How AnonSurf Broke My Kali Linux Network (And How I Fixed IPv4 Connectivity)

When learning cybersecurity, it's common to explore privacy tools like **AnonSurf** in Kali Linux.

AnonSurf promises to route all your system traffic through the Tor network, giving you anonymity while browsing.

But during my lab, I learned an important lesson:

Privacy tools can easily break your networking if you don't understand what they change under the hood.

In this blog, I'll share how AnonSurf caused DNS and IPv4 failures in my Kali VM — and the exact steps I used to fix it.

What is AnonSurf?

AnonSurf is a tool that forces **all system traffic** through the Tor network using:

- iptables rules
- DNS changes
- Tor proxy tunneling

It is designed for privacy-focused workflows such as OSINT research.

However, it modifies core networking components, so mistakes can cause connectivity problems.

How to Install AnonSurf in Kali Linux

AnonSurf is a tool that routes all system traffic through the Tor network using iptables. It is commonly used for privacy-focused browsing and OSINT labs.

This guide shows how to install it on Kali Linux.

Step 1: Update Your System

Before installing anything, update Kali packages:

```
sudo apt update && sudo apt upgrade -y
```

Step 2: Install Required Dependencies

AnonSurf requires Tor and networking tools:

```
sudo apt install tor curl git -y
```

Step 3: Clone the AnonSurf Repository

Download the project from GitHub:

```
git clone https://github.com/Und3rf10w/kali-anonsurf.git
```

Move into the folder:

```
cd kali-anonsurf
```

Step 4: Make the Installer Executable

Give execution permission:

```
chmod +x installer.sh
```

Step 5: Run the Installer

Install AnonSurf system-wide:

```
sudo ./installer.sh
```

Once complete, the `anonsurf` command will be available globally.

Step 6: Verify Installation

Check that AnonSurf is installed:

```
anonsurf
```

You should see usage instructions like:

```
Usage:
 anonsurf {start|stop|restart|change|status}
```

The Problem I Encountered

After starting AnonSurf, I tried a simple test:

```
curl ifconfig.me
```

Instead of showing my IP, I received:

```
Could not resolve host: ifconfig.me
```

This immediately showed that something was wrong with DNS resolution.

DNS Was Broken

AnonSurf modifies the file:

```
/etc/resolv.conf
```

When I opened it, I saw DNS servers like:

```
nameserver 75.75.75.75
nameserver 75.75.76.76
```

These DNS servers were not resolving properly inside my VirtualBox Kali VM.

So the system could not translate domain names into IP addresses.

IPv6 Worked, But IPv4 Failed

After fixing DNS, I noticed something strange:

```
curl ifconfig.me
```

worked and returned an IPv6 address:

```
2601:2c6:4601:...
```

But forcing IPv4 failed:

```
curl -4 ifconfig.me
```

Result:

```
Failed to connect… Could not connect to server
```

This meant:

- IPv6 connectivity was fine
- IPv4 routing was broken

Ping also failed at first:

```
ping google.com
```

Root Cause

AnonSurf had done two major things:

1. Modified DNS settings
2. Applied iptables routing rules for Tor

Even after DNS was restored, leftover firewall rules were interfering with IPv4 traffic.

Step-by-Step Fix

Step 1: Stop AnonSurf

First, I stopped the service:

```
sudo anonsurf stop
```

Step 2: Restore DNS

I edited the resolv.conf file:

```
sudo nano /etc/resolv.conf
```

And replaced everything with:

```
nameserver 8.8.8.8
nameserver 1.1.1.1
```

These are Google and Cloudflare DNS servers.

Step 3: Restart Networking

Then I restarted NetworkManager:

```
sudo systemctl restart NetworkManager
```

Step 4: Reset iptables Rules

To fully remove Tor routing effects:

```
sudo iptables -F
sudo iptables -t nat -F
sudo iptables -X
```

And reset policies:

```
sudo iptables -P INPUT ACCEPT
sudo iptables -P OUTPUT ACCEPT
sudo iptables -P FORWARD ACCEPT
```

Confirming the Fix

Finally, IPv4 worked again:

```
curl -4 ifconfig.me
```

Output:

```
73.xxx.xxx.xxx
```

Ping also worked normally:

```
ping google.com
```

Result:

```
0% packet loss
```

At this point, networking was fully restored.

Key Lesson Learned

This lab taught me an important real-world IT lesson:

Tools like AnonSurf can break networking because they modify DNS and firewall rules at the system level.

For most cybersecurity learners, a safer alternative is using Tor Browser instead of system-wide tunneling.

Final Thoughts

Troubleshooting this issue helped me strengthen skills in:

- Linux networking
- DNS troubleshooting
- IPv4 vs IPv6 behavior

- Firewall (iptables) resets
- VirtualBox lab stability

This is exactly the kind of real-world debugging that IT Support and SOC roles require.