# ***CSC-1002 - 50633 - Ethical Hacking Pen Testing***

***Ethical Hacking – Report***

***Midterm Lab***



***Student Name: Altamash Arif Karlekar***

***Student I’D: A00281563***

***Annexure:***

1. ***Introduction 3-4***
2. ***Network Architecture 5***
3. ***Pentest Report***   ***6- 9***
4. ***Creating a NAT network and Host only Network on virtualbox.*** ***10-13***

*Adding virtual machines to the newly created NAT network and Host only Networks.*

*Primary network adapter ( adapter 1)– NAT network*

*Secondary network (adapter 2) - Host only adapter.*

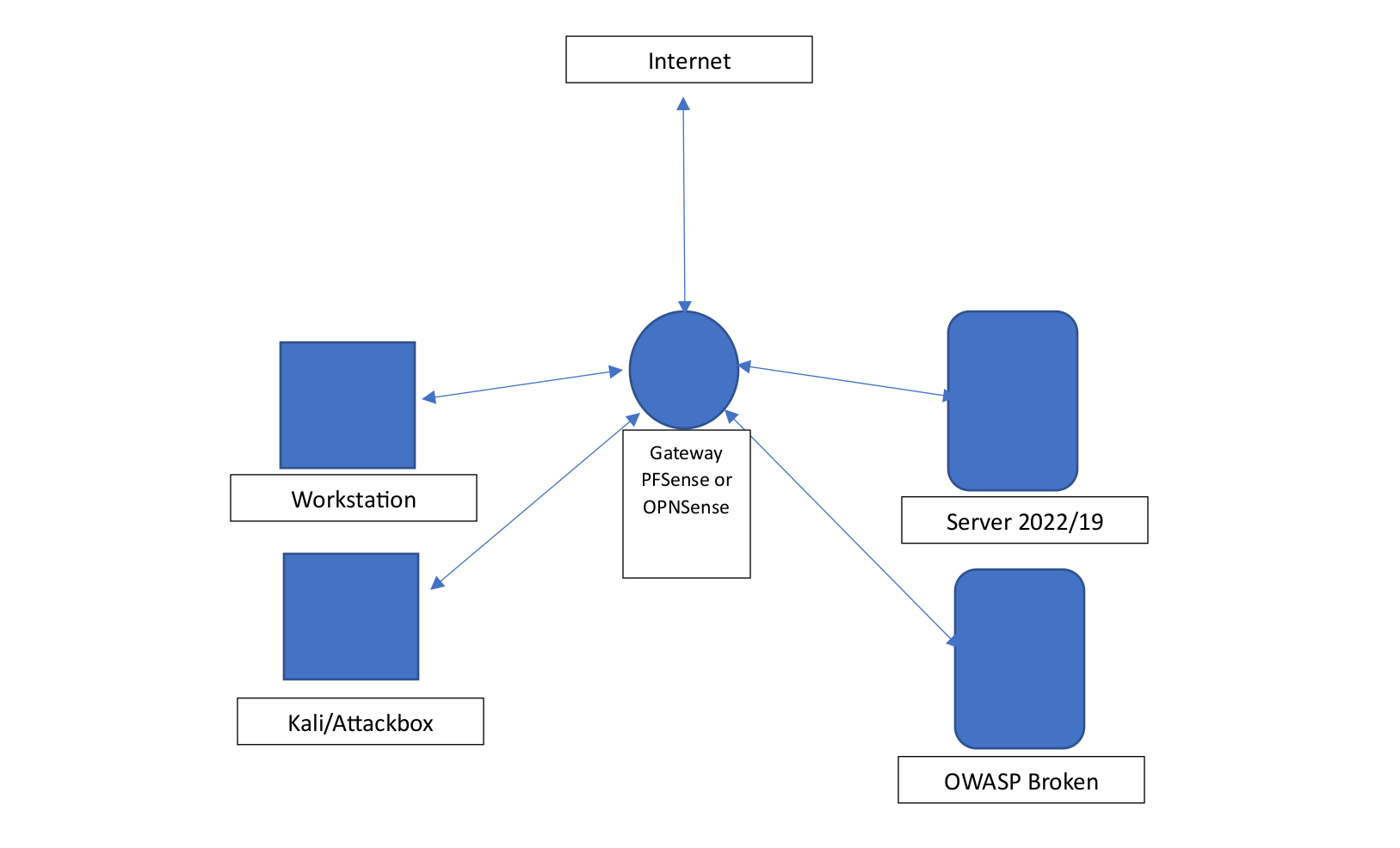
1. ***Setting up Firewall 14-15***

*INTRODUCTION*

*As Archon, a key member of the Arch Angel team, I successfully completed the initial phase of the mission assigned by Evil Co and Associates. Here is a summary of my activities and findings:*

1. *Information Gathering (OSINT):*
   * *Conducted research on Evil Co and Associates, gathering publicly available information.*
   * *Explored employee profiles on LinkedIn to gain insights into the company's structure and potential weak points.*
   * *Scanned social media platforms for any posts by or about the company to identify possible vulnerabilities.*
   * *Scrutinized the company's website for potential loopholes or information leakage.*
2. *Network Enumeration:*
   * *Utilized Parrot Linux to perform network scanning and enumeration of Evil Co's systems.*
   * *Mapped out live hosts, IP addresses, and open ports within their network.*
   * *Documented the findings to create a blueprint of their network systems.*
3. *Classification and Analysis:*
   * *Classified the gathered information and enumeration results according to relevance and potential exploitability.*
   * *Collaborated with the Arch Angel team to conduct preliminary analysis on the potential weak points.*
   * *Identified and documented potential vulnerabilities that could be targeted during the penetration testing phase.*
4. *VMWare Setup and Configuration:*
   * *Setup a virtualized environment using VMWare or a selected hypervisor.*
   * *Configured the following virtual machines (VMs):*
     + *PFSense/OPNSense as a firewall/network gateway.*
     + *Windows Server 2019/2022.*
     + *Parrot or Kali Linux.*
     + *OWASP Broken Application.*
     + *Windows 10/11 Enterprise.*
   * *Configured the network gateway (PFSense/OPNSense) as a firewall, DHCP server, and with two network interface cards (NICS) for NAT and LAN connections.*
   * *Enabled passthrough networking from all VMs through the network gateway.*
5. *Progress Documentation:*
   * *Maintained a detailed log of my activities, including screenshots at each stage.*
   * *Ensured that my name, Travis Lothar Czech, and my student number (1234567890) were clearly visible in the screenshots.*
6. *Report Writing:*
   * *Prepared a comprehensive report for Professor Magneto, summarizing the findings and actions taken during the initial phase.*
   * *Included an overview of Evil Co and Associates, the methods employed for information gathering, the network systems blueprint, potential vulnerabilities identified, and recommendations for the next steps.*
   * *Annex A of the report contained the screenshots documenting the entire process.*

