CS4238: Computer Security Practice

Lecture 2: Networking Overview & Configuration, Attack Framework, Reconnaissance

Outline

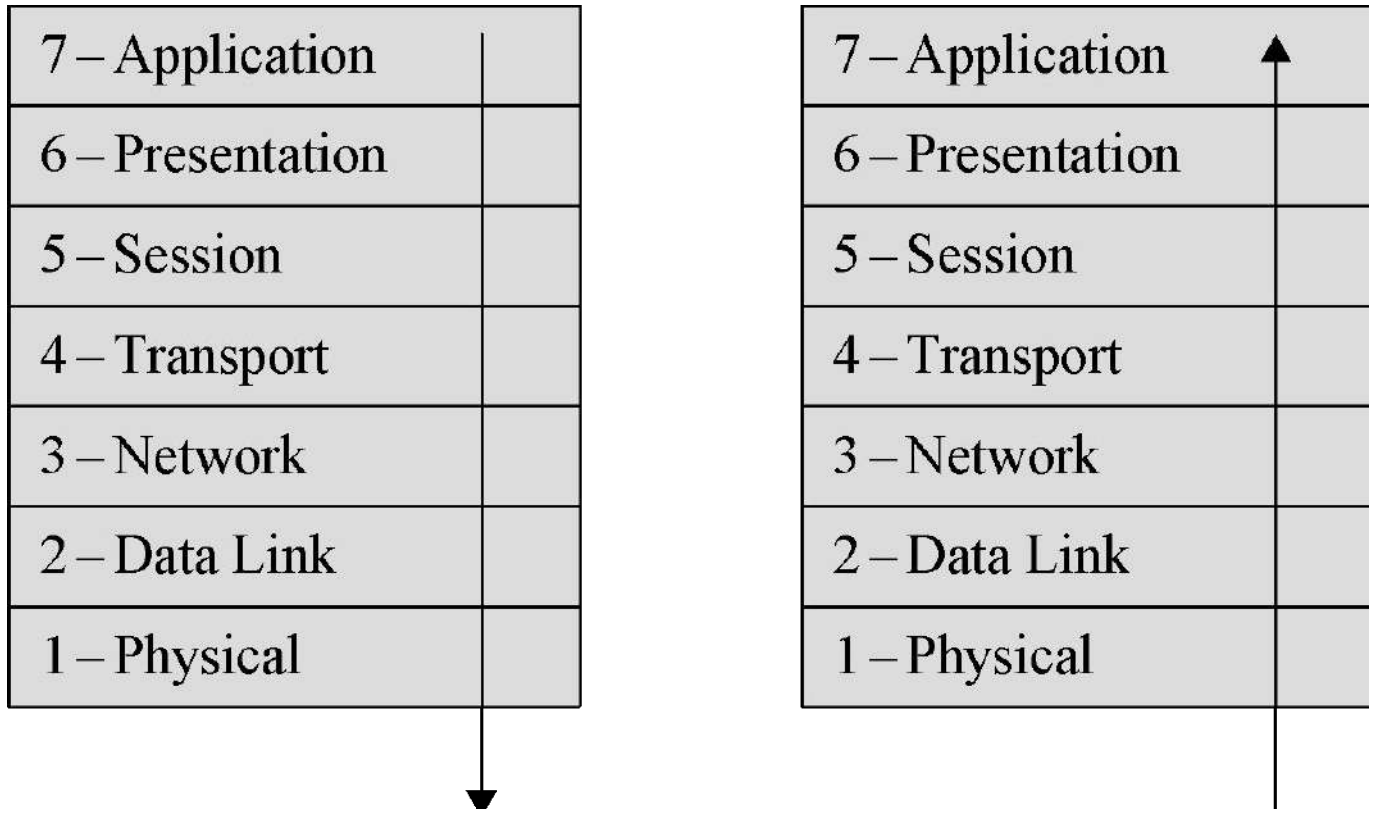
- Networking Overview
- Network Configuration: Linux desktop
- [Network Configuration: Linux router]
- Networking in VirtualBox (VMM)
- Attack Framework
- Reconnaissance

Networking Overview

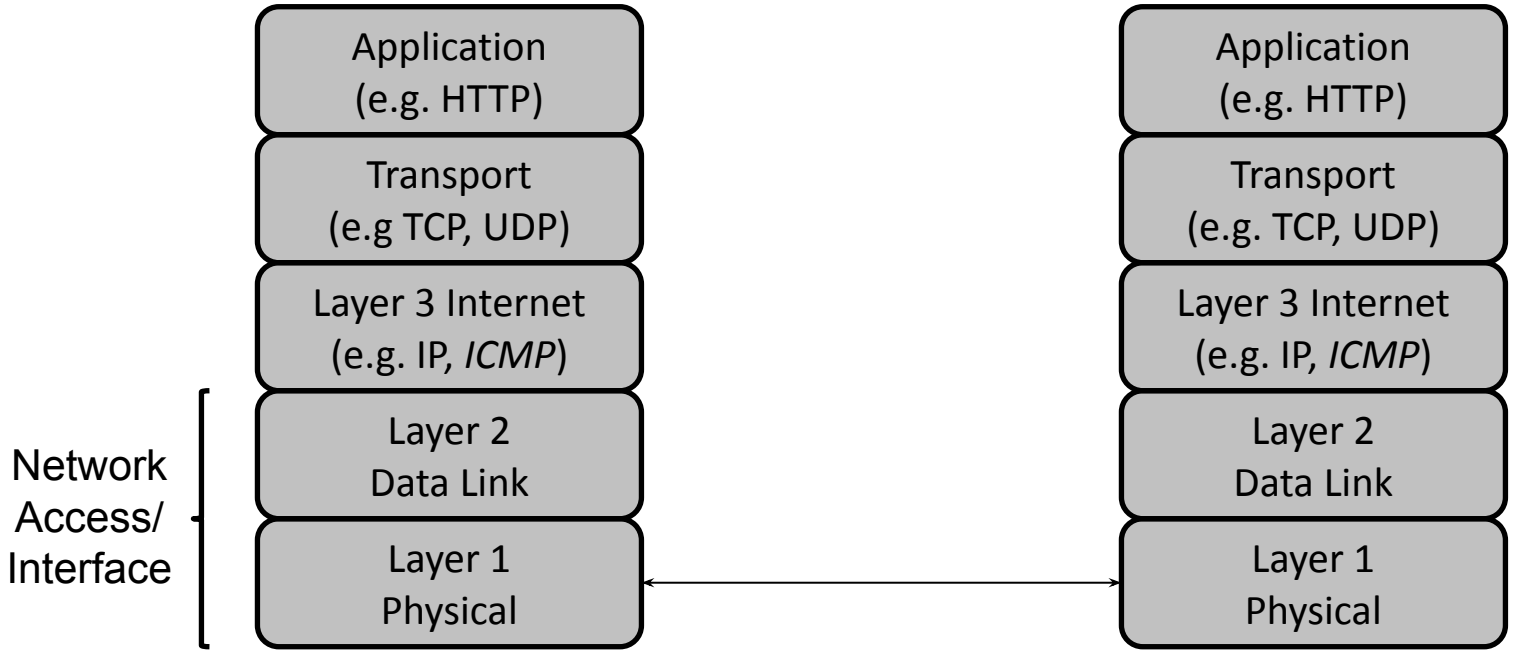
(Chapter 2 of the Reference book 1)

The OSI Seven-Layer Network Model

a conceptual/reference model that standardizes the *communication functions* of a telecommunication/computing system

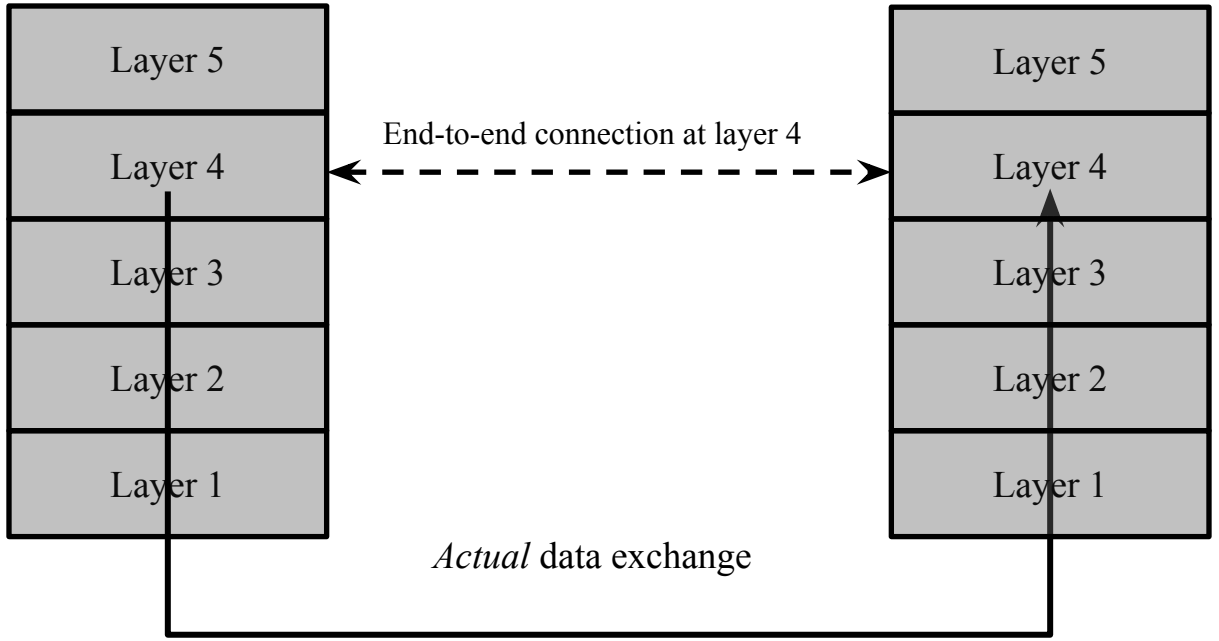


The Internet (TCP/IP) Reference Model

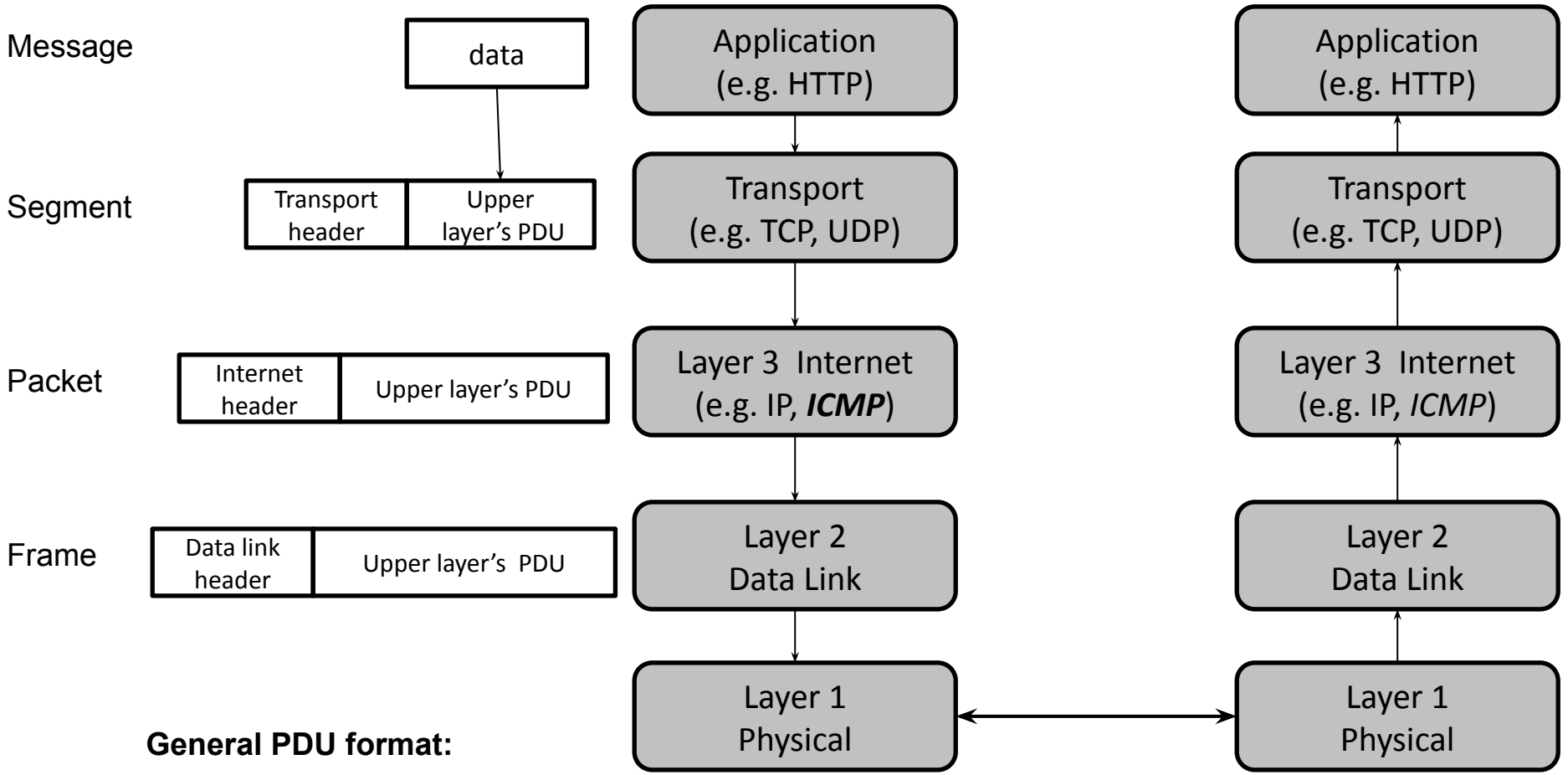


Why Network Layering?

