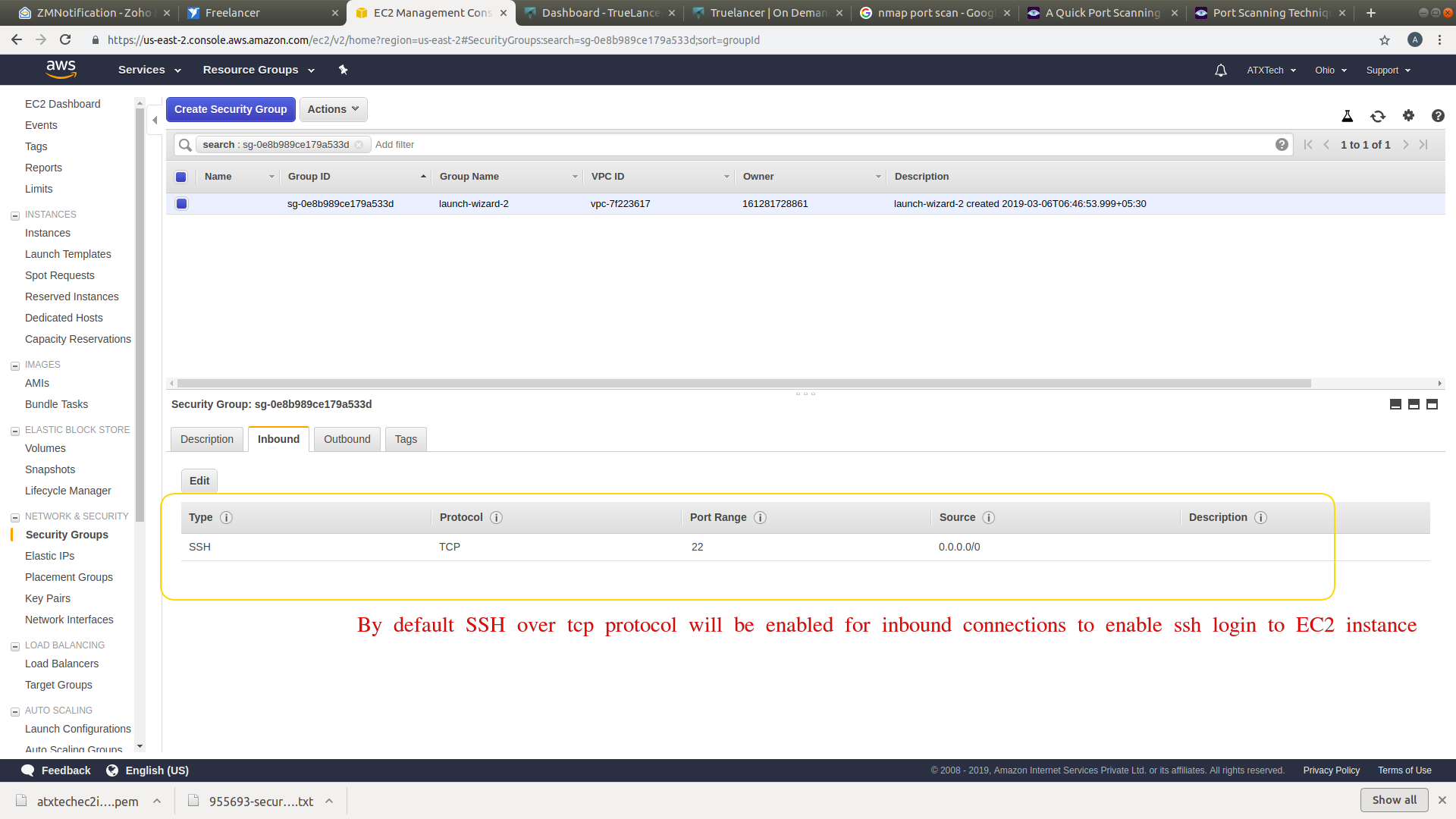
# Security Group configuration with AWS EC2 instanace

This is a guide to setup security group settings in Amazon EC2 instance and verify the security in EC2 instance with ‘nmap’ tool.

