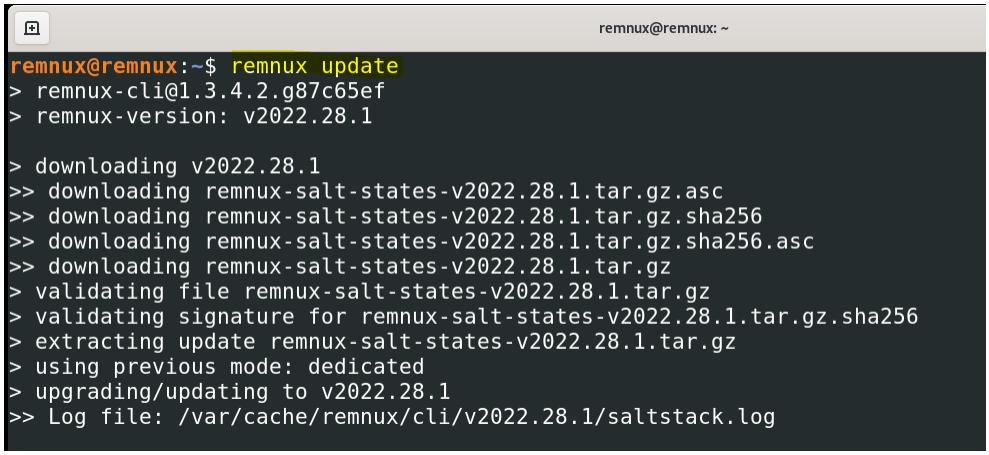
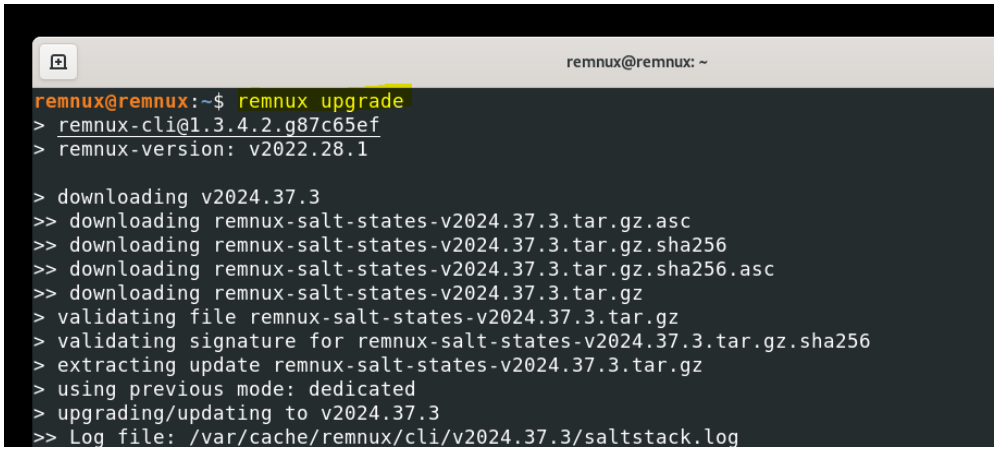
REMnux

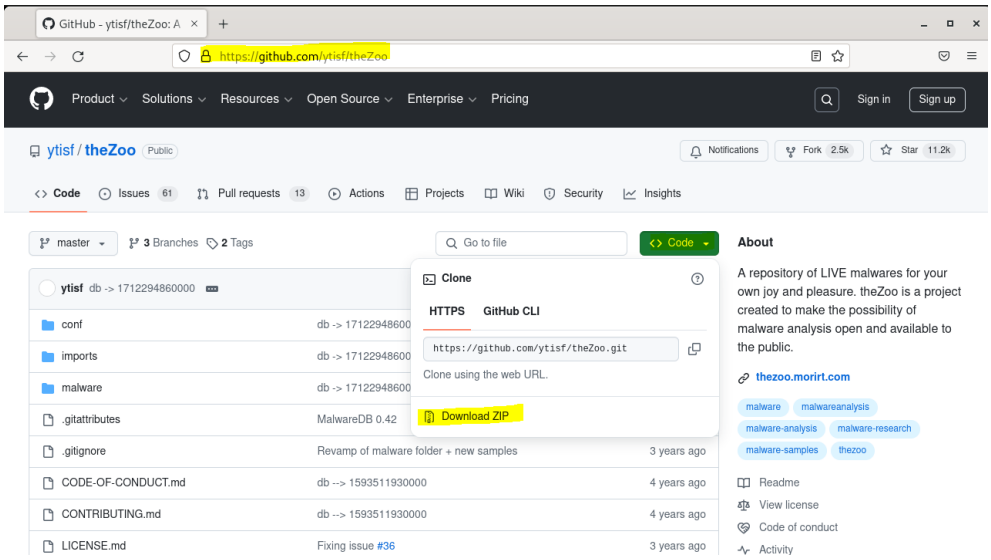
REMnux: *REMnux is a specialized Linux distribution designed for malware analysts and reverse engineers. REMnux is a free and open-source operating system that provides a curated collection of tools and resources for analyzing and dissecting malicious software.*

