

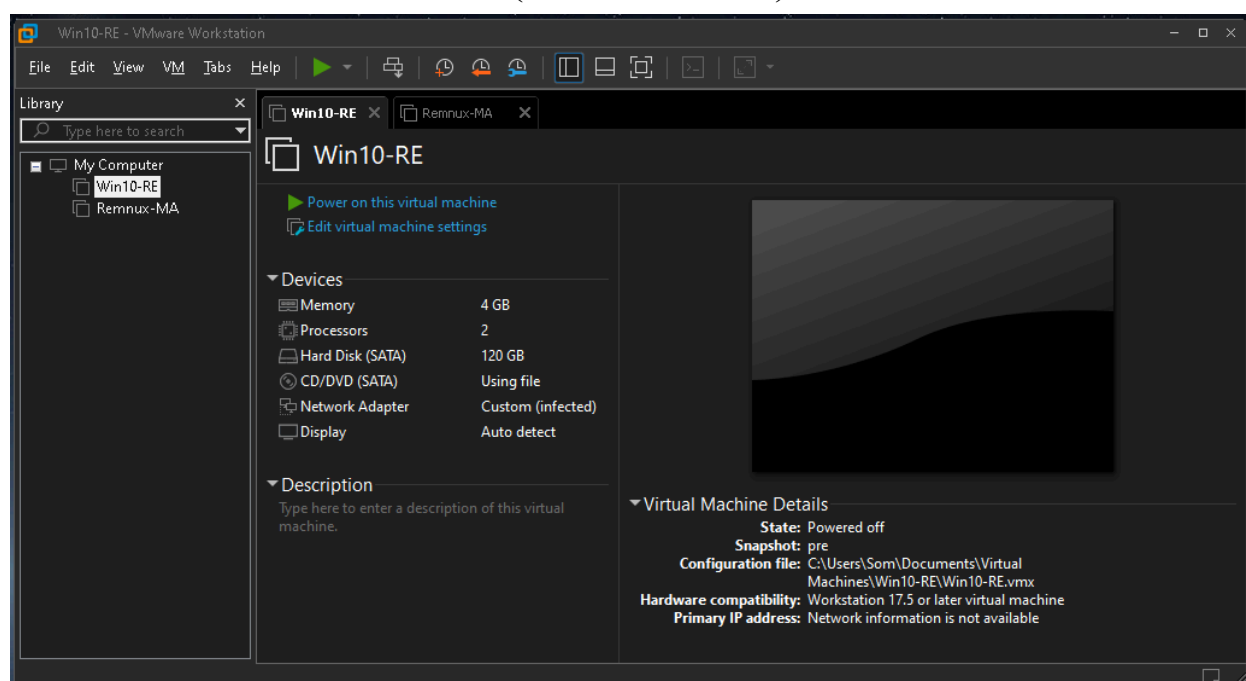
LAB SETUP

(FlareVM + Remnux)

