ITNE2002

Network & Information Security

Project Report

Contents

1. Introduction

In this report, I outline the creation and configuration of a secure network topology using three virtual machines: Kali Linux, Windows 10 and pfSense. These systems connected and positioned in a way so that they mimic a network of an enterprise level. The main reason behind it is that in such environment it is possible to install and try different measures of cybersecurity, starting with the settings of firewall, IDS, and ending with functioning of proxy filter. These tasks include using console to install services for instance Squid, Snort and ClamAV on the Pfense; perform security checks entailing Sweeping detection, port scanning and blacklisting of websites in order to gauge the effectiveness of the network.

That is why this configuration used to show the effectiveness of defensive tools in terms of combating frequent networks threats: Conducting practical security tests and shooting the result is an effective method to deepen the understanding of networks security measures.

2. Network Topology Implementation

Simplified topology is deployed in this work in the manner of three systems where each of them plays its own part in the created emulated network environment. The configuration of each of the virtual machine Further, the layout of the network topology is well configured and guarantees the ability to withstand the security challenges. While installing Kali Linux, Windows 10, and pfSense these three operating systems will ensure the creation of an environment to conduct cybersecurity tests safely away from the other operating systems on the computer.

2.1. Kali Linux Configuration

Kali Linux was configured with two network interfaces:

- **NAT (Network Address Translation**): This makes the VM to access the internet, and through the DHCP server to be assigned an IP address. The NAT interface serves as the path for Outside connection for software update and remote network benchmarking.
- **intNet (Internal Network):** The second interface of this switch is configured and set with an IP address of 192.168.100.100/24 Subnet Mask 255.255.255.0. This is an internal phase where emulation of attacks through the local network is performed, which targets mainly the Windows 10 VM and the pfSense firewall.

This means that Kali Linux can directly access outside services for updates or other external scanning tools while it can launch internal network attack at the same time without putting the internal network in a vulnerable position of outsiders' attack.

2.2. Windows 10 Configuration

Windows 10 was configured similarly, with two network interfaces:

- **intNet (Internal Network)**: Another particular interface named internal network interface was manually configured with an IP address of 192.168.100.101/24 which has same subnet as Kali Linux. This will make Windows 10 VM to be on the internal network where it can interact with Kali Linux as well as the pfSense.
- **Proxy Setup:** The proxy for the Windows 10 VM was assigned to be 192.168.100.1/24 of the pfSense. This proxy configuration secures all outbound traffic from Windows 10 to pass through the Squid to do content filtering or blacklisting.

The system used here as the target system with the current state simulating a user device on Windows 10, will help test network attack scenarios and countermeasures completely.

2.3. pfSense installation and Configuration

The main security system of this topology was chosen to be pfSense it is a free open source firewall/router operating system because of its security features that include stateful packet filtering, intrusion, and proxy.

Installation steps:

Download the pfSense ISO:

We obtained the pfSense installation file from the official website of pfSense. Perhaps, the fact that the ISO file can be used with VirtualBox enabled us to install the firewall using Virtual Machine mode.

Create a Virtual Machine for pfSense:

- I launched VirtualBox and went to the “New” button where we created a new virtual machine.
- The VM was given the name of ‘pfSense’; for the OS type we tagged it as ‘BSD/FreeBSD ‘64-bit’.
- I provisioned at least 1 GB of RAM and 10 GB of storage to the VM.

Attach the pfSense ISO:

- In the VM settings, under "Storage," we selected "Controller: thinks is IDE and then attached the downloaded pfSense ISO to installation as a virtual optical disk.

We ensured the VM had two network adapters:

pfSense, the central element of the topology, was installed with two network interfaces:

- **NAT:** Unlike Kali Linux, this interface serves pfSense to access internet for update and for traffic flow control.
- **intNet (Internal Network**): Another change which was done manually at the internal network interface for IPv4 IP address was 192.168.100.1/24 requirement of subnet mask 255.255.255.0. Being a default connection point for the internal network, pfSense performs firewall state, check IDS and proxy filtering on the traffic between Kali Linux and Windows 10.

Most of the VOIP traffic, internal access, and file sharing is available within internal network and hence pfSense is configured as the internal firewall and router because all the traffic must pass through it and it shall enforce the security measures.

Install pfSense:

- I turned on the VM and chose to boot from the installed pfSense ISO file.
- Just like any other installation, we followed the installation prompts to install pfSense on the virtual disk that was created.

- After installation, I assigned the interfaces: The second Ethernet type is WAN (connected to NAT) and LAN (connected to the internal network).
- I configured the LAN IP address to static as 192.168.100.1/24.

3. Installing Software on pfSense

Additionally, boosting pfSense even further, the installation and setting up of the following core services has added layers of security such as web filtering, intrusion detection, and the scanning of malware.

3.1. Squid Installation

Squid is a strong proxy server on pfSense which controls all web connection for internal wired and wireless network. As it was described above, Squid works as an intermediary that blocks some websites according to rules determined by a user. For this project, Squid was made to deny www.facebook.com from the Windows 10 VM.

Installation steps:

1. Go to package manager of pfSense.

2. To do this you need to download (apt-get) available package options then install Squid from this selection.

3. Set Squid to filter web traffic to 192.168.100.101 which is a Windows 10 machine and use filters to block out certain sites.

3.2. Snort Installation

Snort the powerful IDS software was incorporated into the appliance to aid its capability to detect the network based attacks. One of its abilities is traffic analysis of internal network and informs the user about such matters as ping sweeps or port scanning etc.

Installation steps:

1. Use the command line in pfSense and go to the package manager.

2. Download the Snort package from the package repository to install.

3. Start Snort to analyze the traffic in the internal network 192.168.100.0/24 and to use rules for the indication of dangerous traffic.

3.3. ClamAV Installation

ClamAV is a free antivirus service that can be implemented as a mail gateway, viruses scanner and more. Upon ins titution on pf Sense, Clam AV scans entrance traffic for malicious contents in addition to the firewall and IDS.

Installation steps:

1. To install ClamAV, go to the package manager of pfSense and download ClamAV.

2. Set up all incoming traffic to be automatically scanned so that any attempts to ‘slip through’ the firewalls will be met with an alert that they are infected by a virus.

3.4. Firewall Configuration

With pfSense, firewalls were set to restrict certain kinds of traffics for instance, ICMP traffics from Kali Linux to Windows 10. This gives an opportunity to evaluate firewall performance with regard to denial of communication on the network.

4. Executing Tests and Outputs

The last thing done in the network configuration, and we need to install some software and perform some test to optimize the network security. These tests where done by performing different kind of attacks using Kali Linux and on the other end, pfSense to defend against them.

4.1. Ping Sweep Detection Using Snort

From the Kali Linux, a ping sweep to pfSense and Windows 10 was conducted to determine all active hosts on internal network. Ping sweep was also performed and as expected snort was able to detect it and produce an alert showing that snort does indeed have an intrusion detection ability.

Result: Ping sweep was identified by Snort and there were alerts raised. This proved that Snort can be used to detect network reconnaissance in progress for one, due to the single occurrence.

4.2. Blocking Facebook Using Squid

Squid was set up to deny users in the Windows 10 VM from accessing www.facebook.com. After doing the proxy configuration, anytime I tried accessing Facebook from the Windows machine, I was successfully blocked, this affirmed the fact that the proxy filtering rules where well and alive.

Result: For the Windows 10 VM, the Squid proxy was also configured to block the access to www.facebook.com, which clearly shown that the proxy-base web filtering works efficiently.

4.3. Port Scanning with Nmap

A port scan and OS detection on the Windows 10 VM was conducted with Nmap from the Kali Linux distribution. The following ports were identified as open:

1. Port 80 (HTTP):

This port shows that there is a web service for the operating system that is Windows 10. Although this is frequent, Web connections using unsegmented HTTP can be vulnerable to numerous techniques such as Man in the Middle Attack (MITM). They advise that either this service be turned off or that it be replaced with HTTPS.

2. Port 135 (RPC):

Remote Procedure Call is a core process employed by Windows for making procedures that are present in one process available to other processes. But it is frequently used by hackers motivated by possibilities to execute code from a remote environment or perform DDoS attacks.

3. Port 139/445 (NetBIOS/SMB):

They assist Windows to support services for file sharing. SMB and NetBIOS are most often attacked by cybercriminals, using such a hole as EternalBlue, through which the notorious WannaCry virus spread. It is suggested to close these ports or secure them by means of a powerful authentication.

4. Port 3389 (RDP):

Remote Desktop Protocol (RDP) is used for remote accessing the Windows system. That is why it is considered a high risk service if exposed since the service can be targeted with brute force attacks. It is essential to limit the ability to access it and to use a VPN or have a strong authentication type for this service.

Result: All the open ports had been as listed and it had been ensured that the open services had been closed or protected. Nmap scan also proved by showing that desired ports were closed successfully as well as the other extra unnecessary ports were closed.

4.4. Blocking Ping Messages Using pfSense Firewall

The pfSense firewall was configured to deny Kali Linux to send ping messages to Windows 10. The following result was obtained after the firewall rule was successfully applied, whereby all ping attempts emanating from Kali Linux were successfully dismissed by the firewall thereby affording evidence of the effectiveness of the firewall in deterring network probing.

Result: Packets such as the ICMP (ping) messages from Kali to Windows 10 were prevented showing how firewall works on controlling traffic on the network.

5. Conclusion

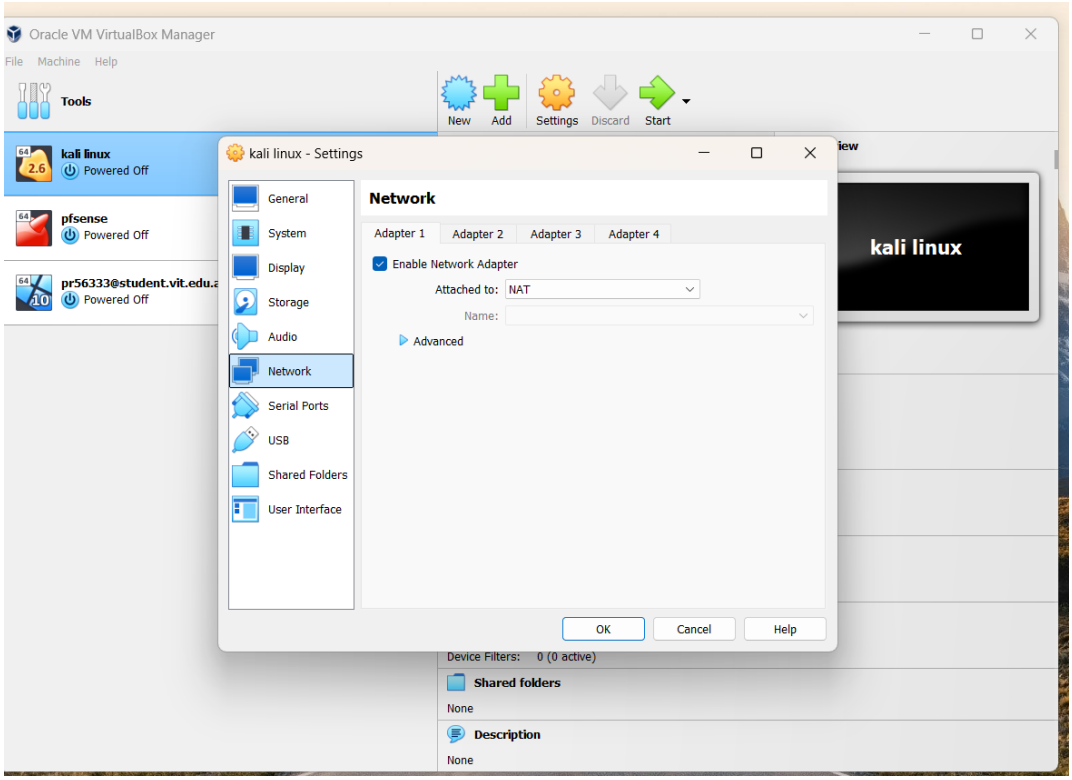
The specifically configured network architecture using the Kali Linux, Windows 10 and pfSense created a perfect environment for assessing the resilience of the networks. That is why, through the use of Squid, Snort, ClamAV, and firewalls settings the network was protected against several sorts of threats. The conducted examinations – ping sweep detection, web traffic filtering, and port scans – showed how well the abovementioned security measures work.

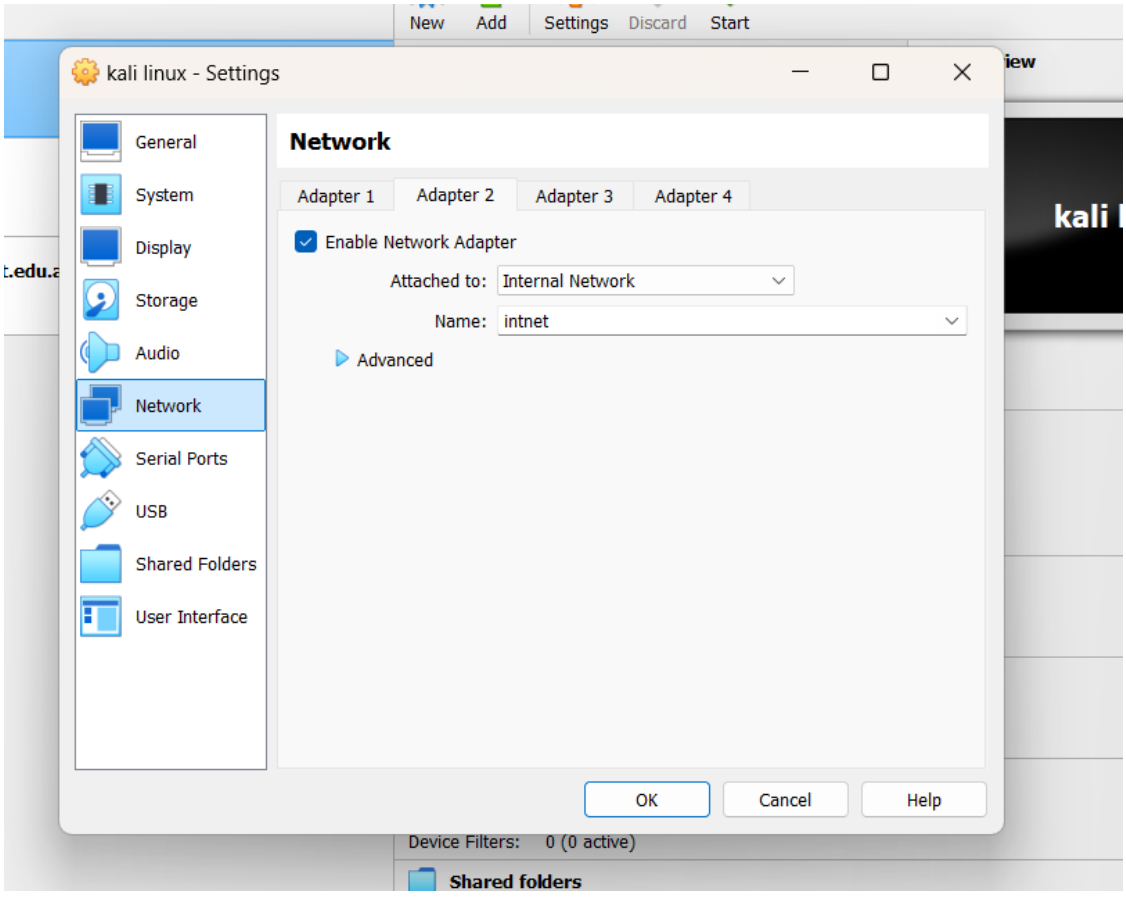
This project raises awareness of the value of different layers in network security since one tool is sufficient to guard against various threats.

