

REMnux

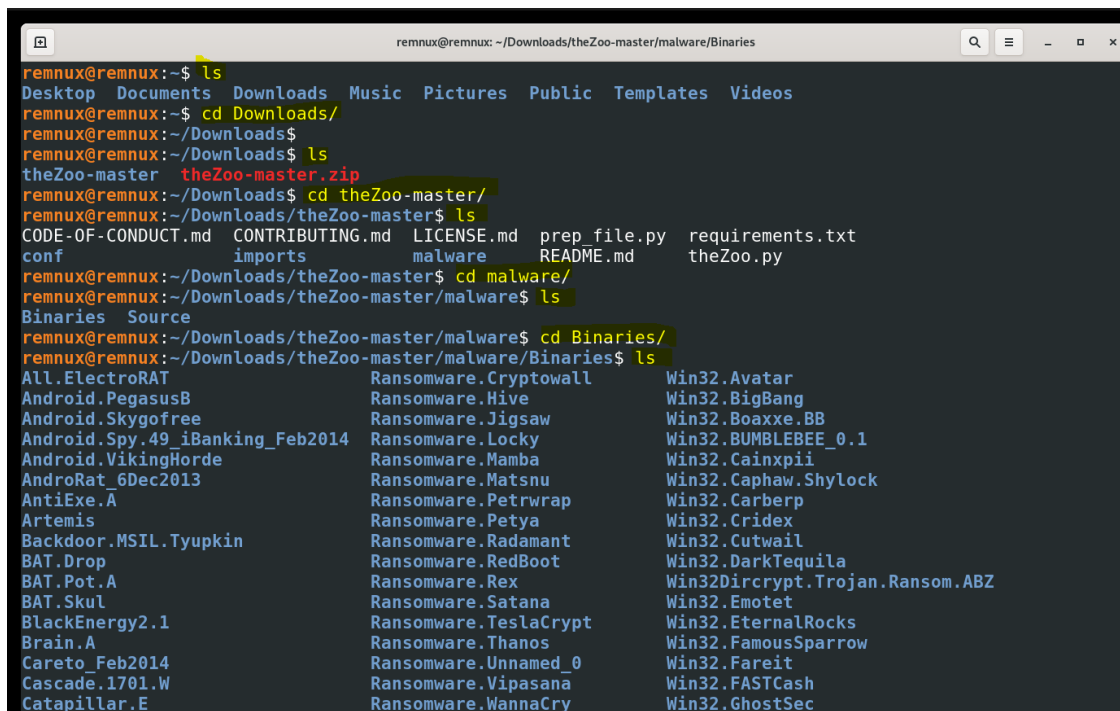
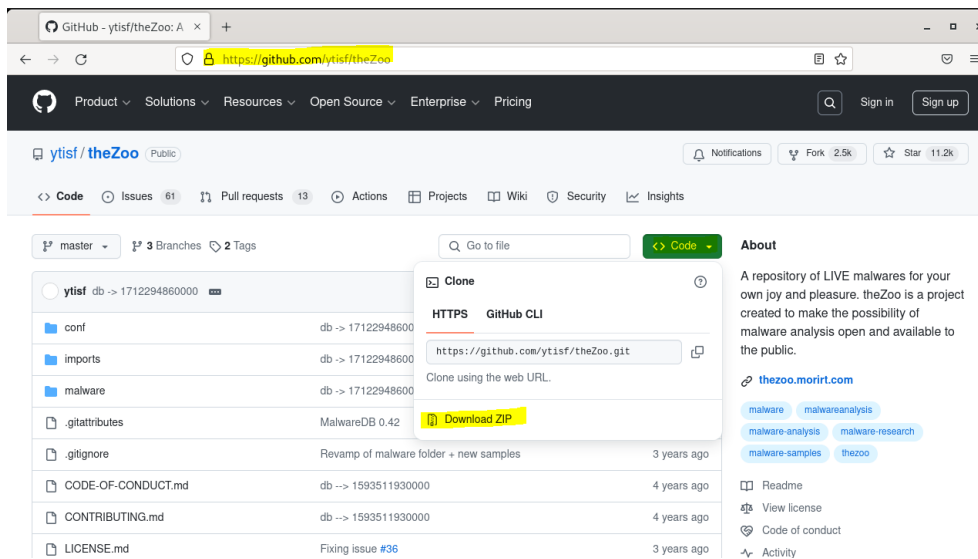
REMnux: REMnux is a specialized Linux distribution designed for malware analysts and reverse engineers. REMnux is a free and open-source operating system that provides a curated collection of tools and resources for analyzing and dissecting malicious software.

