Managing Enterprise Cybersecurity
MIS 4596

Unit #14

Agenda

- OSI Reference Model
- Linux commands for working with:
  - Domain names
  - Network availability of computers
  - Mapping paths data packets take
  - Scanning computer ports
- Vulnerability Scanning Lab
  - Nmap and Metasploitable
- National Vulnerability Database
- Network Address Translation
- Getting started – Introduction to Networking Lab
- Kali's Virtural Machines for labs…

Telecommunication Models

Electromagnetic transmission of data among systems

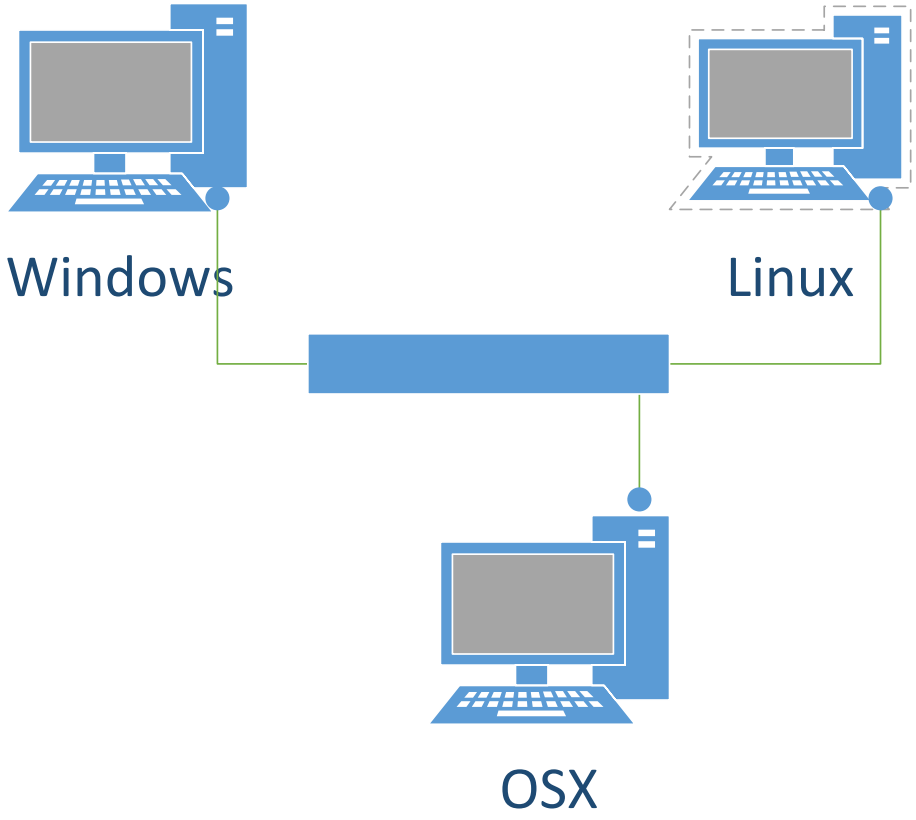
- Through digital, wireless and analog transmission types

- **Models** and standards of the following organizations have shaped our IT communication technology today
  - International Telecommunication Union (ITU)
  - International Standards Organization (ISO)

Information and Communications Technologies (ICT)

Network protocol

- Standard set of rules that determines how systems communicate across networks
- Different systems can use the same protocol to communicate and understand each other despite their differences



Open Systems Interconnection(OSI) Reference Model

OSI Model

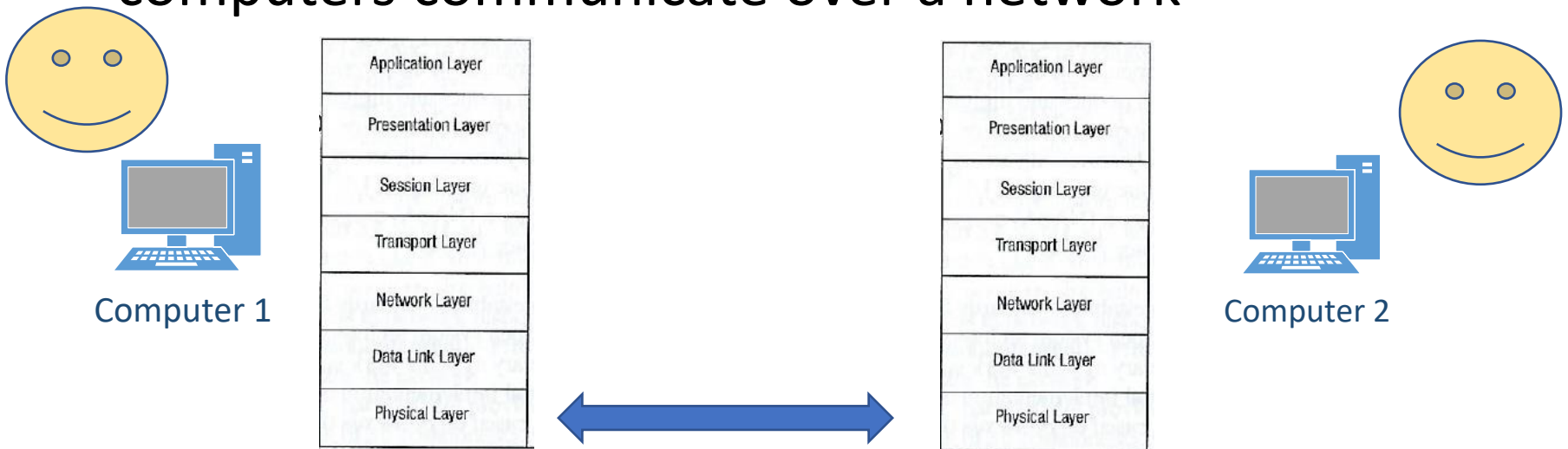
- Guidelines used by vendors, engineers, developers to develop products that enable computer systems to interoperate
- **Open network architecture is**
  - Not owned by vendors and not proprietary
  - Can easily integrate various technologies and vendor implementation of those technologies

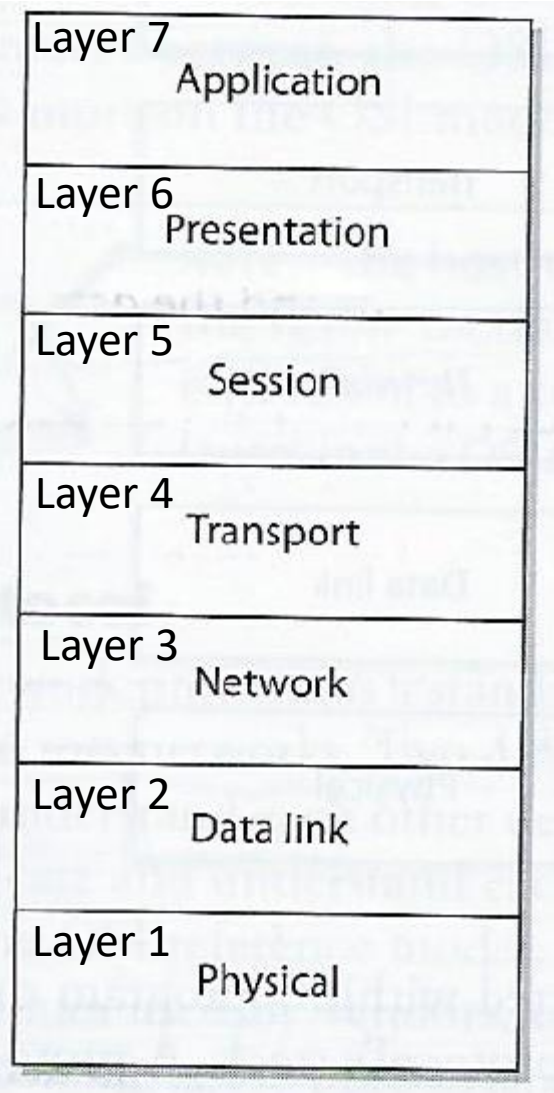
Open Systems Interconnection(OSI) Reference Model – ISO Standard 7498-1

"Layer 8"

OSI Model

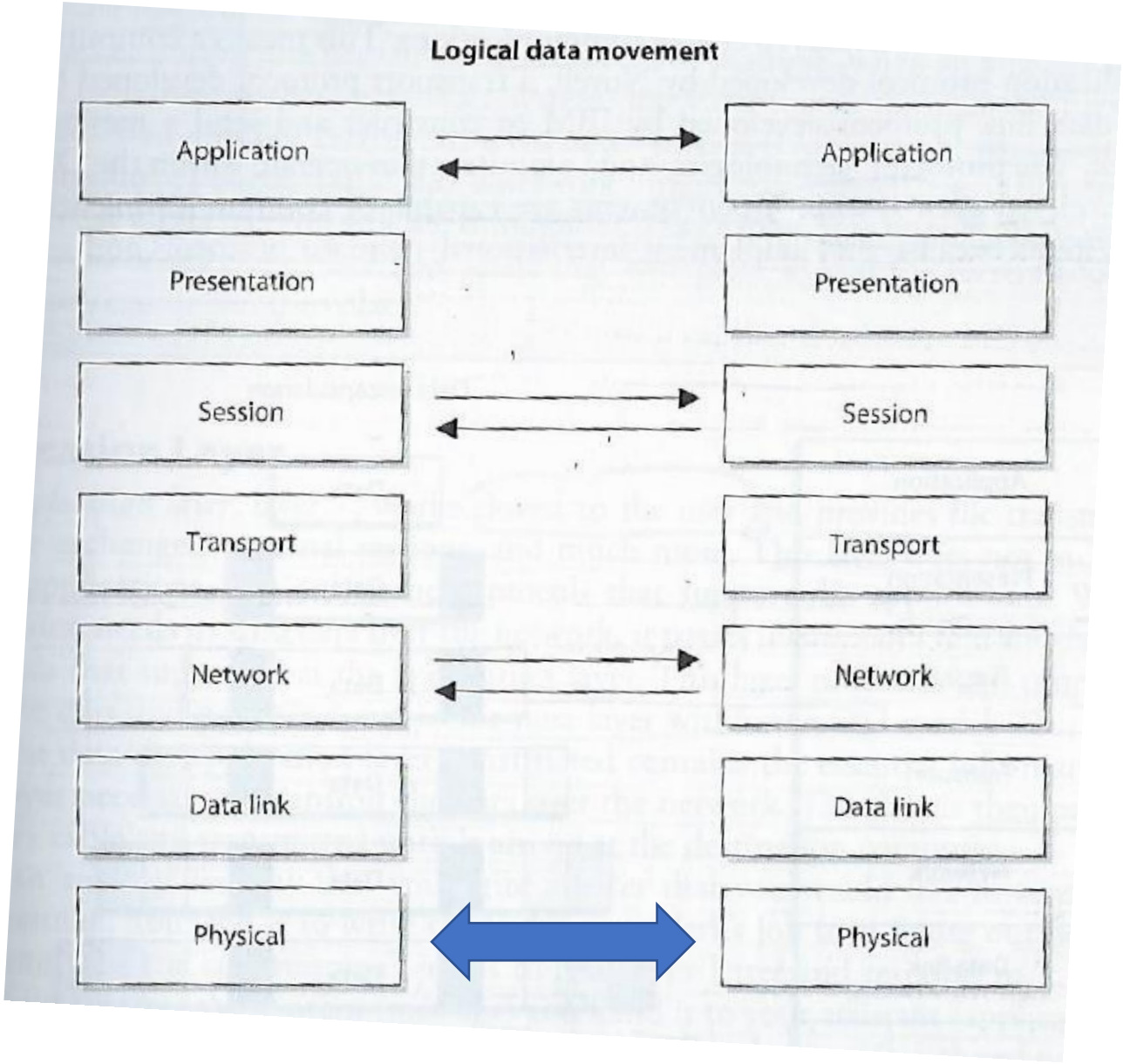
- Guidelines used by vendors, engineers, developers to enable their systems to interoperate
- Layers networking tasks, protocols and services into different layers
- Each layer has its own responsibilities regarding how two computers communicate over a network





Computers communicate via network

- Protocols function in specific OSI layers
- Each protocol on one computer communicates with the same corresponding protocol within the same OSI layer on another computer
- Via logical channels
- At the physical layer electronic/light signals are passed from one computer over a wire/fiber optic cable to the other computer

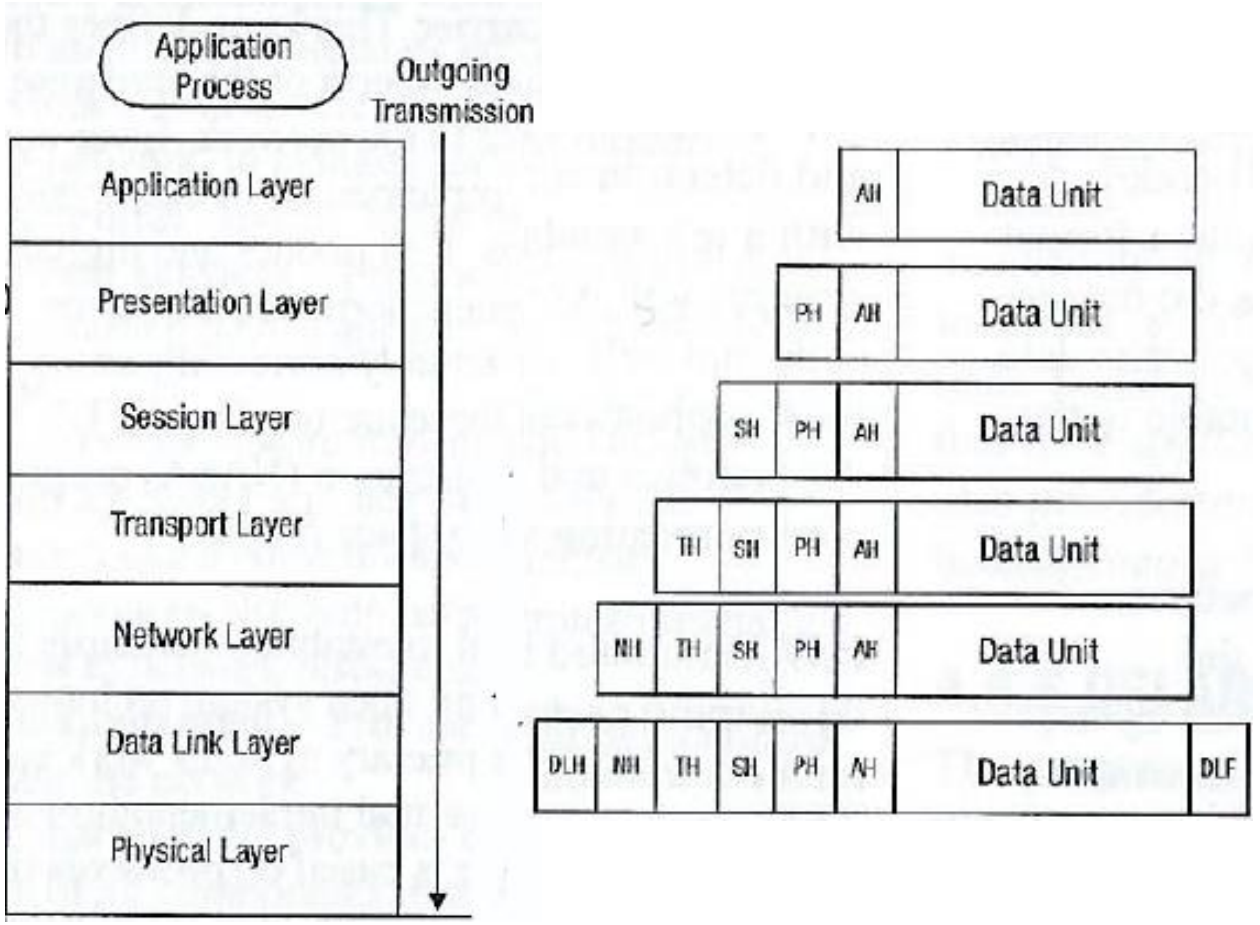


Encapsulation

- Process by which a protocol is used to enable two computers to communicate with each other within a specific OSI layer on each

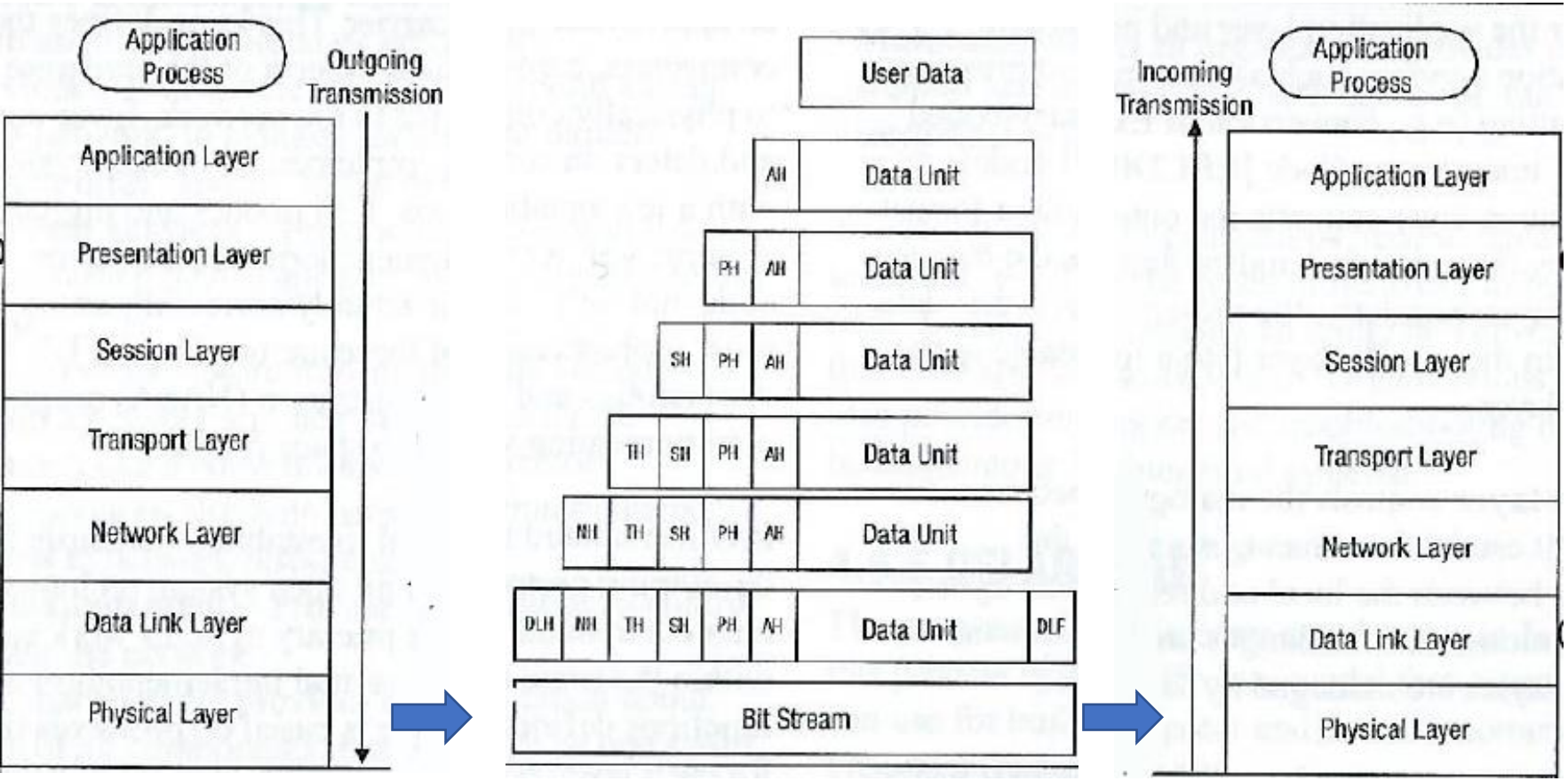
1. A message is constructed within a program on one computer and passed down through the network protocol's stack…

   A protocol at each layer adds its own information to the message, and the message grows in size as it does down the protocol stack



Encapsulation

2. At the physical layer of the network the message is passed by the sending computer as bits via electronic or light pulses (on/off) across the network to the destination computer

