Jon Franck

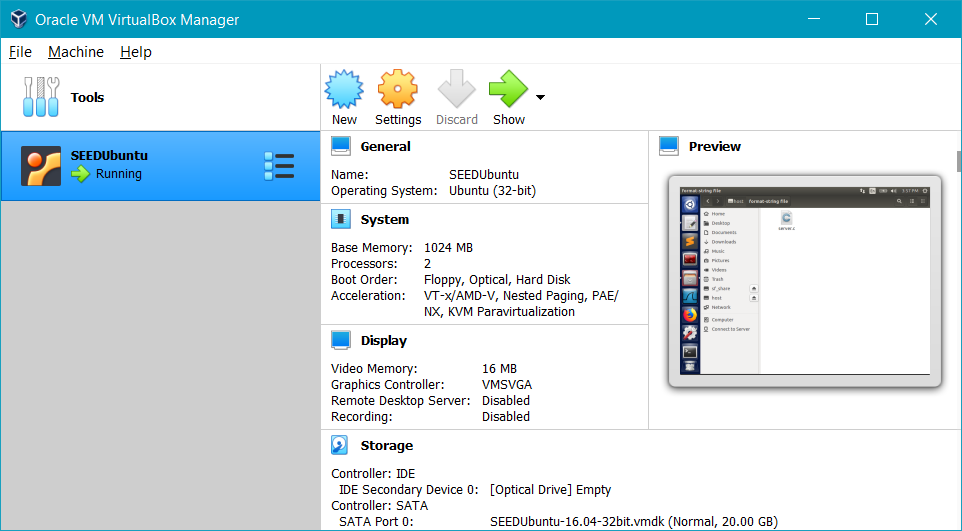
2/13/2021

CSC 4413

# Firewall EvasionLab

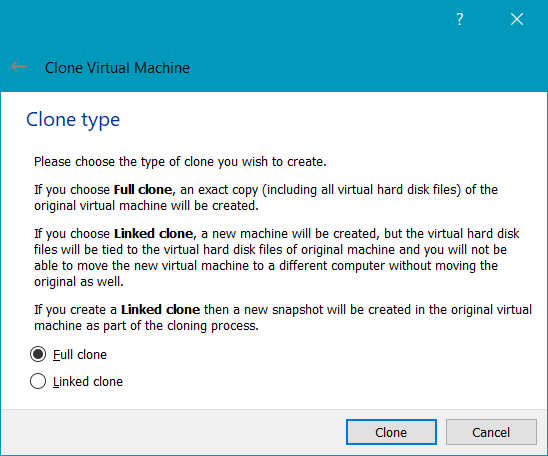
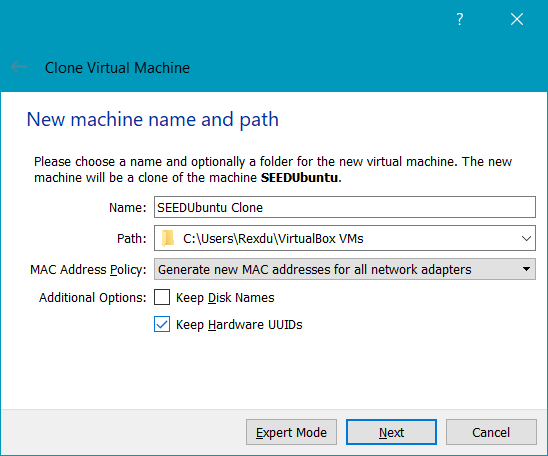
**Objective:** Learn how aVPN works in action and how VPN can help bypass egress firewalls.