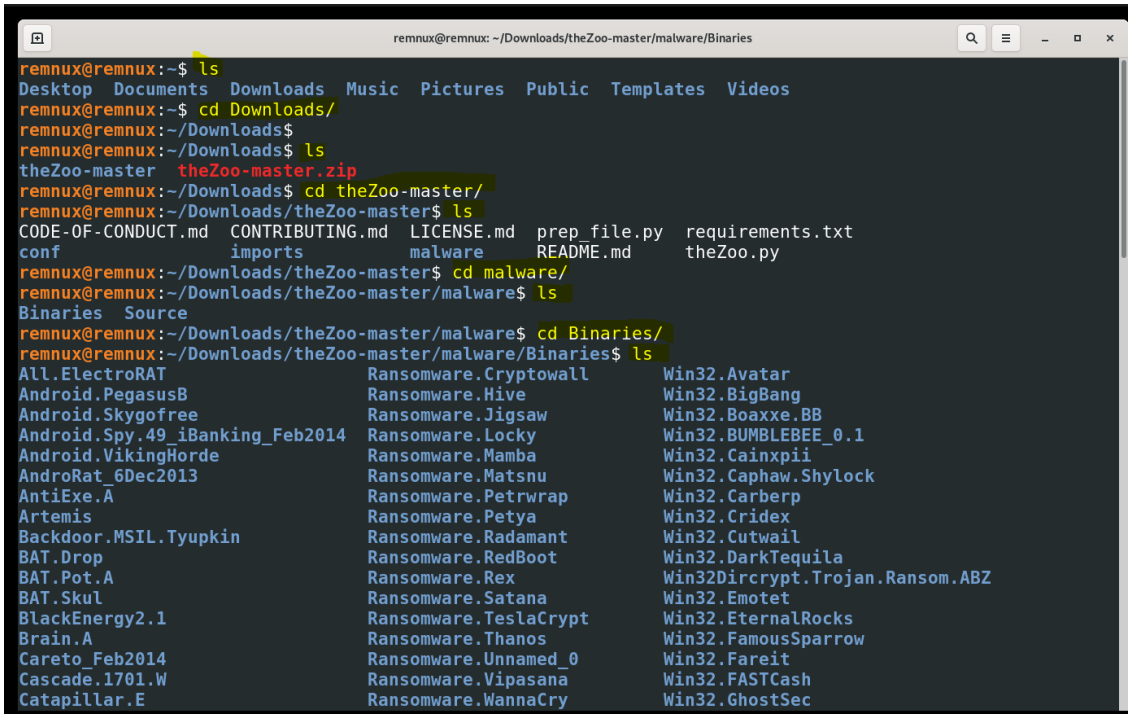
- Download REMnux OVA File from the official website:
  - Link: https://docs.remnux.org/install-distro/get-virtual-appliance
  - Update and upgrade REMnux



