possible.lv

[Workshop]
Live network forensics and reversing network protocols

@KirilsSolovjovs

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

possible.lv

- Use-cases
- Tools
- Networking review
- Setup
- Reversing
- Forensics

+ Lots of hands-on work

Goal of NF & RNP

possible.lv

- 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
- ...

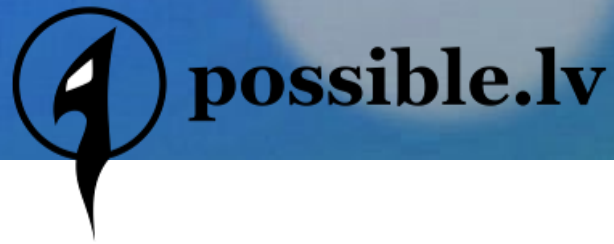
Capturing data locally

possible.lv

- 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*

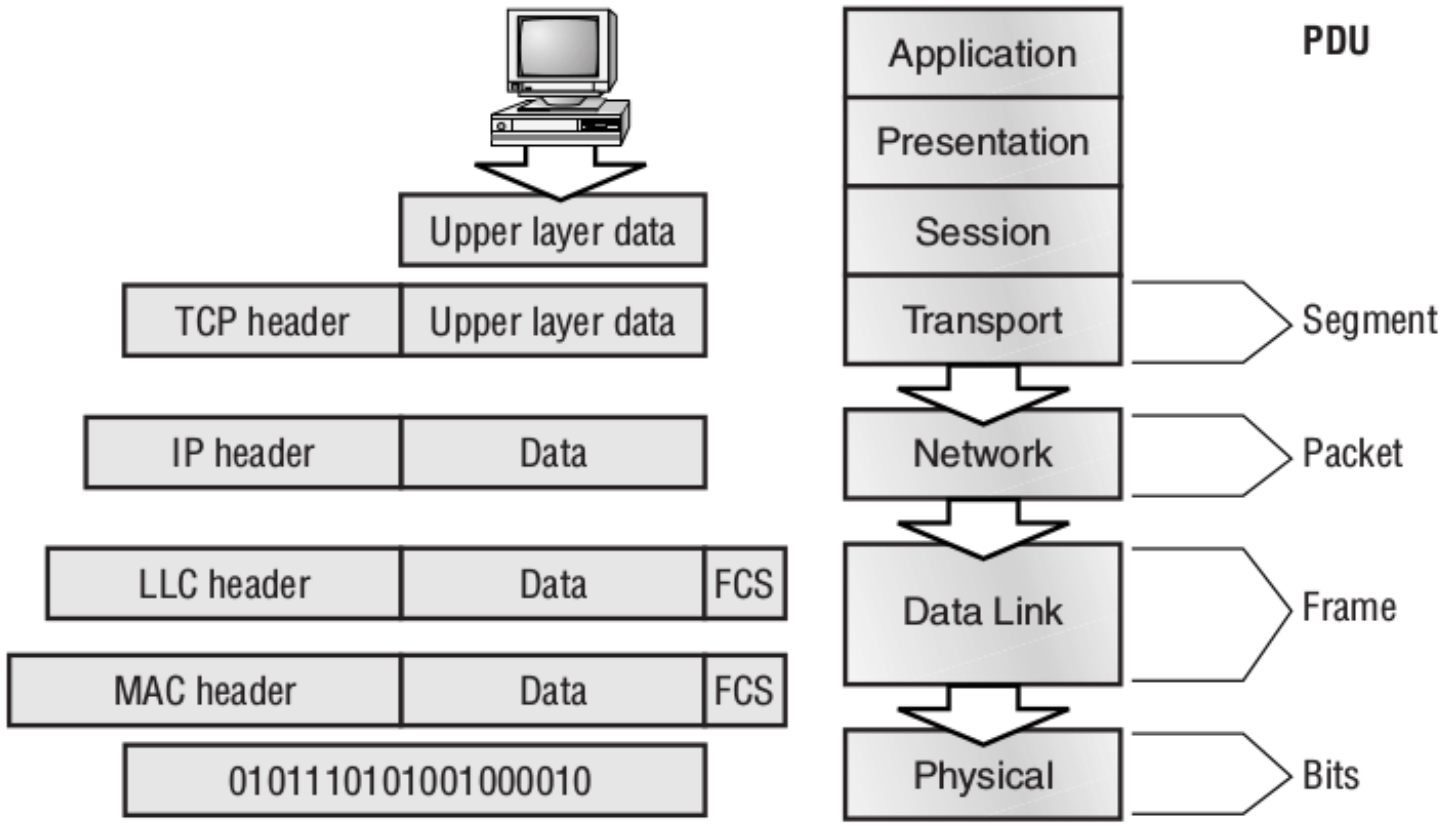
