Kevin Mitnick

- First hacker on the FBI's Most Wanted list.
- "Anything out there is vulnerable to attack given enough time and resources."

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ WF214660921).

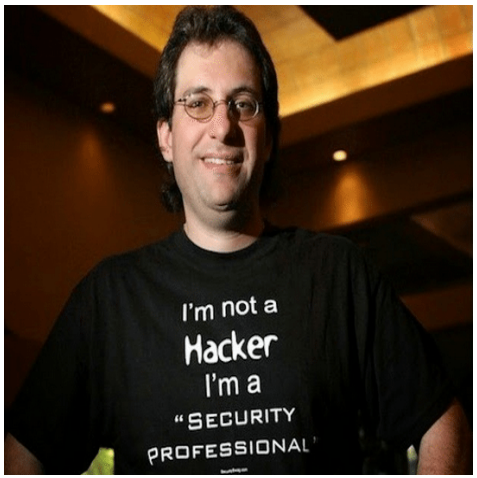
NAME: .....MITNICK, KEVIN DAVID

AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....SOME KNOWN
Social Security Number (s): 550-39-3695
NCIC Fingerprint Classification: ...DOPKDDPM13DIPM19WOI

Kevin Mitnick



- Was a hacker, is a computer security consultant.
- https://en.wikipedia.org/wiki/Kevin_Mitnick
- Never stole or profited from any information he hacked into
- Follow him on twitter: @kevinmitnick
  https://twitter.com/kevinmitnick (206K followers)

The Kevin Mitnick Attack

Who: Kevin Mitnick (The Attacker); Tsutomu Shimomura (The Victim)
When: December 25, 1994
Where: San Diego
What: Shimomura's computer was hacked by Kevin Mitnick
How: ??