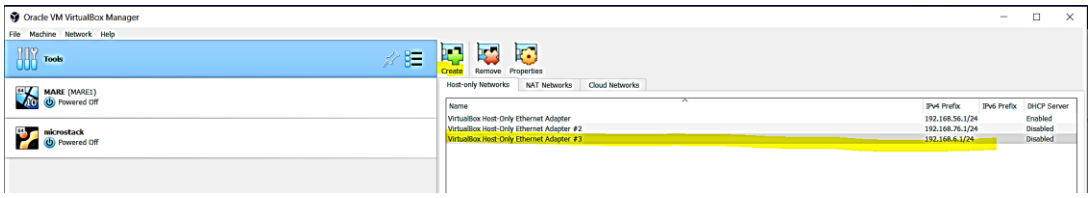


- For malware repository, use the link https://github.com/ytisf/theZoo

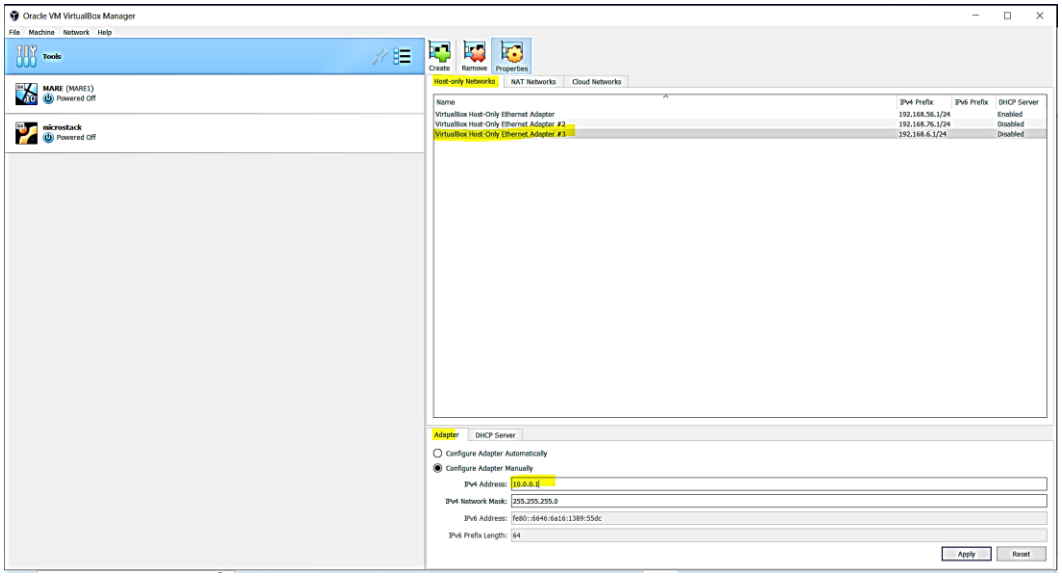




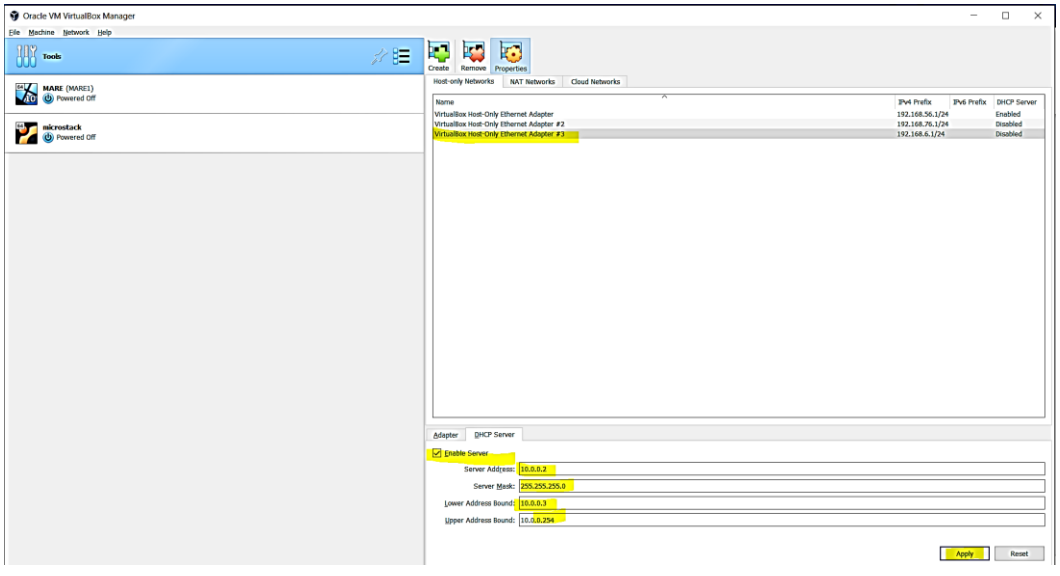
- Create a Host-only network adapter to fully isolate the lab from the host and external network.
  - Goto VirtualBox → Tools > Create > Yes



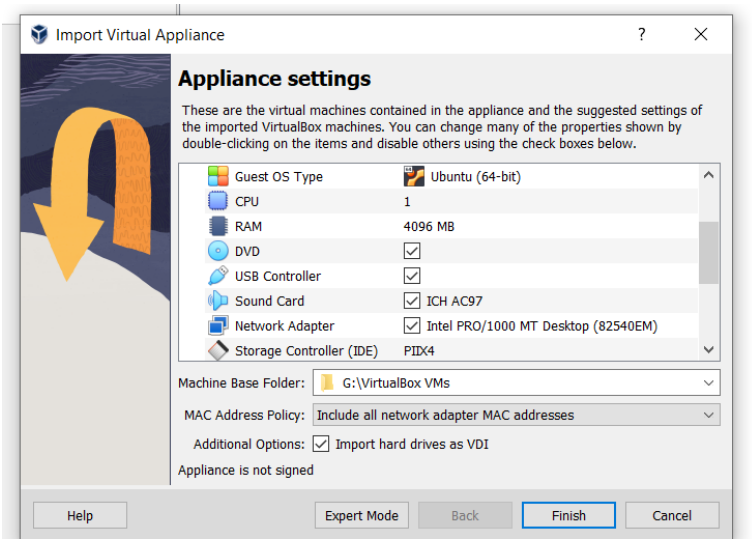
  - Select newly created adapter > Adapter > Configure Address

