### 

With the current era of digital surveillance and network monitoring, it has been increasingly challenging to protect online anonymity and maintain privacy. Classic options like Virtual Private Networks (VPNs) and proxies give consumers some form of protection but nevertheless depend on a centralized server that can be attacked, monitored, and intervened against by governments. To reduce these threats, Anon-Route has been created—a robust and streamlined tool which takes advantage of the Tor network in order to supply anonymous, encrypted internet traffic to Linux users.

Anon-Route is a command-line application which allows the user to install a transparent proxy via the Tor network, ensuring all outbound traffic, whether an application or a protocol, will pass via Tor. Using Tor's Onion Routing method, the tool ensures that the IP address of the user is concealed and all the traffic is anonymized, such that it is virtually impossible for third parties to track the online activities of the user. The tool works by setting up iptables, which is a utility for establishing firewall rules on Linux, to divert traffic through Tor automatically without having to be manually configured by the user.

The core aim of this project is to offer a user-friendly, lightweight, open-source solution for passing internet traffic via the Tor network. Anon-Route focuses on meeting increasing demands for privacy-oriented tools, which are easy to deploy, secure by nature, and that need little manual intervention from the user. Anon-Route seeks to banish the simplicity of typical VPN configurations and supply an easy command-line interface for users to make their anonymity uncomplicated.

This project offers a concrete, real-life application for cyber security professionals, privacy-oriented users, and researchers who require securing anonymity at the network level and operating using Linux-based systems. It enables the user to enjoy their privacy without relying on central services so they can be obscured from observation or tracking processes. With this project, users come to better know network security, privacy practice, and applying safe communication protocols.

# IMPLEMENTATION

The deployment phase of the AnonRoute project is converting the design architecture into a functional solution by employing Bash scripting on Linux. This chapter documents a detailed description of how different parts of the system were implemented, integrated, and tested to produce secure and anonymous routing of all traffic via the Tor network.

### IMPLEMENTATION ENVIORMENT

### The creation and testing of AnonRoute took place in a reproducing and controlled setting for reliability and compatibility assurance.

### Platform

### Operating System: Kali Linux 2023.4 (penetration testing Debian-based distro)

### Kernel Version: Linux kernel 6.x

### Environment: VMware Workstation / VirtualBox virtualized environment

### Execution Shell: GNU Bash (version 5.x)

### Tools and Utilities

### Tor – Executed as the principal anonymity network utility.

### iptables – Utilized for redirection of traffic and firewall configuration.

### netfilter-persistent – (Optional) To persist iptables rules on reboot.

### whois / curl / wget – For IP verification and web requests.

### ANSI escape codes – For colored, formatted CLI output.

### IMPLEMENTATION STEPS

### The process of implementing AnonRoute is divided into several functional modules, each handling a particular feature of the tool.

