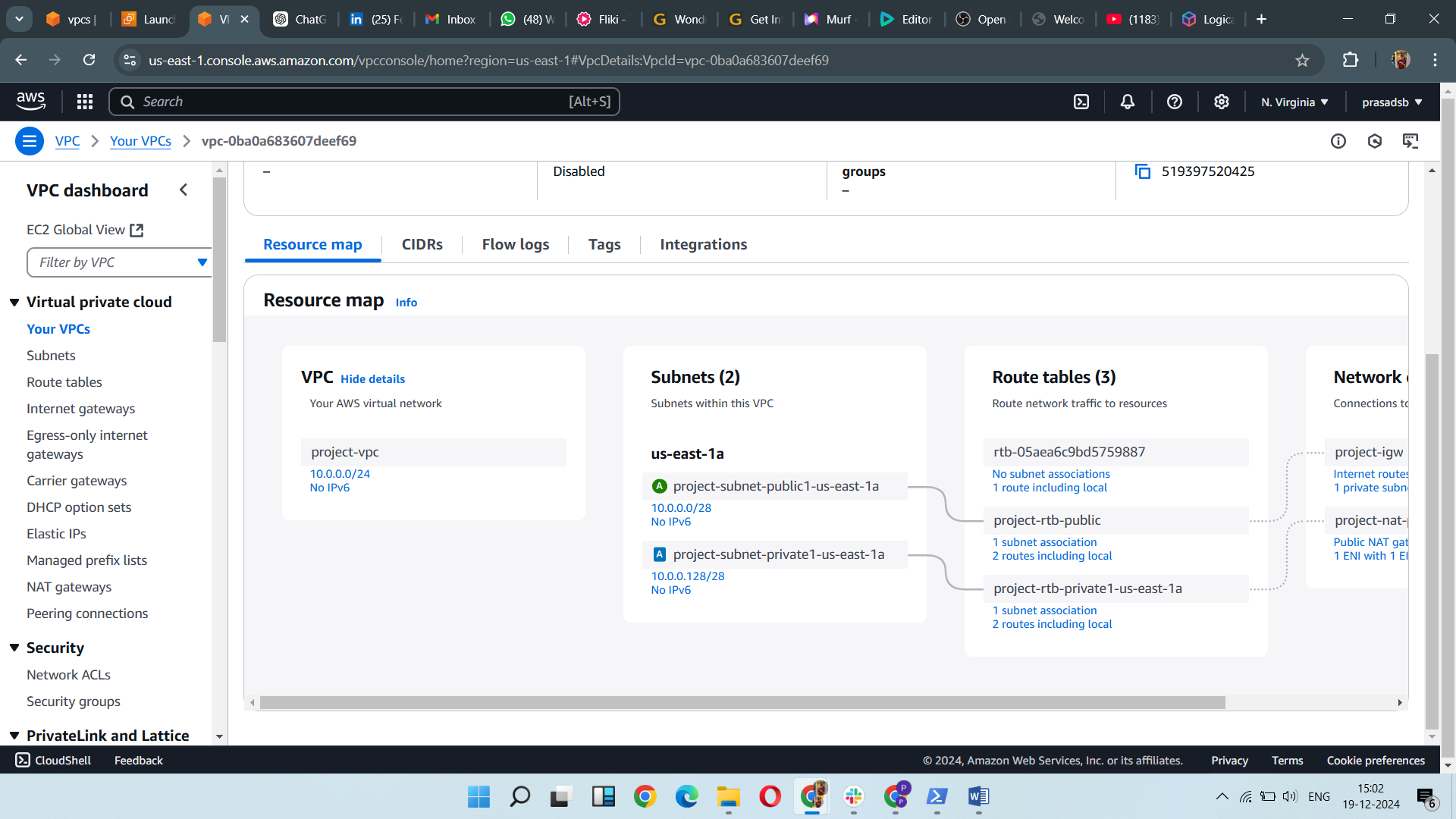
**Basic Networking Topology Implementation**

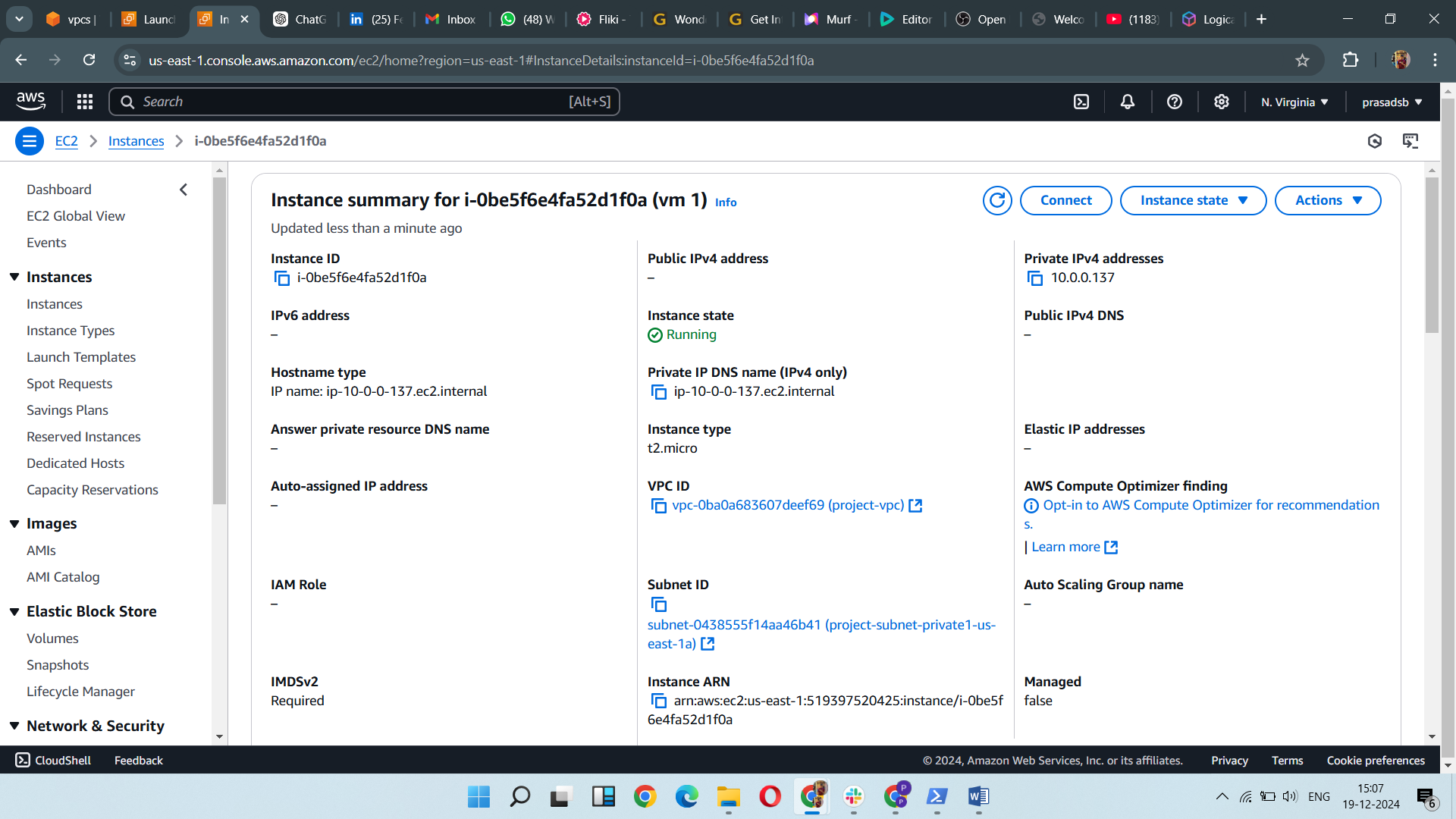
The goal of this task was to design and implement a basic networking topology with two Virtual Machines (VMs) in a cloud environment. One VM was configured as a web server, and