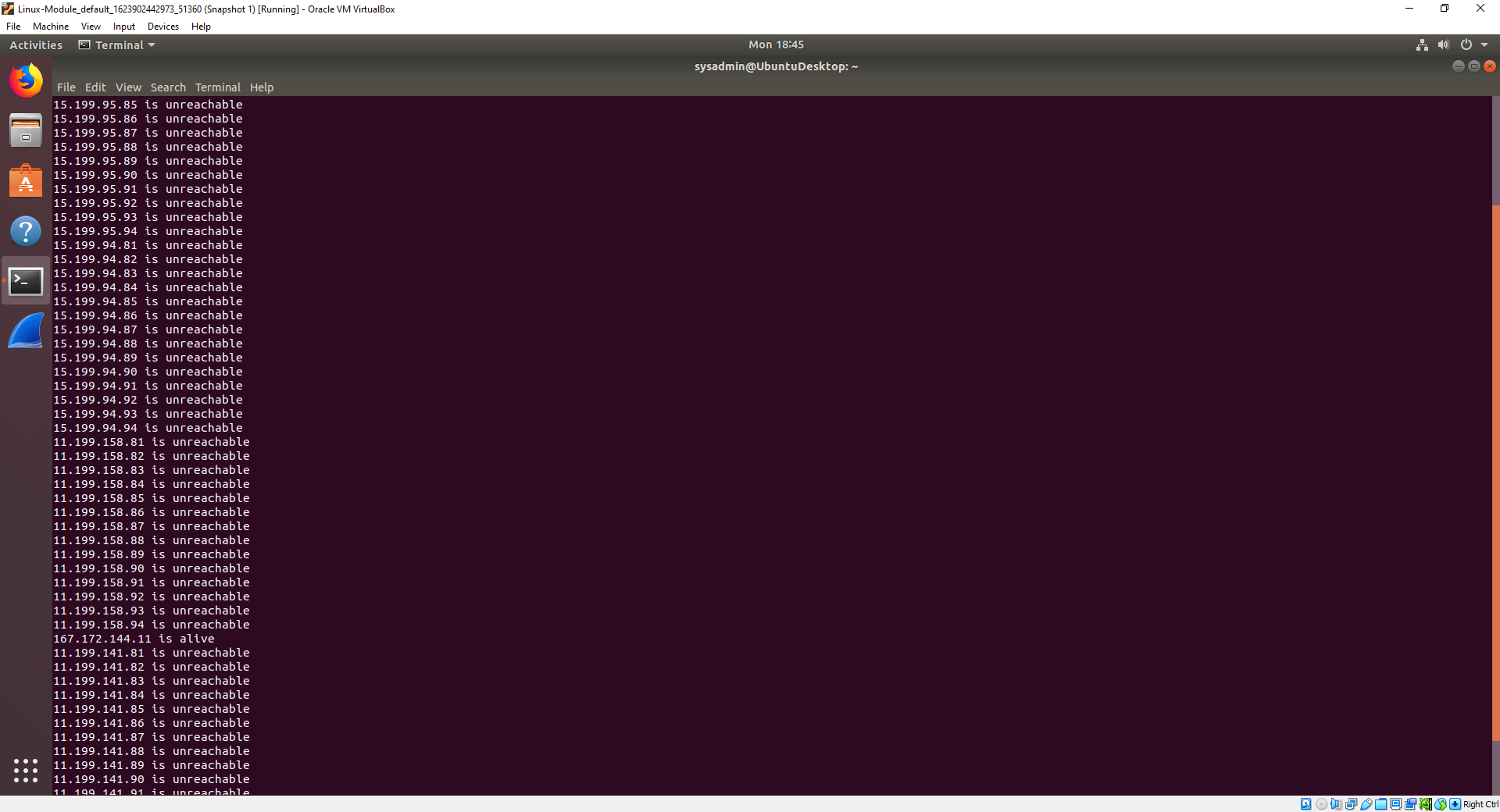
