

## # Nebula Lab Report

### ## 1. Objective

- Deploy a **Nebula Lighthouse** on a cloud VPS (with public IP).
- Configure **Windows PC** (behind NAT) as a Nebula client.
- Establish a secure overlay network between Lighthouse and client.
- Verify connectivity using **ping** and **SSH login**.

---

### ## 2. Environment

- **Operating Systems**: Windows 10 (local PC), Linux VPS (Lighthouse)
- **Software Tools**:
  - Nebula 1.9.6
  - PowerShell
  - GitHub (for report submission)
- **Network Setup**:
  - Lighthouse VPN IP: `192.168.100.1`
  - Client VPN IP: `192.168.100.150`
  - Overlay subnet: `192.168.100.0/24`

---

### ## 3. Steps

#### ### 3.1 Download and Install Nebula

Downloaded from [Releases](https://github.com/slackhq/nebula/releases) and extracted to `C:\nebula\`.

Screenshot 1: Nebula folder structure

---

#### ### 3.2 Obtain Certificates and Keys

Received the following files from the instructor and placed them in `C:\nebula\config\`:

- `ca.crt`
- `tanzelin.crt`
- `tanzelin.key`

Screenshot 2: Certificate files in config folder

---

### ### 3.3 Edit `config.yaml`

Configured as follows (use `/` or double `\\` in paths):

```yaml

pki:

ca: "C:/nebula/config/ca.crt"

cert: "C:/nebula/config/tanzelin.crt"

key: "C:/nebula/config/tanzelin.key"

static\_host\_map:

"192.168.100.1": ["104.243.20.247:554"]

lighthouse:

am\_lighthouse: false

hosts:

- "192.168.100.1"

listen:

host: 0.0.0.0

port: 554

tun:

dev: nebula1

cidr: 192.168.100.150/24

punchy:

punch: true

```
2 # Some options in this file are HUPable, including the pki section. (A HUP will reload credentials from disk without affecting existing
3
4 # PKI defines the location of credentials for this node. Each of these can also be inlined by using the yaml ":" syntax.
5 pki:
6   # The CAs that are accepted by this node. Must contain one or more certificates created by 'nebula-cert ca'
7   ca: "C:\\nebula\\config\\ca.crt"
8   cert: "C:\\nebula\\config\\tanzelin.crt"
9   key: "C:\\nebula\\config\\tanzelin.key"
10  # blocklist is a list of certificate fingerprints that we will refuse to talk to
11  #blocklist:
12  #   - c99d4e650533b92061b09918e838a5a0a6a0ee21eed1d12fd937682865936c72
13  # disconnect_invalid is a toggle to force a client to be disconnected if the certificate is expired or invalid.
14  #disconnect_invalid: false
15
16 # The static host map defines a set of hosts with fixed IP addresses on the internet (or any network).
17 # A host can have multiple fixed IP addresses defined here, and nebula will try each when establishing a tunnel.
```

```
Windows PowerShell
版权所有 (C) Microsoft Corporation. 保留所有权利。
安装最新的 PowerShell, 了解新功能和改进! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> cd C:\nebula\
PS C:\nebula> .\nebula.exe -config .\config\config.yaml
time="2025-09-16T16:09:41+08:00" level=info msg="Firewall rule added" firewallRule="map[caName: caSha: direction:outgoing endPort:0 groups:[] host:any ip: localIp: proto:0 startPort:0]"
time="2025-09-16T16:09:41+08:00" level=info msg="Firewall rule added" firewallRule="map[caName: caSha: direction:incoming endPort:0 groups:[] host:any ip: localIp: proto:0 startPort:0]"
time="2025-09-16T16:09:41+08:00" level=info msg="Firewall started" firewallHashes="SHA:498215dec4e687a2353f51c10838c113bdiaf35ef72b8e8c9f536986ada5417, FNV:2782948616"
2025/09/16 16:09:41 Using existing driver 0.14
2025/09/16 16:09:41 Creating adapter
time="2025-09-16T16:09:42+08:00" level=info msg="listening on 0.0.0.0:554"
time="2025-09-16T16:09:42+08:00" level=error msg="falling back to standard udp sockets" error="bind: The attempted operation is not supported for the type of object referenced."
time="2025-09-16T16:09:42+08:00" level=info msg="Main HostMap created" network=192.168.100.150/24 preferredRanges=[]
time="2025-09-16T16:09:42+08:00" level=info msg="punchy enabled"
time="2025-09-16T16:09:42+08:00" level=info msg="Loaded send_recv_error config" sendRecvError=always
time="2025-09-16T16:09:42+08:00" level=info msg="Nebula interface is active" boringcrypto=false build=1.9.6 interface=nebula network=192.168.100.150/24 udpAddr="[:,554]"
time="2025-09-16T16:09:42+08:00" level=info msg="Handshake message sent" handshake="map[stage:1 style:ix_psk0]" initiatorIndex=17550575 localIndex=17550575 remoteIndex=0 udpAddr="[104.243.20.247:554]" vpnIp=192.168.100.1
time="2025-09-16T16:09:42+08:00" level=info msg="Handshake message received" certName=lighthouse durationNs=443061600 fingerprint=fbf998b866c8275810b0be0c175cd7cbf31be03d0adc2a831ae16f9669a52617 handshake="map[stage:2 style:ix_psk0]" initiatorIndex=17550575 issuer=e430f526e15e22d11dbb26e9482945865f17aa42c800481e66f68d087c892c0 remoteIndex=17550575 responderIndex=569875743 sentCachedPackets=1 udpAddr="104.243.20.247:554" vpnIp=192.168.100.1
time="2025-09-16T16:09:48+08:00" level=info msg="Handshake timed out" durationNs=6701691800 handshake="map[stage:1 style:ix_psk0]" initiatorIndex=2640036116 localIndex=2640036116 remoteIndex=0 udpAddr="" vpnIp=192.168.100.255
```

Microsoft Windows [版本 10.0.26100.6584]  
(c) Microsoft Corporation. 保留所有权利。

C:\Users\lenovo>ping 192.168.100.1

正在 Ping 192.168.100.1 具有 32 字节的数据:

来自 192.168.100.1 的回复: 字节=32 时间=215ms TTL=64

来自 192.168.100.1 的回复: 字节=32 时间=213ms TTL=64

来自 192.168.100.1 的回复: 字节=32 时间=573ms TTL=64

来自 192.168.100.1 的回复: 字节=32 时间=210ms TTL=64

192.168.100.1 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),  
往返行程的估计时间(以毫秒为单位):

最短 = 210ms, 最长 = 573ms, 平均 = 302ms

C:\Users\lenovo>

```
C:\Users\lenovo>ssh nuist@192.168.100.1
The authenticity of host '192.168.100.1 (192.168.100.1)' can't be established.
ED25519 key fingerprint is SHA256:TmUkvmFj55DEVuujeA28kHINrqVK39QgRh9eZ2Uy0zA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.1' (ED25519) to the list of known hosts.
nuist@192.168.100.1's password:
Permission denied, please try again.
nuist@192.168.100.1's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-151-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Sep 16 08:29:40 2025 from 192.168.100.135
```