TRANSPORT PROTOCOLS

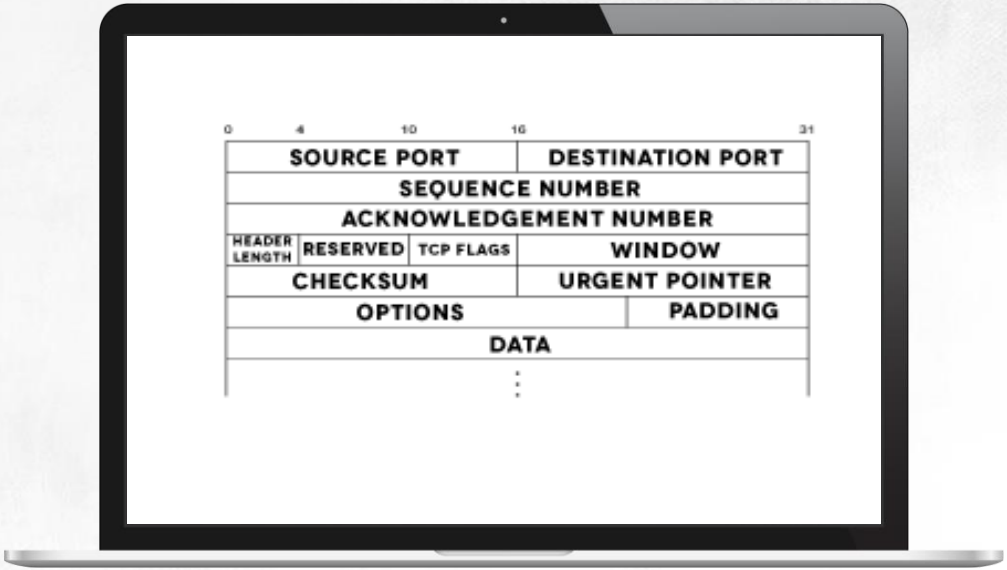
TRANSPORT LAYER

TCP

The transport layer protocols are responsible for establishing communication flow across programs running on peer computers

A socket allows packets to be identified uniquely. It consist of:

- **AN IP** address
- **A TRANSPORT LAYER** protocol (TCP or UDP)
- **PORT NUMBER**



TRANSPORT LAYER

TCP

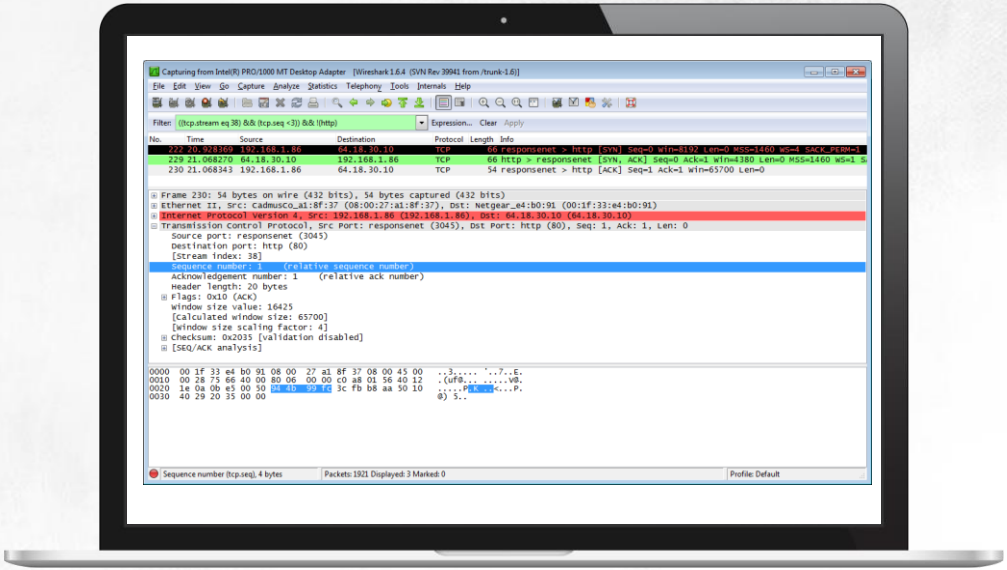
THE TRANSMISSION CONTROL PROTOCOL ESTABLISHES BIDIRECTIONAL SESSIONS

TCP guarantees that all transmitted packets will be delivered and in the sequence in which they were first forwarded

To ensure this:

WHEN A CONNECTION
is being established, TCP uses handshaking to set a session

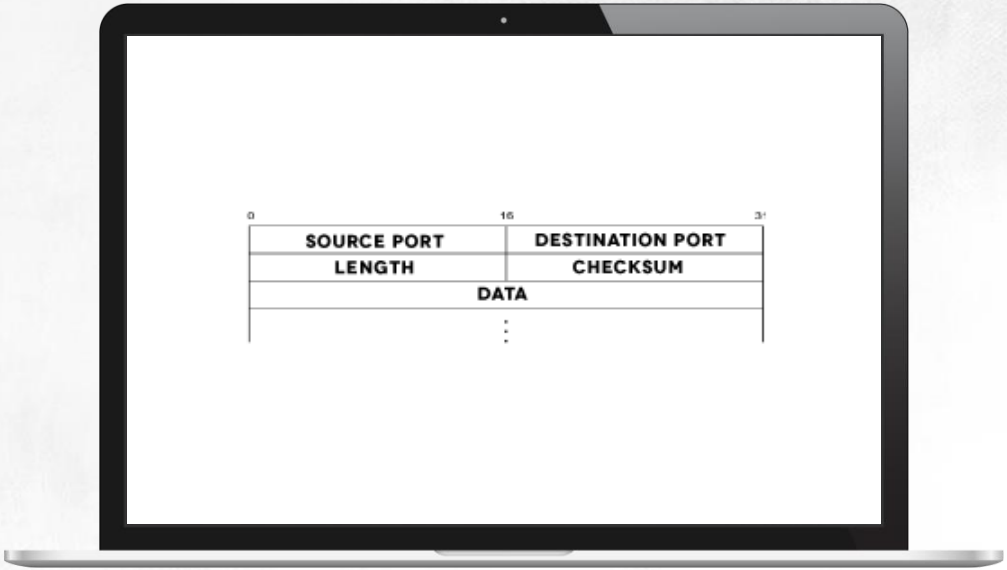
DATA FLOW
is recreated from incoming packets using a moving frame algorithm



