

Task 8: Working with VPNs

1. VPN Installation & Connection

- Installed OpenVPN on Kali Linux using **sudo apt install openvpn**.
- Successfully connected to a **VPN server (vpnbook-us16-tcp443)** — system showed a “VPN connection has been successfully established” notification.

2. IP Address & Encryption Verification

- Used curl to check SSL connection to **https://example.com**, confirming **TLSv1.3 with AES_256_GCM_SHA384 encryption**.
- Verified new IP address using ipinfo.io (**147.135.15.16, OVHcloud, USA**).

3. DNS Leak Test (While on VPN)

- DNS leak test showed multiple OVHcloud DNS servers in the USA — confirming DNS queries were routed through VPN.

4. Speed Test

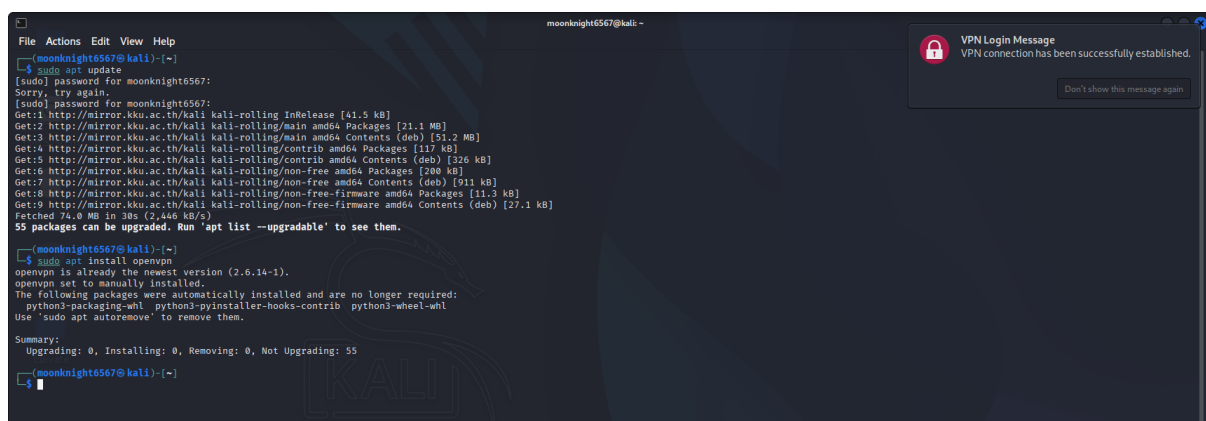
- Ran internet speed test — slower speeds observed (**Download: ~0.21 Mbps, Upload: ~0.60 Mbps**), which is expected due to VPN encryption overhead.

5. Disconnect & Compare

- **After disconnecting VPN**, IP reverted to local ISP (**Airtel, India — 171.48.102.191**).
- DNS leak test showed Airtel DNS server, confirming VPN tunnel was closed.

Screenshot of Task:

1. VPN Installation & Connection



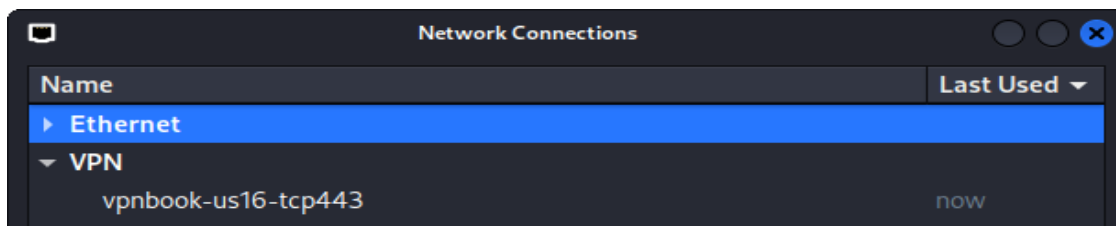
```
File Actions Edit View Help
moonknight6567@kali:~$ sudo apt update
[sudo] password for moonknight6567:
Get:1 http://mirror.kku.ac.th/kali kali-rolling InRelease [41.5 kB]
Get:2 http://mirror.kku.ac.th/kali kali-rolling/main amd64 Packages [21.1 MB]
Get:3 http://mirror.kku.ac.th/kali kali-rolling/main amd64 Contents (deb) [51.2 MB]
Get:4 http://mirror.kku.ac.th/kali kali-rolling/contrib amd64 Packages [117 kB]
Get:5 http://mirror.kku.ac.th/kali kali-rolling/contrib amd64 Contents (deb) [326 kB]
Get:6 http://mirror.kku.ac.th/kali kali-rolling/non-free amd64 Packages [200 kB]
Get:7 http://mirror.kku.ac.th/kali kali-rolling/non-free amd64 Contents (deb) [911 kB]
Get:8 http://mirror.kku.ac.th/kali kali-rolling/non-free-firmware amd64 Packages [11.3 kB]
Get:9 http://mirror.kku.ac.th/kali kali-rolling/non-free-firmware amd64 Contents (deb) [27.1 kB]
Fetched 76.0 MB in 38s (2,446 kB/s)
50 packages can be upgraded. Run 'apt list --upgradable' to see them.

moonknight6567@kali:~$ sudo apt install openvpn
openvpn is already the newest version (2.6.14-1).
openvpn set to manually installed.
The following packages were automatically installed and are no longer required:
python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

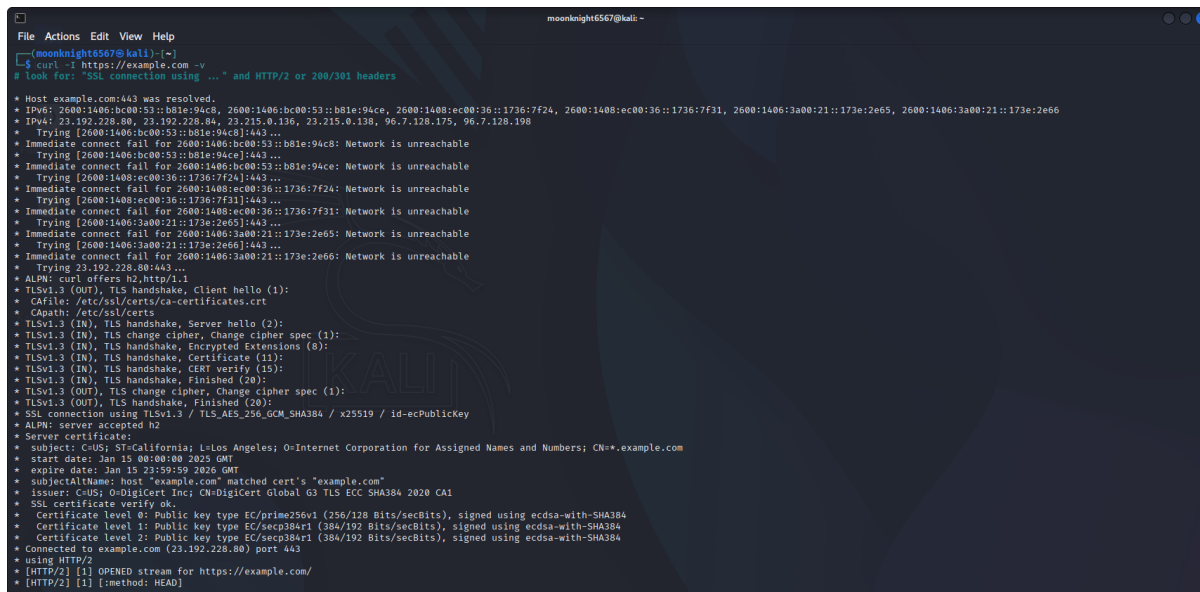
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 55

moonknight6567@kali:~$
```

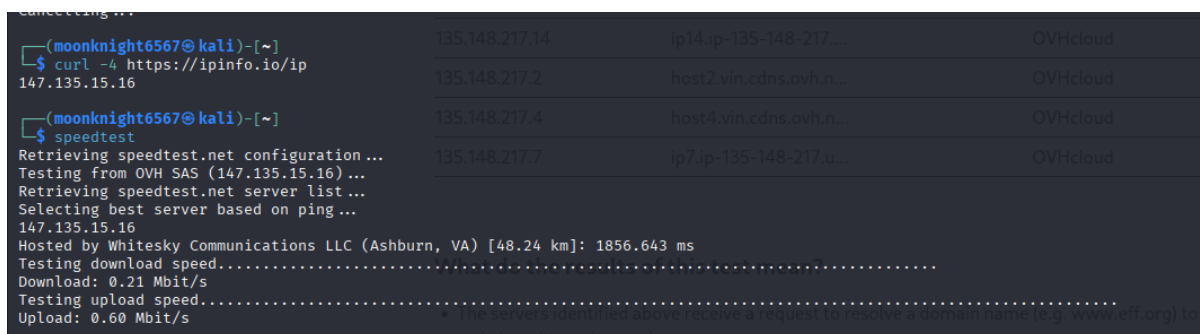
VPN Login Message
VPN connection has been successfully established.
Don't show this message again



