

1. Cybersecurity Basics (10 MCQs)

(Cyber threats, malware, security practices)

1. Which of the following is NOT a cybersecurity threat?

- a) Phishing
- b) Ransomware
- c) Firewall
- d) Man-in-the-middle attack

📌 **Reason:** Firewall ek security tool hai, na ki ek threat.

2. What does a firewall do?

- a) Detects viruses
- b) Blocks unauthorized access
- c) Encrypts passwords
- d) Increases internet speed

📌 **Reason:** Firewall **unauthorized traffic block** karta hai jo system ko hack hone se bachata hai.

3. Which attack tricks users into giving their credentials?

- a) DDoS
- b) Phishing
- c) Ransomware
- d) Brute-force

📌 **Reason:** Phishing me **fake emails ya websites** se users ke **passwords** churaye jate hain.

4. What does an IDS (Intrusion Detection System) do?

- a) Blocks attacks
- b) Detects attacks
- c) Encrypts data
- d) Increases internet speed

📌 **Reason:** IDS sirf **attack detect** karta hai, par usko **block** nahi karta.

5. Which malware locks files and demands ransom?

- a) Trojan
- b) Worm
- c) Ransomware
- d) Adware

 **Reason:** Ransomware system ko **lock** kar deta hai aur **paise (ransom)** maangta hai.

6. What is a botnet?

- a) A group of compromised computers
- b) A network security tool
- c) A type of antivirus
- d) A secure network

 **Reason:** Botnet ka use **DDoS attacks aur spamming** ke liye hota hai.

7. Which attack sends excessive traffic to crash a server?

- a) MITM
- b) DDoS
- c) SQL Injection
- d) Zero-day

 **Reason:** DDoS me multiple systems milkar **ek server pe attack** karte hain.

8. Which password policy is the most secure?

- a) 8 characters minimum
- b) At least one number and special character
- c) 12+ characters with mix of upper/lowercase, numbers, and special chars
- d) Simple and easy to remember

 **Reason:** Strong passwords **cracking** se bachate hain.

9. What is social engineering?

- a) Software attack
- b) Tricking people into revealing information

- c) Virus infection
- d) Encrypting data

📌 **Reason:** Human error ka use karna **social engineering** ka part hai.

10. What is two-factor authentication (2FA)?

- a) Using two passwords
- b) Using password + another verification method
- c) A type of encryption
- d) A backup password system

📌 **Reason:** 2FA extra security layer provide karta hai.

#####
#####

2. Networking Basics (10 MCQs)

(OSI model, IP addresses, ports, network security)

11. What is the full form of IP?

- a) Internet Protocol
- b) Internal Process
- c) Internet Program
- d) Integrated Packet

📌 **Reason:** IP network devices ke address assign karta hai.

12. Which layer of the OSI model deals with encryption?

- a) Physical
- b) Data Link
- c) Network
- d) Application

📌 **Reason:** Encryption **Application Layer** (Layer 7) me hota hai.

13. What is the port number for HTTPS?

- a) 443
- b) 80
- c) 22

- d) 53

📌 **Reason:** HTTPS **secure web communication** ke liye port **443** use karta hai.

14. Which device connects two different networks?

- a) Switch
- b) Hub
- c) Router
- d) Repeater

📌 **Reason:** Router **multiple networks** ko connect karta hai.

15. What is a VPN used for?

- a) Making internet faster
- b) Encrypting internet traffic
- c) Blocking websites
- d) Detecting malware

📌 **Reason:** VPN **secure aur private internet connection** provide karta hai.

16. What is an IP address used for?

- a) Identifying a device on a network
- b) Hiding data
- c) Encrypting files
- d) Increasing internet speed

📌 **Reason:** IP address **devices ki unique identification** karta hai.

17. Which protocol is used to transfer files?

- a) HTTP
- b) FTP
- c) SMTP
- d) POP3

📌 **Reason:** FTP **file transfer protocol** hai jo **data share** karta hai.

18. What does DNS do?

- a) Translates domain names to IP addresses
- b) Encrypts network traffic

- c) Blocks hackers
- d) Speeds up the internet

📌 **Reason:** DNS **human-friendly URLs** ko **IP addresses** me convert karta hai.