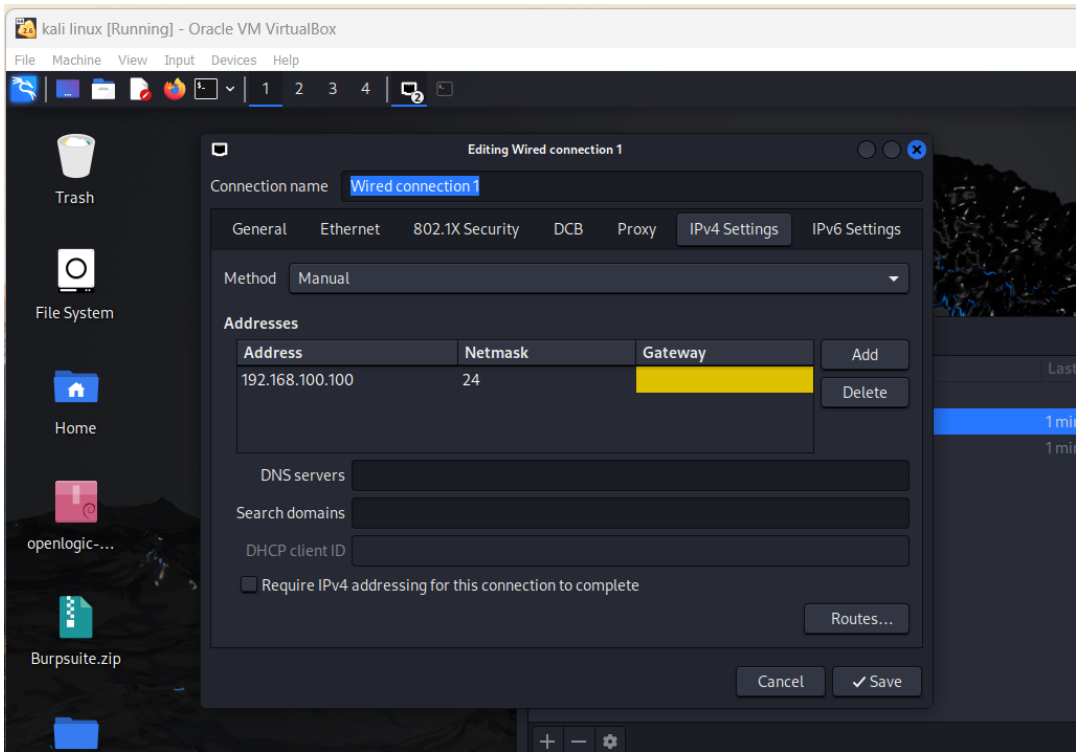
Screenshots

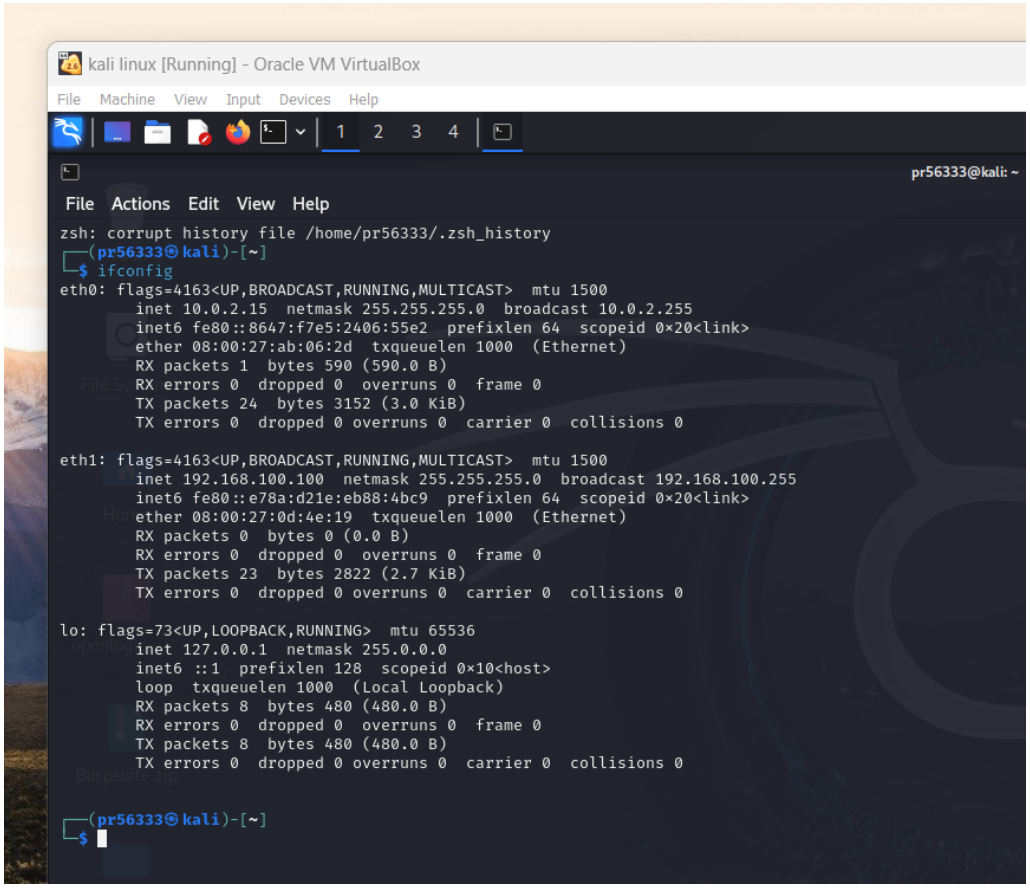
Network Topology

Kali-Linux

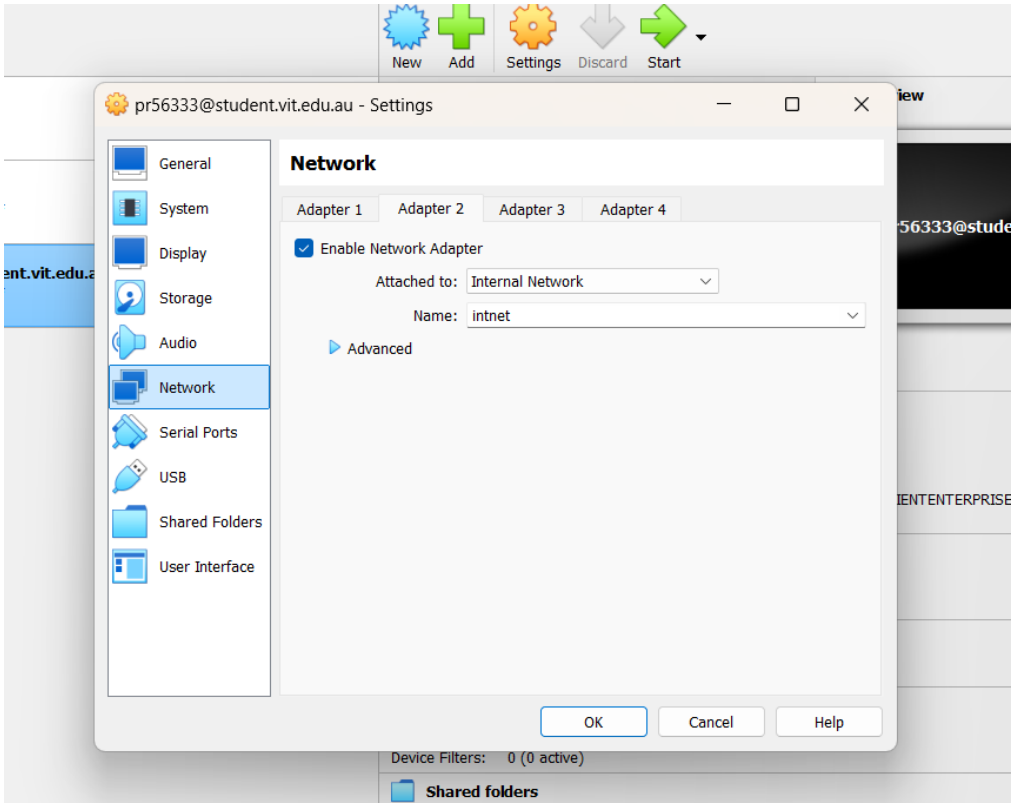


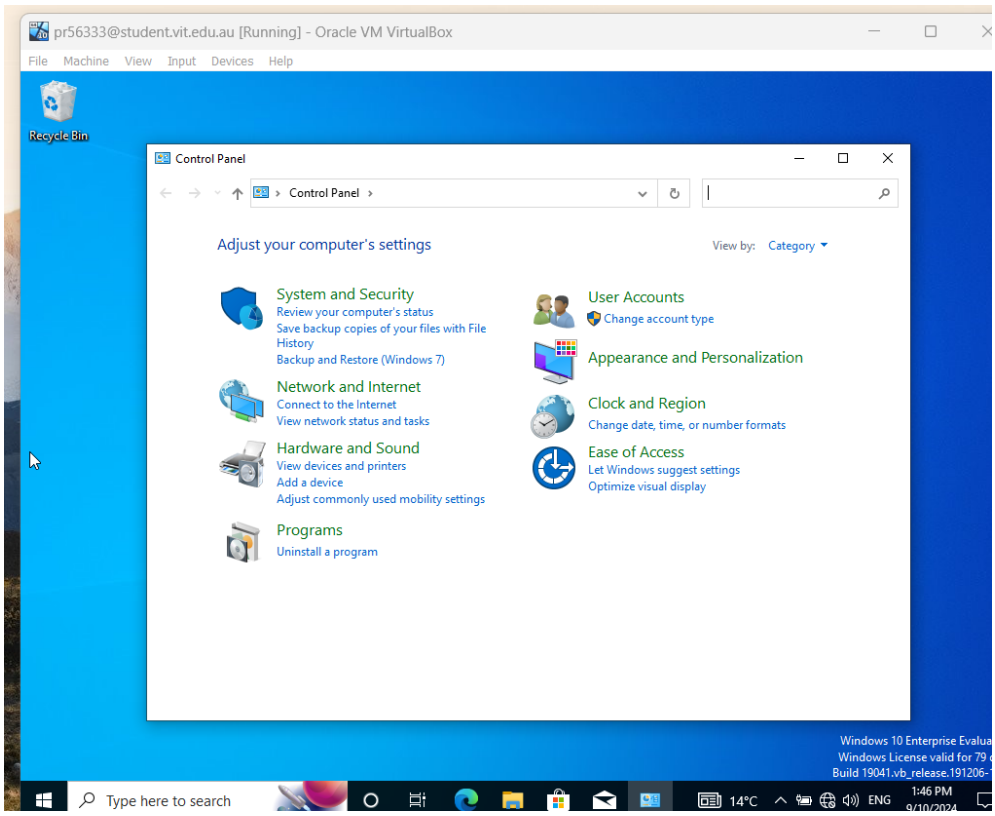


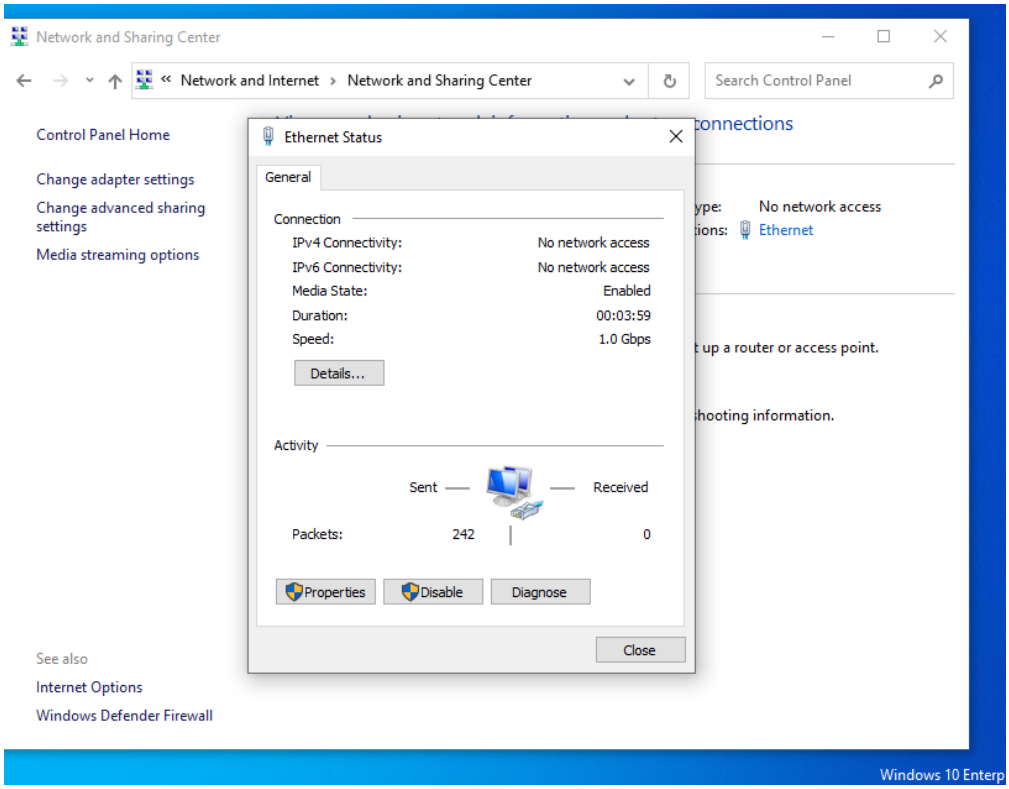

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
openlogic-...
Burpsuite.zip
Editing Wired connection 1
Connection name
Wired connection 1
General
Ethernet
802.1X Security
DCB
Proxy
IPv4 Settings
IPv6 Settings
Method
Manual
Addresses
Address
Netmask
Gateway
192.168.100.100
24
Add
Delete
DNS servers
Search domains
DHCP client ID
Require IPv4 addressing for this connection to complete
Routes...
Cancel
Save

