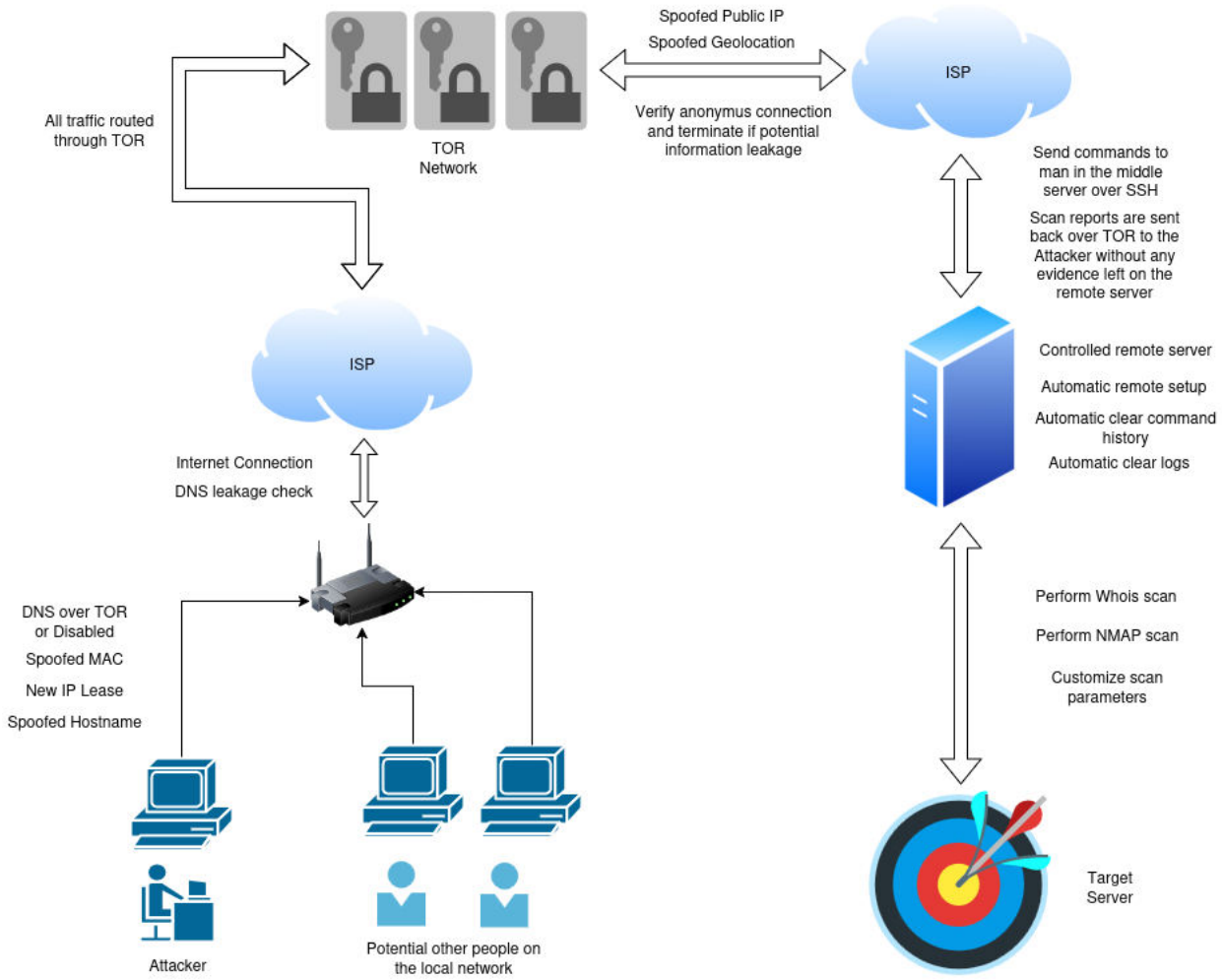
Remote Recon Automation Tool User Manual

This guide explains how to use the **Remote Recon Automation Tool**. This script helps you perform network reconnaissance anonymously using a remote server as a middle man. You need to have SSH access to a Linux VPS and you will be able to scan remote targets anonymously without leaving any traces leading back to you. This is the goal of the project, but keep in mind that nothing is perfect and fails safe, so use with caution.