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

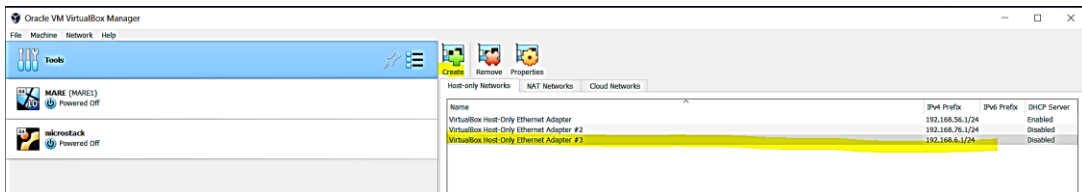
```
remnux@remnux: ~  
remnux@remnux:~$ remnux update  
> remnux-cli@1.3.4.2.g87c65ef  
> remnux-version: v2022.28.1  
  
> downloading v2022.28.1  
>> downloading remnux-salt-states-v2022.28.1.tar.gz.asc  
>> downloading remnux-salt-states-v2022.28.1.tar.gz.sha256  
>> downloading remnux-salt-states-v2022.28.1.tar.gz.sha256.asc  
>> downloading remnux-salt-states-v2022.28.1.tar.gz  
> validating file remnux-salt-states-v2022.28.1.tar.gz  
> validating signature for remnux-salt-states-v2022.28.1.tar.gz.sha256  
> extracting update remnux-salt-states-v2022.28.1.tar.gz  
> using previous mode: dedicated  
> upgrading/updating to v2022.28.1  
>> Log file: /var/cache/remnux/cli/v2022.28.1/saltstack.log
```

```
remnux@remnux: ~  
remnux@remnux:~$ remnux upgrade  
> remnux-cli@1.3.4.2.g87c65ef  
> remnux-version: v2022.28.1  
  
> downloading v2024.37.3  
>> downloading remnux-salt-states-v2024.37.3.tar.gz.asc  
>> downloading remnux-salt-states-v2024.37.3.tar.gz.sha256  
>> downloading remnux-salt-states-v2024.37.3.tar.gz.sha256.asc  
>> downloading remnux-salt-states-v2024.37.3.tar.gz  
> validating file remnux-salt-states-v2024.37.3.tar.gz  
> validating signature for remnux-salt-states-v2024.37.3.tar.gz.sha256  
> extracting update remnux-salt-states-v2024.37.3.tar.gz  
> using previous mode: dedicated  
> upgrading/updating to v2024.37.3  
>> Log file: /var/cache/remnux/cli/v2024.37.3/saltstack.log
```