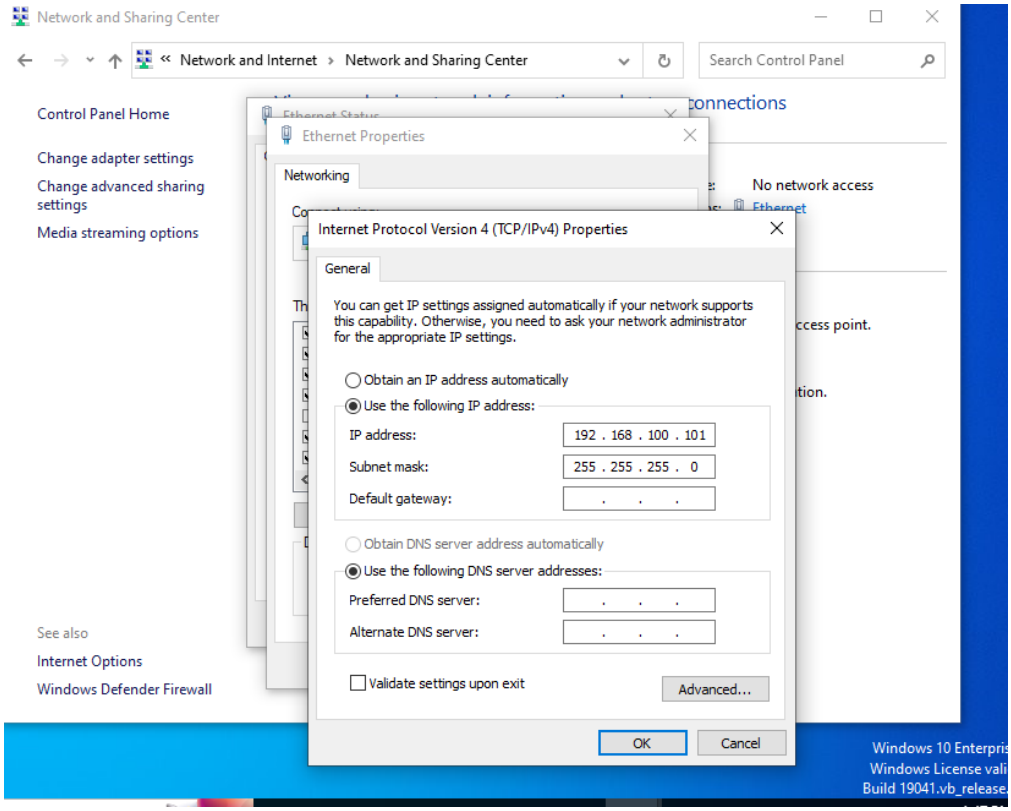

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pr56333@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/pr56333/.zsh_history
(pr56333㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::8647:f7e5:2406:55e2 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:ab:06:2d txqueuelen 1000 (Ethernet)
RX packets 1 bytes 590 (590.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 3152 (3.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.100.100 netmask 255.255.255.0 broadcast 192.168.100.255
inet6 fe80::e78a:d21e:eb88:4bc9 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:0d:4e:19 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 23 bytes 2822 (2.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(pr56333㉿kali)-[~]
$

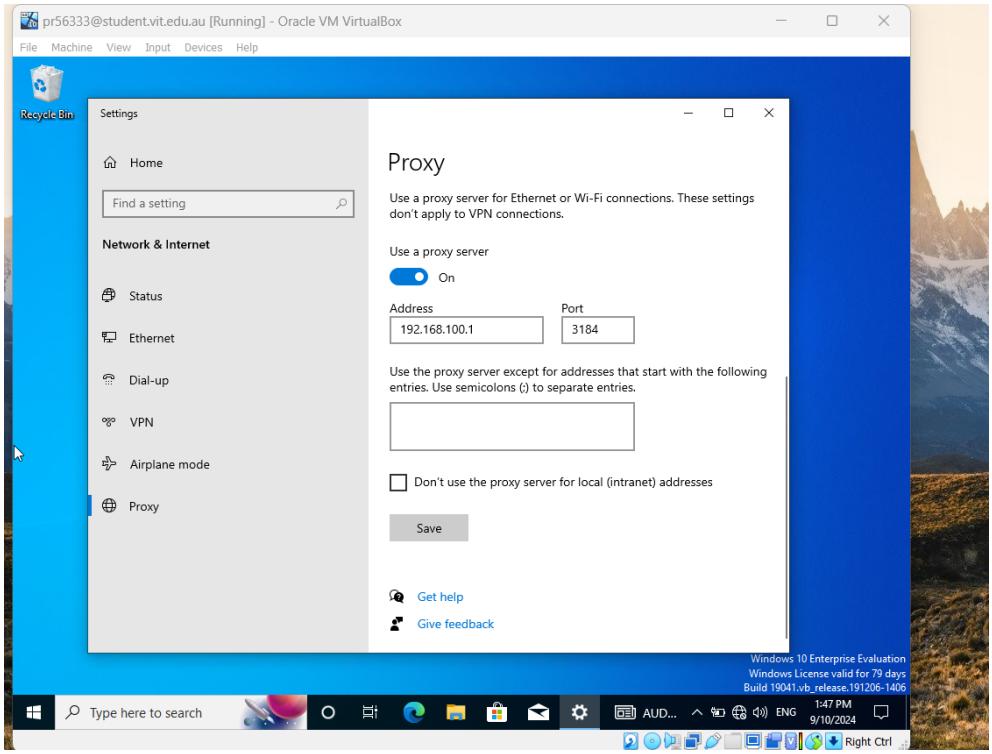
Windows

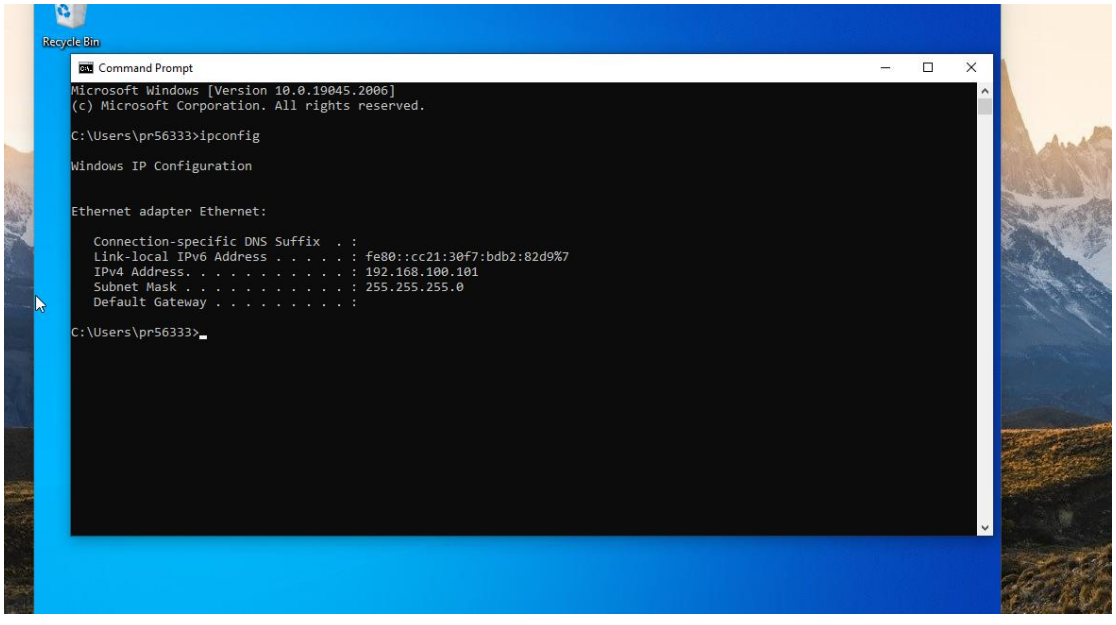

New
Add
Settings
Discard
Start
pr56333@student.vit.edu.au - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
intnet
Advanced
OK
Cancel
Help
Device Filters: 0 (0 active)
Shared folders


pr56333@student.vit.edu.au [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
Connect to the Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display
Type here to search
14°C
ENG
1:46 PM

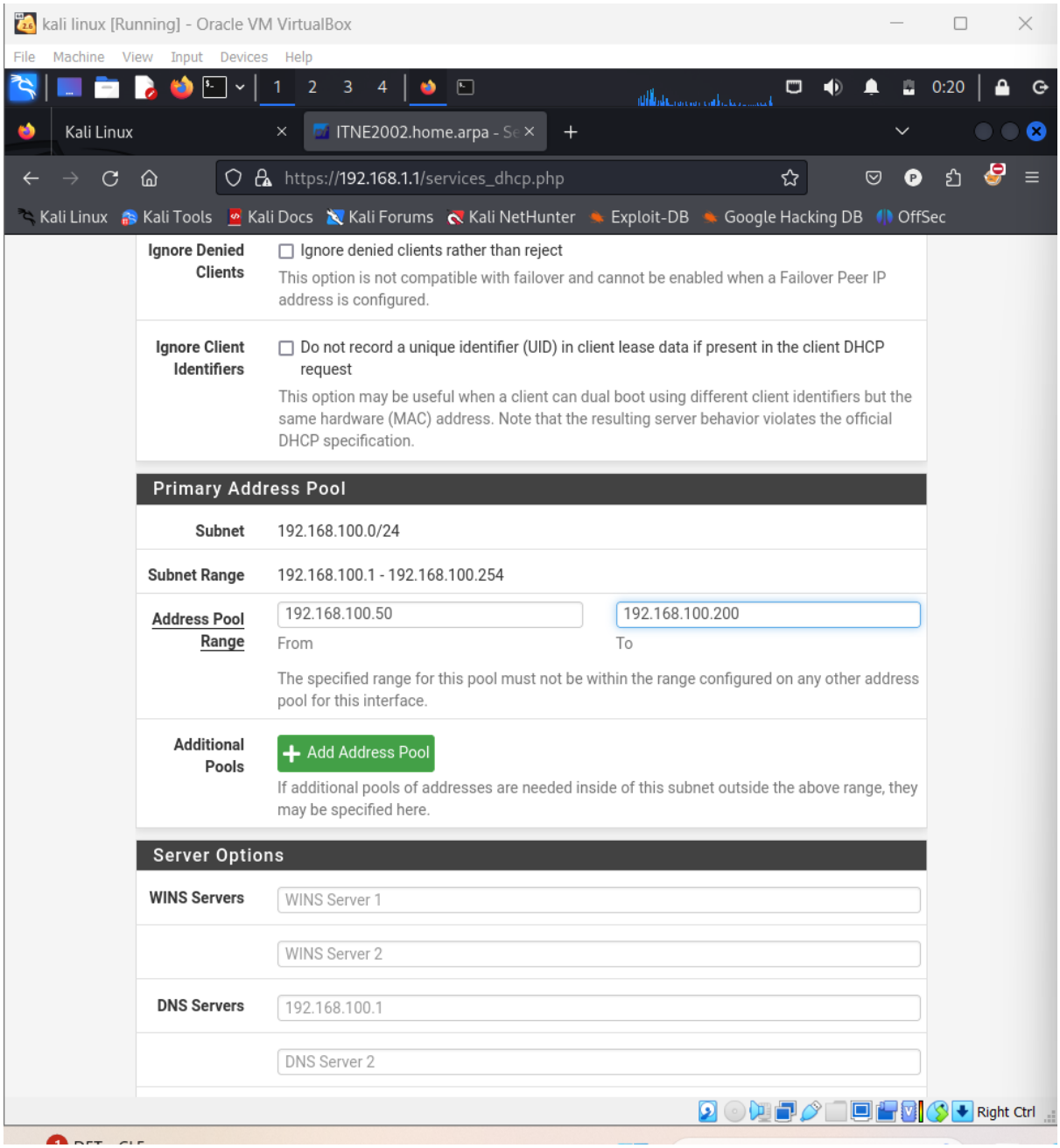

Network and Sharing Center
Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
Ethernet Status
General
Connection
IPv4 Connectivity: No network access
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:03:59
Speed: 1.0 Gbps
Details...
Activity
Sent
Received
Packets: 242 0
Properties
Disable
Diagnose
Close
See also
Internet Options
Windows Defender Firewall

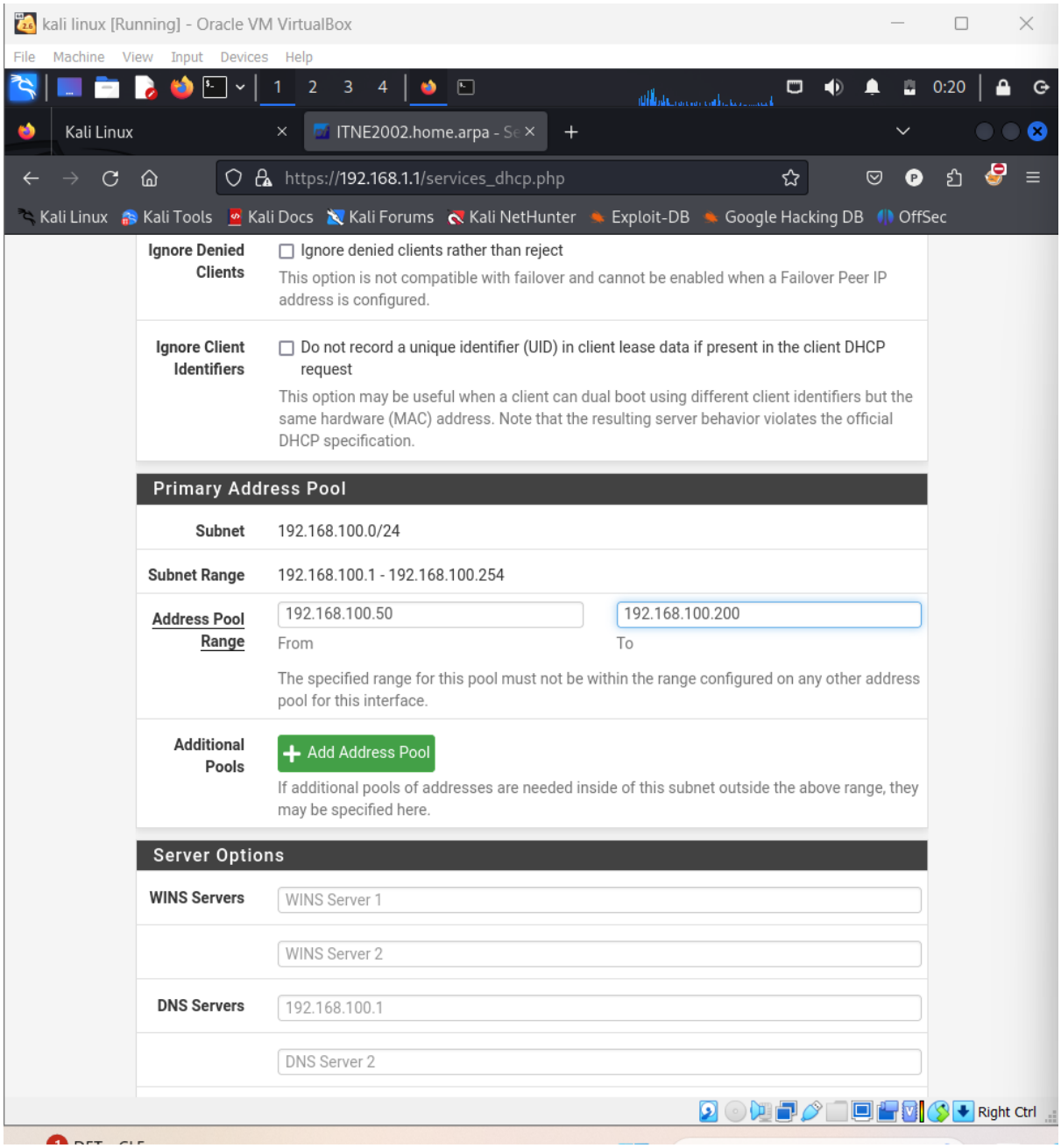

Network and Sharing Center
Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
Ethernet Properties
Networking
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 100 . 101
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
See also
Internet Options
Windows Defender Firewall

