

# **[Workshop]**

# **Live network forensics and reversing network protocols**

# About me

- Programming → sysad → networking
- IT security for the past 10+ y
- Owner and Lead Researcher at Possible Security
- Hacking and breaking things
  - <http://kirils.org/>
  - <http://possiblesecurity.com/news/>



# Workshop contents

- Use-cases
  - Tools
  - Networking review
  - Setup
  - Reversing
  - Forensics
- + Lots of hands-on work

# Goal of NF & RNP

- Discover how a tool of interest communicates ultimately leading to full understanding of it's design
- Examples

# Tools

- netflow
- flow-tools
- ngrep
- wireshark
- kismet
- arping
- scapy
- Throwing Star Lan Tap
- HackRF One
- Wifi Pineapple TETRA
- TPLink TL-WN722N
- facedancer
- ...

# Capturing data locally

- Just make sure to enable promiscuous mode\* and you're all set.
  - \* do not drop packets not addressed to you
- Network card drivers have to support this.
- PRO TIP: Can also be used to capture USB data, GSM data, etc...\*
  - \* may require additional tools

# Capturing data remotely

- What if you're not physically present on the wire?
  - port mirroring
  - TaZmen Sniffer Protocol (TZSP)
  - capture with tcpdump and import a cap file later
    - `tcpdump -i eth0 -s 65535 -w blah`



# ISO/OSI+DoD model



possible.lv

OSI (Open Source Interconnection) 7 Layer Model

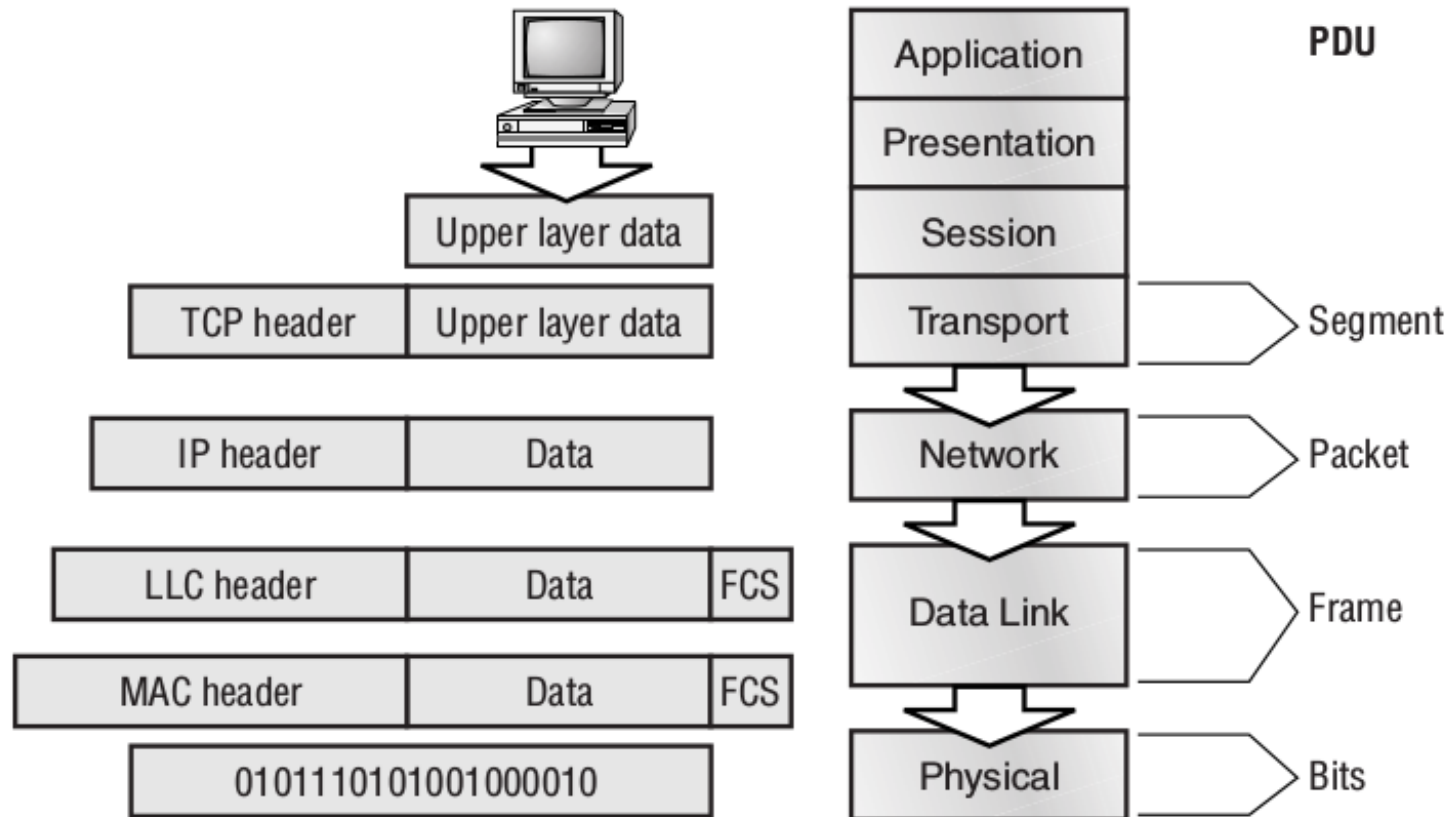
Layer	Application/Example	Central Device/ Protocols	DOD4 Model
<b>Application (7)</b> Serves as the window for users and application processes to access the network services.	<b>End User layer</b> Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	<b>User Applications</b>  SMTP	<b>Process</b>
<b>Presentation (6)</b> Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	<b>Syntax layer</b> encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT	
<b>Session (5)</b> Allows session establishment between processes running on different stations.	<b>Synch &amp; send to ports</b> (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	<b>Logical Ports</b>  RPC/SQL/NFS NetBIOS names	
<b>Transport (4)</b> Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	<b>TCP</b> Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	<b>PACKET FILTERING</b>  TCP/SPX/UDP	<b>Host to Host</b>
<b>Network (3)</b> Controls the operations of the subnet, deciding which physical path the data takes.	<b>Packets</b> ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		<b>Routers</b>  IP/IPX/ICMP
<b>Data Link (2)</b> Provides error-free transfer of data frames from one node to another over the Physical layer.	<b>Frames</b> ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	<b>Switch Bridge WAP</b> PPP/SLIP	<b>Land Based Layers</b>  <b>Network</b>
<b>Physical (1)</b> Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	<b>Physical structure</b> Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	<b>Hub</b>	