### 1. Default Security Group settings in EC2 instance

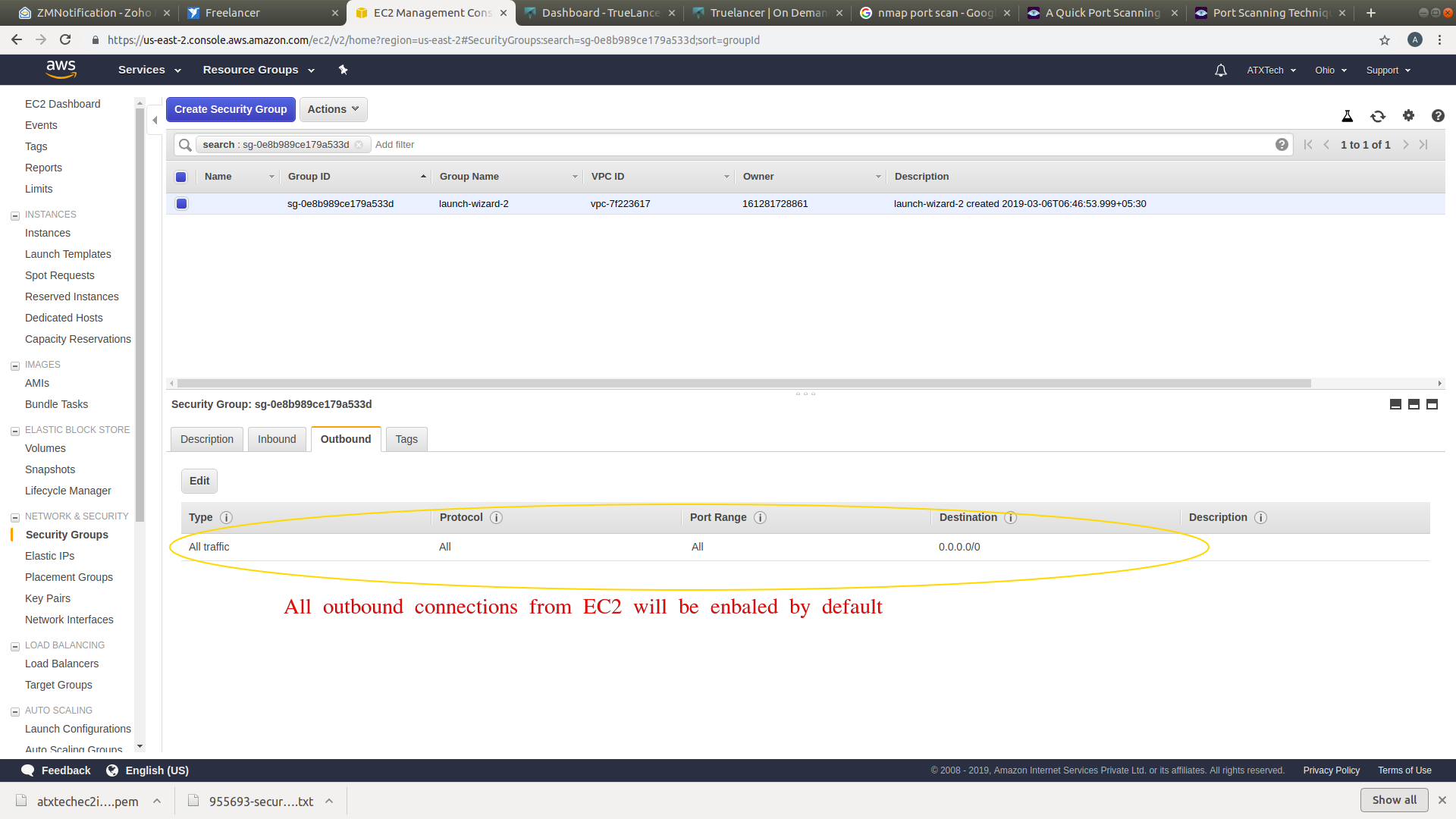
When we create a new instance in EC2, the default service enbaled is ‘ssh’ at port 22 to enabled ssh remote login to EC2 instance.

Default inbound rule:



In outbound rule ‘All traffic’ communication will be enabled. Means any network communication from EC2 instance to outside network is enabled. Since it is outbound connection from EC2 instance, no security issues.

Default outbound rule:



### 2. Check the ports/services present in EC2 instance using ‘nmap’ tool

nmap is a network exploration tool and security scanner in Linux. Using this too we can analyse and verify the network connects in EC2 instance from our local system.

Install ‘nmap’ in our local system using ‘apt’