1. Overview

The tool's main goal is to be as easy to use as possible so everything is completely automated. You will be prompted for all user information that is required after running the script.

```
rad@ideapad-pro:~/Desktop/Network Research Project$ sudo bash remote_control.sh
================================================================================

  Remote Recon Automation Tool
  Version: 1.0
  Author: Radostin Tonev
  Date: 13/07/2025
  Description: This script automates anonymus network reconnaissance on a target
  leveraging remote VPS as a middleman.

  It will perform the following actions:
  1. Automatically install required applications on the local and remote machines.
  2. Spoof MAC address and Hostname for anonymity within local network.
  3. Disable local DNS queries.
  4. Activate Tor-based proxy-chain for connecting to remote server.
  5. Block all traffic except Tor using firewall rules (handled by Nipe).
  6. Connect to the remote server via SSH and execute scans on specified target.
  7. Export scan results and audit logs.
  8. Clean up traces on the remote machine so even if it is compromised there will
     be no traces of the scans.

  The tool currently suports Nmap and Whois scans.

  Note: This script is intended for educational purposes only. Use responsibly and
  ensure you have permission to scan the target systems.

================================================================================
```

2. Requirements

- **Operating System:** Linux (Tested on Debian/Ubuntu-based).
- **Privileges:** You must run the script as `root` (using `sudo`).
- **Internet Connection:** Required for installing dependencies and Tor.
- **Remote Server:** An accessible Linux server with SSH enabled.

3. Configuration

You can adjust these settings at the top of the script:

Important note: If you run the script from VirtualBox VM MAC Spoofing will cause connectivity issues. Make sure **`MAC_SPOOFING_ENABLED=false`** if you run the script from virtual environment.

- **`DISABLE_DNS`**: Set to `true` to disable local DNS queries, or `false` to keep them enabled.
- **`MAC_SPOOFING_ENABLED`**: Set to `true` to enable MAC address spoofing, or `false` to disable it.

---

4. How to Use

1. **Save the Script:** Save the provided bash script (e.g., as `recon.sh`).
2. **Make Executable:**
   ```
   chmod +x recon.sh
   ```
3. **Run the Script:**
   ```
   sudo ./recon.sh or sudo bash recon.sh
   ```

4.1. Script Flow

The script will guide you through these steps:

1. **Header Display:** Shows tool information and purpose.
2. **Dependency Installation (Local):** Installs `sshpass`, `cpanm`, `git`, `macchanger`, `dhclient`, and `Nipe`.
3. **Anonymization Setup (Local):**
   - If enabled, changes your MAC address and renews DHCP lease.
   - If enabled, disables local DNS queries by modifying `/etc/resolv.conf`.
   - Activates Nipe to route traffic through Tor.

```
2025-07-14_18:52:38 - Setting up anonymity for local machine...

2025-07-14_18:52:38 - Attempting to change MAC address for local anonymity...
2025-07-14_18:52:38 - Found interface: wlp0s20f3. Changing MAC address...
2025-07-14_18:52:38 - Attempting to renew DHCP lease to apply new MAC address...
Error: ipv4: Address already assigned.
Setting LLMNR support level "yes" for "2", but the global support level is "no".
2025-07-14_18:52:45 - Renewed DHCP lease for wlp0s20f3.
2025-07-14_18:52:45 - New local IP address for wlp0s20f3: 192.168.1.102
2025-07-14_18:52:45 - MAC address successfully changed for .

2025-07-14_18:52:45 - Disabling local DNS queries by backing up and modifying /etc/resolv.conf...
2025-07-14_18:52:45 - Original /etc/resolv.conf backed up to /tmp/resolv.conf.bak_20250714_185233
2025-07-14_18:52:45 - Local DNS queries disabled (resolv.conf set to 127.0.0.1).
2025-07-14_18:52:45 - Nipe is not active. Attempting to start Nipe...
2025-07-14_18:53:01 - Nipe started successfully.
```

4. **Anonymity Check:** Verifies Nipe's status (spoofed IP/country) and checks for DNS leaks, verifies MAC address.

```
2025-07-14_18:53:01 - Performing mandatory anonymity checks...
2025-07-14_18:53:03 - Network connection is anonymus via Nipe.
2025-07-14_18:53:03 - --> Spoofed Country: DE
2025-07-14_18:53:03 - --> Spoofed IP Address: 185.220.101.104
2025-07-14_18:53:03 - No DNS leaks detected.
2025-07-14_18:53:03 - MAC address for wlp0s20f3 is successfully changed to 36:3d:f3:75:6b:9b.
2025-07-14_18:53:03 - Anonymity checks passed.
```

5. **Remote Server Details:** Prompts you to enter:
   - Remote server IP address
   - Remote server SSH username
   - Remote server SSH password (input will be hidden) The script then tests the SSH connection.