19. What is the default subnet mask for Class C IP?

- a) 255.0.0.0
- b) 255.255.0.0
- c) 255.255.255.0
- d) 255.255.255.255

📌 **Reason:** Class C me **default subnet mask 255.255.255.0** hota hai.

20. Which of the following is a private IP address?

- a) 192.168.1.1
- b) 8.8.8.8
- c) 1.1.1.1
- d) 123.45.67.89

📌 **Reason:** 192.168.x.x **private IP range** me aata hai.

3. Cryptography Basics (10 MCQs)

(*Encryption, Hashing, Cryptographic Attacks, Digital Signatures*)

21. Which encryption algorithm is most secure for modern use?

- a) DES
- b) RSA
- c) AES
- d) MD5

📌 **Reason:** AES (**Advanced Encryption Standard**) modern aur fast encryption ke liye **most secure** mana jata hai.

22. Which hashing algorithm is commonly used for password storage?

- a) SHA-256
- b) MD5
- c) DES

- d) AES

 **Reason:** SHA-256 passwords store karne ke liye **secure** hai, whereas MD5 easily break ho saktा hai.

23. Which cryptographic method uses two keys (public & private)?

- a) Symmetric encryption
- b) Asymmetric encryption 
- c) Hashing
- d) Steganography

 **Reason:** Asymmetric encryption (RSA) me ek public aur ek private key use hoti hai.

24. Which of the following is a one-way encryption technique?

- a) AES
- b) RSA
- c) Hashing 
- d) Blowfish

 **Reason:** Hashing **one-way function** hai jo **original data recover nahi hone deta**.

25. What is the purpose of a digital signature?

- a) Encrypting data
- b) Authenticating the sender's identity 
- c) Compressing data
- d) Increasing internet speed

 **Reason:** Digital signatures verify karte hain ki **data sender legit hai ya nahi**.

26. What is the main weakness of symmetric encryption?

- a) Too slow
- b) Uses too much power
- c) Key distribution problem 
- d) Requires two keys

 **Reason:** Symmetric encryption me **same key** dono taraf honi chahiye, jo **securely share karna risky** hota hai.

27. Which of the following is NOT a cryptographic attack?

- a) Brute-force
- b) Phishing
- c) Man-in-the-middle
- d) Dictionary attack

❖ **Reason:** Phishing **social engineering attack** hai, cryptographic attack nahi.

28. Which encryption mode adds randomness to prevent patterns?

- a) ECB
- b) CBC
- c) SHA
- d) MD5

❖ **Reason:** CBC (Cipher Block Chaining) **previous block ka result next block ke saath mix** karta hai, taaki patterns na bane.

29. Which algorithm is used for digital signatures?

- a) AES
- b) DES
- c) RSA
- d) SHA-1

❖ **Reason:** RSA asymmetric encryption **digital signatures** generate karne ke liye use hota hai.

30. Which cryptographic concept ensures that data has not been changed?

- a) Confidentiality
- b) Integrity
- c) Authentication
- d) Availability

❖ **Reason:** Integrity ensure karta hai ki **data transmission ke dauraan modify nahi hua.**

4. Ethical Hacking (10 MCQs)

(Hacking Techniques, Tools, Attack Types, Penetration Testing)

31. What is the first step in ethical hacking?

- a) Scanning
- b) Gaining access
- c) Reconnaissance
- d) Exploitation

 **Reason:** Reconnaissance me hacker **target ki information gather** karta hai.

32. Which hacking tool is used for network scanning?

- a) Wireshark
- b) Nmap
- c) Burp Suite
- d) Metasploit

 **Reason:** Nmap network scanning aur **open ports detect** karne ke liye use hota hai.

33. What does a penetration test simulate?

- a) A real cyber attack
- b) A software update
- c) A secure system
- d) A phishing campaign

 **Reason:** Penetration testing **real-world hacking attack** simulate karta hai taaki vulnerabilities detect ho sakein.

34. What is a zero-day attack?

- a) An attack on the first day of the month
- b) An attack on a new vulnerability before a fix is available
- c) A virus with zero impact
- d) A type of phishing attack

 **Reason:** Zero-day attacks **unpatched vulnerabilities ka use** karke hoti hain.

35. Which of the following is an example of social engineering?

- a) SQL injection
- b) Phishing

- c) Buffer overflow
 - d) Cross-site scripting
- 👉 **Reason:** Social engineering me **human error ka faayda** uthaya jata hai, jaise **phishing emails.**

36. Which hacking technique captures network packets?

- a) Sniffing
 - b) Spoofing
 - c) Brute-force
 - d) Malware
- 👉 **Reason:** Sniffing me hacker **network traffic capture** karta hai sensitive information nikalne ke liye.