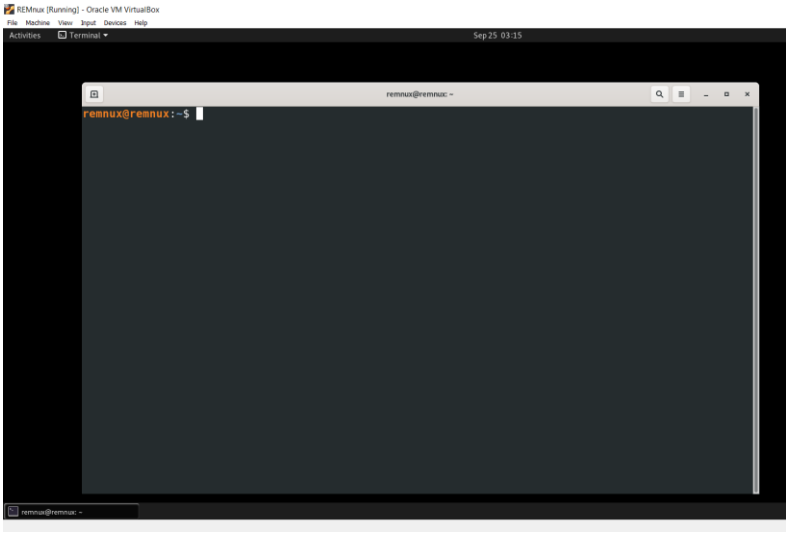


  - Select newly created adapter > DHCP Server > Configure Address

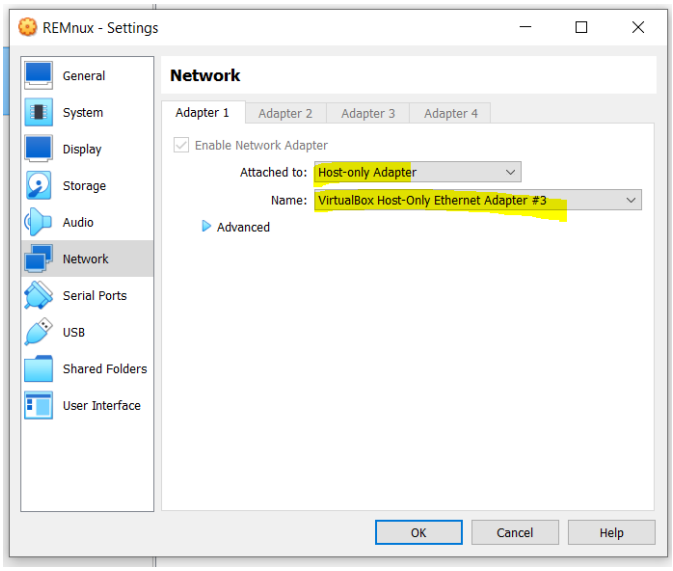


- Import REMnux OVA file in VirtualBox, start the REMnux VM
  - Double click the REMnux OVA