TRANSPORT LAYER

UDP

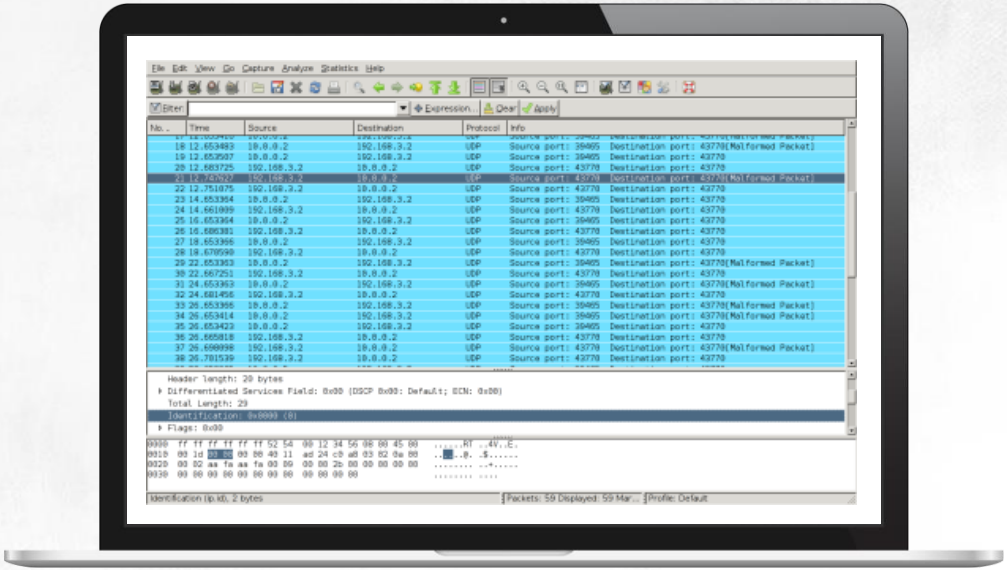
UDP
is a connectionless protocol, and won't protect you from packet loss



TRANSPORT LAYER

UDP

DUE TO THESE problems the UDP protocol is mostly used for services that transmit small data packets (one message long) asynchronously, like DNS servers



TRANSPORT LAYER

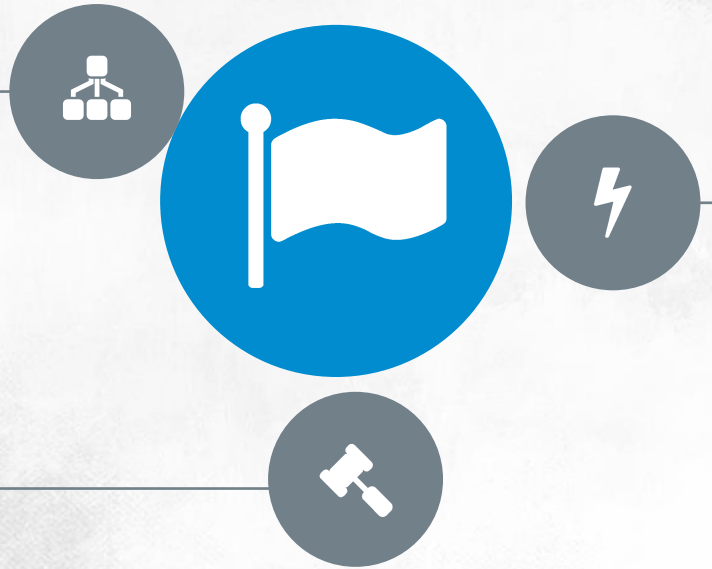
Threats: Enumerating Remote Computers

STILL

remaining, though, are the threats of using this layer's protocols to scan and enumerate remote computers' weak points

WHILE

While you could patch up the security of layer three using IP Sec, tightening security in layer four is as simple as blocking unused computer ports (using firewalls) and monitoring networks for scan attempts



THE NUMBER

one threat in layer four is the vulnerability that makes attackers able to determine next sequence numbers of messages transmitted in a TCP session, and it has been eliminated already. All modern operating systems are now using pseudorandom sequence numbers

EXERCISE

Transport Layer Attack

AN AUTOMATED ATTACK
on a badly-protected
computer using Metasploit

SESSION LAYER

THE DEFINITIONS OF the upper-layer functions in the OSI model are more blurred than the functions of their lower-layer counterparts

A SEPARATE MODULE focuses on authentication and authorisations mechanisms

SESSION LAYER

THE TYPICAL THREATS in layer five include session hijacking: the attacker gaining control over the session of an authenticated remote user. Session hijacking can be the interception and use of cookie-stored credentials or determining the session ID of another user and connecting to it

WHILE REMOTE USER authentication protocols have to be configured appropriately, securing the session layer is the responsibility of web application designers

THANKS