6. **Dependency Installation (Remote):** Installs `nmap` and `whois` on the remote server.

7. **Reconnaissance:**
   - Prompts for the **target IP address or hostname**.
   - Asks if you want to change default **Nmap options** (default: `-Pn -sV`).
   - Asks if you want to change default **Whois options** (default: empty).
   - Executes Whois and Nmap scans on the remote server against the target.
8. **Cleanup:** Clears bash history, logs, and temporary files on the remote server to remove traces. Here is example auth.log file after cleanup.

Note that there is no SSH logs originating from the script execution.

```
root@remoterecon:~# cat /var/log/auth.log
2025-07-14T15:56:03.446605+00:00 remoterecon sudo: pam_unix(sudo:session): session closed for user root
2025-07-14T15:56:03.601272+00:00 remoterecon sshd[1615]: Received disconnect from 185.220.101.104 port 36169:11: disconnected by use
2025-07-14T15:56:03.601396+00:00 remoterecon sshd[1615]: Disconnected from user root 185.220.101.104 port 36169
2025-07-14T15:56:03.601827+00:00 remoterecon sshd[1615]: pam_unix(sshd:session): session closed for user root
2025-07-14T15:56:03.609380+00:00 remoterecon systemd-logind[694]: Session 20 logged out. Waiting for processes to exit.
2025-07-14T15:56:03.611600+00:00 remoterecon systemd-logind[694]: Removed session 20.
2025-07-14T15:56:13.790433+00:00 remoterecon sshd[1708]: Invalid user git from 64.226.123.144 port 33224
2025-07-14T15:56:13.799605+00:00 remoterecon sshd[1708]: pam_unix(sshd:auth): check pass; user unknown
2025-07-14T15:56:13.799729+00:00 remoterecon sshd[1708]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
.226.123.144
2025-07-14T15:56:16.008834+00:00 remoterecon sshd[1708]: Failed password for invalid user git from 64.226.123.144 port 33224 ssh2
2025-07-14T15:56:16.073490+00:00 remoterecon sshd[1708]: Connection closed by invalid user git 64.226.123.144 port 33224 [preauth]
2025-07-14T16:00:43.961069+00:00 remoterecon sshd[1713]: Accepted password for root from 89.215.142.219 port 45896 ssh2
2025-07-14T16:00:43.963422+00:00 remoterecon sshd[1713]: pam_unix(sshd:session): session opened for user root(uid=0) by root(uid=0)
2025-07-14T16:00:43.967718+00:00 remoterecon systemd-logind[694]: New session 21 of user root.
root@remoterecon:~#
```

9. **Summary:** Displays paths to the generated `whois_results_*.txt`, `nmap_results_*.txt`, and `recon_log_*.txt` files in your current working directory.

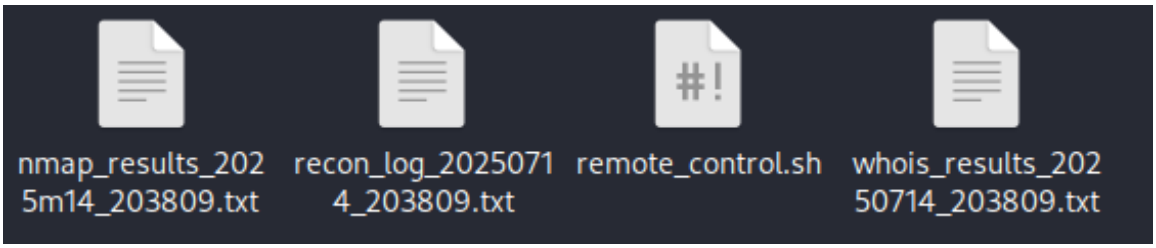
10. **Restoration:** Restores local MAC address, DNS settings, and stops Nipe upon exit. Basically restore your local machine to its original state and configuration.

---

5. Output Files

All output files are saved in the directory where you run the script:

- **`recon_log_YYYYMMDD_HHMMSS.txt`**: Detailed log of all script actions, useful for debugging.
- **`whois_results_YYYYMMDD_HHMMSS.txt`**: Contains the results of the Whois query.
- **`nmap_results_YYYYMMDD_HHMMSS.txt`**: Contains the results of the Nmap scan.



