

# Cybersecurity & Networking – Practical Assignment

## Section A: Basic Networking Concepts (Q1–Q10)

### 1. Explore OSI Model Layers

The OSI Model is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven distinct layers. This structure helps break down complex network interactions into manageable parts, making it easier to design, troubleshoot, and understand network systems.

#### 7 layers of the OSI Model

Layer Number	Layer Name	Description
7	Application	Interfaces directly with end-user applications, enabling network services for software.
6	Presentation	Translates, encrypts, and compresses data for the application layer.
5	Session	Manages sessions and controls dialogues between computers.
4	Transport	Ensures reliable data transfer with error checking and flow control (e.g., TCP, UDP).
3	Network	Handles routing and forwarding of data packets (e.g., IP addresses).

Layer Number	Layer Name	Description
7	Application	Interfaces directly with end-user applications, enabling network services for software.
2	Data Link	Provides node-to-node data transfer and handles error correction from the physical layer.
1	Physical	Transmits raw bit streams over a physical medium (e.g., cables, switches).

## 2. Difference Between Router and Modem

A modem and a router are two distinct devices that work together to provide internet access, but they serve very different purposes.

A modem is the device that connects your home to the internet through your Internet Service Provider (ISP). It acts as a bridge, converting the signals from your ISP, whether cable, DSL, fiber, or satellite, into digital data your devices can understand. Without a modem, you cannot access the internet at all, as it is the gateway between your home network and the wider internet. Typically, a modem has one connection to the ISP and one output that connects to a single device, often a router.

On the other hand, a router takes the internet connection provided by the modem. It distributes it to multiple devices in your home, either via Ethernet cables or wirelessly through Wi-Fi. It creates a local network (LAN), allowing your computers, smartphones, tablets, and other devices to communicate with each other and share the internet connection. The router assigns local IP addresses to each device and manages data traffic within the network. Additionally, routers often provide security features, such as firewalls and Wi-Fi encryption, to protect your network.

To summarize:

Aspect	Modem	Router
Primary Role	Connects to ISP and provides internet access	Distributes internet to multiple devices and manages local network
Connection	One input from ISP, one output to router or device	Connects to modem and multiple devices via Ethernet or Wi-Fi
Network Type	Wide Area Network (WAN)	Local Area Network (LAN)
IP Address	Has a public IP address from ISP	Assigns local IP addresses to devices
Wireless Capability	Usually none	Provides Wi-Fi connectivity
Security	Basic connectivity	Includes firewalls, encryption, parental controls

Many modern devices combine both modem and router functions into a single unit called a gateway, simplifying setup and reducing hardware

### 3. IP Address Classes & Binary Format Conversion

**IP addresses** are numerical labels assigned to devices on a network, and in IPv4, these addresses are divided into five classes: A, B, C, D, and E. Each class serves a different purpose and is identified by the value of the first octet (the first 8 bits) of the address.

- **Class A** addresses range from 1.0.0.0 to 126.255.255.255 and are meant for networks with a large number of hosts. The first bit is always 0, and the remaining seven bits in the first octet identify the network, while the last 24 bits identify the host. This allows for 126 networks and over 16 million hosts per network.
- **Class B** addresses span from 128.0.0.0 to 191.255.255.255. Here, the first two bits are 10, with the next 14 bits for the network and the last 16 bits for hosts, supporting 16,384 networks and 65,534 hosts per network.
- **Class C** addresses go from 192.0.0.0 to 223.255.255.255. The first three bits are 110, with 21 bits for the network and 8 bits for hosts, allowing for over 2 million networks and 254 hosts per network.
- **Class D** (224.0.0.0 to 239.255.255.255) is reserved for multicasting, not for typical host addressing.
- **Class E** (240.0.0.0 to 254.255.255.255) is reserved for experimental purposes.

#### **Binary Format Conversion:**

An IPv4 address is written in dotted decimal notation (e.g., 192.168.1.1), but computers use binary. To convert, each decimal octet is translated to an 8-bit binary number. For example, 192.168.1.1 becomes:

- 192 → 11000000
- 168 → 10101000
- 1 → 00000001
- 1 → 00000001

So, 192.168.1.1 in binary is 11000000.10101000.00000001.00000001

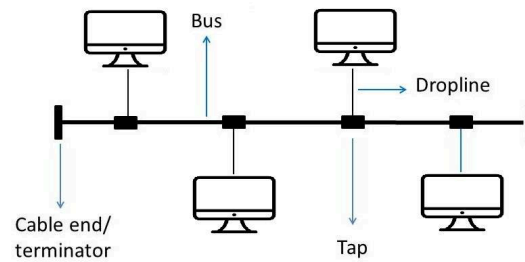
#### **4. Configure IP Address using CLI**

#### **5. Network Topologies Visualization**

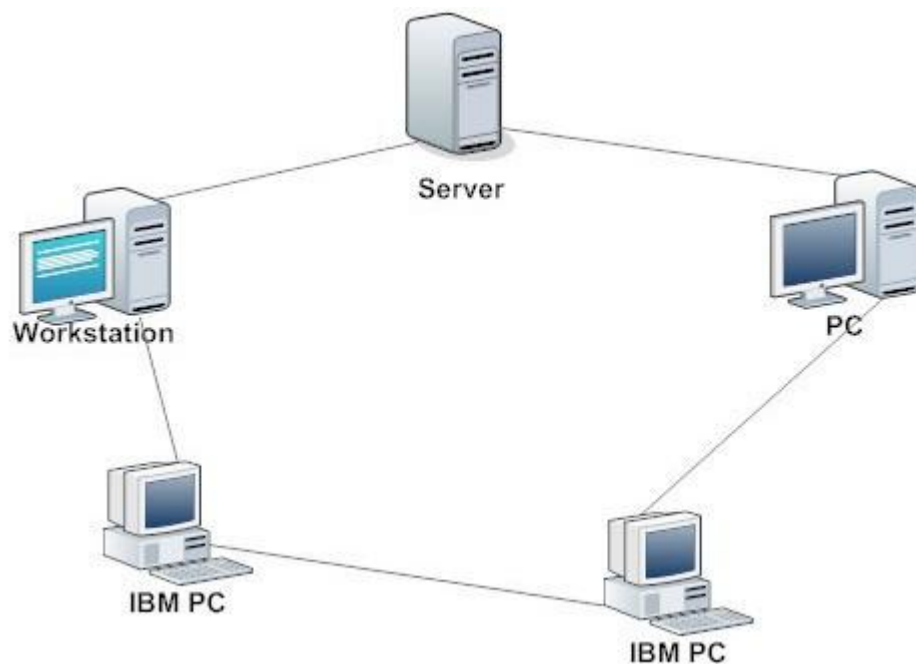
A network topology visualization is a diagram that shows how different devices (like computers, printers, switches, and routers) are physically or logically connected in a network. Such diagrams help in understanding the structure, design, and data flow within a network, making troubleshooting and planning much easier.