- It partitions a complex communication system into several abstraction layers
- The peer entities at the same layer N “conceptually” communicate with each other by executing a protocol at that layer



Network Layers and Message Encapsulation

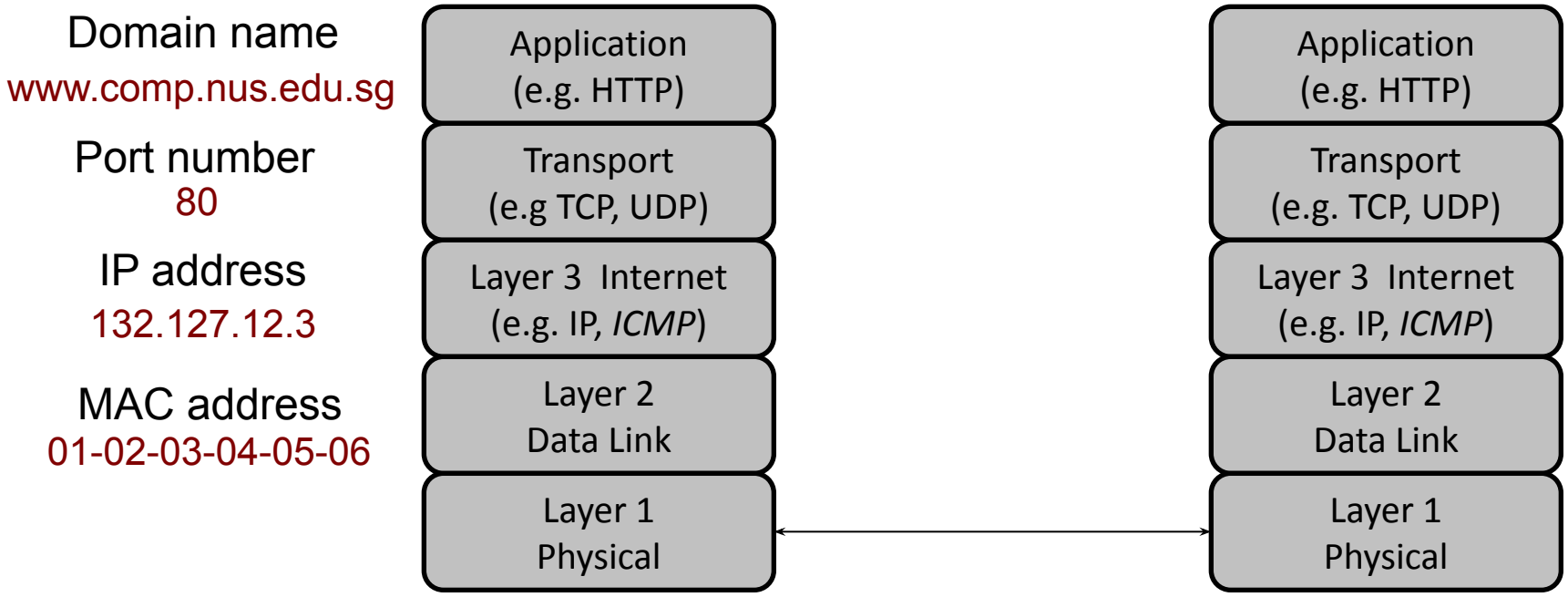


General PDU format:

Header: meta data **Payload**: the message/information intended to be sent

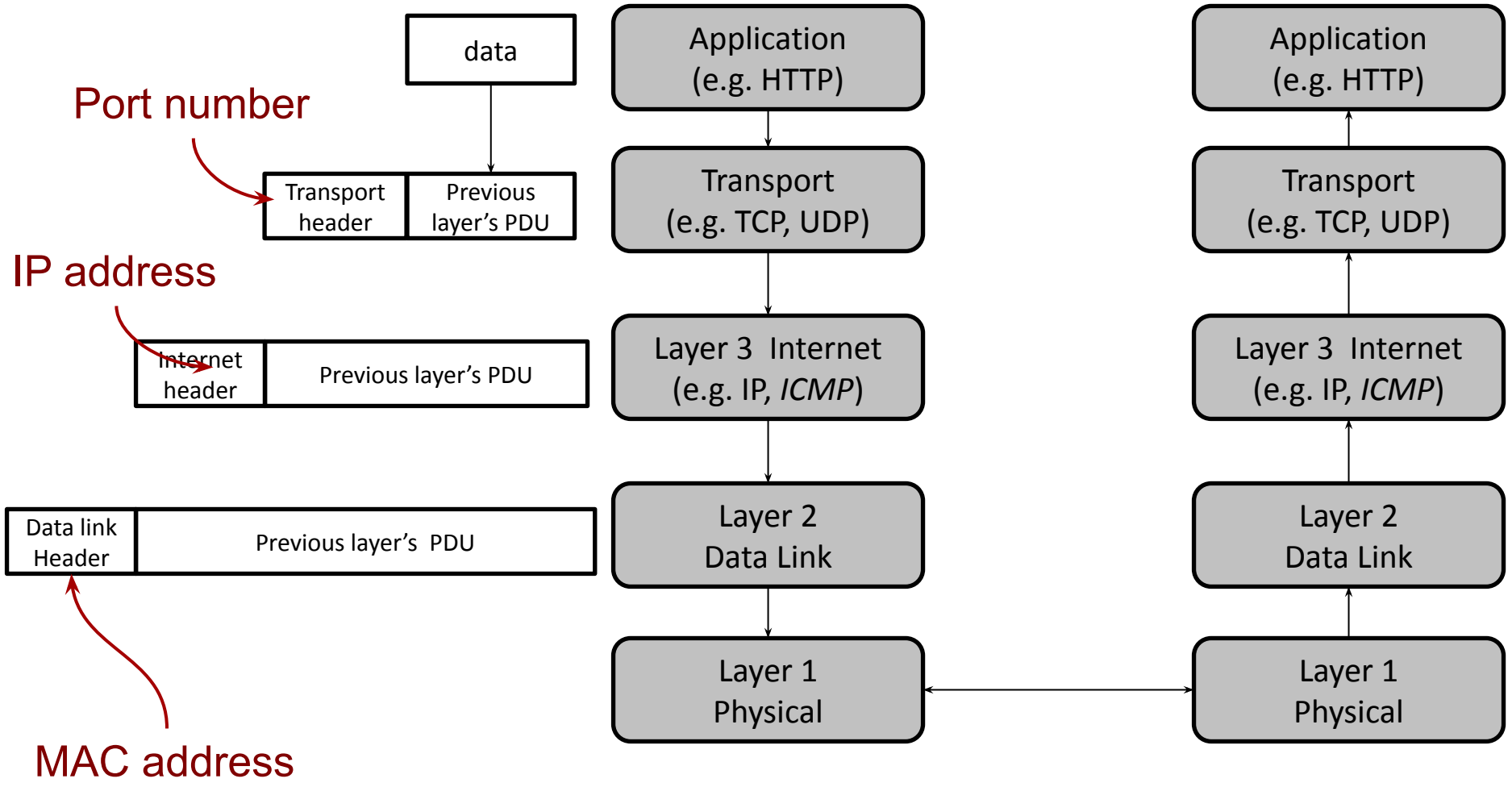
Internet Layers: Different Addressing Schemes

- Different **addressing schemes** at different layers



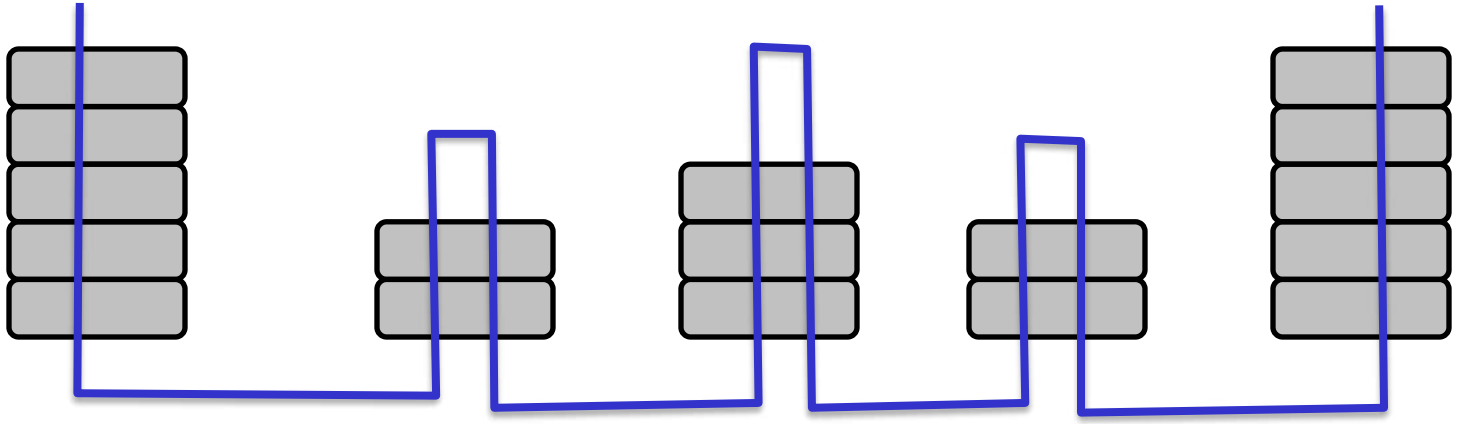
Note: MAC (medium access control) is *not* to be confused with crypto's MAC

Addressing at Various Layers



Multiple Hops from Sender to Destination

- Note that data may go through **multiple hops**
- Can you guess each device type in the diagram below?
- Some networking devices: router, switch, hub, repeater

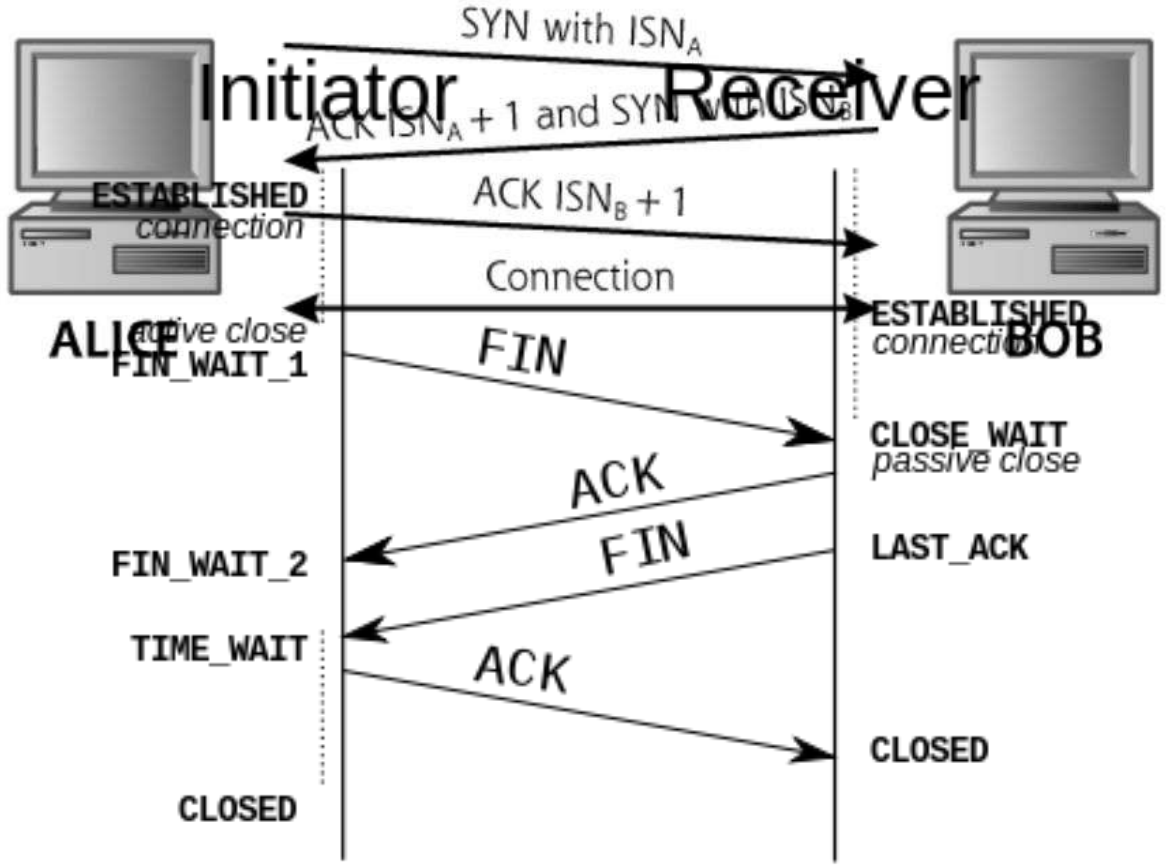


Relevant Networking Concepts

- TCP/IP Layers
  - Application
  - Transport
  - Network
  - Data Link
  - Physical
- TCP and UDP
- IP and ICMP
- Routing
  - NAT
- Firewall
- Ethernet and 802.11
  - ARP
- SSL and TLS
- IPSec and VPN