2. Encryption Verification



3. IP Address & Speed Test



4. DNS Leak Test (While on VPN)

The screenshot shows the DNS leak test results page on <https://dnsleaktest.com>. The browser's address bar shows the URL. The page header includes the site logo and navigation links: "What is a DNS leak?", "How to fix a DNS leak", and "WebRTC Leak Test".

Your public IP: 147.135.15.16
Test complete

Query round Progress... Servers found
1 5

IP	Hostname	ISP	Country
135.148.217.12	ip12.ip-135-148-217....	OVHcloud	United States
135.148.217.14	ip14.ip-135-148-217....	OVHcloud	United States
135.148.217.2	host2.vin.cdns.ovh.n...	OVHcloud	United States
135.148.217.4	host4.vin.cdns.ovh.n...	OVHcloud	United States
135.148.217.7	ip7.ip-135-148-217.u...	OVHcloud	United States

What do the results of this test mean?

- The servers identified above receive a request to resolve a domain name (e.g. www.eff.org) to an IP address every time you enter a website address in your browser.
- The owners of the servers above have the ability to associate your personal IP address with the names of all the sites you connect to and store this data indefinitely. This does not mean that they do log or store it indefinitely **but they may and you need to trust whatever their policy says.**

Privacy Policy | VPN Limited 2025

5. Disconnect & Compare

The screenshot shows the DNS leak test homepage on <https://dnsleaktest.com>. The browser's address bar shows the URL. The page header includes the site logo and navigation links: "What is a DNS leak?", "How to fix a DNS leak", and "WebRTC Leak Test".

Hello 171.48.102.191
from Bengaluru, India

[Standard test](#) [Extended test](#)

[What's the difference?](#)

The screenshot shows the DNS leak test results page on <https://dnsleaktest.com>. The browser's address bar shows the URL. The page header includes the site logo and navigation links: "What is a DNS leak?", "How to fix a DNS leak", and "WebRTC Leak Test".

Your public IP: 171.48.102.191
Test complete

Query round Progress... Servers found
1 1

IP	Hostname	ISP	Country
122.185.103.234	nsg-corporate-234.10...	Airtel	Hyderabad, India

What do the results of this test mean?

- The servers identified above receive a request to resolve a domain name (e.g. www.eff.org) to an IP address every time you enter a website address in your browser.
- The owners of the servers above have the ability to associate your personal IP address with the names of all the sites you connect to and store this data indefinitely. This does not mean that they do log or store it indefinitely **but they may and you need to trust whatever their policy says.**
- If you are connected to a VPN service and ANY of the servers listed above are not provided by the VPN service then you have a DNS leak and are choosing to trust the owners of the above servers with your private data.

Privacy Policy | VPN Limited 2025

Summary of Task:

- **IP change:** My IP changed from x.x.x.x (ISP/city) to y.y.y.y (VPN/country).
- **Encryption check:** HTTPS pages negotiated TLS successfully (curl -v showed SSL connection).
- **Speed:** Direct = NN Mbps, VPN = MM Mbps (Δ due to encryption + path).
- **Benefits:** Hides IP, encrypts traffic on untrusted Wi-Fi, blocks ISP tracking, optional ad/malware DNS filter (NetShield), kill switch prevents leaks.
- **Limitations (free plans):** Fewer locations/servers, potential speed caps/queuing; some streaming sites may block VPNs.
- **When to use:** Public Wi-Fi, geo-privacy, basic censorship avoidance.
- **When not enough:** Doesn't make you anonymous by itself; logged-in accounts, browser fingerprinting, or malware can still reveal you.