the other as a client. SSH was used to securely transfer files between the two machines.

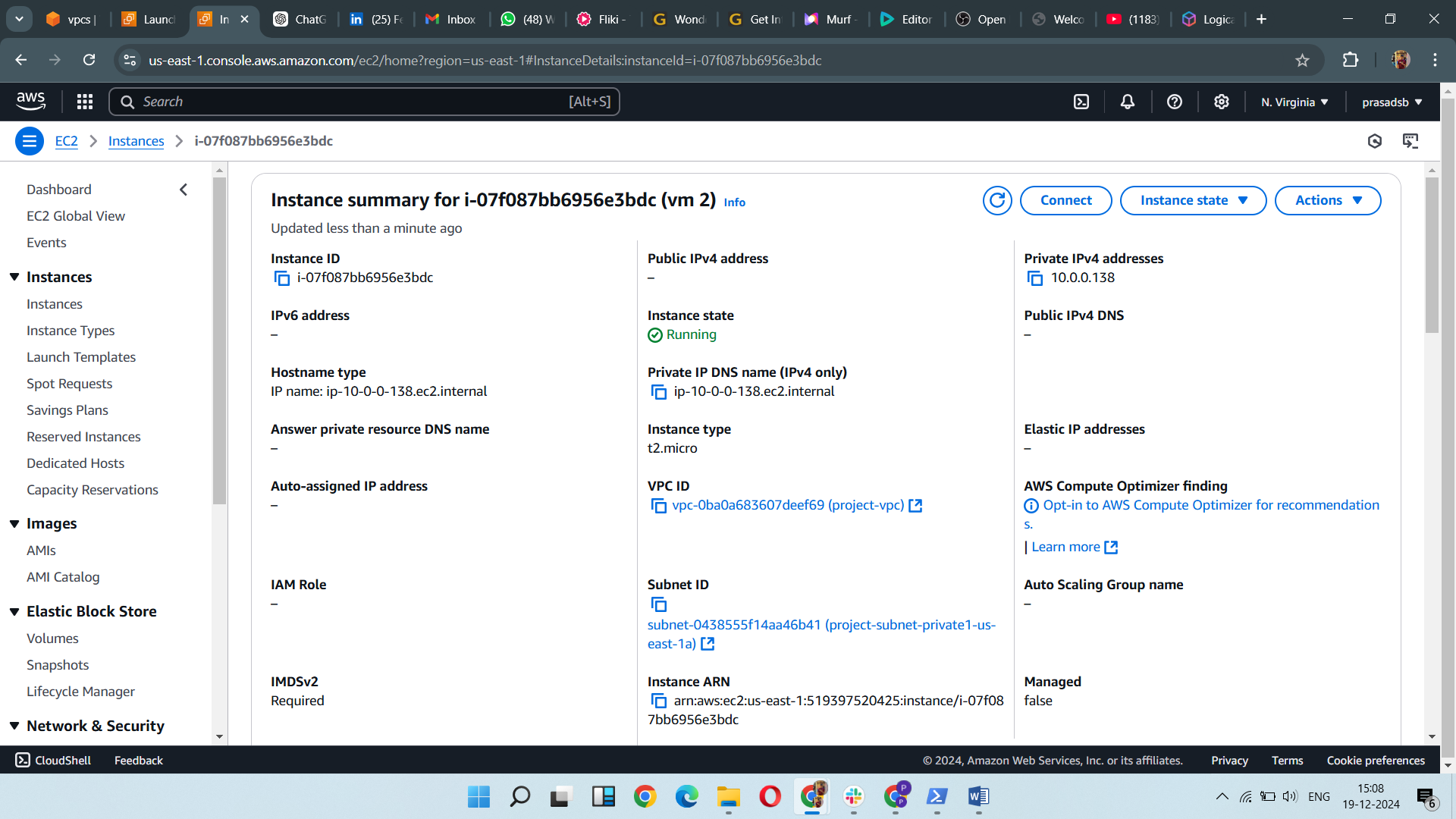
A Virtual Private Cloud (VPC) was created with one public subnet and one private subnet to ensure network isolation and secure communication between the instances.

