  59002  >  www  [SYN]  Seq=0  Len=0
MSS=1460
# Response is SYN/ACK so we can conclude that the port is indeed open
0.844707  72.14.207.99  ->  192.168.1.100  TCP  www  >  59002  [SYN,  ACK]  Seq=0  Ack=1
Win=8190  Len=0  MSS=1460
# Since we do not want to complete the connection, we send RST to google
0.844736 192.168.1.100 -> 72.14.207.99 TCP 59002 > www [RST] Seq=1 Len=0
```

TCP ACK Scan

- To test if a host is reachable (i.e., if a port is filtered or unfiltered).
  - Reply RST if unfiltered.
  - Reply mothering if filtered.

Unfiltered response:

```
# Sending ACK packet to the target on port 80
0.425238  192.168.1.100  ->  216.34.181.45  TCP  63851  >  www  [ACK]  Seq=0  Ack=0
Win=2048 Len=0
# We have received  RST back meaning the port is unfiltered
0.459511 216.34.181.45 -> 192.168.1.100 TCP www > 63851 [RST] Seq=0 Len=0
```

Filtered response

```
# Sending ACK packet to the target on port 666
1.728128  192.168.1.100  ->  216.34.181.45  TCP  46985  >  666  [ACK]  Seq=0  Ack=0
Win=4096 Len=0
# We have received no response so we try one more time and give up.
1.908035  192.168.1.100  ->  216.34.181.45  TCP  46986  >  666  [ACK]  Seq=0  Ack=0
Win=3072 Len=0
```

TCP Connect Scan

- The “classical” form
  - Reply RST if port is closed
  - Reply SYN,ACK if port is open.

Below is a complete packet trace of a typical TCP Connect scan.

```
# sending initial SYN of the three-way handshake to google.com on port 80 (www):
0.514699  192.168.1.100  ->  72.14.207.99  TCP  58851  >  www  [SYN]  Seq=0  Len=0
MSS=1460 TSV=18536702 TSER=0 WS=2
# receiving SYN/ACK from google indicating an open port port 80 (www):
0.603326 72.14.207.99 -> 192.168.1.100 TCP www > 58851 [SYN, ACK] Seq=0 Ack=1
Win=8190 Len=0 MSS=1460
# we complete the three-way handshake by sending ACK back to google with a
received sequence number:
0.603362  192.168.1.100  ->  72.14.207.99  TCP  58851  >  www  [ACK]  Seq=1  Ack=1
Win=5840 Len=0
# at last we are sending RST back to google to close the connection:
0.603629 192.168.1.100 -> 72.14.207.99 TCP 58851 > www [RST, ACK] Seq=1 Ack=1
Win=5840 Len=0
```

Here is a packet trace of a scanner attempting to connect to a closed port:

```
# sending initial SYN to port 666 of a local 192.168.1.104 machine
0.163866  192.168.1.100  ->  192.168.1.104  TCP  59079  >  666  [SYN]  Seq=0  Len=0
MSS=1460 TSV=18703363 TSER=0 WS=2
# we received RST back so we know that the port is closed
0.163956 192.168.1.104 -> 192.168.1.100 TCP 666 > 59079 [RST, ACK] Seq=0 Ack=1
Win=0 Len=0
```

TCP XMAS Scan

- To determine if a port is closed.
  - FIN,PSH,URG is sent.
  - If a port is closed, RST will be replied.
  - *"The RFC 793 expected behavior is that any TCP segment with an out-of-state Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets"* – CAPEC

Xmas Scan:

```
# sending Xmas packet to the target host
0.131860 192.168.1.100 -> 192.168.1.104 TCP 50984 > 666 [FIN, PSH, URG] Seq=0
Urg=0 Len=0
# we've got RST back so we can conclude the port is closed
0.131959 192.168.1.104 -> 192.168.1.100 TCP 666 > 50984 [RST, ACK] Seq=0 Ack=0
Win=0 Len=0
```