TOR To Protect Your System

by

AKSHARA PINNOJU

TABLE OF CONTENTS

1. INTRODUCTION

In this project, I explored TOR (The Onion Router) for anonymous browsing and proxychains for added privacy. TOR allows users to protect their identity and location by routing traffic through a decentralized network.

2. User Management & System Setup

Creating and managing user accounts is essential for secure system access.

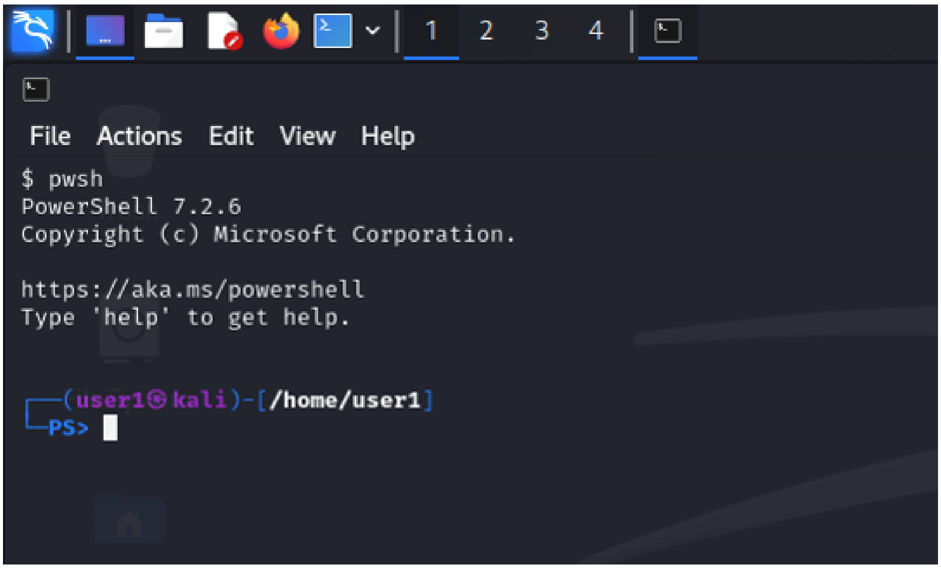
Commands I Used

1) **sudo adduser user1**
Creates a new user named 'user1' with a home directory.

2) **sudo useradd -m user2**
Adds 'user2' to the sudo group, granting administrative privileges.

3) **sudo -s /bin/bash user1**
Gives 'user1' a root shell with full system control.

4) **sudo chsh -s /bin/bash user2**
Changes the default shell for 'user2' to Bash for better usability.



```
$ pwsh
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

┌──(user1㉿kali)-[/home/user1]
└─PS> 
```

3. TOR Installation & Configuration

Installing **TOR** to enable anonymous internet access.

Commands I Used

1) **sudo apt install tor**
Installs the TOR service on the system from official repositories.

2) **sudo systemctl restart tor.service**
Restarts the TOR service to apply changes.

3) **sudo systemctl stop tor.service**
Manually stops the TOR service when needed.

4) **sudo systemctl start tor.service**
Manually starts the TOR service when needed.

4. Proxychains Setup

Configuring proxychains to route traffic through TOR for anonymity.