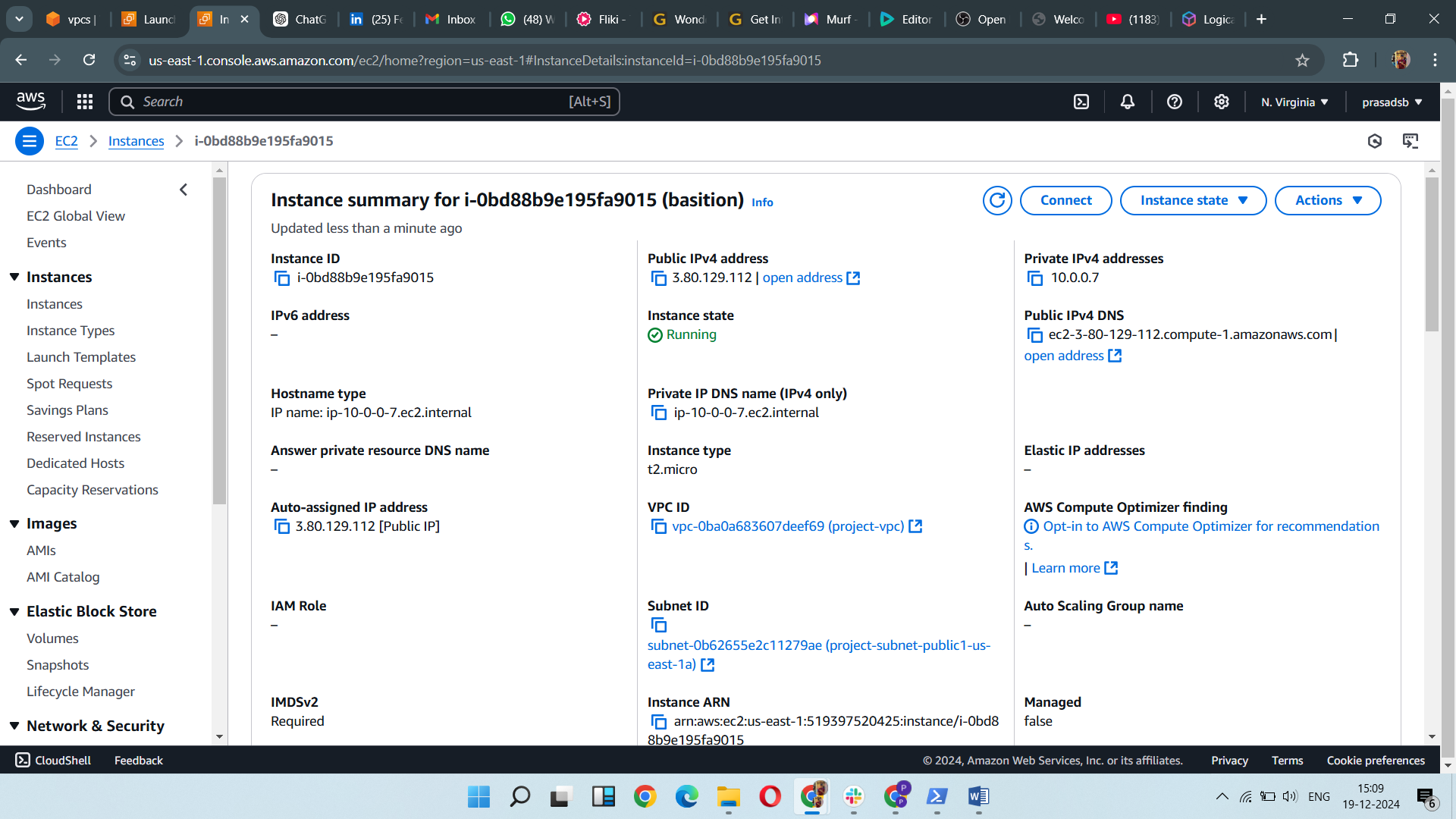


Three EC2 instances were created:

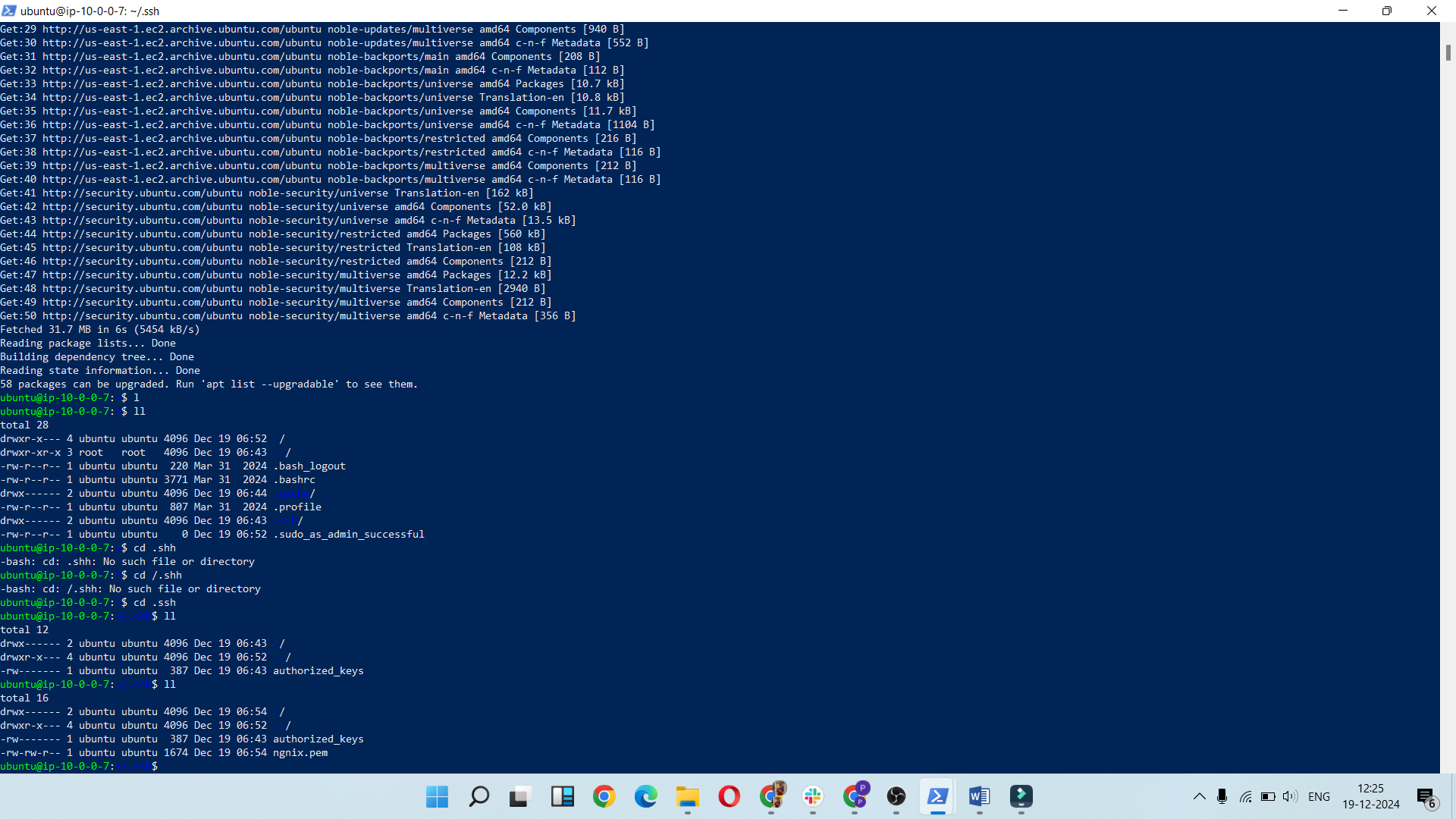
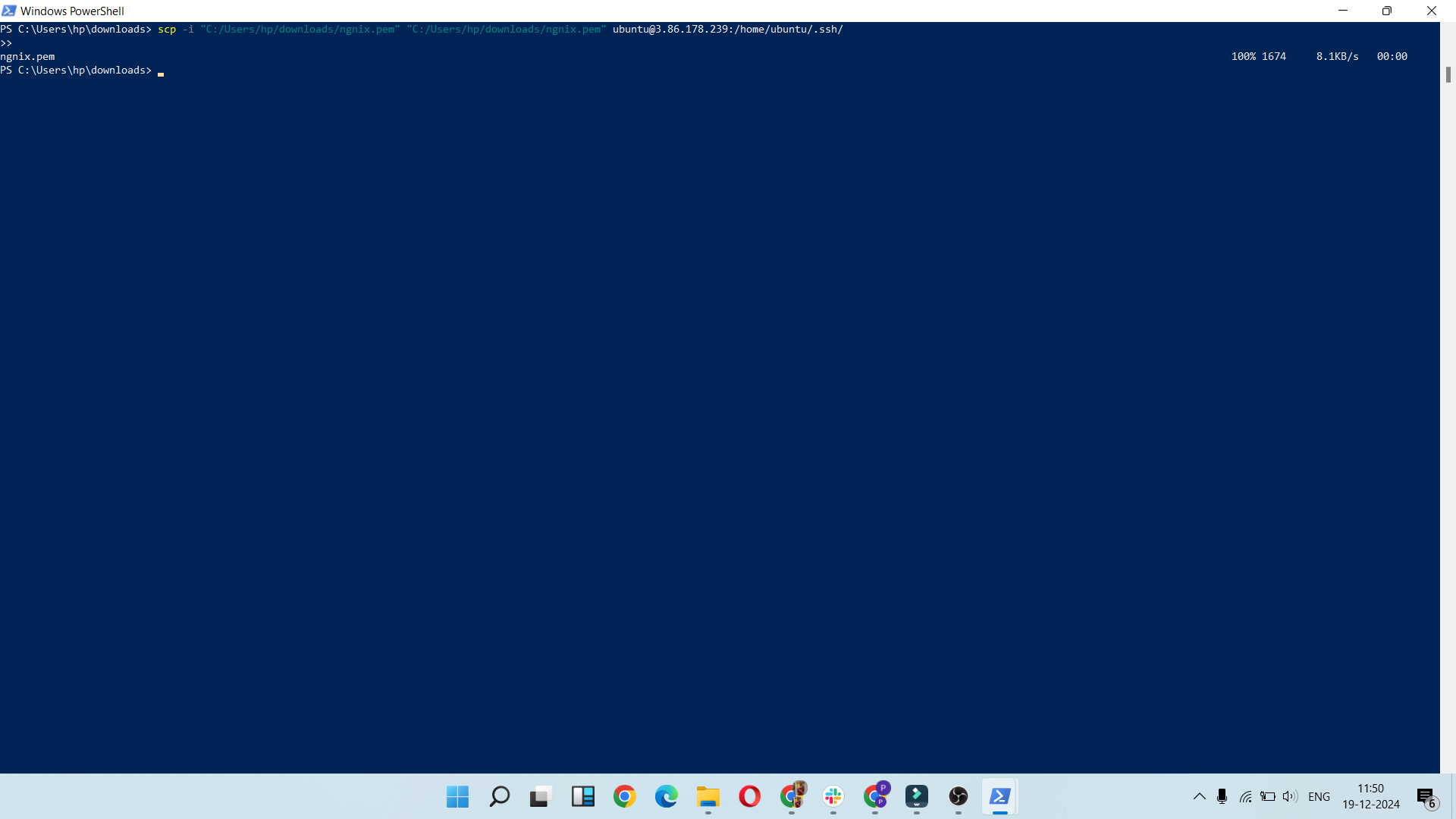
* **Bastion Host (Public IP)**: An EC2 instance