---

6. Troubleshooting

- **"Script must be run as root"**: Always use `sudo ./recon.sh`.
- **Dependency Installation Errors**: Check your internet connection. If `apt` fails, manually install the missing packages.
- **MAC Address Change Fails**: Ensure `macchanger` is installed (`sudo apt install macchanger`) and your network interface is not in use. The script tries to bring the interface down and up.
- **Nipe Issues (Status: false, failed to start)**:
  - Verify `cpanm` and Perl dependencies are correctly installed.
  - Check your internet connection; Nipe needs to connect to Tor.
  - Try restarting the script.
  - Disable MAC spoofing
- **SSH Connection Errors**:
  - Double-check the remote server's IP, username, and password.
  - Ensure SSH is running on the remote server.
  - Make sure your local machine can reach the remote server (firewall rules, network connectivity).
- **DNS Leak Detected**: This means your DNS queries might not be going through Tor. The script will exit. Ensure Nipe is working correctly or that `DISABLE_DNS` is set to `true` and is successfully applied.
- **Remote Cleanup Failure**: Some cleanup commands might require specific permissions or might not apply to all Linux distributions. The script attempts to run them with `sudo` and continues even if some fail.

---

7. Customization

- **Nmap/Whois Options:** You can specify custom Nmap and Whois command-line options when prompted by the script.
- **Adding More Scans:** To add more remote commands, edit the `do_recon` function in the script and add your `sshpass` command:

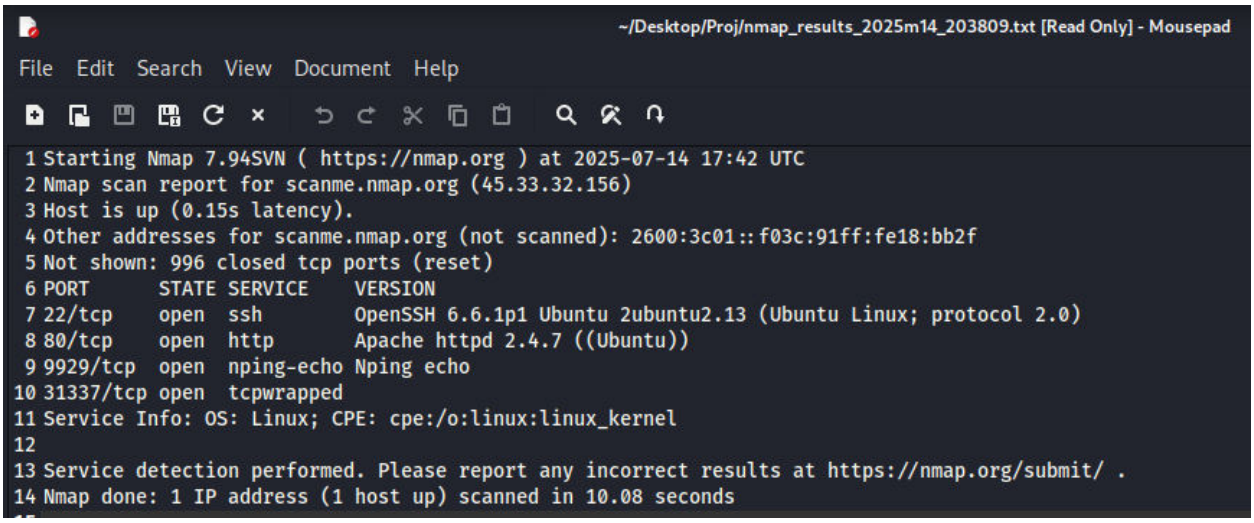
```
# Example: run a traceroute
# $(sshpass -p "$SSH_PASS" ssh -o StrictHostKeyChecking=no -p
"$DEFAULT_REMOTE_SSH_PORT" "$SSH_USER@$SSH_IP" "traceroute
$TARGET_ADDRESS") > "$TRACEROUTE_FILE"
```