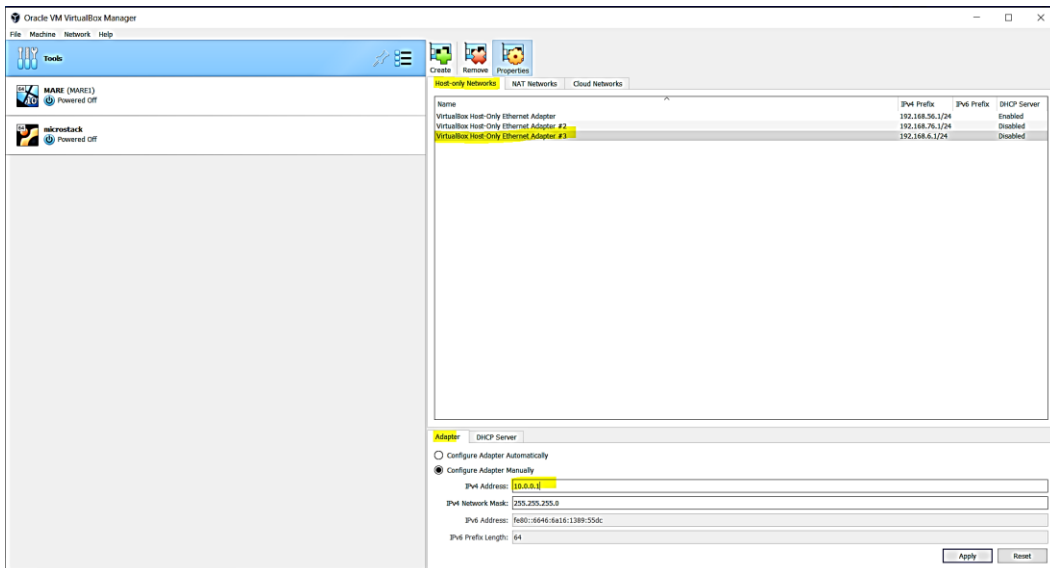
- For malware repository, use the link
<https://github.com/ytisf/theZoo>



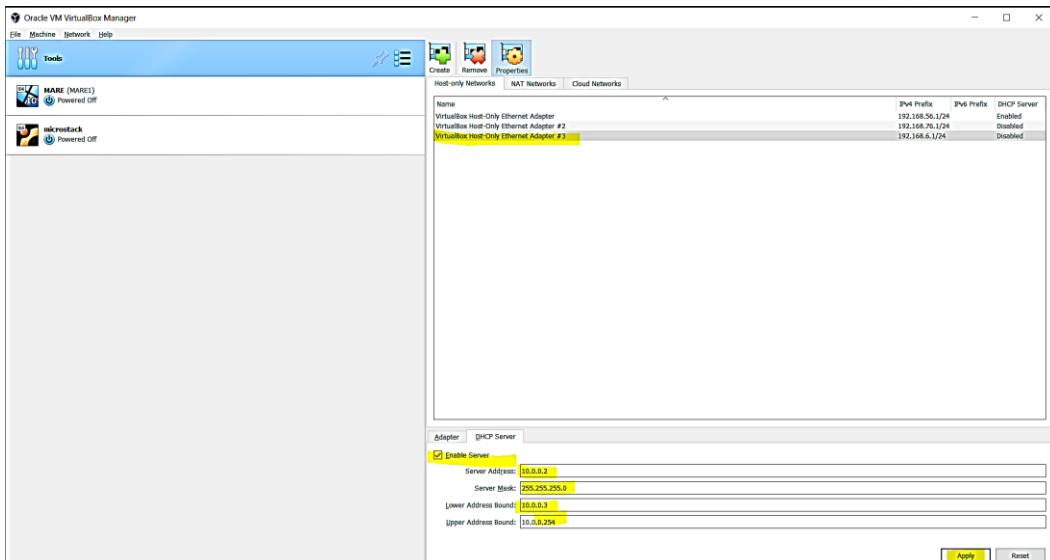
- Create a Host-only network adapter to fully isolate the lab from the host and external network.
 - Goto VirtualBox → Tools > Create > Yes