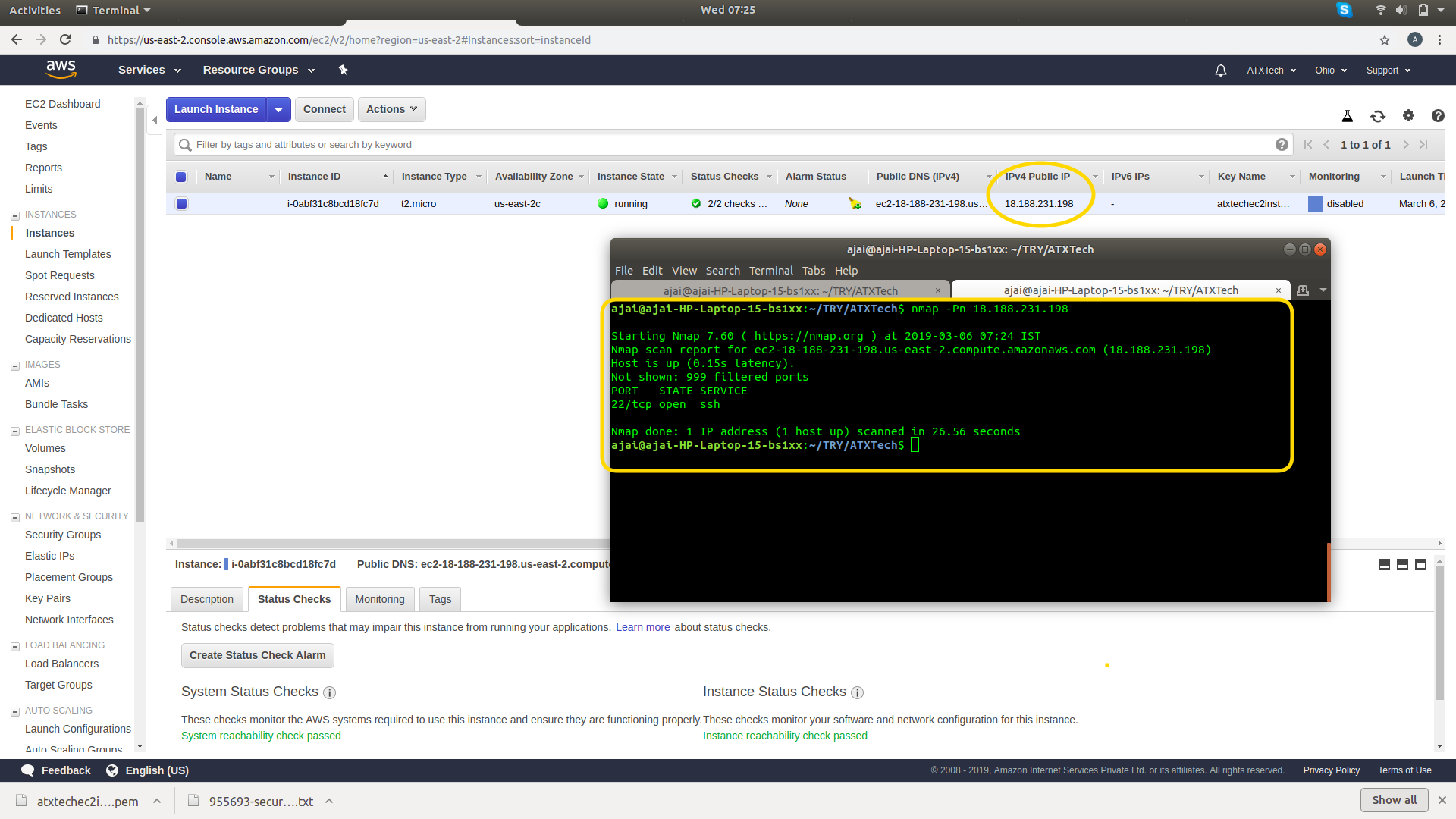
$ sudo apt install nmap

To know the open ports and service in EC2, start nmap port scan using below command from our local machine.

$ nmap -Pn <IP address of EC2 instance>

Here we can see the ‘ssh’ service in port 22 is enbaled over TCP protocol. The state is also ‘open’ since ssh deamon service(sshd) is already running in EC2 instance by default.

Nmap scan result:



### 2. For example: Enable custom port 8888

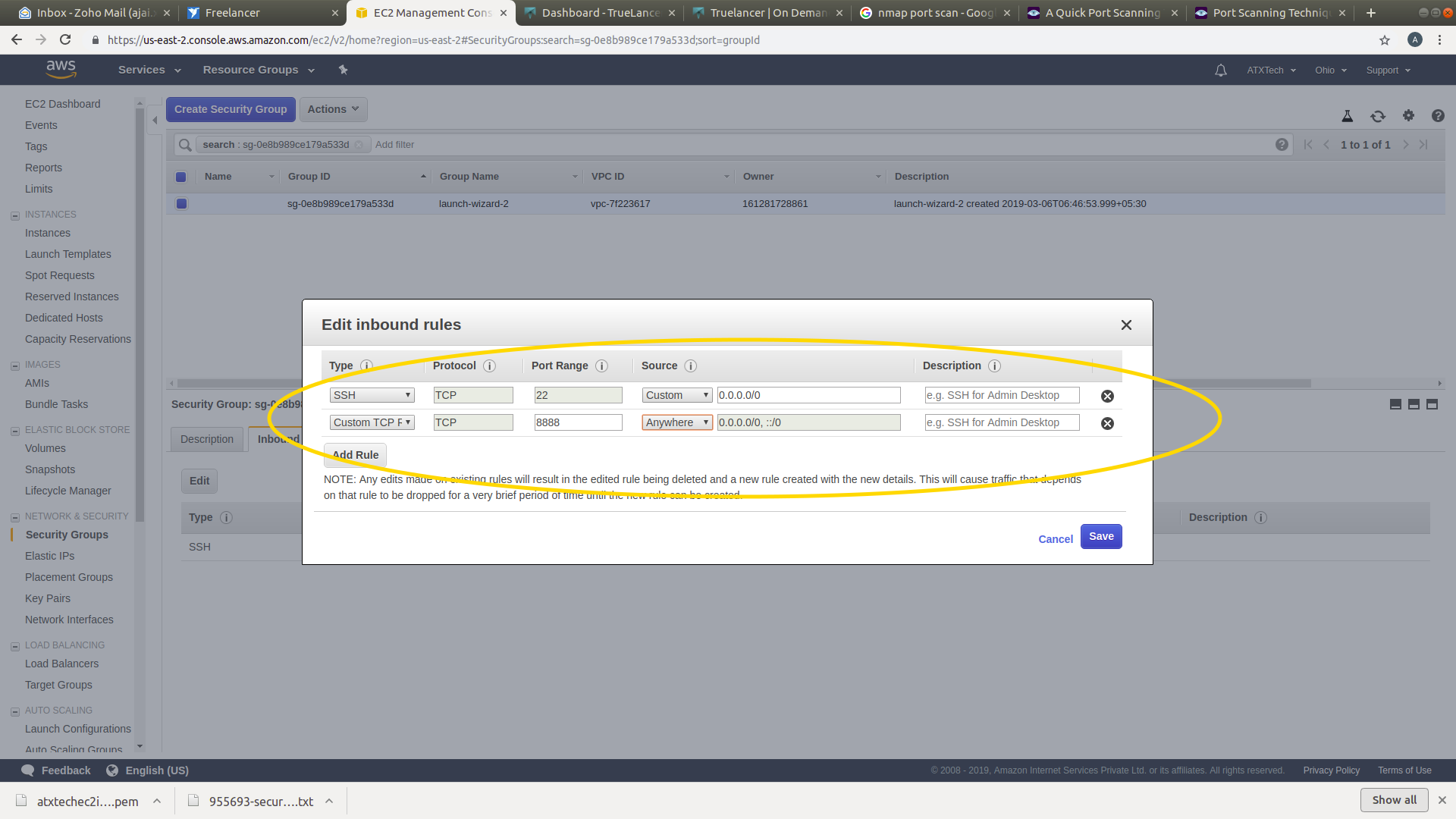
Now we can enable port 8888 over TCP protocol. See the inbound rule creation in below screenhsot.