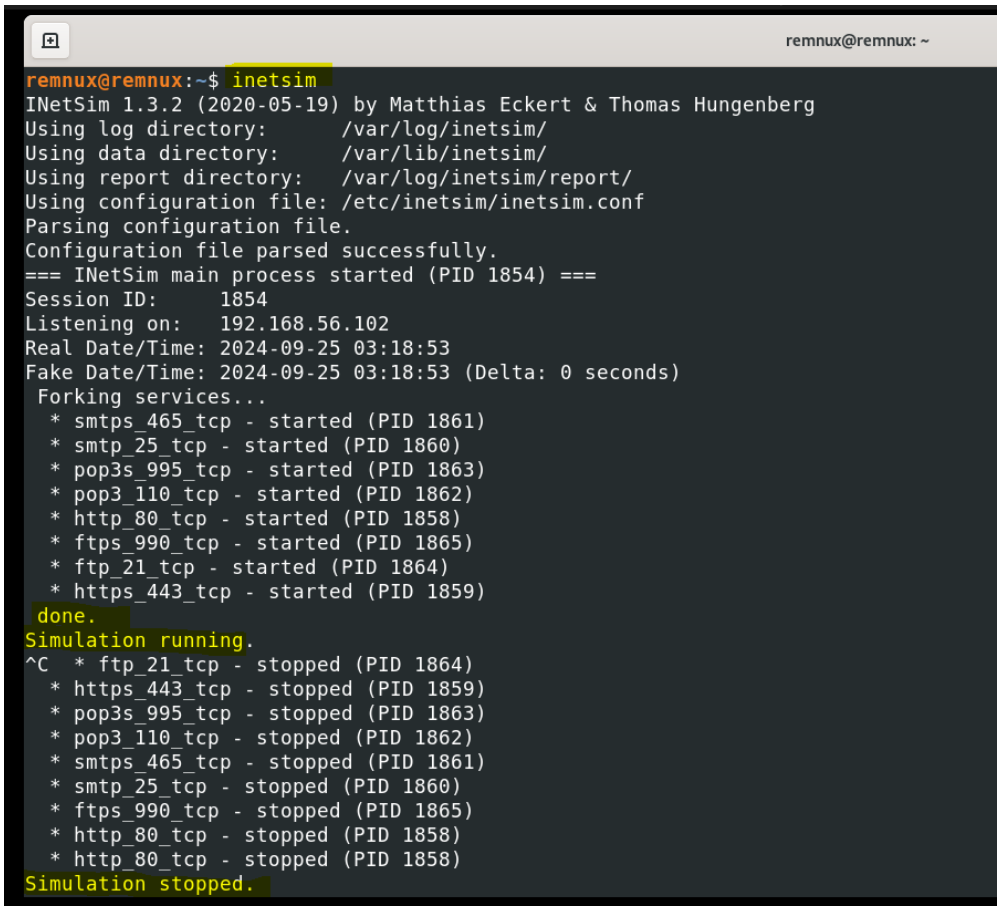




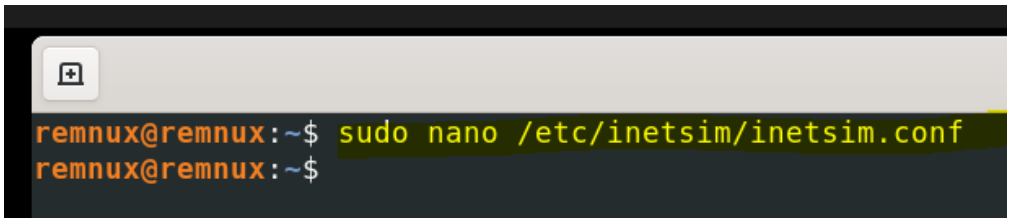
  - Change REMnux network adapter from NAT to Host-only Adapter.

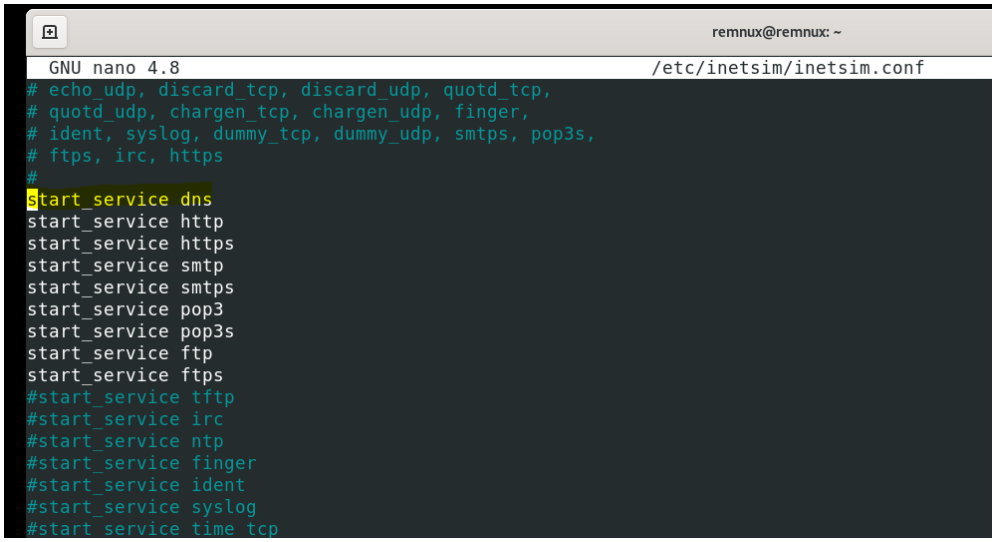


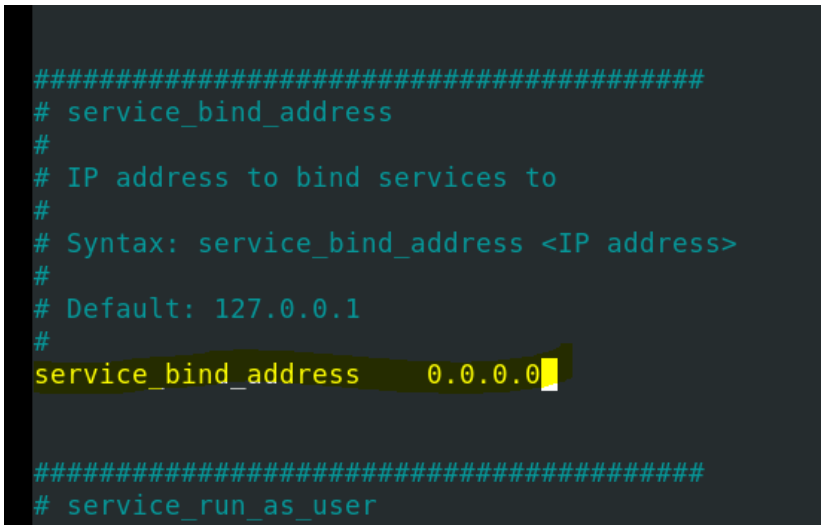
- Set up a fake DNS server to resolve the DNS query for malware.
  - For example, downloading some second-stage payload from the remote server.
  - INetSim is a software suite for simulating common internet services in a lab environment, e.g. for analyzing the network behaviour of unknown malware samples.
  - INetSim supports simulation of the following services: HTTP, SMTP, POP3, DNS, FTP, NTP, TFTP, IRC, Ident, Finger, Syslog, 'Small servers' (Daytime, Time, Echo, Chargen, Discard, Quotd)