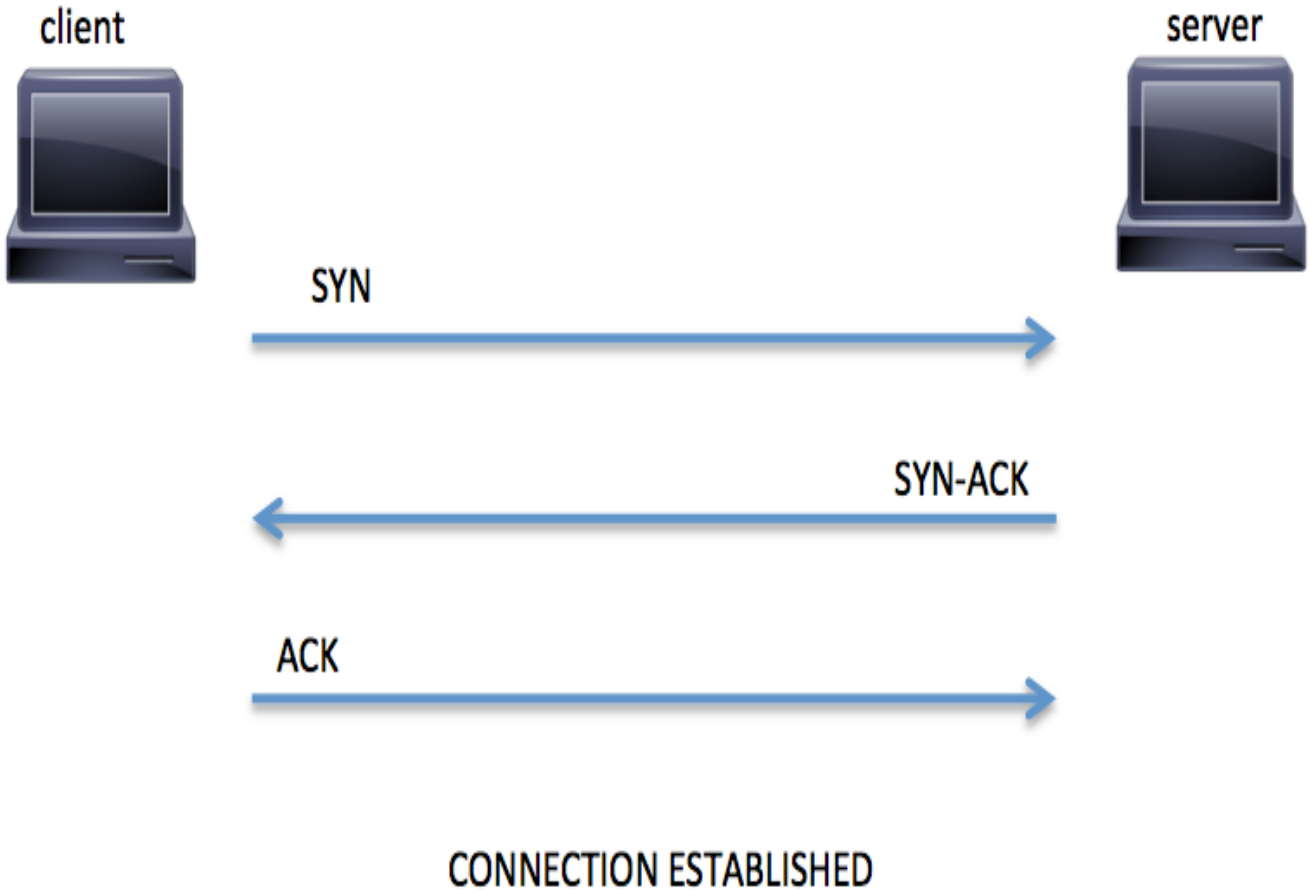
The Kevin Mitnick Attack

Attack against the TCP 3-way handshake.
Attacking mechanisms used:

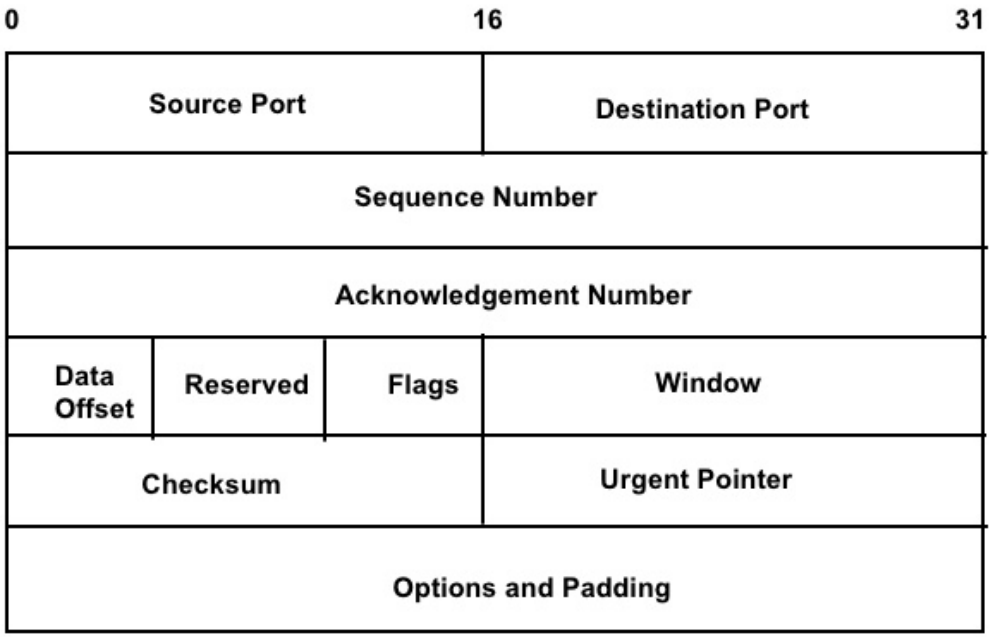
- IP spoofing
- SYN flood
- TCP sequence number prediction