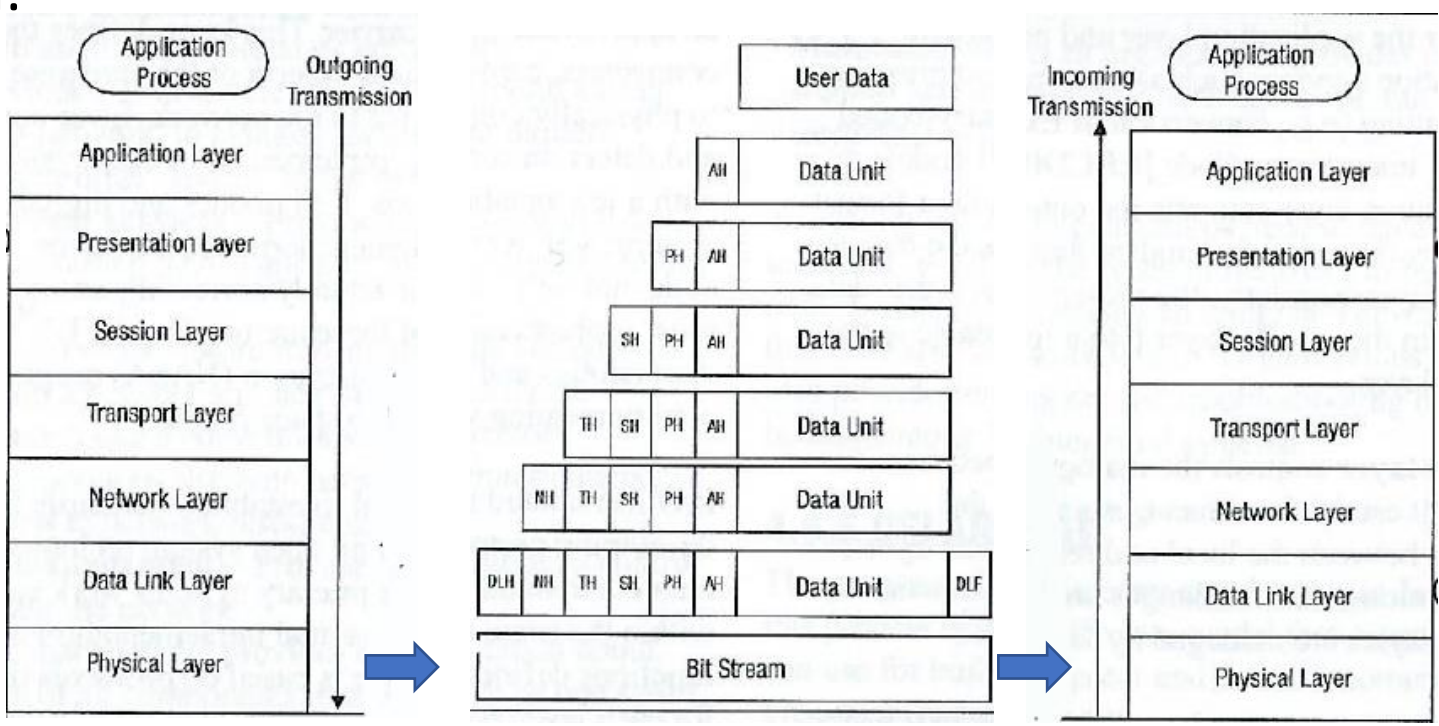


3. At the destination computer the encapsulation is reversed taking the message apart via the protocols of each layer until the data is ready for the application processing

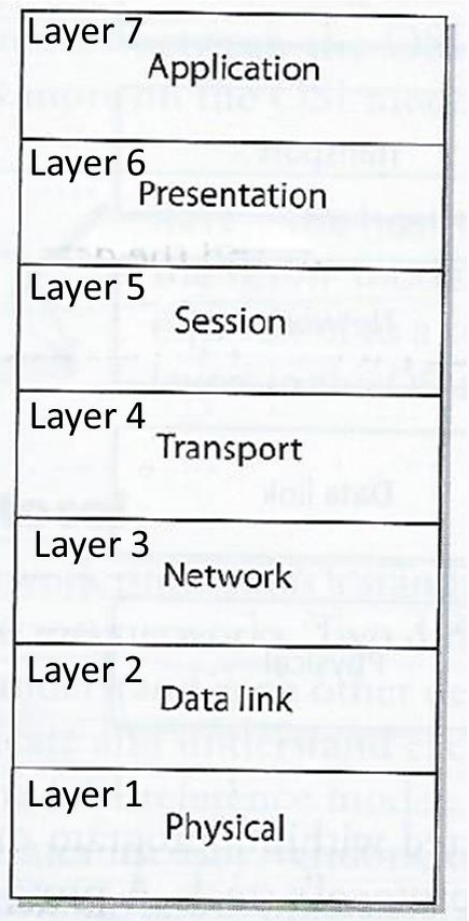
OSI Network Model

- A protocol at each layer expects the data in a particular format (“syntax”) and performs specific control functions on the data
- Data for control functions are added by the protocols at each layer in the form of headers and trailers of the datagram/packet/frame
- Each layer has a connection point (“interface”) that allows it to communicate with 3 other layers, communications with:

1. Interface of the layer above
2. Interface of the layer below it
3. Communications with the same layer in the interface of the destination computer



OSI Layers

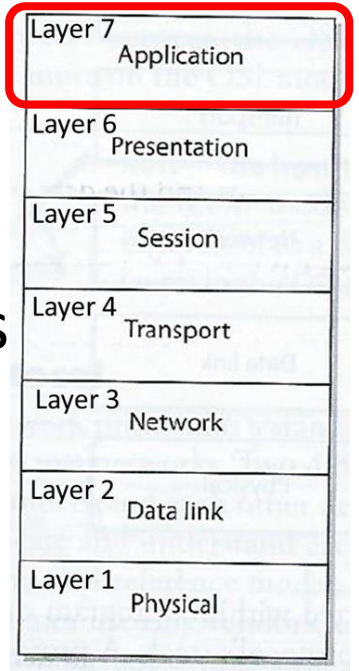


- Specifications for each layer's interface is very structured
- Implementing international standard protocols and interfaces within different vendors' technologies makes them part of an "open system" in which computers can communicate with one another
- Being part of an open system of protocols makes the different layers of a common network stack vulnerable and targets of attack

A network can be:

1. Used as a channel of an attack – i.e. as a resource for an attacker
   - For example: *Attacker sends a virus via a network channel from one system to another*
2. The target of an attack
   - For example: *Attacker carries out a denial-of-service (DoS) attack which sends a large volume of badly formed protocol message traffic over a network link to bog it down*

Layer 7: Application Layer



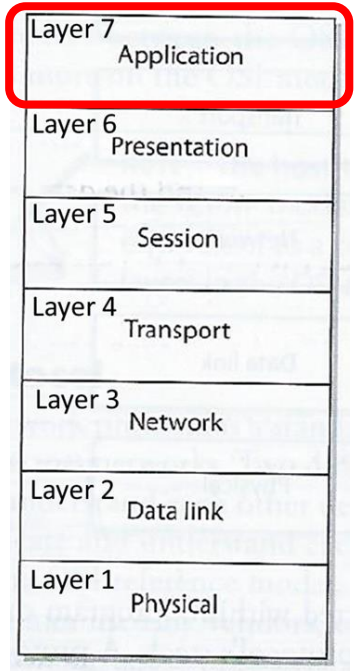
Works closest to the user – providing protocols that support the user's applications

For example: File transmissions, message exchanges, terminal sessions…

- When an application needs to send data over the network, it passes instructions and the data through the protocols that support it at the application layer

Application layer properly formats the data and sends it down to the presentation layer… (after data makes it through all the layers it has all the information needed to transmit it over the network)

Layer 7: Application Layer

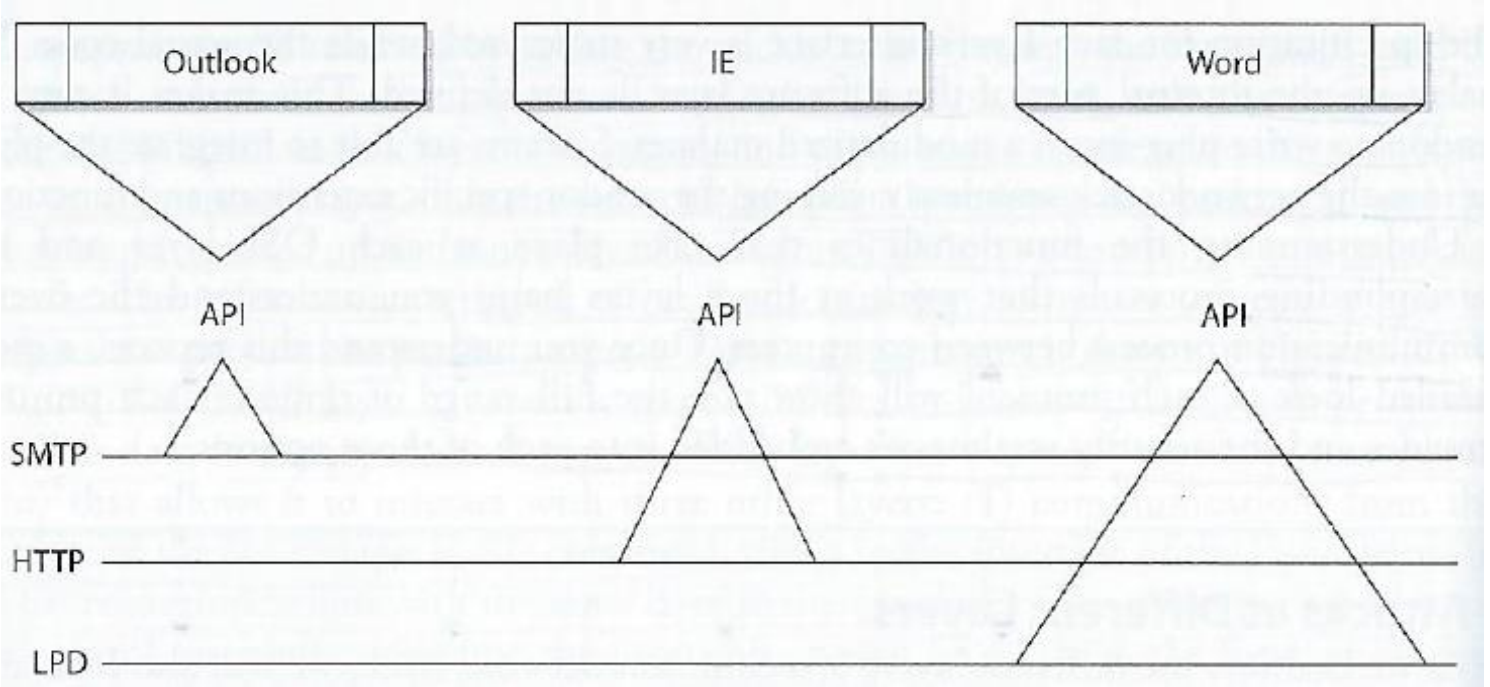


Protocols functioning at this layer communicate include:

- SMTP – Simple Mail Transfer Protocol
- HTTP – Hyper Text Transfer Protocol
- DNS – Domain Name System
- IRC – Internet Relay Chat
- LPD – Line Printer Daemon

Applications communicate with Layer 7 protocols by sending requests using Application Program Interface (API) libraries

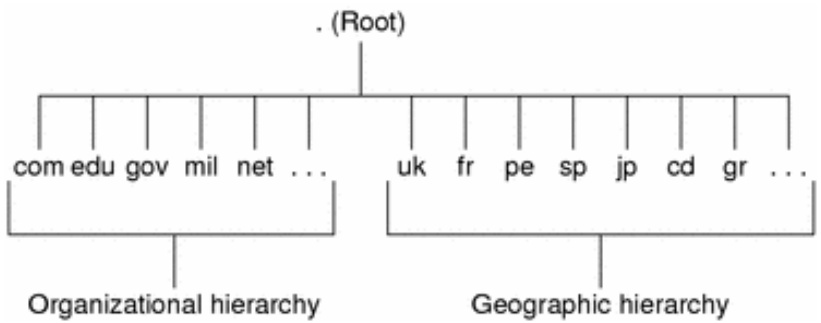
E.g. Outlook user clicks send, and the email client sends this information to SMTP which adds information to the user's message and passes it down to the Presentation Layer



Domain Name System (DNS)

- Basically, it is the internet directory
- Consists of a tree of domain names
- Example:

  Root -> .edu -> temple.edu



The root directory, which is represented as a dot (.), and two top level domain hierarchies:

- one organizational
- one geographical

Organizational Domains

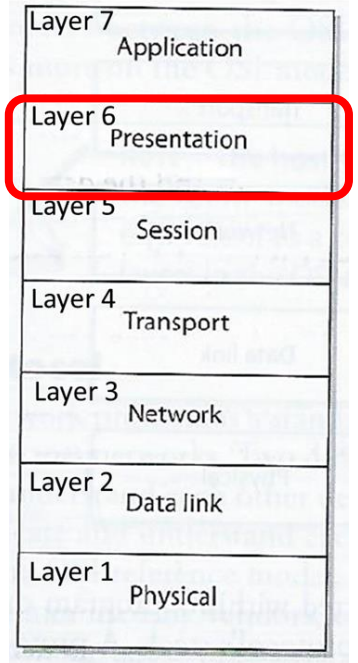
Domain	Purpose
com	Commercial organizations
edu	Educational institutions
gov	Government institutions
mil	Military groups
net	Major network support centers
org	Nonprofit organizations and others
int	International organizations

The geographic hierarchy assigns each country in the world a two or three-letter identifier

The hierarchy also provides official names for the geographic regions within each country, for example:

- domains in Britain are subdomains of the uk top-level domain, Japanese domains are subdomains of jp, and so on

Layer 6: Presentation Layer



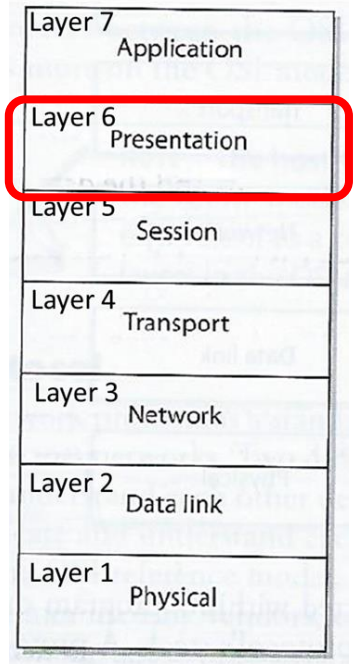
Receives data from the application layer protocol and puts it in a standard format with annotation that enables understanding by the processes operating at Layer 6 on destination computer

Presentation layer

1. Translates the format of data an application is using into a standard format used for passing messages over a network
2. Adds file type data to tell destination computer the file type and how to process and present it
3. Handles compression and encryption requests and adds data that enables the receiving computer to know how to decompress and decrypt the data

Application layer properly formats the data and sends it down to the presentation layer… (after data makes it through all the layers it has all the information needed to transmit it over the network)

Layer 6: Presentation Layer

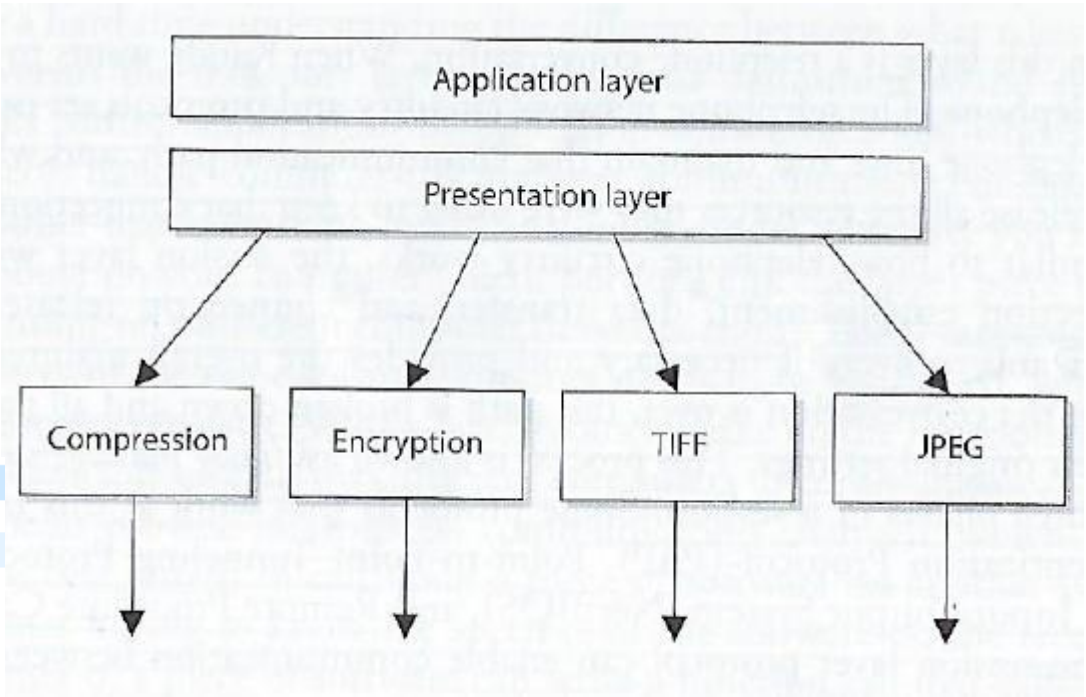


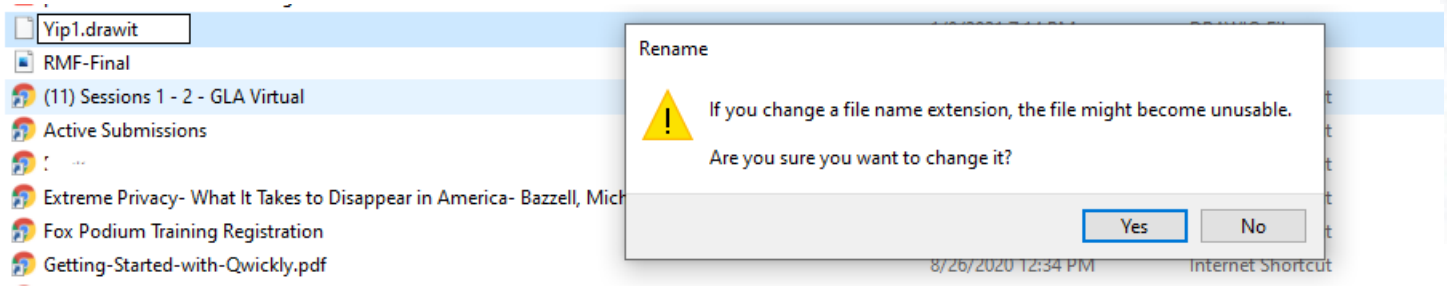
Protocols functioning at this layer communicate include:

- MIME – Multipurpose Internet Main Extensions standards
- TIFF - Tagged Image File Format
- GIF – Graphic Interchange Format
- JPEG – Joint Photographic Experts Group

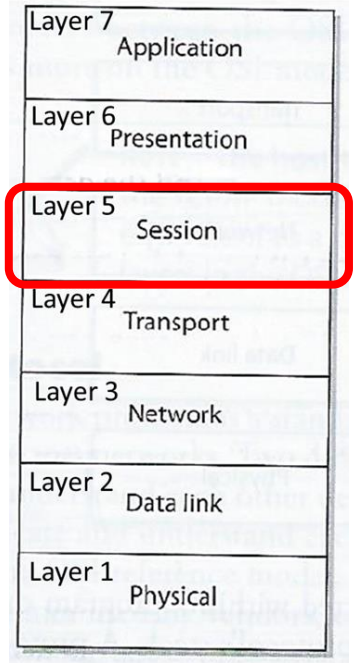
For example,

1. *User compresses file(s) on a Windows computer, sends it to someone on Linux computer*
2. *Linux computer receives the file, it looks at the file header, interprets the header's MIME type (Content-Type: application/zip) and knows what application can decompress the file*
3. *If systems does not have a program that understands the compression/decompression instructions, the file is displayed to the user with an unassociated icon*





Layer 5: Session Layer



When two applications need to communicate or transfer data between themselves, Layer 5 is responsible for:

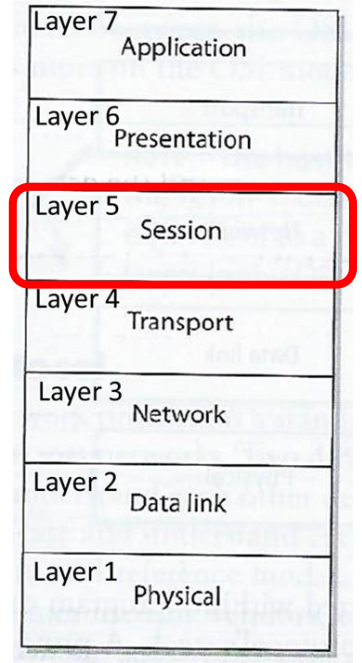
1. Establishing a connection between two applications
2. Dialog management to maintain the connection during the transfer of data
   - *Restarts and recovers the session to maintain the connection if needed*
3. Controlling release of the connection

- Provides inter-process communication channels, enables one software module on a local system to call a second software module running on a remote system. The results of the second module are retuned to the first system over the same session protocol channel

The session layer protocol enables 3 different modes of communications between 2 applications running on different computers across the network:

1. ***Simplex:*** *Communication takes place in one direction (very seldom used)*
2. ***Half-duplex:*** *Communication takes place in both directions, but only one application can send information at a time*
3. ***Full-duplex:*** *Communication takes place in both directions , and both applications can send information at the same time*