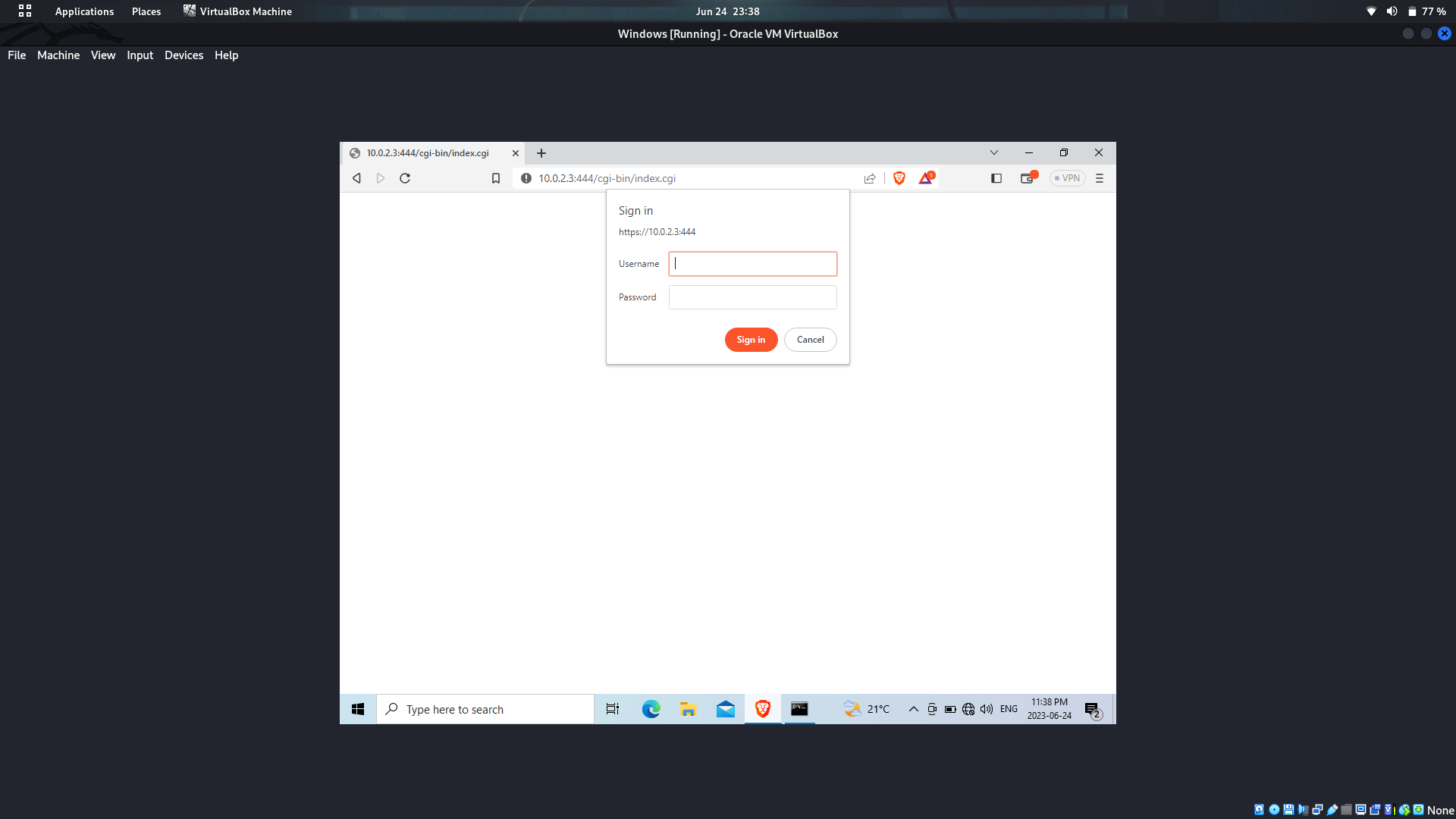
***Network Architecture :***



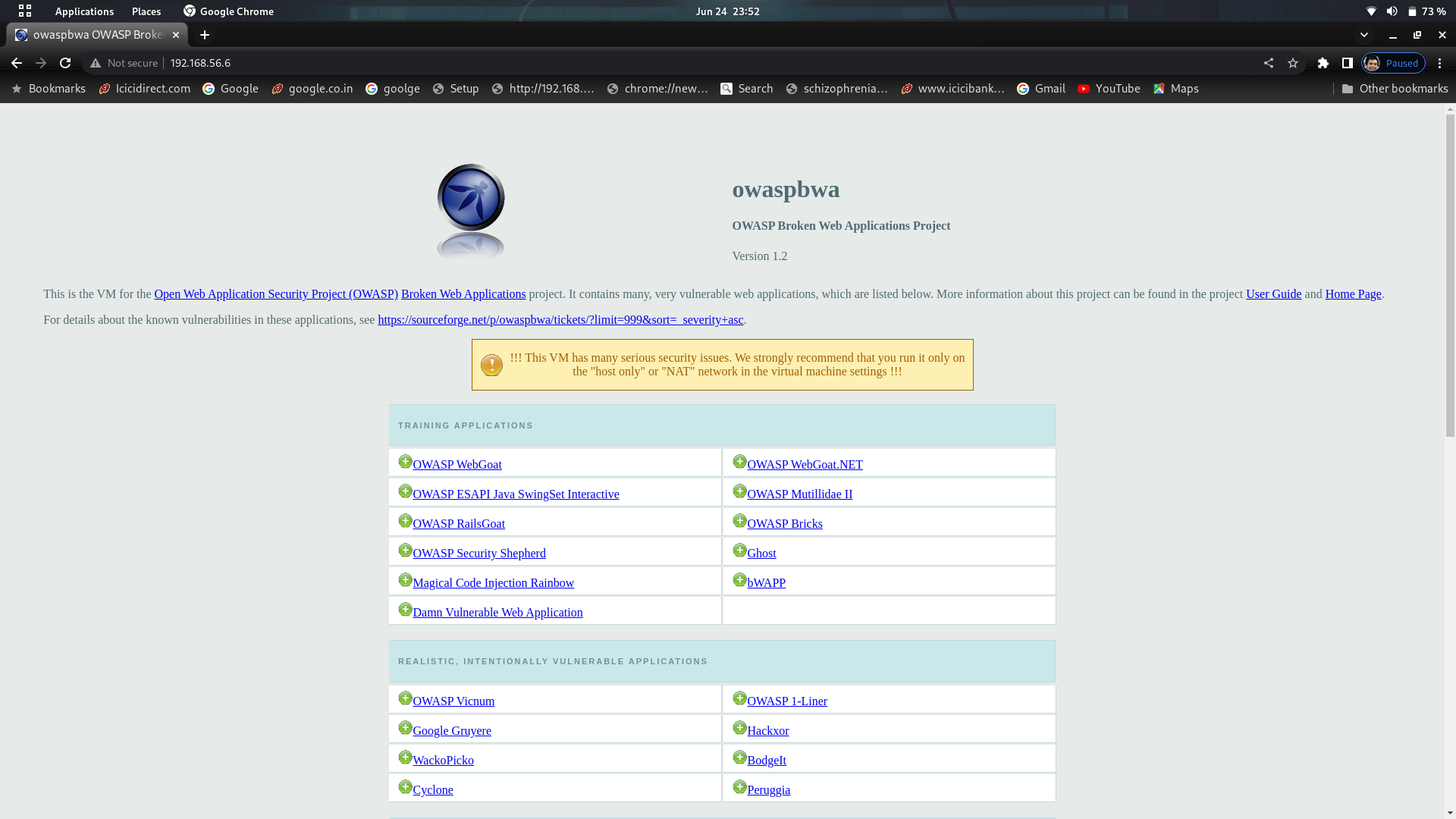
***Pentest Report***

*Checking if the firewall is working on the Network by loading firewall IP in host’s browser.*