TCP 3-way Handshake

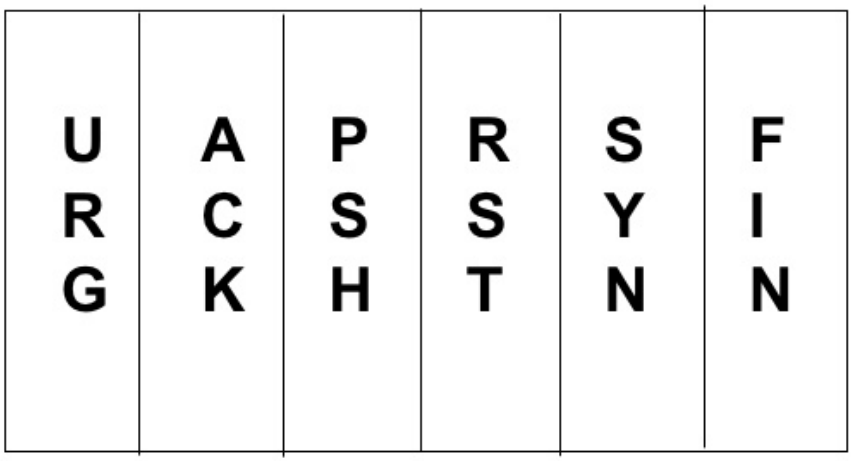
TCP 3-way Handshake



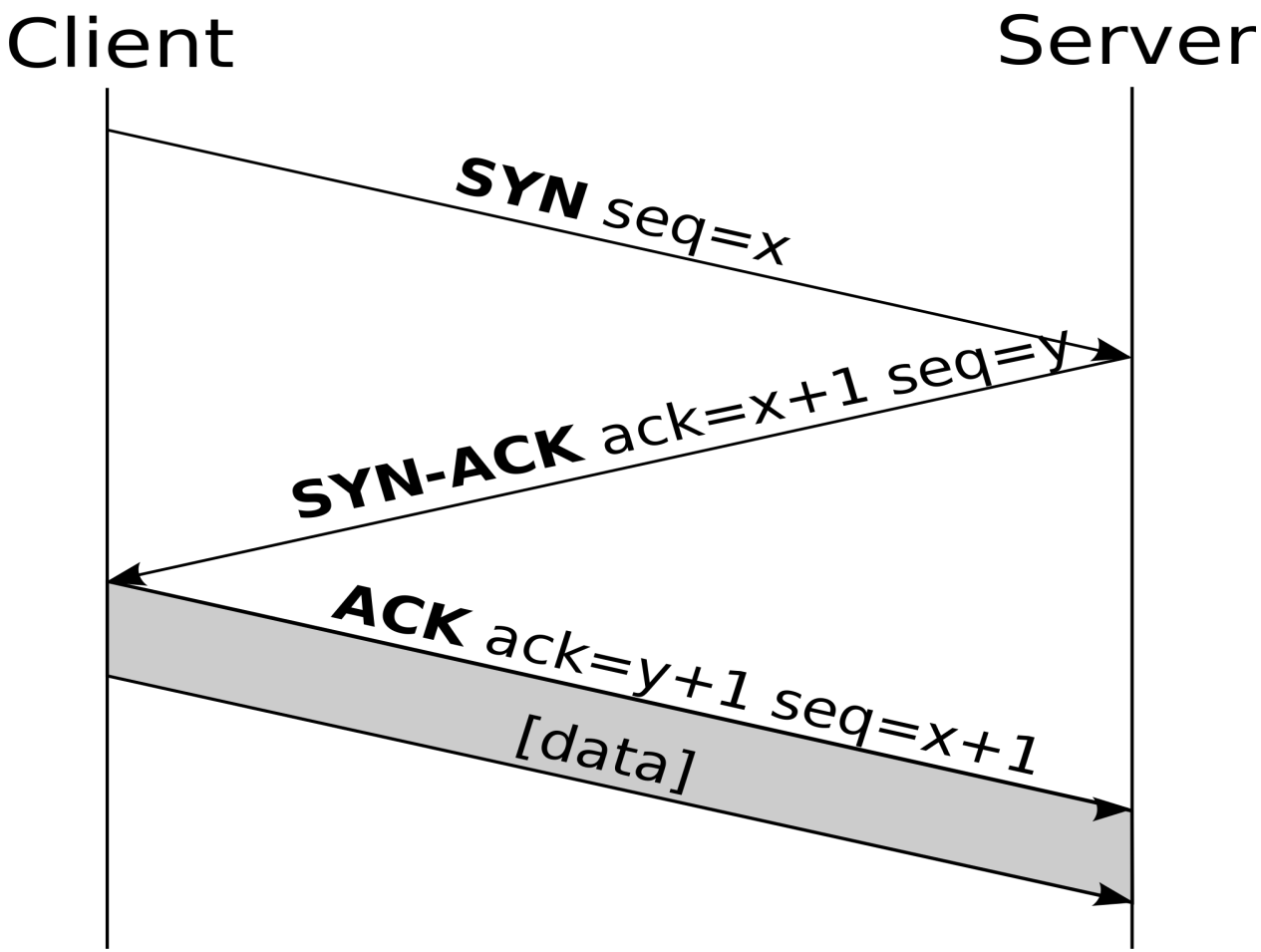
TCP Header


TCP Header
0
16
31
Source Port
Destination Port
Sequence Number
Acknowledgement Number
Data Offset
Reserved
Flags
Window
Checksum
Urgent Pointer
Options and Padding