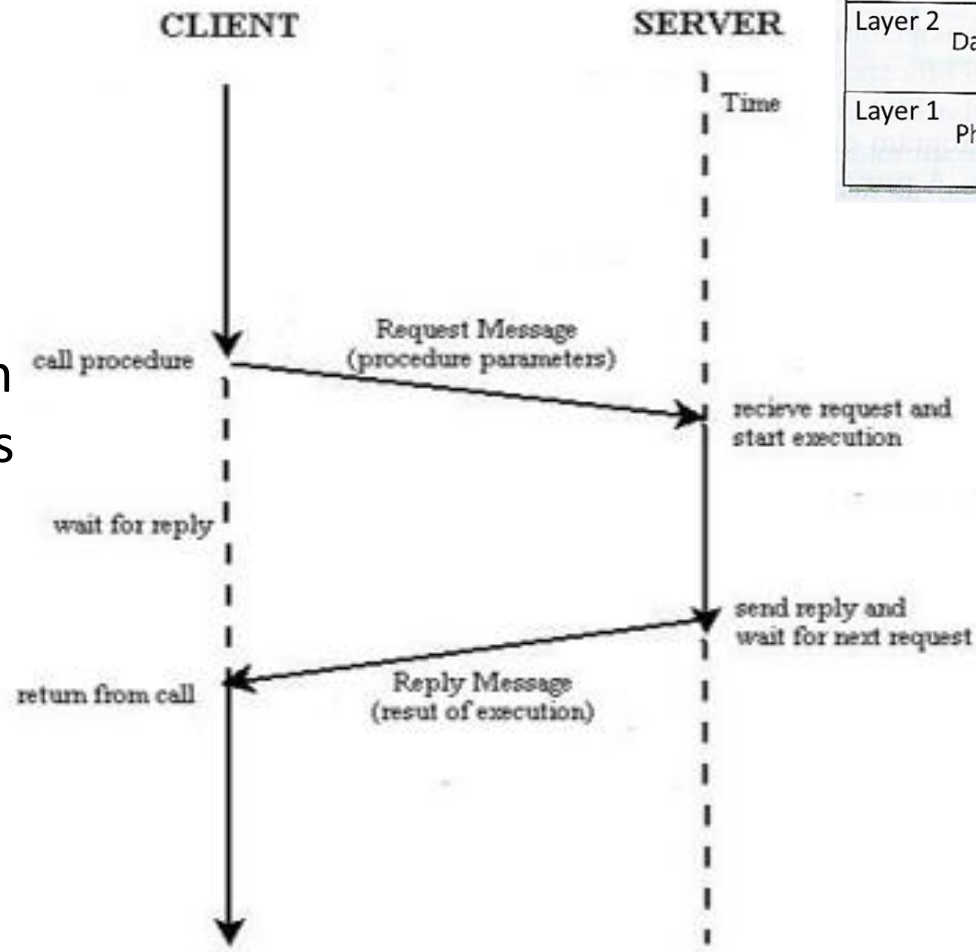
Layer 5: Session Layer



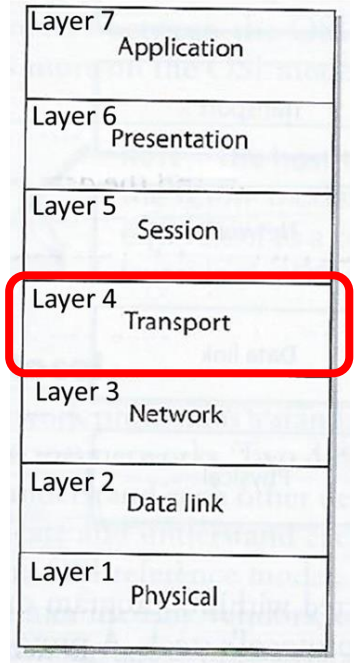
Provides inter-process communication channels, enables one software module on a local system to call a second software module running on a remote system. The results of the second module are retuned to the first system over the same session protocol channel

Session layer protocols provide the middleware functionality that connects and maintains the connection between software applications on different computers as they communicate (i.e. application to application communication)

- Client-server model
- Service oriented architecture (SOA)



Layer 4: Transport Layer

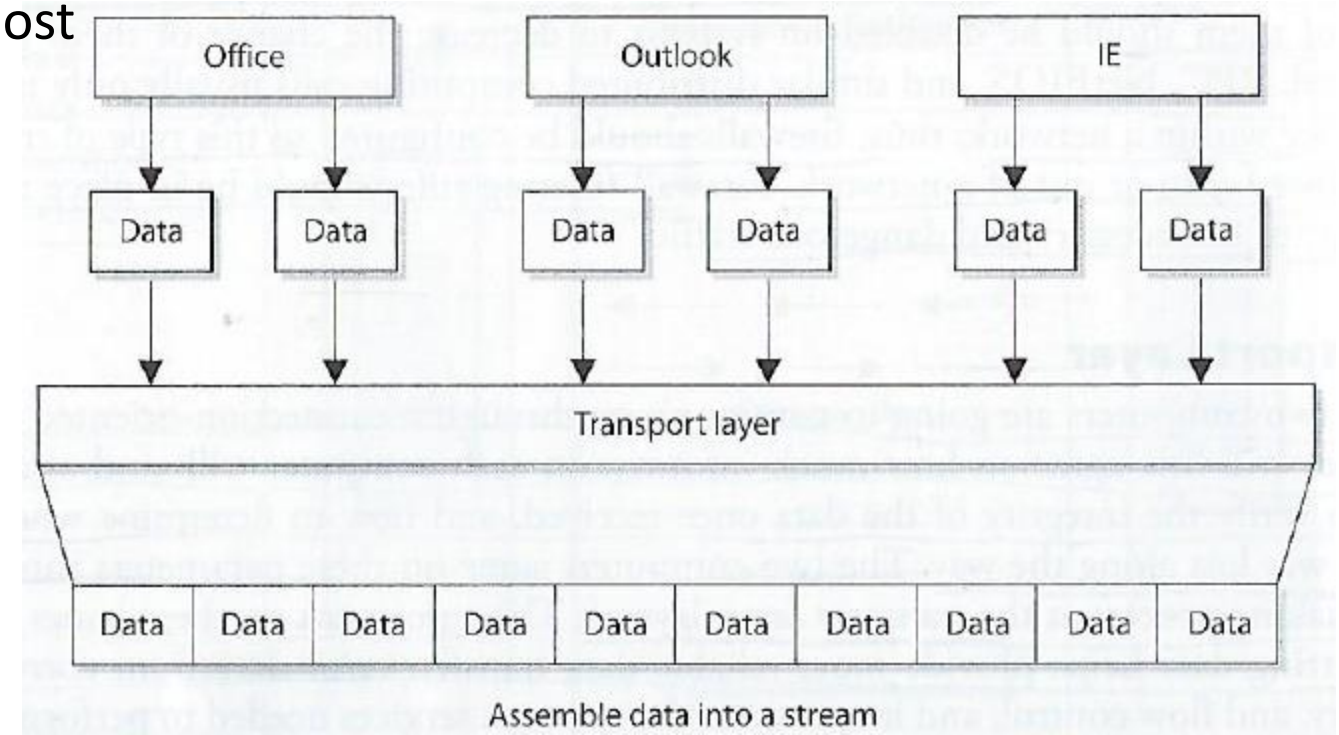


Establishes a logical connection between two computer systems and provides end-to-end data transport services

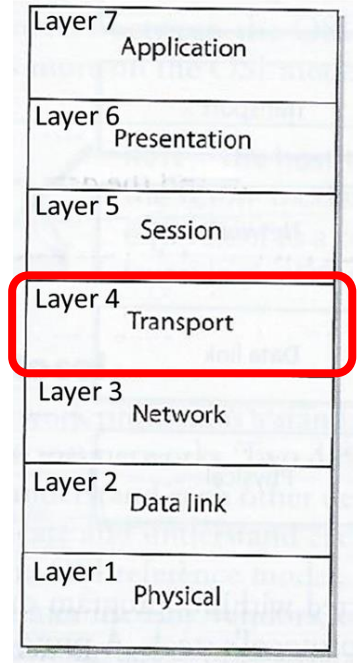
Provides connection level protocols for two computers to engage in a "handshaking process" and agree on parameters for:

1. How much data each computer will send at a time
2. How to verify data integrity once received
3. How to determine if a data packet was lost

Receives data from different applications and assembles their data into a stream for transmission over the network



Layer 4: Transport Layer



Transport layer protocol controls data flow across computer to computer connections without tracking connections between individual pairs of applications communicating across the network

Protocols:

- TCP – Transmission Control Protocol

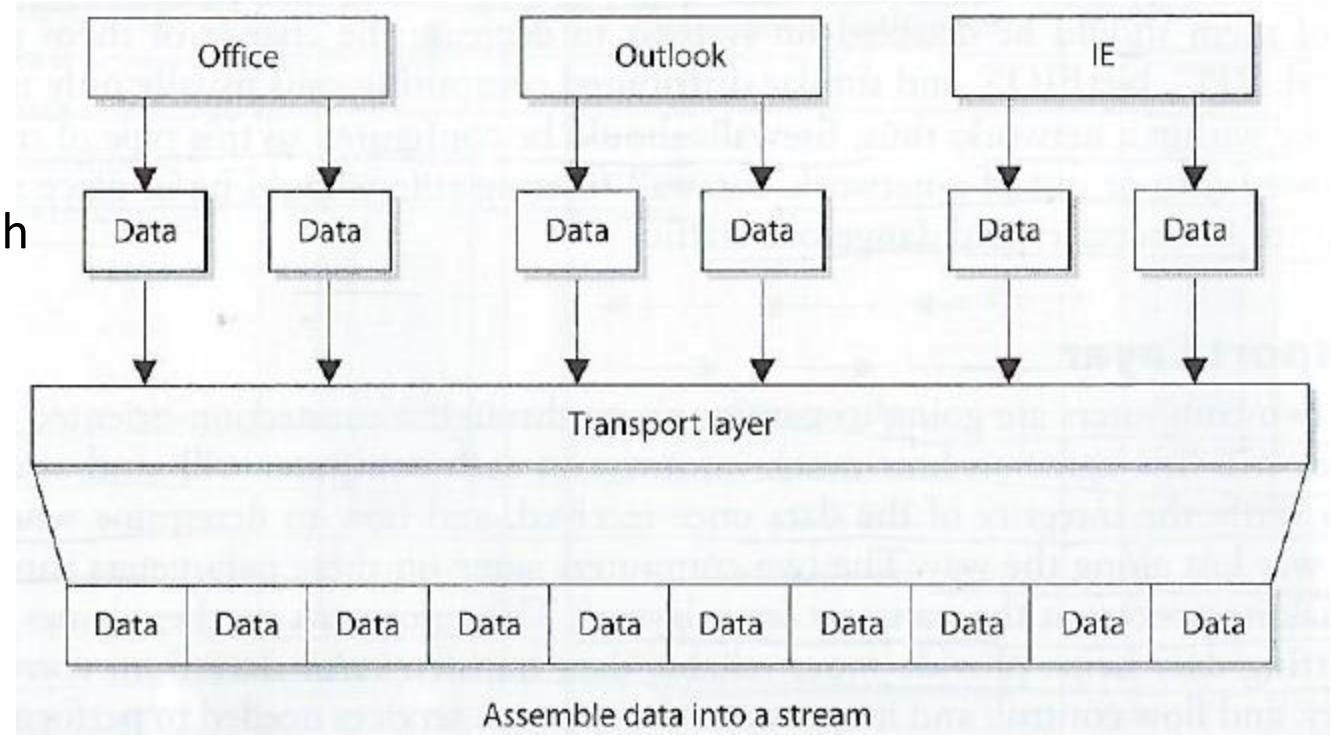
  Connection-oriented provides reliable data transmission

- UDP – User Datagram Protocol

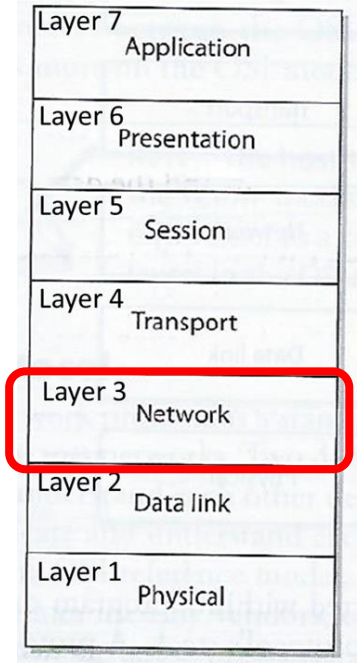
  Connectionless

TLS – Transport Layer Security protocol, straddles both Session and Transport layers

After the Transport Layer appends it's information to the data message, it is called either a TCP "segment" or a UDP "Packet"



Layer 3: Network Layer's



Routing protocols

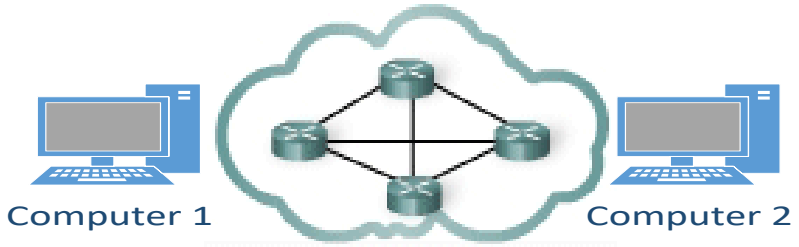
- Build and maintain routing tables

  Routing tables are maps of the network
- Determine best route (via "hops") to send packet from source computer to destination computer
- Inserts information into the data packet's header consisting of addresses (source and destination) and routes to their destination
- Do not guarantee delivery of packets

  Transport layer protocols catch problems and resend packets as needed (TCP not UDP)

Routers operate on OSI Layer 3

After the Network Layer appends it's information to the data message, it converts it to binary format and the unit of data is called a "packet"



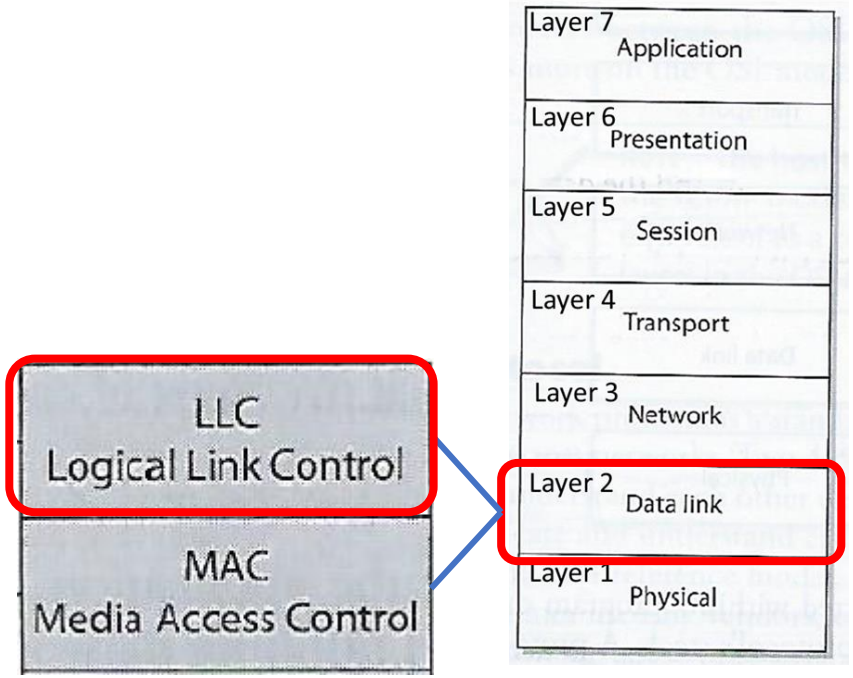
Layer 2: Data Link Layer

Translates the data packet with header/footer information accumulated from layers above into

- LAN (Local Area Network) or WAN (Wide Area Network) binary format for transmission over the network transmission line

After the network layer adds its routing information into the data packet, it passes the packet to the Data Link Layer's LCC sublayer

- LCC sublayer takes care of flow of control and error checking and passes it to the MAC sublayer

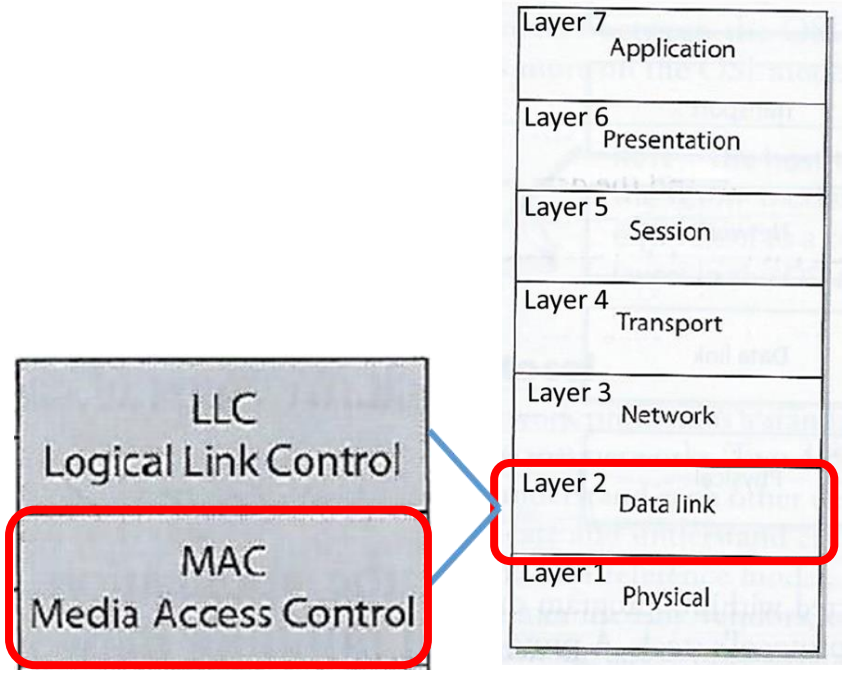


Switches operation on OSI Layer 2

Layer 2: Data Link Layer

The MAC sublayer determines if the data will be transmitted over a LAN or WAN, the network type and protocols and puts the last header and trailer on the packet before it is “put on the wire” and transmitted

- Each network type uses different protocols, NICs (network interface cards), cables, and transmission methods
- The MAC sublayer determines the format of the data frame for transmission over the particular type network the computer’s NIC is attached to

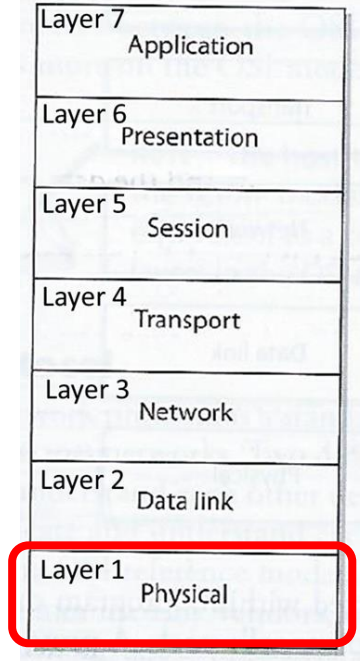


The computer’s network card bridges the data link and physical layers, takes data passed down from the user’s application through the 6 layers above and its network card driver encodes the bits at the data link layer

Each component has a different:

- *Header data format structure*
- *Protocol for physical transmission across the network type (coaxial, twisted pair, fiber optic cable; or wireless)*

Layer 1: Physical Layer

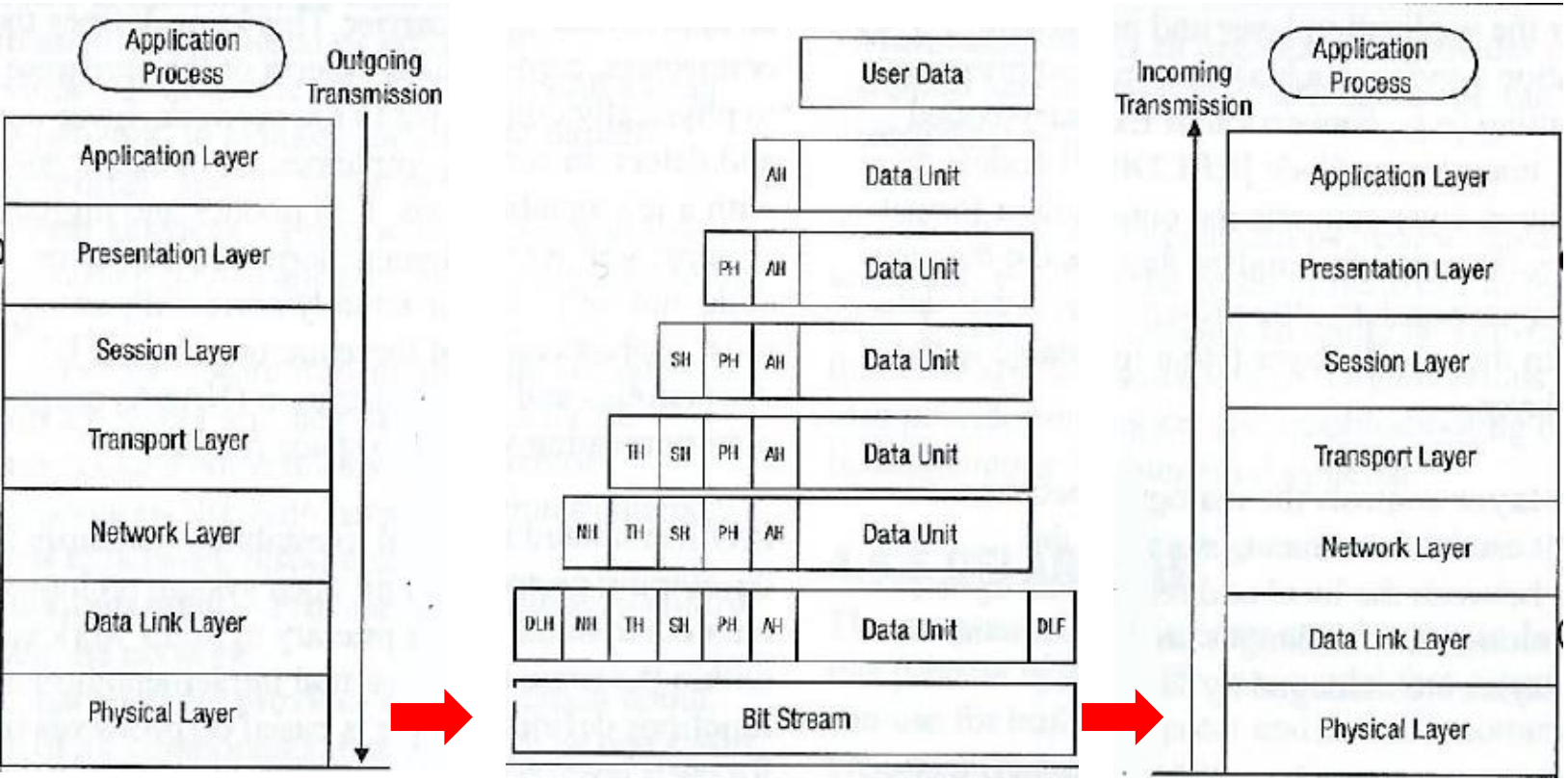


The Network Interface Card (NIC)