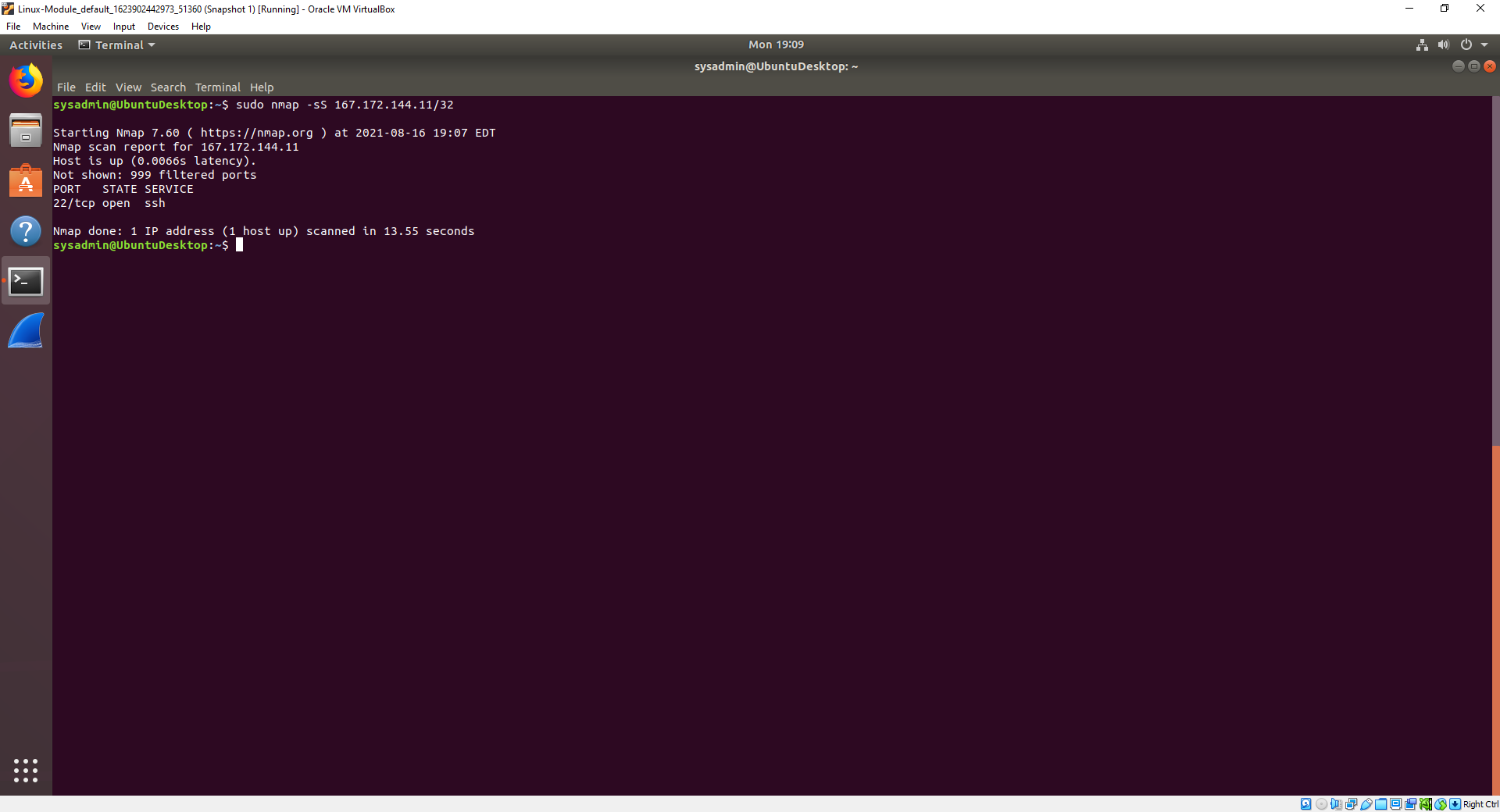
Step 1