was created in the public subnet, with a public IP for access.
* **Web Server (Private IP)**: An EC2 instance was created in the private subnet, configured as a web server.
* **Client (Private IP)**: Another EC2 instance was created in the private subnet, configured as the client.

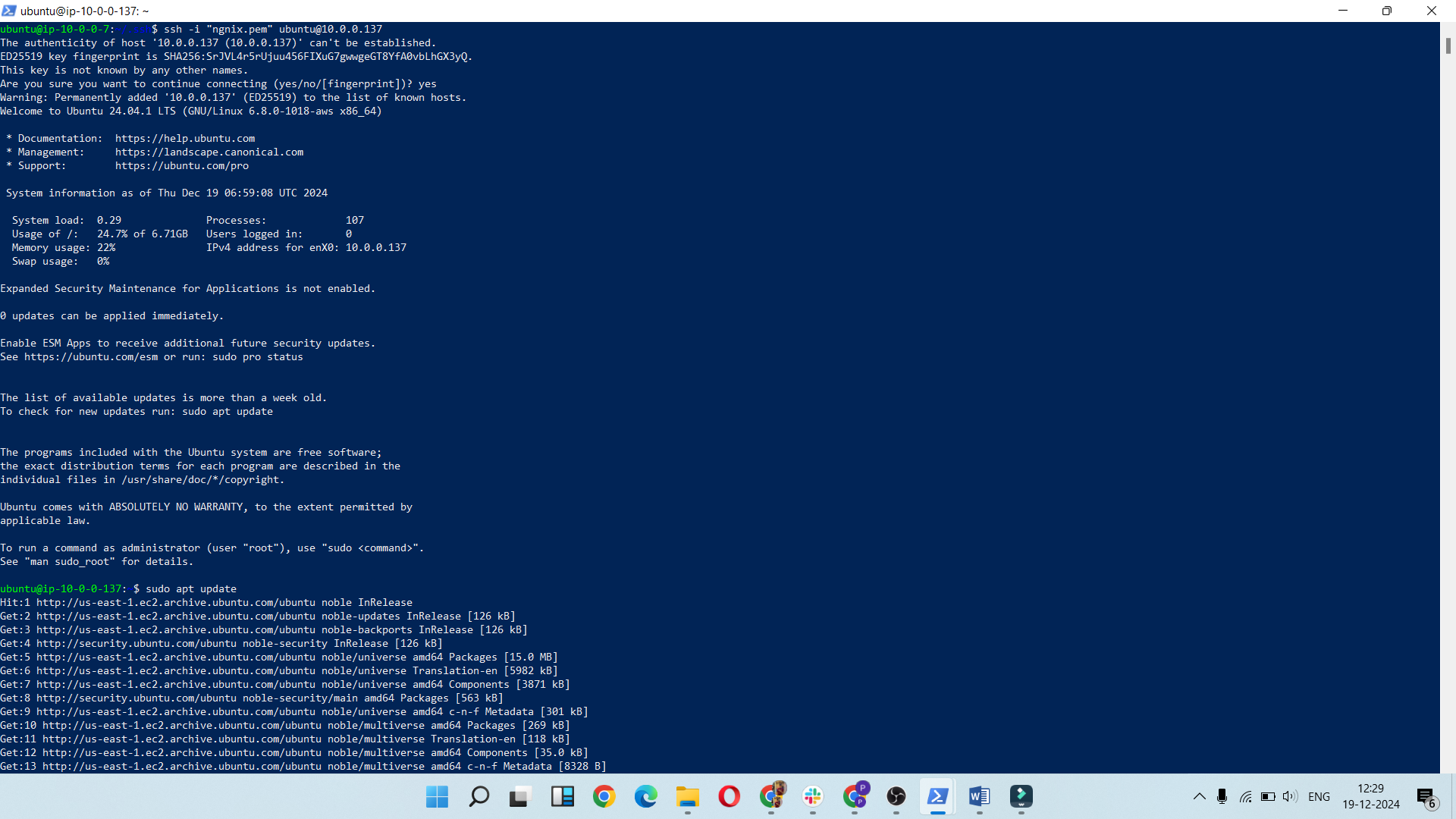




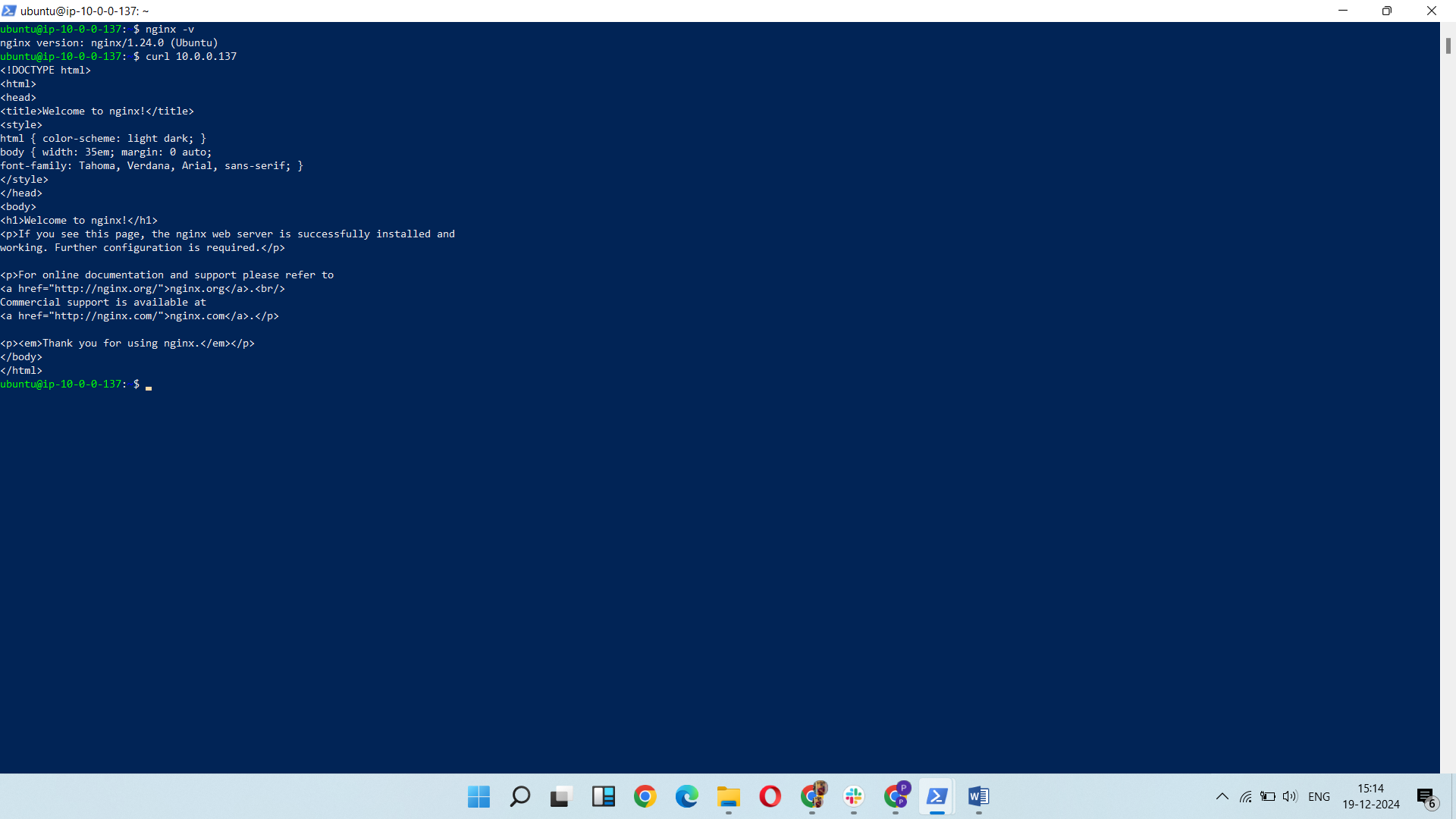


* SSH keys were securely transferred from the local machine to the bastion host using SCP.
* The bastion host was then used as an intermediary to access the private instances (web server and client), bypassing the lack of public IPs on those machines.