ISO/OSI+DoD model

OSI (Open Source Interconnection) 7 Layer Model

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

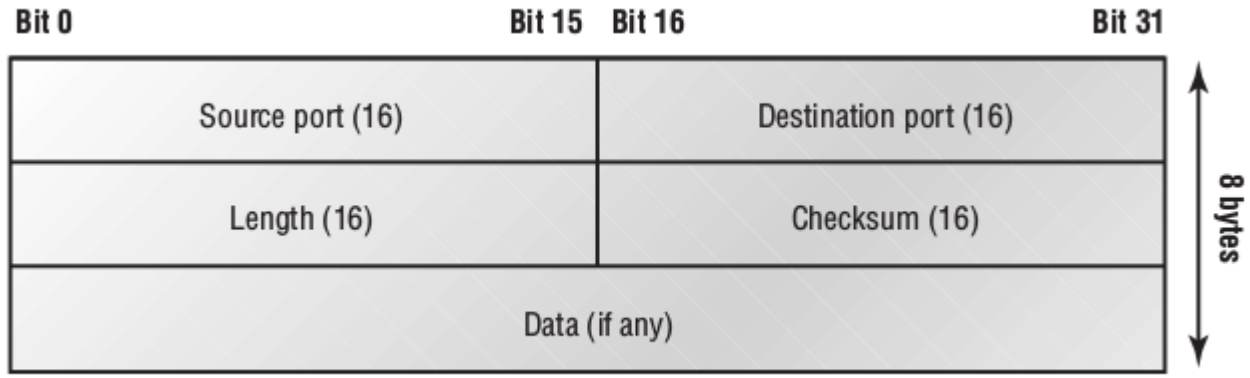
GATEWAY: Can be used on all layers

Encapsulation



User Datagram Protocol

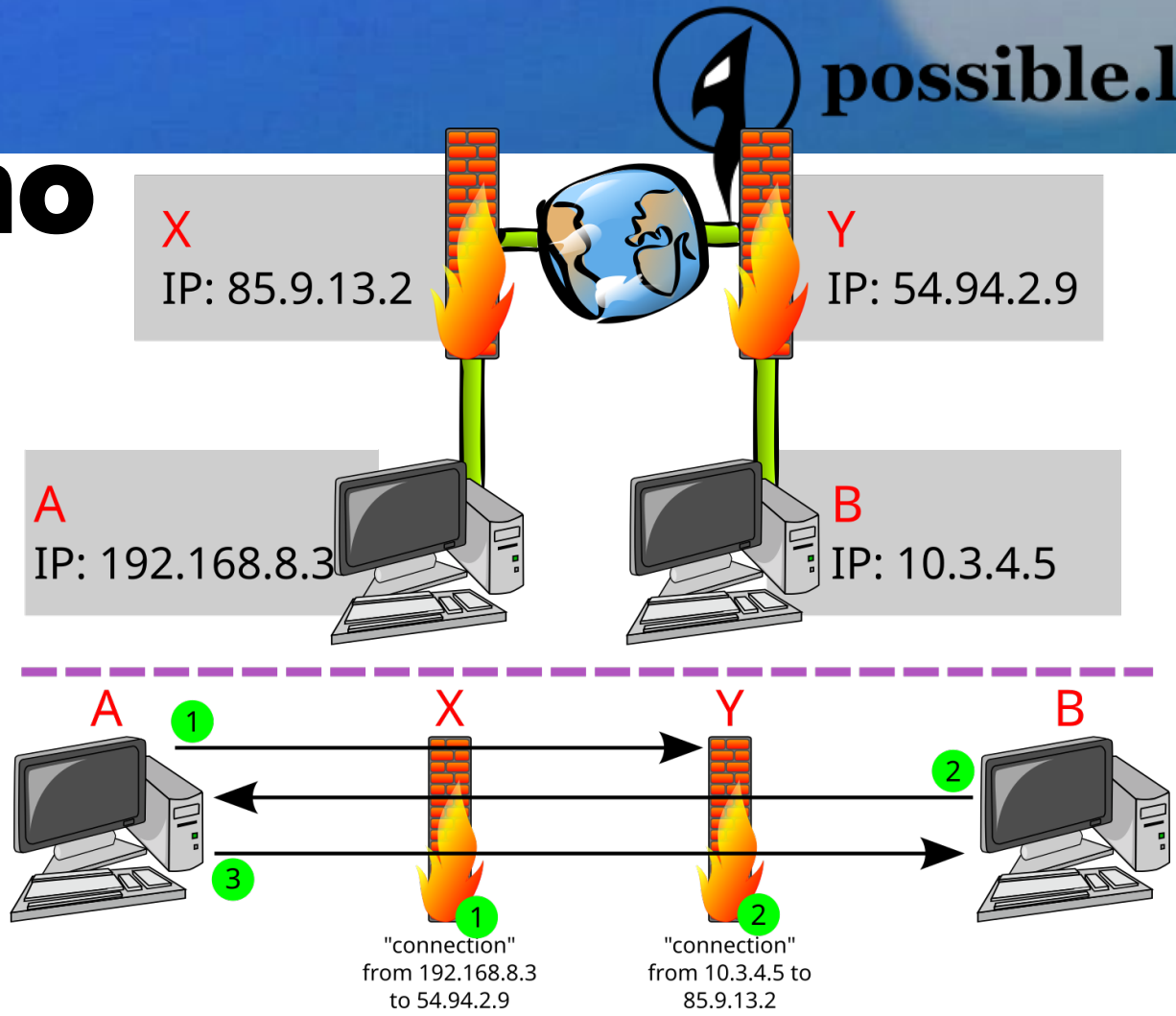
- Stateless, transaction-oriented
- "Best effort" transport
- Notable features include:
  - Minimalist design
  - No control
  - No retransmissions



possible.lv

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