TCP Header

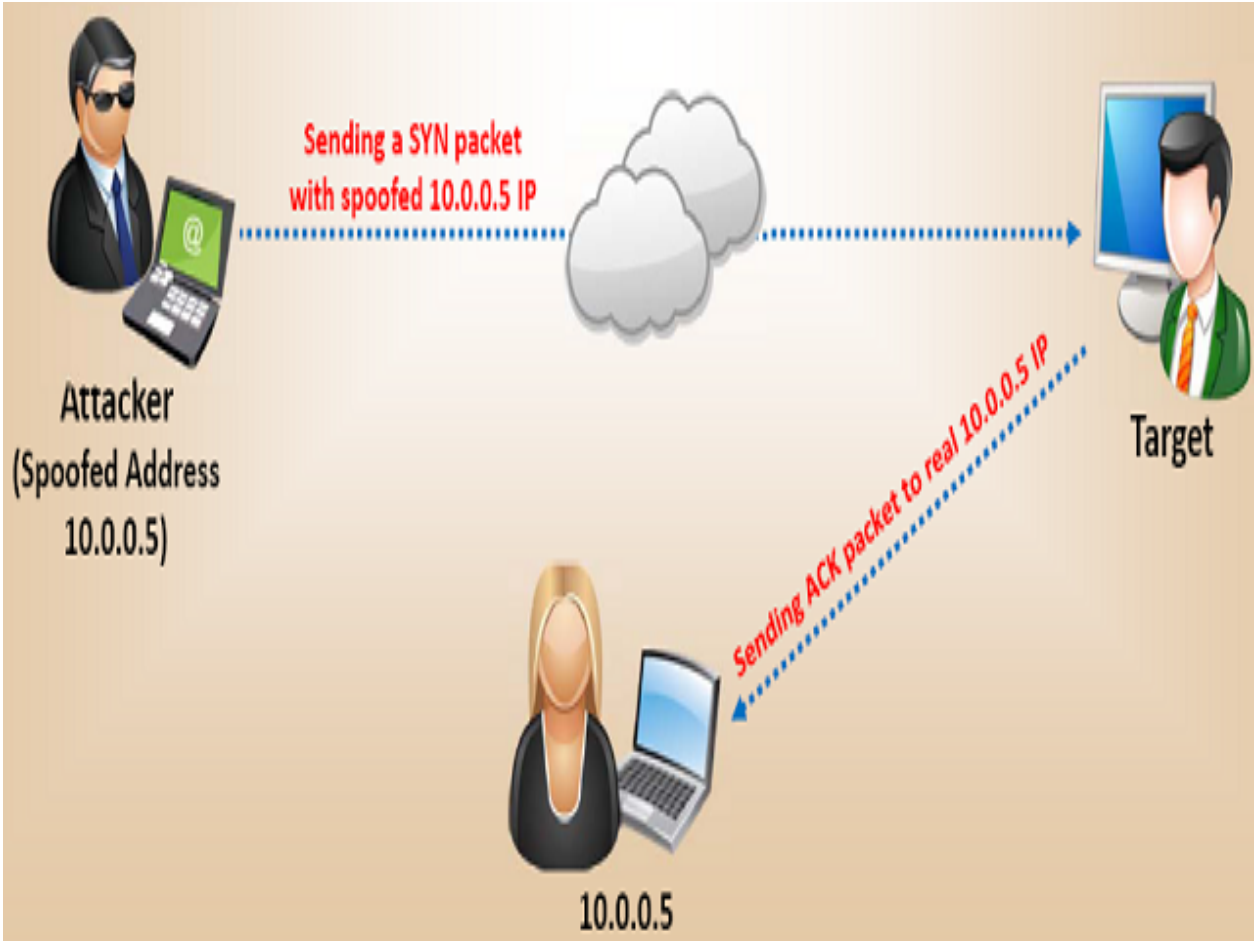


TCP 3-way Handshake



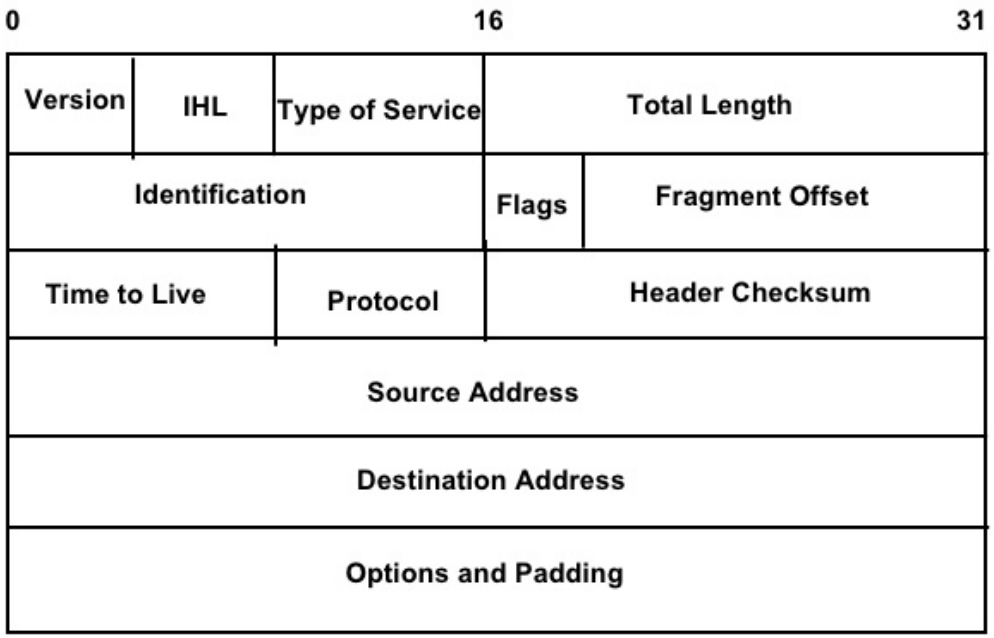
IP Spoofing

A technique in which an attacker creates IP packets with a false source IP address, so as to conceal its identity or impersonate another computer system.