37. What does SQL Injection exploit?

- a) Weak passwords
 - b) Database vulnerabilities
 - c) Open ports
 - d) Unpatched software
- 👉 **Reason:** SQL injection **database me malicious SQL queries execute** karke sensitive data expose karta hai.

38. What is the primary purpose of a honeypot?

- a) To block hackers
 - b) To trap and study hackers
 - c) To secure passwords
 - d) To speed up a network
- 👉 **Reason:** Honeypot ek fake system hota hai jo **hackers ko attract karta hai** aur unki activities track karta hai.

39. Which operating system is most used by ethical hackers?

- a) Windows
- b) Kali Linux
- c) macOS

- d) iOS

 **Reason:** Kali Linux hacking aur penetration testing ke liye specially design kiya gaya hai.

40. Which type of attack floods a network with traffic to make it unavailable?

- a) DDoS
- b) Man-in-the-middle
- c) SQL Injection
- d) Phishing

 **Reason:** DDoS attack me multiple systems ek server pe traffic bhej kar usko crash kar dete hain.

•

-  **1. Basic Linux Commands (100% Expected)**
-  Linux ethical hacking aur cybersecurity ke liye must-have OS hai (Kali Linux, Parrot OS, etc.)

Command	Function (Usage)
ls	Directory ke files list karta hai.
cd [folder]	Directory change karne ke liye.
pwd	Current working directory dikhata hai.
mkdir [folder]	New directory create karta hai.
rm -rf [folder]	Folder aur uske content delete karta hai.
cp [file] [destination]	File copy karta hai.
mv [file] [destination]	File move ya rename karta hai.
chmod 777 [file]	File ke permissions change karta hai.
chown user:user [file]	File ka owner change karta hai.
find / -name [filename]	System me koi file search karne ke liye.

-  **Pro Tip:** Agar "file/directory management" se related question aaye toh ye commands yaad rakho!

•

-  **2. Network Scanning & Security (Linux)**

- 💡 Ye commands ethical hacking aur penetration testing me bohot use hote hain!

Command	Function (Usage)
ifconfig	System ka IP address aur network details show karta hai.
ip a	ifconfig ka alternative hai (modern Linux distros me).
netstat -tulnp	Active network connections aur open ports dikhata hai.
nmap -sV [IP]	Target IP address ka open ports aur services scan karta hai.
ping [IP]	Network connectivity check karne ke liye.
traceroute [IP]	Target tak packets ka path dikhata hai.
whois [domain]	Domain name ka owner aur IP info dikhata hai.
tcpdump -i eth0	Network traffic sniff karne ke liye.
curl [URL]	Web request bhejne ke liye (web scraping aur API testing).
wget [URL]	Web page ya file download karne ke liye.

- 💡 **Pro Tip:** Agar "network scanning aur security" se question aaye toh **Nmap, netstat, ping ya whois ke commands yaad rakho!**
-

☒ 3. Process & Task Management (Linux)

- 💡 Agar system pe background me kaunse processes chal rahe hain, ye check karna ho toh ye commands use hote hain!

Command	Function (Usage)
ps aux	System ke sabhi running processes show karta hai.
top	Live system processes aur CPU usage dikhata hai.
kill -9 [PID]	Process forcefully terminate karne ke liye.
htop	top ka advanced version jo colored aur interactive hai.
service [service-name] status	Koi service active hai ya nahi , ye check karne ke liye.
systemctl start/stop/restart [service]	Services start, stop ya restart karne ke liye.