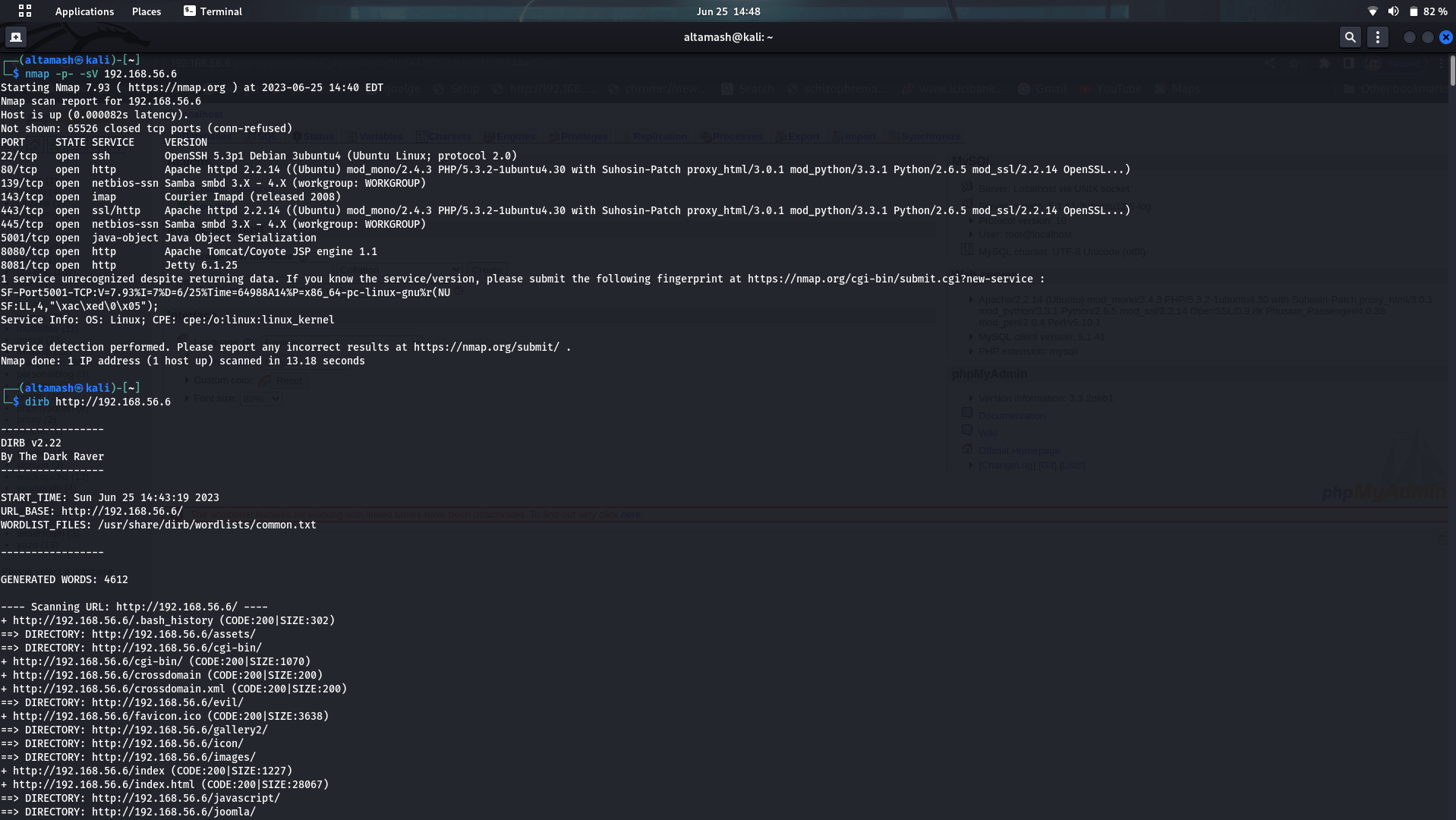
*Click on the advanced tab and move further ignoring the warning.*



*Step 4.2 : OWASP enumeration through kali linux and web login*



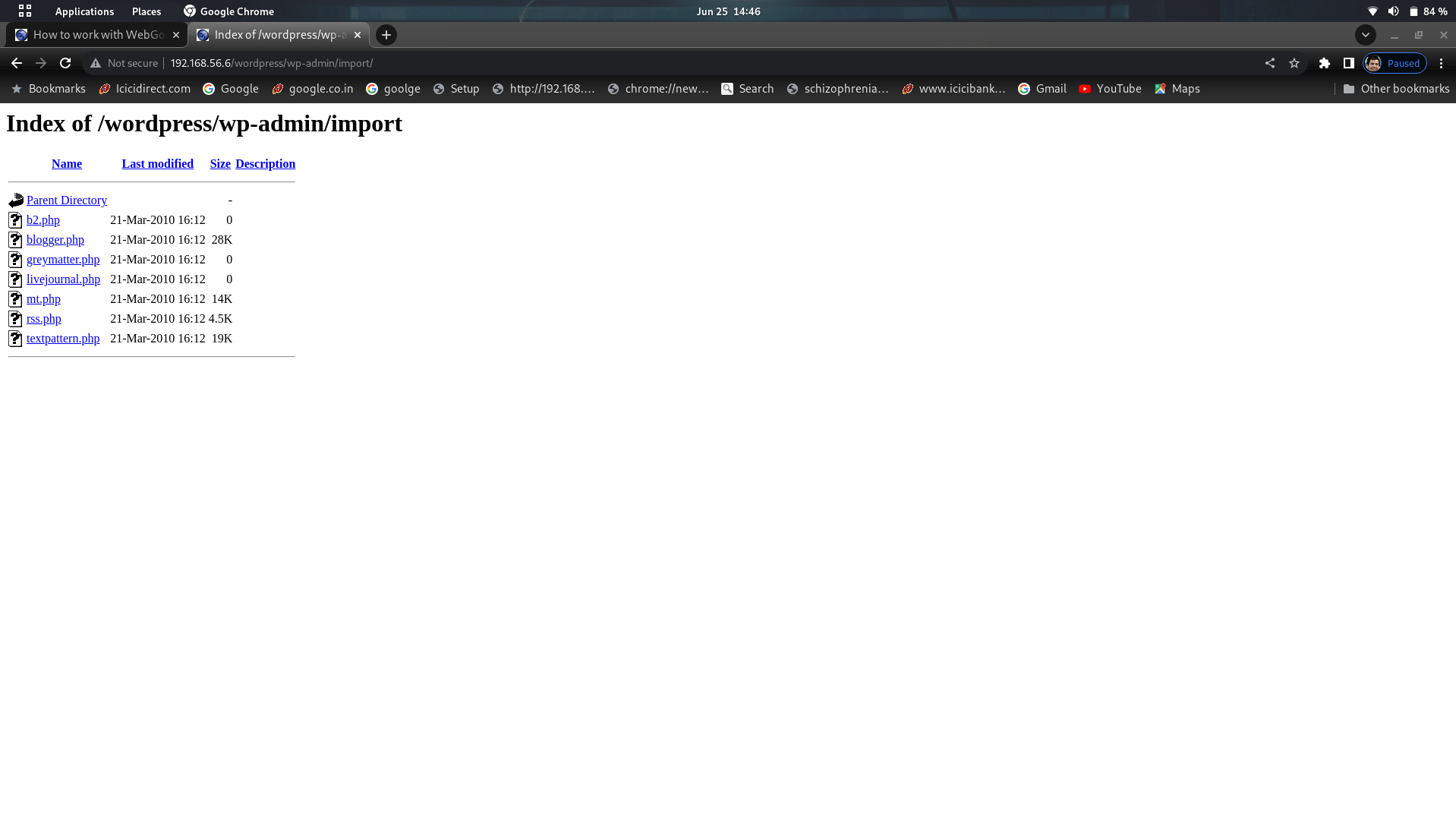
***Dirb*** *: DIRB is a command line based tool to brute force any directory based on wordlists.*



