Project : REMOTE CONTROL

This Bash script automates remote control and reconnaissance tasks while ensuring anonymity. It performs the following key functions:

1. Dependency Installation

- Installs required tools (sshpass, curl, nmap, whois, perl) if not already available.

2. Anonymity Check with Nipe

- Uses Nipe to route network traffic through Tor, ensuring anonymity before executing any remote actions.

3. Remote Operations via SSH

- Connects to a user-specified remote server via SSH.
- Gathers system details: Public IP, uptime, and country.
- Performs reconnaissance on a target:
    - Executes a Whois lookup.
    - Runs an Nmap scan to detect open ports.
- Retrieves scan results from the remote system.
- Cleans up temporary files on the remote machine after execution.

4. Logging and Auditing

- Logs execution steps: Anonymity status, remote commands, and scan results.

- The script needs the user ‘root’ to operate.
  In the example you can see that the script checks for ‘root’ user.

```
Starting the script...
You are not root.. exiting...
```

- The script needs the user ‘root’ to operate.
  In the example you can see that the script checks for ‘root’ user.

```
Starting the script...
[*] sshpass is already installed.
[*] curl is already installed.
[*] nmap is already installed.
[*] whois is already installed.
[*] perl is already installed.
[*] Nipe is already installed.
[*] Starting Nipe...
[*] Nipe is active. Verifying anonymity...
Enter the remote server IP address:
```

- After using the script with user ‘root’, the script proceeds to check if all tools needed are installed.

```
Enter the remote server IP address: [redacted]
Enter the username for the remote server: kali
Enter the password for the remote server:
Enter the target address to scan: [redacted]
[*] Connecting to the remote server...
Remote Server Details:
Country: [redacted]
Public IP: [redacted]
Uptime:  up 51 minutes
Performing Whois on [redacted]...
Scanning [redacted] with Nmap...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-27 16:04 EST
Nmap scan report for [redacted]
Host is up (0.00085s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
[*] Retrieving results from the remote server...
Removing txt files from remote server...
Please provide path+name of the output directory (e.g., /home/kali/Desktop/REMOTE_CONTROL)
```

- User provides a remote ip address, username, password and a target ip to scan on the remote ip address.

```
Please provide path+name of the output directory (e.g., /home/kali/Desktop/REMOTE_CONTROL)
REMOTE_CONTROL_TEST
Script completed successfully. Logs saved in: REMOTE_CONTROL_TEST/project_log.txt
```

- The script asks for a directory name for the files to be saved in.


```
1  2025-02-27 16:04:10 - Dependencies checked and installed.
2  2025-02-27 16:04:10 - Nipe installed and configured.
3  [*] Starting Nipe...
4  2025-02-27 16:04:11 - Anonymity check completed using Nipe.
5  2025-02-27 16:04:32 - Remote server: [redacted]
6  2025-02-27 16:04:32 - Username: kali
7  2025-02-27 16:04:32 - Target address: [redacted]
8  2025-02-27 16:04:35 - Whois and Nmap results retrieved and deleted from remote server.
9  2025-02-27 16:04:35 - Remote operations and data collection(whois and nmap) completed.
```

- Example of the log file.