Common network topologies you might see in a diagram include:

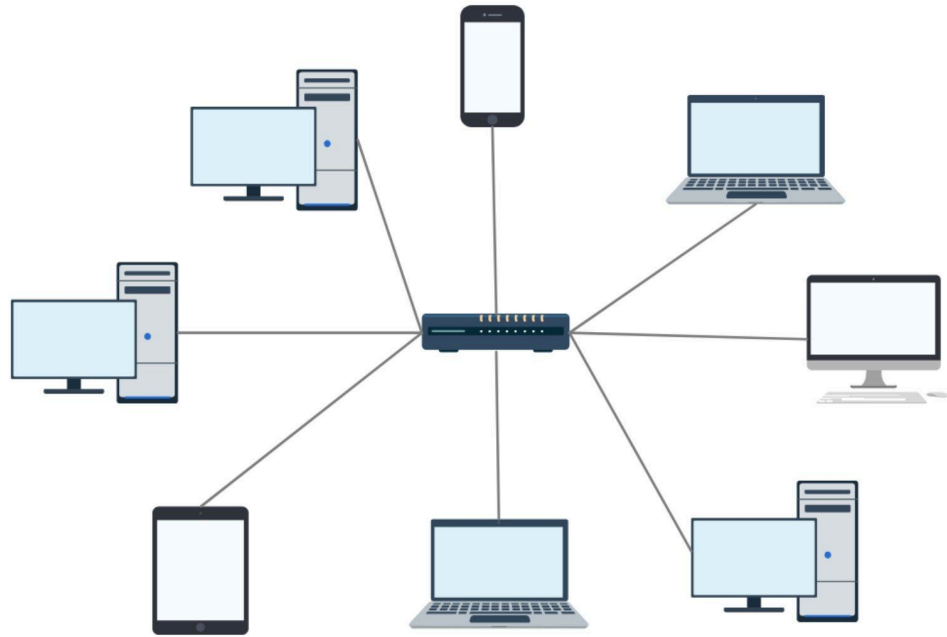
- **Bus Topology:** All devices are connected to a single central cable (the bus). Data travels along this backbone, and each device taps into it. This is simple and cost-effective but can be disrupted if the main cable fails.



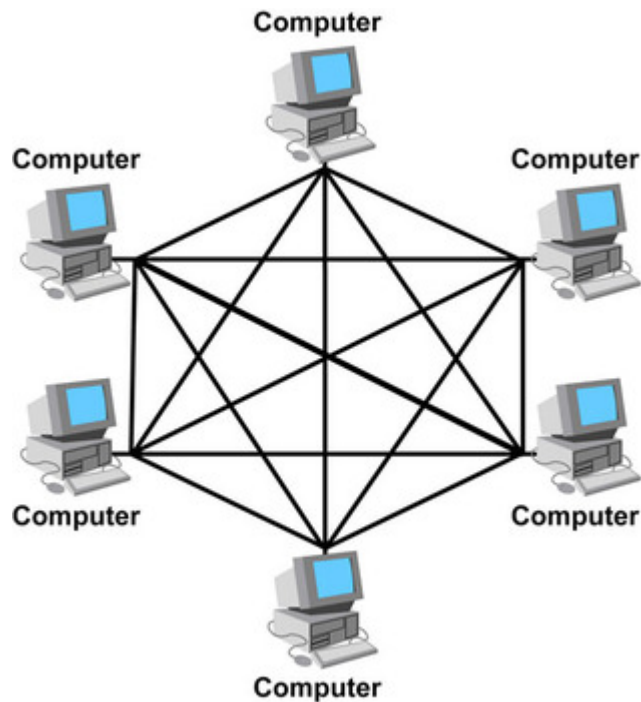
- **Ring Topology:** Each device connects to exactly two others, forming a closed loop. Data travels in one direction, passing through each device until it reaches its destination. If one device fails, the whole network can be affected unless a dual ring is used.



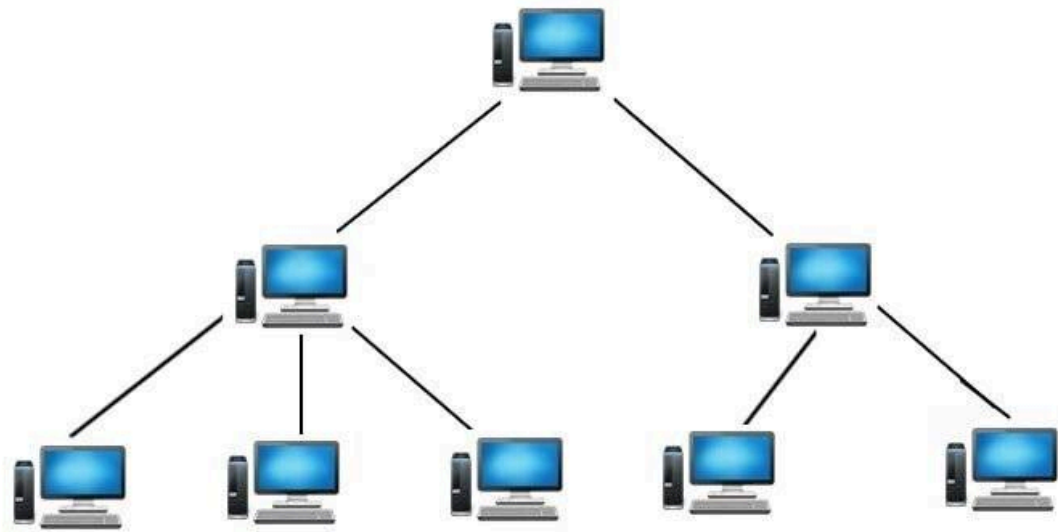
- **Star Topology:** All devices connect to a central hub or switch. This makes it easy to manage and expand, but if the hub fails, the entire network goes down