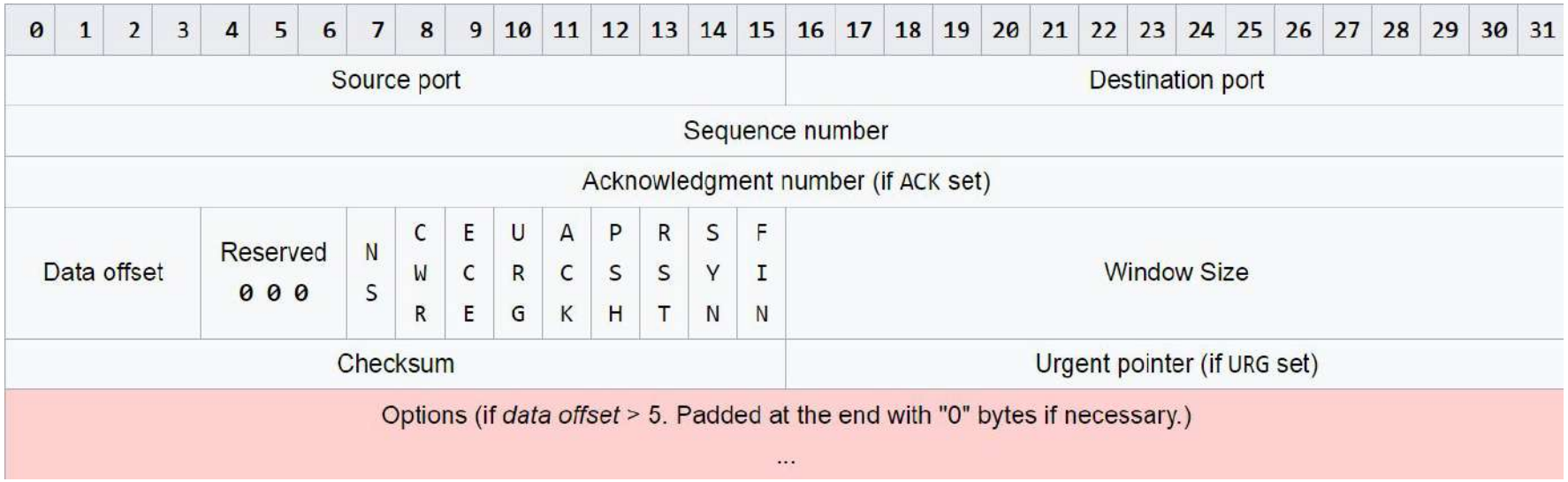
TCP vs UDP

- UDP is connection-less:
  - No mechanism for feedback
  - Best-effort Delivery (lossy!)
  - Good for Apps that are ok with packet losses!
- TCP is connection-oriented:
  - Has Feedback mechanism
  - Lossless transmission
  - Good for Apps that prioritize quality over speed.



TCP

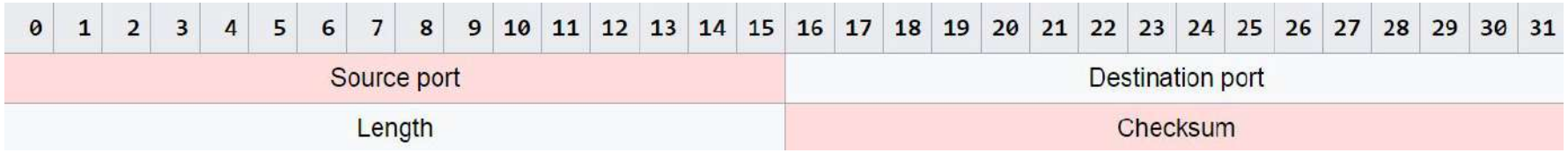
- TCP header format:



Source: Wikipedia

UDP

- Connectionless transport protocol
- UDP header format:



- Used among others by DNS (port 53), BOOTP/DHCP (port 67 & 68), TFTP (port 69), SNMP (port 161)

IP

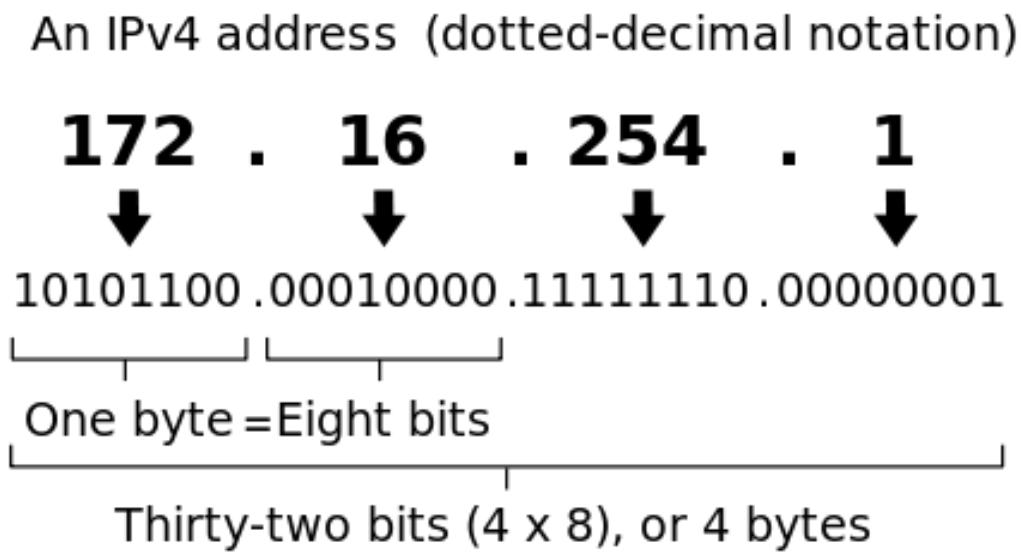
- Importance of IP:
  - “Anything over IP and IP over anything”
  - The waist (glue point) of protocol-stack’s hourglass
- IP header format:

Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Version				IHL				DSCP						ECN		Total Length															
32	Identification																Flags			Fragment Offset											
64	Time To Live								Protocol								Header Checksum															
96	Source IP Address																															
128	Destination IP Address																															
160	Options (if IHL > 5)																															
192																																
224																																
256																																

Source: Wikipedia

IPv4 Address

- Dotted-decimal notation:
- **Network address** and **host address components**
- Classful network architecture (1981-1993):
- Classless Inter-Domain Routing (CIDR):
  - CIDR notation (e.g. 192.168.2.0/24)



IPv4 Address

- Special IP addresses:
  - Localhost address: 127.0.0.1
  - Private addresses:
    - 10.0.0.0 – 10.255.255.255: 24-bit host ID (24-bit block)
    - 172.16.0.0 – 172.31.255.255: 20-bit host ID (20-bit block)
    - 192.168.0.0 – 192.168.255.255: 16-bit host ID (16-bit block)
    - Not routable on the public Internet
    - Usually used together with NAT or proxy
  - Automatic Private IP Addressing (APIPA) or auto-IP address: 169.254.1.0 – 169.254.254.255
    - E.g. when DHCP server is unavailable

Protocols on Top of IP

Some of the common payload protocols are:

Protocol Number	Protocol Name	Abbreviation
1	Internet Control Message Protocol	ICMP
2	Internet Group Management Protocol	IGMP
6	Transmission Control Protocol	TCP
17	User Datagram Protocol	UDP
41	IPv6 encapsulation	ENCAP
89	Open Shortest Path First	OSPF
132	Stream Control Transmission Protocol	SCTP

Source: Wikipedia

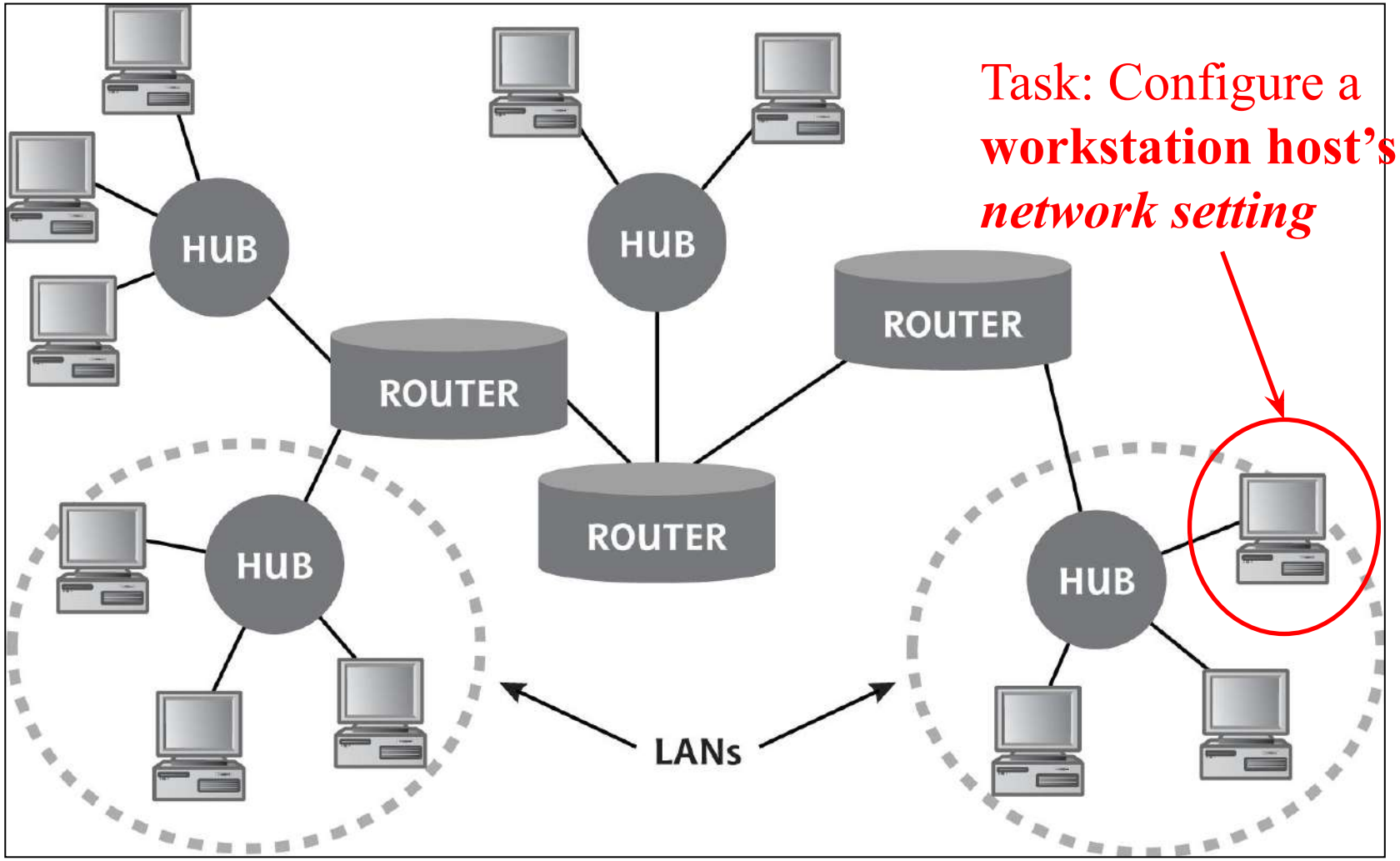
ICMP

- A supporting protocol for sending error messages and operational information
- Used by ping and traceroute tools
- ICMP header format:

- Some control messages (with their ICMP Types):
  - Echo Reply (0), Destination Unreachable (3), Redirect Message (5), Echo Request (8), Time Exceeded (11), Parameter Problem: Bad IP header (12)