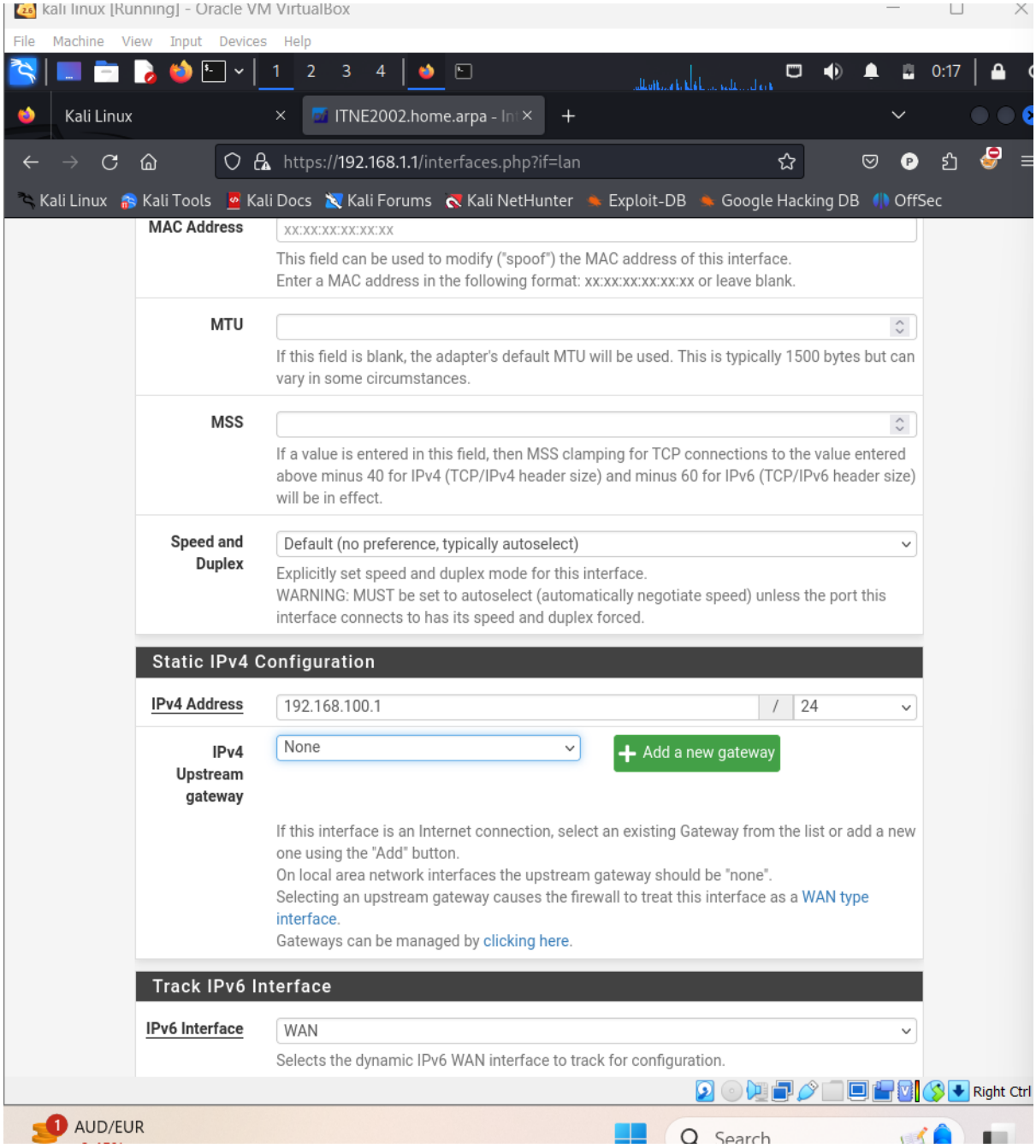

pr56333@student.vit.edu.au [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Airplane mode
Proxy
Proxy
Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.
Use a proxy server
On
Address
192.168.100.1
Port
3184
Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries.
Don't use the proxy server for local (intranet) addresses
Save
Get help
Give feedback
Windows 10 Enterprise Evaluation
Windows License valid for 79 days
Build 19041.vb_release.191206-1406
Type here to search
AUD...
ENG
1:47 PM
9/10/2024
Right Ctrl

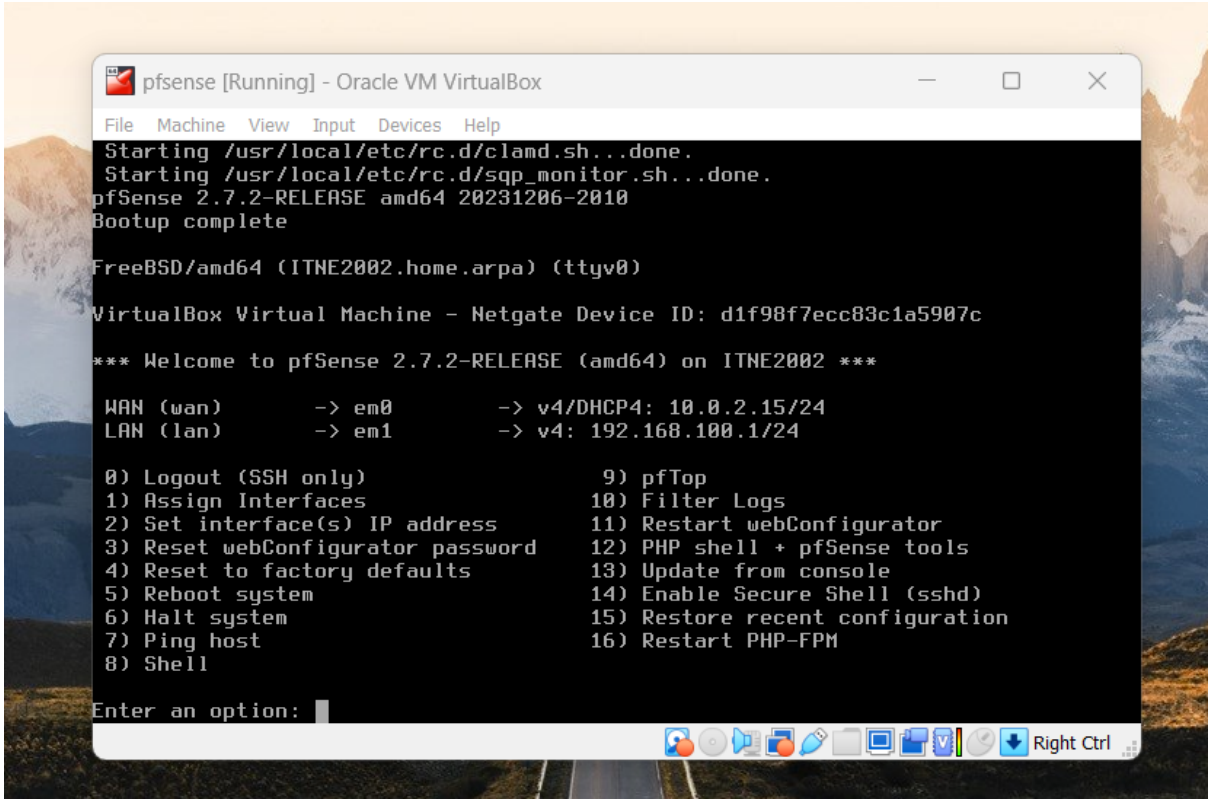

Recycle Bin
Command Prompt
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.
C:\Users\pr56333>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::cc21:30f7:bdb2:82d9%7
IPv4 Address. . . . . : 192.168.100.101
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
C:\Users\pr56333>

Pfsense

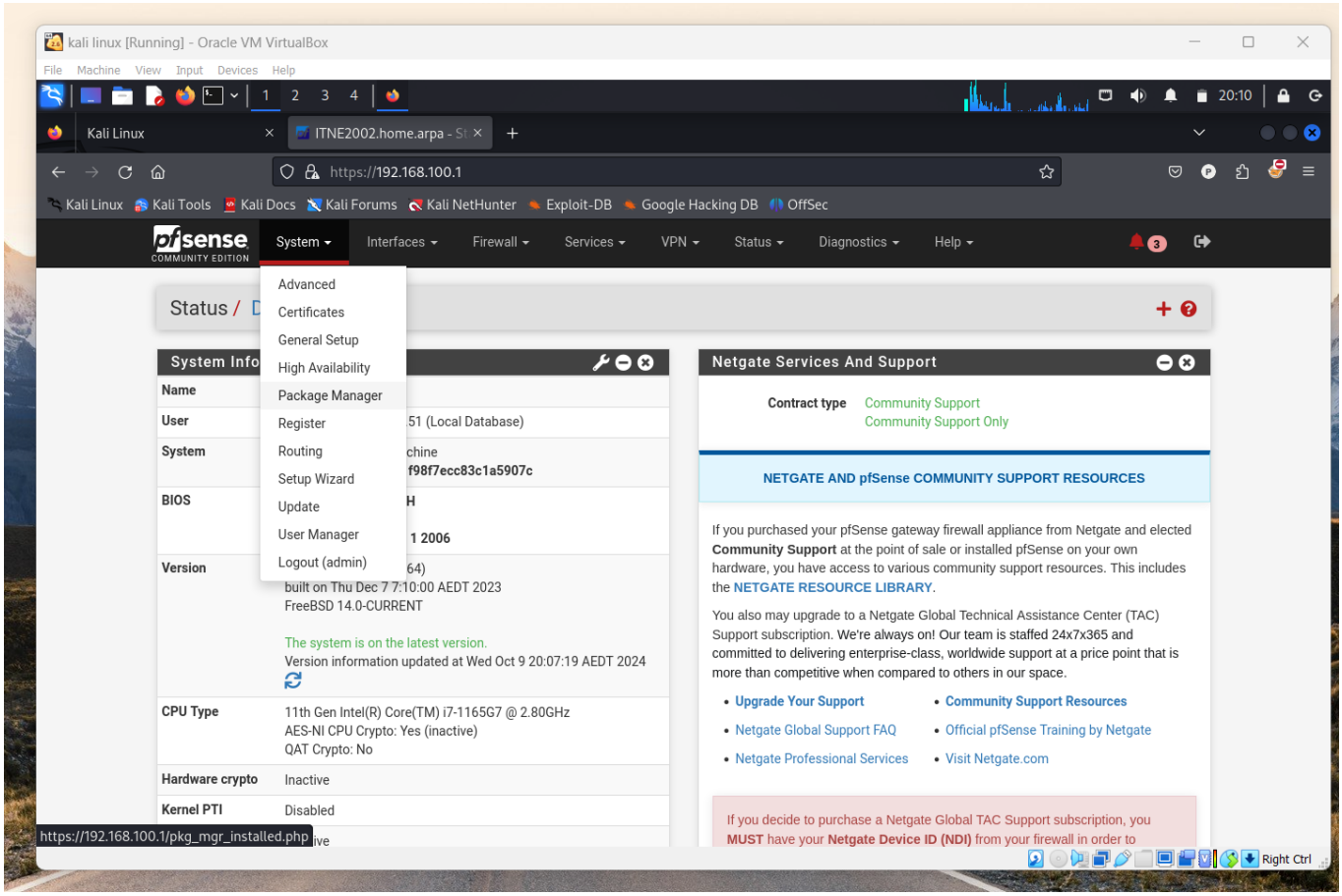

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
ITNE2002.home.arpa - Se
https://192.168.1.1/services_dhcp.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Ignore Denied Clients
Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers
Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Primary Address Pool
Subnet
192.168.100.0/24
Subnet Range
192.168.100.1 - 192.168.100.254
Address Pool Range
192.168.100.50
From
192.168.100.200
To
The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools
Add Address Pool
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.
Server Options
WINS Servers
WINS Server 1
WINS Server 2
DNS Servers
192.168.100.1
DNS Server 2
Right Ctrl

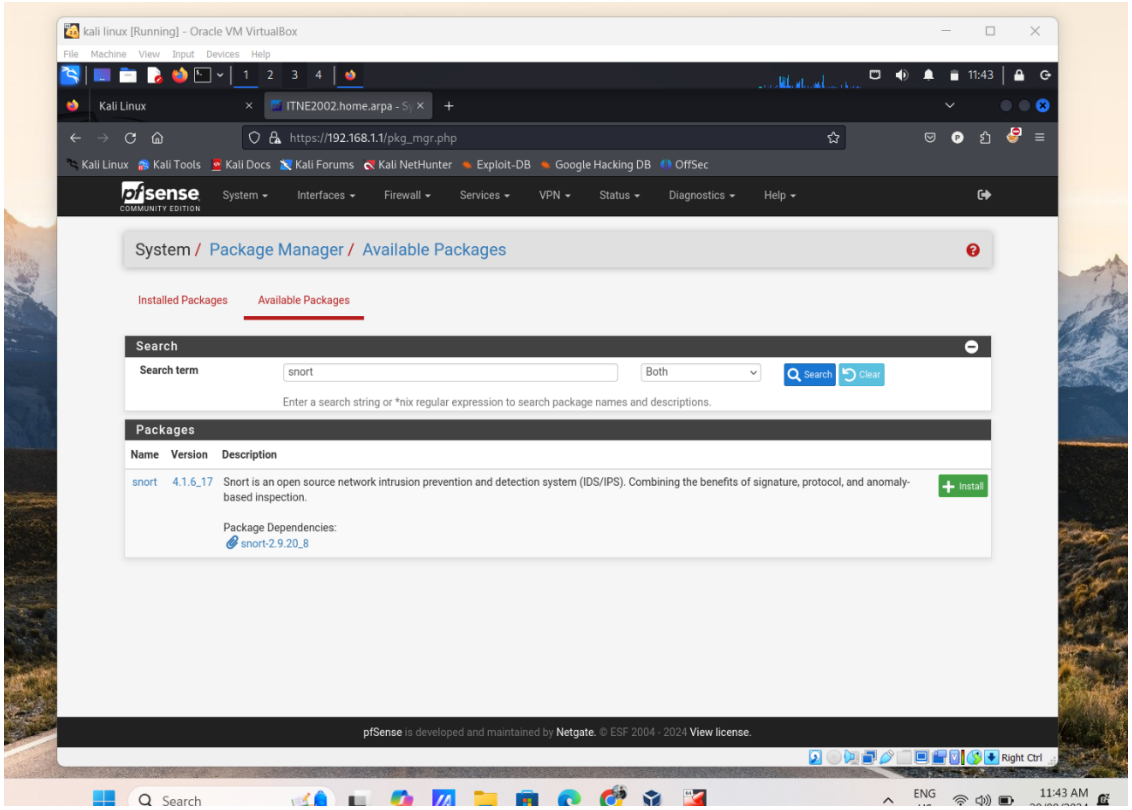

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
ITNE2002.home.arpa - Se
https://192.168.1.1/services_dhcp.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Ignore Denied Clients
Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers
Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Primary Address Pool
Subnet
192.168.100.0/24
Subnet Range
192.168.100.1 - 192.168.100.254
Address Pool Range
192.168.100.50
From
192.168.100.200
To
The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools
Add Address Pool
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.
Server Options
WINS Servers
WINS Server 1
WINS Server 2
DNS Servers
192.168.100.1
DNS Server 2
Right Ctrl