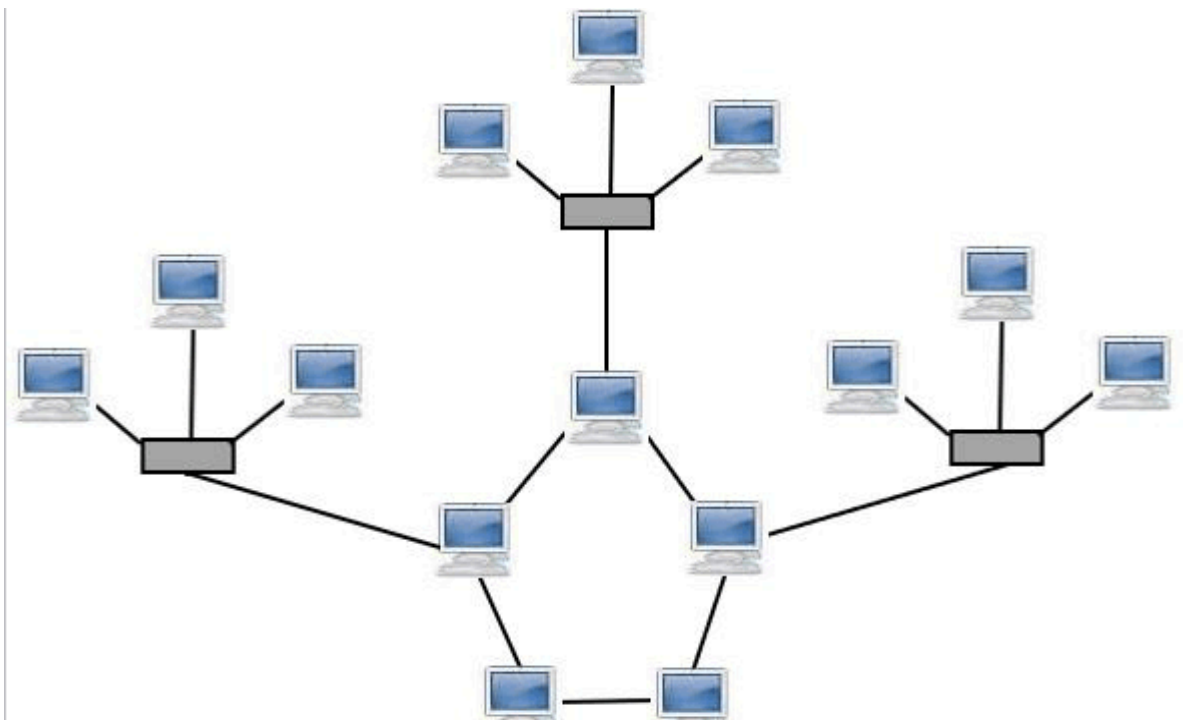
- 
- **Mesh Topology:** Every device is connected to every other device. This provides high redundancy and reliability but is complex and expensive to implement.



- **Tree Topology:** A hybrid of star and bus topologies, with groups of star-configured devices connected to a linear bus backbone. It allows for scalable and hierarchical networks.



- 
- **Hybrid Topology:** Combines two or more different topologies to meet specific needs, often seen in large or complex networks
- 



## 6. Subnetting and CIDR Practice

### Practice Subnetting IPv4:

- To learn how to Subnet: watch the [free training videos](#) listed beneath the problem generator
- To practice Subnetting: Click on the [New Problem] button below
- Solve the five attributes for the given Target IP and CIDR
- Click [check] to check if your answer was correct
- Click [show] to view correct answers
- Type "." or "/" in any input box to jump to the next box (*desktop only*)
- Keyboard [ENTER] button will perform following action:
  - ☒ Show all
  - ☐ Check All

New Problem	Target IP address	43	.	209	.	158	.	117	/	23
-------------	-------------------	----	---	-----	---	-----	---	-----	---	----

	IP address	Check/Show	Answer	Correct?
Network	43 . 209 . 158 . 0	Check Show	43 . 209 . 158 . 0	YES
First Host	43 . 209 . 158 . 1	Check Show	43 . 209 . 158 . 1	YES
Last Host	43 . 209 . 209 . 254	Check Show	43 . 209 . 159 . 254	NO
Broadcast	43 . 209 . 209 . 255	Check Show	43 . 209 . 159 . 255	NO
Next Subnet	43 . 209 . 160 . 0	Check Show	43 . 209 . 160 . 0	YES
Check or Show ALL		Check Show		

- **Network Address:**

The /23 subnet covers two consecutive /24s.

The third octet (158) in binary is 10011110. With a /23 mask, the last bit of the third octet is part of the network portion.

- The network address is 43.209.158.0.

- **First Host:**

The first usable IP is the network address plus one:

- 43.209.158.1

- **Last Host:**

The broadcast address minus one. (See broadcast address below.)

- 43.209.159.254

- **Broadcast Address:**

The /23 subnet includes all addresses from 43.209.158.0 to 43.209.159.255.

- 43.209.159.255

- **Next Subnet:**

The next /23 subnet starts right after the broadcast address:

- 43.209.160.0



## 7. Trace Route a Website and Observe Hops

### For Canva:

```
Microsoft Windows [Version 10.0.22631.5472]
(c) Microsoft Corporation. All rights reserved.

C:\Users\khush>tracert www.canva.com

Tracing route to www.canva.com [104.16.102.112]
over a maximum of 30 hops:

  1    2 ms    8 ms    2 ms  192.168.1.1
  2   33 ms    9 ms    6 ms  10.10.32.1
  3    *      *      *    Request timed out.
  4    *      *      6 ms  102.199.193.103-gigantic.gtels.in [103.193.199.102]
  5   44 ms   48 ms   7 ms  sfynodprgcl712107-gigantic.gtels.in [103.193.199.185]
  6   54 ms   13 ms  62 ms  104.23.231.12
  7   66 ms    *      *    104.23.231.11
  8    7 ms    7 ms    6 ms  104.16.102.112

Trace complete.

C:\Users\khush>
```

### For Google:

```
C:\Users\khush>tracert www.google.com

Tracing route to www.google.com [142.250.192.164]
over a maximum of 30 hops:

  1    2 ms    1 ms    2 ms  192.168.1.1
  2    6 ms    6 ms    6 ms  10.10.32.1
  3    *      *      *    Request timed out.
  4    7 ms    6 ms    *    102.199.193.103-gigantic.gtels.in [103.193.199.102]
  5    9 ms    7 ms    7 ms  sfynodprgcl712107-gigantic.gtels.in [103.193.199.185]
  6    7 ms    7 ms    7 ms  142.250.168.72
  7    7 ms    7 ms    7 ms  142.251.66.173
  8    6 ms    7 ms    8 ms  172.253.73.195
  9    7 ms    7 ms    7 ms  del11s11-in-f4.1e100.net [142.250.192.164]

Trace complete.
```