- 💡 **Pro Tip:** Agar "running process ya system performance" se question aaye toh **top, ps aux, aur kill yaad rakho!**
-

☒ 4. Important Windows Commands (CMD & PowerShell)

- 💡 Windows me security aur hacking ke liye **CMD & PowerShell commands important hain!**

Command	Function (Usage)
ipconfig	Windows network settings aur IP address dikhata hai.
netstat -ano	Active network connections aur listening ports show karta hai.
ping [IP]	Network connectivity check karta hai.
tracert [IP]	Route tracing karta hai (network troubleshooting).
tasklist	System ke sabhi running processes dikhata hai.
taskkill /PID [PID] /F	Specific process force stop karta hai.
systeminfo	System ka hardware aur OS details dikhata hai.
wmic useraccount get name	Windows ke sabhi user accounts list karta hai.
net user [username] /add	Windows me new user account banata hai .
net user [username] *	Kisi user ka password reset karne ke liye.

- 💡 **Pro Tip:** Agar "Windows me network aur security" se question aaye toh ipconfig, netstat, aur tasklist yaad rakho!
-

- ⚡ **5. File & User Management (Windows & Linux)**
- 💡 Agar system ke users aur files ke permissions ka question aaye toh ye commands help karenge!

Command (Linux)	Command (Windows)	Function (Usage)
ls -l	dir	Files aur folders ka detailed list dikhata hai.
touch [file]	echo. > file.txt	Empty file create karne ke liye.
rm -rf [folder]	del /s /q [file]	File/folder permanently delete karta hai.
chmod 777 [file]	icacls file /grant Everyone:F	File ka permission change karta hai.
useradd [username]	net user [username] /add	New user create karta hai.
passwd [username]	net user [username] *	User password change karta hai.

- 💡 **Pro Tip:** Agar file permissions aur user management se related question aaye toh chmod, icacls, aur useradd yaad rakho!
-

- 🚀 **6. Most Common Commands in Cybersecurity Competitions**
- 💡 Agar sirf 10 important commands yaad rakhni hain toh ye yaad rakho!

Linux	Windows
ifconfig	ipconfig
nmap -sV [IP]	netstat -ano

Linux	Windows
whois [domain]	tracert [IP]
ps aux	tasklist
kill -9 [PID]	taskkill /PID [PID] /F
chmod 777 [file]	icacls file /grant Everyone:F
tcpdump -i eth0	netsh wlan show networks
find / -name [file]	dir /s [file]
wget [URL]	curl [URL]
systemctl restart [service]	net stop/start [service]

ports ki jankari jo puchhe ja saqte hia

ChatGPT said:

🔥 **Important Ports for Hacking Competition (100% Expected Questions) 🏆**

MCQ round me **ports** se related questions **100% aayenge!** Ye list tumhe **full marks** dila sakti hai. 🏆

🔑 **1. Most Common Ports (Ye 100% Yaad Rakho!)**

💡 **Competition me agar kisi protocol ka port number pucha jaye toh ye table yaad rakhni zaroori hai!**

Port	Protocol/Service	Use Case
20,	FTP (File Transfer Protocol)	File transfer ke liye.
21		
22	SSH (Secure Shell)	Secure remote login ke liye.

Port	Protocol/Service	Use Case
23	Telnet	Remote access (but insecure).
25	SMTP (Simple Mail Transfer Protocol)	Email send karne ke liye.
53	DNS (Domain Name System)	Domain name resolution ke liye.
67, 68	DHCP (Dynamic Host Configuration Protocol)	Automatic IP allocation.
80	HTTP (HyperText Transfer Protocol)	Web browsing (unencrypted).
110	POP3 (Post Office Protocol v3)	Email receive karne ke liye.
143	IMAP (Internet Message Access Protocol)	Email access karne ke liye.
443	HTTPS (Secure HTTP)	Secure web browsing.
445	SMB (Server Message Block)	Windows file sharing.
3389	RDP (Remote Desktop Protocol)	Remote desktop access.

 **Pro Tip:** Agar MCQ me **web browsing ka secure version** pucha jaye toh **port 443 (HTTPS)** yaad rakho!

2. Ethical Hacking & Penetration Testing Ports

 Agar question me "hacking tools aur exploits" se related ports aaye toh ye important hain!

Port	Service/Use Case
21	FTP Exploitation (Weak credentials se hack kiya jata hai)
22	SSH Brute Force Attacks
53	DNS Spoofing & Poisoning
80, 443	Web Application Hacking (XSS, SQL Injection)
139, 445	SMB Exploits (EternalBlue, WannaCry Attack)
3306	MySQL Database Hacking

Port	Service/Use Case
3389	RDP Exploits (Brute Force Attacks)

 **Pro Tip:** Agar hacking aur exploits se related MCQ aaye toh **445 (SMB Exploit)**, **3389 (RDP Attack)**, aur **3306 (Database Hack)** yaad rakho!