- Produces and interprets electromagnetic signals
- Converts bits into signals or voltages suitable for transmission across the LAN or WAN technology it is connected
- Determines synchronization, data transfer rates, line noise and transmission techniques based on the physical connection to electrical, optical or mechanical equipment

E.g. A '1' bit transmitted via Ethernet would be translated by the NIC to +0.5-volt electric signal, and '0' bit would be transmitted as 0-volts

Layer 1: Physical Layer



Data/file requests and terminals

Standard formats, encryption, compression

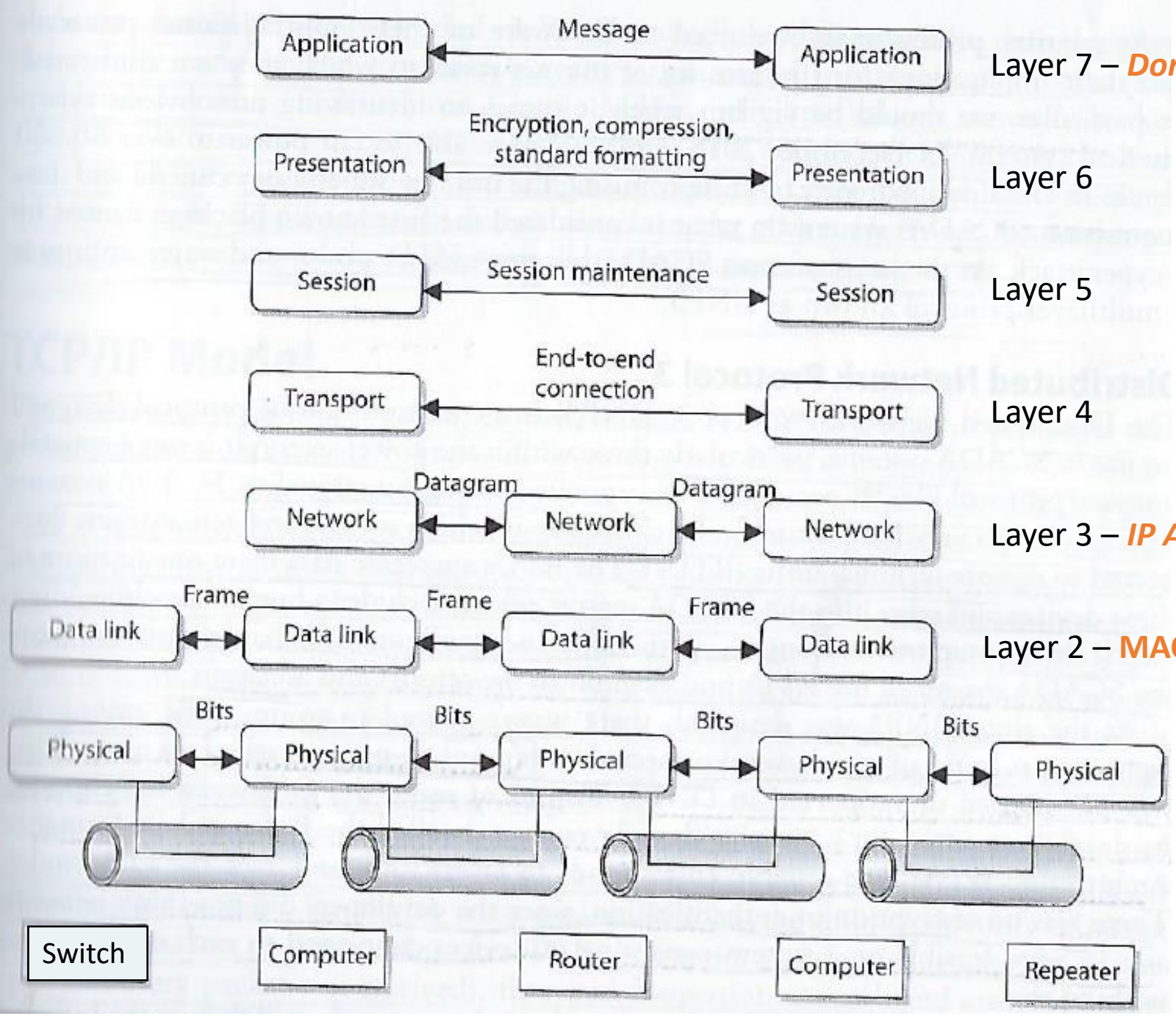
Applications communicating data

Computers communicating

Routing packets formed

Data frames ready for transfer

Signal processing



Layer 7 – ***Domain Name e.g. temple.edu***

Layer 6

Layer 5

Layer 4

Layer 3 – ***IP Address e.g. 155.247.166.60***

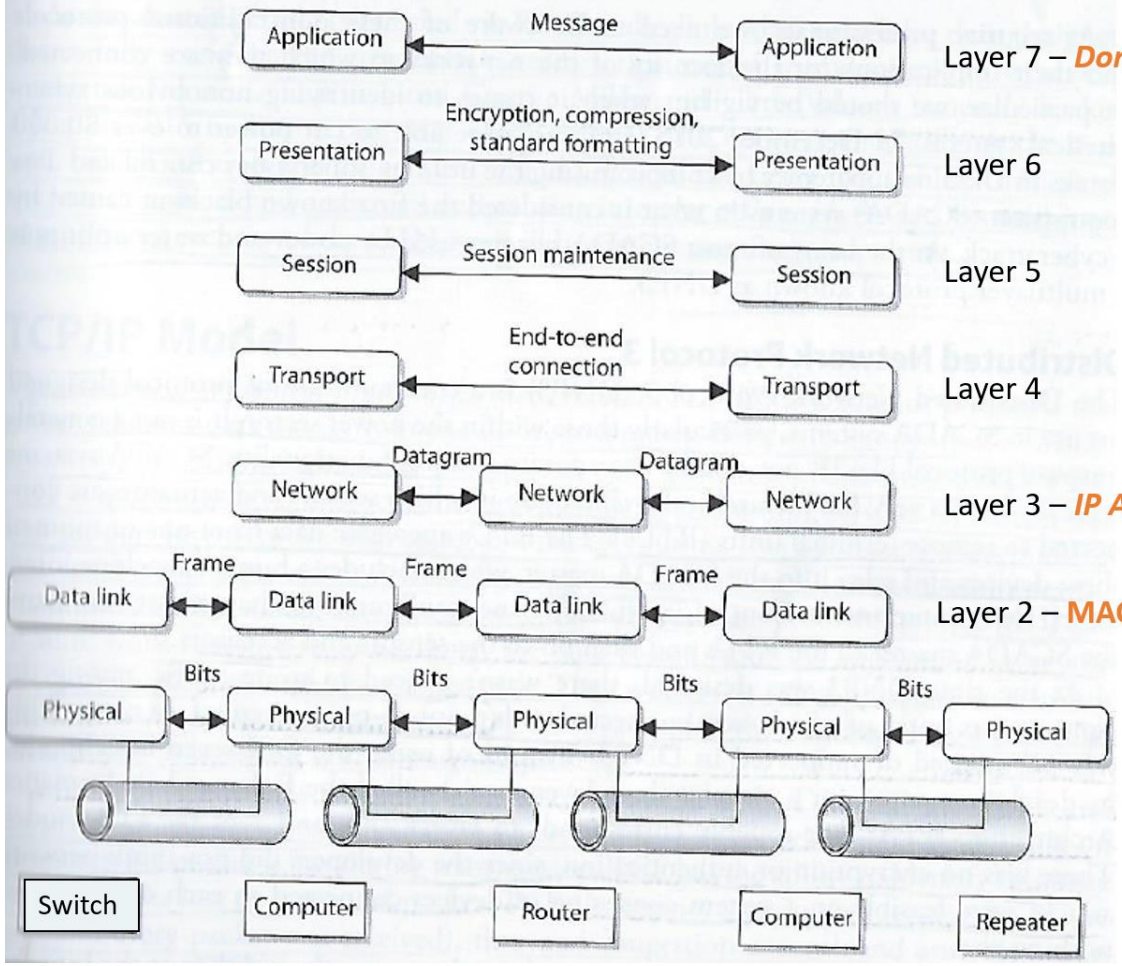
Layer 2 – **MAC (Media Access Control) Address**

Layer 1

Note: Synonyms for host computer across the OSI Model

Linux commands for working with:

- Domain names
- Network availability of computers
- Mapping paths data packets take
- Scanning computer ports

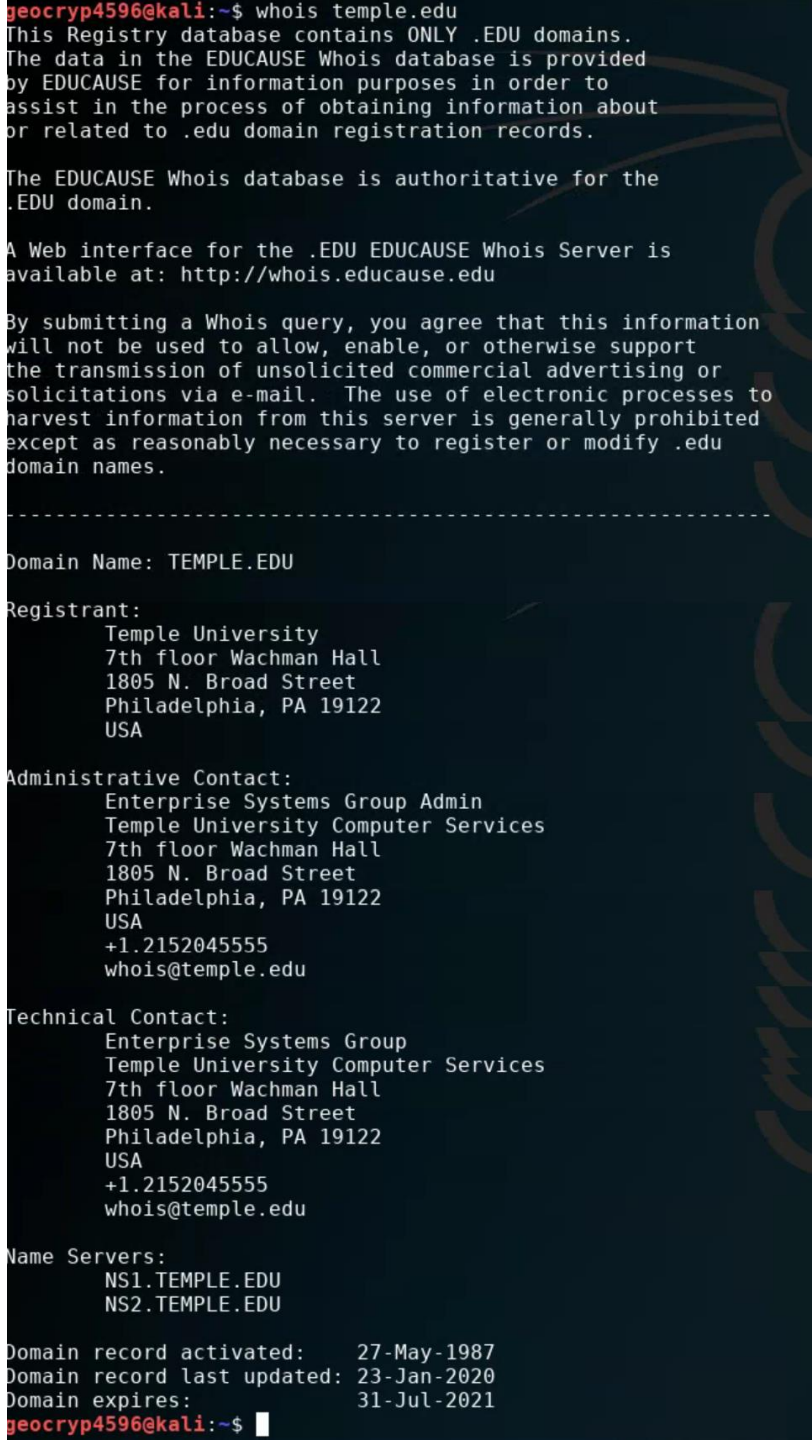


Note: Synonyms for host computer across the OSI Model

whois

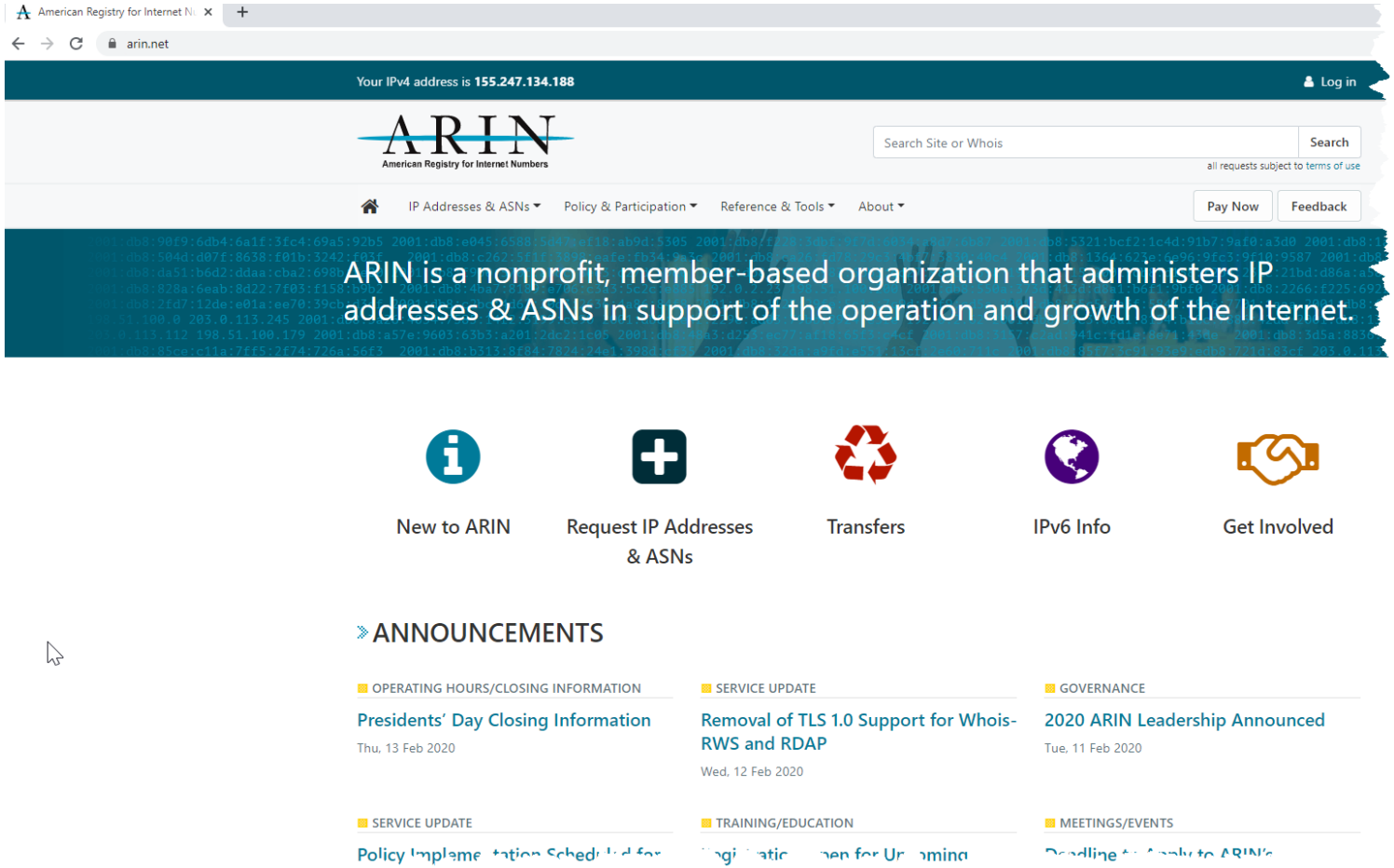
- Database to lookup domain name, IP address, and who registered the address
- Web-based or Command line
  - whois temple.edu

http://www.networksolutions.com/whois/index.jsp

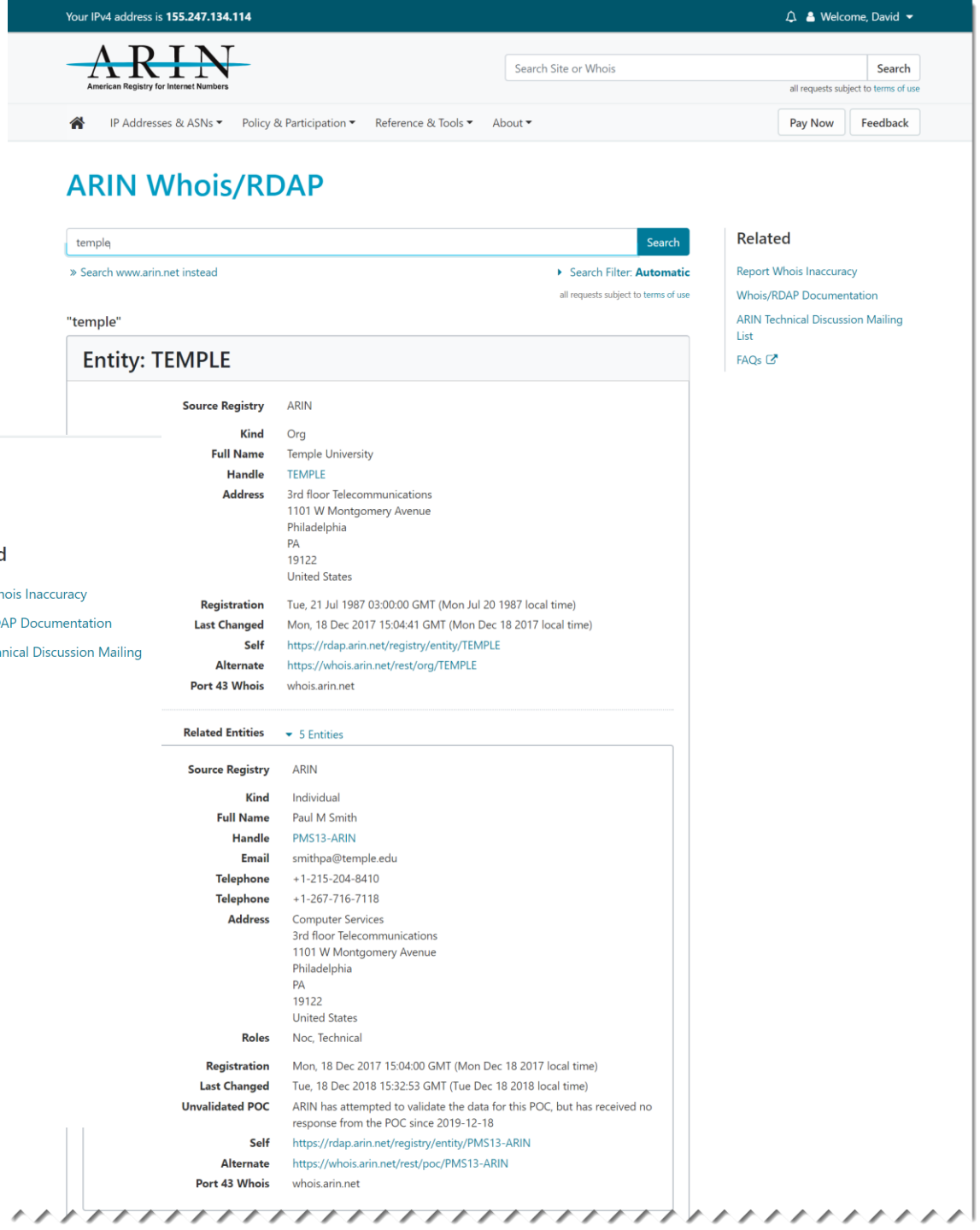


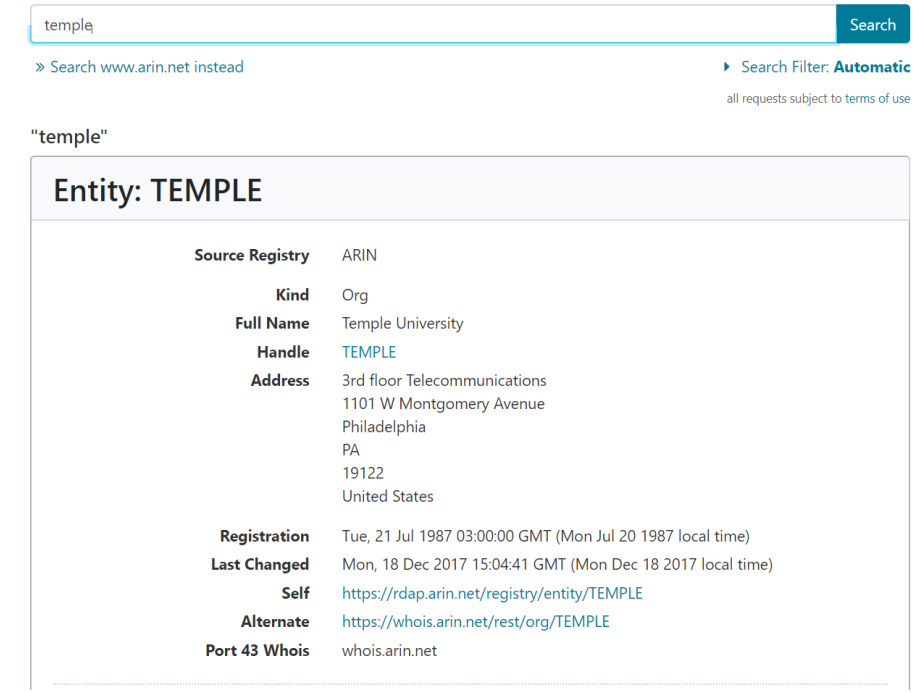
ARIN

- American Registry for Internet Numbers
- Regional Internet Registry for US, Canada, and many Caribbean islands
- ARIN is one of five regional registries
- Provides services related to the technical coordination and management of Internet number resources