## Step 1: Configure the Virtual Image



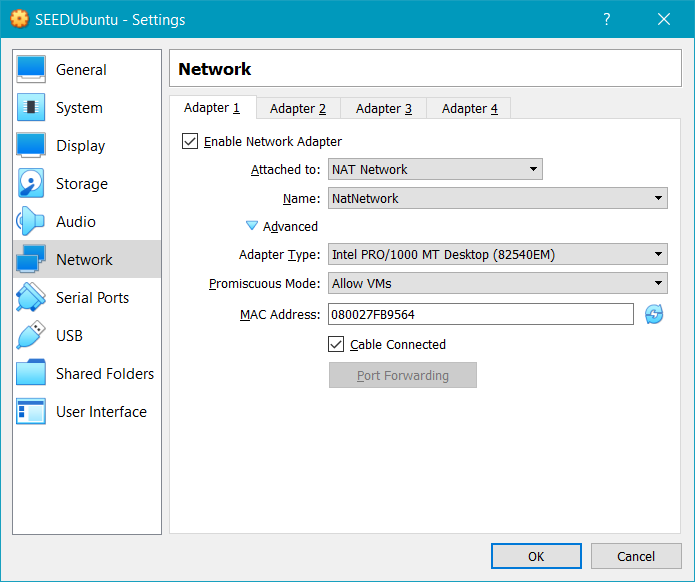
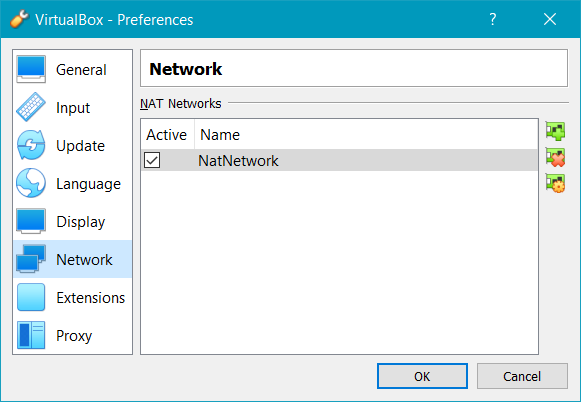
SEEDUbuntu downloaded from <https://seedsecuritylabs.org/lab_env.html>

### Create a Clone



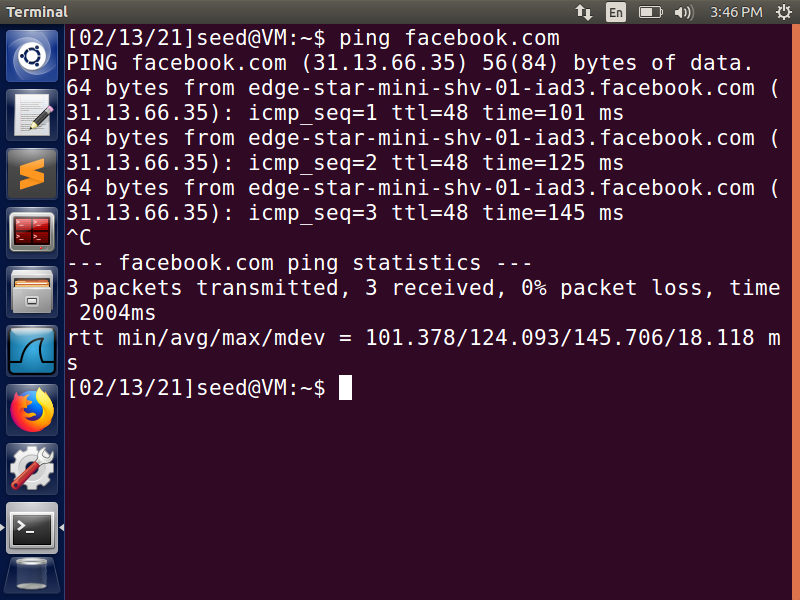
Clone the virtual machine in order to be able to run two at the same time.