Network Configuration: Linux Desktop

Setting up a Computer

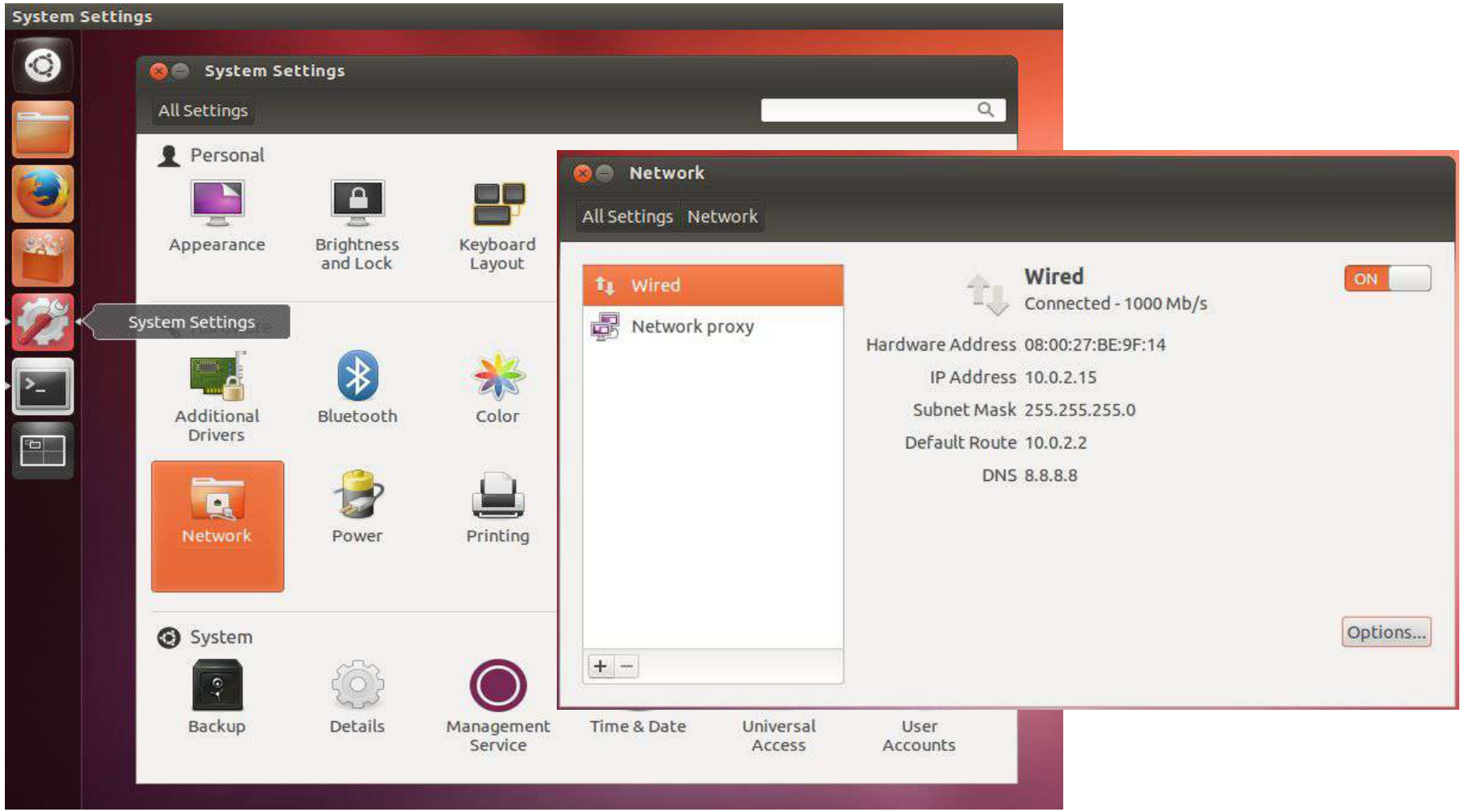


Computer Network Configuration

- Information needed to connect a computer to the Internet:
  - IP Address
  - Network mask
  - Gateway
  - DNS server
- How to obtain such information?
  - Automatic setting through DHCP
  - Manual setting

Configuration in Ubuntu Linux

- “System Settings” □ “Network”

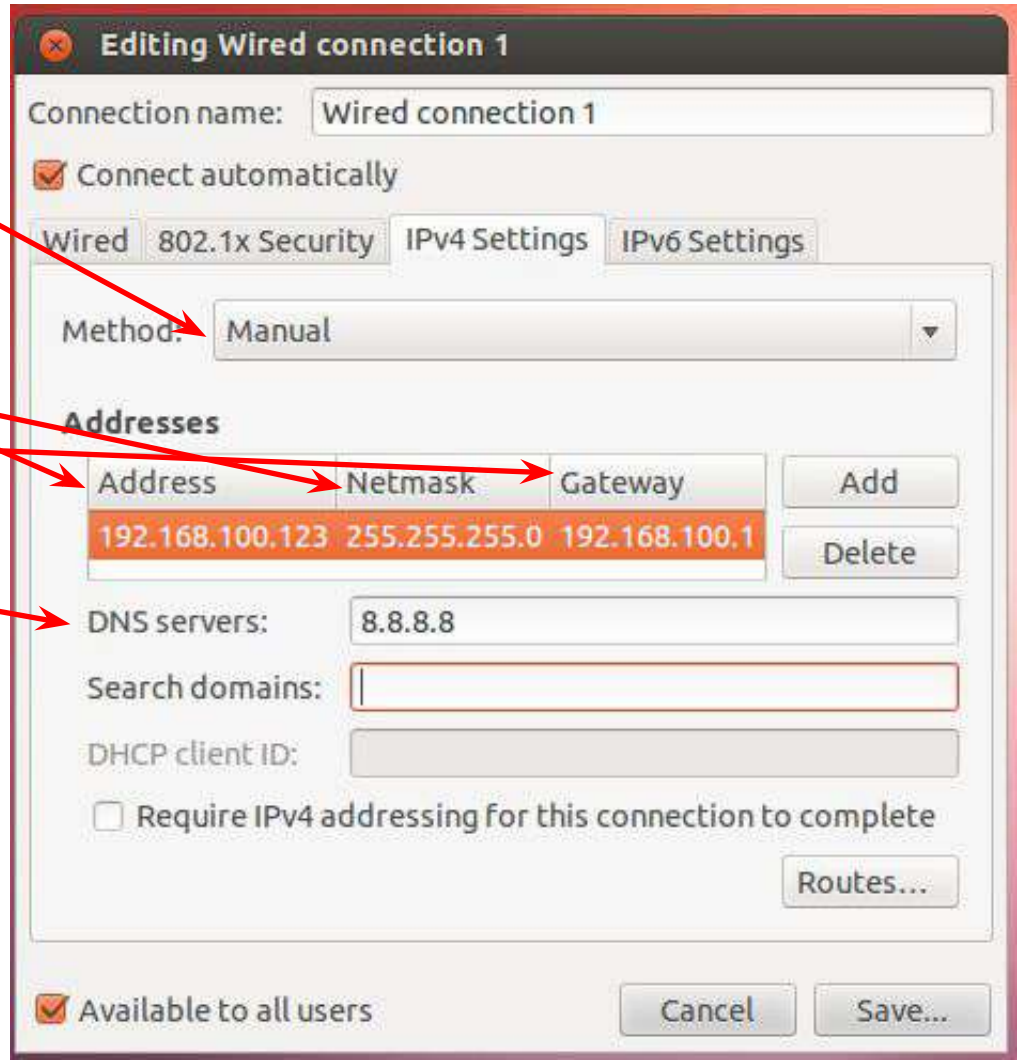


Automatic Network Settings (DHCP)

- Select your network interface, and click the “Options” button
- Select “IPv4 Settings” tab
- Set method to “Automatic (DHCP)” in order to automatically obtain network settings from DHCP server

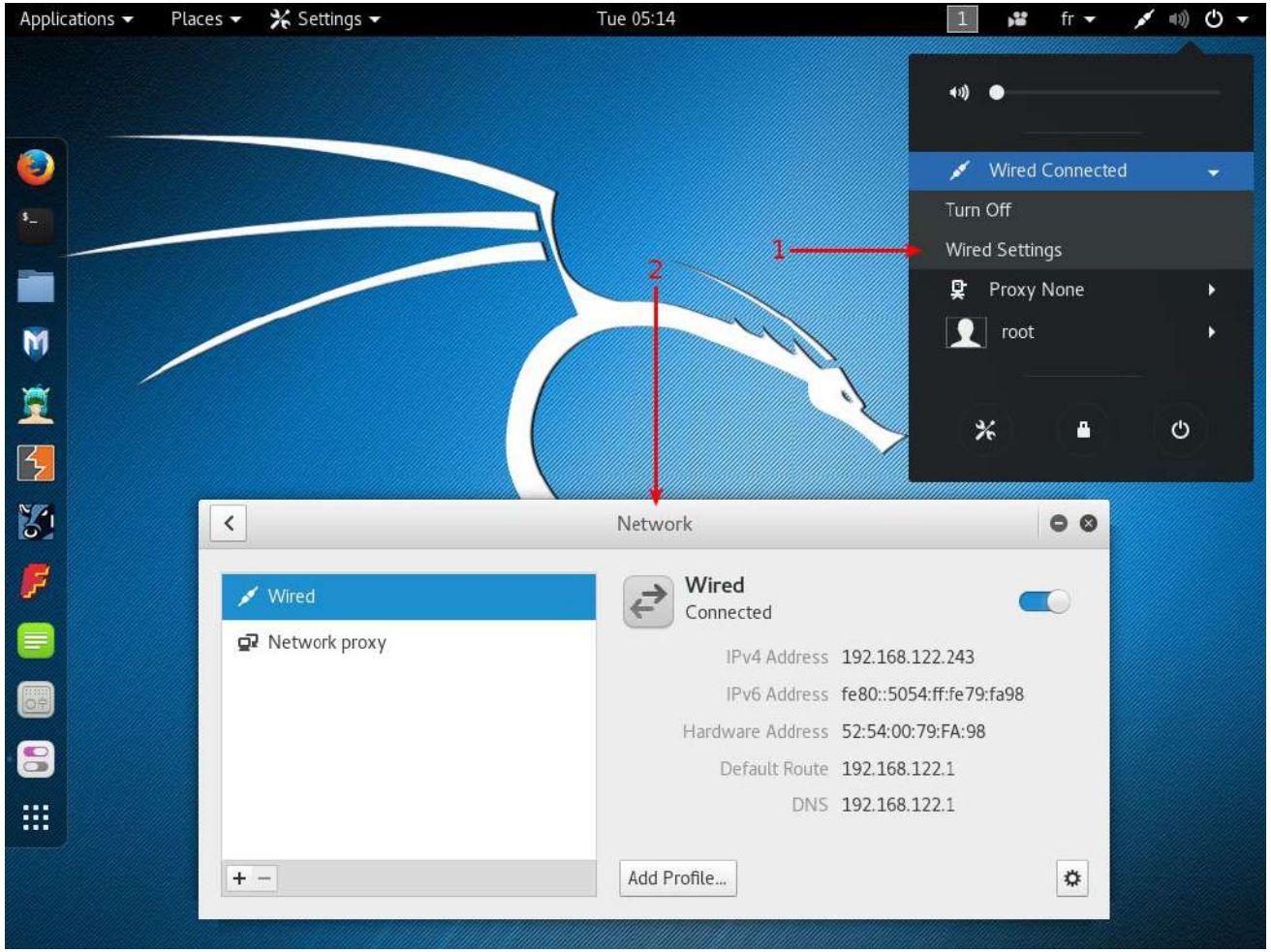
Manual Network Settings

- Set method to “Manual”
  - IP Address
  - Network mask
  - Gateway
  - DNS server



Configuration in Kali Linux

- NetworkManager setting interface:



Source: "Kali Linux Revealed", Hertzog et al., 2017

Network Setting File and Commands

- Manual network setting steps:
  - **`ifdown`** `<network-device>`
  - **`Modify /etc/network/interfaces`**
  - **`ifup`** `<network-device>`
- Setting `/etc/network/interfaces` for a plain DHCP configuration:

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
```

Network Setting File and Commands

- Setting /etc/network/interfaces for a static IP configuration:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.0.3
netmask 255.255.255.0
broadcast 192.168.0.255
network 192.168.0.0
gateway 192.168.0.1
```

Configuring Kali Linux: Services

- Managing services:
  - E.g. ssh:
    - `systemctl start ssh`
    - `systemctl enable ssh`
    - `systemctl reload ssh`
  - E.g. Apache:
    - `systemctl start apache2`
    - `a2enmod module`
    - `a2dismod module`

Some Useful Commands

- Check and start/stop network interfaces using ifconfig :
  - List network interfaces:
    - All interfaces (up and down) whose drivers are loaded:

```
ifconfig -a
```

    - All interfaces that are up:

```
ifconfig
```

    - A particular interface (e.g. eth0):

```
ifconfig eth0
```

  - Start and stop a network interface (e.g. eth0):

```
ifconfig eth0 down
ifconfig eth0 up
```

Consistent Network Device Naming

- A convention for naming Ethernet adapters in Linux
- Created ~2009 to replace the old ethX naming:
  - Issues on multihomed machines
  - NICs would be named based on the order in which they were found by the kernel as it booted
- Device naming rules:
  - Onboard interfaces at firmware index nos: eno[1-N]
  - Interfaces at PCI Express hotplug slot nos: ens[1-N]
  - Adapters in the specified PCI slot, with slot index no on the adapter enp<PCI-slot>s<card-index-no>

Some Useful Commands

- Newer ip command from iproute2:
  - List network interfaces:
    - All interfaces (up and down) whose drivers are loaded: `ip addr show`
    - A particular interface (e.g. eth0): `ip addr show eth0`
    - IPv4 or IPv6 addresses only: `ip -4|-6 addr show`
  - Stop and start a network interface (e.g. eth0):

```
ip link set eth0 down
ip link set eth0 up
```

Linux Network Commands:Deprecated and New

- Old-style network utilities from net-tools (ifconfig, route, ...) are supposed to be replaced by iproute2:
- ifconfig → ip
- route → ip
- arp → ip
- netstat → ss (socket statistics)

- Sample command comparisons:
  - `route -n` **vs** `ip route show`
  - `route add default gw` <gateway-IP-addr> **vs**
    `ip route add default via` <gateway-IP-addr>

References: ip Command

- https://phoenixnap.com/kb/linux-ip-command-examples
- https://www.howtogeek.com/657911/how-to-use-the-ip-command-on-linux/

[Network Configuration: Linux Router]

(To be discussed in Lecture 6)

Networking in VirtualBox (VMM)