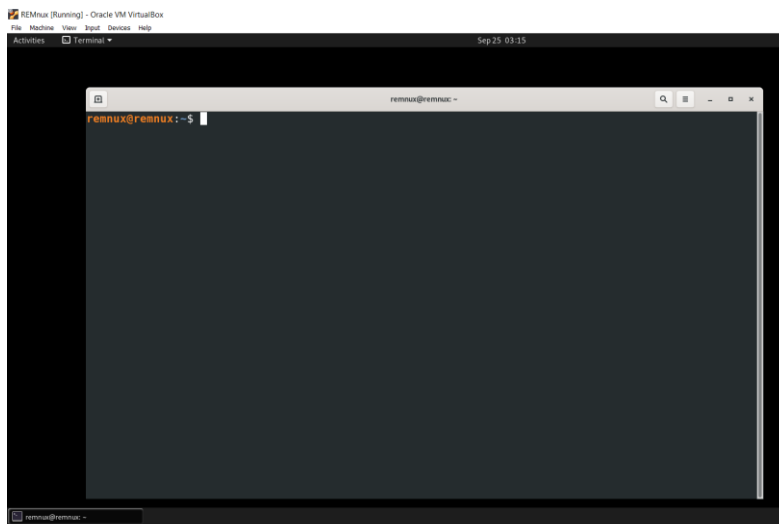
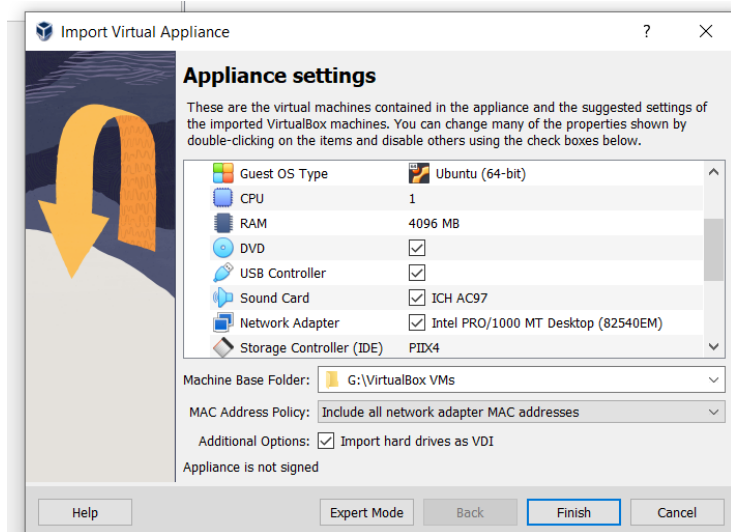
- Select newly created adapter > Adapter > Configure Address



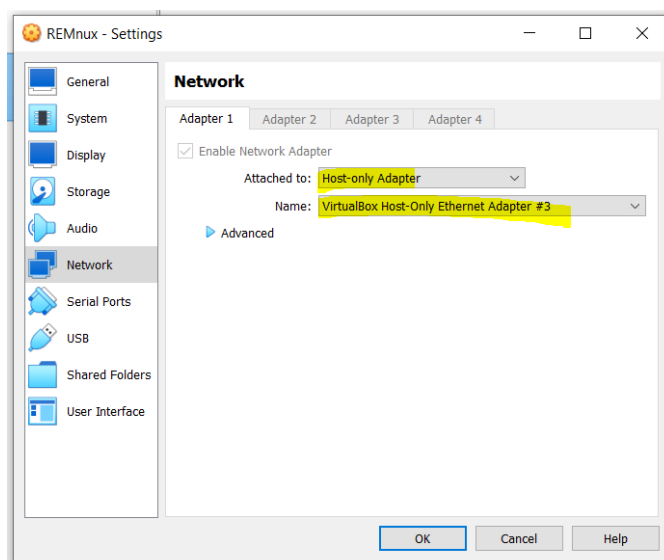
- Select newly created adapter > DHCP Server > Configure Address



- 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.



```
remnux@remnux:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:02:11:8f brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.3/24 brd 10.0.0.255 scope global dynamic enp0s3
        valid_lft 552sec preferred_lft 552sec
    inet6 fe80::a00:27ff:fe02:118f/64 scope link
        valid_lft forever preferred_lft forever
remnux@remnux:~$
```