### For Wikipedia:

```
Tracing route to www.google.com [142.250.192.164]
over a maximum of 30 hops:

  1    2 ms    2 ms    2 ms  192.168.1.1
  2    7 ms    5 ms    6 ms  10.10.32.1
  3    *      *      *    Request timed out.
  4    *      6 ms    *    102.199.193.103-gigantic.gtels.in [103.193.199.102]
  5    8 ms    7 ms    7 ms  sfynodprgcl712107-gigantic.gtels.in [103.193.199.185]
  6    8 ms    6 ms    7 ms  142.250.168.72
  7    8 ms    7 ms    7 ms  142.251.66.173
  8    8 ms    8 ms    8 ms  172.253.73.195
  9    7 ms    7 ms    7 ms  del11s11-in-f4.1e100.net [142.250.192.164]

Trace complete.
```

8. Check DNS Records of a Website

zekai.com

WHOIS search results

Domain Information



Name	ZEKAI.COM
Registry Domain ID	92600856_DOMAIN_COM-VRSN
Registered On	2002-11-27T03:54:43Z
Expires On	2025-11-27T03:54:43Z
Updated On	2022-08-31T15:44:23Z
Domain Status	client delete prohibited client transfer prohibited client update prohibited
Name Servers	DNS1.EASYDNS.COM DNS2.EASYDNS.NET DNS3.EASYDNS.CA

🔒 **codways.com is taken**

We still might be able to get it for you. [See How](#)

## WHOIS search results

### Domain Information



Name	CODWAYS.COM
Registry Domain ID	2899318038_DOMAIN_COM-VRSN
Registered On	2024-07-15T06:13:35Z
Expires On	2026-07-15T06:13:35Z
Updated On	2024-07-15T06:28:49Z
Domain Status	client transfer prohibited
Name Servers	NS1.MD-IN-40.WEBHOSTBOX.NET NS2.MD-IN-40.WEBHOSTBOX.NET

## Registrant Contact



Name	Redacted for Privacy
Organization	Privacy service provided by Withheld for Privacy ehf
Phone	tel:+354.4212434
Fax	-
Email	7992ad9afebd4d88b09ef64fcfcb5490.protect@withheldforprivacy.com
Mailing Address	Kalkofnsvegur 2, Reykjavik, Capital Region, 101

## Technical Contact



Name	Redacted for Privacy
Organization	Privacy service provided by Withheld for Privacy ehf
Phone	tel:+354.4212434
Fax	-
Email	7992ad9afebd4d88b09ef64fcfcb5490.protect@withheldforprivacy.com

## 9. Test and Understand the DHCP Process

The Dynamic Host Configuration Protocol (DHCP) is fundamental to how modern networks operate, making it easy for devices to join a network without manual configuration. When a device (like a laptop or smartphone) connects to a network, it needs an IP address and other network settings to communicate. DHCP automates this process, ensuring devices receive the correct configuration without human intervention.

The DHCP process is typically described by the acronym DORA, which stands for Discover, Offer, Request, and Acknowledge. Here's how it works:

- Discover: When a device connects to the network, it broadcasts a DHCPDISCOVER message to find available DHCP servers. Since the device doesn't yet have an IP address, it uses the special address 0.0.0.0 as the source and 255.255.255.255 as the destination, ensuring all servers on the local network see the request.
- Offer: Each DHCP server that receives the discover message responds with a DHCPOFFER. This message includes an available IP address and other configuration details like the subnet mask, default gateway, and DNS servers.
- Request: The client then sends a DHCPREQUEST message, indicating which offer it is accepting (usually the first one received). This message is also broadcast so all servers know which offer was accepted.
- Acknowledge: Finally, the selected DHCP server sends a DHCPACK (acknowledgment) message, confirming the assignment and providing all necessary network configuration. The client can now use the assigned IP address and access the network.

This process happens quickly and transparently every time a device joins a network, making DHCP a critical service for both home and enterprise environments. It not only simplifies network management but also helps prevent address conflicts by keeping track of which IP addresses are in use

Command :

ipconfig /release: to release the ip address

Request a New IP Address from the DHCP Server: ipconfig /renew

Display All Network Configuration Details: ipconfig /all

```

Ethernet adapter vEthernet (WSL (Hyper-V firewall)):

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::bfd1:6926:9e59:be1%34
    IPv4 Address. . . . . : 172.29.160.1
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1091:64d1:13ab:def6%12
    Default Gateway . . . . . : 

Ethernet adapter Bluetooth Network Connection:

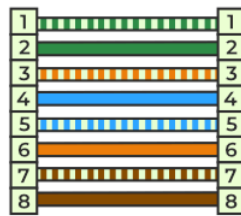
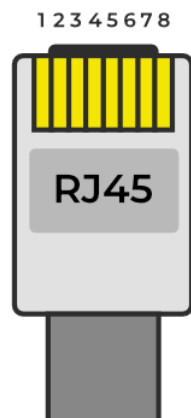
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

```

## 10.Understand the Role of RJ-45 and RJ-6

RJ-45 and RJ-6 serve distinct roles in networking and communications, each tailored for different types of connections and signals.

RJ-45 is a standardized connector primarily used for Ethernet networking. It features eight pins and is designed to terminate twisted-pair cables, such as Cat5, Cat5e, and Cat6, which are widely used in local area networks (LANs). The RJ-45 connector allows devices like computers, switches, and routers to connect to a wired network, enabling high-speed data transfer. Inside the connector, the eight wires are arranged according to specific color codes (T568A or T568B standards) to ensure proper signal transmission and compatibility. RJ-45 connectors are essential for structured cabling in offices, data centers, and homes, supporting speeds up to 10 Gbps depending on the cable type.