3. Well-Known Ports (MCQ Favorite!)

 Agar "ports categories" ka question aaye toh ye classification yaad rakho!

Port Range	Category	Example
0 - 1023	Well-Known Ports	HTTP (80), HTTPS (443), SSH (22)
1024 - 49151	Registered Ports	MySQL (3306), RDP (3389)
49152 - 65535	Dynamic (Ephemeral) Ports	
	Temporary client connections	

 **Pro Tip:** MCQ me **Well-Known Ports** ka question aane ke high chances hote hain!

4. Real-World Cyber Attack Ports (Exam Tricky Questions!)

 Agar question me "Kis port pe famous cyber attack hua?" aaye toh ye yaad rakho!

Attack Name	Vulnerable Port	Description
EternalBlue (WannaCry Ransomware)	445 (SMB)	Windows file sharing exploit.
Heartbleed Attack	443 (HTTPS, OpenSSL Bug)	Secure connection ka data leak.
DNS Poisoning Attack	53 (DNS)	Fake website redirect attack.
RDP Brute Force Attack	3389 (RDP)	Remote Desktop ke weak passwords ko hack karna.

 **Pro Tip:** Agar MCQ me **famous attack ka vulnerable port** pucha jaye toh **445 (SMB Exploit)** ya **3389 (RDP Hack)** yaad rakho!

5. Top 10 Ports to Memorize for Full Marks

 Agar sirf 10 yaad rakhne hain toh ye sabse important hain!

Port Protocol Use

22	SSH	Secure remote access
53	DNS	Domain resolution
80	HTTP	Web browsing (insecure)
443	HTTPS	Secure web browsing
445	SMB	Windows file sharing (Exploits)
3389	RDP	Remote desktop (Hacking Target)
3306	MySQL	Database service
25	SMTP	Email sending
67/68	DHCP	Automatic IP allocation
21	FTP	File transfer

 **Pro Tip:** Agar MCQ me "Most commonly hacked ports" aaye toh **445 (SMB), 3389 (RDP), aur 3306 (MySQL)** yaad rakho!

 **Round 2 (Challenge Round) – CTF Topics & Strategies** 

Is round me **real-world hacking challenges** aayenge. Tumhe **flags** (hidden codes) dhundne padenge **web apps, databases, encrypted messages, ya system vulnerabilities** me.

Agar **CTF jeetna hai toh ye topics MUST prepare karo!** 

- ◆ **1. Web Exploitation (Website Hacking)**

💡 Agar challenge me kisi website ko hack karke flag dhundna hai, toh ye techniques kaam aayengi:

Expected Challenges:

- ✓ **Hidden Files & Directories:** robots.txt, .git, .env file me sensitive data.
- ✓ **SQL Injection:** Database hack karke flag extract karna.
- ✓ **XSS (Cross-Site Scripting):** JavaScript payload se flag reveal karna.
- ✓ **LFI/RFI (Local/Remote File Inclusion):** ../../etc/passwd jese payloads ka use.

⚡ **CTF Tips:**

- ◆ **Nikto & Dirb:** Website me **hidden files aur vulnerabilities** dhundne ke liye.

bash

CopyEdit

nikto -h http://target.com

dirb http://target.com

◆ **SQL Injection ke liye basic payloads:**

sql

CopyEdit

' OR 1=1 --

" OR "1"="1

admin' --

◆ **XSS Test (JavaScript Alert Payload):**

html

CopyEdit

<script>alert('Hacked')</script>

◆ **LFI Test (File Inclusion Attack):**

bash

CopyEdit

http://target.com/index.php?page=../../../../etc/passwd

- ◆ **2. Cryptography (Encryption & Hash Cracking)**

💡 Agar challenge me encrypted ya encoded text diya ho, toh ye methods kaam aayengi:

✓ **Expected Challenges:**

✓ **Base64 Encoding/Decoding:**

bash

CopyEdit

```
echo "SGFja2VyU2VjcmV0" | base64 -d
```

✓ **Caesar Cipher Decryption:** Shift -3 ke saath try karo.