Type: Custom TCP

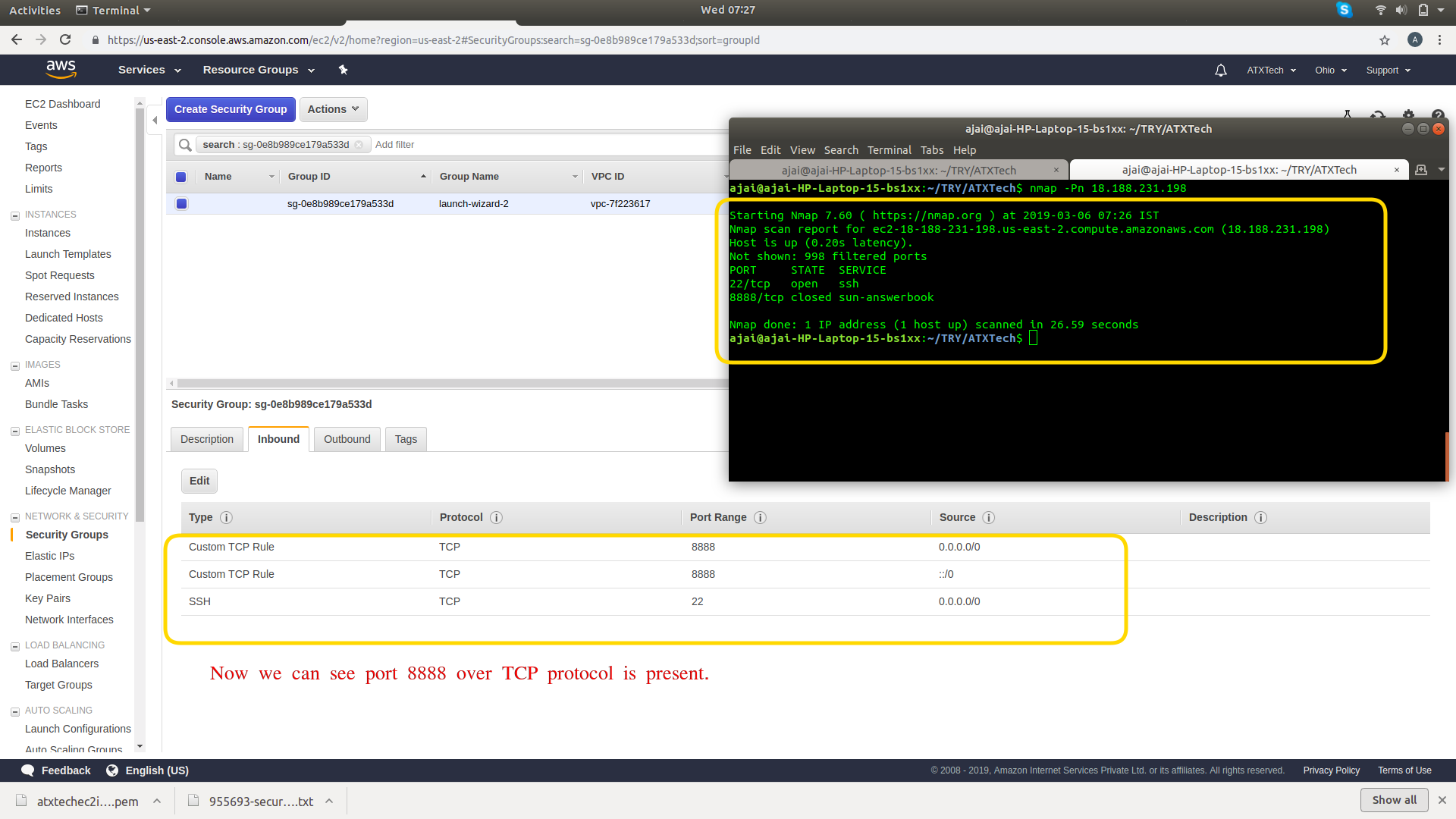
Protocol: TCP

Port: 8888

Source: Anywhere (Instead of this, also we can give our machine ip for more security)