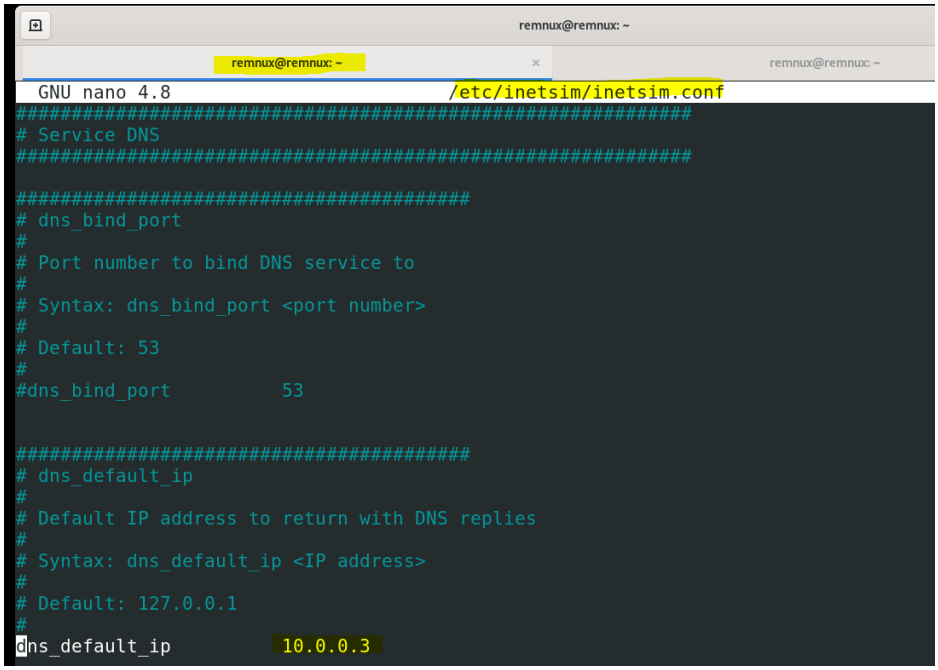


- Enable the DNA service- open the inetsim. conf file to enable the DNS service.