✓ **Hash Cracking (MD5, SHA1, SHA256):**

bash

CopyEdit

```
hashcat -m 0 -a 0 hash.txt rockyou.txt
```

```
john --wordlist=rockyou.txt hash.txt
```

✓ **RSA Encryption Challenges:** Private key extract karke decrypt karna.

⚡ **CTF Tips:**

- ◆ **Try Base64 first:** Agar string SGFja2Vy jese lage, toh Base64 decode karo.
 - ◆ **Online Tools:** CyberChef cryptography ke liye best hai!
 - ◆ **Hash Cracking ke liye RockYou.txt wordlist use karo.**
-

- ◆ **3. Root Access & Privilege Escalation**

💡 Agar challenge me system pe root/admin access lena ho, toh ye methods use karo:

✓ **Expected Challenges:**

✓ **SUID Exploitation:** Agar find / -perm -u=s -type f 2>/dev/null me **binary with root permissions** mile.

✓ **Kernel Exploits:** uname -a se Linux version check karke exploit dhundho.

✓ **Misconfigured Cronjobs:** /etc/crontab me kuch suspicious scripts run ho rahe hain kya?

⚡ **CTF Tips:**

◆ **Check sudo privileges:**

bash

CopyEdit

sudo -l

◆ **Check for world-writable files:**

bash

CopyEdit

find / -writable -type f 2>/dev/null

◆ **Automated tools (for fast enumeration):**

bash

CopyEdit

linpeas.sh # Linux Privilege Escalation

winpeas.exe # Windows Privilege Escalation

◆ **4. Common MySQL Injection (Database Hacking)**

💡 Agar database ka access chahiye toh SQL injection use hoga!

✓ **Expected Challenges:**

✓ **Login Bypass using SQLi:**

sql

CopyEdit

admin' --

" OR "1"="1

✓ **Extract Tables & Columns:**

sql

CopyEdit

```
' UNION SELECT table_name FROM information_schema.tables --
```

✓ **Dump Database using SQLMap:**

bash

CopyEdit

```
sqlmap -u "http://target.com/login.php?id=1" --dbs --batch
```

⚡ **CTF Tips:**

◆ **SQLi ke liye automated tools:**

bash

CopyEdit

```
sqlmap -u "http://target.com/index.php?id=1" --dump
```

◆ **Manual SQLi ke liye error-based approach try karo:**

sql

CopyEdit

```
' ORDER BY 1 --
```

```
' UNION SELECT 1,2,3,4 --
```

◆ **5. Password Cracking**

💡 **Agar challenge me password diya ho (hashed ya encoded), toh isko crack karna padega!**

✓ **Expected Challenges:**

✓ **Brute Force with Hydra:**

bash

CopyEdit

```
hydra -l admin -P rockyou.txt target.com ssh
```

✓ **John the Ripper for Hashes:**

bash

CopyEdit

```
john --wordlist=rockyou.txt hash.txt
```

✓ Cracking ZIP file password:

bash

CopyEdit

```
fcrackzip -u -D -p rockyou.txt secret.zip
```

⚡ CTF Tips:

- ◆ RockYou.txt wordlist sabse effective hai!
- ◆ If hash is unknown, use:

bash

CopyEdit

```
hashid <hash>
```

- ◆ Online Crackers bhi use kar sakte ho: [CrackStation](#)
-

◆ 6. OSINT (Open Source Intelligence)

💡 Agar challenge me kisi website ya user ke baare me info dhundni ho, toh ye tools use karo!

✓ Expected Challenges:

✓ Finding Hidden Emails & Usernames:

bash

CopyEdit

```
theHarvester -d target.com -l 500 -b google
```

✓ Checking Website History: Wayback Machine

✓ Checking Exposed Data: [HaveIBeenPwned](#)

✓ Tracking Social Media Footprints: [OSINT Framework](#)

⚡ CTF Tips:

- ◆ Google Dorking se secret data nikalne ki koshish karo:

bash

CopyEdit

site:target.com filetype:pdf "confidential"

◆ **ExifTool se image metadata check karo:**

bash

CopyEdit

exiftool image.jpg

◆ **People search engines try karo:**

- <https://www.spokeo.com>
- <https://namechk.com>

🔥 **Final Tips to Crack Round 2 (Challenge Round)**

- ✓ CTF ke pehle, TryHackMe & HackTheBox pe practice karo!
- ✓ Basic Linux & Windows commands revise karo (specially privilege escalation ke)!
- ✓ Burp Suite aur SQLMap automate scanning ke liye ready rakho!
- ✓ Google Dorking aur OSINT tools ka use karna seekho!
- ✓ CTF challenges ko team me solve karo, kyunki multiple skills ka use hota hai!