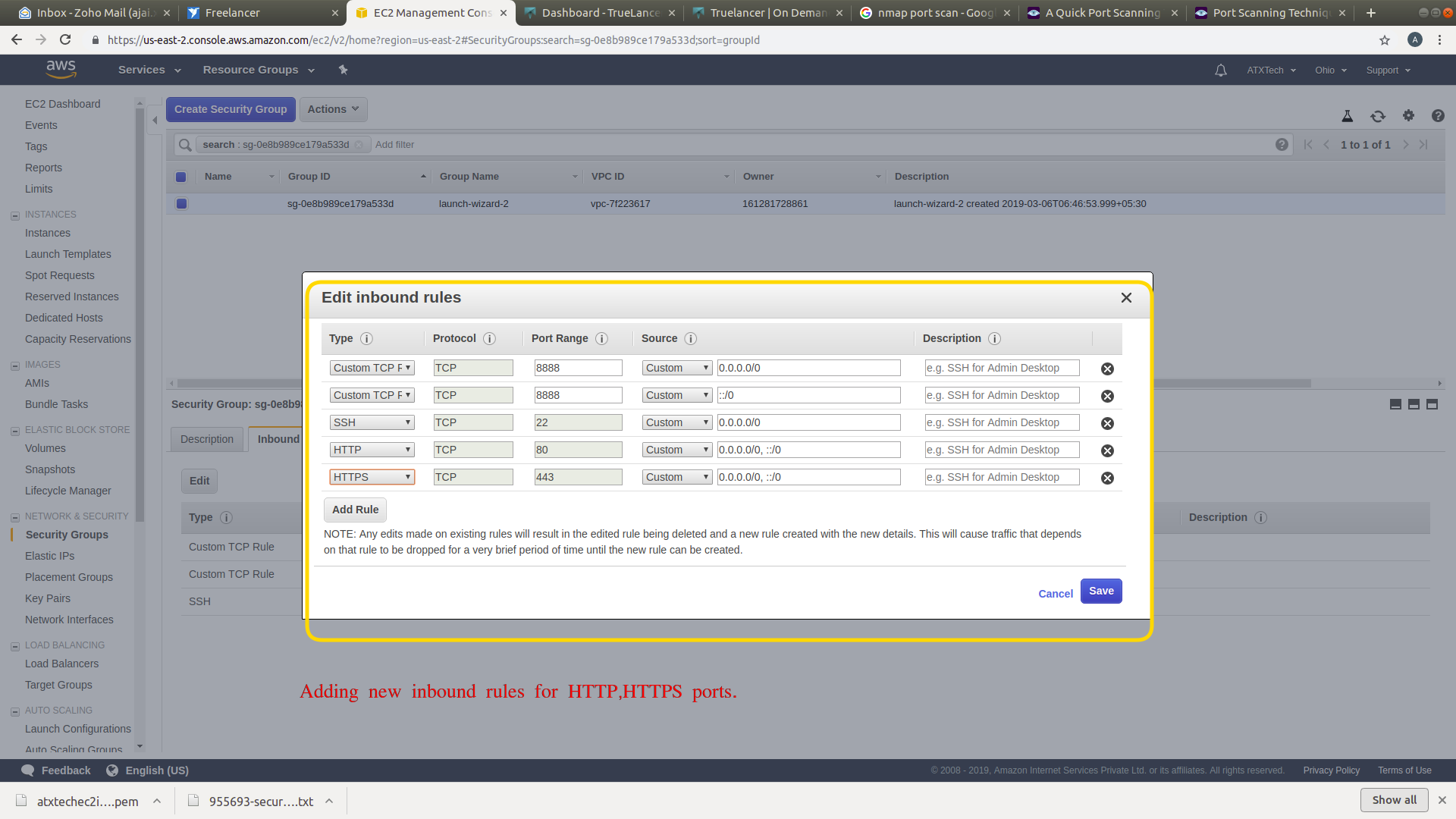


Now run ‘nmap’ port scan and it should list port 8888/tcp in the list as below. That means port 8888 over TCP port is enabled. But we can see the state is ‘closed’ becuase there is no service/application is using/running with port 8888 inside EC2 instance.