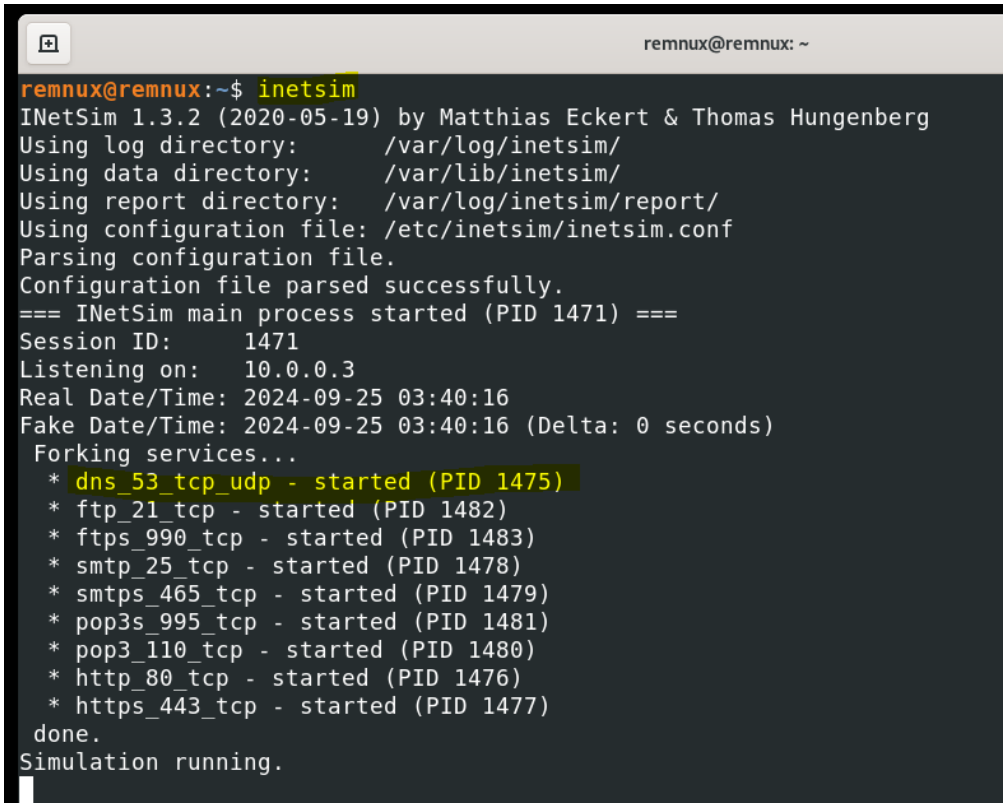




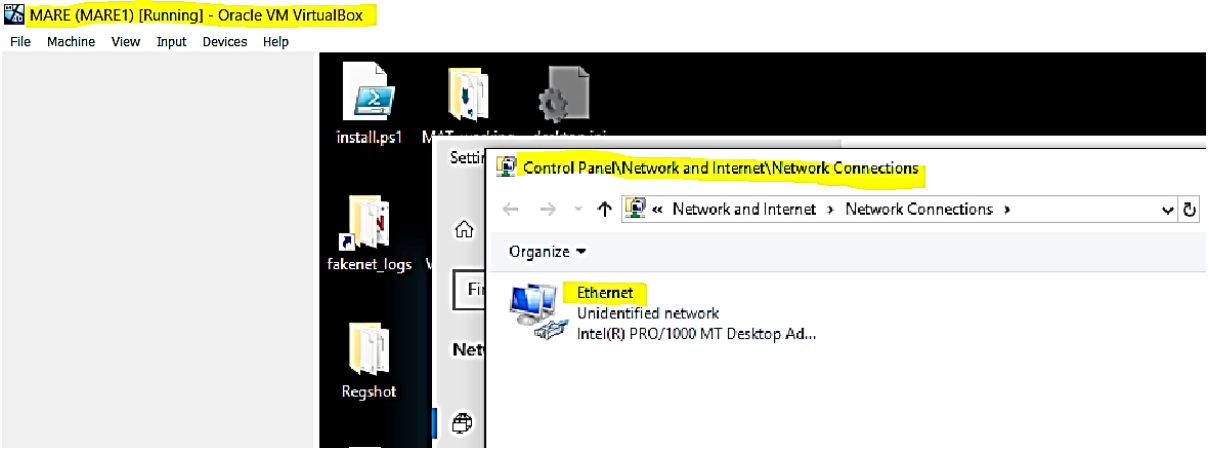


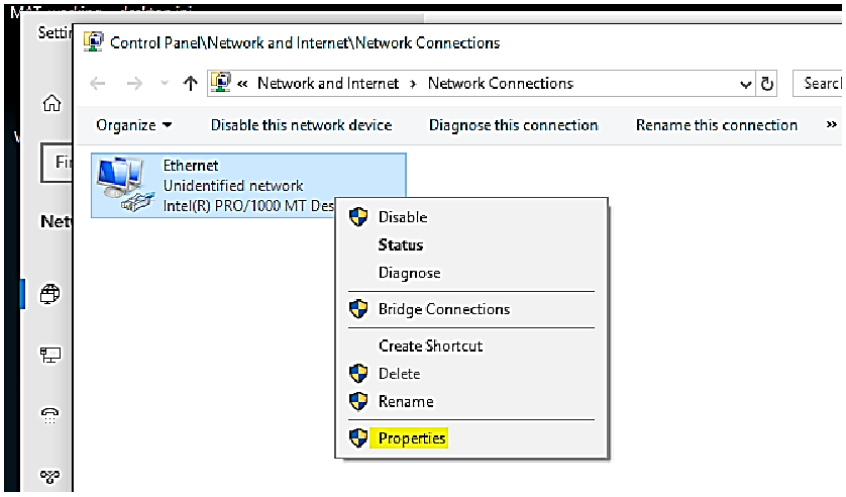


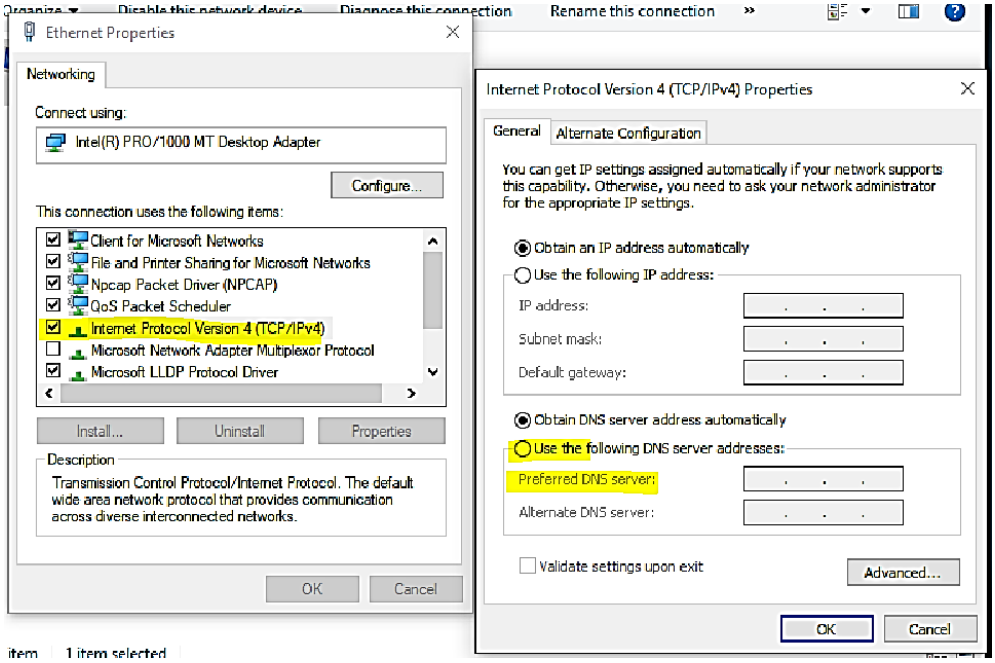
- Now press ctrl+o then press enter to save changes and then ctrl+x to exit.
- Using inetsim check if DNS service is up and running