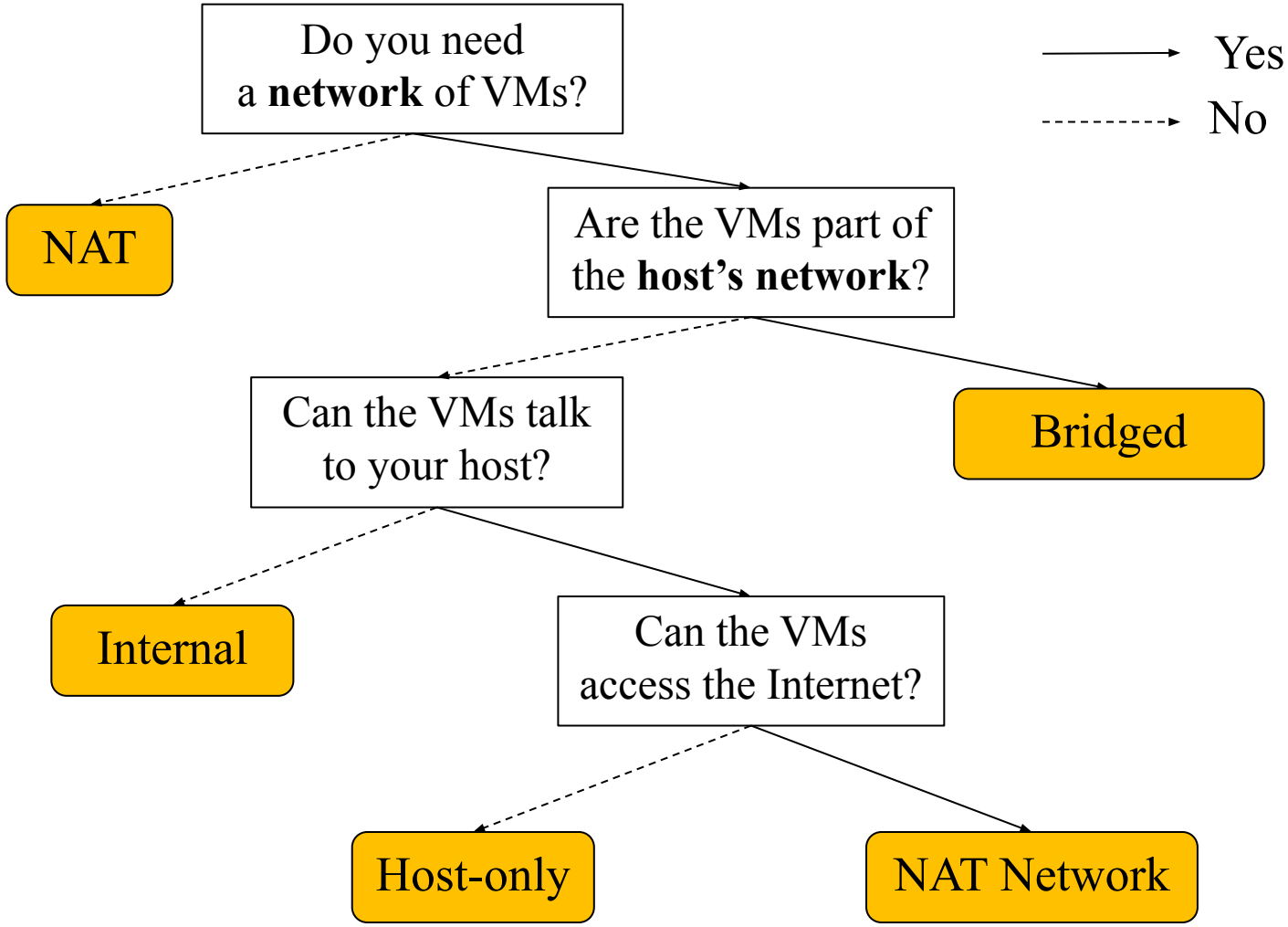
Networking in VirtualBox (Updated)

- Various networking modes in VirtualBox:

Mode	VM→Host	VM←Host	VM1↔VM2	VM→Net/LAN	VM←Net/LAN
Host-only	+	+	+	–	–
Internal	–	–	+	–	–
Bridged	+	+	+	+	+
NAT	+	Port forward	–	+	Port forward
NATservice	+	Port forward	+	+	Port forward

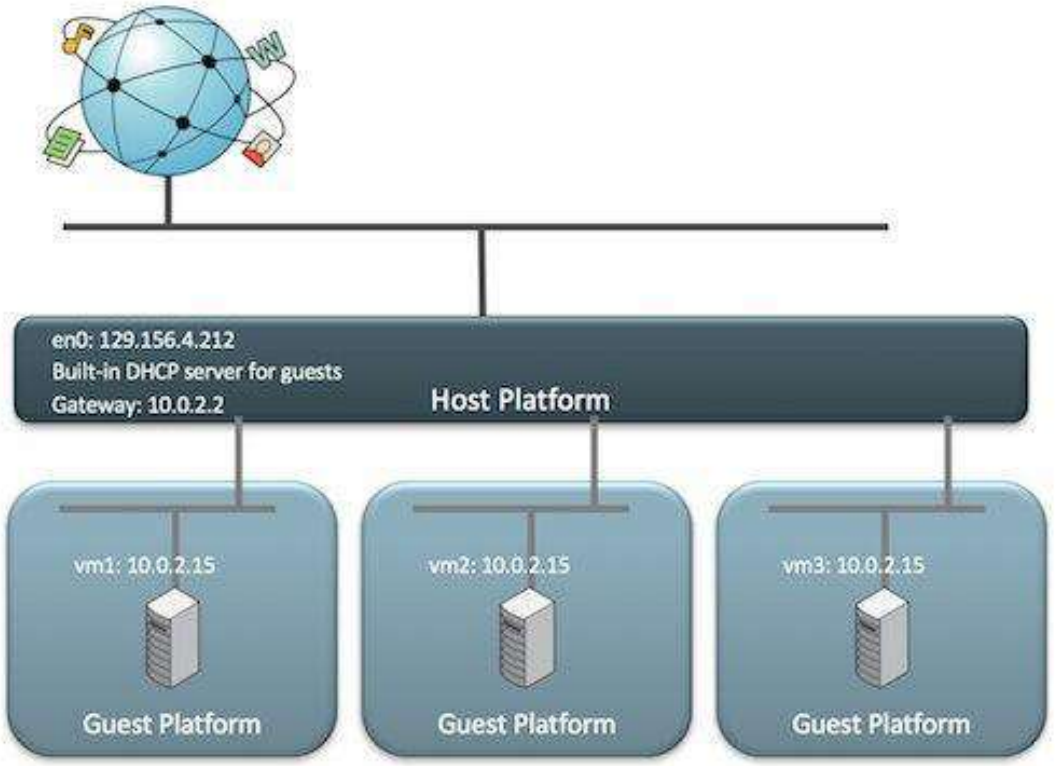
- Question: How do you choose a suitable networking mode for your need?

Networking in VirtualBox: Selection



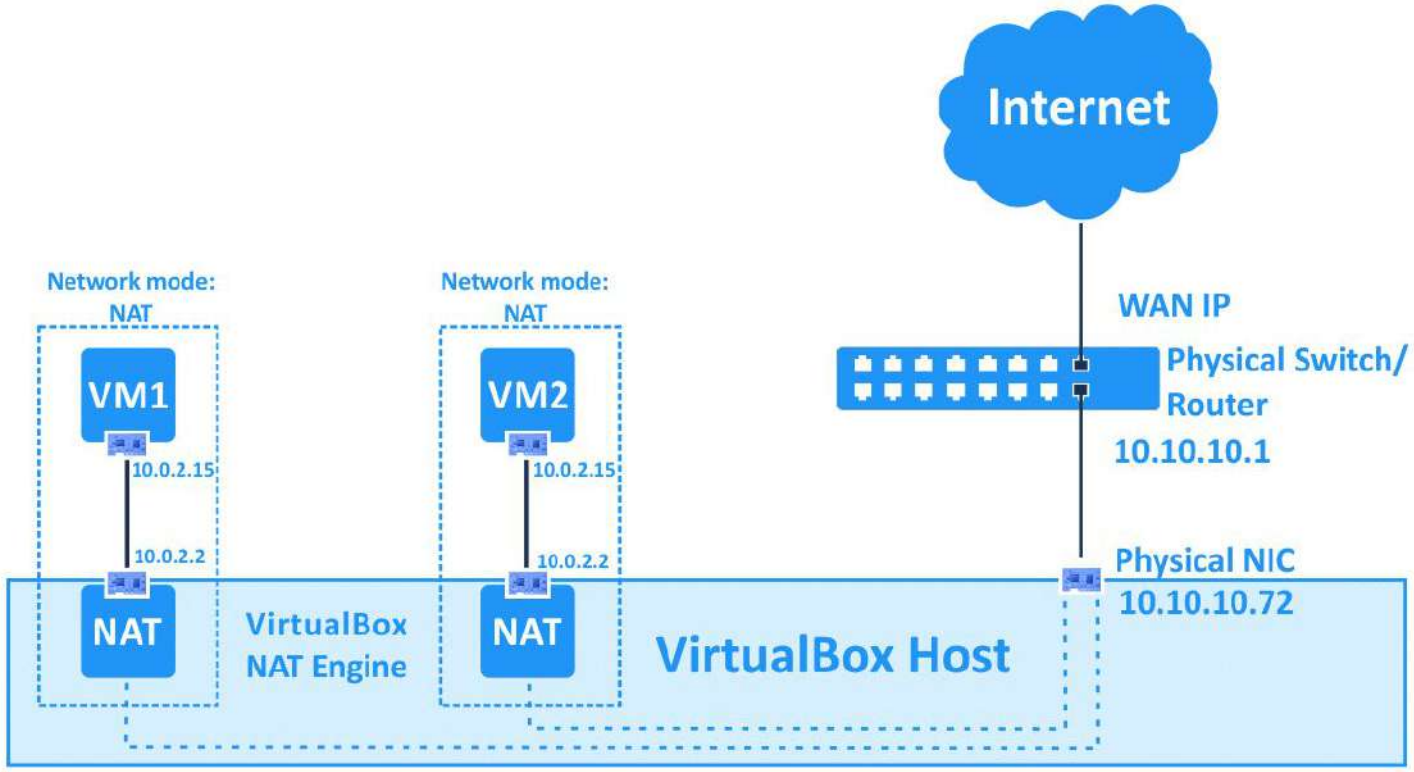
Additional Explanation: Illustration

- See: https://blogs.oracle.com/scoter/networking-in-virtualbox-v2
- NAT mode:



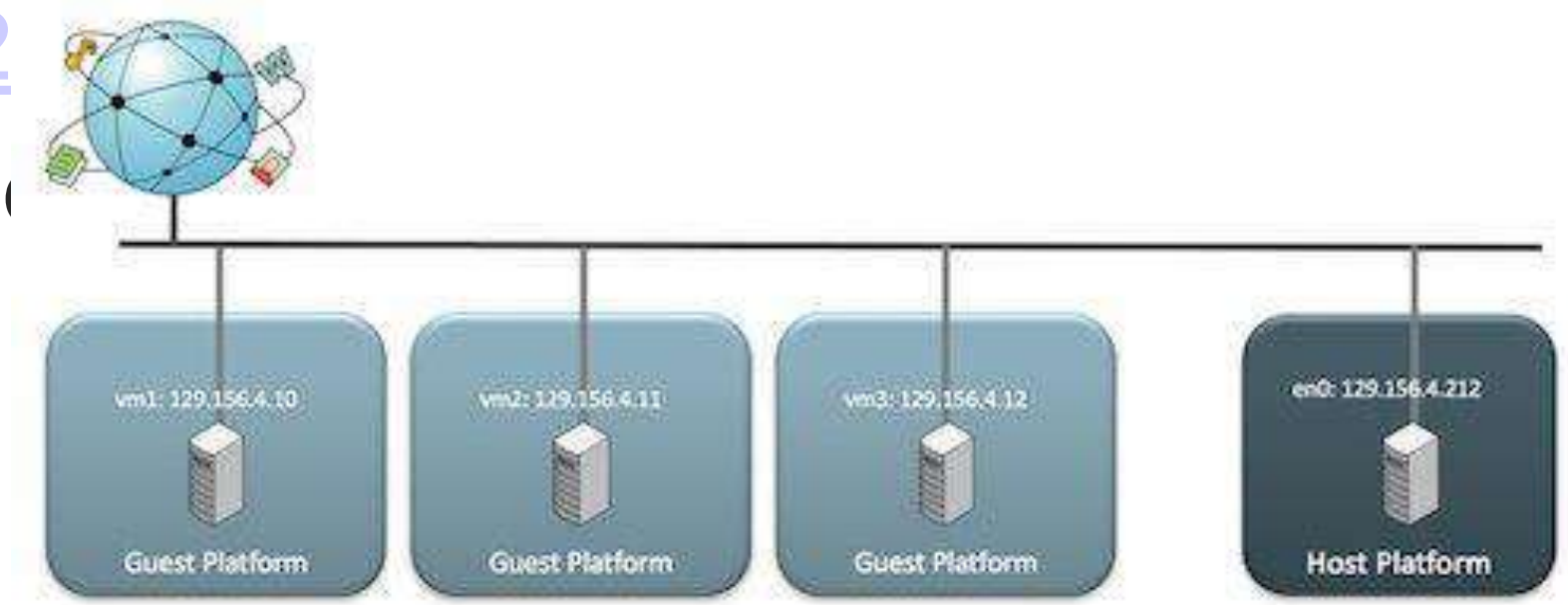
Additional Explanation: Illustration

- See: https://www.nakivo.com/blog/virtualbox-network-setting-guide/
- NAT mode:



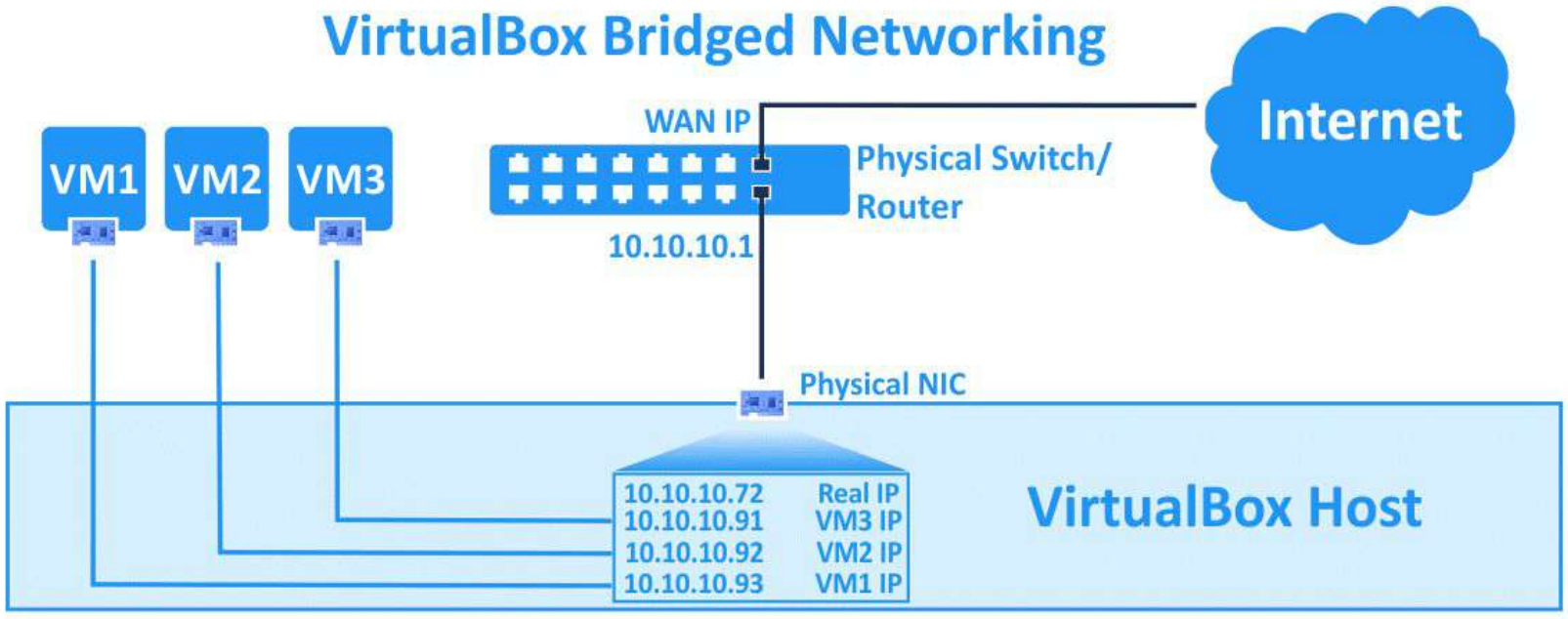
Additional Explanation: Illustration

- See: https://blogs.oracle.com/scoter/networking-in-virtualbox-v2
- Bridge



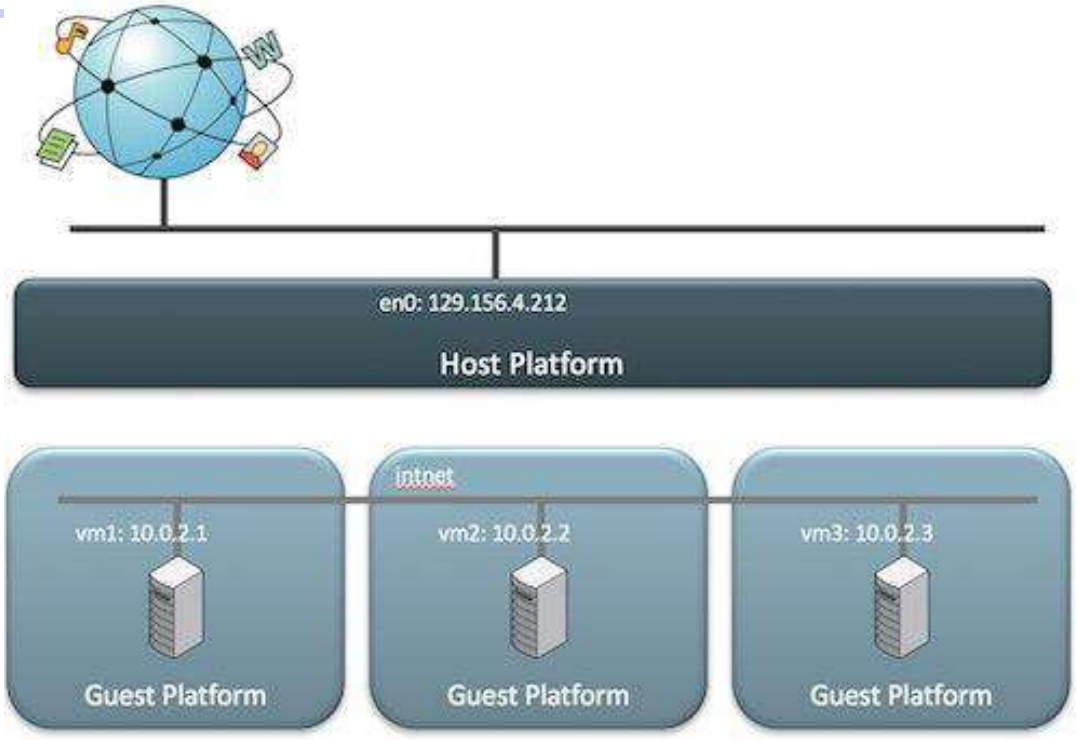
Additional Explanation: Illustration

- See: https://www.nakivo.com/blog/virtualbox-network-setting-guide/
- Bridge



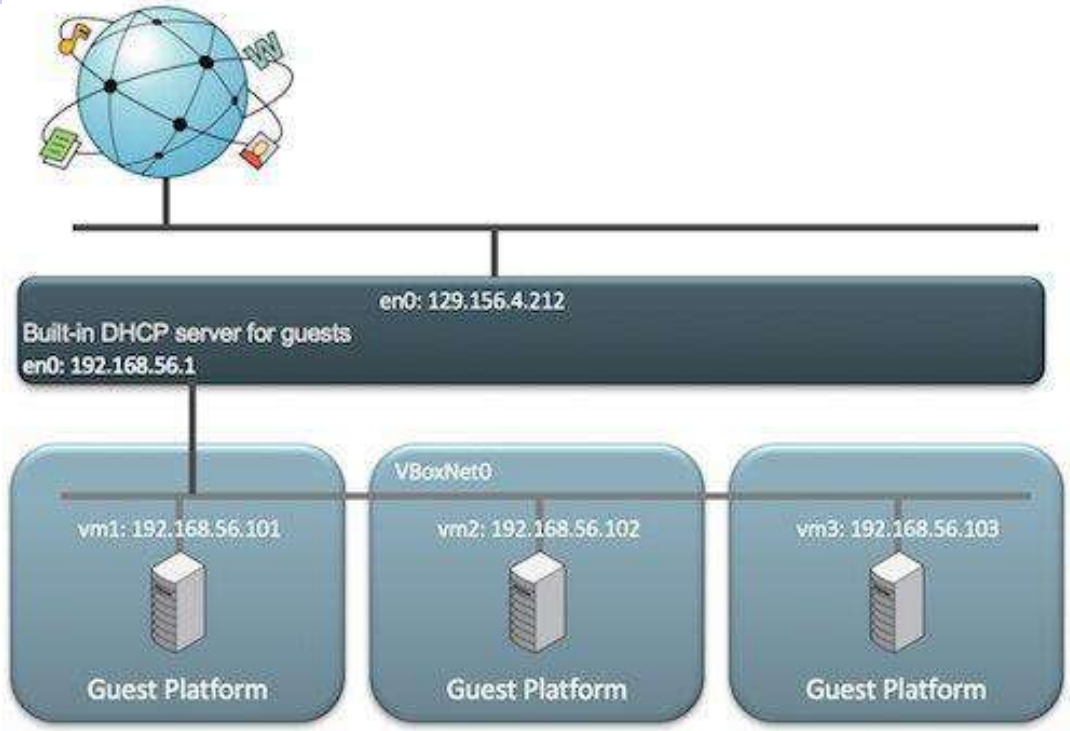
Additional Explanation: Illustration

- See: https://blogs.oracle.com/scoter/networking-in-virtual box-v2
- Internal mode:



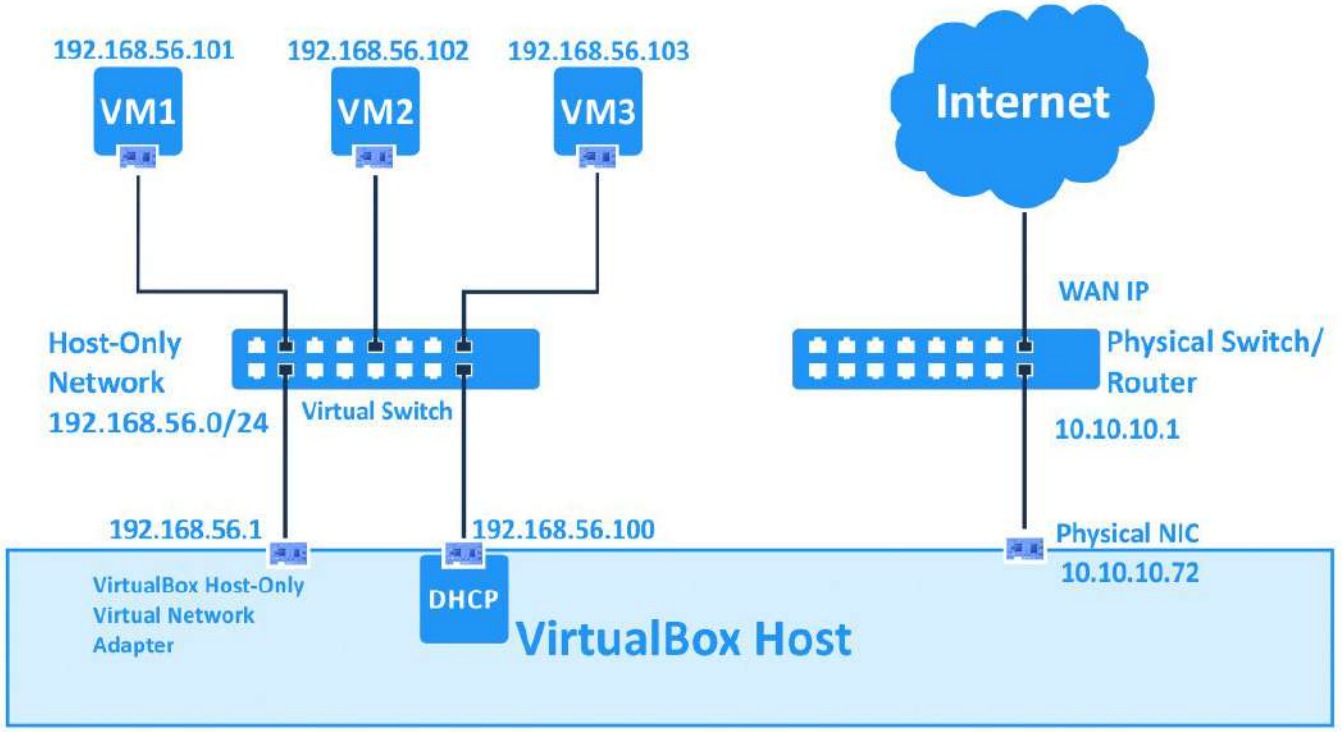
Additional Explanation: Illustration

- See: https://blogs.oracle.com/scoter/networking-in-virtual box-v2
- Host-only mode:



