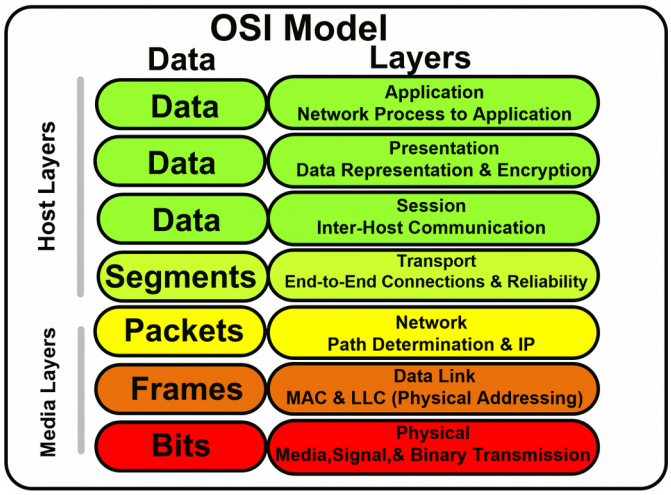
TCP/IP Attacks, Defenses and Security Tools

Based on International Journal of Science and Modern Engineering (IJISME)
ISSN: 2319-6386, Volume-1, Issue-10, September 2013
By Abdullah H. Alqahtani, Mohsin Iftikhar

Agenda

- Short introduction of TCP/IP
- TCP SYN Attack
- Defense against TCP SYN Attack (extra)
- IP Spoofing
- Defense against IP Spoofing

Where are we?



We are at
- Layer 3 Packets: IP Protocol
- Layer 4 Segments: TCP Protocol

TCP/IP – Collection of communication protocols operating over the Internet.

They provide:
- data formatting,
- adressing
- routing of packets

TCP – Transmission Control Protocol
IP – Internet Protocol

IP – Layer 3

- IP is responsible for routing of packets (datagrams) over the network to their destination
- Datagrams can take different routes to reach destination and arrive out of sequence
- Each node on the network makes a decision about the next hop a datagram arrives at

IP – Internet Protocol
* Routing datagrams
* Datagrams take different paths
* Nodes decide the next hop on of the datagram path

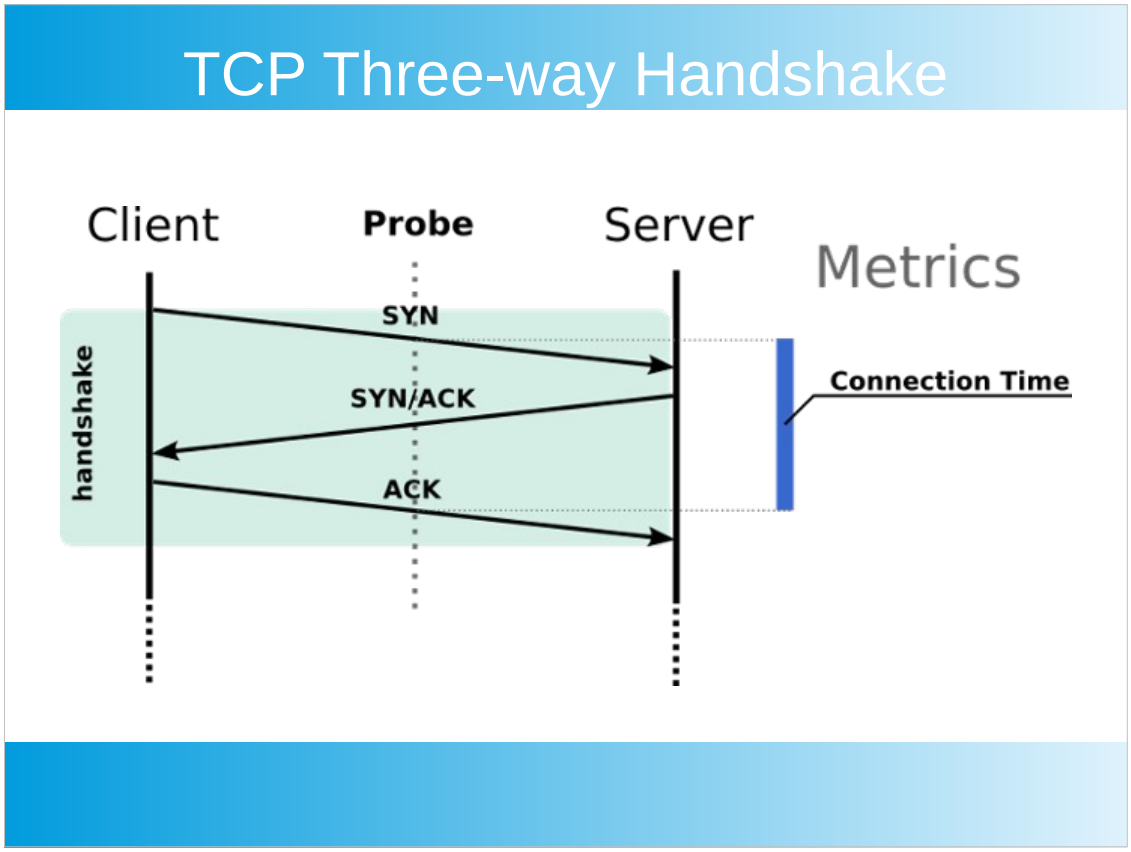
Nodes use certain routing protocols:
* not reliable – no delivery guarantee
* connectionless protocol – no flow control, no error detection, no error correction