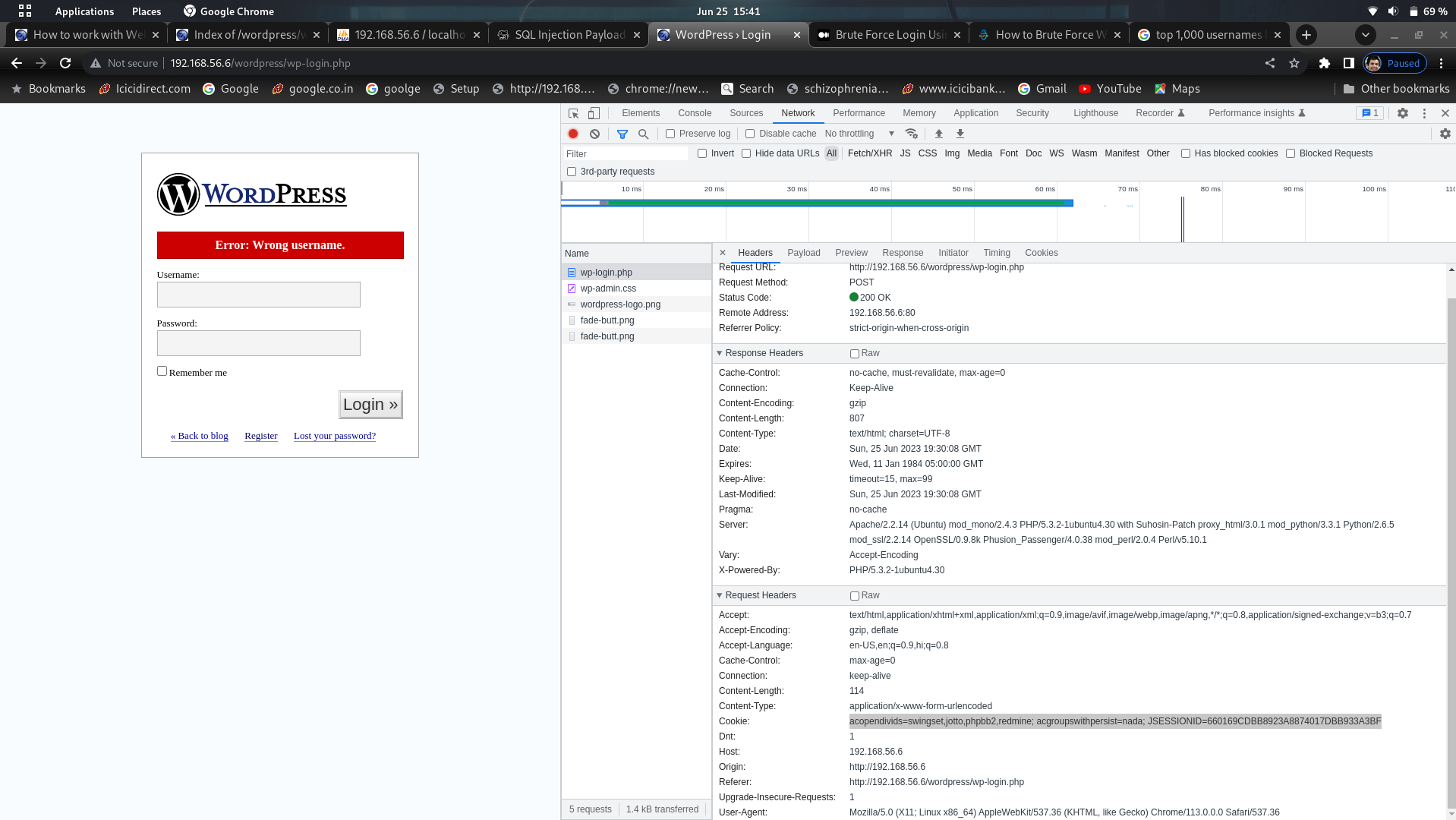
*Directories captured :*

* [*http://192.168.56.6/wordpress/wp-admin/*](http://192.168.56.6/wordpress/wp-admin/)
* [*http://192.168.56.6/phpmyadmin/index.php?*](http://192.168.56.6/phpmyadmin/index.php?)