### Network Configuration

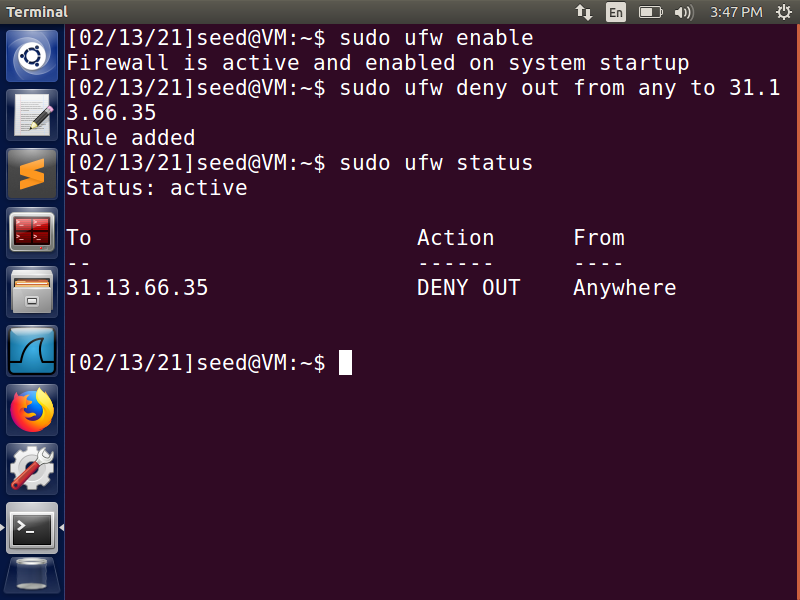


Create a new NatNetwork Adapter and enable it for both VM (make sure all other network adapters are disabled). Set the Promiscuous Mode to Allow VMs.

## Step 2: Configure the Firewall



Ping a website you wish to block to make sure you can access it to begin with.



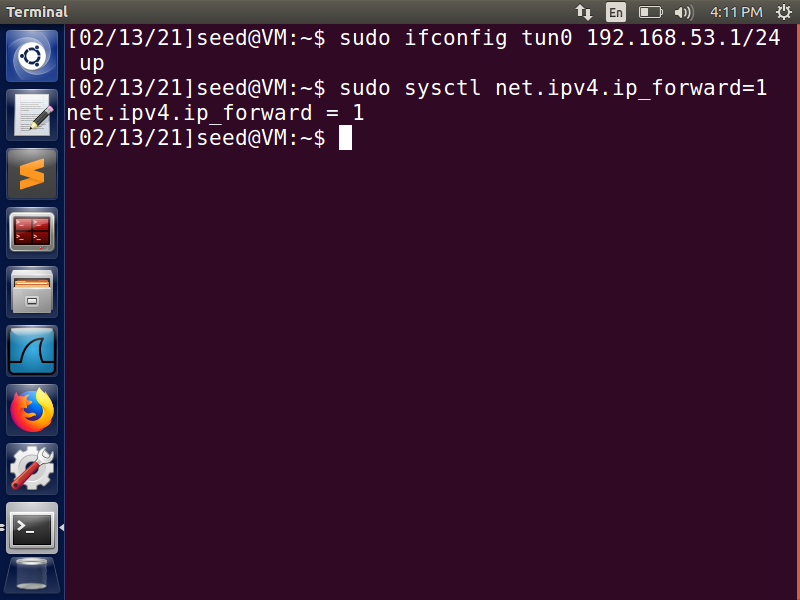
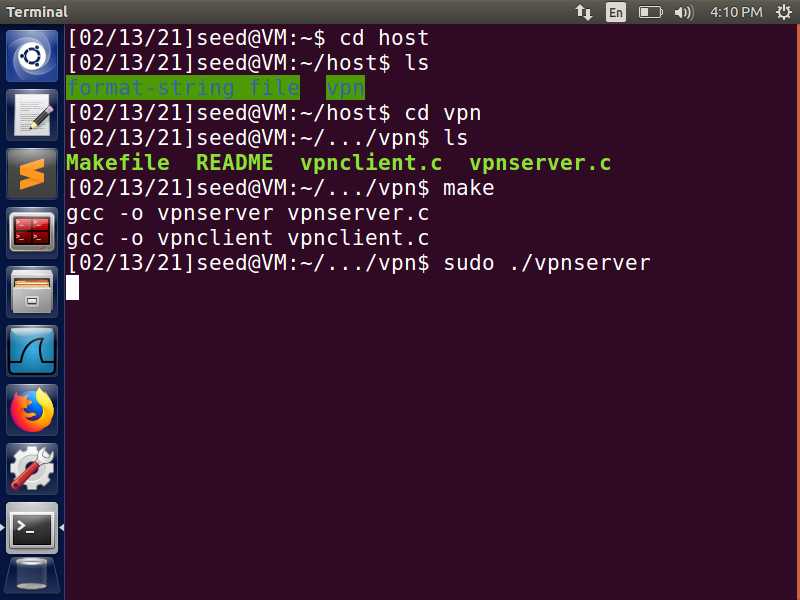
Enable the firewall with sudo privileges and add a rule blocking access to the previous website.



When you ping the website again it should tell you that it is not allowed.