Summary

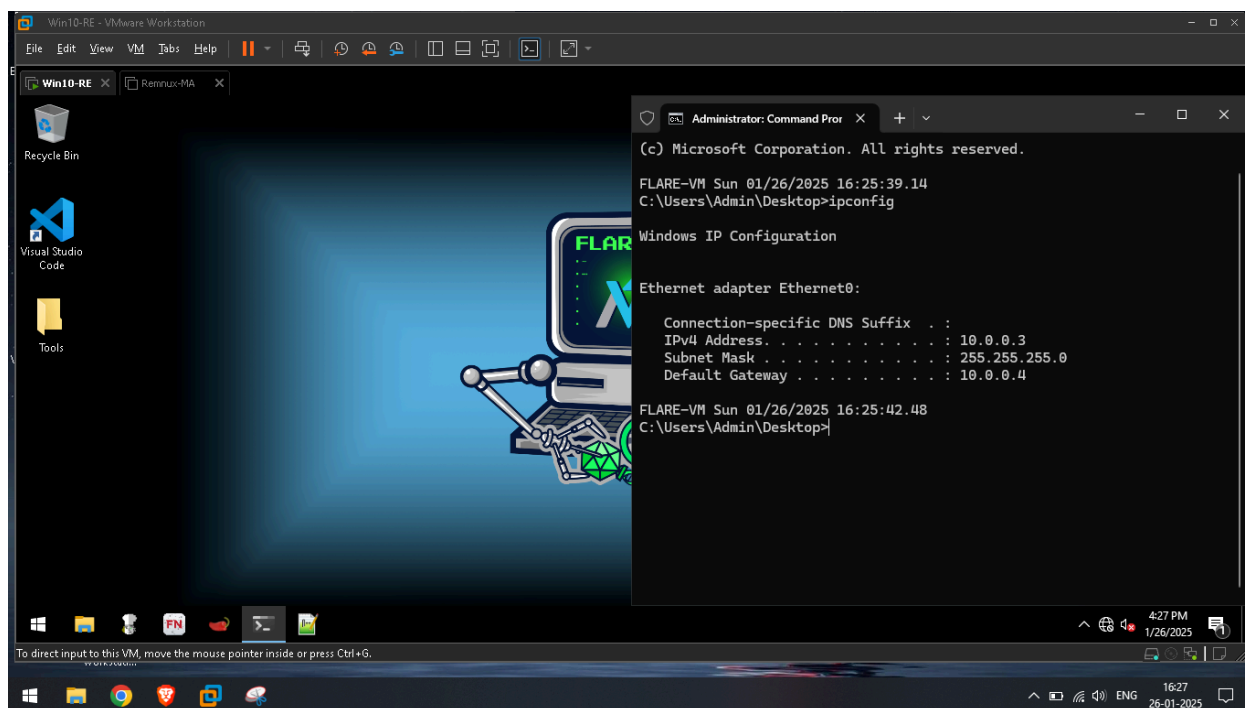
This is a lab setup to analyse malwares in a safe environment. Vmware workstation pro (personal-use) is used to host Windows 10 Pro also known as FlareVM and Linux Ubuntu also known as Remnux. A separate virtual network adapter is used to isolate the network environment and allow only these 2 machines to communicate with each other. Both machines also have snapshots called as Pre-Detonate to allow the user to revert to a clean stage.

Vmware Workstation Pro (Personal Use)