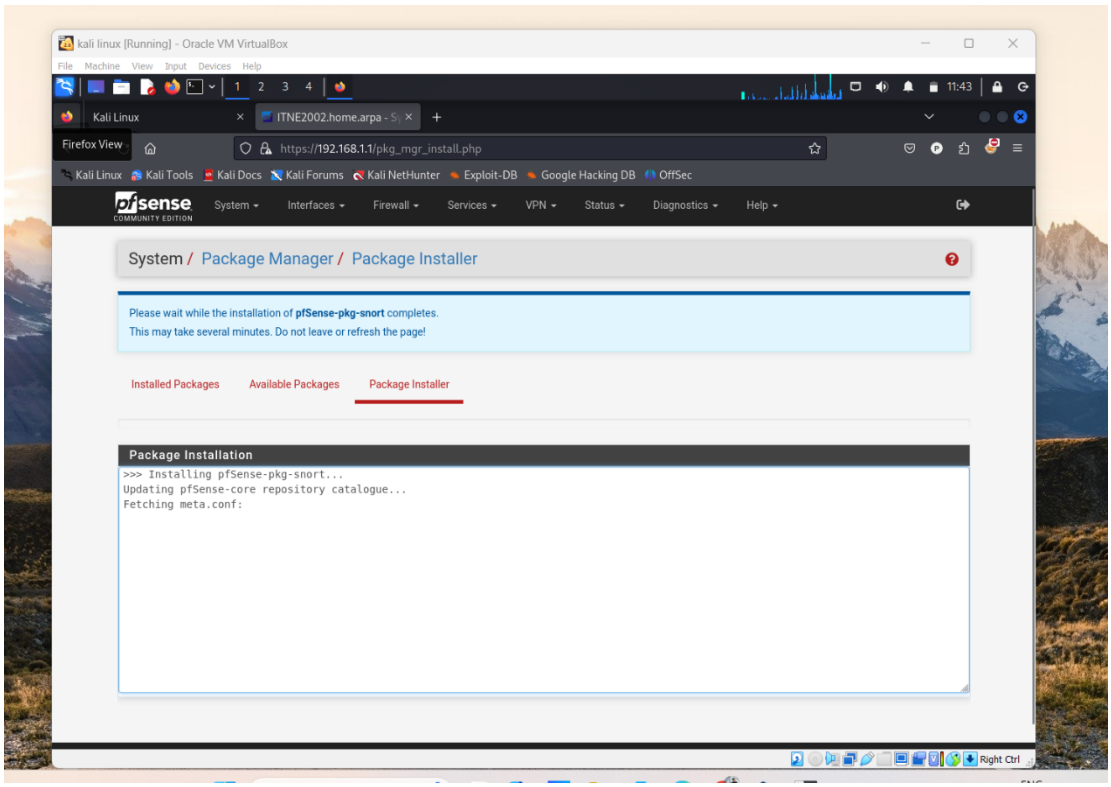

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
ITNE2002.home.arpa - In
https://192.168.1.1/interfaces.php?if=lan
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
MAC Address
xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
192.168.100.1
/
24
IPv4 Upstream gateway
None
Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by clicking here.
Track IPv6 Interface
IPv6 Interface
WAN
Selects the dynamic IPv6 WAN interface to track for configuration.
Right Ctrl
AUD/EUR
Search

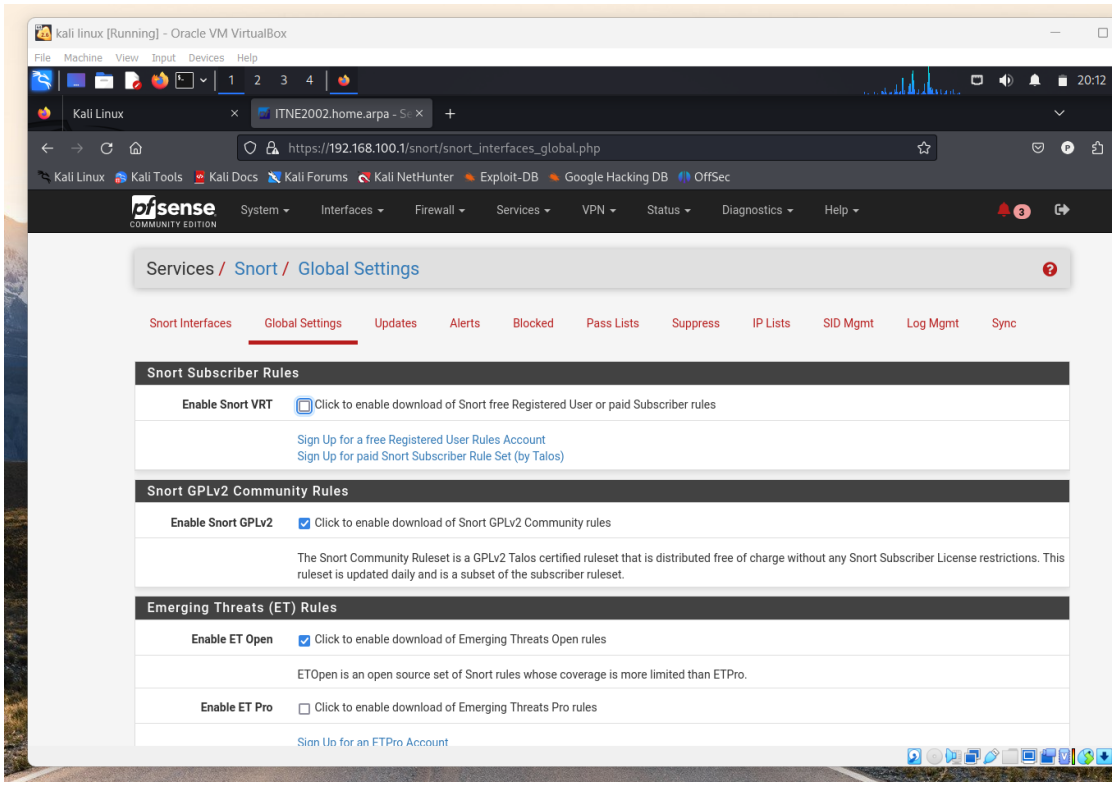

pfsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Starting /usr/local/etc/rc.d/clamd.sh...done.
Starting /usr/local/etc/rc.d/sqp_monitor.sh...done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete
FreeBSD/amd64 (ITNE2002.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: d1f98f7ecc83c1a5907c
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on ITNE2002 ***
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN (lan) -> em1 -> v4: 192.168.100.1/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:
Right Ctrl

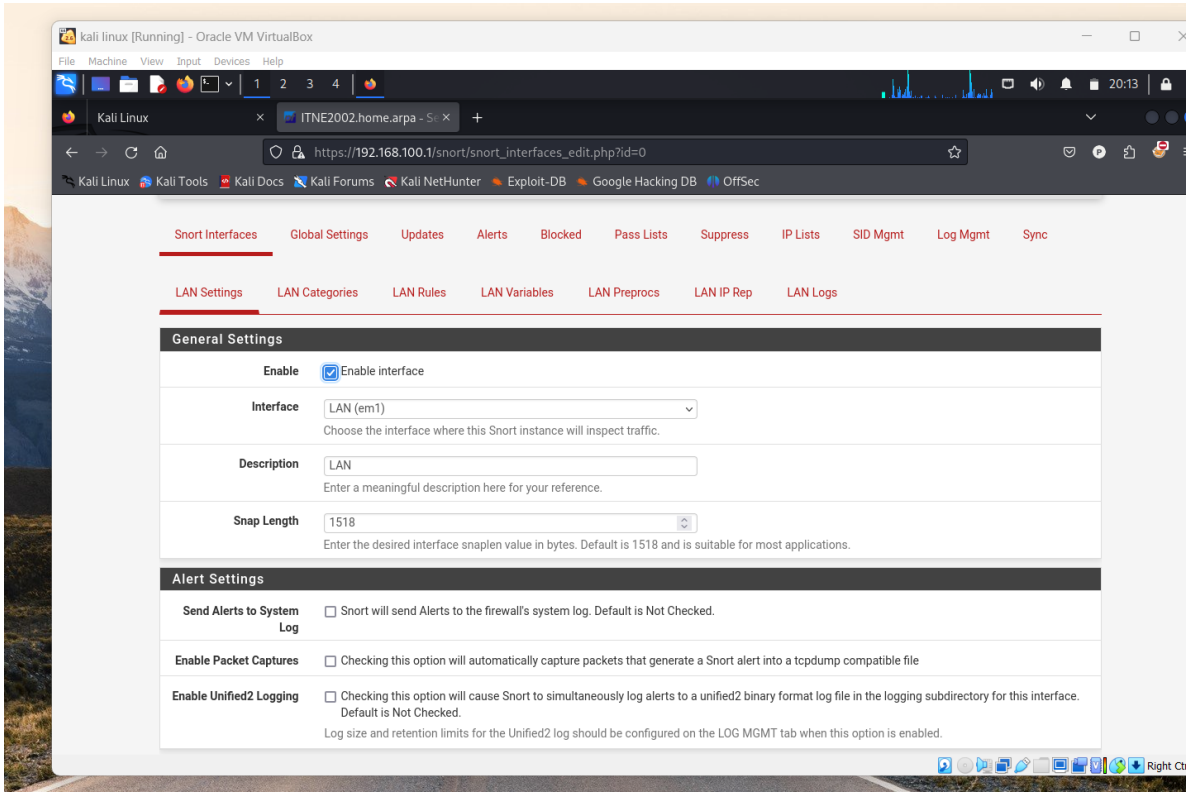
a. Configure Snort to detect local intrusions and attack the pfSense system through Kali Linux using ping sweep and attach the report.

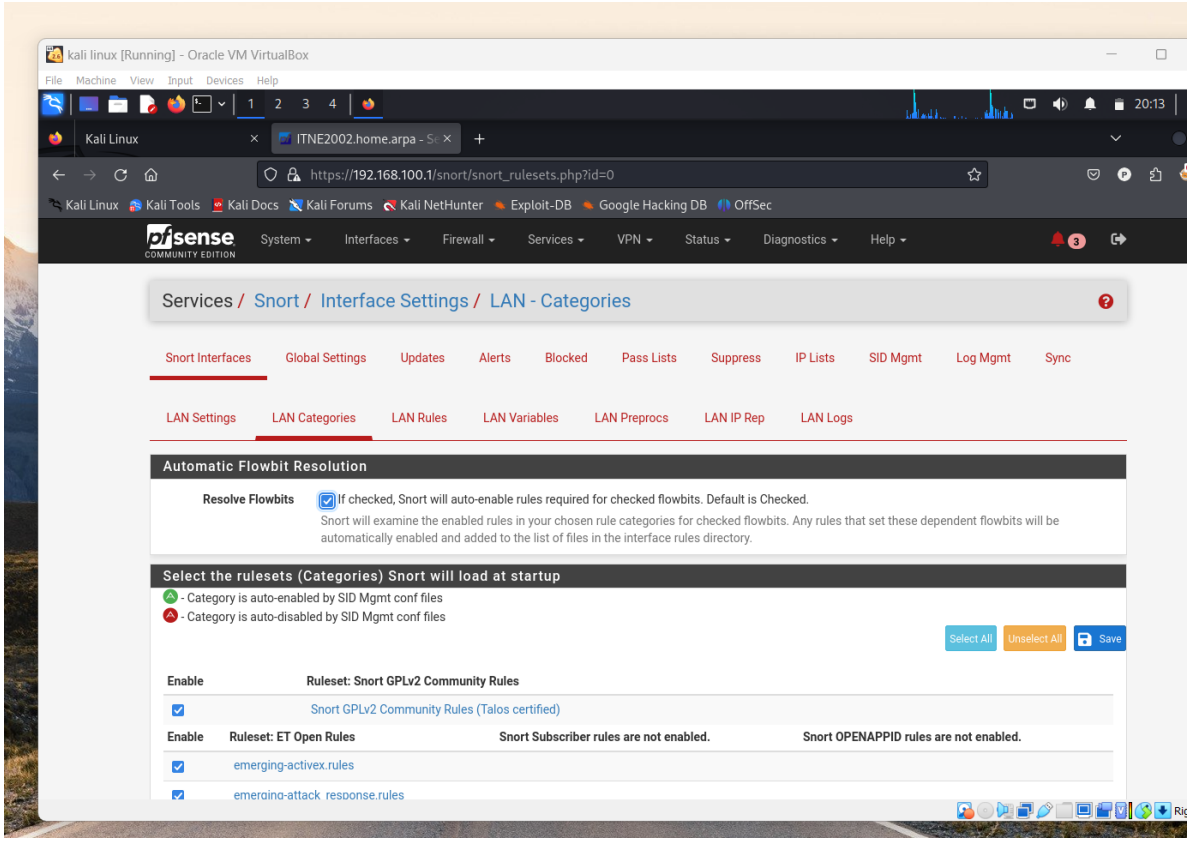


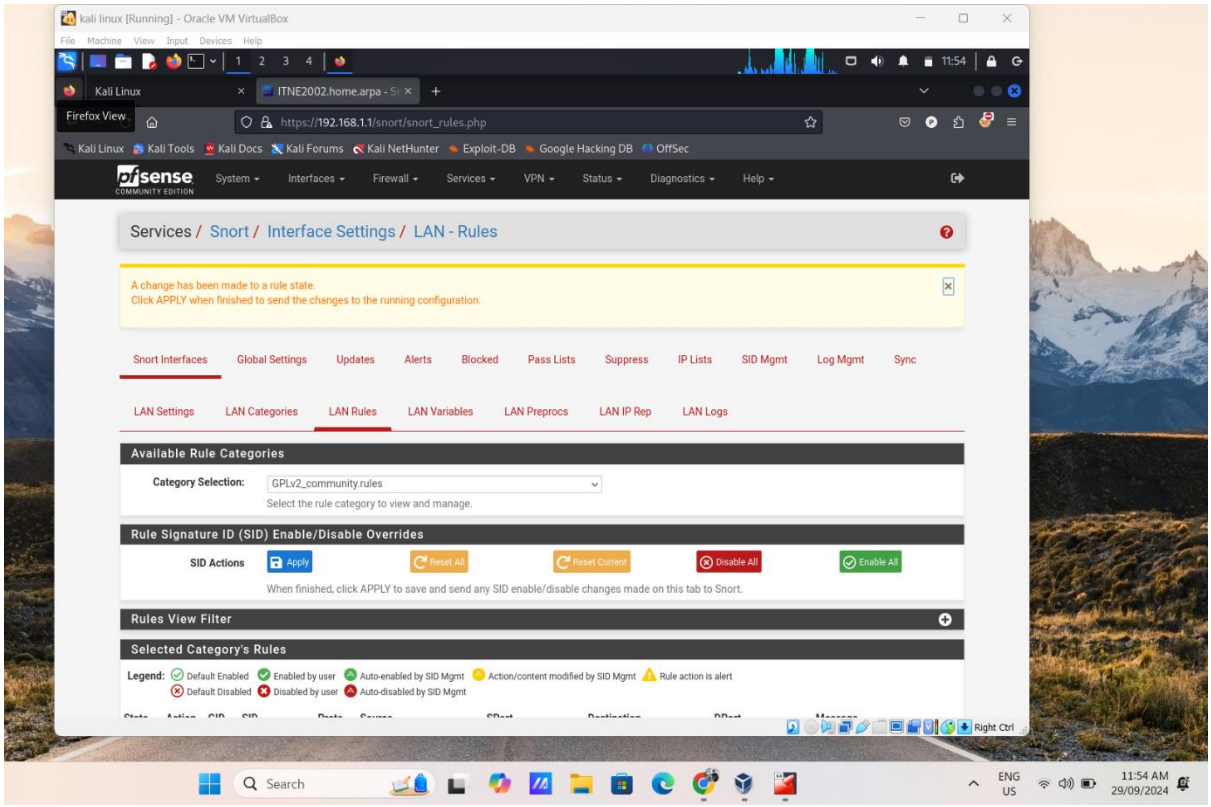

kali linux [Running] - Oracle VM VirtualBox
Kali Linux
ITNE2002.home.arpa
https://192.168.1.1/pkg_mgr.php
pfsense
System / Package Manager / Available Packages
Installed Packages
Available Packages
Search
Search term
snort
Both
Search
Clear
Enter a search string or *nix regular expression to search package names and descriptions.
Packages
Name
Version
Description
snort
4.1.6_17
Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.
Install
Package Dependencies:
snort-2.9.20_8
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