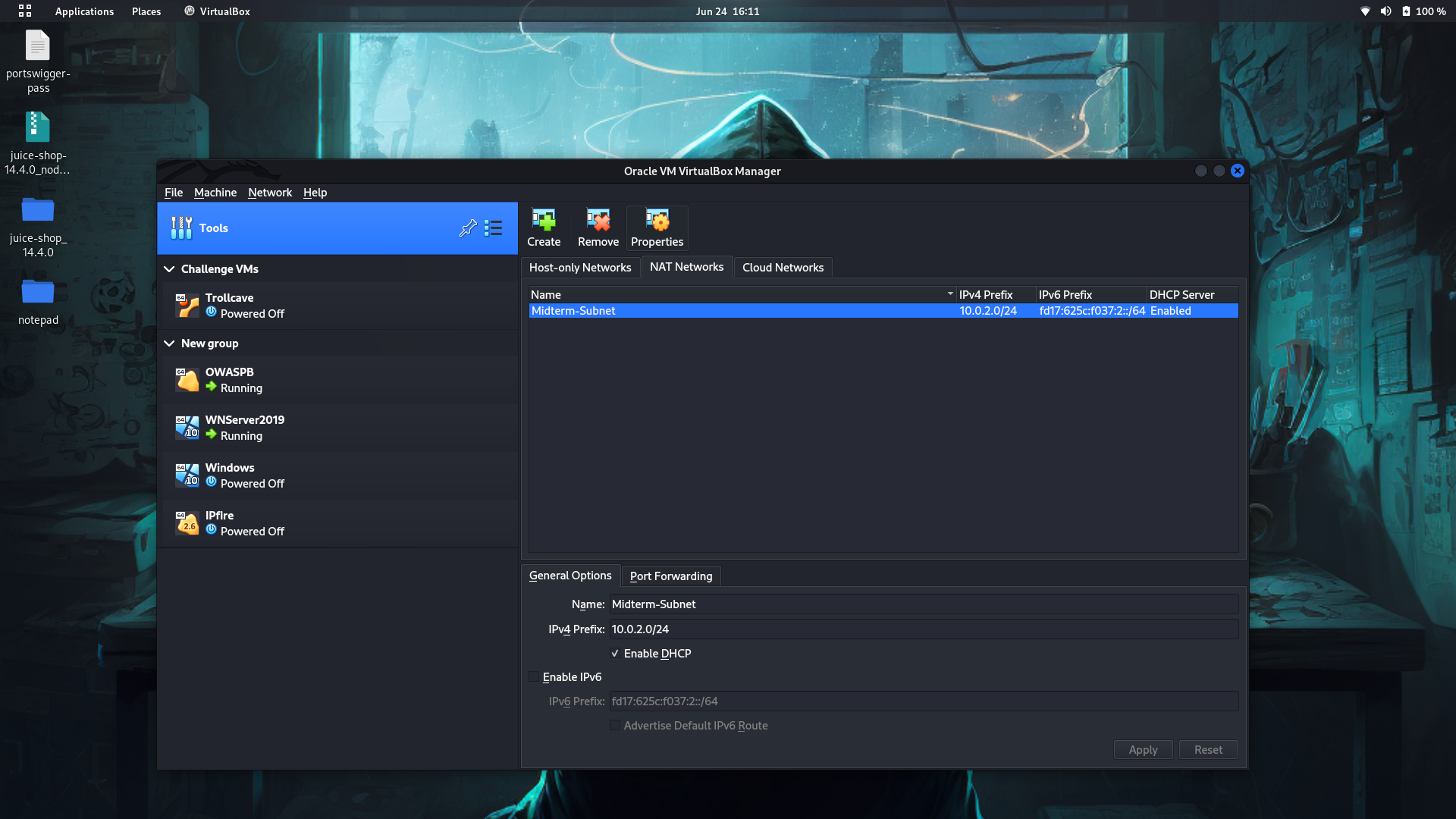


***Cookie found :***

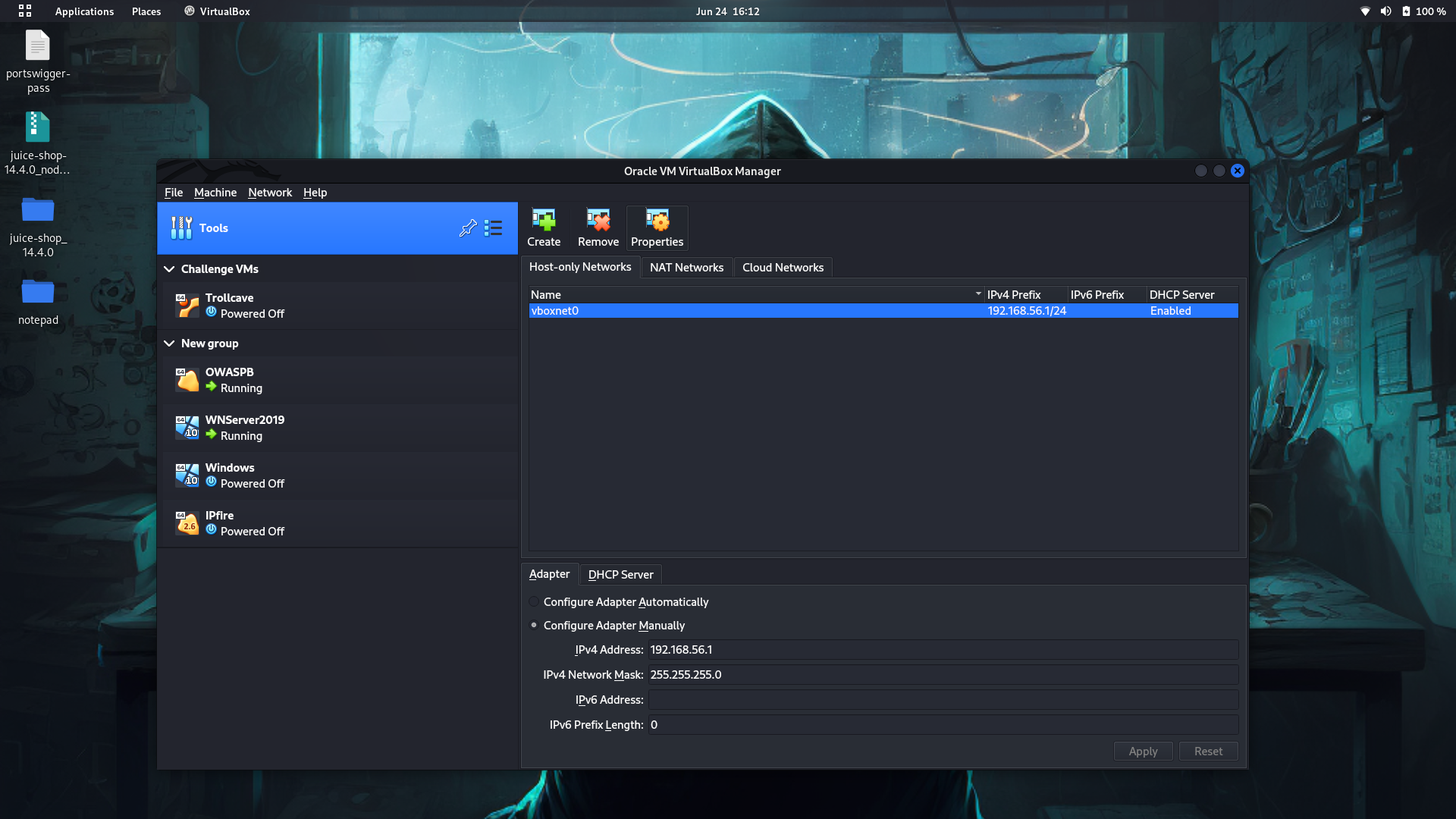


***Report***

*Step 1 : Creating a* ***NAT network*** *and* ***Host only Network*** *on virtualbox.*



*b.*

[[1]](#footnote-28856)