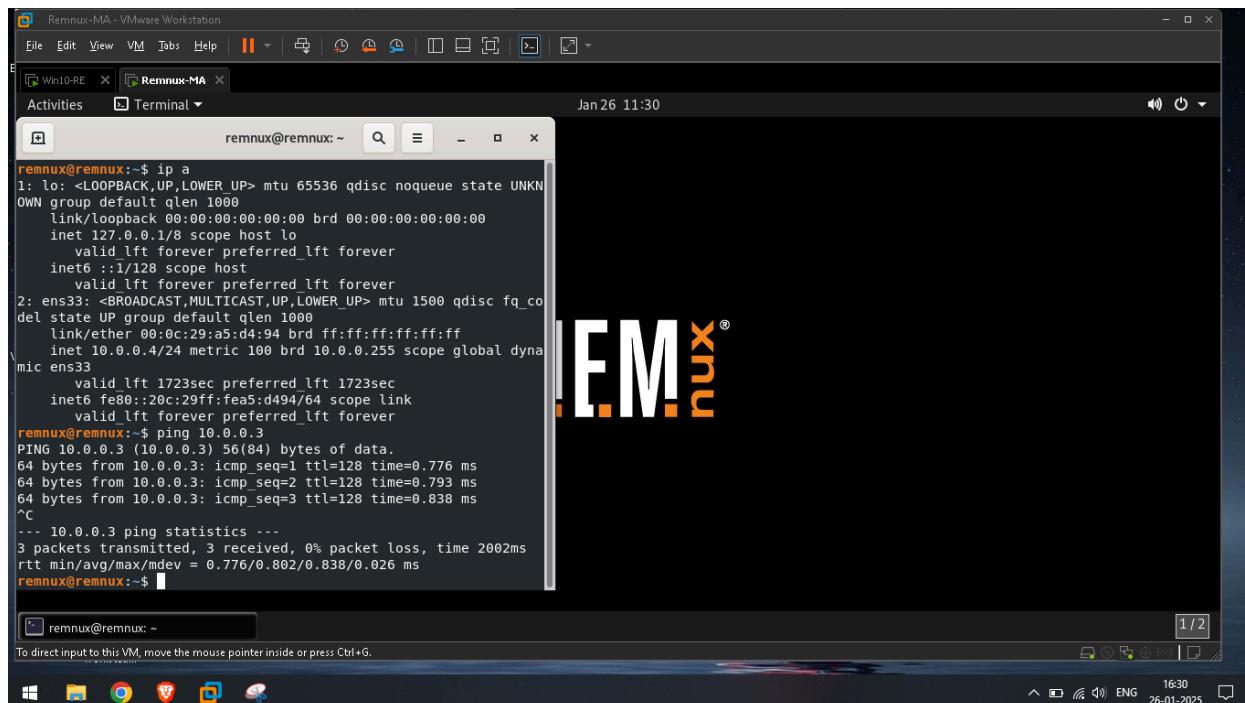


cont..