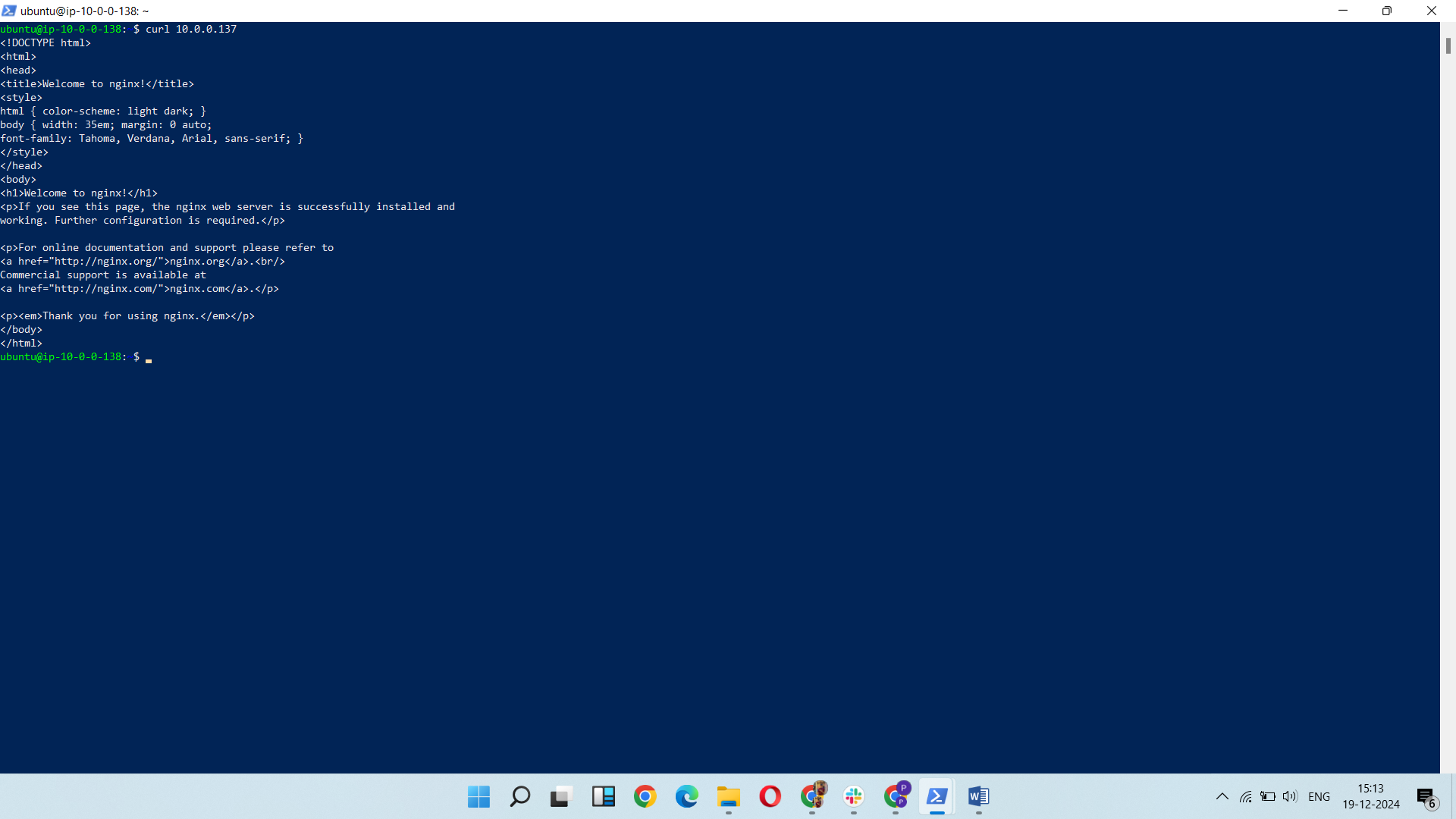




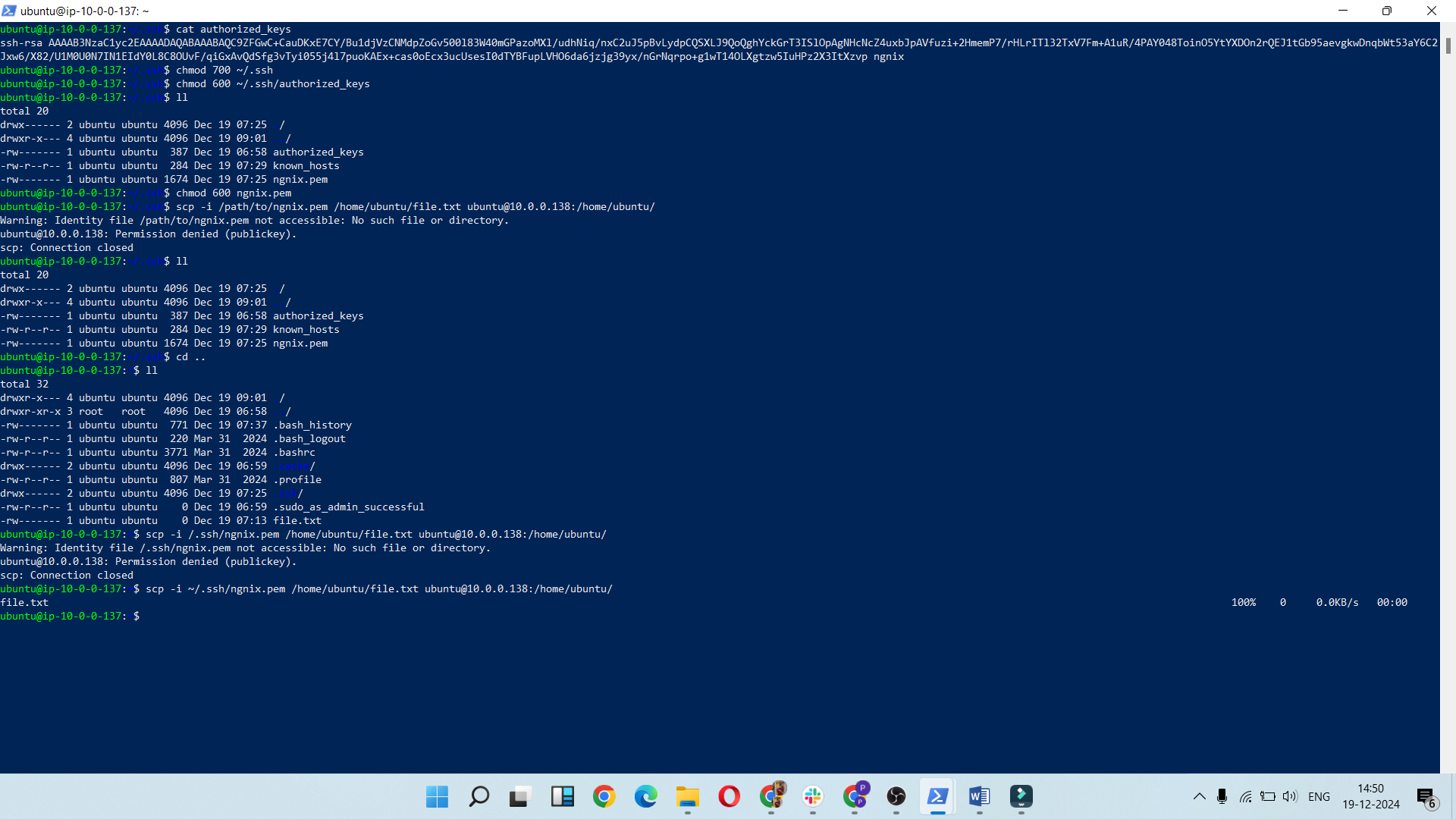
* Nginx was installed on the web server, and the appropriate firewall rules (HTTP/80) were added to the security group, enabling the client to access the web page hosted on the server.