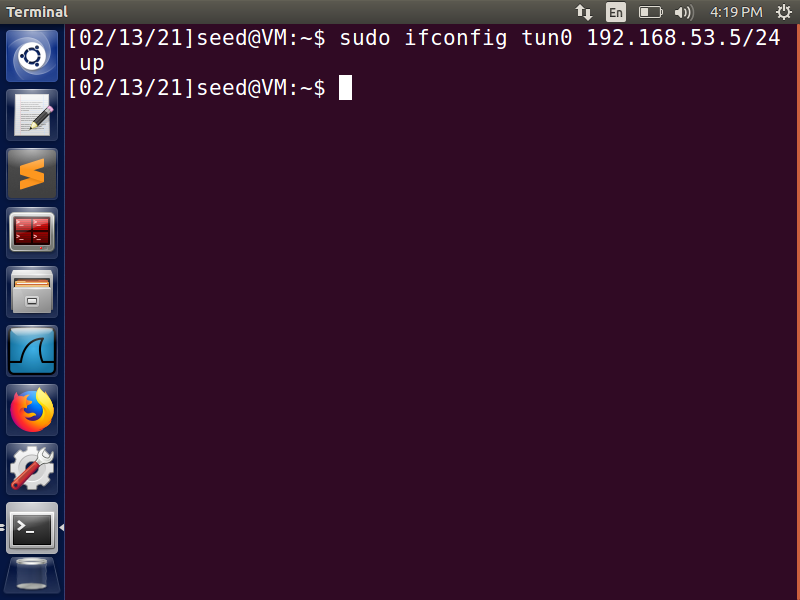
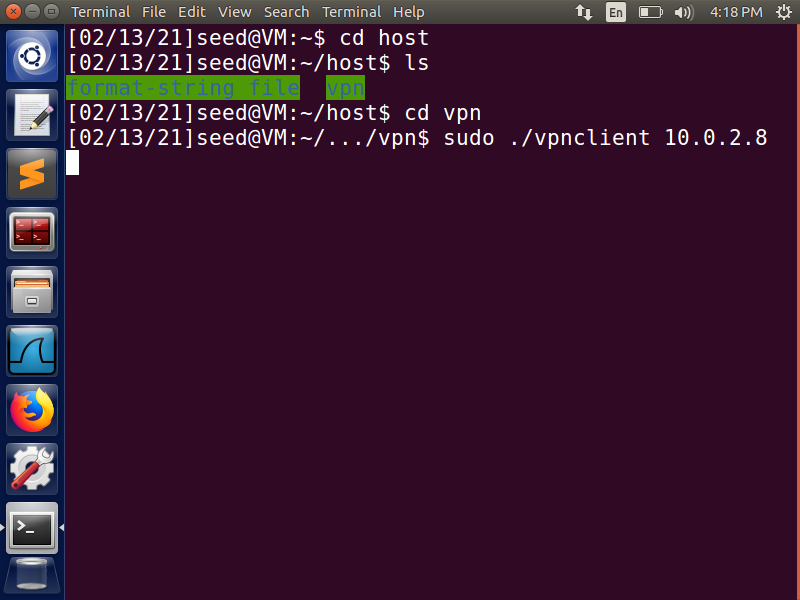
## Step 3: Setup the VPN

**Task 1 – Run the VPN Server**



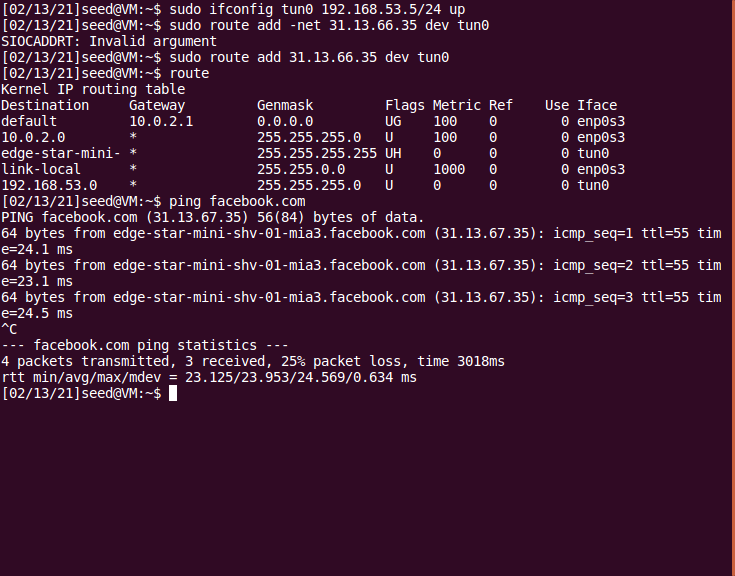
Compile the vpnserver and vpnclient programs and run the vpnserver on the first VM. Then in another terminal assign an IP address to the tunnel interface and activate it; then enable IP forwarding on the VM so that it can act as a gateway.