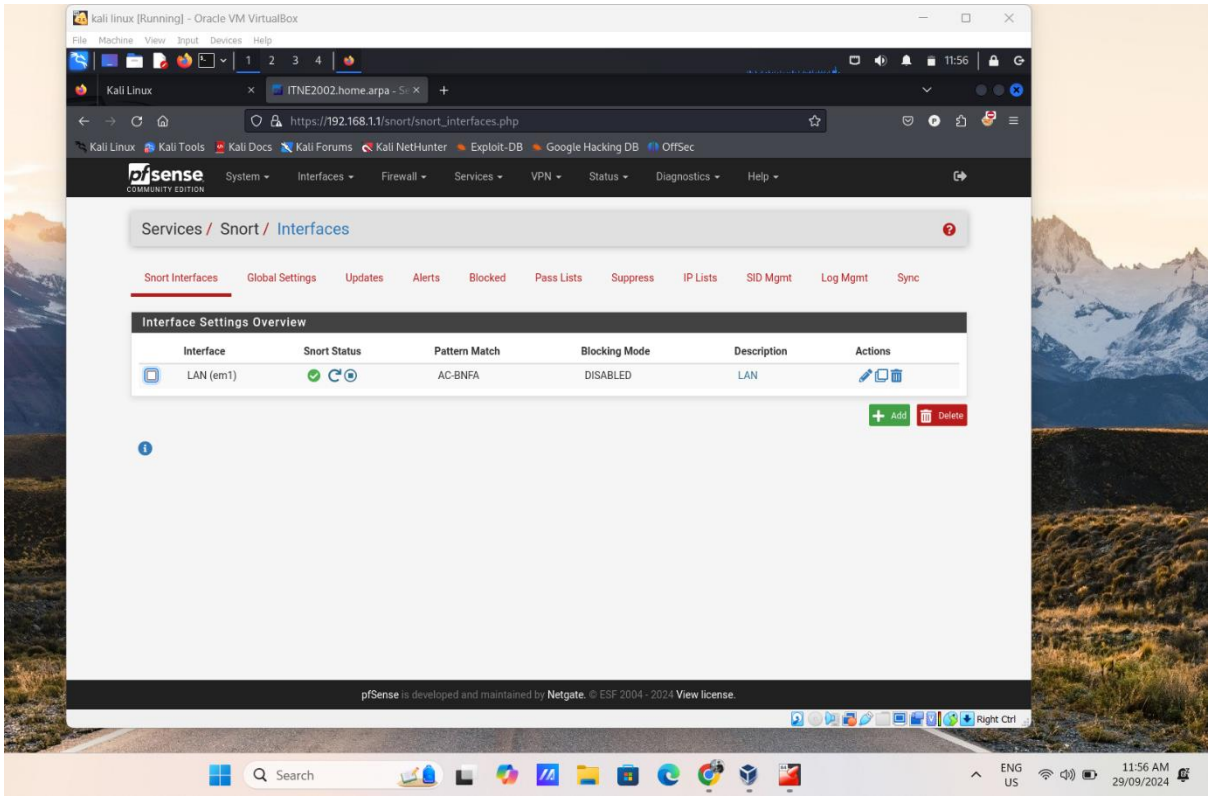

kali linux [Running] - Oracle VM VirtualBox
Kali Linux
ITNE2002.home.arpa
Firefox View
https://192.168.1.1/pkg_mgr_install.php
pfsense
System / Package Manager / Package Installer
Please wait while the installation of pfSense-pkg-snort completes.
This may take several minutes. Do not leave or refresh the page!
Installed Packages
Available Packages
Package Installer
Package Installation
>>> Installing pfSense-pkg-snort...
Updating pfSense-core repository catalogue...
Fetching meta.conf:

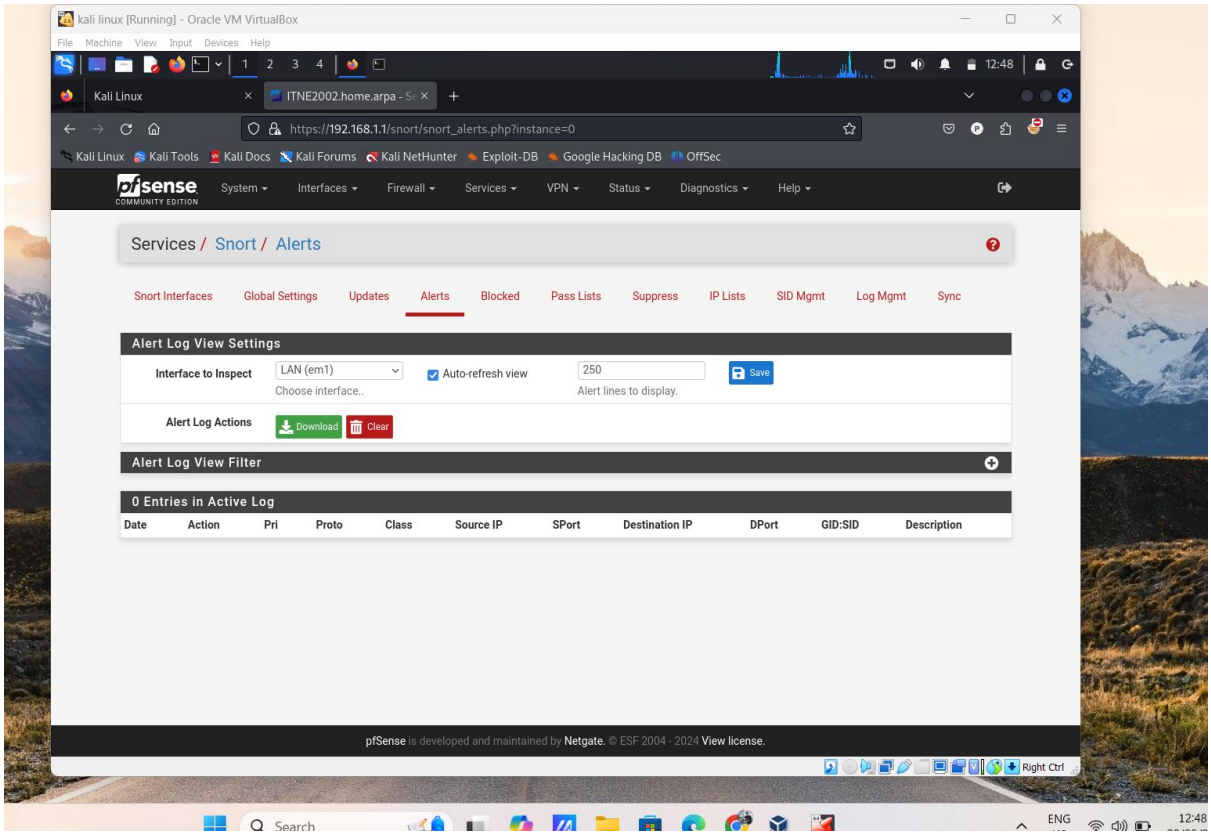

kali linux [Running] - Oracle VM VirtualBox
Kali Linux
ITNE2002.home.arpa
https://192.168.100.1/snort/snort_interfaces_global.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Services / Snort / Global Settings
Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync
Snort Subscriber Rules
Enable Snort VRT
Click to enable download of Snort free Registered User or paid Subscriber rules
Sign Up for a free Registered User Rules Account
Sign Up for paid Snort Subscriber Rule Set (by Talos)
Snort GPLv2 Community Rules
Enable Snort GPLv2
Click to enable download of Snort GPLv2 Community rules
The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.
Emerging Threats (ET) Rules
Enable ET Open
Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.
Enable ET Pro
Click to enable download of Emerging Threats Pro rules
Sign Up for an ETPro Account

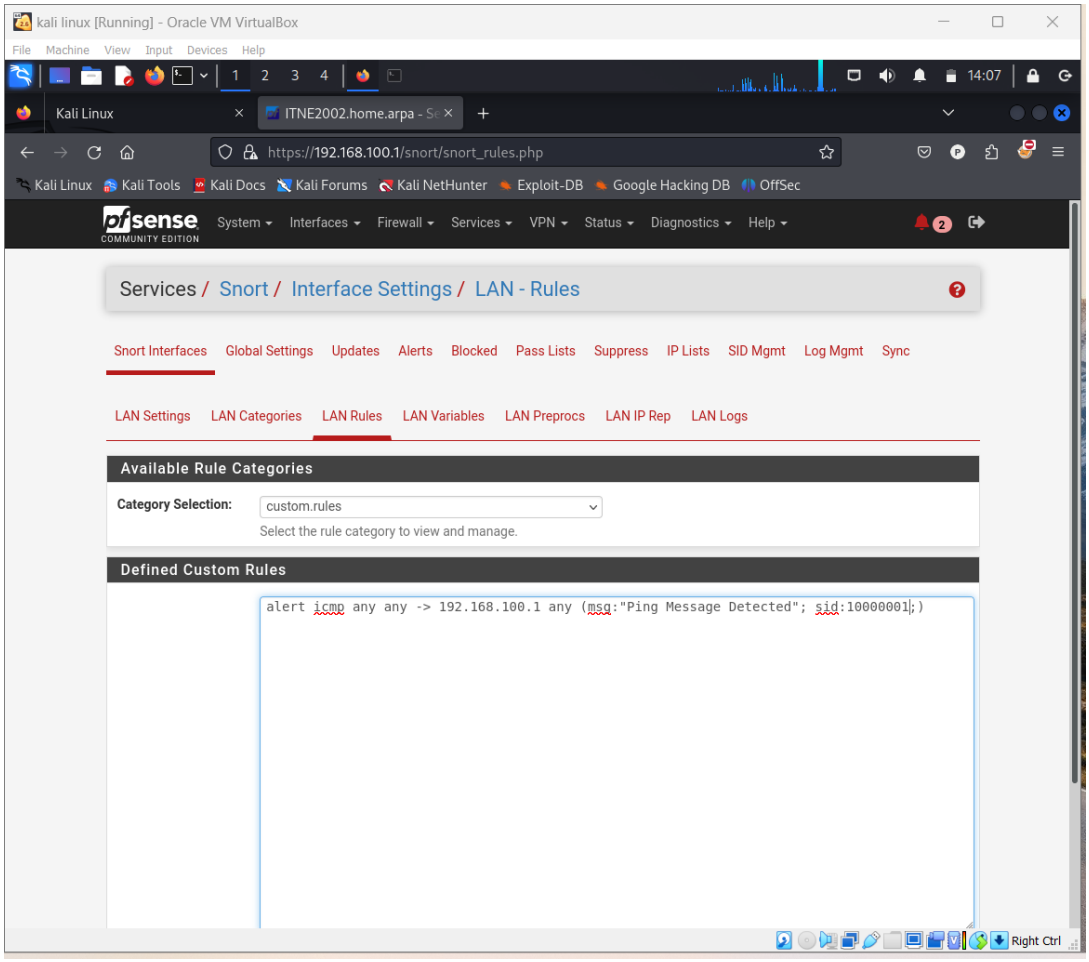

kali linux [Running] - Oracle VM VirtualBox
Kali Linux
ITNE2002.home.arpa
https://192.168.100.1/snort/snort_interfaces_edit.php?id=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync
LAN Settings LAN Categories LAN Rules LAN Variables LAN Preprocs LAN IP Rep LAN Logs
General Settings
Enable
Enable interface
Interface
LAN (em1)
Choose the interface where this Snort instance will inspect traffic.
Description
LAN
Enter a meaningful description here for your reference.
Snap Length
1518
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.
Alert Settings
Send Alerts to System Log
Snort will send Alerts to the firewall's system log. Default is Not Checked.
Enable Packet Captures
Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Enable Unified2 Logging
Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.


kali linux [Running] - Oracle VM VirtualBox
Kali Linux
ITNE2002.home.arpa
https://192.168.100.1/snort/snort_rulesets.php?id=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Services / Snort / Interface Settings / LAN - Categories
Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync
LAN Settings LAN Categories LAN Rules LAN Variables LAN Preprocs LAN IP Rep LAN Logs
Automatic Flowbit Resolution
Resolve Flowbits
If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.
Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.
Select the rulesets (Categories) Snort will load at startup
- Category is auto-enabled by SID Mgmt conf files
- Category is auto-disabled by SID Mgmt conf files
Select All
Unselect All
Save
Enable
Ruleset: Snort GPLv2 Community Rules
Snort GPLv2 Community Rules (Talos certified)
Enable
Ruleset: ET Open Rules
Snort Subscriber rules are not enabled.
Snort OPENAPPID rules are not enabled.
emerging-activex.rules