- 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)

```
remnux@remnux:~$ inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1854) ===
Session ID: 1854
Listening on: 192.168.56.102
Real Date/Time: 2024-09-25 03:18:53
Fake Date/Time: 2024-09-25 03:18:53 (Delta: 0 seconds)
Forking services...
* smtps_465_tcp - started (PID 1861)
* smtp_25_tcp - started (PID 1860)
* pop3s_995_tcp - started (PID 1863)
* pop3_110_tcp - started (PID 1862)
* http_80_tcp - started (PID 1858)
* ftps_990_tcp - started (PID 1865)
* ftp_21_tcp - started (PID 1864)
* https_443_tcp - started (PID 1859)
done.
Simulation running.
^C * ftp_21_tcp - stopped (PID 1864)
* https_443_tcp - stopped (PID 1859)
* pop3s_995_tcp - stopped (PID 1863)
* pop3_110_tcp - stopped (PID 1862)
* smtps_465_tcp - stopped (PID 1861)
* smtp_25_tcp - stopped (PID 1860)
* ftps_990_tcp - stopped (PID 1865)
* http_80_tcp - stopped (PID 1858)
* http_80_tcp - stopped (PID 1858)
Simulation stopped.
```

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

```
remnux@remnux:~$ sudo nano /etc/inetsim/inetsim.conf
remnux@remnux:~$
```

```
remnux@remnux: ~
GNU nano 4.8 /etc/inetsim/inetsim.conf
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargin_tcp, chargin_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp
start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
#start_service time_tcp
```

```
#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 0.0.0.0
#####
# service_run_as_user
```