Agar kisi specific challenge ya concept pe deep explanation chahiye toh batao!



🔥 **CTF Platforms Guide: CTFd, HackTheBox & TryHackMe 🚀**

Tumhara hacking competition CTFd, HackTheBox (HTB), ya TryHackMe (THM) pe hoga. Har platform ka alag style hota hai, toh pehle se practice karna important hai!



◆ **1. CTFd (Jeetne Ka Formula)**

 CTFd ek common CTF platform hai jo mostly beginners & intermediate level ke liye hota hai.

CTFd Challenges (Expected Types)

- ✓ Web Exploitation (XSS, SQL Injection, File Inclusion)
- ✓ Cryptography (Base64, RSA, Hash Cracking)
- ✓ Forensics (Steganography, Packet Capture Analysis)
- ✓ Reverse Engineering (CrackMe Challenges, Binary Exploitation)

CTFd Ke Fastest Winning Tips:

- ◆ First 10-15 minutes: "Easy" wale challenges solve karo.
- ◆ Burp Suite, SQLMap, Dirb use karo: Web challenges ke liye.
- ◆ Use CyberChef for Cryptography: CyberChef
- ◆ Try Common CTF Flag Formats:

bash

CopyEdit

flag{this_is_a_flag}

CTF{hacking_is_fun}

- ◆ Google Dorking: Agar site indexed hai toh kuch sensitive info nikal sakte ho.

bash

CopyEdit

site:ctfd.com inurl:challenge

2. HackTheBox (HTB) (Professional-Level Hacking)

 HTB me "machines" hack karni padti hain jo real-world penetration testing ke close hoti hain.

HTB Challenges (Expected Types)

- ✓ Web Exploitation (SQLi, LFI, RCE)
- ✓ Privilege Escalation (Linux & Windows)
- ✓ Reverse Engineering & Binary Exploitation
- ✓ Active Directory Attacks

HTB Ke Fastest Winning Tips:

- ◆ **Nmap aur Gobuster se scanning shuru karo:**

bash

CopyEdit

```
nmap -A -T4 target.com
```

```
gobuster dir -u http://target.com -w /usr/share/wordlists/dirb/common.txt
```

- ◆ **Exploit-DB me target ke liye exploit dhundo:**

bash

CopyEdit

```
searchsploit Wordpress 5.0
```

- ◆ **Linux Privilege Escalation check karo:**

bash

CopyEdit

```
sudo -l
```

```
find / -perm -u=s -type f 2>/dev/null
```

- ◆ **Windows Privilege Escalation ke liye WinPEAS use karo.**

👉 HTB pe "Starting Point" aur "Easy Boxes" solve karo competition ke pehle!

- ◆ **3. TryHackMe (THM) (Beginner-Friendly)**

💡 THM ek guided CTF platform hai jo basics se advance hacking sikhata hai.

✓ **THM Challenges (Expected Types)**

✓ Beginner to Advanced Web Exploitation

✓ Cryptography & Hash Cracking

✓ Privilege Escalation (Linux & Windows)

✓ OSINT & Network Analysis

⚡ **THM Ke Fastest Winning Tips:**

- ◆ **Walkthrough rooms pehle solve karo:**

- "Basic Pentesting"

- "Web Exploitation"

- "Linux Privilege Escalation"
 - ◆ THM ke rooms ka use competition ke liye karo:
- "Overpass" → SSH Cracking & PrivEsc
- "Pickle Rick" → Web Exploitation
- "Burp Suite Basics" → Web Attacks

👉 THM pe "Free" wale rooms pe practice karo, sabse zyada questions inhi se aayenge!

🔥 Final Strategy to Win the Competition

- ✓ CTFd: Jaldi solve karne wale easy flags pe focus karo.
- ✓ HackTheBox: Agar root access mil gaya toh full points!
- ✓ TryHackMe: Agar walkthroughs yaad hain toh easy win!
- ✓ Google Dorking, Hash Cracking aur Nmap se speed badhao!