### ****Project Setup****

### Installed all required dependencies using:

### 

Figure . Setup commands

### Verified that the tor service is enabled and properly configured to listen on:

### TransPort: 9040

### DNSPort: 5353

### Downloading AnonRoute From Github

### 

Figure . Downloading Repository from GitHub

### Enter Anon-Route Directory and Install it

### 

Figure . Navigating Anon-Route

### 

Figure . Installing Anon-Route

### Commands

### Start transparent proxy through Anon-Route

### <sudo anonrote -t> or <sudo anonroute --tor>

### 

Figure . Command 1 Starting TOR Proxy

### OUTPUT:

### 

### 

Figure . Anon-Route Interface

### Reset iptables and return to Clearnet navigation

### <sudo anonrote -c> or <sudo anonroute --clearnet>

### 

Figure . Command 2 Clearnet Navigation

### OUTPUT:

### 

Figure . Command 2 Output

### Check status of program and services

### <sudo anonrote -s> or <sudo anonroute --status>

### 

Figure . Command 3 Checking Status

### OUTPUT

### 

Figure Command 3 Output

### Show public IP address

### <sudo anonrote -i > or <sudo anonroute --ipinfo>

### 

Figure . Command 4 IP Information

### OUTPUT

### 

Figure . Command 4 Output

### Display current IP Table Rules

### <sudo anonrote -tb> or <sudo anonroute --table>

### 

Figure . Command 5 Showing IP Table Rules

### OUTPUT

### 

Figure . IP Table Rules

### Display system's CPU, RAM, and disk usage performance

### <sudo anonrote -rc> or <sudo anonroute –resource-check>

### 

Figure . Command 6 Resource Check

### OUTPUT

### 

Figure . System Performance

### Rotate the Tor IP automatically after 10 seconds

### <sudo anonrote -rip> or <sudo anonroute –rotate-ip>

### 

Figure . Command 7 Rotating IP

### OUTPUT

### 

Figure . Command 7 Output

### Restart tor service and change IP address

### <sudo anonrote -r> or <sudo anonroute --restart>

### 

Figure . Command 9 Restarting TOR services

### OUTPUT

### 

Figure . Command 9 Output

### Display program version and exit

### <sudo anonrote -v> or <sudo anonroute --version>

### 

Figure . Command 10 Version

### OUTPUT

### 

Figure . Current version of Anon-Route

### Help Message for learners

### <sudo anonrote -h> or <sudo anonroute --help>

### 

Figure Command 9 Show Help Menu

### OUTPUT

### 

Figure . Help Menu

### SCRIPT MODULARIZATION

Table 4‑‑ Script Modularization

### 

### ERROR HANDELING AND VALIDATIONS

### Dependency Checks: The user is notified and the script terminates if tor or iptables is not found.

### Root Privilege Check: The script inspects for root privileges and refuses to run if it is not run as root or with the use of sudo.

### Tor Service Failure: The script notifies the user if the Tor service doesn't start, instructing the user to check the service logs manually.

### Invalid Input: If the user has entered an invalid menu option, a warning message is shown and the menu is refreshed.

### SECURITY CONSIDERATION

### All non-Tor outgoing traffic is blocked so that there will be zero leaks.

### DNS leaks are avoided by forwarding DNS requests through Tor's DNSPort.

### Whitelisting just Tor's UID prevents an attempt to establish a routing loop for Tor's own traffic.

### The script won't store user data or log anything, making it private

### IMPROVEMENTS FROM PREVIOUS TOOLS

* Compared to tools like Kalitorify or toriptables2, **AnonRoute**:
  + Uses reduced logic and fewer dependencies.
  + Delivers immediate status feedback.
  + Maintenance of modular functions is significantly easier.
  + Includes additional functionality such as restart and IP validation.

# CONCLUSION

# SUMMARY OF THE PROJECT

# The AnonRoute project was created with the main objective of facilitating anonymous web surfing by directing all internet traffic through the Tor network via a transparent proxy mechanism. The tool was written as a Bash shell script specifically for Kali Linux, which automated the setup of iptables, the Tor service, and DNS leak protection to provide privacy and anonymity.

# During this project, the tool exhibited features such as:

# Autmatically launching and closing the Tor-based proxy.

# Redirecting all TCP traffic to use Tor.

# Avoiding DNS leaks by making DNS resolution occur through Tor.

# Enabling checking the users current public IP to confirm anonymity.

# Having a lightweight and easy-to-use command-line interface.

# The project was successfully completed and shown to be useful in enhancing privacy on the Internet by hiding the actual IP address and blocking leakage of traffic out of the Tor network.

# KEY OUTCOMES

# Secure and Anonymous Routing: AnonRoute offered a trustworthy means of anonymizing internet traffic via Tor.

# Automated Setup: All system-level settings required for the tool were automated, so it was available even to users with minimal technical expertise.

# DNS Leak Protection: By sending DNS requests via Tor, AnonRoute prevented DNS leaks that would reveal user anonymity.

# User Control: The software gave users the convenience to initiate, shut down, reboot, and observe their anonymous routing configuration seamlessly.

**FUTURE WORK**

* **Graphical User Interface (GUI):** Including a GUI frontend for simpler interaction.
* **Multi-platform Support:** Expanding support to other Linux distributions and even Windows with WSL.
* **Advanced Traffic Routing:** Allowing user-specified applications to route selectively over Tor while leaving others on the normal network
* **Integration with VPN:** Merging Tor with VPN layers for increased anonymity.

**FINAL WORDS**

AnonRoute is a solid foundation for privacy-oriented users and researchers who seek to investigate secure traffic routing through open-source networks such as Tor. As privacy concerns expand around the world, technologies such as AnonRoute help create a protective barrier against surveillance, tracking, and censorship. This project not only fulfills technical requirements but also helps promote the ethical significance of digital freedom.