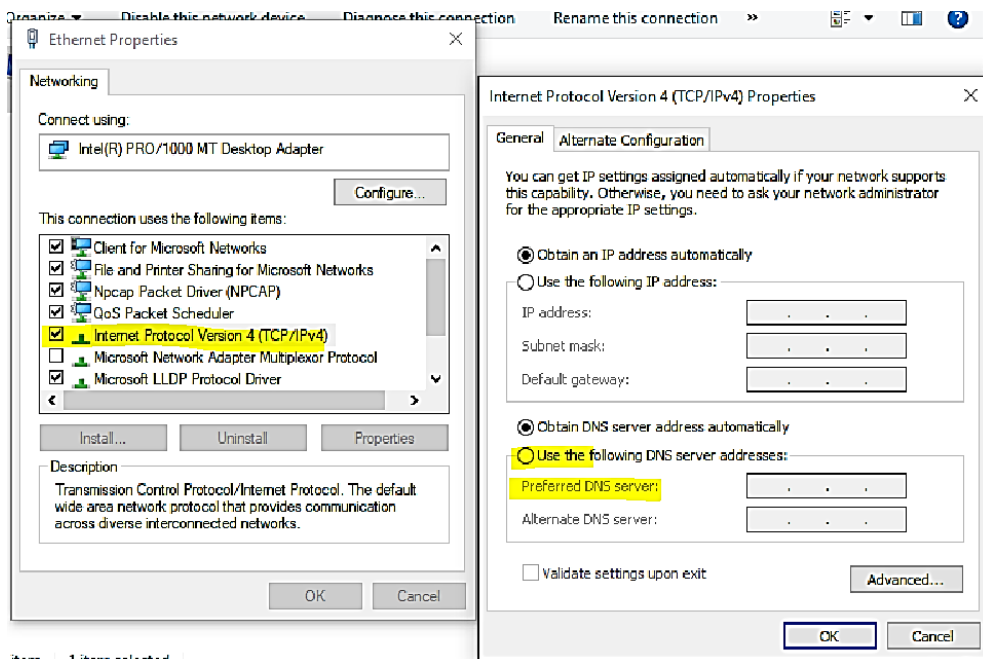
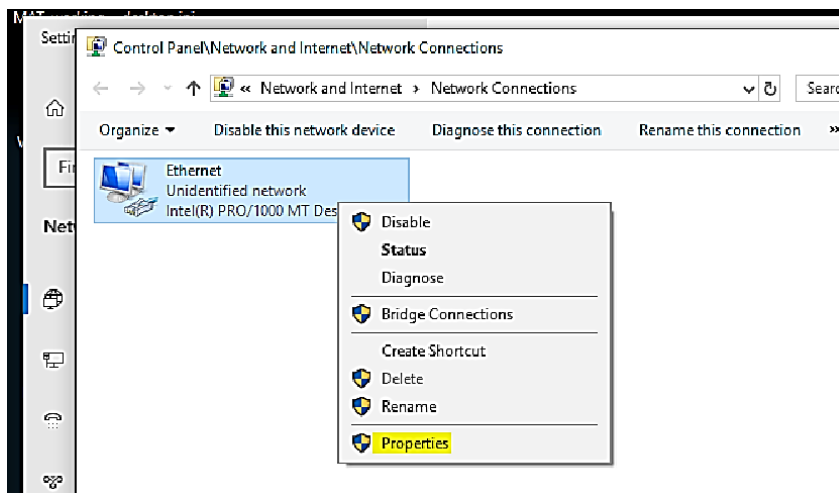
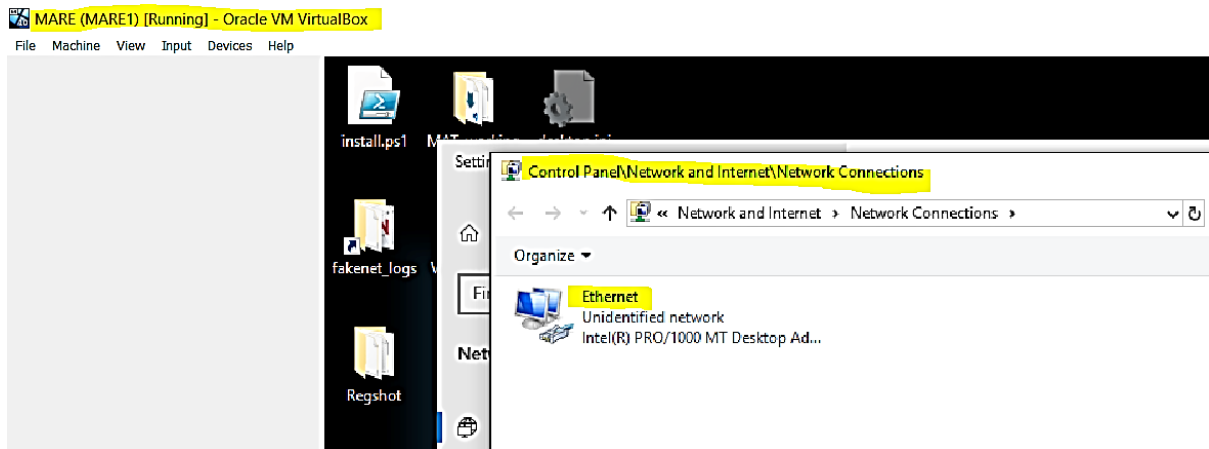
```
remnux@remnux: ~
GNU nano 4.8 /etc/inetsim/inetsim.conf
#####
# Service DNS
#####
#####
# dns_bind_port
#
# Port number to bind DNS service to
#
# Syntax: dns_bind_port <port number>
#
# Default: 53
#
#dns_bind_port          53

#####
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
#dns_default_ip          10.0.0.3
```