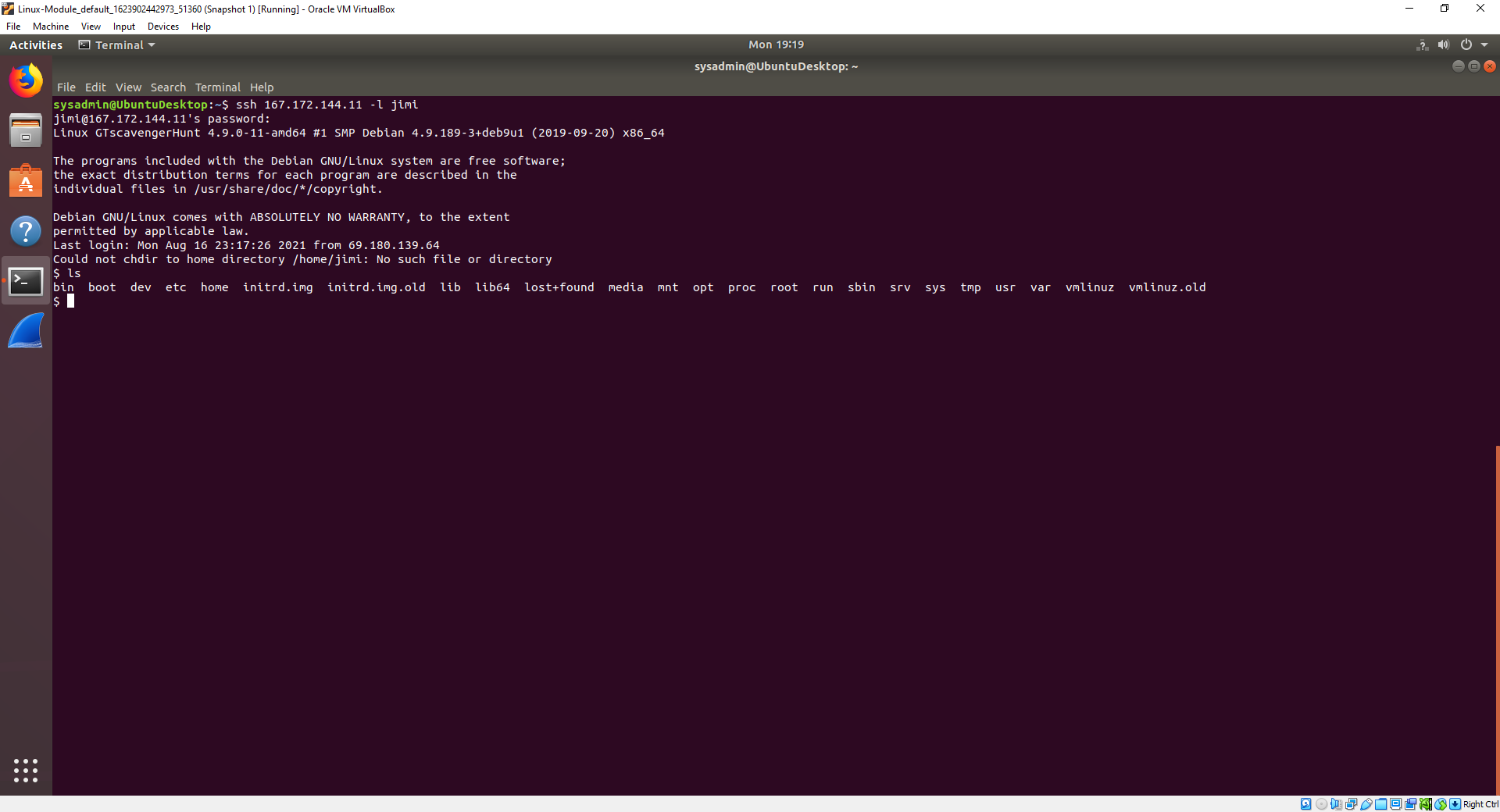
* Level 3: Network.