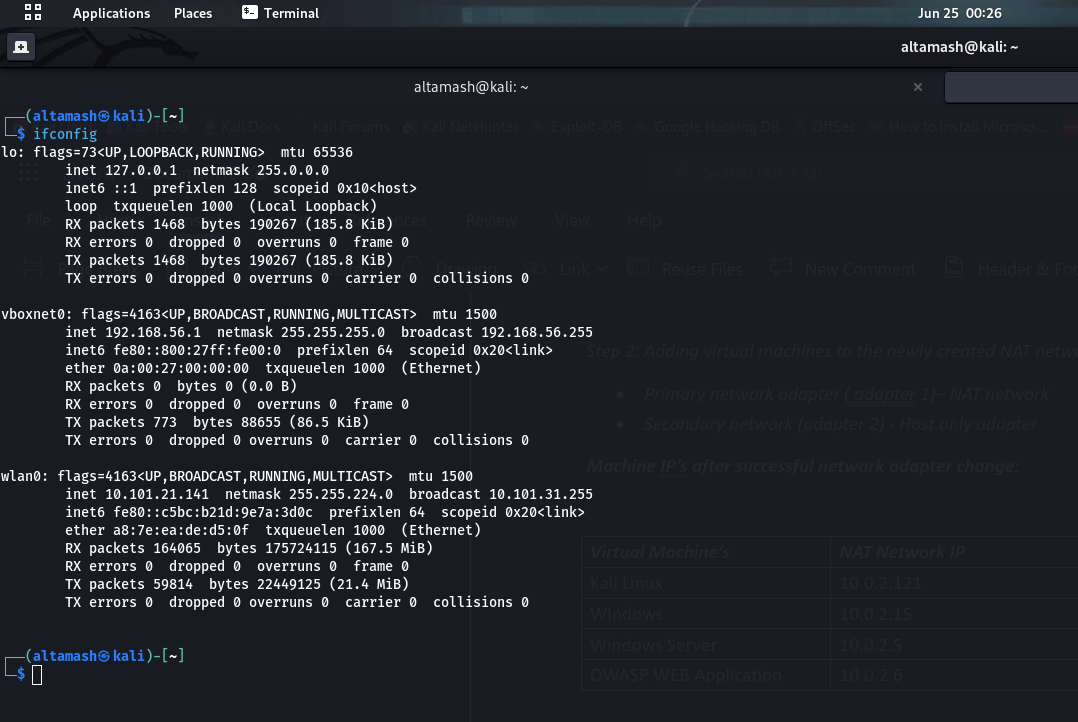
*Step 2: Adding virtual machines to the newly created NAT network and Host only Networks.*

* *Primary network adapter ( adapter 1)– NAT network*
* *Secondary network (adapter 2) - Host only adapter*

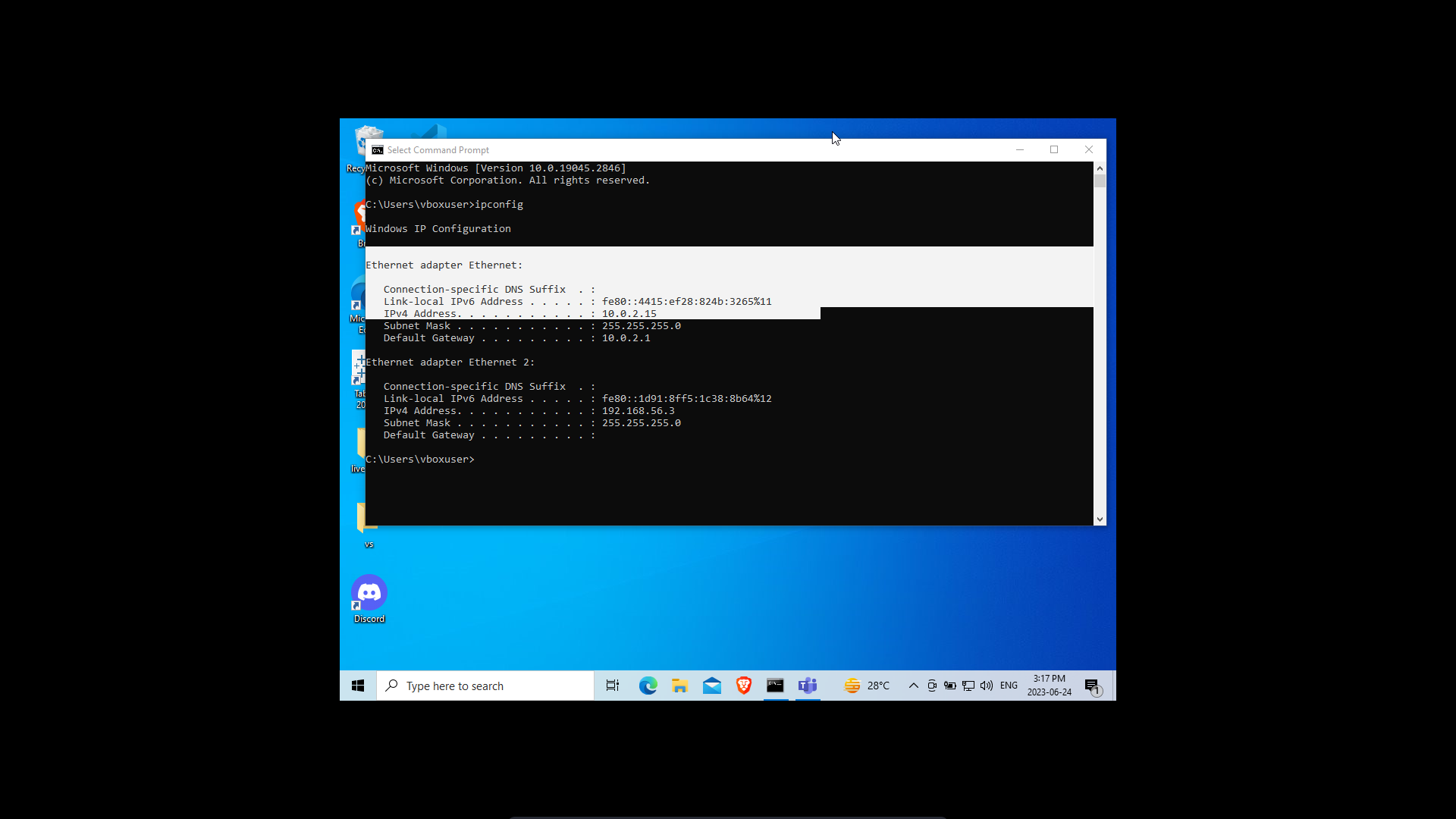
***Machine IP’s after successful network adapter change:***

|  |  |  |
| --- | --- | --- |
| ***Virtual Machine’s*** | ***NAT Network IP*** | ***Host only Network IP*** |
| Kali Linux | 10.0.2.121 | 192.168.56.1 |
| WIndows | 10.0.2.15 | 192.168.56.3 |
| Windows Server | 10.0.2.5 | 192.168.56.4 |
| OWASP WEB Application | 10.0.2.6 | 192.168.56.6 |