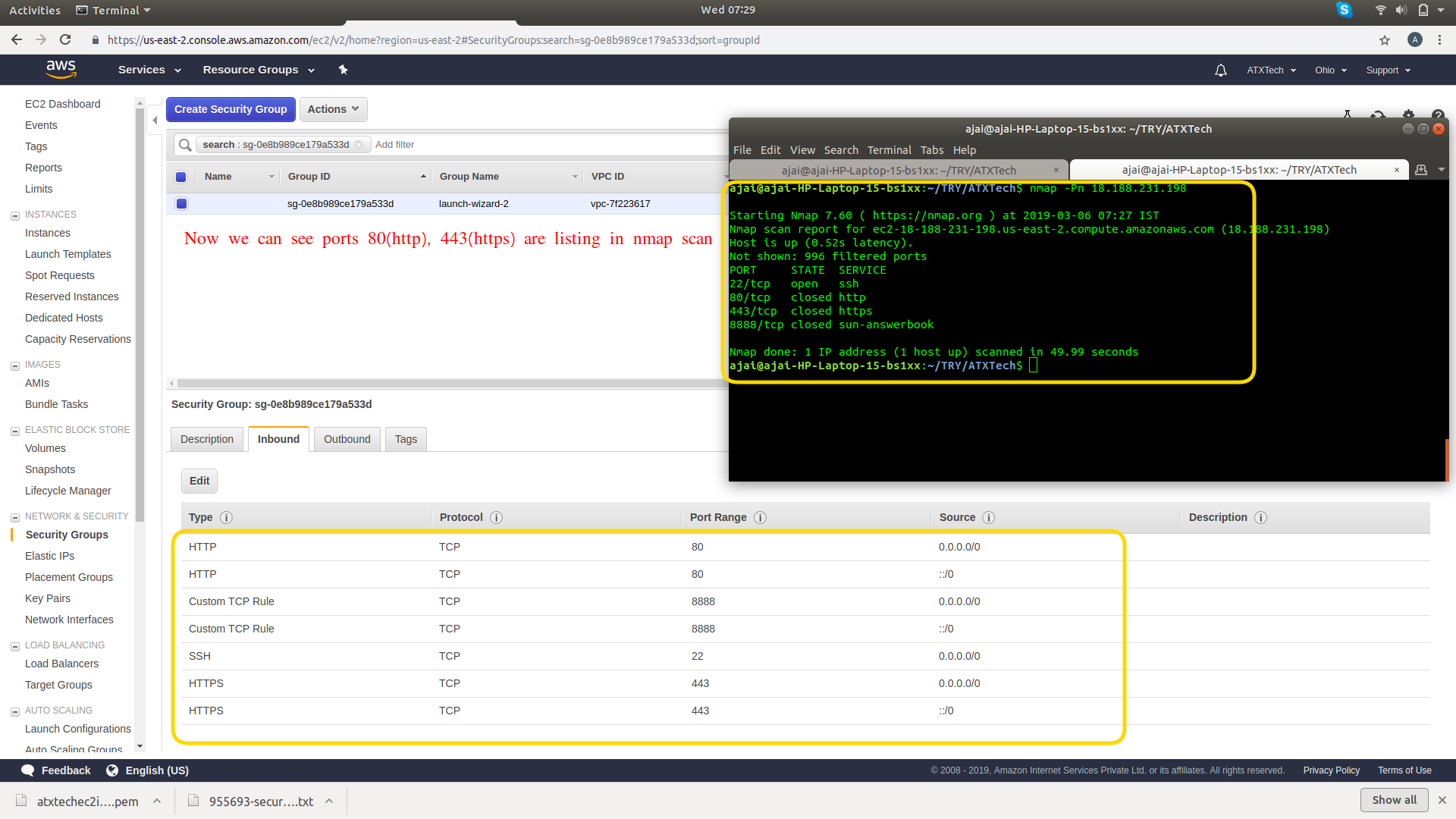


### 3. Enabling HTTP and HTTPS connections

To enable webserver or HTTP,HTTPS connecions in EC2, add inbound rules like below.



Now run ‘nmap’ port scan and it should list port 80/tcp, 443/tcp in the list as below. That means port 80 over TCP for HTTP and port 443 over TCP for HTTPS is enabled. But we can see the state is ‘closed’ becuase there is no service/application is using/running with port 80,443 inside EC2 instance.