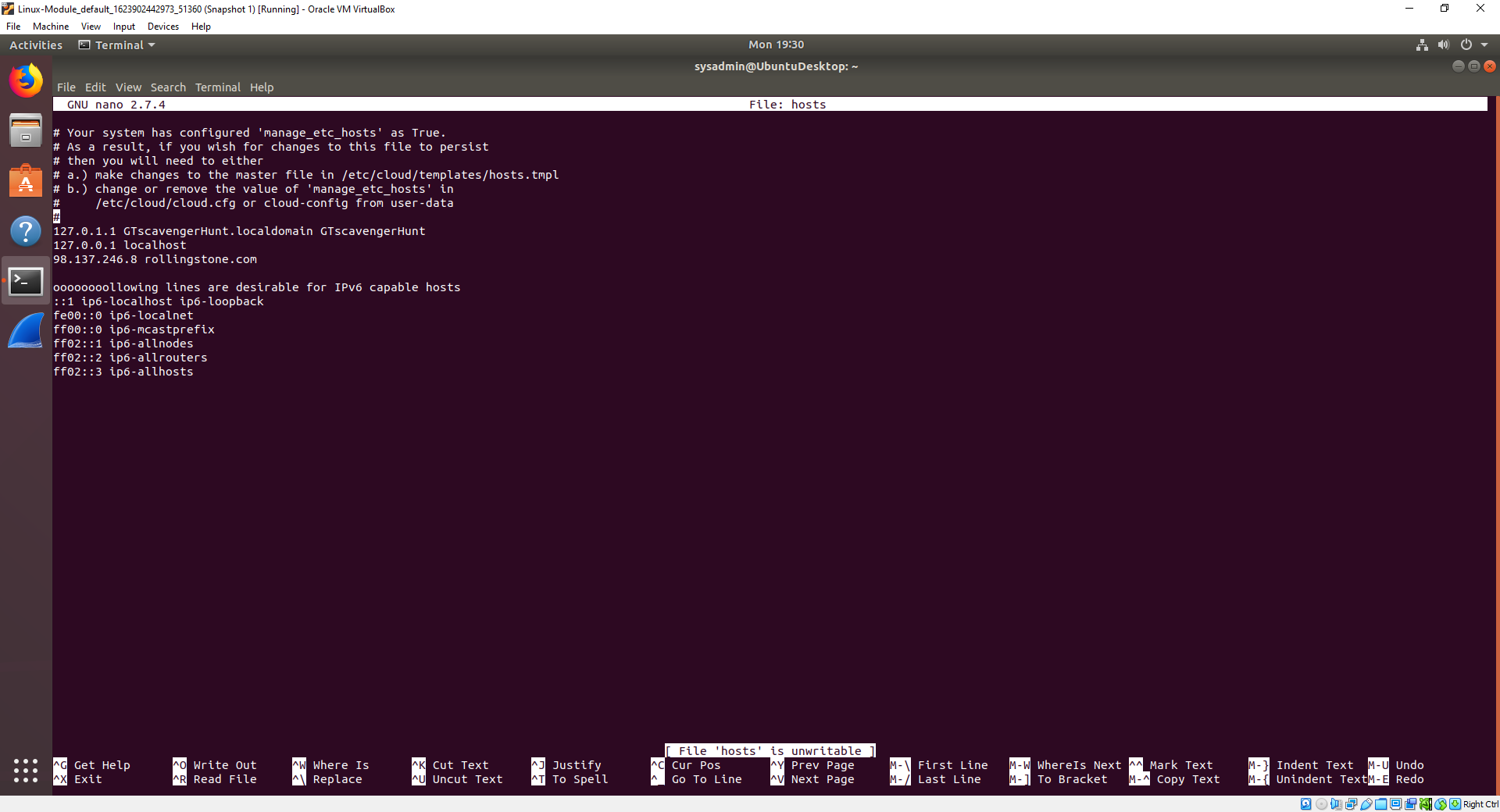
Step 2

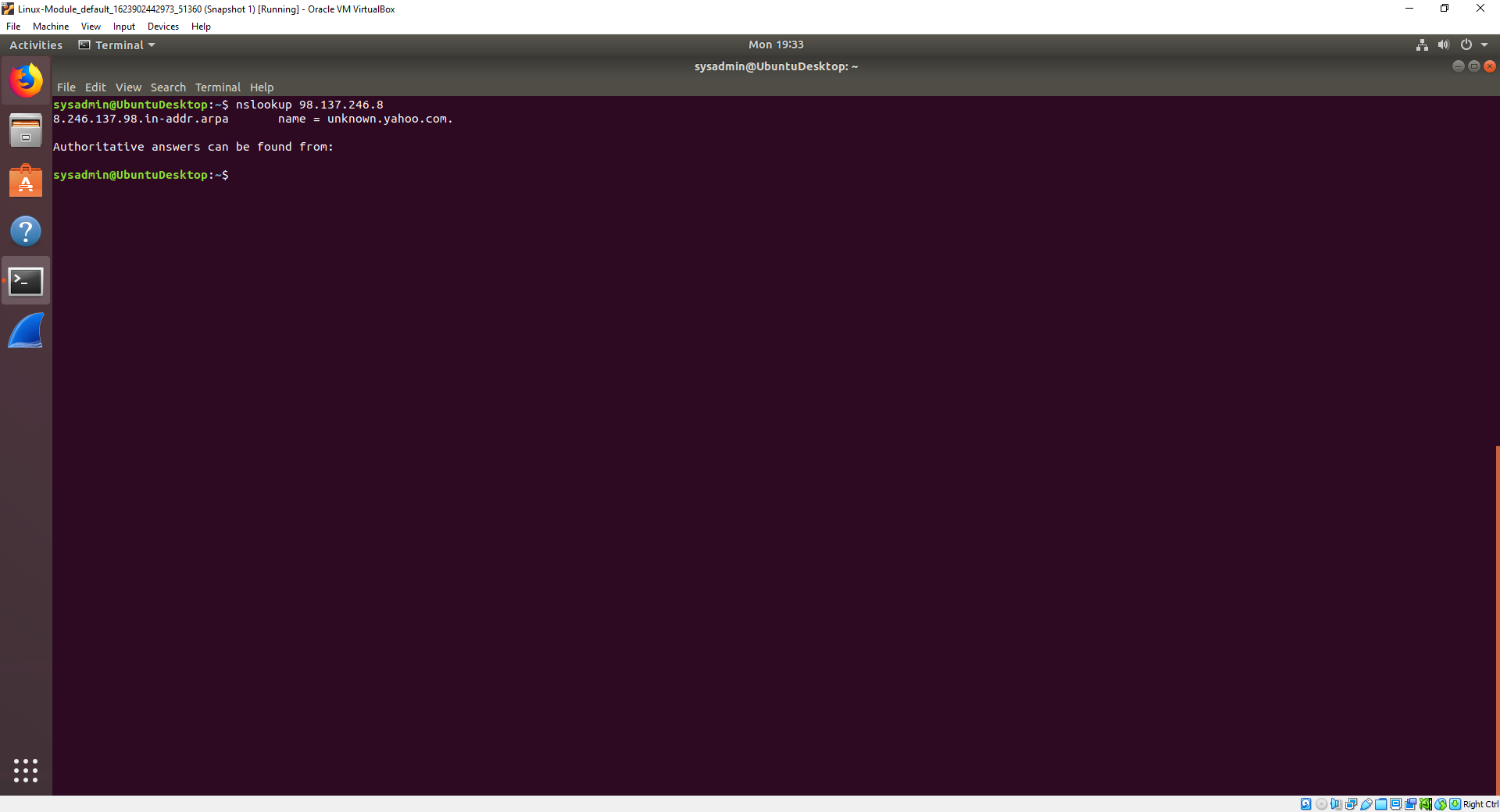


* Level 2: Data
* Port 22 is the default port and should be closed..