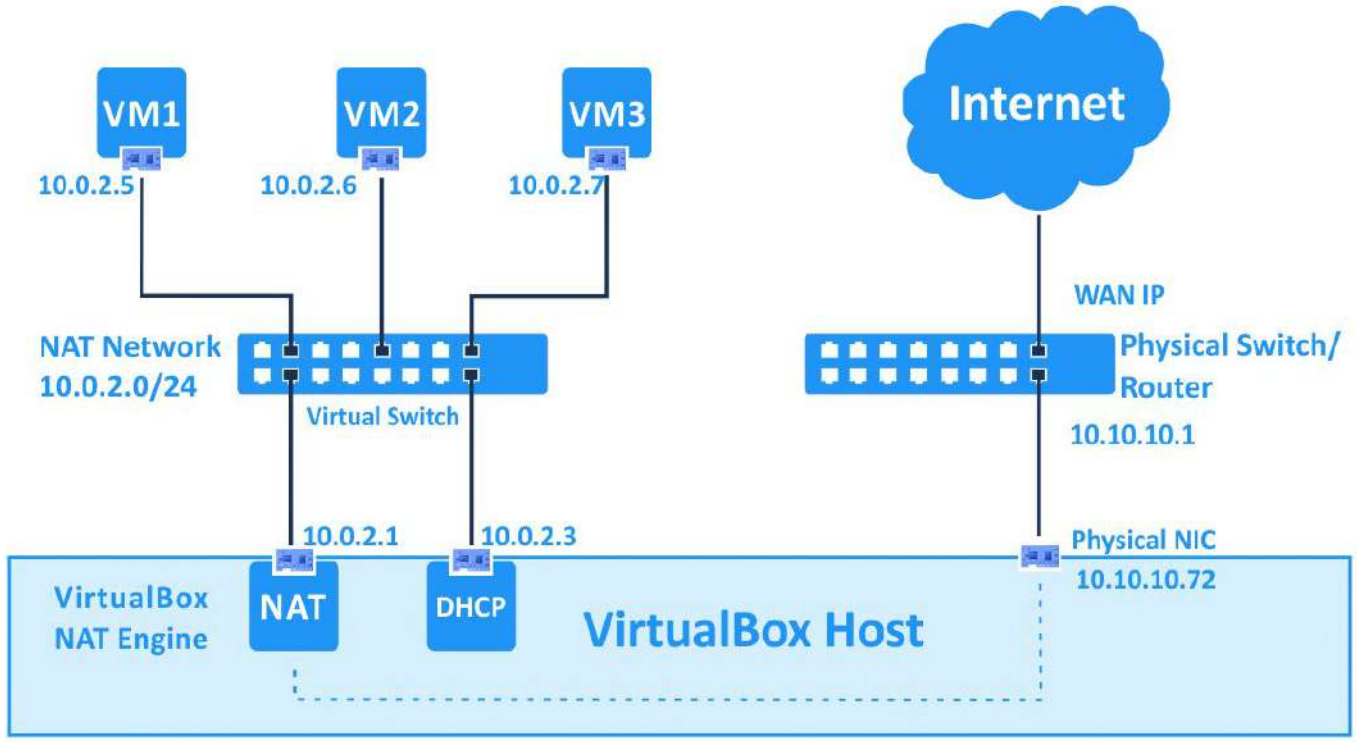
Additional Explanation: Illustration

- See: https://www.nakivo.com/blog/virtualbox-network-setting-guide/
- Host-only



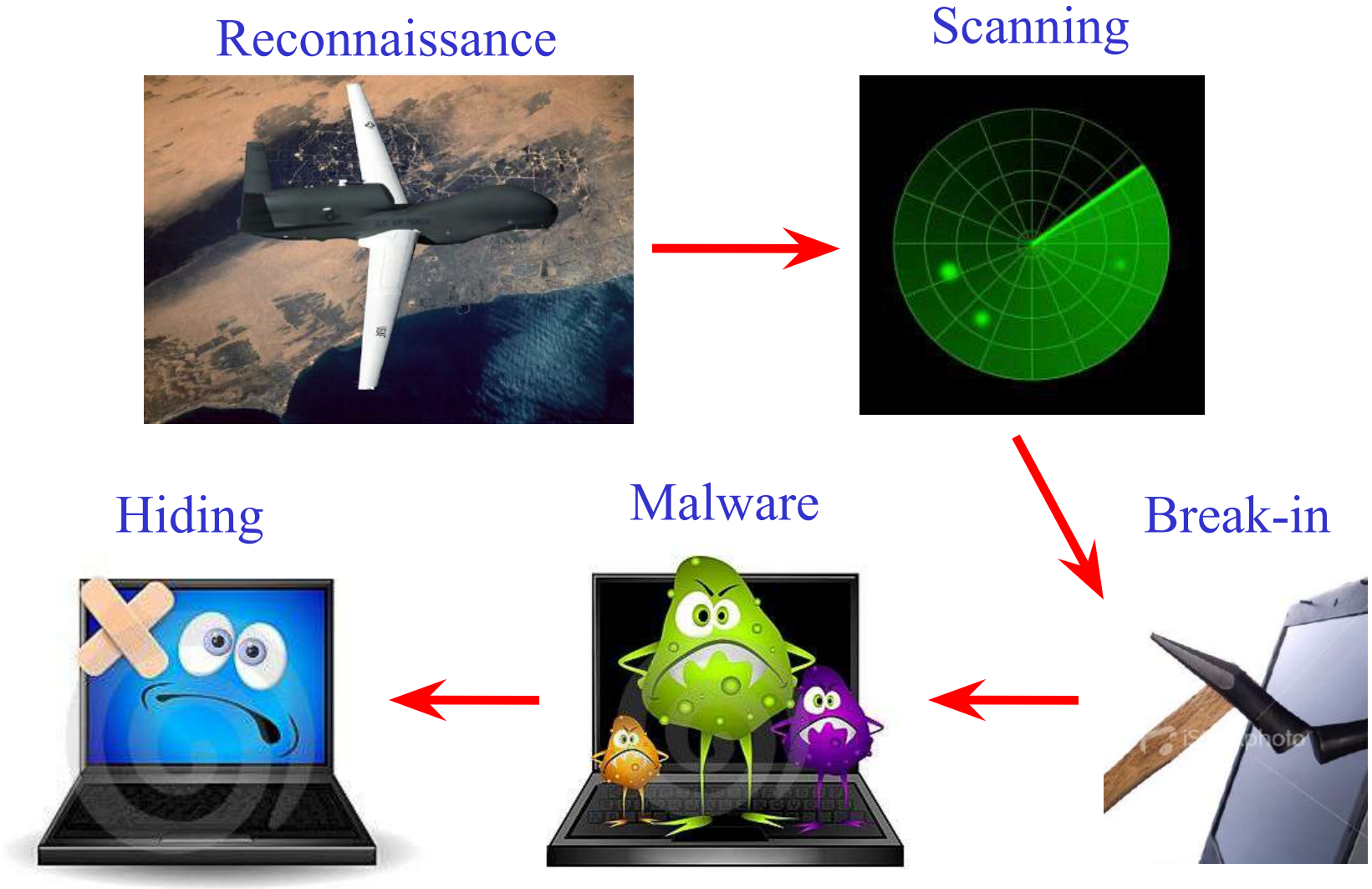
Additional Explanation: Illustration

- See: https://www.nakivo.com/blog/virtualbox-network-setting-guide/
- NAT network mode:



Attack Framework

Big Picture of Attacks



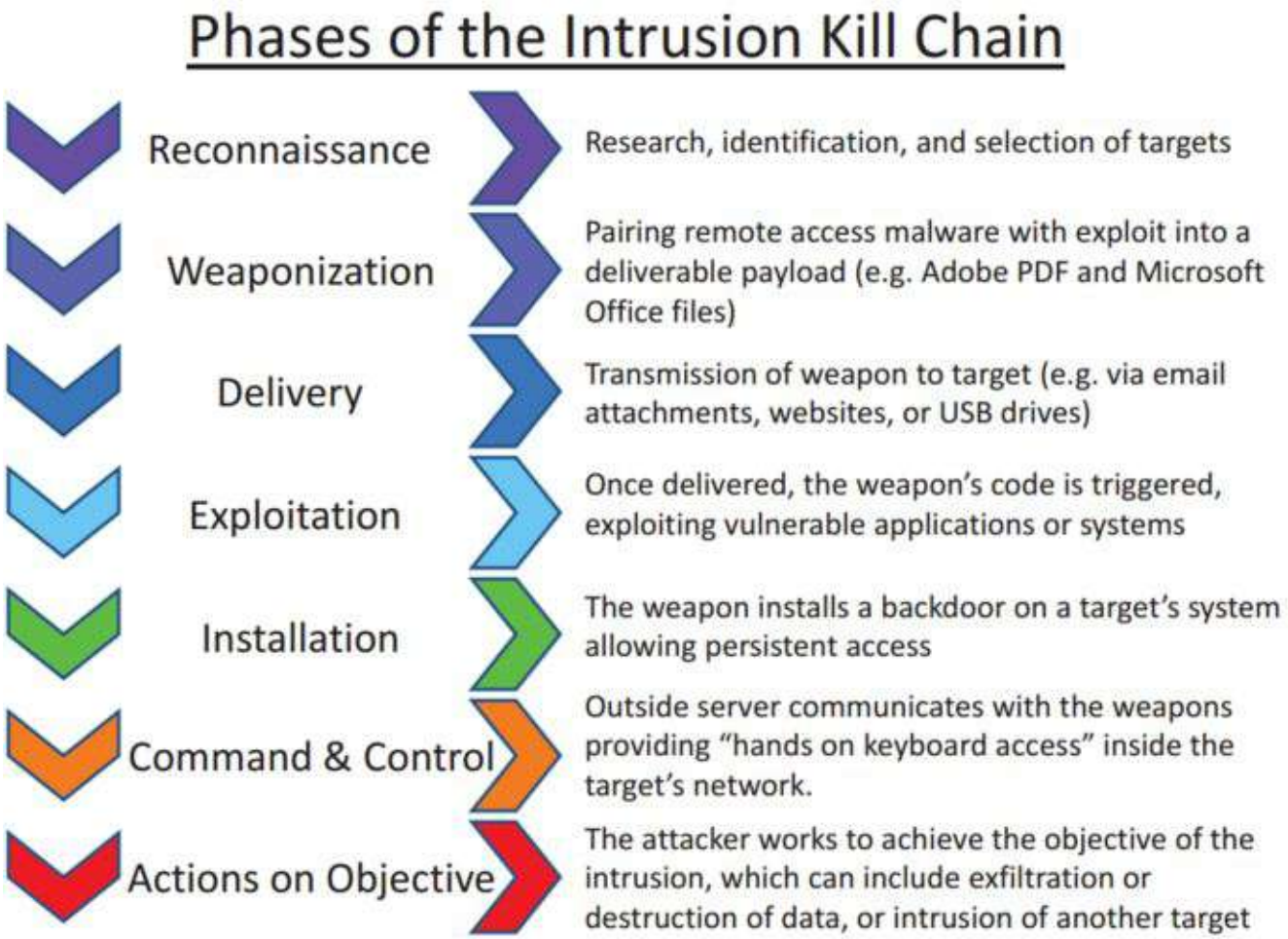
Attack Frameworks: Non-Computing

- **Military kill chain**: a military concept related to the structure of an attack
- F2T2EA steps/phases:
  - Find: Identify a target
  - Fix: Fix the target's location
  - Track: Monitor the target's movement
  - Target: Select weapon or asset to use
  - Engage: Apply the weapon to the target
  - Assess: Evaluate effects of the attack
- End-to-end process as a "chain"

Attack Frameworks: Cyber Kill Chain

- Cyber kill chain:
  - A new "intrusion kill chain" by **Lockheed-Martin** to defend computer networks
  - Starting from reconnaissance to targeted data exfiltration

Attack Frameworks: Cyber Kill Chain



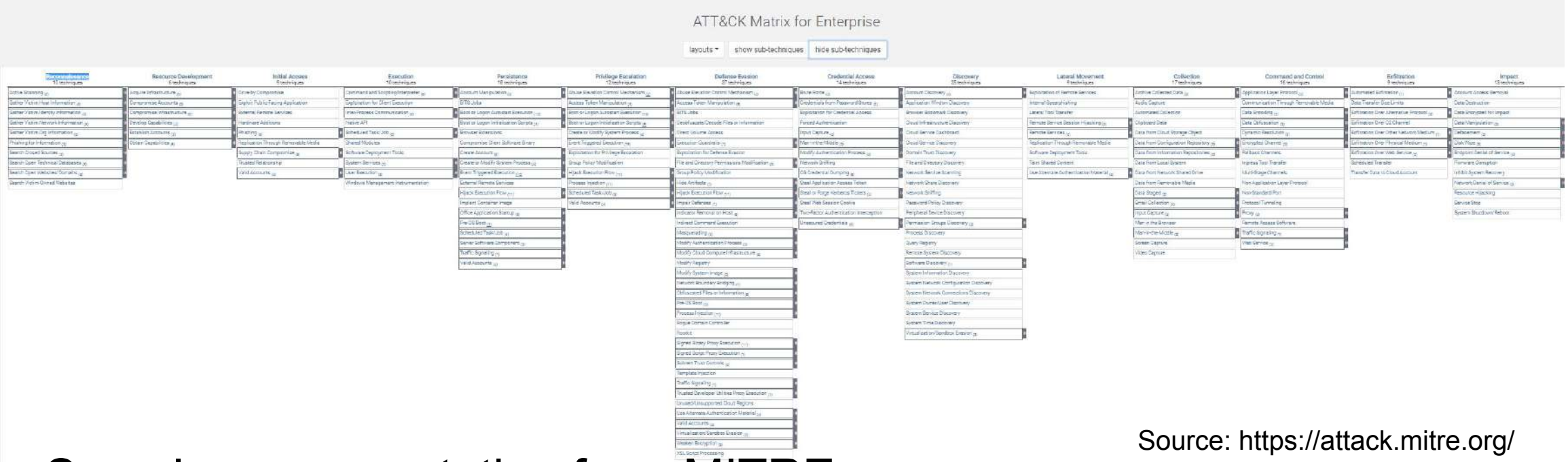
Attack Frameworks: FireEye's Kill Chain

- FireEye's kill chain:
  - Emphasizes the persistence of threats: a threat does not end after one cycle
  - Phases:
    - Reconnaissance
    - Initial intrusion into the network
    - Establish a backdoor into the network
    - Obtain user credentials
    - Install various utilities
    - Privilege escalation/lateral movement/data exfiltration
    - **Maintain persistence**

Attack Frameworks: MITRE ATT&CK

- MITRE ATT&CK (https://attack.mitre.org/)
  - A kill chain framework from MITRE
  - Tactics, techniques & procedures (TTPs) used by malicious actors
  - 3 main matrices: enterprise, mobile, ICS
  - Phases for Enterprise: reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command & control, exfiltration, impact