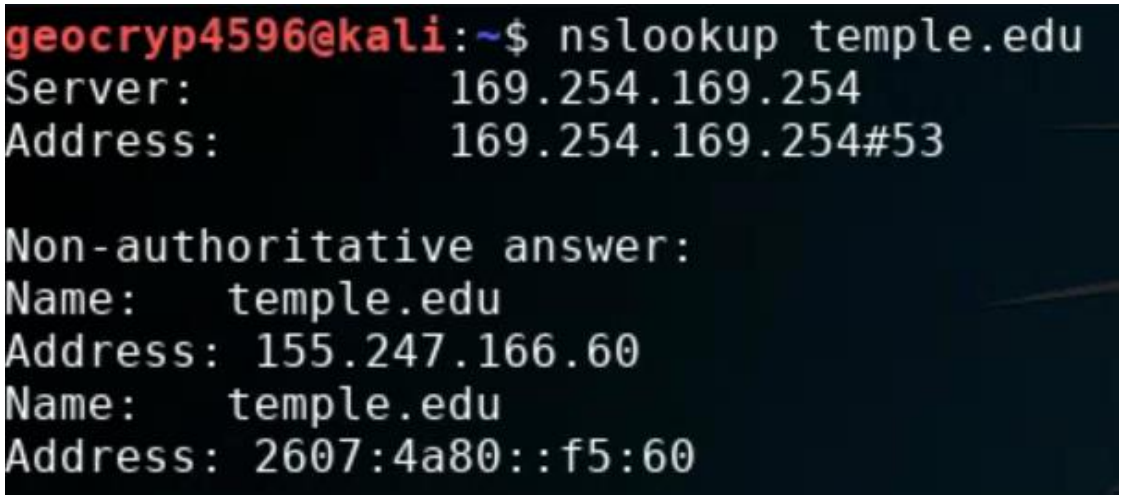
ARIN


Your IPv4 address is 155.247.134.114
Welcome, David
ARIN
American Registry for Internet Numbers
Search Site or Whois
Search
all requests subject to terms of use
IP Addresses & ASNs
Policy & Participation
Reference & Tools
About
Pay Now
Feedback
ARIN Whois/RDAP
temple
Search
» Search www.arin.net instead
Search Filter: Automatic
all requests subject to terms of use
"temple"
Entity: TEMPLE
Source Registry ARIN
Kind Org
Full Name Temple University
Handle TEMPLE
Address 3rd floor Telecommunications
1101 W Montgomery Avenue
Philadelphia
PA
19122
United States
Registration Tue, 21 Jul 1987 03:00:00 GMT (Mon Jul 20 1987 local time)
Last Changed Mon, 18 Dec 2017 15:04:41 GMT (Mon Dec 18 2017 local time)
Self https://rdap.arin.net/registry/entity/TEMPLE
Alternate https://whois.arin.net/rest/org/TEMPLE
Port 43 Whois whois.arin.net
Related Entities 5 Entities
Source Registry ARIN
Kind Individual
Full Name Paul M Smith
Handle PMS13-ARIN
Email smithpa@temple.edu
Telephone +1-215-204-8410
Telephone +1-267-716-7118
Address Computer Services
3rd floor Telecommunications
1101 W Montgomery Avenue
Philadelphia
PA
19122
United States
Roles Noc, Technical
Registration Mon, 18 Dec 2017 15:04:00 GMT (Mon Dec 18 2017 local time)
Last Changed Tue, 18 Dec 2018 15:32:53 GMT (Tue Dec 18 2018 local time)
Unvalidated POC ARIN has attempted to validate the data for this POC, but has received no response from the POC since 2019-12-18
Self https://rdap.arin.net/registry/entity/PMS13-ARIN
Alternate https://whois.arin.net/rest/poc/PMS13-ARIN
Port 43 Whois whois.arin.net
Related
Report Whois Inaccuracy
Whois/RDAP Documentation
ARIN Technical Discussion Mailing List
FAQs


ARIN Whois/RDAP
temple
Search
» Search www.arin.net instead
Search Filter: Automatic
all requests subject to terms of use
"temple"
Entity: TEMPLE
Source Registry ARIN
Kind Org
Full Name Temple University
Handle TEMPLE
Address 3rd floor Telecommunications
1101 W Montgomery Avenue
Philadelphia
PA
19122
United States
Registration Tue, 21 Jul 1987 03:00:00 GMT (Mon Jul 20 1987 local time)
Last Changed Mon, 18 Dec 2017 15:04:41 GMT (Mon Dec 18 2017 local time)
Self https://rdap.arin.net/registry/entity/TEMPLE
Alternate https://whois.arin.net/rest/org/TEMPLE
Port 43 Whois whois.arin.net
Related
Report Whois Inaccuracy
Whois/RDAP Documentation
ARIN Technical Discussion Mailing List
FAQs

DNS

- nslookup – for querying DNS server
  - Example
    - By domain name: nslookup temple.edu
    - By IP address: nslookup 169.254.169.254



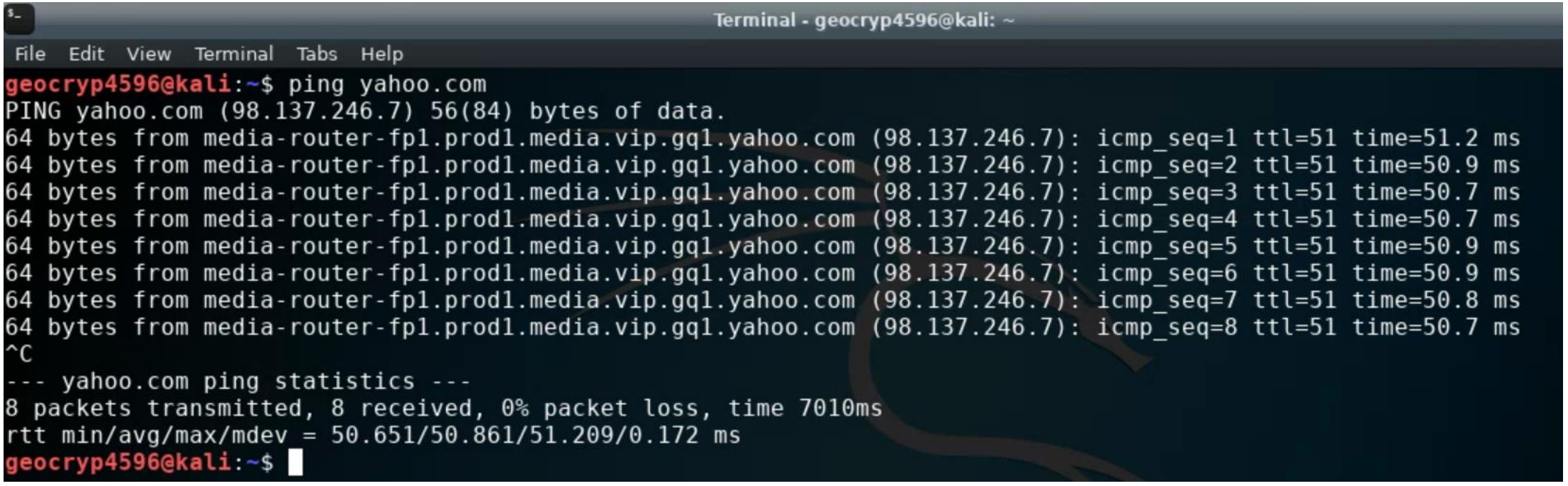
DNS

```
geocryp4596@kali:~$ nslookup 155.247.166.60
;; Truncated, retrying in TCP mode.
60.166.247.155.in-addr.arpa     name = www.tucat.temple.edu.
60.166.247.155.in-addr.arpa     name = mobile.temple.edu.
60.166.247.155.in-addr.arpa     name = www.disabilities.temple.edu.
60.166.247.155.in-addr.arpa     name = Tudad.temple.edu.
60.166.247.155.in-addr.arpa     name = thb3.org.
60.166.247.155.in-addr.arpa     name = research.temple.edu.
60.166.247.155.in-addr.arpa     name = tcalc.temple.edu.
60.166.247.155.in-addr.arpa     name = helpdesk.ocis.temple.edu.
60.166.247.155.in-addr.arpa     name = moulder.temple.edu.
60.166.247.155.in-addr.arpa     name = universitycollege.temple.edu.
60.166.247.155.in-addr.arpa     name = templeent.org.
60.166.247.155.in-addr.arpa     name = government.temple.edu.
60.166.247.155.in-addr.arpa     name = bover.temple.edu.
60.166.247.155.in-addr.arpa     name = teaching.temple.edu.
60.166.247.155.in-addr.arpa     name = community.temple.edu.
60.166.247.155.in-addr.arpa     name = www.thb3.org.
60.166.247.155.in-addr.arpa     name = cla.temple.edu.
60.166.247.155.in-addr.arpa     name = policies.temple.edu.
60.166.247.155.in-addr.arpa     name = phonebook.temple.edu.
60.166.247.155.in-addr.arpa     name = tutr.temple.edu.
60.166.247.155.in-addr.arpa     name = toatest.temple.edu.
60.166.247.155.in-addr.arpa     name = its.temple.edu.
60.166.247.155.in-addr.arpa     name = selfgovernstudycle.edu.
60.166.247.155.in-addr.arpa     name = groupstudy.temple.edu.
60.166.247.155.in-addr.arpa     name = webaudit.temple.edu.
60.166.247.155.in-addr.arpa     name = www.research.temple.edu.
60.166.247.155.in-addr.arpa     name = finance.temple.edu.
60.166.247.155.in-addr.arpa     name = www.challengeandchange.temple.edu.
60.166.247.155.in-addr.arpa     name = givingreport.temple.edu.
60.166.247.155.in-addr.arpa     name = techcenter.temple.edu.
60.166.247.155.in-addr.arpa     name = disabilities.temple.edu.
60.166.247.155.in-addr.arpa     name = templeent.com.
60.166.247.155.in-addr.arpa     name = cph.temple.edu.
60.166.247.155.in-addr.arpa     name = www.templeent.net.
60.166.247.155.in-addr.arpa     name = crc.temple.edu.
60.166.247.155.in-addr.arpa     name = diamonddollars.temple.edu.

Authoritative answers can be found from:

geocryp4596@kali:~$
```

```
geocryp4596@kali:~$ nslookup temple.edu
Server:         169.254.169.254
Address:        169.254.169.254#53

Non-authoritative answer:
Name:   temple.edu
Address: 155.247.166.60
Name:   temple.edu
Address: 2607:4a80::f5:60
```

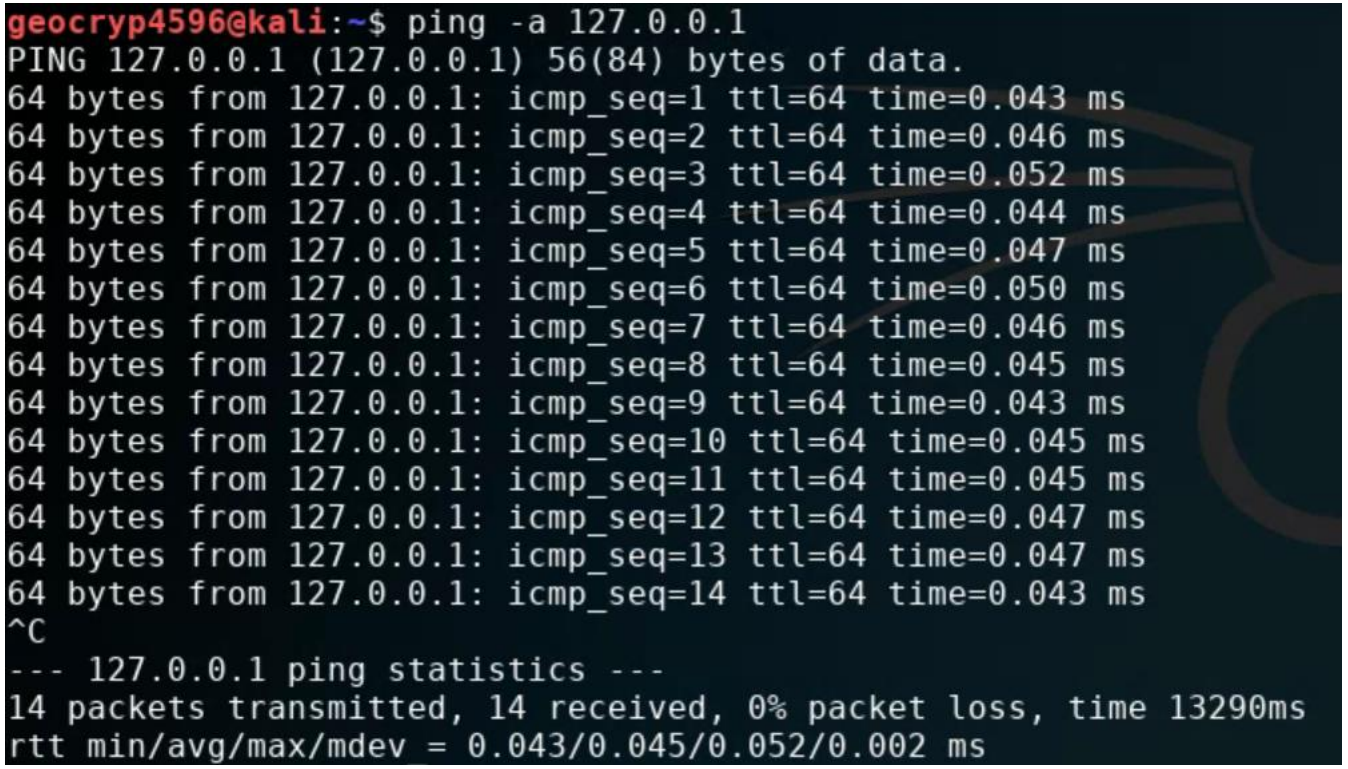
PING – Packet InterNet Groper

- Networking utility
- Used to test whether a host is “alive” on the Internet Protocol (IP) network
- It measures the time it takes for a message sent from one host to reach another and echo back to the original host
- Ctrl+C can stop the ping command

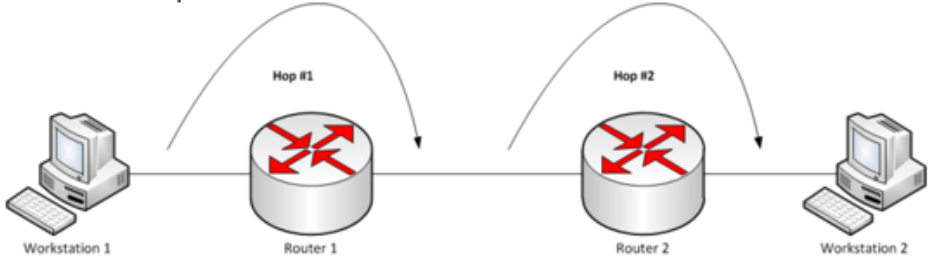


Ping – yourself via your loopback address

- 127.0.0.1 is a special reserved IP address, called a loopback address
- When you ping this address, you are testing your own system to make sure it is working properly
- If this IP does not return an appropriate response, the problem is with your system, not the network, nor the Internet service provider (ISP), or your target URL
- -a parameter resolves to hostname if possible



Traceroute & tracert




```
File  Edit  View  Terminal  Tabs  Help
geocryp4596@kali:~$ traceroute yahoo.com
traceroute to yahoo.com (98.137.246.7), 30 hops max, 60 byte packets
 1  209.85.241.122 (209.85.241.122)  11.246 ms 209.85.250.34 (209.85.250.34)  10.970 ms 209.85.241.125 (209.85.241.125)  11.576 ms
 2  108.170.244.5 (108.170.244.5)  11.047 ms 108.170.243.172 (108.170.243.172)  12.299 ms 108.170.244.5 (108.170.244.5)  11.001 ms
 3  * * *
 4  et-19-1-0.clr2-a-gdc.gq1.yahoo.com (67.195.37.99)  54.576 ms ae-5.pat1.dnx.yahoo.com (216.115.96.34)  49.261 ms  49.271 ms
 5  ae-6.pat1.gqb.yahoo.com (216.115.101.195)  54.596 ms  55.010 ms  57.126 ms
 6  et-1-0-0.msr2.gq1.yahoo.com (66.196.67.113)  54.449 ms et-19-1-0.msr2.gq1.yahoo.com (66.196.67.111)  53.909 ms et-18-1-0.msr1.gq1.yahoo.com (66.196.67.103)  49.919 ms
 7  et-1-0-0.clr2-a-gdc.gq1.yahoo.com (67.195.37.97)  50.270 ms et-19-1-0.clr2-a-gdc.gq1.yahoo.com (67.195.37.99)  53.394 ms et-1-0-0.clr2-a-gdc.gq1.yahoo.com (67.195.37.97)  50.877 ms
 8  et-18-6.bas2-2-flk.gq1.yahoo.com (98.137.120.27)  54.361 ms et-16-6.bas1-2-flk.gq1.yahoo.com (98.137.120.6)  53.610 ms et-18-6.bas1-2-flk.gq1.yahoo.com (98.137.120.25)  50.504 ms
 9  media-router-fp1.prod1.media.vip.gq1.yahoo.com (98.137.246.7)  50.526 ms  50.881 ms  50.366 ms
geocryp4596@kali:~$
```

Traceroute (Mac and Linux) and tracert (Windows) are computer network diagnostic commands for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network

- The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path); the sum of the mean times in each hop is a measure of the total time spent to establish the connection

- Traceroute proceeds unless all sent packets are lost more than twice; then the connection is considered lost and the route cannot be evaluated

Ping, on the other hand, only computes the final round-trip times from the destination point

Scanning

- Goals:
  - Find live network hosts, firewalls, routers, printers, etc.
  - Work out network topology
  - Operating systems used
  - Open ports
  - Available network services
  - Potential vulnerabilities
- While minimizing the chance of disrupting operations – have permission!

Scanning

Increasing disruption

Types of scans:

- Sweep – Send a series of probes to find live hosts (does not cause disruption)
  - (ICMP ping) “pinging the network”
- Trace – use tools like traceroute and/or tracert to map network
- Port scanning – Checks for open TCP or UDP ports
- Fingerprinting – Determines the operating system (OS) running on the computer
- Version scanning – finding versions of services and protocols
- Vulnerability scanning – looks for weaknesses in OS, versions, and configurations (may cause disruptions!)