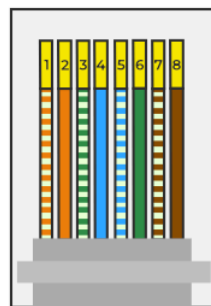
Ethernet Patch Cable



Ethernet Crossover Cable

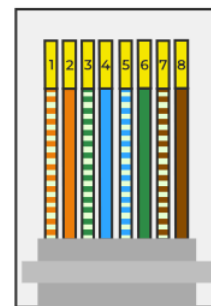
RJ-6, on the other hand, is not a standard networking connector like RJ-45. The term is often confused with RG-6, which is a type of coaxial cable commonly used for cable television, satellite, and broadband internet connections. RG-6 cables carry radio frequency (RF) signals and are terminated with F-type connectors, not RJ-6. These cables are optimized for transmitting high-frequency signals over longer distances with minimal loss, making them ideal for TV and internet service delivery.

Hold the Copper Strips  
Towards Your Face



T-568A

Hold the Copper Strips  
Towards Your Face



T-568B

1. Mint Orange
2. Orange
3. Mint Green
4. Blue
5. Mint Blue
6. Green
7. Mint Brown
8. Brown

Connector/Cable	Primary Use	Cable Type	Typical Application

<u>RJ-45</u>	Ethernet/data networking	Twisted-pair (Cat5/6)	LAN, computers, switches, routers
<u>RG-6</u>	TV, satellite, broadband RF	Coaxial	Cable TV, satellite, broadband

RJ-45 is the connector you see on Ethernet cables for computer networks, while RG-6 (often mistakenly called RJ-6) is a coaxial cable for TV and broadband, terminated with different connectors. Understanding their roles helps ensure you use the right cable and connector for your networking or media setup

## Section B: Data & Product Security (10 Questions)

### 11. Symmetric vs Asymmetric Encryption Demo

Symmetric and asymmetric encryption are two fundamental cryptographic techniques used to secure data, each with distinct mechanisms and use cases.

**Symmetric encryption:** uses a single secret key for both encrypting and decrypting information. This means the sender and receiver must both possess the same key and keep it confidential. Popular symmetric algorithms include AES, DES, and 3DES. Symmetric encryption is fast and efficient, making it ideal for encrypting large amounts of data, such as files or entire disk drives. However, the main challenge is securely sharing the secret key between parties if someone intercepts this key, they can decrypt all the data

### 12. Create Hashes of a File

#### What is a Hash?

A hash is a fixed-length string of characters generated by a hashing algorithm (like MD5, SHA-1, SHA-256) from a file or message. Even a tiny change in the file content will completely change the hash.

#### How Hashing Works:



1. You upload or input a file or string.
2. A hash algorithm (e.g., MD5) processes the input.

• Supports unlimited files of any size

Drop files here or click to select

and hash them all

Choose files

Khushi\_2409...NMENT.pdf

Khushi\_2409301011\_DOCKER ASSIGNMENT.pdf - 2697392 bytes

MD5: e3c94a866ace670a938844fd2386e5ec

SHA1: 26a0c48b149a3f013464744e631faf14fbda5588

SHA256: f38c8d97e6f84c4be0ba596691f20b3c6335383825a934cddb7aa193af55b53e

SHA512: 8a4ae7fca65dd03e143a6338b3eb722c9c7470ddf943da0ea5857ae64ae267119845a6f68a3694ebd7660146340374b8c9c5577e6fc650347e24c903a8f7ce71

Check out our online symmetric and asymmetric encryption tools.

Symmetric Encryption

Asymmetric Encryption

**Symmetric Encryption**

Plaintext

hey this is khushi

Key: 397

Generate Key

Encrypt ↓

Decrypt ↑

Ciphertext

gtrBēāgrhAēhAēNgAAgrē

**Asymmetric encryption**, also known as public key cryptography, uses a pair of mathematically related keys: a public key and a private key. The public key is shared openly and is used to encrypt data, while the private key is kept secret and is used to decrypt data. Only the holder of the private key can decrypt messages encrypted with the corresponding public key. Algorithms like RSA and ECC are common in asymmetric encryption. This approach solves the key distribution problem of symmetric encryption, as the private key never needs to be transmitted or shared. However, asymmetric encryption is slower and more resource-intensive, so it's typically used for smaller amounts of data or for securely exchanging symmetric keys

Symmetric Encryption

Asymmetric Encryption

Asymmetric Encryption

Plaintext

641

Public Key: 10147 Private Key: 139

Generate Keys

Encrypt ↓

Decrypt ↑

Ciphertext

\_]Z

## 14. Explore Phishing Techniques and Prevention

Phishing is a form of social engineering attack where cybercriminals impersonate legitimate entities to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal identification details. Phishing attacks exploit human psychology, often using urgency, fear, or curiosity to prompt victims to act without careful scrutiny

### Common Phishing Techniques

Technique	Description
Email Phishing	Mass emails that appear to come from trusted sources, urging recipients to click malicious links, download infected files, or provide sensitive data
Spear Phishing	Targeted emails crafted using specific information about the victim, making the deception more convincing and personalized
Whaling	Attacks aimed at high-profile individuals (e.g., CEOs, executives) to gain access to sensitive corporate data or authorize fraudulent transactions

Smishing	Phishing conducted via SMS/text messages, often containing malicious links or requests for personal information
Vishing	Voice phishing, where attackers call victims pretending to be from reputable organizations to extract sensitive information
Clone Phishing	Attackers copy legitimate emails, replace links or attachments with malicious versions, and resend them to the original recipients
Pharming	Manipulating DNS or redirecting users from legitimate websites to fake ones to steal credentials
Angler Phishing	Attackers pose as customer service representatives on social media to trick users into revealing personal information
Pop-up Phishing	Fake pop-up messages on websites or devices that prompt users to click links or download malware
Evil Twin Phishing	Setting up rogue Wi-Fi hotspots to intercept data from unsuspecting users

#### Prevention Strategies

- **User Education:** Regularly train employees and users to recognize suspicious emails, messages, and websites. Teach them to verify sender addresses, avoid clicking unknown links, and be wary of urgent requests.
- **Multi-Factor Authentication (MFA):** Require MFA wherever possible, so that stolen credentials alone are not enough for attackers to gain access.
- **Email Security Solutions:** Use advanced email filters and anti-phishing tools to detect and block malicious messages before they reach users.

- **Verify Requests:** Always confirm sensitive requests (like fund transfers) through a secondary communication channel, especially those appearing urgent or unusual.
- **Keep Software Updated:** Regularly update operating systems, browsers, and security tools to patch vulnerabilities that attackers might exploit.
- **Use Secure Connections:** Encourage the use of secure, verified Wi-Fi networks, and educate about the risks of public or untrusted hotspots.
- **Monitor and Respond:** Employ security solutions that detect and respond to suspicious activities, such as IBM Guardium Data Detection and Response, to identify threats in real time.