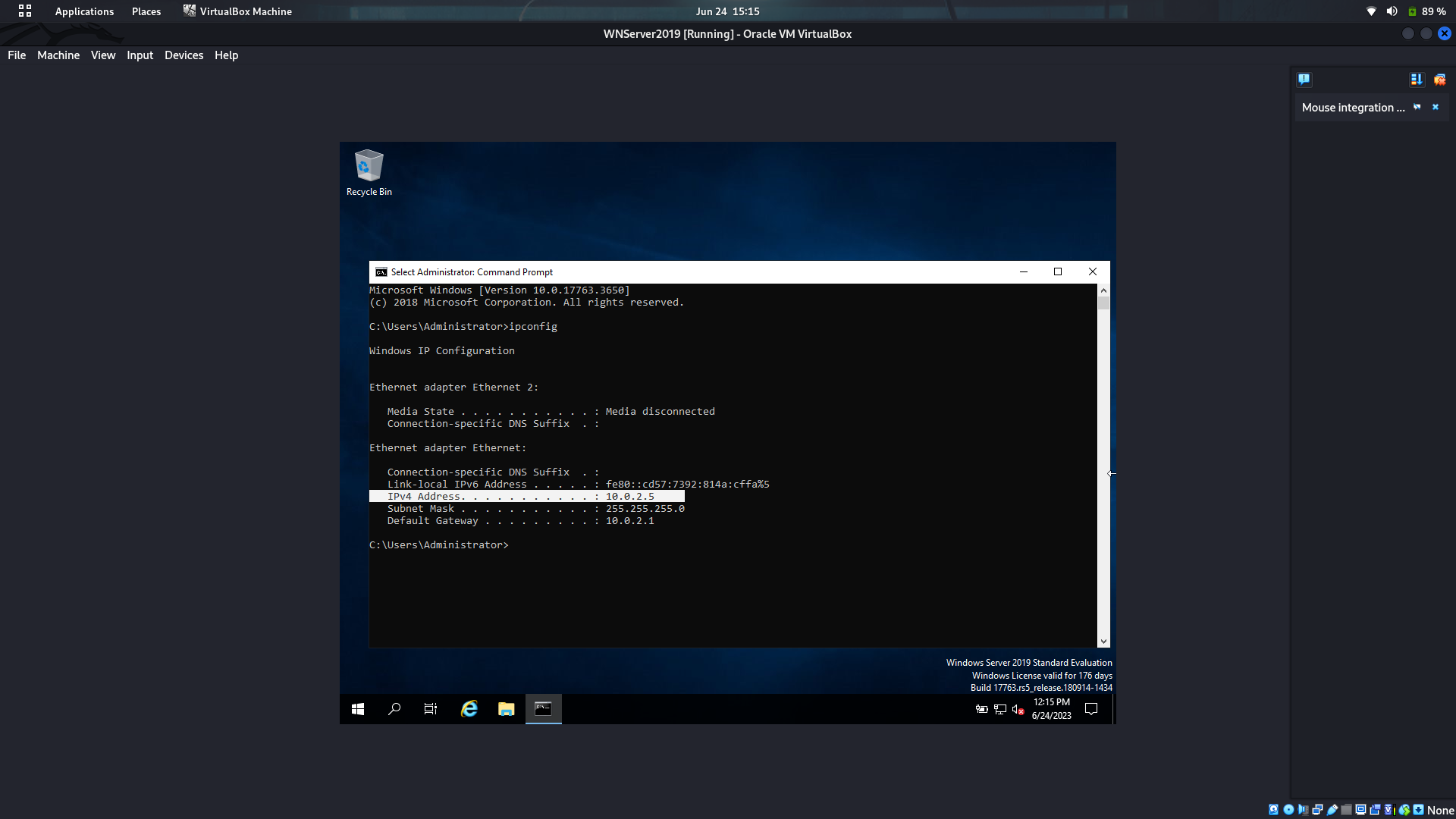
*A.*



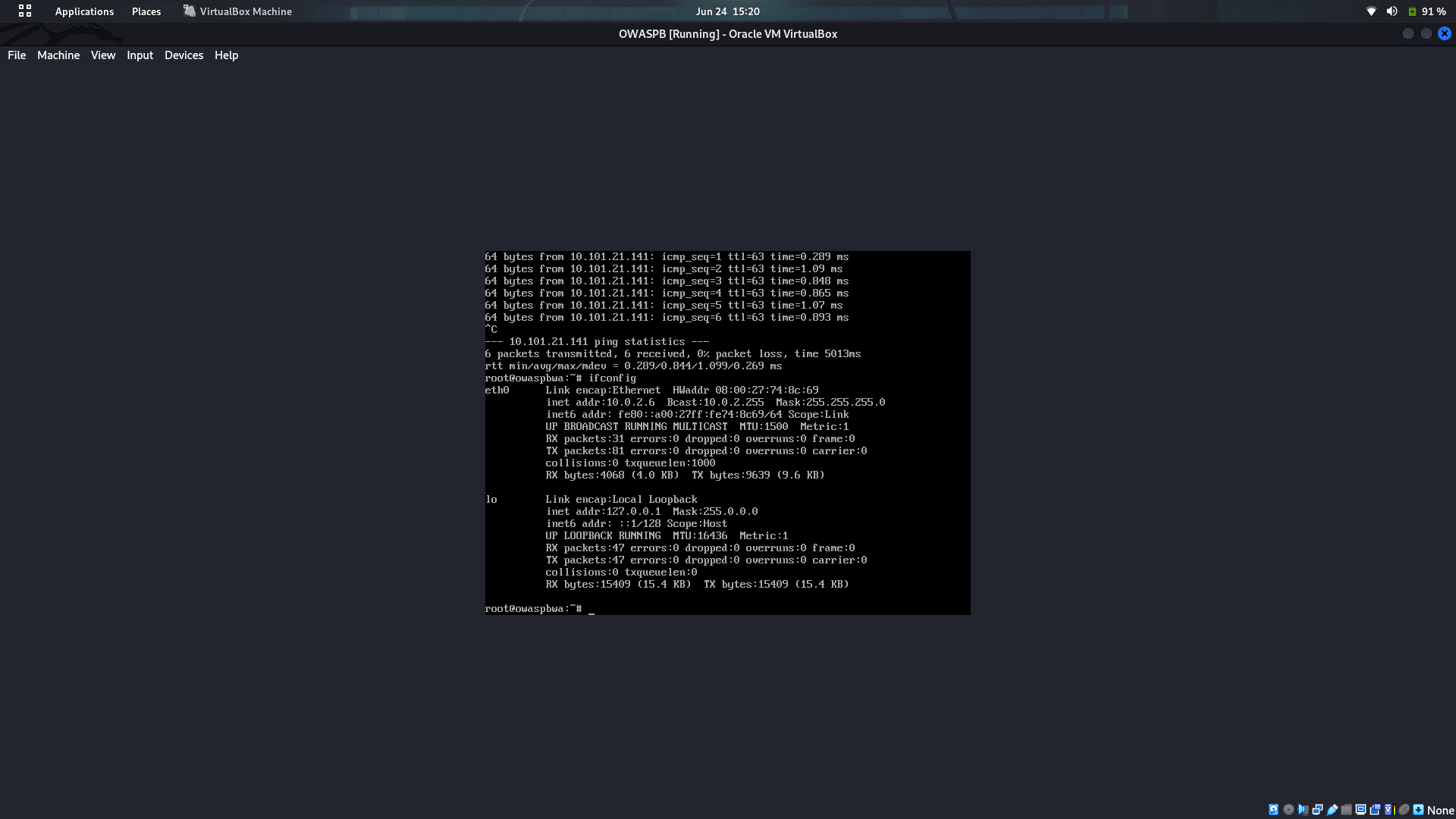
*B.*



*C.*



*D.*



***Step 3: Setting up FIrewall***

*PFSense firewall issue : Boot Loop*

***Corrupted file system*** *from* ***pfSense*** *resp.* ***freeBSD*** *which is the base from* ***pfSense****.*

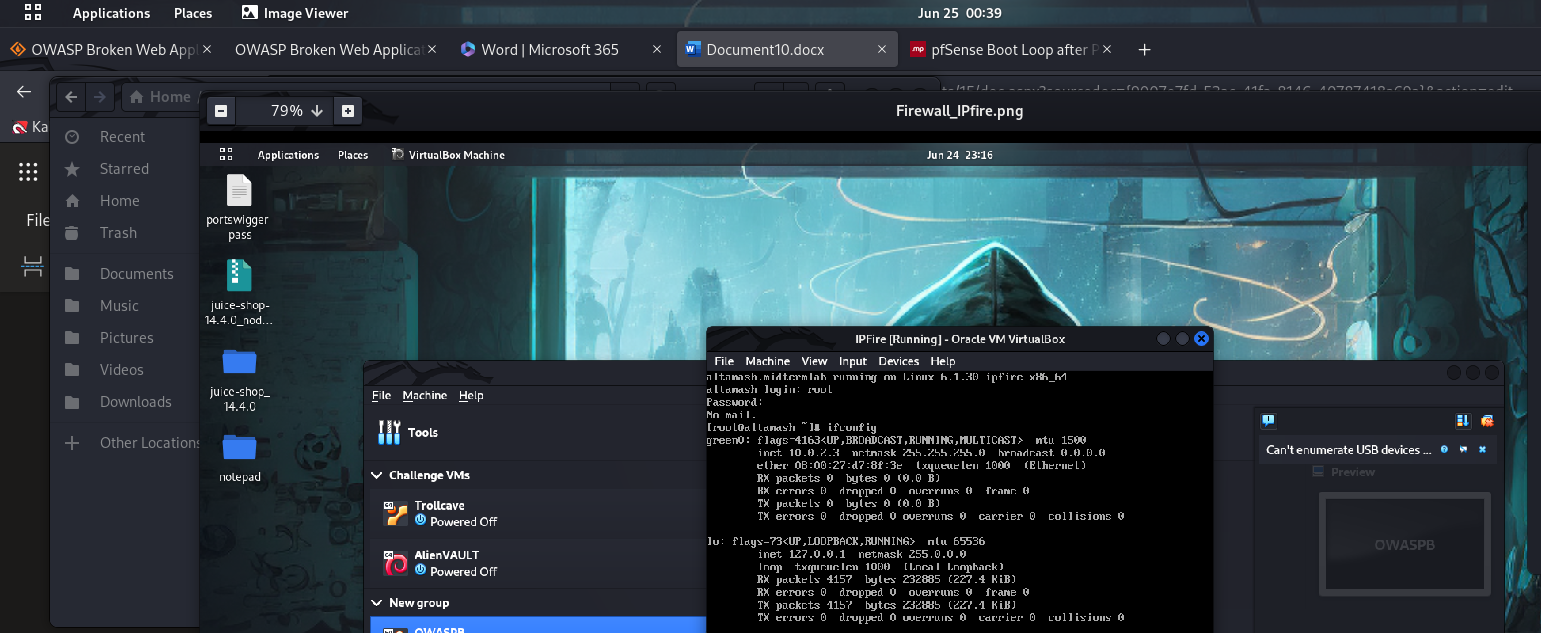
*In* ***pfSense 2.3.x*** *and before**the only filesystem type was* [***UFS***](https://en.wikipedia.org/wiki/Unix_File_System) *which unfortunately is prone to filesystem corruption after power loss.*