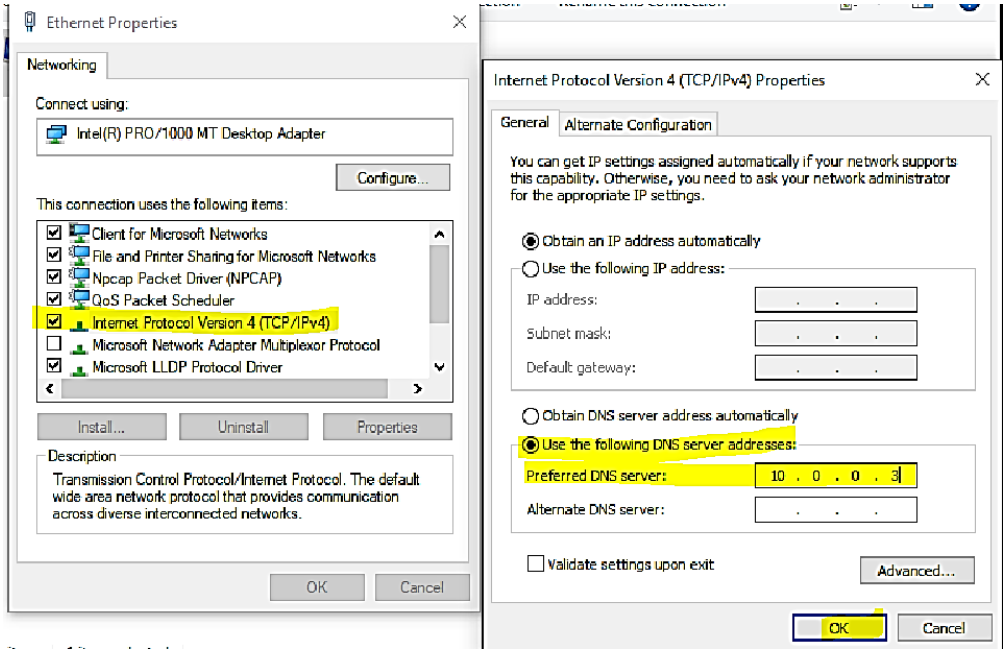


- Configure the Fake DNS server IP on FlareVM - REMnux VM will serves as DNS server.
    - Launch the Flare-VM machine – network and sharing centre-change adapter settings

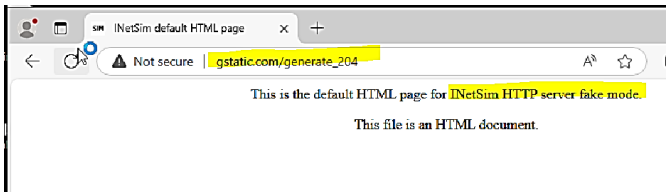


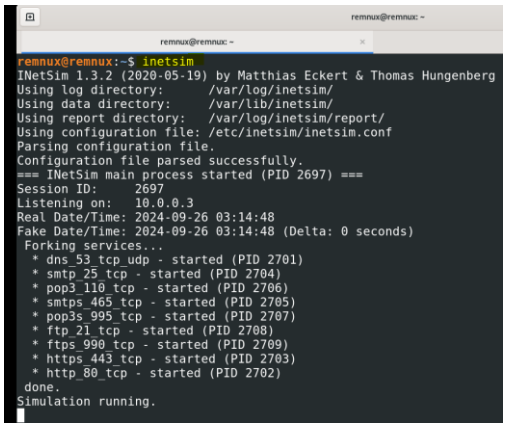






- Testing our REMnux server is configured & working as required.
- Launch the browser in windows 10 VM machine with Flare-VM (MARE) and type the following in the address bar: **gstatic.com/generate_204**





- Server Response from our fake DNS server (REMnux-VM)
  - Launch the browser in windows 10 VM machine with Flare-VM (MARE) and type the following in the address bar: **gstatic.com/generate_204/xyz.exe**
  - Inetsim default binary file is downloaded which is not harmful. That will help malware analysts uncover the malware behavior if it is downloading malicious payload from a remote server.