

# Agenda

- ▶ Review: the Kevin Mitnick Attack
- ▶ The TCP Reset Attack

Kevin Mitnick is           .

- ▶ A. A hacker who hacked into Jennifer Lawrence's iCloud account and released her nude photos online.
- ▶ B. A professor at BSU.
- ▶ C. A hacker who was on the FBI's most wanted list.
- ▶ D. Kim Kardashian's husband.



The Kevin Mitnick attack was against the \_\_.

- ▶ A. TCP 1-way handshake
- ▶ B. TCP 2-way handshake
- ▶ C. TCP 3-way handshake
- ▶ D. TCP 4-way handshake

The Kevin Mitnick attack was against the \_\_.

- ▶ A. TCP 1-way handshake
- ▶ B. TCP 2-way handshake
- ▶ C. TCP 3-way handshake
- ▶ D. TCP 4-way handshake

SYN flood is \_\_.

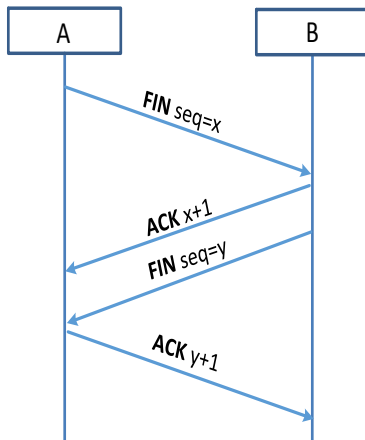
- ▶ A. A flood caused by the Hurricane Harvey.
- ▶ B. A technique used by attackers to make the target machine busy.
- ▶ C. A technique used to establish a TCP connection.
- ▶ D. A technique used to synchronize emails between Hillary Clinton's private email server and the government's official email server.

SYN flood is \_\_.

- ▶ A. A flood caused by the Hurricane Harvey.
- ▶ B. A technique used by attackers to make the target machine busy.
- ▶ C. A technique used to establish a TCP connection.
- ▶ D. A technique used to synchronize emails between Hillary Clinton's private email server and the government's official email server.

# Closing a TCP connection - Civilized Method

Two parties both say goodbye - following TCP FIN Protocol.





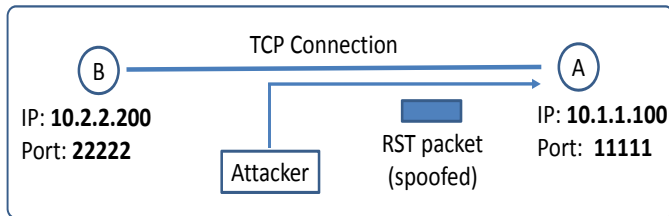
# Closing a TCP connection - Rude Method

One party sends a single RST packet to the other; for emergency use only, e.g., when there is no time to do the FIN protocol, or when errors detected.

# TCP Reset Attack

Attacker spoofs a TCP RST packet from A to B or from B to A, so as to close a TCP connection. A type of DOS attack.

# TCP Reset Attack



# TCP Reset Packet

Version	Header length	Type of service				Total length				
Identification						Flags	Fragment offset			
Time to live		Protocol				Header checksum				
Source IP address: <b>10.2.2.200</b>										
Destination IP address: <b>10.1.1.100</b>										
Source port: <b>22222</b>						Destination port: <b>11111</b>				
Sequence number										
Acknowledgement number										
TCP header length		U	A	P	R	S	F	Window size		
		R	C	S	S	Y	I			
		G	K	H	T	N	N			
Checksum						Urgent pointer				

IP

TCP

A large portion of the material is adapted/copied from:

- ▶ Computer Security - A Hands-on Approach by Wenliang Du
- ▶ Guide to Network Defense and Countermeasures - Randy Weaver, Dawn Weaver, Dean Farwood