* *So, here I chose to run an alternative firewall called* ***“IPFire”***

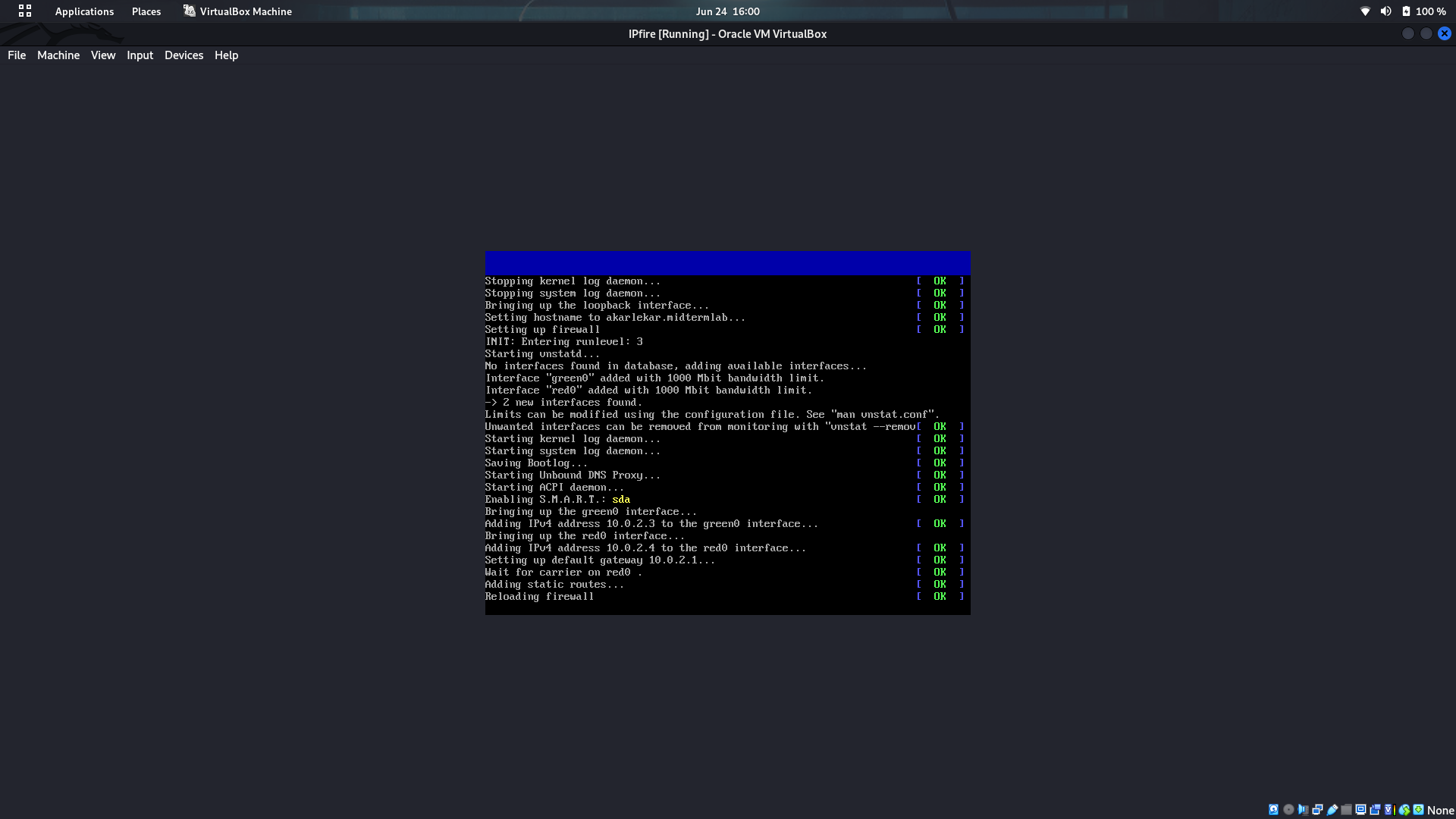
*Step 3.1:*

*Adding the NAT Network in* ***Green genre*** *and setting it’s IP to static “***10.0.2.3/24”**

*Adding the Host only adapter in* ***Red Genre*** *and setting it’s IP to static* **“192.168.56.8”**



*Step 3.2 : After successful configuration of Firewall, start the firewall on your designated networks.*



1. [↑](#footnote-ref-28856)