- Always target your scans by IP address rather than URL or domain name

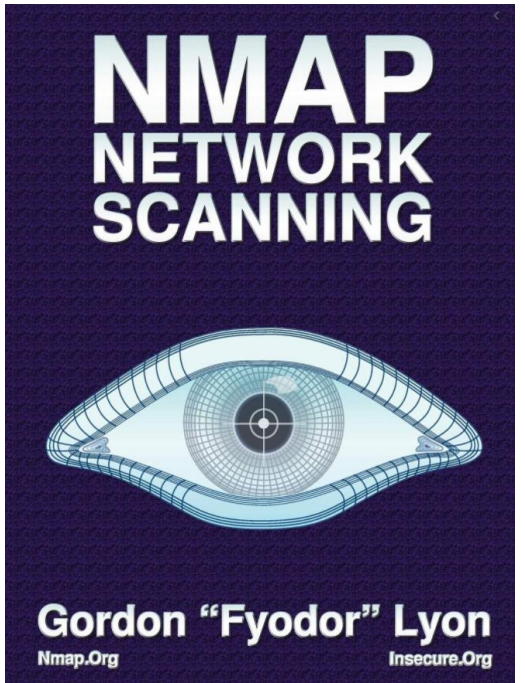
nmap – “Network Mapper”

A free and open-source utility for network security auditing

Nmap uses raw IP packets to determine:

- What hosts are available on the network
- What services (application name & version) those hosts are offering
- What operating systems (& OS version) they are running
- What type of packet filters/firewalls are in use
- …and other useful information…

NMAP Network Scanning by Gordon “Fyodor” Lyon, 2008



A suitable target for nmap: Metasploitable

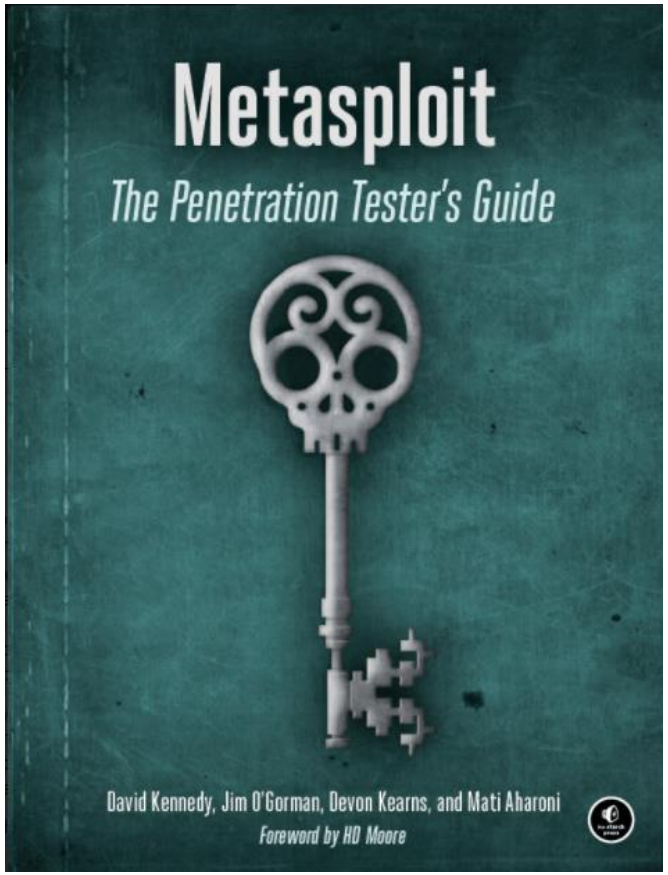
- Deliberately developed vulnerable version of Linux
- Created to support training on the Metasploit Framework

Metasploit Project

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7. Wikipedia

Developer: HD Moore

Programming language: Ruby



Vulnerability Scanning Lab

Lab: Vulnerability Scanning

By Drs. Anthony Vance and Dave Eargle

This lab uses the following VMs:

- Kali
- Metasploitable2

Important!

- Read the section **here** on how to launch the Metasploitable2 virtual machine within Kali.
- Ensure that you can `ping` Metasploitable2 from Kali, and Kali from Metasploitable2, before continuing the lab.
- Use the addresses shown in the **infosec-net network map**.

The objective of this lab is to create a report of potential vulnerabilities for a virtual machine. The VM is a Ubuntu-based Linux distribution called MetaSploitable2, which is specifically designed to teach penetration testing skills such as vulnerability scanning.

During the lab, you may envision yourself as a defender, checking an organizational assets for vulnerabilities visible from an external perspective with the ultimate intention of patching them. Alternatively, you may envision yourself as an attacker, checking a target victim asset for vulnerabilities, with the ultimate intention of exploiting them. Both defenders and attackers may perform the same steps of vulnerability scanning.

Part 0. Ensure that your metasploitable2 instance is up-to-date

Follow instructions for turning on Metasploitable…

Using the virtual machines within Kali

1. The virtual machines are accessed using `virt-manager`. First, you should make sure that your user account is a member of the `libvirt` group.

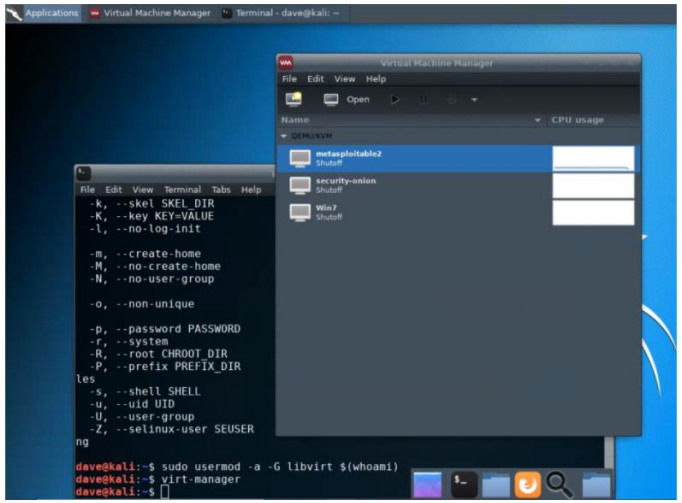
```
sudo usermod -a -G libvirt $(whoami)
```

> Heads up! This will need to be run each time you create a new Kali instance.

Alternatively, log in as root (password `toor`):

```
su root
```

2. Then, from a terminal, run `virt-manager` to get an interface such as the following:



https://anthonyvance.com/security-assignments/labs/lab_vulnerability_scanning.html

Computer ports

https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

Port Ranges	Category
0 - 1,023	Well-Known Ports
1,024 - 49,151	Registered Ports
49,152 - 65,535	Private/Dynamic Ports

Port #	Portocol	Description	Status
0	TCP, UDP	Reserved; do not use (but is a permissible source port value if the sending process does not expect messages in response)	Offical
1	TCP, UDP	TCPMUX	Offical
5	TCP, UDP	RJE (Remote Job Entry)	Offical
7	TCP, UDP	ECHO protocol	Offical
9	TCP, UDP	DISCARD protocol	Offical
11	TCP, UDP	SYSTAT protocol	Offical
13	TCP, UDP	DAYTIME protocol	Offical
17	TCP, UDP	QOTD (Quote of the Day) protocol	Offical
18	TCP, UDP	Message Send Protocol	Offical
19	TCP, UDP	CHARGEN (Character Generator) protocol	Offical
20	TCP	FTP - data port (FTP-d)	Offical
21	TCP	FTP - control (command) port (FTP-c)	Offical
22	TCP, UDP	SSH (Secure Shell) - used for secure logins, file transfers (scp, sftp) and port forwarding	Offical
23	TCP, UDP	Telnet protocol - unencrypted text communications	Offical
25	TCP, UDP	SMTP (Simple Mail Transport Protocol) - used for e-mail routing between mailservers	Offical
26	TCP, UDP	RSFTP - A simple FTP-like protocol	Unoffical
35	TCP, UDP	QMS Magicolor 2 printer	Unoffical
37	TCP, UDP	TIME protocol	Offical
38	TCP, UDP	Route Access Protocol	Offical
39	TCP, UDP	Resource Location Protocol	Offical
41	TCP, UDP	Graphics	Offical
42	TCP, UDP	Host Name Server	Offical
43	TCP	WHOIS protocol	Offical
49	TCP, UDP	TACACS Login Host protocol	Offical
53	TCP, UDP	DNS (Domain Name System)	Offical
57	TCP	MTP, Mail Transfer Protocol	Offical
67	UDP	BOOTP (BootStrap Protocol) server; also used by DHCP (Dynamic Host Configuration Protocol)	Offical
68	UDP	BOOTP client; also used by DHCP	Offical
69	UDP	TFTP (Trivial File Transfer Protocol)	Offical
70	TCP	Gopher protocol	Offical
79	TCP	Finger protocol	Offical
80	TCP	HTTP (HyperText Transfer Protocol) - used for transferring web pages	Offical
81	TCP	Torpark - Onion routing ORport	Unoffical
82	UDP	Torpark - Control Port	Unoffical
88	TCP	Kerberos - authenticating agent	Offical

101	TCP	HOSTNAME	
102	TCP	ISO-TSAP protocol	
107	TCP	Remote Telnet Service	
109	TCP	POP, Post Office Protocol, version 2	
110	TCP	POP3 (Post Office Protocol version 3) - used for retrieving E-mails	Offical
111	TCP, UDP	SUNRPC protocol	
113	TCP	ident - old server identification system, still used by IRC servers to identify its users	Offical
115	TCP	SFTP, Simple File Transfer Protocol	
117	TCP	UUCP-PATH	
118	TCP, UDP	SQL Services	Offical
119	TCP	NNTP (Network News Transfer Protocol) - used for retrieving newsgroups messages	Offical
123	UDP	NTP (Network Time Protocol) - used for time synchronization	Offical
135	TCP, UDP	EPMAP / Microsoft RPC Locator Service	Offical
137	TCP, UDP	NetBIOS NetBIOS Name Service	Offical
138	TCP, UDP	NetBIOS NetBIOS Datagram Service	Offical
139	TCP, UDP	NetBIOS NetBIOS Session Service	Offical
143	TCP, UDP	IMAP4 (Internet Message Access Protocol 4) - used for retrieving E-mails	Offical
152	TCP, UDP	BFTP, Background File Transfer Program	
153	TCP, UDP	SGMP, Simple Gateway Monitoring Protoc	
156	TCP, UDP	SQL Service	
158	TCP, UDP	DMSP, Distributed Mail Service Protocol	
161	TCP, UDP	SNMP (Simple Network Management Prot	
162	TCP, UDP	SNMPTRAP	
170	TCP	Print-srv	
179	TCP	BGP (Border Gateway Protocol)	
194	TCP	IRC (Internet Relay Chat)	
201	TCP, UDP	AppleTalk Routing Maintenance	
209	TCP, UDP	The Quick Mail Transfer Protocol	
213	TCP, UDP	IPX	
218	TCP, UDP	MPP, Message Posting Protocol	
220	TCP, UDP	IMAP, Interactive Mail Access Protocol, ve	
259	TCP, UDP	ESRO, Efficient Short Remote Operations	
264	TCP, UDP	BGMP, Border Gateway Multicast Protocol	
311	TCP	Apple Server-Admin-Tool, Workgroup-Man	
318	TCP, UDP	TSP, Time Stamp Protocol	
323	TCP, UDP	IMMP, Internet Message Mapping Protocol	
383	TCP, UDP	HP OpenView HTTPs Operations Agent	
366	TCP, UDP	SMTP, Simple Mail Transfer Protocol. ODM Relay	
369	TCP, UDP	Rpc2portmap	
371	TCP, UDP	ClearCase albd	
384	TCP, UDP	A Remote Network Server System	
387	TCP, UDP	AURP, AppleTalk Update-based Routing P	
389	TCP, UDP	LDAP (Lightweight Directory Access Proto	

401	TCP, UDP	UPS Uninterruptible Power Supply	Offical
411	TCP	Direct Connect Hub port	Unoffical
427	TCP, UDP	SLP (Service Location Protocol)	Offical
443	TCP	HTTPS - HTTP Protocol over TLS/SSL (encrypted transmission)	Offical
444	TCP, UDP	SNPP, Simple Network Paging Protocol	
445	TCP	Microsoft-DS (Active Directory, Windows shares, Sasser worm, Agobot, Zobotworm)	Offical
445	UDP	Microsoft-DS SMB file sharing	Offical
464	TCP, UDP	Kerberos Change/Set password	Offical
465	TCP	SMTP over SSL - CONFLICT with registered Cisco protocol	Conflict
500	TCP, UDP	ISAKMP, IKE-Internet Key Exchange	Offical
512	TCP	exec, Remote Process Execution	
512	UDP	comsat, together with biff: notifies users of new c.q. yet unread e-mail	
513	TCP	Login	
513	UDP	Who	
514	TCP	rsh protocol - used to execute non-interactive commandline commands on a remote system and see the screen return	
514	UDP	syslog protocol - used for system logging	Offical
515	TCP	Line Printer Daemon protocol - used in LPD printer servers	

593	TCP, UDP	HTTP RPC Ep Map	Offical
604	TCP	TUNNEL	
631	TCP, UDP	IPP, Internet Printing Protocol	
636	TCP, UDP	LDAP over SSL (encrypted transmission)	Offical
639	TCP, UDP	MSDP, Multicast Source Discovery Protocol	
646	TCP	LDP, Label Distribution Protocol	
647	TCP	DHCP Failover Protocol	
648	TCP	RRP, Registry Registrar Protocol	
652	TCP	DTCP, Dynamic Tunnel Configuration Protocol	
654	TCP	AODV, Ad hoc On-Demand Distance Vector	
665	TCP	sun-dr, Remote Dynamic Reconfiguration	Unoffical
666	UDP	Doom, First online FPS	
674	TCP	ACAP, Application Configuration Access Protocol	
691	TCP	MS Exchange Routing	Offical
692	TCP	Hyperwave-ISP	
695	TCP	IEEE-MMS-SSL	
698	TCP	OLSR, Optimized Link State Routing	
699	TCP	Access Network	
700	TCP	EPP, Extensible Provisioning Protocol	

Port # / Layer	Name	
1080	socks	SOCKS network application proxy services
1236	bvcontrol [rmtcfg]	Remote configuration server for Gracilis Packeten network switches[
1300	h323hostcallsc	H.323 telecommunication Host Call Secure
1433	ms-sql-s	Microsoft SQL Server
1434	ms-sql-m	Microsoft SQL Monitor
1494	ica	Citrix ICA Client
1512	wins	Microsoft Windows Internet Name Server
1524	ingreslock	Ingres Database Management System (DBMS) lock services
1525	prospero-np	Prospero non-privileged
1645	datametrics [old-radius]	Datametrics / old radius entry
1646	sa-msg-port [oldradacct]	sa-msg-port / old radacct entry

Metasploitable is accessed over HTTP default port 80 192.168.55.102:80

Virtual Machines for the Security Labs

By Drs. Anthony Vance and Dave Eargle

This page documents virtual machines that I have prepared for students in my class to use to complete the labs.

Setting up your virtual lab

I have created a Kali virtual machine image on Google Cloud Platform which is using nested virtualization to host within it several virtual machines: a Windows instance, a Metasploitable2 instance, and a security onion instance. They are hosted using `kvm` and `libvirt` and accessed using `virt-manager`.

Read these instructions to get oriented to and set up on Google Cloud Platform, and to get access to the Kali virtual machine. Anyone should be able to see and use the custom class kali image if they join this Google Group (public access):

`infosec-net` Network Map

The network map is as follows:

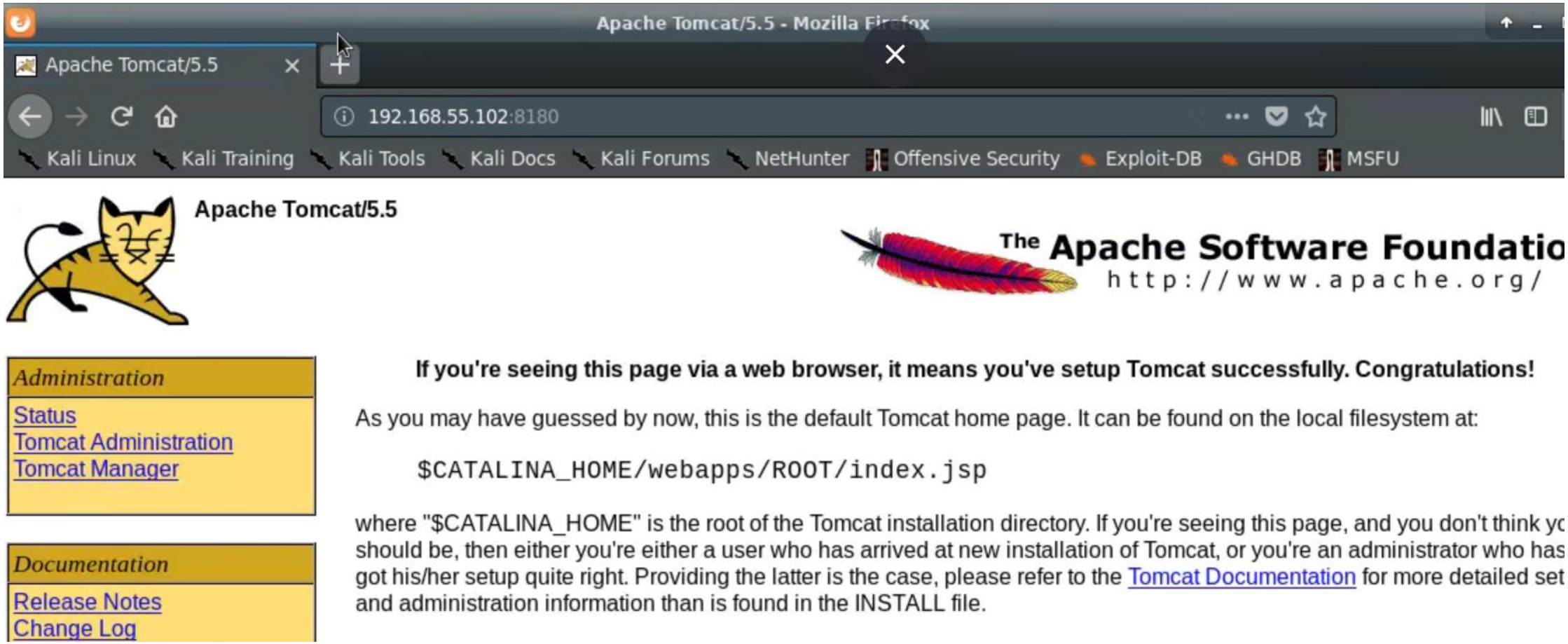
IP Address	Machine
192.168.55.101	Kali (the host)
192.168.55.100	Windows 7
192.168.55.102	Metasploitable2
192.168.55.103	Security Onion


```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

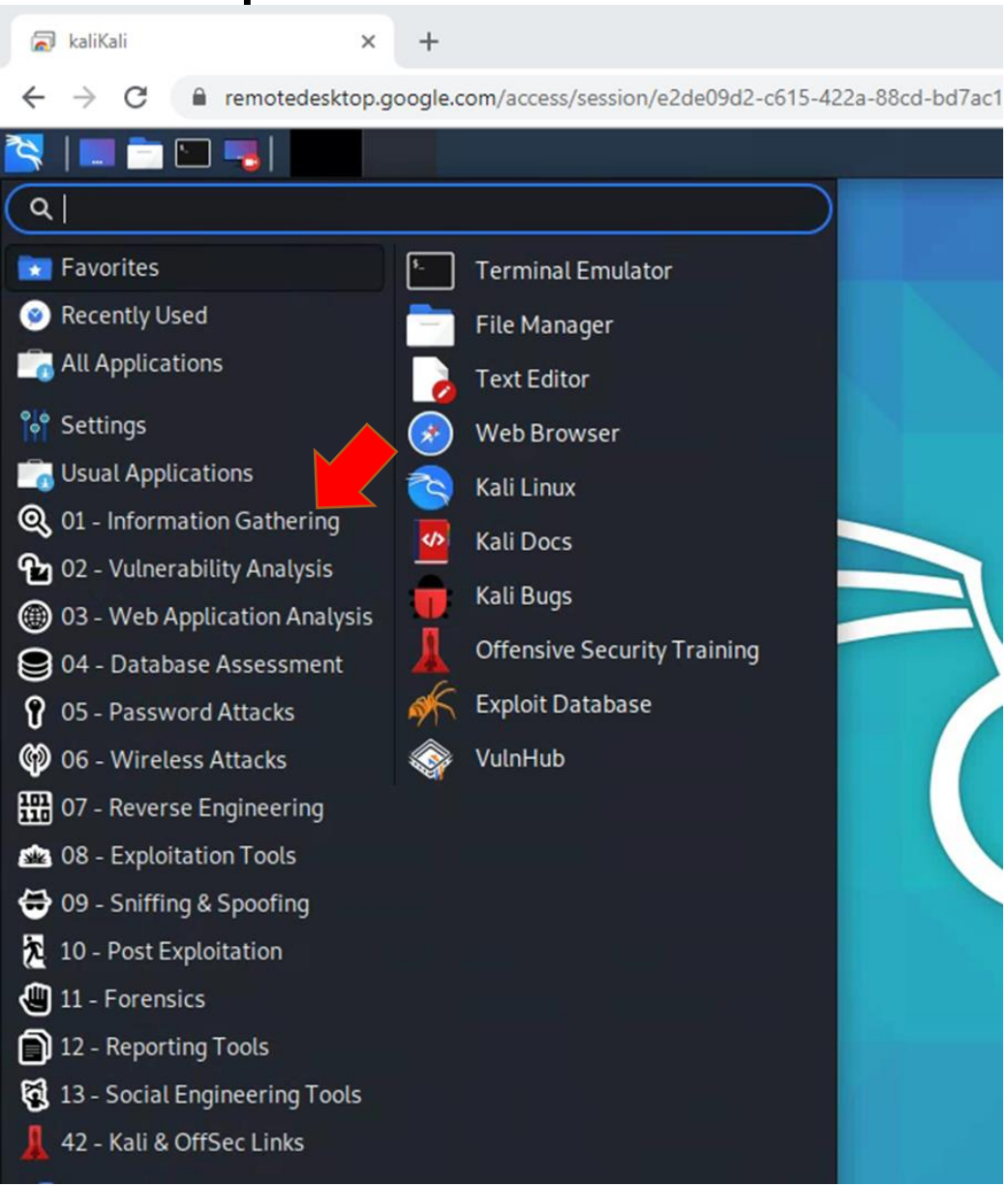
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

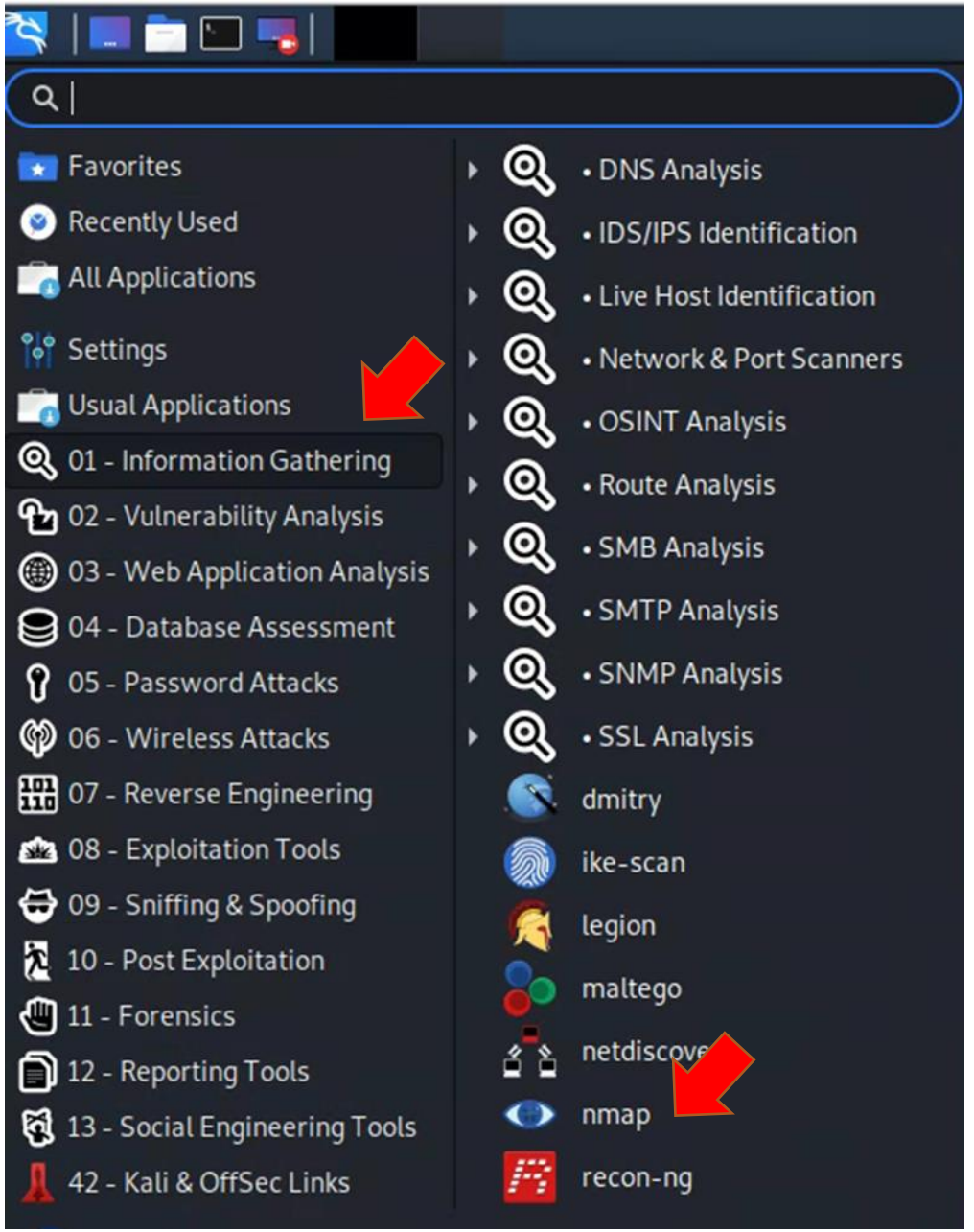
192.168.55.102:8180

Tomcat (within the Metasploitable Linux server) provides a "pure Java" HTTP web server environment in which Java code can run

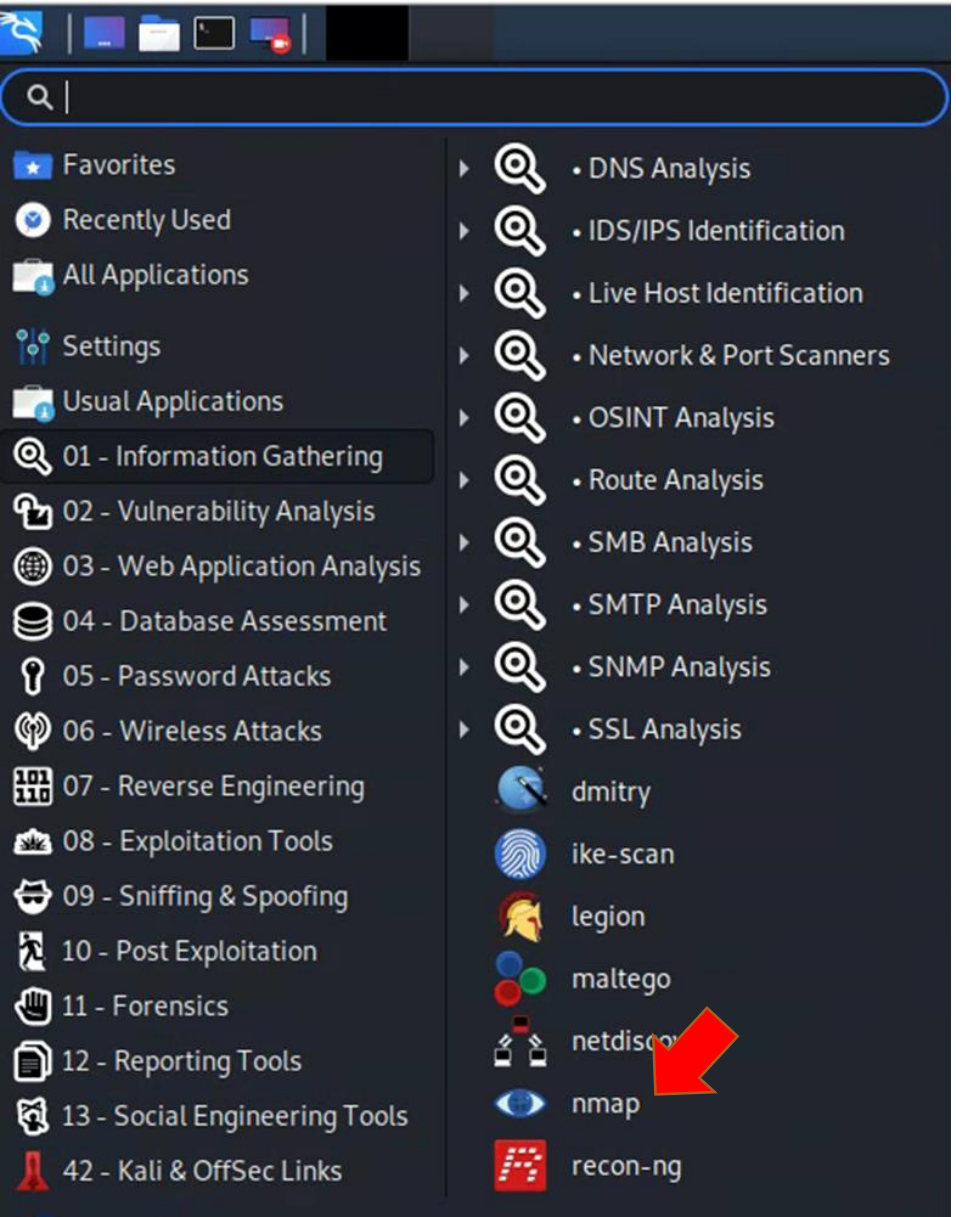


Nmap location on Kali



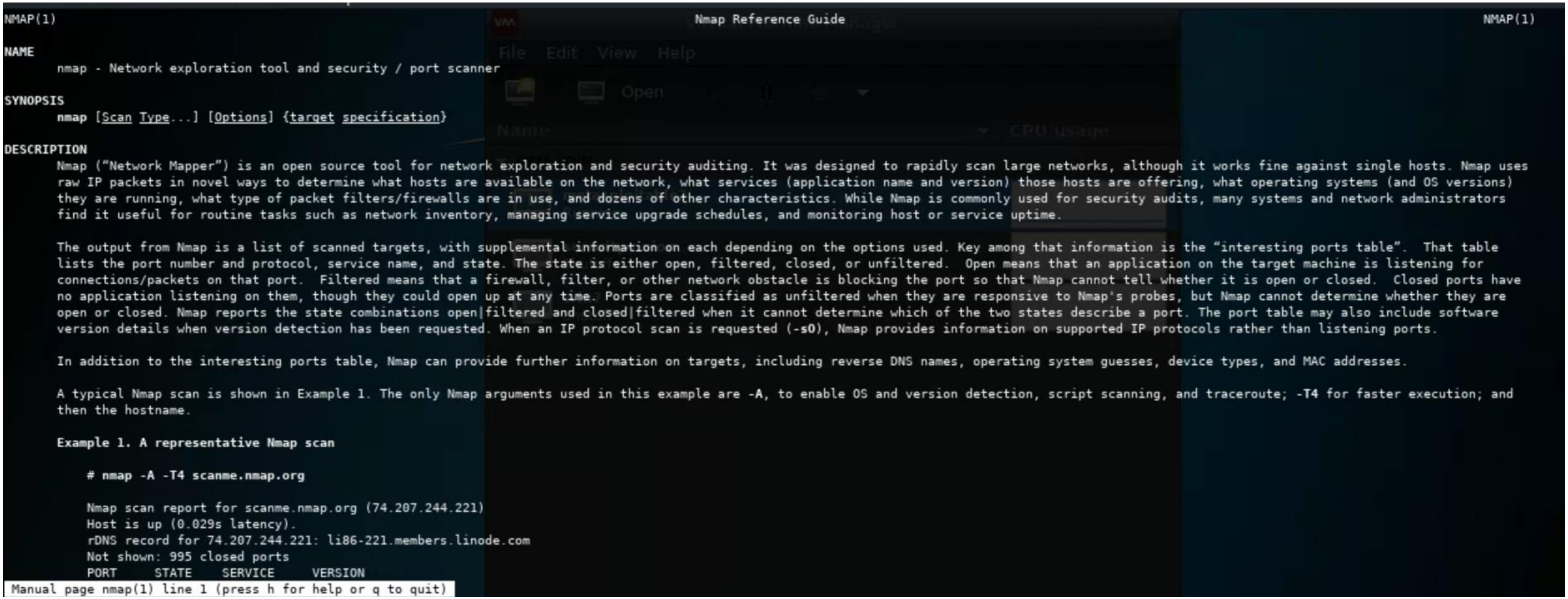


Starting nmap

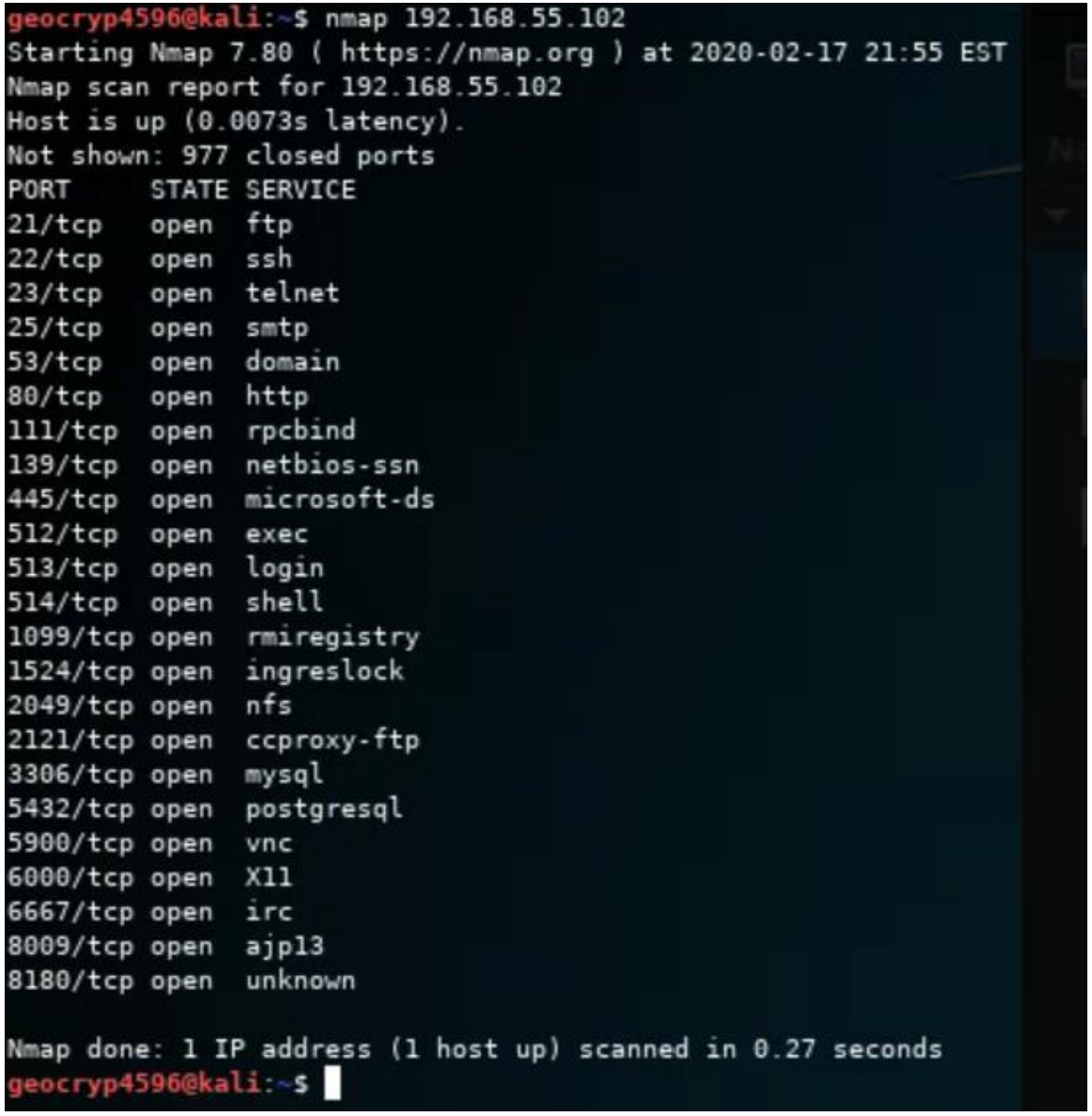