**Task 2 – Run the VPN Client**



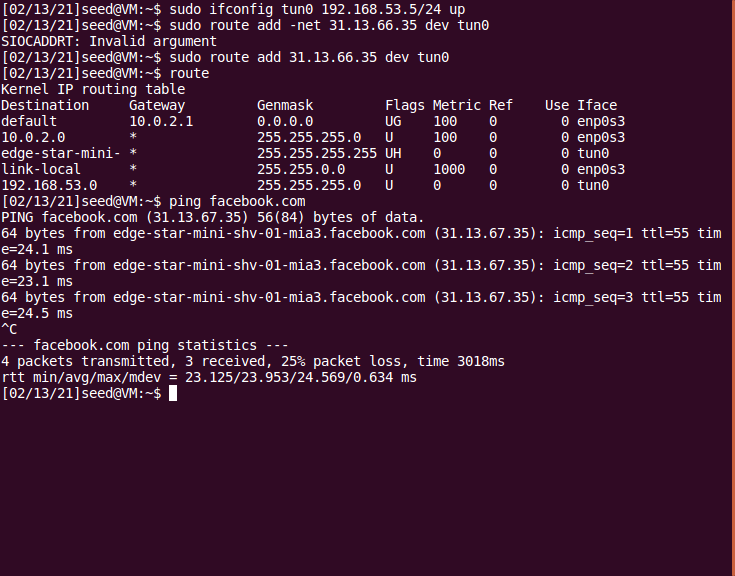
On the second VM run the vpnclient program and in another terminal assign an IP address to the tunnel interface.

**Task 3 – Setup Routing**

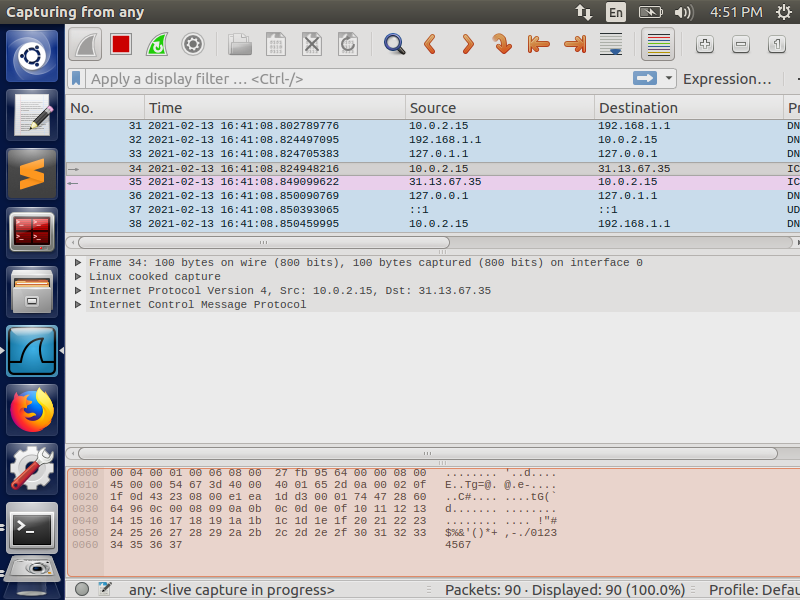


By using the route command, we can send all packages going to 31.13.66.35 (Facebook.com) to the VPN tunnel (tun0).

## Step 4: Bypass the Firewall



Here we can see that the ping to facebook.com was successful and no longer denied.



Using Wireshark, we can verify that the ping was sent through the VPN tunnel (192.168.1.1) to the Server VM (10.0.2.15) , then to facebook.com (31.13.67.35), and all the way back through the tunnel.