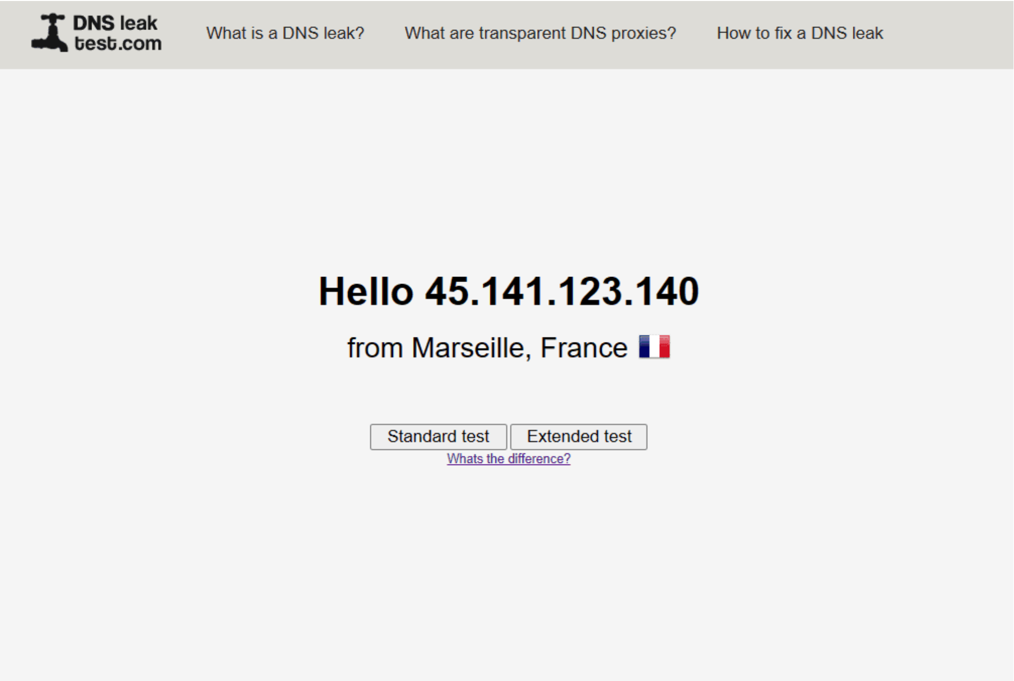
Commands I Used

1) **sudo nano /etc/proxychains4.conf**
Opens the ProxyChains configuration file for editing.

```
socks5 5.189.229.42 1080
socks5 89.201.4.136 33427
socks5 165.22.88.91 1080
socks5 192.162.84.208 1080
```

These proxies enhance anonymity by routing traffic through multiple locations.

2) proxychains firefox www.dnsleaktest.com
Launches Firefox through proxychains to test DNS leaks.



Hello 45.141.123.140

from Marseille, France

5. VPN Integration for Added Security

Using VPNBook, a free VPN service, to add another layer of privacy.

Commands I Used

1) unzip VPNBook.com-OpenVPN-FR1.zip
Extracts the downloaded VPN configuration files.

2) openvpn vpnbook-de4-tcp443.ovpn
Starts an OpenVPN connection using the VPNBook configuration.

6. DNS Leak Testing & Network Configuration

Using VPNBook, a free VPN service, to add another layer of privacy.

Commands I Used

1) **cat /etc/resolv.conf**
Displays the system’s current DNS resolver settings.

2) **systemctl restart NetworkManager**
Restarts the network service to apply DNS changes.

3) **nano /etc/resolv.conf**
Opens the file for editing to manually configure DNS settings.

4) **nameserver 1.1.1.1**
Sets Cloudflare's DNS (1.1.1.1) for improved privacy.

7. Password Reset & System Hardening

Resetting passwords and ensuring system security.

Commands I Used

1) **restart machine**
Reboots the system to enter recovery mode.

2) **in grub press e**
in Linux - ro to rw init=/bin/bash
Modifies GRUB boot parameters to enable root access.

3) **passwd**
Changes the system password for improved security.

8. Conclusion

Through this project, I explored how **Tor** enhances online anonymity by routing traffic through multiple relays, making it difficult to track a user's real IP address. I set up Tor, configured ProxyChains to route traffic through various SOCKS5 proxies, and tested DNS leaks to ensure privacy. Additionally, I integrated a **VPN** for an extra layer of security and learned how to manage the Tor service efficiently. By combining **Tor, ProxyChains, and a VPN**, I gained practical experience in securing internet connections and minimizing online tracking risks, reinforcing the importance of anonymity in cybersecurity.

Appendix: Project Requirement

Below is the original project requirement provided by **Plasmid Innovation** as part of the Cybersecurity Internship Training.

Project link:

https://github.com/Aksharapinnoju/TOR-to-protect-your-systemm