```
File  Actions  Edit  View  Help

> Executing "nmap"
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {targ
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networ
  Ex: scanme.nmap.org, microsoft.com/24, 1
  -iL <inputfilename>: Input from list of
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: E
  --excludefile <exclude_file>: Exclude li
HOST DISCOVERY:
  -sL: List Scan - simply list targets to
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip h
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP
  -PE/PP/PM: ICMP echo, timestamp, and net
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always re
  --dns-servers <serv1[,serv2],...>: Speci
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each hos
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/W
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified po
    Ex: -p22; -p1-65535; -p U:53,111,137,T
  --exclude-ports <port ranges>: Exclude t
  -F: Fast mode - Scan fewer ports than th
  -r: Scan ports consecutively - don't ran
  --top-ports <number>: Scan <number> most
  --port-ratio <ratio>: Scan ports more co
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine servi
  --version-intensity <level>: Set from 0
  --version-light: Limit to most likely pr
  --version-all: Try every single probe (i
  --version-trace: Show detailed version s
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is
          directories, script-files or sc
  --script-args=<n1=v1,[n2=v2,...]>: provi
  --script-args-file=filename: provide NSE
  --script-trace: Show all data sent and r
  --script-updatedb: Update the script dat
  --script-help=<Lua scripts>: Show help a
          <Lua scripts> is a comma-separa
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
phillipnontenure@kali:~$
```

For help: man nmap



Nmap command line scan of Metasploitable2



Security question:

Do I need all these port open?

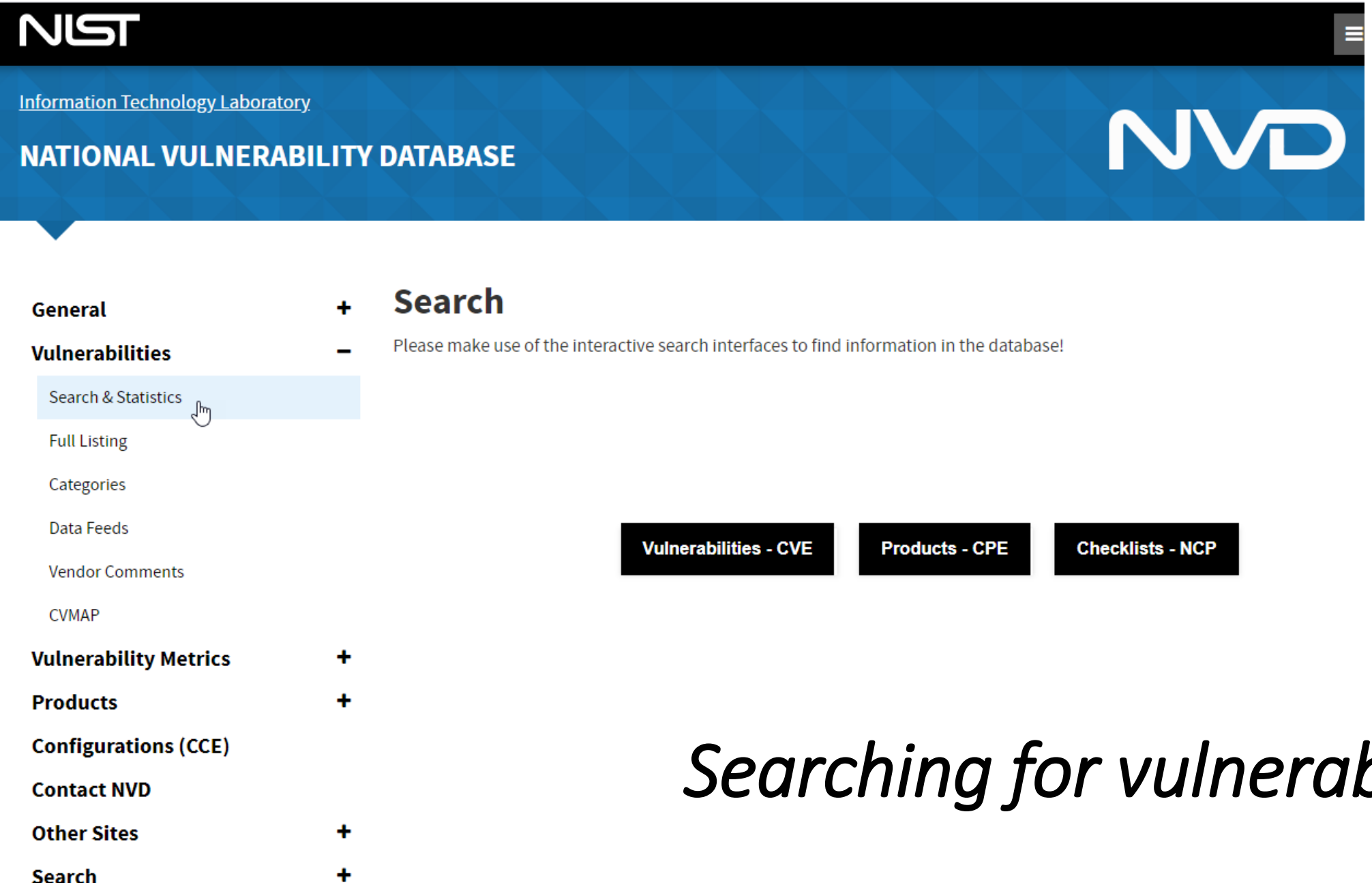
If you do not need them, they should be closed!

Do not get hung up on what the ports are commonly associated with service,
"i.e. 80 is the port commonly associated with HTTP"

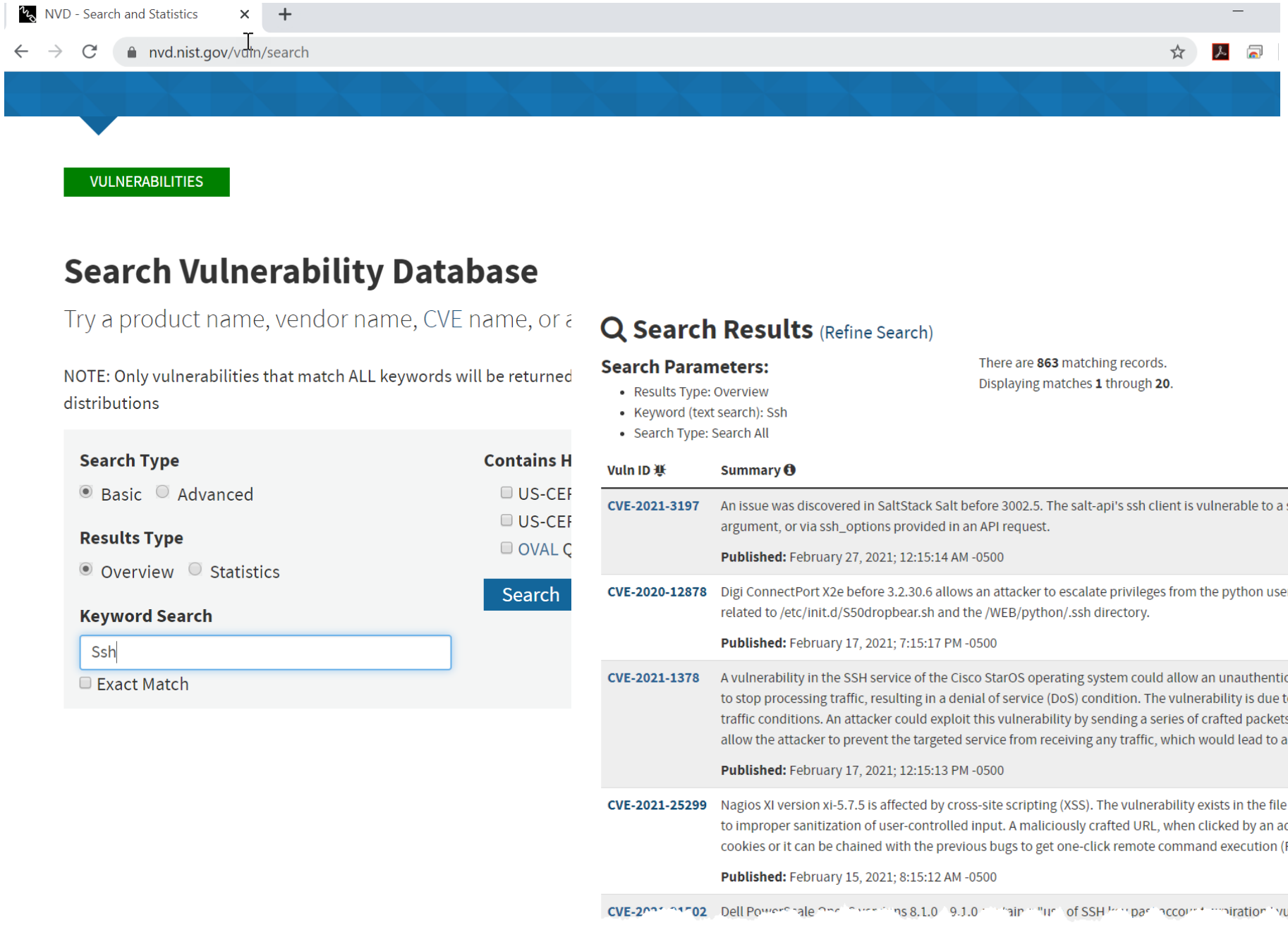
You can put any service anywhere…

Interesting ports for finding possible vulnerabilities to attack:

- ftp
- ssh
- telnet
- smtp (Mail)
- Domain (DNS)
- http (Web Server)
- mysql (database management system)
- postgresql (database management system)



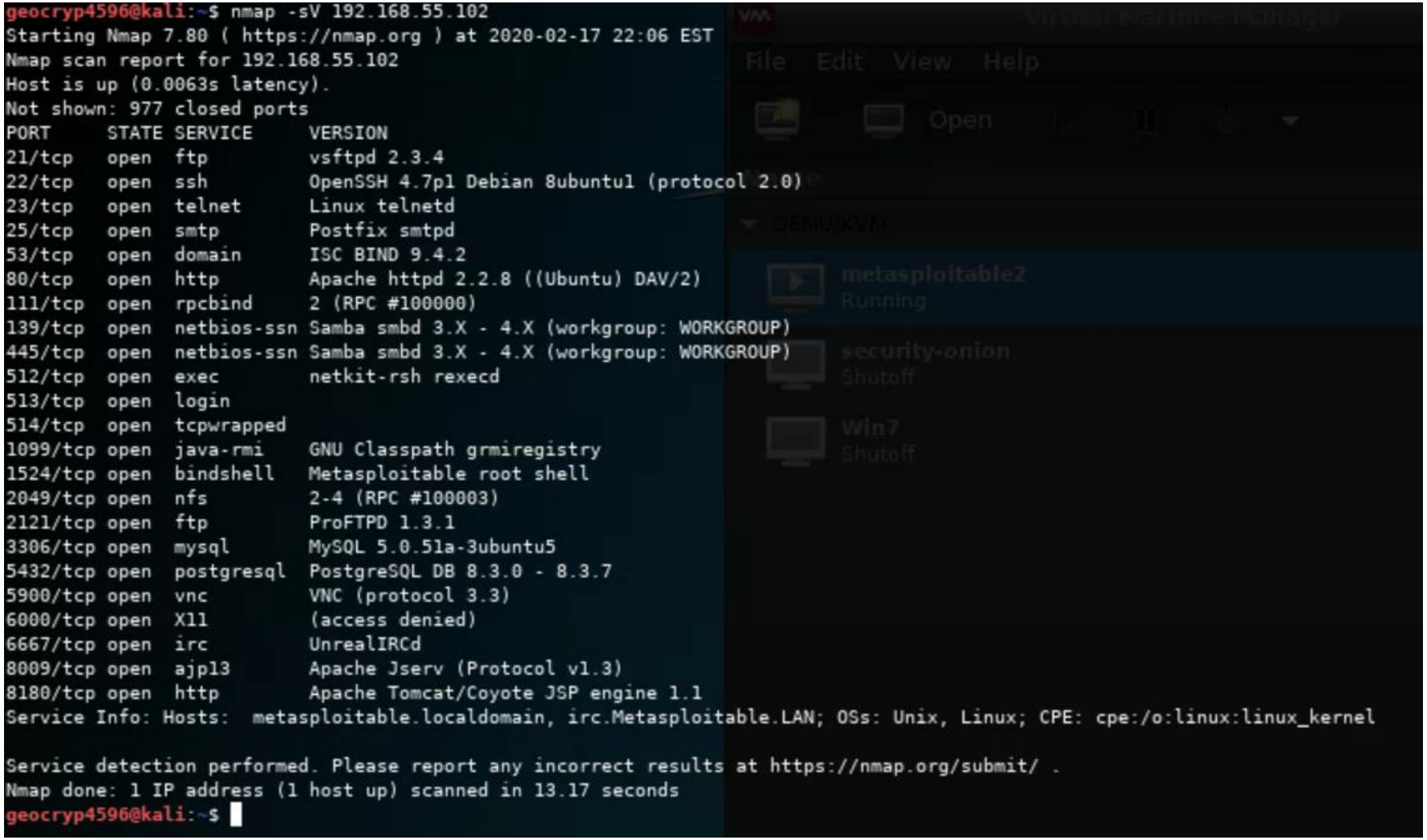
Searching for vulnerabilities


NVD - Search and Statistics
nvd.nist.gov/vuln/search
VULNERABILITIES
Search Vulnerability Database
Try a product name, vendor name, CVE name, or a
NOTE: Only vulnerabilities that match ALL keywords will be returned
distributions
Search Type
Basic
Advanced
Results Type
Overview
Statistics
Keyword Search
Ssh
Exact Match
Contains H
US-CEF
US-CEF
OVAL Q
Search
Search Results (Refine Search)
Search Parameters:
Results Type: Overview
Keyword (text search): Ssh
Search Type: Search All
There are 863 matching records.
Displaying matches 1 through 20.
Sort results by: Publish Date Descending
Sort
1 2 3 4 5 6 7 8 9 10 > >>
Vuln ID
Summary
CVSS Severity
CVE-2021-3197
An issue was discovered in SaltStack Salt before 3002.5. The salt-api's ssh client is vulnerable to a shell injection by including ProxyCommand in an argument, or via ssh_options provided in an API request.
Published: February 27, 2021; 12:15:14 AM -0500
V3.x:(not available)
V2.0:(not available)
CVE-2020-12878
Digi ConnectPort X2e before 3.2.30.6 allows an attacker to escalate privileges from the python user to root via a symlink attack that uses chown, related to /etc/init.d/S50dropbear.sh and the /WEB/python/.ssh directory.
Published: February 17, 2021; 7:15:17 PM -0500
V3.1: 7.8 HIGH
V2.0: 7.2 HIGH
CVE-2021-1378
A vulnerability in the SSH service of the Cisco StarOS operating system could allow an unauthenticated, remote attacker to cause an affected device to stop processing traffic, resulting in a denial of service (DoS) condition. The vulnerability is due to a logic error that may occur under specific traffic conditions. An attacker could exploit this vulnerability by sending a series of crafted packets to an affected device. A successful exploit could allow the attacker to prevent the targeted service from receiving any traffic, which would lead to a DoS condition on the affected device.
Published: February 17, 2021; 12:15:13 PM -0500
V3.1: 7.5 HIGH
V2.0: 5.0 MEDIUM
CVE-2021-25299
Nagios XI version xi-5.7.5 is affected by cross-site scripting (XSS). The vulnerability exists in the file /usr/local/nagiosxi/html/admin/sshterm.php due to improper sanitization of user-controlled input. A maliciously crafted URL, when clicked by an admin user, can be used to steal his/her session cookies or it can be chained with the previous bugs to get one-click remote command execution (RCE) on the Nagios XI server.
Published: February 15, 2021; 8:15:12 AM -0500
V3.1: 6.1 MEDIUM
V2.0: 4.3 MEDIUM
CVE-2021-21502
Dell PowerScale OneFS versions 8.1.0 9.1.0 ... of SSH ... vulnerability. A user on the net... rk with th...
V3.1: 9.8 CR...

nmap parameters

-sV Attempts to determine version of service running

- this is information used to plan an attack

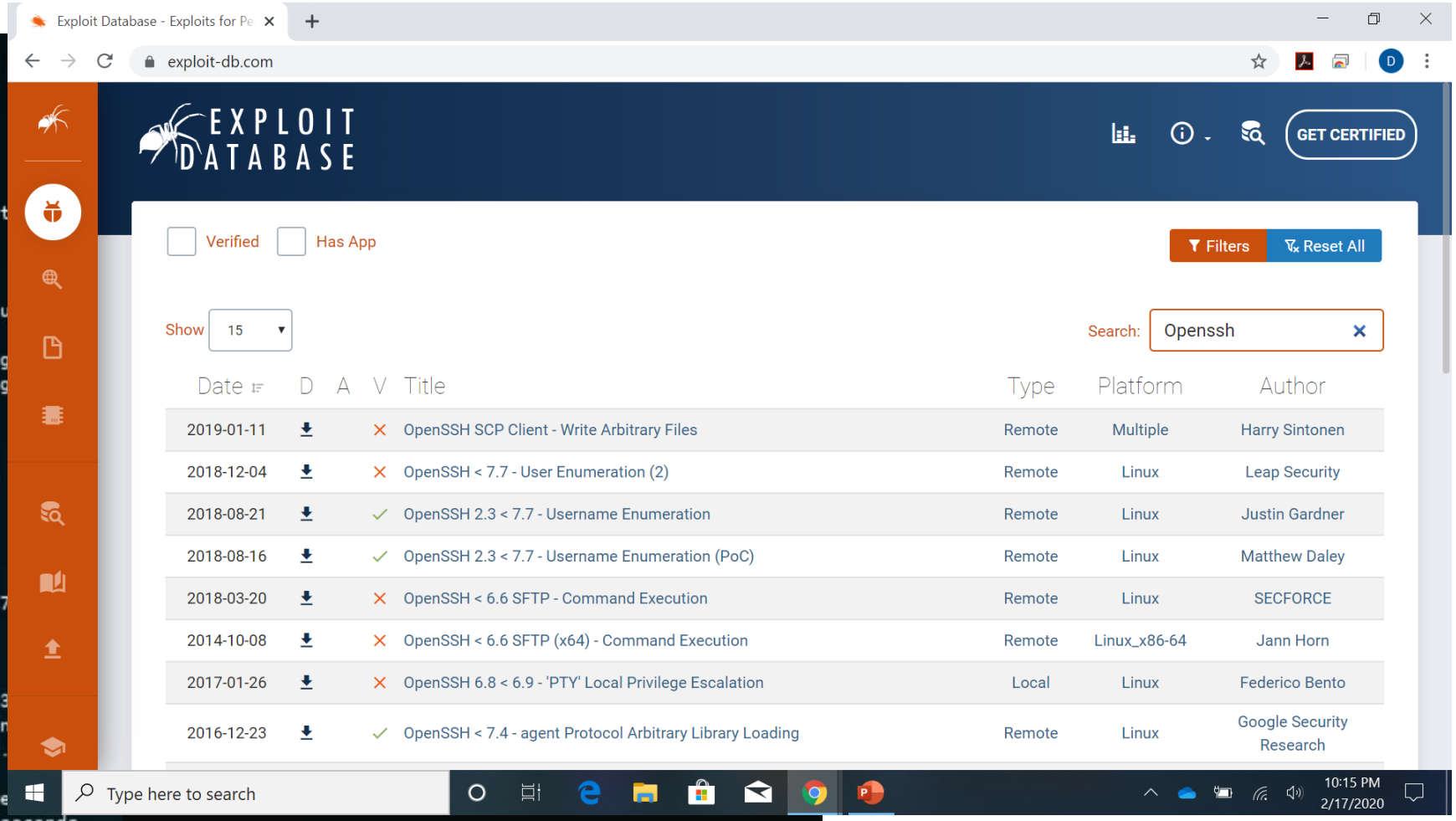


nmap parameters

-sV Attempts to determine version of service running

- this is information used to plan an attack

```
geocryp4596@kali:~$ nmap -sV 192.168.55.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-17
Nmap scan report for 192.168.55.102
Host is up (0.0063s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubunt
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workg
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workg
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3
8180/tcp open  http        Apache Tomcat/Coyote JSP en
Service Info: Hosts:  metasploitable.localdomain, irc.

Service detection performed. Please report any incorre
Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
geocryp4596@kali:~$
```



Network Address Translation (NAT)

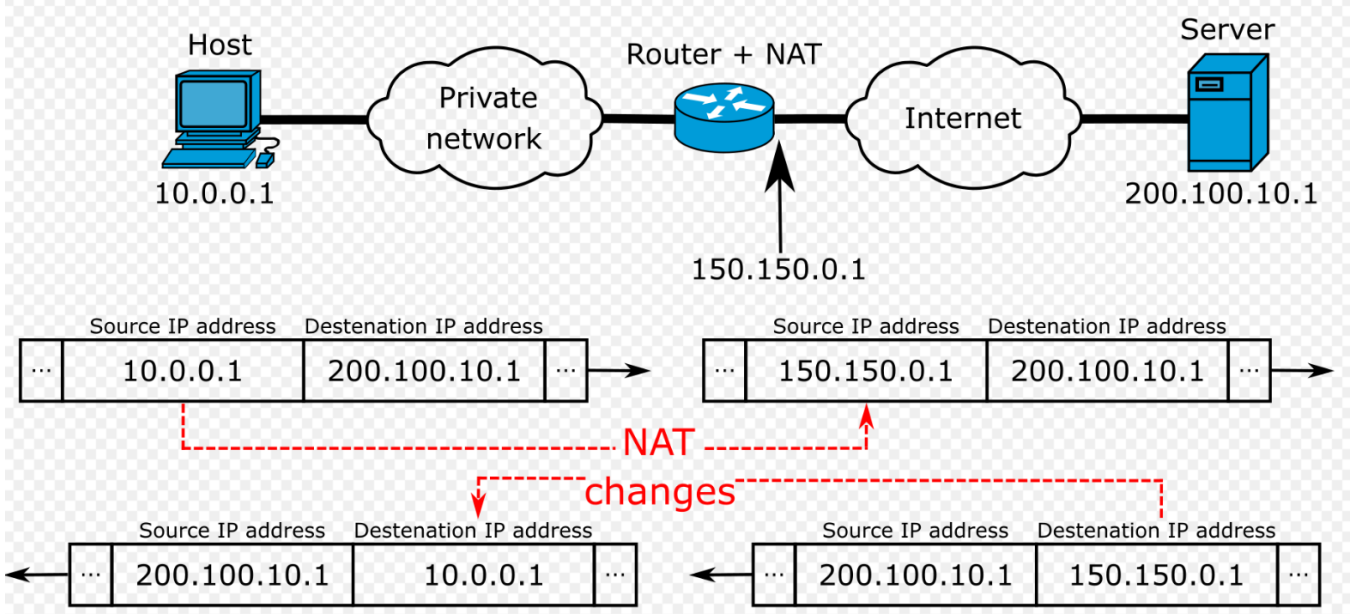
- Search Google for “What is my IP Address”
- Open a terminal and type:
  - Windows: ipconfig
  - Max/Linux: ifconfig
- Does Google report the same IP address as your local computer reports using ipconfig/ifconfig?
- Why not?

Network Address Translation (NAT)

The majority of NATs map multiple private hosts to one publicly exposed IP address

- In a typical configuration, a local network is connected to a router which is also connected to the Internet with a *public* address assigned by an Internet service provider
- As traffic passes through the router with NAT from the local network to the Internet, the source address in each packet is translated on the fly from a private address to the public address

- The router tracks basic data about each active connection (particularly the destination address and port)
- When a reply returns to the router, it uses the connection tracking data it stored during the outbound phase to determine the private address on the internal network to which to forward the reply



To get started…

…do the *Introduction to Networking – Activity*

MIS
MANAGEMENT INFORMATION SYSTEMS

Managing Enterprise Cybersecurity

MIS 4596.001 ▪ Spring 2021 ▪ David Lanter

SCHEDULE | ABOUT | LABS | LECTURE MATERIALS

Labs

Lab: Threat Modeling with Attack Trees

Lab: Web Privacy and Anonymity

Lab: Symmetric Encryption and Hashing

Lab: Asymmetric Encryption

Lab: Digital Certificates

Lab: Password Cracking

Lab: Vulnerability Scanning

Lab: Exploitation

Lab: Social Engineering

Lab: Network Security Monitoring and Security Onion

Lab: Malware Analysis

Tutorials

Tutorial: Introduction to Linux

Tutorial: Introduction to Linux – Supplemental Cowsay Miniadventure

Tutorial: Introduction to Google Cloud Platform

Tutorial: Introduction to Networking

Lab Supplementary Files

RECENT ANNOUN

[More Announcements…]

Infosec Management Home Labs Tutorials

Traceroute
Email Headers
Physical location on the internet
Shodan

Introduction to Networking

By Drs. Anthony Vance and Dave Eargle

Attribution: This page is based on an activity developed by Jennifer Urban and Chris Hoofnagle at UC Berkley.

Do the following activities to help you learn about networking.

Traceroute

The Traceroute command shows the network route or path between your computer and another device on the internet or network.

1. From your computer or Kali Linux VM, open a terminal.

On a Mac, you can do this by clicking command & the space bar and typing `terminal`. In Linux and Mac, the command is `traceroute`.

On Windows, search for `cmd` and press enter. A terminal window should open. On Windows, the command is `tracert`.

1. Type:

```
traceroute yahoo.com
```

Look at all the "hops" of your request to "trace the route," or in other words, follow the path of your request between your computer and one of Yahoo's servers.

Your Kali VM has a private network setup for virtual machines you will be using in your labs

Part 0. Ensure that your metasploitable2 instance is up-to-date

Part 1. Host Discovery and Scanning using NMAP

Part 2. Nessus

Lab: Vulnerability Scanning

By Drs. Anthony Vance and Dave Eargle

This lab uses the following VMs:

Setting up your virtual lab

Using the virtual machines within Kali

Starting and accessing virtual machines

Updating the virtual machines

Using snapshots

How I created the virtual machines

Using the virtual machines within Kali

1. The virtual machines are accessed using `virt-manager`. First, you should make sure that your user account is a member of the `libvirt` group.

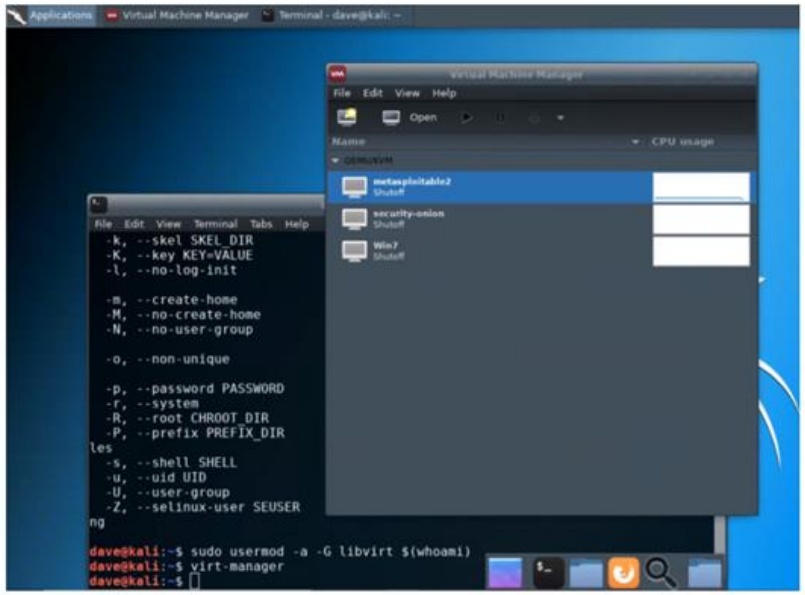
```
sudo usermod -a -G libvirt $(whoami)
```

Heads up! This will need to be run each time you create a new Kali instance.

Alternatively, log in as root (password `toor`):

```
su root
```

2. Then, from a terminal, run `virt-manager` to get an interface such as the following:



`infosec-net` Network Map

The network map is as follows:

IP Address	Machine
192.168.55.101	Kali (the host)
192.168.55.100	Windows 7
192.168.55.102	Metasploitable2
192.168.55.103	Security Onion

Agenda

- ✓OSI Reference Model
- ✓Linux commands for working with:
  - ✓Domain names
  - ✓Network availability of computers
  - ✓Mapping paths data packets take
  - ✓Scanning computer ports
- ✓Vulnerability Scanning Lab
  - ✓Nmap and Metasploitable
- ✓National Vulnerability Database
- ✓Network Address Translation
- ✓Getting started – Introduction to Networking Lab
- ✓Kali's Virtural Machines for labs…