By understanding the many forms of phishing and implementing layered prevention strategies, individuals and organizations can significantly reduce their risk of falling victim to these pervasive attacks.

## 16. Understand Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) is a widespread web vulnerability that allows attackers to inject malicious client-side scripts—most often JavaScript—into web pages viewed by other users. When a user visits a compromised page, the malicious script executes in their browser, potentially stealing session cookies, credentials, or performing actions on behalf of the user without their consent<sup>7</sup>.

### Main Types of XSS

Type	Description
Stored XSS	<p>The malicious script is permanently stored on the server (e.g., in a database or comment field). Every user who views the affected page is exposed to the attack.</p> <p>This is considered the most severe form because it does not require user interaction beyond visiting the page</p>

Reflected XSS	<p>The malicious script is reflected off the web server, typically via a URL or form input. It is not stored; instead, the user must be tricked into clicking a crafted link or submitting a form. The attack is executed immediately in the user's browser as part of the server's response</p>
DOM-based XSS	<p>The vulnerability exists in client-side code. The malicious payload is never sent to the server; instead, it is processed by JavaScript in the browser, often via manipulation of the DOM using unsanitized user input (</p>

## How XSS Works

- An attacker finds a way to inject a script into a web page (via input fields, URLs, or other user-controllable data).
- The web application fails to properly sanitize or escape this input.
- The script is delivered to other users, executing in their browsers with the same privileges as the legitimate site.
- The attacker can steal session tokens, impersonate users, redirect victims, or perform actions as the victim.

## Section C: Tools & Ethical Hacking (10 Questions)

### 21. Run an Nmap Scan

```

Command Prompt
Microsoft Windows [Version 10.0.22631.5472]
(c) Microsoft Corporation. All rights reserved.

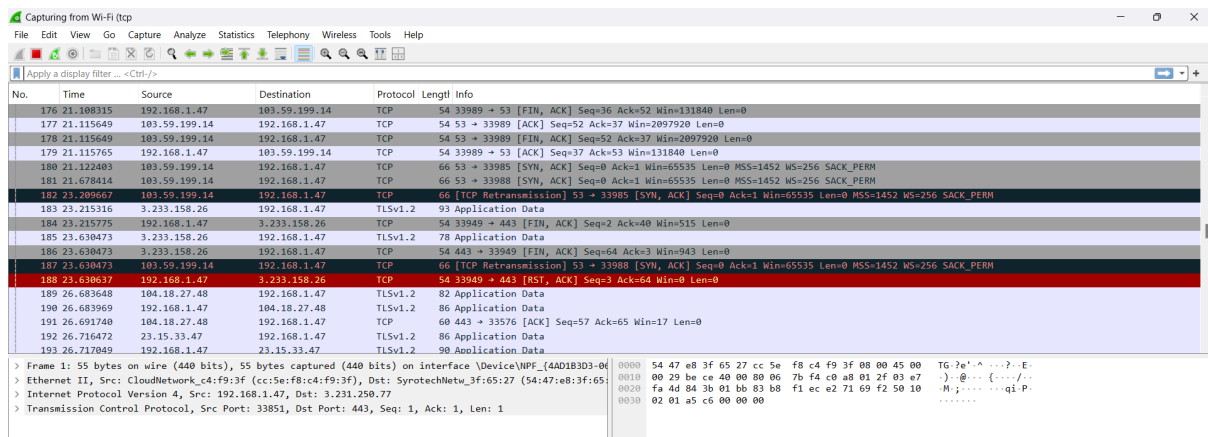
C:\Users\khush>nmap --version
Nmap version 7.97 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.4.7 openssl-3.0.16 nmap-libssh2-1.11.1 nmap-libz-1.3.1 nmap-libpcap-1.8.2 nmap-libnet-1.18.0 ipv6
Compiled without:
Available nsock engines: iocp poll select

C:\Users\khush>nmap 192.168.1.1
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-08 14:41 +0530
Nmap scan report for 192.168.1.1
Host is up (0.0085s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    filtered telnet
53/tcp    open  domain
80/tcp    open  http
139/tcp   filtered netbios-ssn
443/tcp   open  https
445/tcp   filtered microsoft-ds
MAC Address: 54:47:E8:3F:65:27 (Syrotech Networks.)

Nmap done: 1 IP address (1 host up) scanned in 5.80 seconds

```

## 22. Sniff Network Traffic using Wireshark



The screenshot shows a Wireshark capture of network traffic. The packet list on the left shows several packets, with packet 188 highlighted in red. The packet details pane on the right shows the structure of packet 188, which is a TCP RST, ACK packet. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
176	21.198315	192.168.1.47	103.59.199.14	TCP	54	33989 → 53 [FIN, ACK] Seq=36 Ack=52 Win=131840 Len=0
177	21.115649	103.59.199.14	192.168.1.47	TCP	54	53 → 33989 [ACK] Seq=52 Ack=37 Win=2097920 Len=0
178	21.115649	103.59.199.14	192.168.1.47	TCP	54	53 → 33989 [FIN, ACK] Seq=52 Ack=37 Win=2097920 Len=0
179	21.115765	192.168.1.47	103.59.199.14	TCP	54	33989 → 53 [ACK] Seq=37 Ack=53 Win=131840 Len=0
180	21.122403	103.59.199.14	192.168.1.47	TCP	66	53 → 33985 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 WS=256 SACK_PERM
181	21.678414	103.59.199.14	192.168.1.47	TCP	66	53 → 33988 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 WS=256 SACK_PERM
182	21.209567	103.59.199.14	192.168.1.47	TCP	66	[TCP Retransmission] 53 → 33985 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 WS=256 SACK_PERM
183	23.215316	3.233.158.26	192.168.1.47	TLSv1.2	93	Application Data
184	23.215775	192.168.1.47	3.233.158.26	TCP	54	33949 → 443 [FIN, ACK] Seq=2 Ack=40 Win=515 Len=0
185	23.630473	3.233.158.26	192.168.1.47	TLSv1.2	78	Application Data
186	23.630473	3.233.158.26	192.168.1.47	TCP	54	443 → 33949 [FIN, ACK] Seq=64 Ack=3 Win=943 Len=0
187	23.630473	103.59.199.14	192.168.1.47	TCP	66	[TCP Retransmission] 53 → 33988 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452 WS=256 SACK_PERM
188	23.630637	192.168.1.47	3.233.158.26	TCP	54	33949 → 443 [RST, ACK] Seq=3 Ack=64 Win=0 Len=0
189	26.683648	104.18.27.48	192.168.1.47	TLSv1.2	82	Application Data
190	26.683969	192.168.1.47	104.18.27.48	TLSv1.2	86	Application Data
191	26.691740	104.18.27.48	192.168.1.47	TCP	60	443 → 33576 [ACK] Seq=57 Ack=65 Win=17 Len=0
192	26.716472	23.15.33.47	192.168.1.47	TLSv1.2	86	Application Data
193	26.717049	192.168.1.47	23.15.33.47	TLSv1.2	90	Application Data