GATEWAY

Can be used on all layers

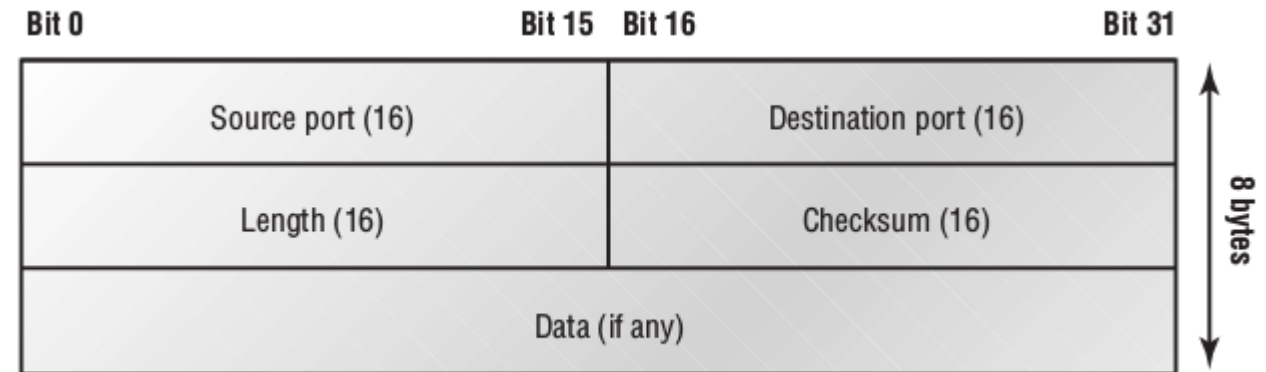


# Encapsulation



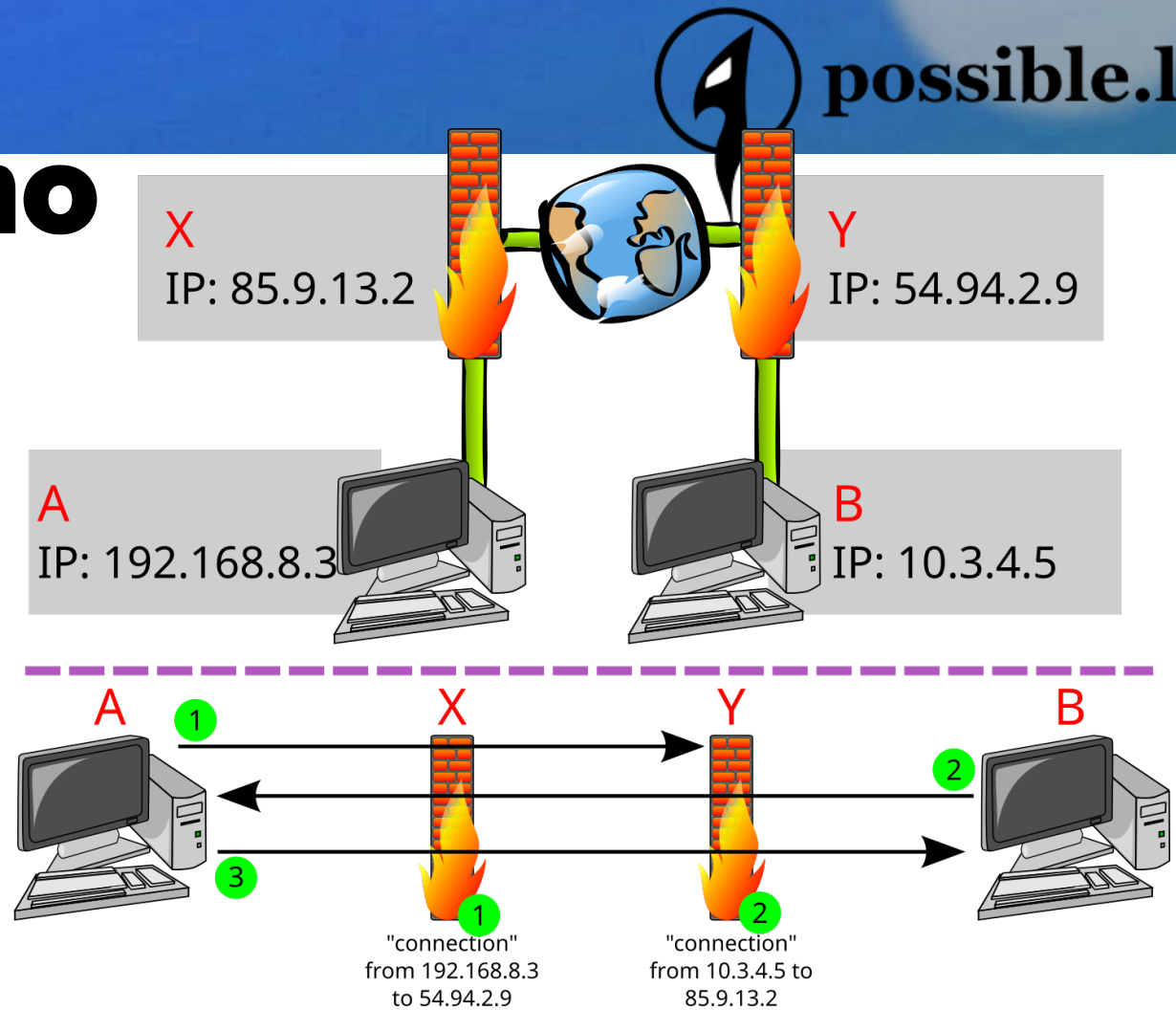
# User Datagram Protocol

- Stateless, transaction-oriented
- "Best effort" transport
- Notable features include:
  - Minimalist design
  - No control
  - No retransmissions



# Fun demo

- Punching holes in firewalls and NAT routers with UDP



# Setup

- 1) Analysis target
- 2) Analysis machine
- 3) Arrangement to intercept and decrypt data

# Flow tools

- CALEA
- netflow, tzsp
- tcpdump
- ngrep
- → aplay