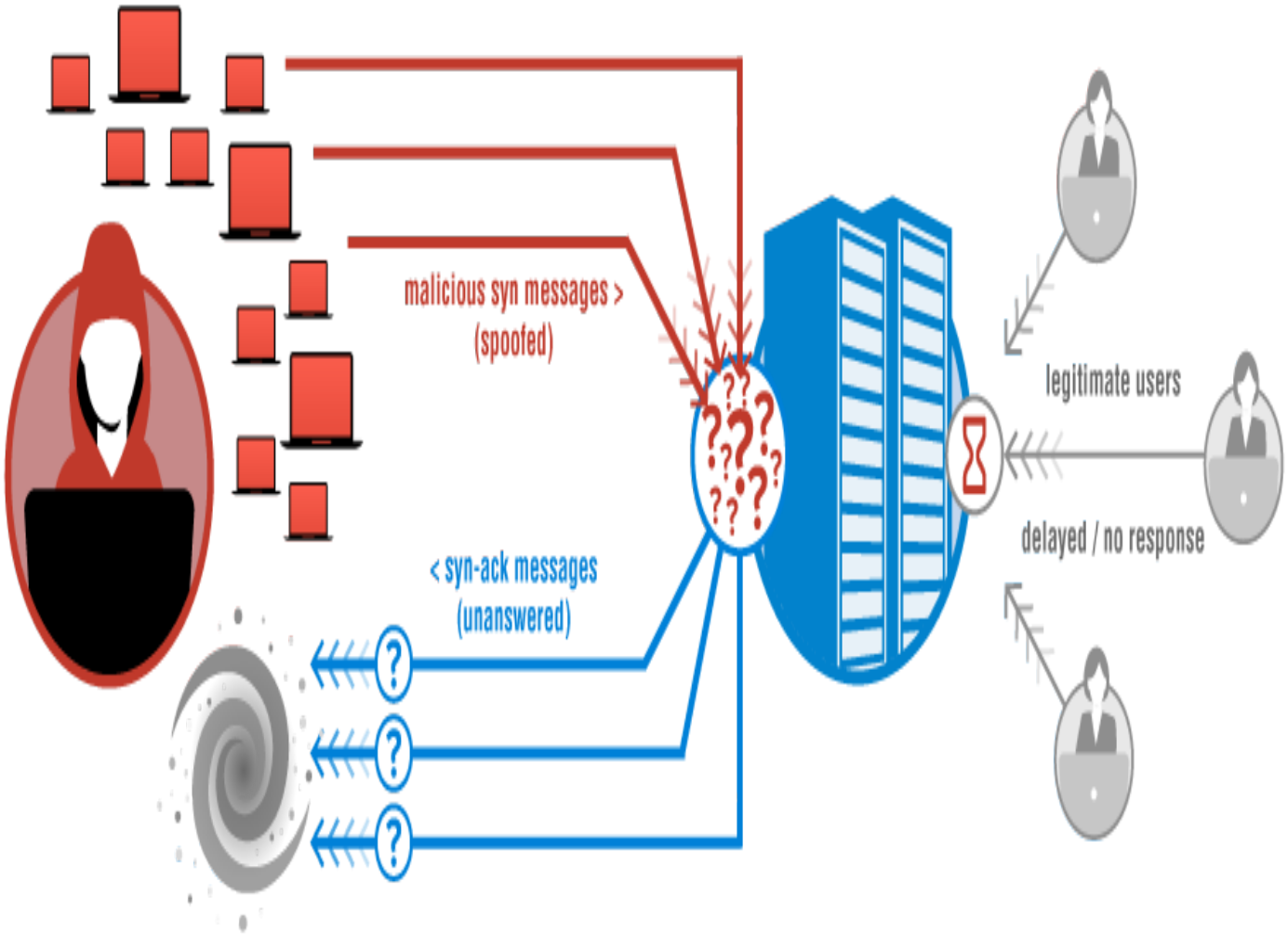


IP Spoofing

IP Header



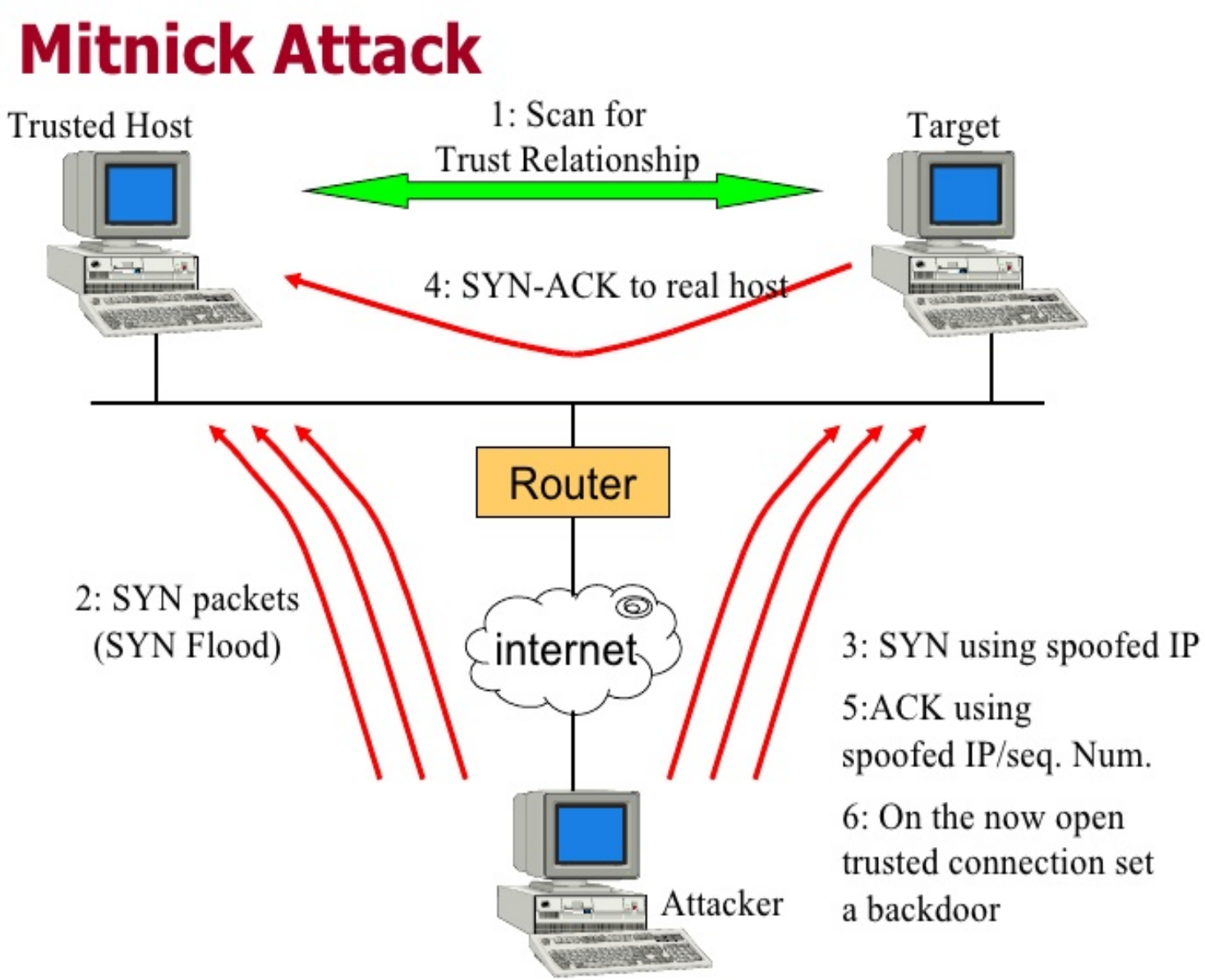
SYN Flood


malicious syn messages >
(spoofed)
< syn-ack messages
(unanswered)
legitimate users
delayed / no response

TCP Sequence Number Prediction

Mitnick sent SYN request to the Target and received SYN/ACK response. Then he sent RESET response to keep the Target from being filled up. He repeated this for twenty times. He found there is a pattern between two successive TCP sequence numbers. It turned out that the numbers were not random at all. The latter number was greater than the previous one by 128000.

The Kevin Mitnick Attack



Consequence

- Caught in 1995
- Charged with wire fraud (14 counts), possession of unauthorized access devices (8 counts), interception of wire or electronic communications, unauthorized access to a federal computer, and causing damage to a computer
- 46 months and 3 years probation
- Released 21 Jan 2000
- Cannot have anything to do with a PC until 20 Jan 2003

Other Interesting Resources

Freedom Downtime: A documentary produced by 2600: The Hacker Quarterly in response to Track Down. (Available on youtube. https://www.youtube.com/watch?v=77ILA5Cso3w)

The Art of Deception: A book written by Kevin Mitnick in 2002, explains how social engineering can be combined with hacking.

Question

Why the attack happened on Christmas Day?

Question

Why the attack happened on Christmas Day?

Shimomura's machine has to be idle for the attack to succeed.
New Internet connections would change the initial sequence number and make it more difficult to predict the sequence number.