Frame 11: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF{4AD1B3D3-04} Ethernet II, Src: CloudNetwork\_c4:f9:3f (cc:5e:f8:c4:f9:3f), Dst: SyrotechNetw\_3f:65:27 (54:47:e8:3f:65:27) Internet Protocol Version 4, Src: 192.168.1.47, Dst: 3.231.250.77 Transmission Control Protocol, Src Port: 33851, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

Key Source IP:

- 192.168.1.47

Key Observations:

### 1. Communication Attempt:

- Your machine 192.168.1.47 is trying to **connect to port 443 (HTTPS)** on 3.233.158.26.
- Port 443 is typically used for **secure web connections (HTTPS)**.

### 2. RST, ACK Packet (Frame 188):

- Line 188 shows a **RST, ACK** packet from 192.168.1.47 to 3.233.158.26.
- This means your machine is **resetting** the connection. It usually happens when:

- The target port is **closed**
- The session was **rejected**
- Or some **firewall** or **software** interrupted the handshake.

### 3. TCP Retransmissions (Frames 182 and 187):

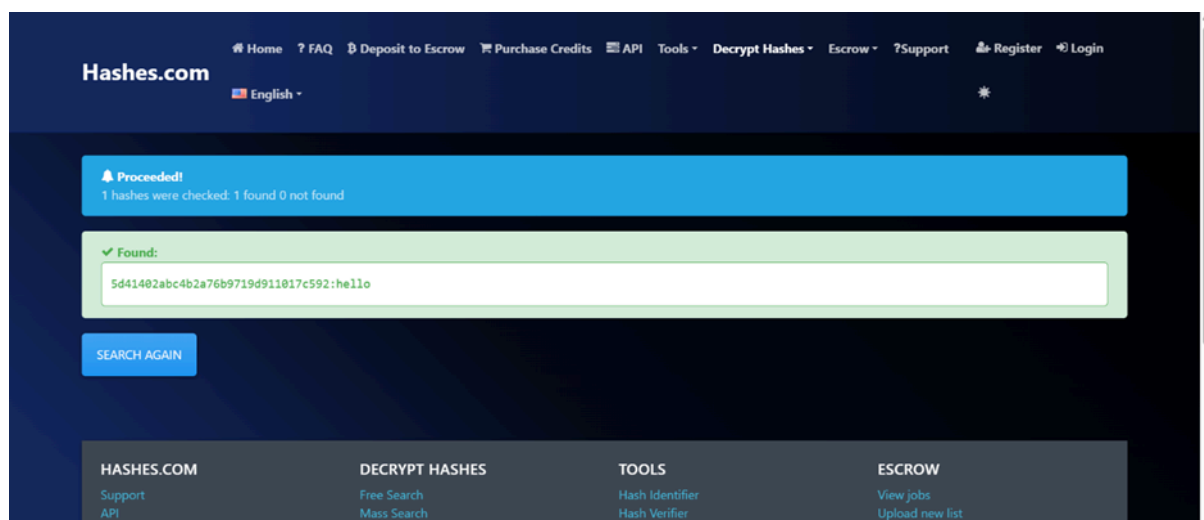
- IP 103.59.199.14 is sending TCP packets to 192.168.1.47, but it's **retransmitting** (Frame 182 and 187).
- This means it's **not getting a response back** — possibly **dropped packets** or **network delay**.

#### 4. TLS Packets:

- TLSv1.2 packets (Frames 183, 185, etc.) show **encrypted data exchange** over port 443 — a sign of a **secured connection in progress**.

## 25. Use John the Ripper for Password Cracking

Purpose	Command Example
Basic crack	john.exe hash.txt
Use wordlist	john.exe --wordlist=password.lst hash.txt
Show cracked passwords	john.exe-show hash.txt