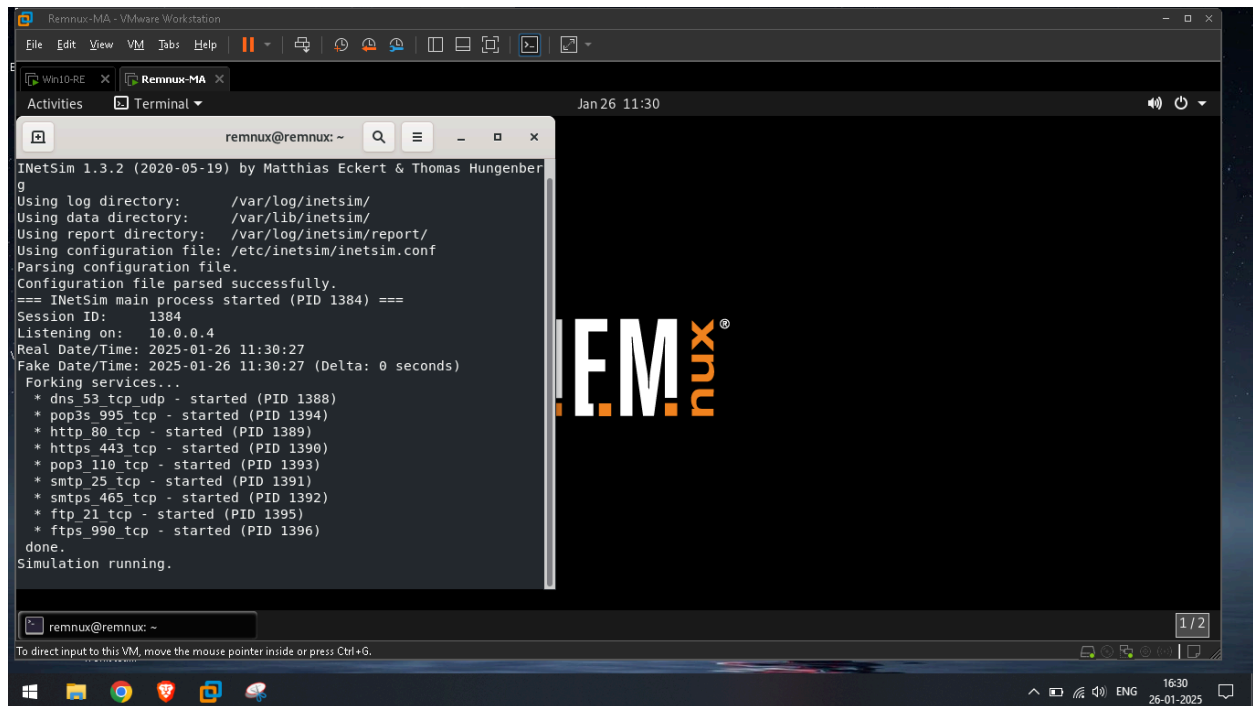
FlareVM



Remnux

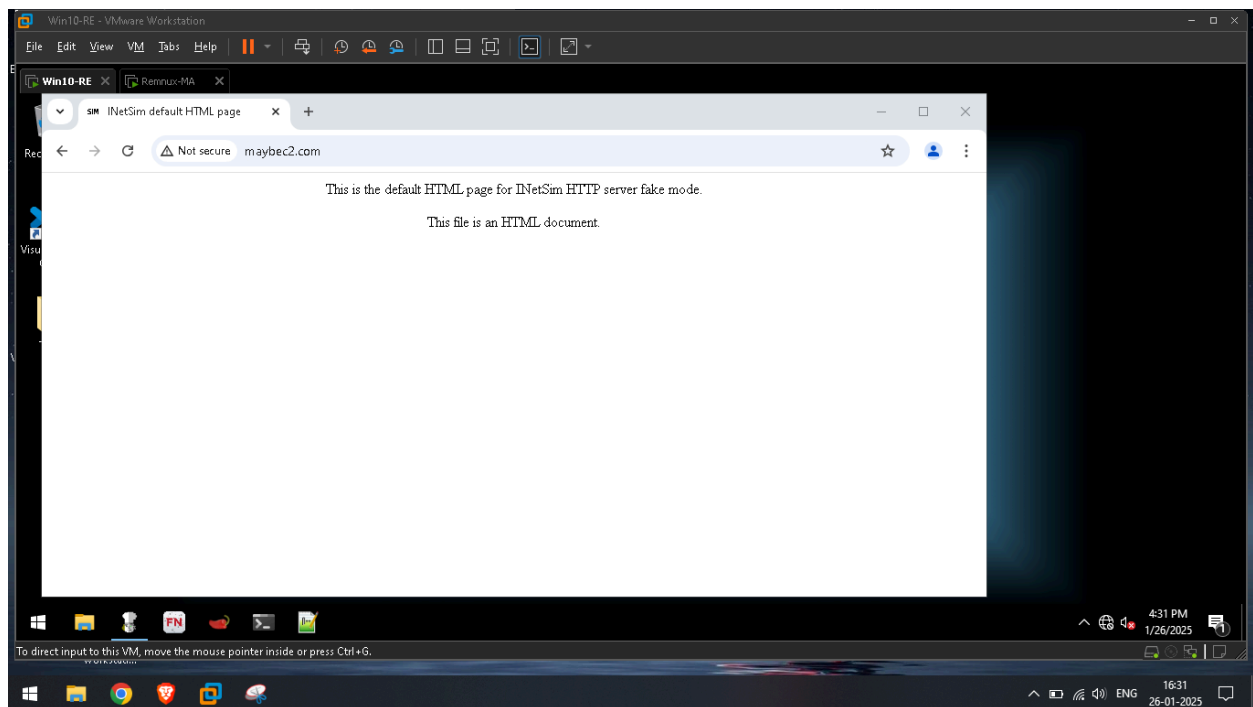


Network Simulation (Inetsim)



The screenshot shows a terminal window titled "Remnux-MA - VMware Workstation" with a sub-window "Terminal". The terminal output displays the InetSim 1.3.2 startup process. It lists the log, data, report, and configuration directories, confirms the configuration file is parsed successfully, and shows the main process starting (PID 1384). A list of services being forked is shown, including dns, pop3s, http, https, pop3, smtp, smtps, ftp, and ftps. The simulation is running, and a large "REM!xnu" logo is visible in the background.

```
remnux@remnux: ~  
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 1384) ===  
Session ID: 1384  
Listening on: 10.0.0.4  
Real Date/Time: 2025-01-26 11:30:27  
Fake Date/Time: 2025-01-26 11:30:27 (Delta: 0 seconds)  
Forking services...  
* dns 53 tcp_udp - started (PID 1388)  
* pop3s 995 tcp - started (PID 1394)  
* http 80 tcp - started (PID 1389)  
* https 443 tcp - started (PID 1390)  
* pop3 110 tcp - started (PID 1393)  
* smtp 25 tcp - started (PID 1391)  
* smtps 465 tcp - started (PID 1392)  
* ftp 21 tcp - started (PID 1395)  
* ftps 990 tcp - started (PID 1396)  
done.  
Simulation running.
```



Virtual Network Adapter

infected	Host-only	-	Connected	Enabled	10.0.0.0
----------	-----------	---	-----------	---------	----------

Conclusion

With this simple setup we can safely conduct basic to advanced Malware Analysis without being afraid of infecting the host machine.