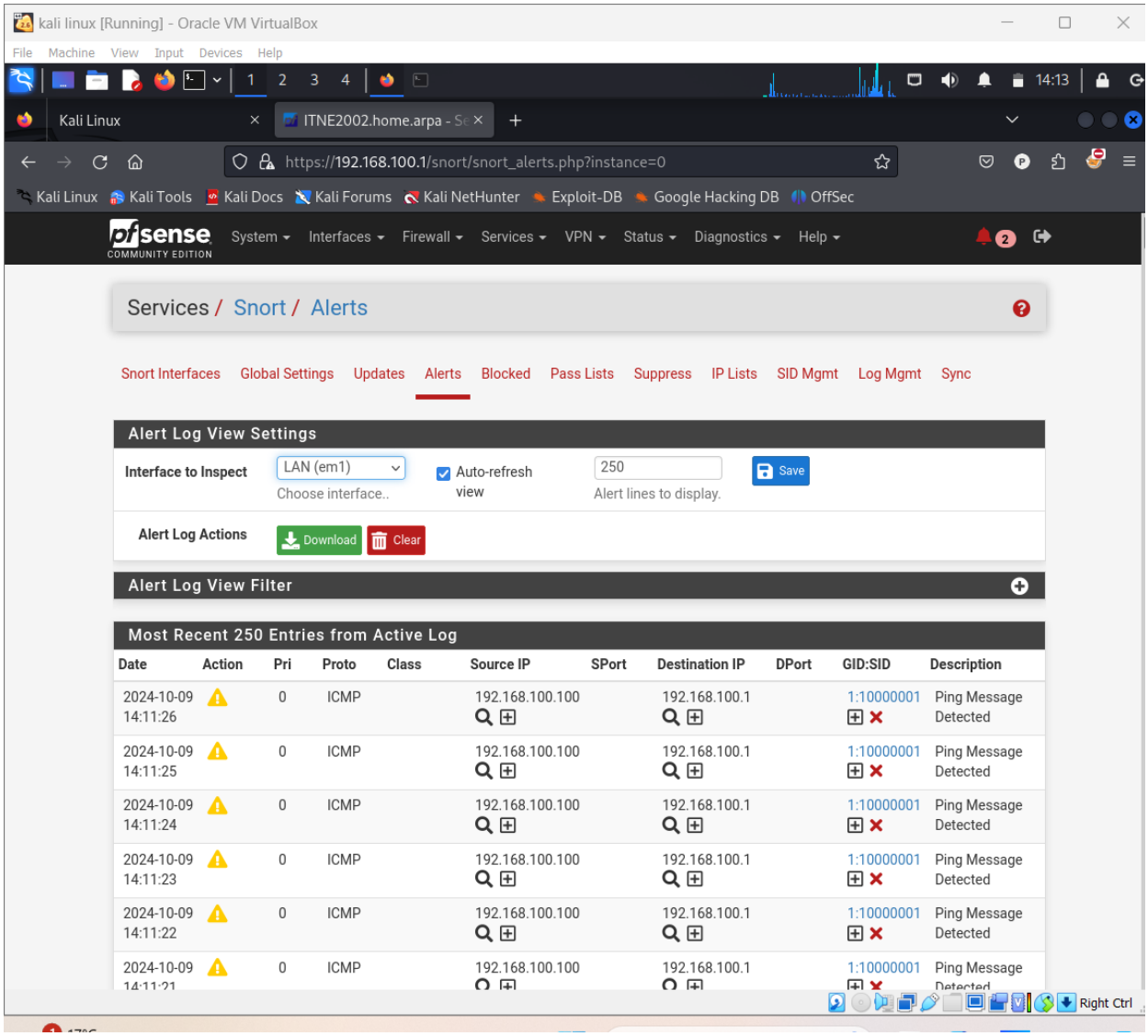

kali linux [Running] - Oracle VM VirtualBox
Kali Linux
ITNE2002.home.arpa
Firefox View
https://192.168.1.1/snort/snort_rules.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Services / Snort / Interface Settings / LAN - Rules
A change has been made to a rule state.
Click APPLY when finished to send the changes to the running configuration.
Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync
LAN Settings LAN Categories LAN Rules LAN Variables LAN Preprocs LAN IP Rep LAN Logs
Available Rule Categories
Category Selection:
GPLv2_community.rules
Select the rule category to view and manage.
Rule Signature ID (SID) Enable/Disable Overrides
SID Actions
Apply
Reset All
Reset Current
Disable All
Enable All
When finished, click APPLY to save and send any SID enable/disable changes made on this tab to Snort.
Rules View Filter
Selected Category's Rules
Legend:
Default Enabled
Enabled by user
Auto-enabled by SID Mgmt
Action/content modified by SID Mgmt
Rule action is alert
Default Disabled
Disabled by user
Auto-disabled by SID Mgmt
Right Ctrl
Search
ENG US
11:54 AM 29/09/2024


kali linux [Running] - Oracle VM VirtualBox
Kali Linux
ITNE2002.home.arpa
https://192.168.1.1/snort/snort_interfaces.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Services / Snort / Interfaces
Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync
Interface Settings Overview
Interface Snort Status Pattern Match Blocking Mode Description Actions
LAN (em1) AC-BNFA DISABLED LAN
Add Delete
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Right Ctrl
Search
ENG US
11:56 AM 29/09/2024

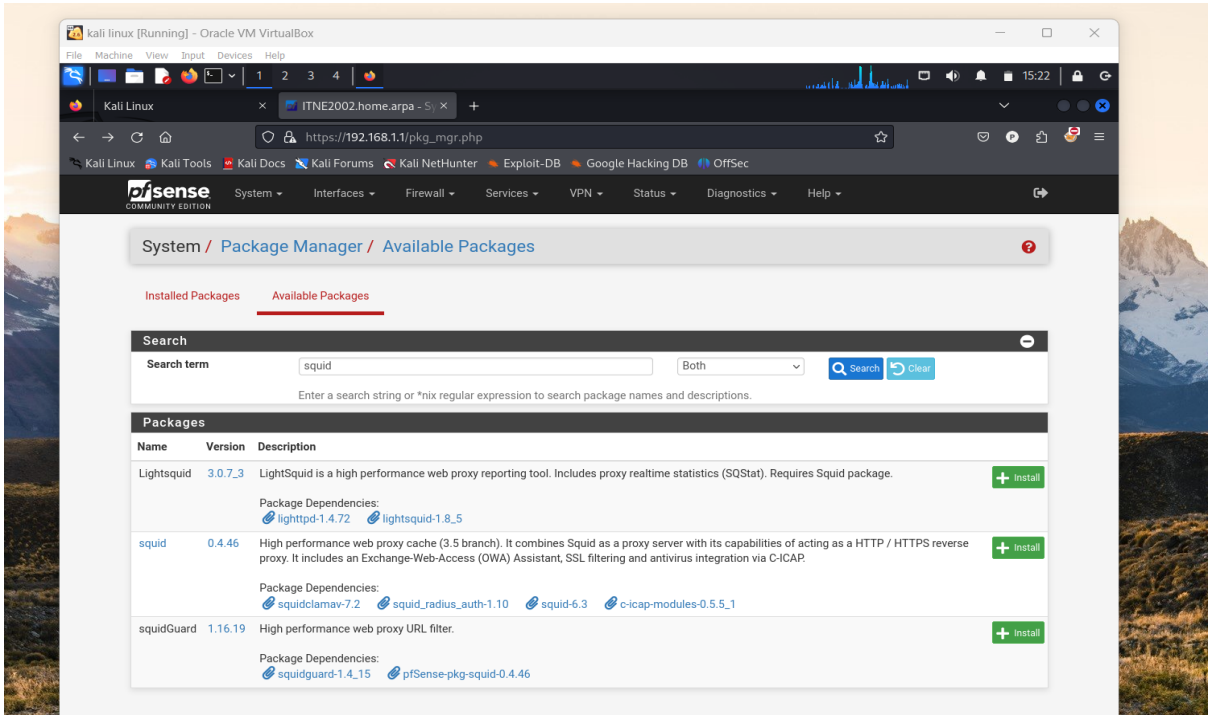

kali linux [Running] - Oracle VM VirtualBox
Kali Linux
ITNE2002.home.arpa
https://192.168.1.1/snort/snort_alerts.php?instance=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Services / Snort / Alerts
Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync
Alert Log View Settings
Interface to Inspect LAN (em1) Choose interface..
Auto-refresh view
250 Alert lines to display.
Save
Alert Log Actions Download Clear
Alert Log View Filter
0 Entries in Active Log
Date Action Pri Proto Class Source IP SPort Destination IP DPort GID:SID Description
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Right Ctrl
Search
ENG
12:48

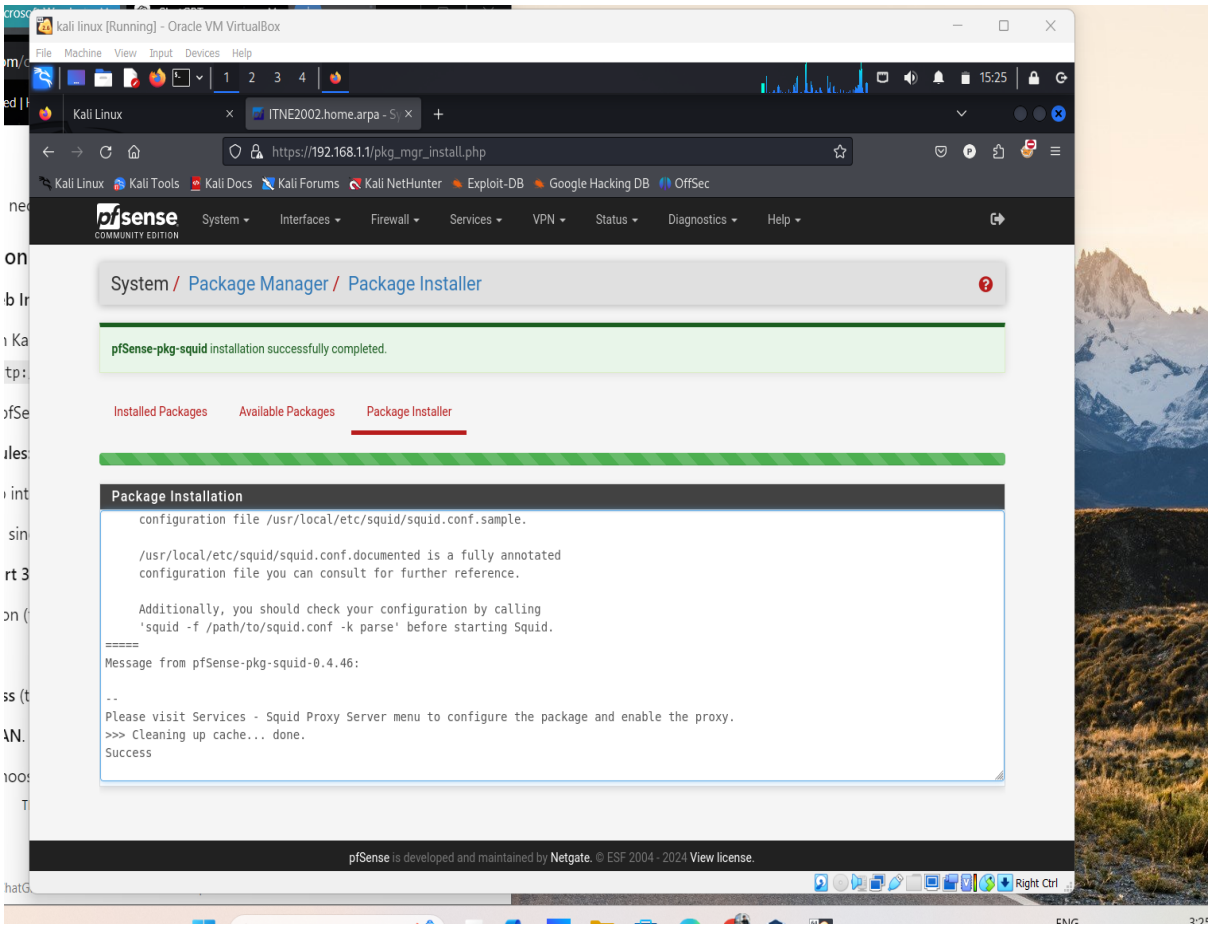


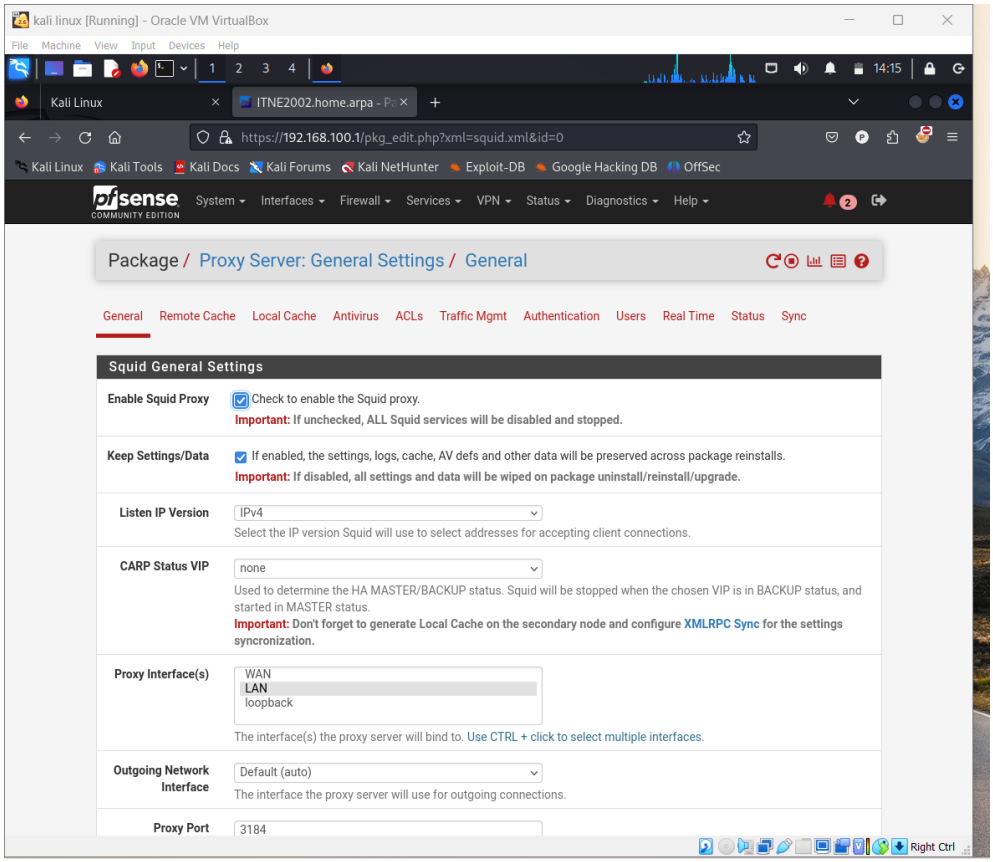

```
Nmap done: 256 IP addresses (3 hosts up) scanned in 1.80 seconds

┌──(pr56333㉿kali)-[~]
└─$ ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_seq=1 ttl=64 time=0.817 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=0.426 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=64 time=0.758 ms
64 bytes from 192.168.100.1: icmp_seq=4 ttl=64 time=0.664 ms
64 bytes from 192.168.100.1: icmp_seq=5 ttl=64 time=0.562 ms
64 bytes from 192.168.100.1: icmp_seq=6 ttl=64 time=0.352 ms
64 bytes from 192.168.100.1: icmp_seq=7 ttl=64 time=0.515 ms
64 bytes from 192.168.100.1: icmp_seq=8 ttl=64 time=0.612 ms
64 bytes from 192.168.100.1: icmp_seq=9 ttl=64 time=0.930 ms
64 bytes from 192.168.100.1: icmp_seq=10 ttl=64 time=0.950 ms
64 bytes from 192.168.100.1: icmp_seq=11 ttl=64 time=1.30 ms
64 bytes from 192.168.100.1: icmp_seq=12 ttl=64 time=1.07 ms
64 bytes from 192.168.100.1: icmp_seq=13 ttl=64 time=1.08 ms
64 bytes from 192.168.100.1: icmp_seq=14 ttl=64 time=0.542 ms
64 bytes from 192.168.100.1: icmp_seq=15 ttl=64 time=0.586 ms
64 bytes from 192.168.100.1: icmp_seq=16 ttl=64 time=0.511 ms
64 bytes from 192.168.100.1: icmp_seq=17 ttl=64 time=0.532 ms
64 bytes from 192.168.100.1: icmp_seq=18 ttl=64 time=0.589 ms
64 bytes from 192.168.100.1: icmp_seq=19 ttl=64 time=0.475 ms
64 bytes from 192.168.100.1: icmp_seq=20 ttl=64 time=0.569 ms
64 bytes from 192.168.100.1: icmp_seq=21 ttl=64 time=0.801 ms
64 bytes from 192.168.100.1: icmp_seq=22 ttl=64 time=0.940 ms
64 bytes from 192.168.100.1: icmp_seq=23 ttl=64 time=0.596 ms
64 bytes from 192.168.100.1: icmp_seq=24 ttl=64 time=0.628 ms
64 bytes from 192.168.100.1: icmp_seq=25 ttl=64 time=0.620 ms
64 bytes from 192.168.100.1: icmp_seq=26 ttl=64 time=0.179 ms
64 bytes from 192.168.100.1: icmp_seq=27 ttl=64 time=0.425 ms
```