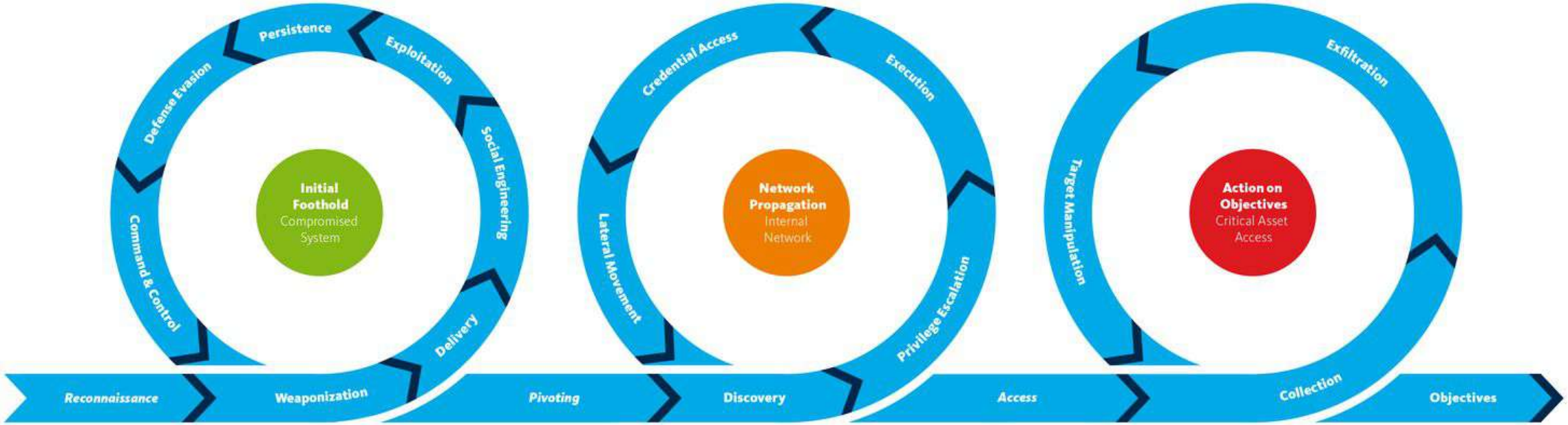
MITRE ATT&CK: Enterprise



Source: https://attack.mitre.org/

See also a presentation from MITRE:
https://www.youtube.com/watch?v=bkfwMADar0M

Even More? Unified Kill Chain



And Others: Penetration-Testing, Compliance Frameworks

- Penetration Testing Execution Standard (PTES)
- Open Source Security Testing Methodology Manual (OSSTM)
- OWASP testing guide: for web pen-testing
- PCI Data Security Standard (PCI DSS)
- ...

Phase 1: Reconnaissance

Progress Overview

- System attacks and defenses:
  - Reconnaissance
  - Scanning
  - Automated vulnerability finding
  - Automated exploitation
  - Vulnerability discovery, e.g., fuzzing
  - Attacks to gain access, e.g., buffer overflow attacks and defenses

Low-Tech Reconnaissance

- **Dumpster diving**
- **Social engineering**: exploiting the human element of a computer system
  - Fraud phone call (with spoofed caller ID), email spam, phishing
  - Countermeasures:
    - Users must check the identity of the other end of the communication
    - Governments can set up a hotline number
    - Governments can educate users
- **Physical break-in**

Searching the Fine Web

- Google Hacking: **using operators** to search google.
  - Use **quotes** for exact phrase: " ... "
  - **number ranges**, e.g 1..10 midterms
  - **info:** information about link
  - site:[domain], link:[web page], intitle:[term(s)], related:[site], cache:[page], filetype:[suffix], not (-), plus (+)
  - Complete List: https://ahrefs.com/blog/google-advanced-search-operators/

Searching the Fine Web

- What can you find?
- You can try the following searches:
  - inurl:wp-login.php
  - inurl:<domain-suffix>/[administrator|admin] [password|user|login]
  - intitle:"Index of"
  - inurl:view/index.[shtml|html]
  - inurl:viewer_index.[shtml|html]

Searching the Fine Web

- More of these?
  - Johnny Long's books: "Google Hacking for Penetration Testers"
  - Google Hacking Database (GHDB) site: https://www.exploit-db.com/google-hacking-database
  - Also check the available categories, e.g. "Files containing passwords", …

Searching the Fine Web

- Google phone book search:
  - Service now retired
  - Could have search terms:
    - rphonebook, phonebook, ...
  - Current alternatives: www.zabasearch.com, …
- Other types of searches:
  - TinEye (tineye.com): reverse image search
  - Metagoofil: metadata of public documents
  - LLMs? What could go wrong!

Social Networks

- Not just Google – social networks contain information about people/organizations
  - LinkedIn
  - Facebook
  - Instagram
  - Job sites
  - ...

can use docusign as a bait

Internet Archive

- The Internet may not forget
  - Google cache: click the down arrow next to any returned search-result entry
  - Google images
  - Internet Archive Wayback Machine
    - http://archive.org/web/
  - Advertisement Alert!:
  - What is the solution? Privacy laws. How to implement them? Work with me!

From the Wayback Machine

Whois Database

- Whois databases: a variety of data elements regarding the assignment of domain names
- Important information about a site:
  - Names: administrator, contact person
  - Telephone numbers
  - Emails
  - Postal addresses
  - Registration dates
  - Name servers
- Access: whois command, who.is, www.whois.net

Whois Caveats

- Information may not be accurate:
  - Validation obligation on registrars
  - Whois privacy/private registration
    - Hide details behind proxy information
  - Whois accuracy study: 2010-02-19
    - 1,419 representative domain names
    - 23% owner's correct name and physical address
    - 29% with fake or dubious information

Open Source Intelligence (OSINT)

- Derived from freely-accessible sources: public records, information shared by organizations
- Benefit for attackers:
  - Queries are not sent to the target domain directly
  - Reconnaissance activities are not recorded in the target domain's log files

Domain Name System (DNS)

- Query name servers
  - Tools:
    - nslookup: standard Unix tool, but a feature like zone transfer is usually disabled now
    - dig (domain information groper)
    - host
  - Operations to obtain:
    host's IP, name servers, mail servers, reverse name resolution (dig -x), …

Domain Name System (DNS)

- Some familiarization with DNS records:
  - A : Address
  - AAAA : IPv6 address
  - HINFO : Host information
  - MX : Mail eXchange
  - NS : Name Server
  - TXT : Text
- Resources:
  - DNS HOWTO: http://tldp.org/HOWTO/DNS-HOWTO.html
  - DiG HOWTO: https://www.madboa.com/geek/dig/

Domain Name System (DNS)

- Ultimate target: zone transfer
  (see https://en.wikipedia.org/wiki/DNS_zone_transfer)
- Zone transfer using nslookup:

```
$ nslookup
> server [target-name-server]
> set type=any
ls -d [target-domain]
```

- Zone transfer using dig:

```
$ dig @[target-name-server] [target-domain] -t AXFR
```

- Example of site with an unrestricted zone transfer: ZoneTransfer.me
  Read: https://digi.ninja/projects/zonetransferme.php

Zone Transfer of ZoneTransfer.me

```
dig axfr @nsztm1.digi.ninja zonetransfer.me

; <<>> DiG 9.9.5-3ubuntu0.6-Ubuntu <<>> axfr @nsztm1.digi.ninja zonetransfer.me
; (1 server found)
;; global options: +cmd
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 201
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.        301     IN      TXT     "google-site-verification=tyP28J7JAUHA9f
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      MX      20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me.        7200    IN      A       217.147.180.162
zonetransfer.me.        7200    IN      NS      nsztm1.digi.ninja.
zonetransfer.me.        7200    IN      NS      nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me. 14000 IN     SRV     0 0 5060 www.zonetransfer.me.
```

Source: https://digi.ninja/projects/zonetransferme.php

Zone Transfer of ZoneTransfer.me

```
dr.zonetransfer.me.      300     IN      LOC     53 20 56.558 N 1 38 33.526 W 0.00m 1m 10
DZC.zonetransfer.me.     7200    IN      TXT     "AbCdEfG"
email.zonetransfer.me.   2222    IN      NAPTR   1 1 "P" "E2U+email" "" email.zonetransfe
email.zonetransfer.me.   7200    IN      A       74.125.206.26
Info.zonetransfer.me.    7200    IN      TXT     "ZoneTransfer.me service provided by Rob
internal.zonetransfer.me. 300    IN      NS      intns1.zonetransfer.me.
internal.zonetransfer.me. 300    IN      NS      intns2.zonetransfer.me.
intns1.zonetransfer.me.  300     IN      A       167.88.42.94
intns2.zonetransfer.me.  300     IN      A       167.88.42.94
office.zonetransfer.me.  7200    IN      A       4.23.39.254
ipv6actnow.org.zonetransfer.me. 7200 IN AAAA     2001:67c:2e8:11::c100:1332
owa.zonetransfer.me.     7200    IN      A       207.46.197.32
robinwood.zonetransfer.me. 302   IN      TXT     "Robin Wood"
rp.zonetransfer.me.      321     IN      RP      robin.zonetransfer.me. robinwood.zonetra
sip.zonetransfer.me.     3333    IN      NAPTR   2 3 "P" "E2U+sip" "!^.*$!sip:customer-se
sqli.zonetransfer.me.    300     IN      TXT     "' or 1=1 --"
sshock.zonetransfer.me.  7200    IN      TXT     "() { :]}\; echo ShellShocked"
staging.zonetransfer.me. 7200    IN      CNAME   www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301 IN A 127.0.0.1
testing.zonetransfer.me. 301     IN      CNAME   www.zonetransfer.me.
vpn.zonetransfer.me.     4000    IN      A       174.36.59.154
```

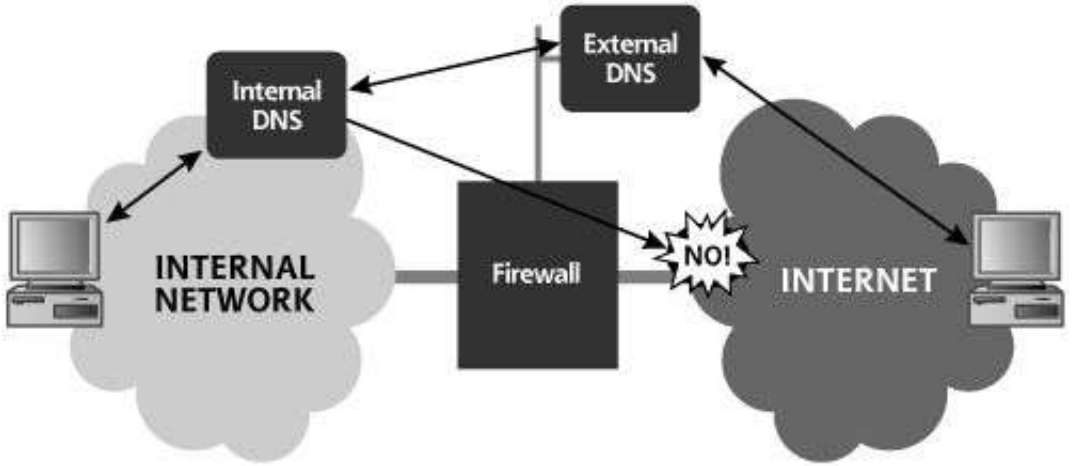
Source: https://digi.ninja/projects/zonetransferme.php

Domain Name System (DNS)

- Other web-based DNS reconnaissance tools/services:
  - ViewDNS.info (https://viewdns.info/): also check its nice “IP history” feature
  - Central Ops: http://centralops.net/
  - G Suite Toolbox’s Dig: https://toolbox.googleapps.com/apps/dig/

Domain Name System (DNS)

- Countermeasures:
  - Allow a zone transfer only between the primary name server and secondary name server(s)
  - Deploy a split-horizon/split-view/split-brain DNS:



Source: Skoudis & Liston, Counter Hack Reloaded

Other Popular Recon Tools (Kali Linux)

- Some other recon tools are available in Kali Linux
- Examples:
  - theHarvester: look for email addresses https://tools.kali.org/information-gathering/theharvester
  - Maltego (https://www.paterva.com): https://tools.kali.org/information-gathering/maltego-teeth

Other Popular (Web-based) Recon Tools

- Numerous web-based recon tools are also available
- They issue various queries to obtain publicly available information about the targets
- Some examples:
  - Netcraft (https://www.netcraft.com)
  - Centralops.net (https://centralops.net)
  - Shodan (https://www.shodan.io): Search IoT devices

Output of Reconnaissance

- After the reconnaissance phase, attackers know:
  - Telephone numbers
  - Domain names
  - IP addresses
  - Servers
  - Technical contact information
  - People information
  - …

Progress Overview: Next Week

- System attacks and defenses:
  - Reconnaissance
  - Scanning
  - Automated vulnerability finding
  - Automated exploitation
  - Vulnerability discovery, e.g. fuzzing
  - Attacks to gain access, e.g., buffer overflow attacks and defenses

Your Lab 0 (Self-Lab): Reminder!

- Please get your set-up ready for Lab 1:
  - Install VirtualBox/VMware
  - Install Kali Linux
  - Install Ubuntu Linux 20.04 x64

Kali Linux: Extra

- Kali NetHunter:
  - A free & open-source Kali-based Mobile Penetration Testing Platform for Android devices
  - Download: https://www.offensive-security.com/kali-linux-nethunter-download/
  - Documentation: https://www.kali.org/docs/nethunter/

Questions?

See you next week!