TCP – Layer 4

- TCP Built on top of IP
- Data stream is broken into segments
- Reliable – guarantees segment delivery
- Error detection + correction
- Three-way handshake

Mechanisms used by TCP:
* sequence numbers of segments
* acknowledgments
* three-way handshakes
* timers

Three-way handshake:
- establish connection between two parties

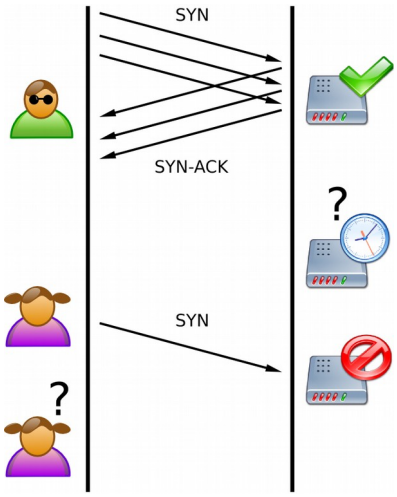


1. SYN packet with ISN sent to the server
SYN – Synchronize
ISN – Initial Sequence Number

2. Server responds with SYN ACK package
SYN – Synchronize
ACK – Acknowledgement

3. Client sends an ACK package to acknowledge the server's SYN package

TCP SYN Attacks



Server has limited resources. It sets aside resources for proceeding with each SYN request.

Attacker sends multiple SYN requests without ever ACK'nowledging them.

This attack was named TCP SYN Flooding attack.

Legit users would not be able to receive service.

This is a DoS attack: Denial of Service

SYN Flooding Countermeasures

- Defenses Against TCP SYN Flooding Attacks - The Internet Protocol Journal - Volume 9, Number 4
- IPSec
- SCTP – Stream Control Transmission Protocol
- TCP End-Host Countermeasures
- TCP Network-based Countermeasures

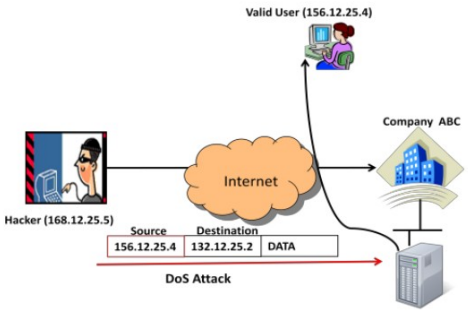
Countermeasures:
- use other protocols: IPSec / SCTP

End-Host Countermeasures
- Tweaking the settings of TCP servers:
* Increase TCP Backlog
* Reduce the SYN-RECEIVED Timer
* SYN Caches
* SYN Cookies

Network-Based Countermeasures
- Filtering
- Filtering & Proxies
- Firewall
- Active monitor

IP Spoofing

- Fake IP packets: identity concealing or impersonation
- DoS Attacks against legit business looking like it originates from legit users



IP spoofing – Faking the origin of packets to conceal the source or impersonate other user's machines

Characteristics:
- hard to trace back to the attacker

Defense against IP Spoofing

- Encrypted session in the router
- ACL: Acess Control Lists
- Filtering packets
- Using the upper layer checking

1. Encrypted session: trusted hosts communicate securely with local hosts
2. ACL used to block traffic
 * from the outside that originates from an internal IP address
 * from internal ip's going outside the network

3. Blocking incoming packets that do not meet security policy criteria

Filtering by destination port

4. Using sequence number from the TCP protocol making it harder to spoof.