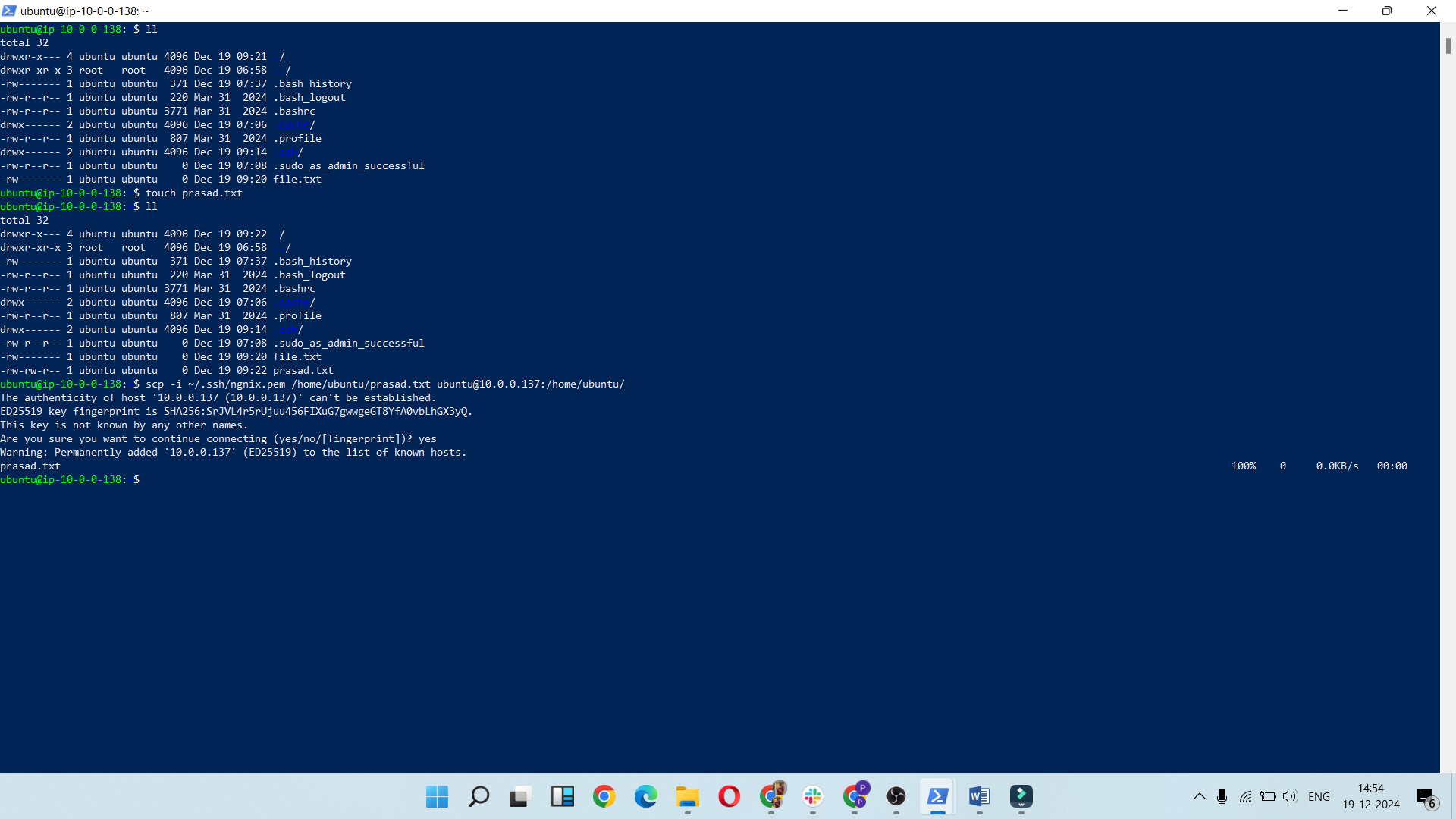


* This is the client virtual machine.



* The file transfer process was carried out using SCP, both from the client to the server and vice versa. This demonstrated the use of secure file transfer over SSH.





Basic Architecture