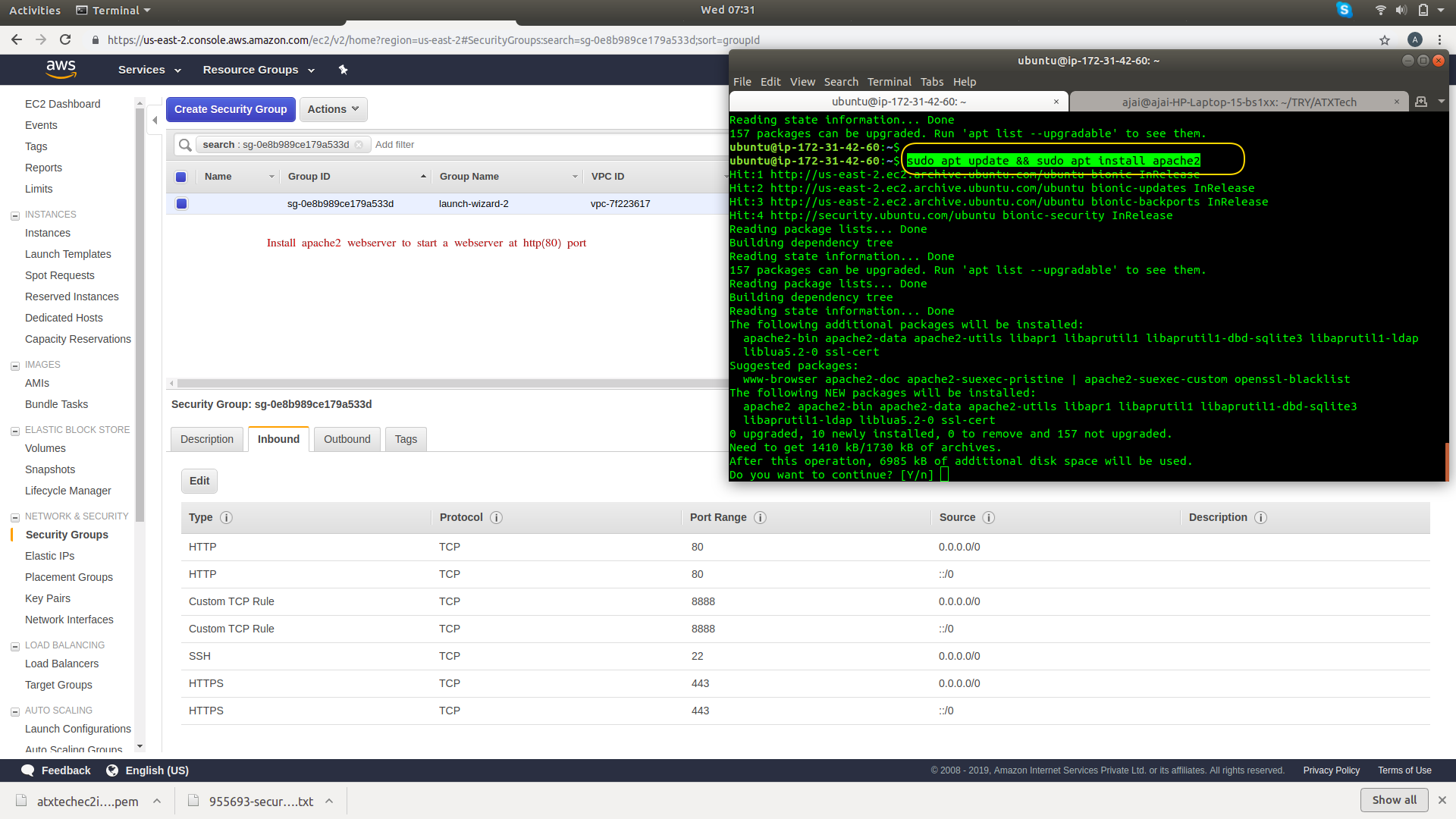


### 4. Enabling webserver at port 80/tcp over HTTP

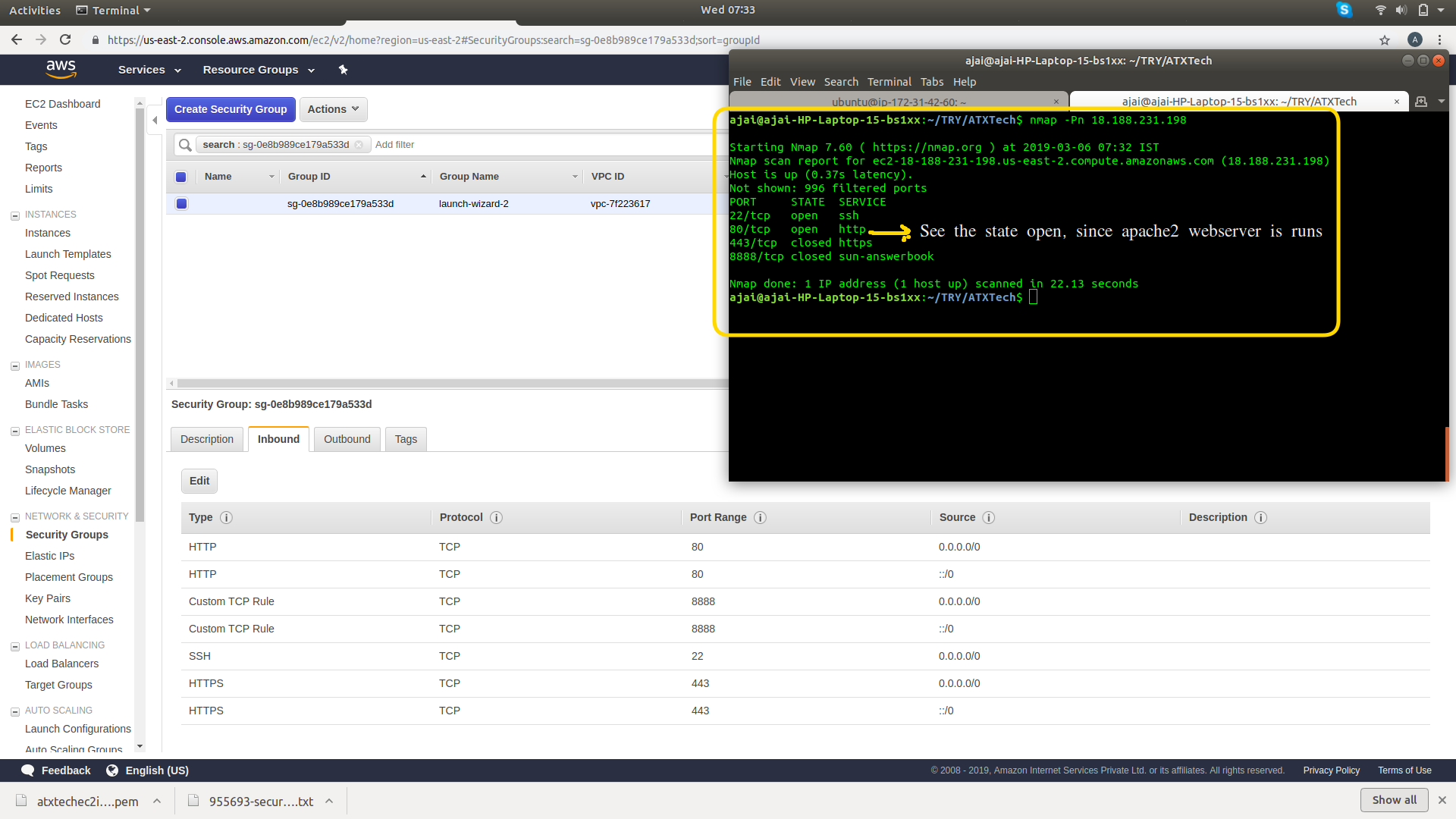
If we install a webserver application like apache2, we can see that service will be using port 80/tcp over HTTP.

Install apache2 using apt in ec2 instance.

$ sudo apt install apache2



Now if we scan using nmap, we can see the port 80/tcp state is open because the apache2 webserver service is using port 80/tcp and waiting for incoming connections.



Now if we open the EC2 instance’s IP address in web browser, we can see the default HTML page like below.