---

8. Entire Flow in screenshots:

```
2025-07-14_20:38:09 - Starting Recon Automation Tool...

2025-07-14_20:38:09 - Checking and installing required dependencies on local machine...
2025-07-14_20:38:09 - sshpass is already installed locally.
2025-07-14_20:38:09 - cpanm is already installed locally.
2025-07-14_20:38:09 - git is already installed locally.
2025-07-14_20:38:10 - macchanger is already installed locally.
2025-07-14_20:38:10 - dhclient is already installed locally.
2025-07-14_20:38:10 - All required APT dependencies are already installed on local machine.
2025-07-14_20:38:10 - Nipe is already installed and configured in /root/nipe.
2025-07-14_20:38:10 - Nipe installation completed successfully.

2025-07-14_20:38:10 - Setting up anonymity for local machine...
2025-07-14_20:38:10 - MAC spoofing is disabled. Skipping MAC address change.

2025-07-14_20:38:10 - Disabling local DNS queries by backing up and modifying /etc/resolv.conf...
2025-07-14_20:38:10 - Original /etc/resolv.conf backed up to /tmp/resolv.conf.bak_20250714_203809
2025-07-14_20:38:10 - Local DNS queries disabled (resolv.conf set to 127.0.0.1).
2025-07-14_20:38:10 - Nipe is not active. Attempting to start Nipe...
2025-07-14_20:38:18 - Nipe started successfully.

2025-07-14_20:38:18 - Performing mandatory anonymity checks...
2025-07-14_20:38:20 - Network connection is anonymus via Nipe.
2025-07-14_20:38:20 - ⟶ Spoofed Country: BG
2025-07-14_20:38:20 - ⟶ Spoofed IP Address: 93.123.109.116
2025-07-14_20:38:21 - No DNS leaks detected.
2025-07-14_20:38:21 - Skipping MAC address change check as MAC spoofing is not enabled.
2025-07-14_20:38:21 - Anonymity checks passed.

Enter remote server IP address: 185.227.110.68
Enter remote server SSH username: root
Enter remote server SSH password:

2025-07-14_20:39:14 - Attempting to connect to remote server: root@185.227.110.68
2025-07-14_20:39:21 - Remote server info: Remote server IP: 93.123.109.116
Remote server uptime: up 3 minutes

2025-07-14_20:39:21 - Setting up remote server for reconnaissance...
2025-07-14_20:39:21 - Checking and installing required dependencies on remote server (root@185.227.110.68)...
2025-07-14_20:39:23 - nmap is already installed on remote server.
2025-07-14_20:39:23 - whois is already installed on remote server.
2025-07-14_20:39:23 - All required dependencies are already installed on remote server.
2025-07-14_20:39:23 - Remote server setup completed.

Enter the target address (IP or hostname) to scan:
```

```
Enter the target address (IP or hostname) to scan: scanme.nmap.org
2025-07-14_20:42:24 - Target address set to: scanme.nmap.org

Do you want to change the default Nmap options? [-Pn -sV]:
Do you want to change the default Whois options? []:
2025-07-14_20:42:38 - Executing Whois for scanme.nmap.org on remote server (root@185.227.110.68)...
2025-07-14_20:42:41 - Whois command executed successfully on remote server.
2025-07-14_20:42:41 - Whois results saved to /home/kali/Desktop/Proj/whois_results_20250714_203809.txt
2025-07-14_20:42:41 - Executing Nmap scan for open ports on scanme.nmap.org from remote server (root@185.227.110.68)...
2025-07-14_20:42:53 - Nmap scan executed successfully on remote server.
2025-07-14_20:42:53 - Nmap results saved to /home/kali/Desktop/Proj/nmap_results_2025m14_203809.txt

2025-07-14_20:42:53 - Clean up traces on remote machine (root@185.227.110.68)...
2025-07-14_20:42:55 - Remote machine cleanup completed successfully.

2025-07-14_20:42:55 - All done.

2025-07-14_20:42:55 - Whois results saved to: /home/kali/Desktop/Proj/whois_results_20250714_203809.txt
2025-07-14_20:42:55 - Nmap results saved to: /home/kali/Desktop/Proj/nmap_results_2025m14_203809.txt
2025-07-14_20:42:55 - Audit log saved to: /home/kali/Desktop/Proj/recon_log_20250714_203809.txt
2025-07-14_20:42:55 - Script will now exit and all configurations will be restored to original state...

2025-07-14_20:42:55 - dhclient is already with default settings.
2025-07-14_20:42:55 - Restoring original local DNS configuration...
2025-07-14_20:42:55 - Original /etc/resolv.conf restored.
2025-07-14_20:42:55 - DNS backup file removed.
2025-07-14_20:42:55 - MAC spoofing was not executed, skipping MAC address restoration.
2025-07-14_20:42:55 - Nipe stopped. Tor circuit is no longer active.
```



Example NMAP scan report.

Created by radtonev

radtonev@gmail.com

https://github.com/radtonev

https://www.linkedin.com/in/radtonev/