Step 3

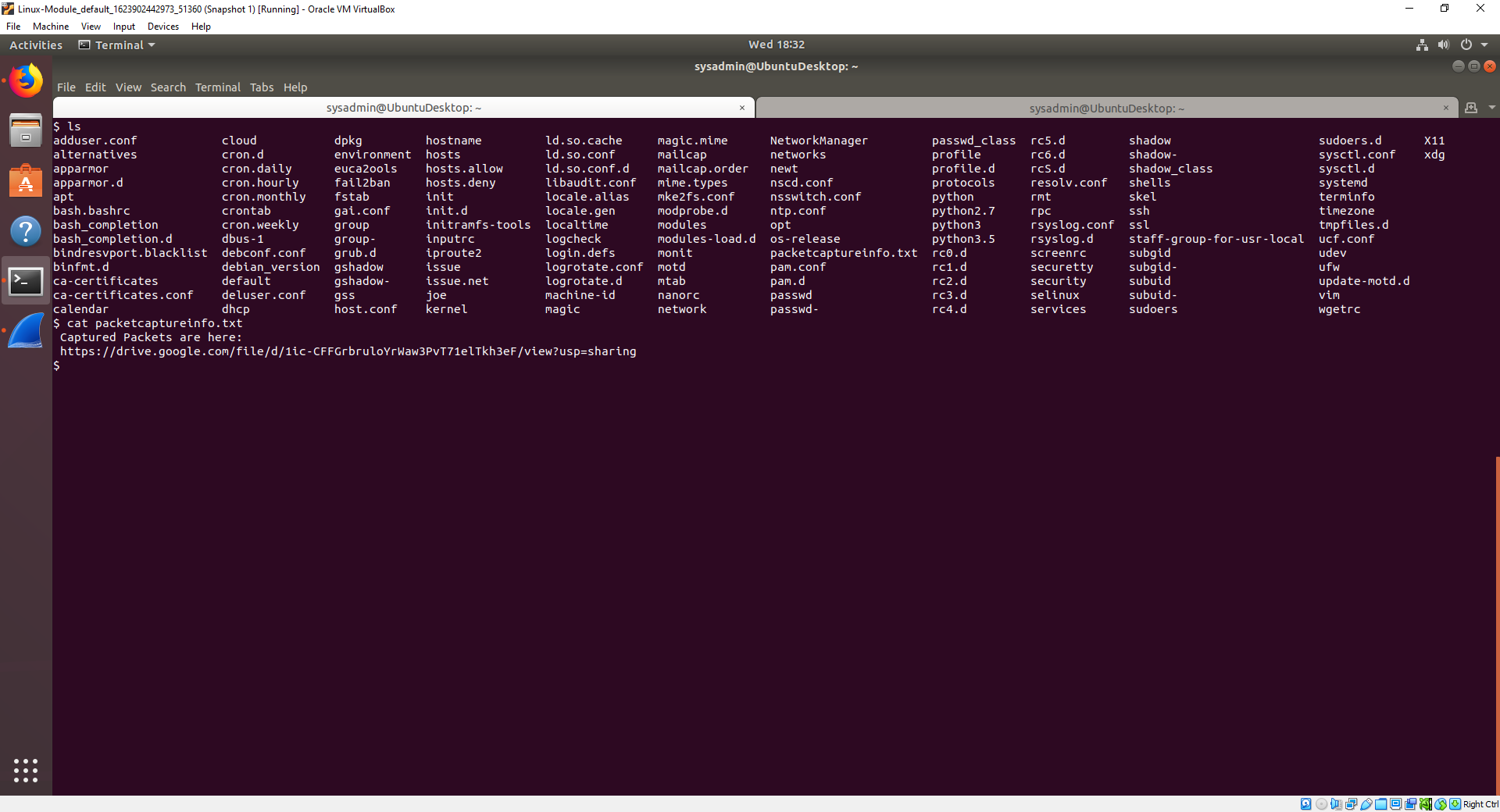


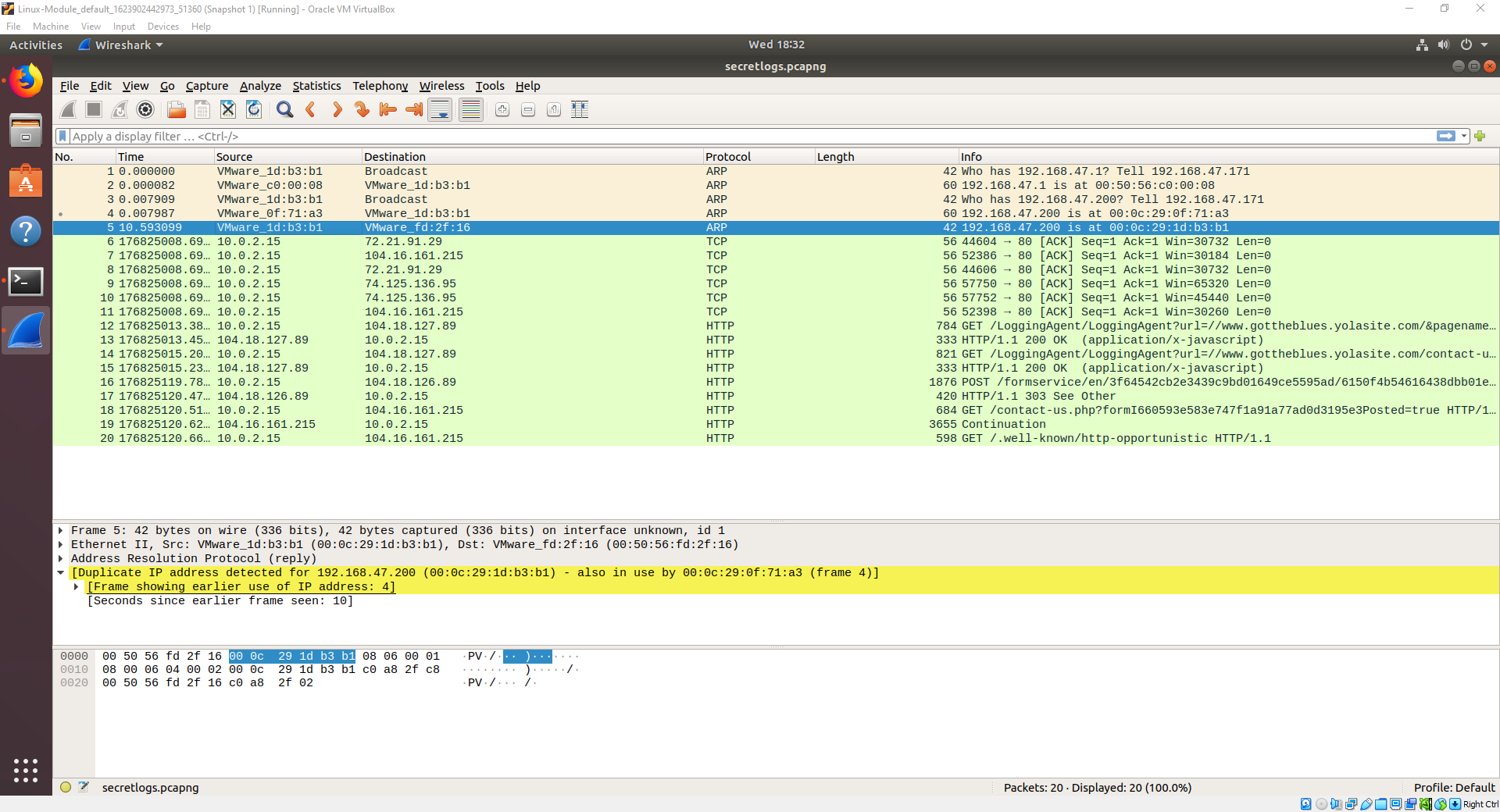




* Level 5: Session.
* This is DNS Spoofing and can reroute web pages.
* Use encryption like SSL/TLS which would prevent or mitigate the possibility of a website being compromised by DNS Spoofing.

Step 4





* Duplicate IP is Level 3: Network.
* This is an ARP poisoning attack. Traffic can be routed to a malicious device instead of the intended destination.
* Dynamic ARP Inspection (DAI) can be configured to limit the rate at which ARP messages can pass through the switch.