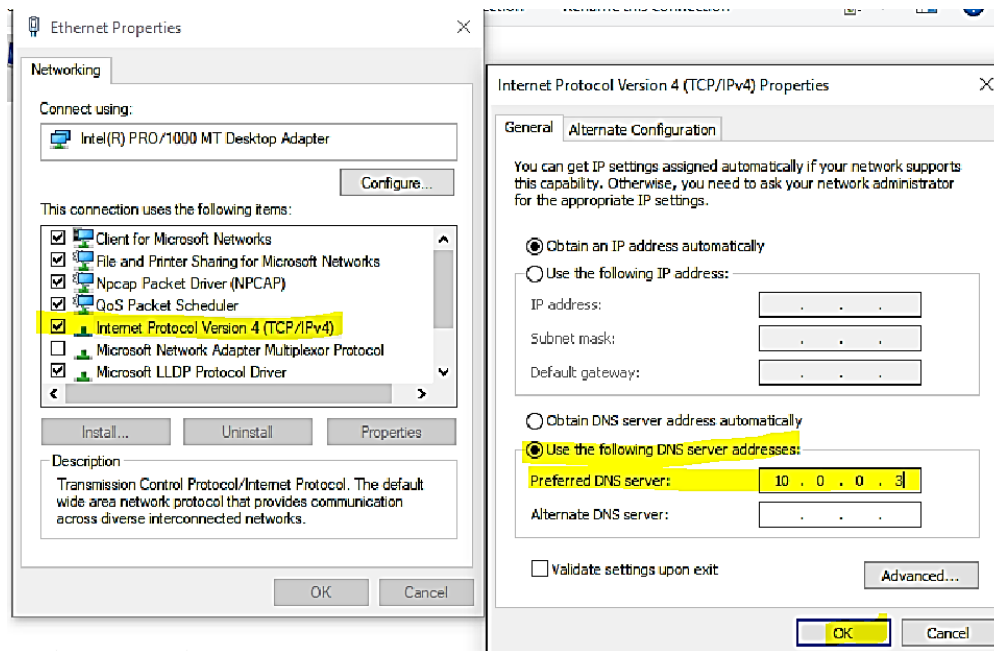
- Now press ctrl+o then press enter to save changes and then ctrl+x to exit.
- Using inetsim check if DNS service is up and running

```
remnux@remnux: ~
remnux@remnux:~$ inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1471) ===
Session ID: 1471
Listening on: 10.0.0.3
Real Date/Time: 2024-09-25 03:40:16
Fake Date/Time: 2024-09-25 03:40:16 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 1475)
* ftp_21_tcp - started (PID 1482)
* ftps_990_tcp - started (PID 1483)
* smtp_25_tcp - started (PID 1478)
* smtps_465_tcp - started (PID 1479)
* pop3s_995_tcp - started (PID 1481)
* pop3_110_tcp - started (PID 1480)
* http_80_tcp - started (PID 1476)
* https_443_tcp - started (PID 1477)
done.
Simulation running.
```

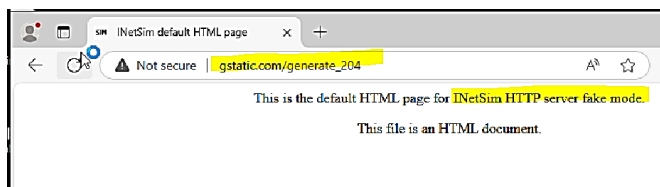
- Configure the Fake DNS server IP on FlareVM - REMnux VM will serve as DNS server.
 - Launch the Flare-VM machine – network and sharing centre-change adapter settings



item 1 item selected



- 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



```
remnux@remnux:~$ inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 2697) ===
Session ID: 2697
Listening on: 10.0.0.3
Real Date/Time: 2024-09-26 03:14:48
Fake Date/Time: 2024-09-26 03:14:48 (Delta: 0 seconds)
Forking services...
* dns 53 tcp.udp - started (PID 2701)
* smtp 25 tcp - started (PID 2704)
* pop3 110 tcp - started (PID 2706)
* smtps 465 tcp - started (PID 2705)
* pop3s 995 tcp - started (PID 2707)
* ftp 21 tcp - started (PID 2708)
* ftps 990 tcp - started (PID 2709)
* https 443 tcp - started (PID 2703)
* http 80 tcp - started (PID 2702)
done.
Simulation running.
```

- 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.