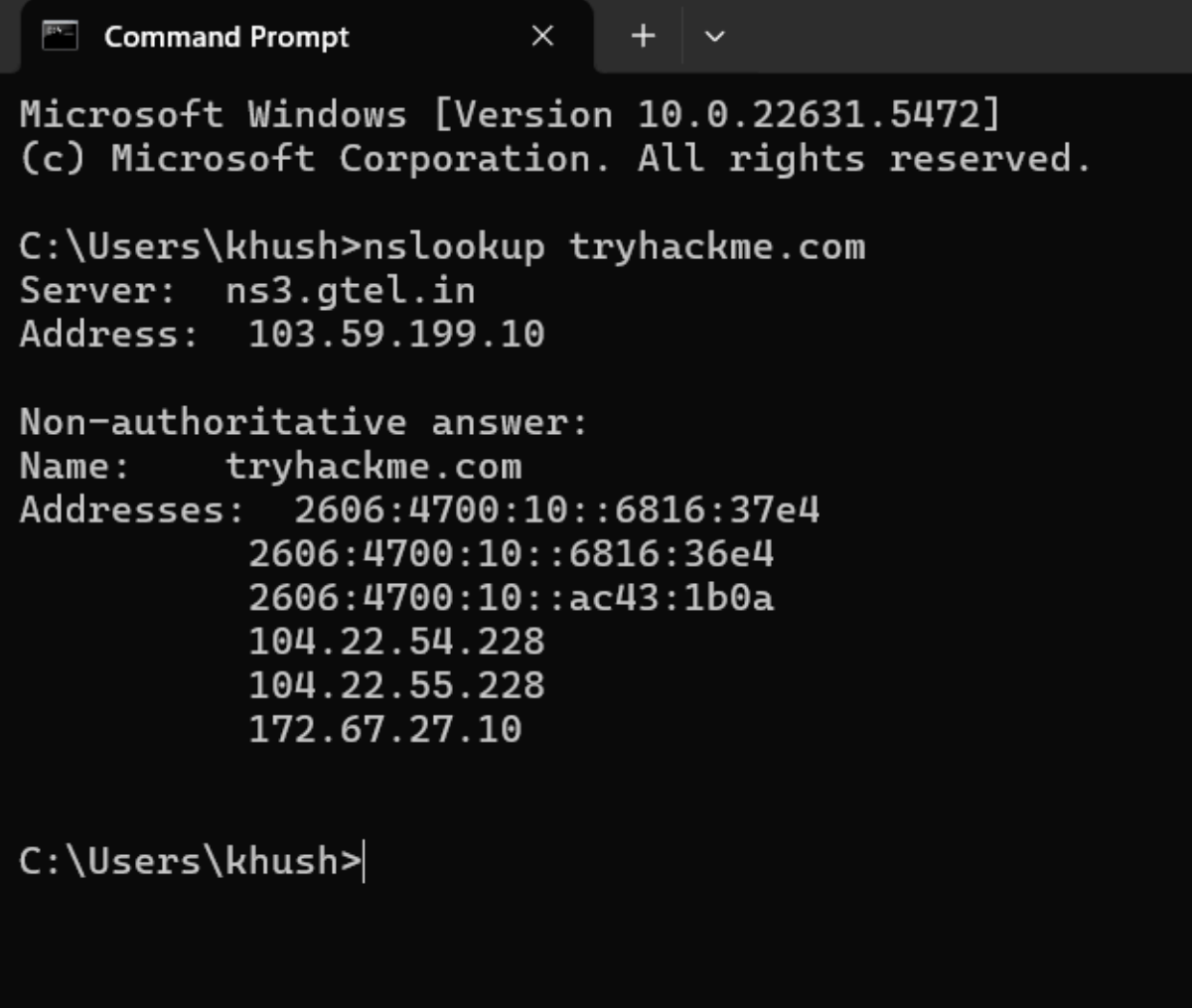


## 27. Practice DNS Enumeration TryHackMe – DNS Enumeration

The goal of this task is to check the DNS (Domain Name System) records of a website to retrieve its IP address(es) using the nslookup command in Windows Command Prompt.

Tool Used:

- Command Prompt (cmd)
- Command: nslookup tryhackme.com

A screenshot of a Windows Command Prompt window. The title bar says "Command Prompt" with standard window controls. The text inside shows the Windows version (10.0.22631.5472) and copyright notice. The user is at the prompt C:\Users\khush> and has entered the command nslookup tryhackme.com. The output shows the server ns3.gtcl.in at address 103.59.199.10. It then displays a "Non-authoritative answer:" for the name tryhackme.com, listing six IP addresses: two IPv6 addresses (2606:4700:10::6816:37e4 and 2606:4700:10::6816:36e4) and four IPv4 addresses (2606:4700:10::ac43:1b0a, 104.22.54.228, 104.22.55.228, and 172.67.27.10). The prompt ends with C:\Users\khush>|.

```
Microsoft Windows [Version 10.0.22631.5472]
(c) Microsoft Corporation. All rights reserved.

C:\Users\khush>nslookup tryhackme.com
Server:  ns3.gtcl.in
Address:  103.59.199.10

Non-authoritative answer:
Name:     tryhackme.com
Addresses: 2606:4700:10::6816:37e4
          2606:4700:10::6816:36e4
          2606:4700:10::ac43:1b0a
          104.22.54.228
          104.22.55.228
          172.67.27.10

C:\Users\khush>|
```

## 28. Use Nikto to Find Web Vulnerabilities

Nikto is a classic open-source web server scanner that's a go-to for anyone looking to quickly identify common web vulnerabilities. Think of it as a reconnaissance tool that acts like a persistent, curious web surfer, probing your web server for known weaknesses, misconfigurations, and outdated components.



When you use Nikto, you simply point it at a target web server (an IP address or a URL), and it starts performing thousands of checks. It looks for things like vulnerable CGI scripts, insecure default files that shouldn't be publicly accessible, outdated web server software (like Apache or Nginx), and even checks for common security headers

## **29.Explore OWASP Top 10 Vulnerabilities OWASP Top 10 Live Labs**

The OWASP Top 10 is a crucial awareness document for web application security, detailing the most critical security risks. The latest version, OWASP Top 10: 2021, highlights ten categories of vulnerabilities that every developer and security professional should understand.

### **OWASP Top 10 Vulnerabilities (2021)**

**Broken Access Control (A01:2021):** This is the top risk, where users can access or perform actions beyond their authorized permissions. Think of changing a URL parameter to view another user's account (Insecure Direct Object Reference - IDOR) or accessing administrative functions as a regular user.

**Cryptographic Failures (A02:2021):** Previously "Sensitive Data Exposure," this involves inadequate protection of sensitive data. Examples include storing passwords in plain text, using weak encryption algorithms, or transmitting data over unencrypted connections.

**Injection (A03:2021):** Occurs when untrusted data is sent to an interpreter as part of a command, leading to unintended execution. SQL Injection, where malicious code is inserted into database queries, and Cross-Site Scripting (XSS), injecting scripts into web pages, are prime examples.

**Insecure Design (A04:2021):** A new category focusing on design flaws and architectural weaknesses. This isn't about bad code, but about inherent design problems, like a lack of robust business logic validation or insufficient rate limiting allowing brute-force attacks.

**Security Misconfiguration (A05:2021):** Often due to insecure default settings, incomplete configurations, or exposed cloud storage. Using default credentials, unpatched software, or verbose error messages revealing sensitive information fall into this category.

Vulnerable and Outdated Components (A06:2021): Using libraries, frameworks, or other software modules with known vulnerabilities. The infamous Log4Shell vulnerability is a recent, critical example of this risk.

Identification and Authentication Failures (A07:2021): Weaknesses in authentication or session management, allowing attackers to compromise user identities. This includes weak password policies, predictable session IDs, or the absence of multi-factor authentication (MFA).

Software and Data Integrity Failures (A08:2021): A new focus on integrity verification, including insecure deserialization and issues in CI/CD pipelines. This covers scenarios where malicious code or data is introduced due to a lack of integrity checks.

Security Logging and Monitoring Failures (A09:2021): Insufficient logging or monitoring of security events, allowing attacks to go undetected. Lack of proper audit trails or alerts for suspicious activities falls here.

Server-Side Request Forgery (SSRF) (A10:2021): When a web application fetches a remote resource without validating the user-supplied URL, enabling attackers to make the server request internal or other sensitive systems.