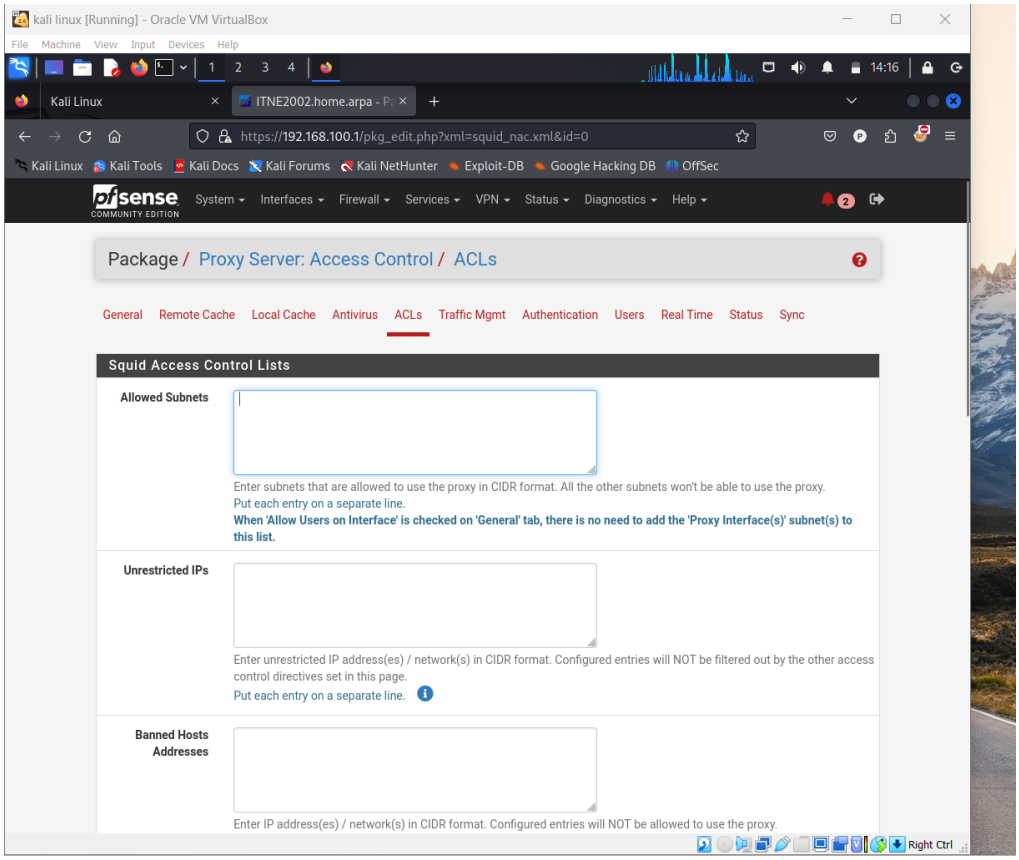

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
ITNE2002.home.arpa - Se
https://192.168.100.1/snort/snort_alerts.php?instance=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Services / Snort / Alerts
Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync
Alert Log View Settings
Interface to Inspect
LAN (em1)
Choose interface..
Auto-refresh view
250
Alert lines to display.
Save
Alert Log Actions
Download
Clear
Alert Log View Filter
Most Recent 250 Entries from Active Log
Date Action Pri Proto Class Source IP SPort Destination IP DPort GID:SID Description
2024-10-09 14:11:26 0 ICMP 192.168.100.100 192.168.100.1 1:10000001 Ping Message Detected
2024-10-09 14:11:25 0 ICMP 192.168.100.100 192.168.100.1 1:10000001 Ping Message Detected
2024-10-09 14:11:24 0 ICMP 192.168.100.100 192.168.100.1 1:10000001 Ping Message Detected
2024-10-09 14:11:23 0 ICMP 192.168.100.100 192.168.100.1 1:10000001 Ping Message Detected
2024-10-09 14:11:22 0 ICMP 192.168.100.100 192.168.100.1 1:10000001 Ping Message Detected
2024-10-09 14:11:21 0 ICMP 192.168.100.100 192.168.100.1 1:10000001 Ping Message Detected
Right Ctrl

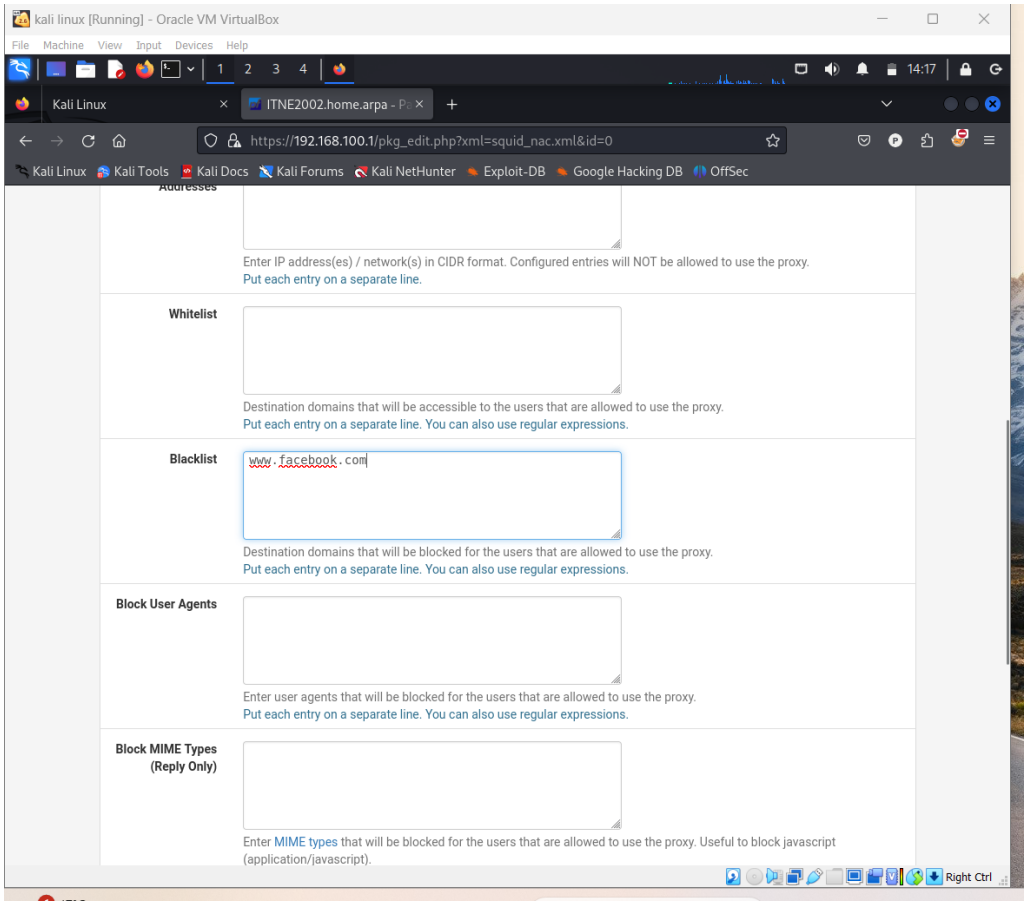
b. Use Squid to block (blacklist) www.facebook.com and attempt to access Facebook from the Windows 10 VM. Attach the output of the Windows.

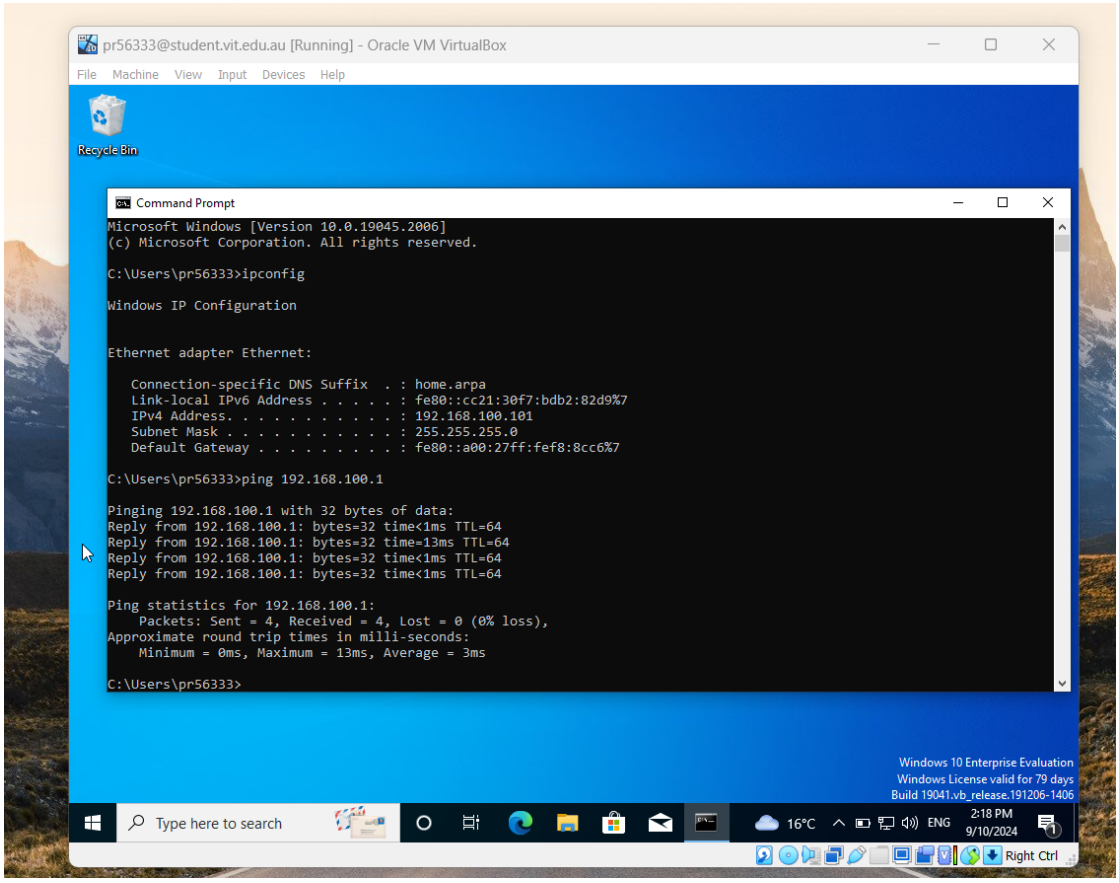


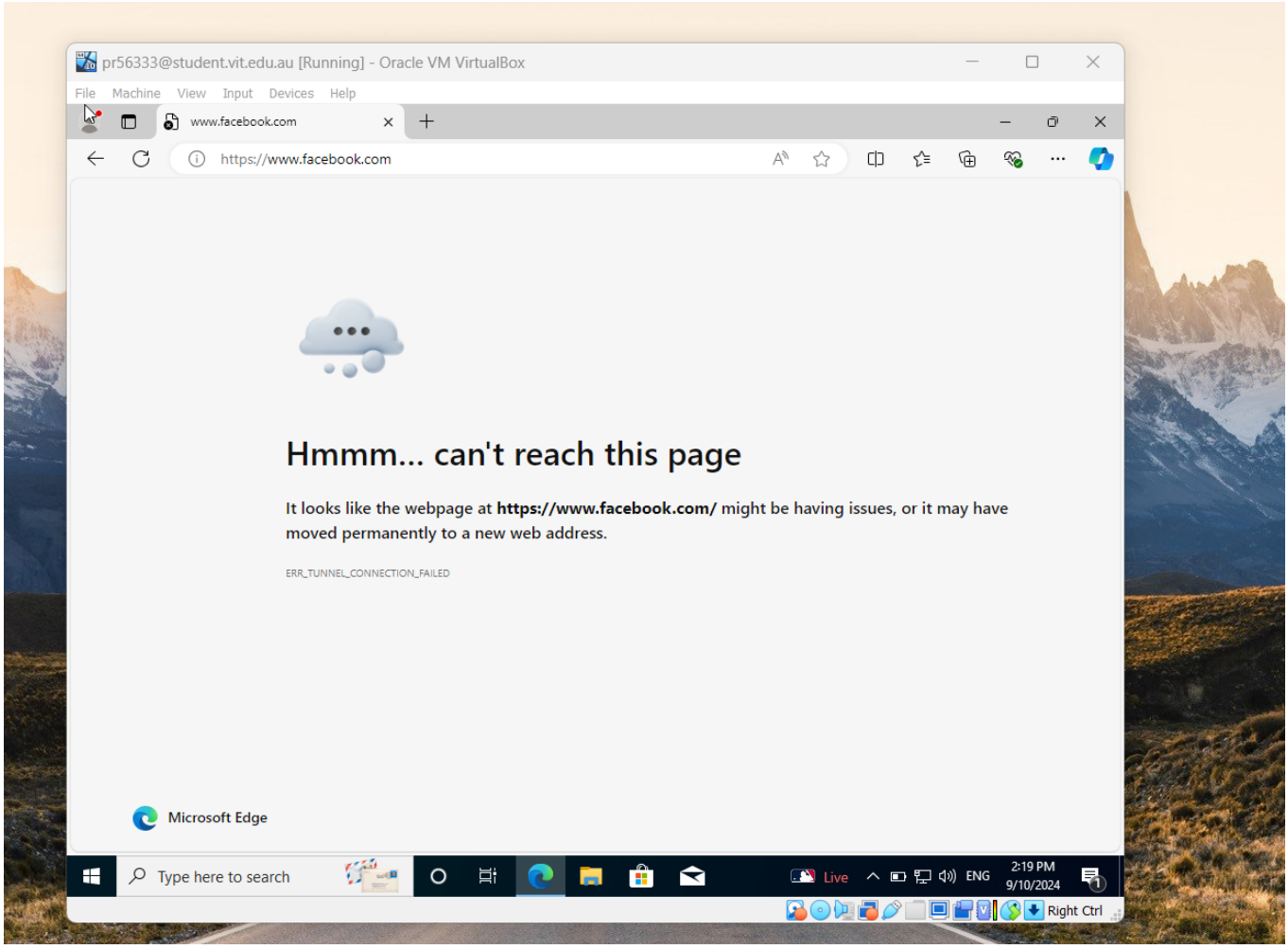



kali linux [Running] - Oracle VM VirtualBox
Kali Linux
ITNE2002.home.arpa
https://192.168.100.1/pkg_edit.php?xml=squid.xml&id=0
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Package / Proxy Server: General Settings / General
General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status Sync
Squid General Settings
Enable Squid Proxy
Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.
Keep Settings/Data
If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
Listen IP Version
IPv4
Select the IP version Squid will use to select addresses for accepting client connections.
CARP Status VIP
none
Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.
Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings syncronization.
Proxy Interface(s)
WAN
LAN
loopback
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
Outgoing Network Interface
Default (auto)
The interface the proxy server will use for outgoing connections.
Proxy Port
3184

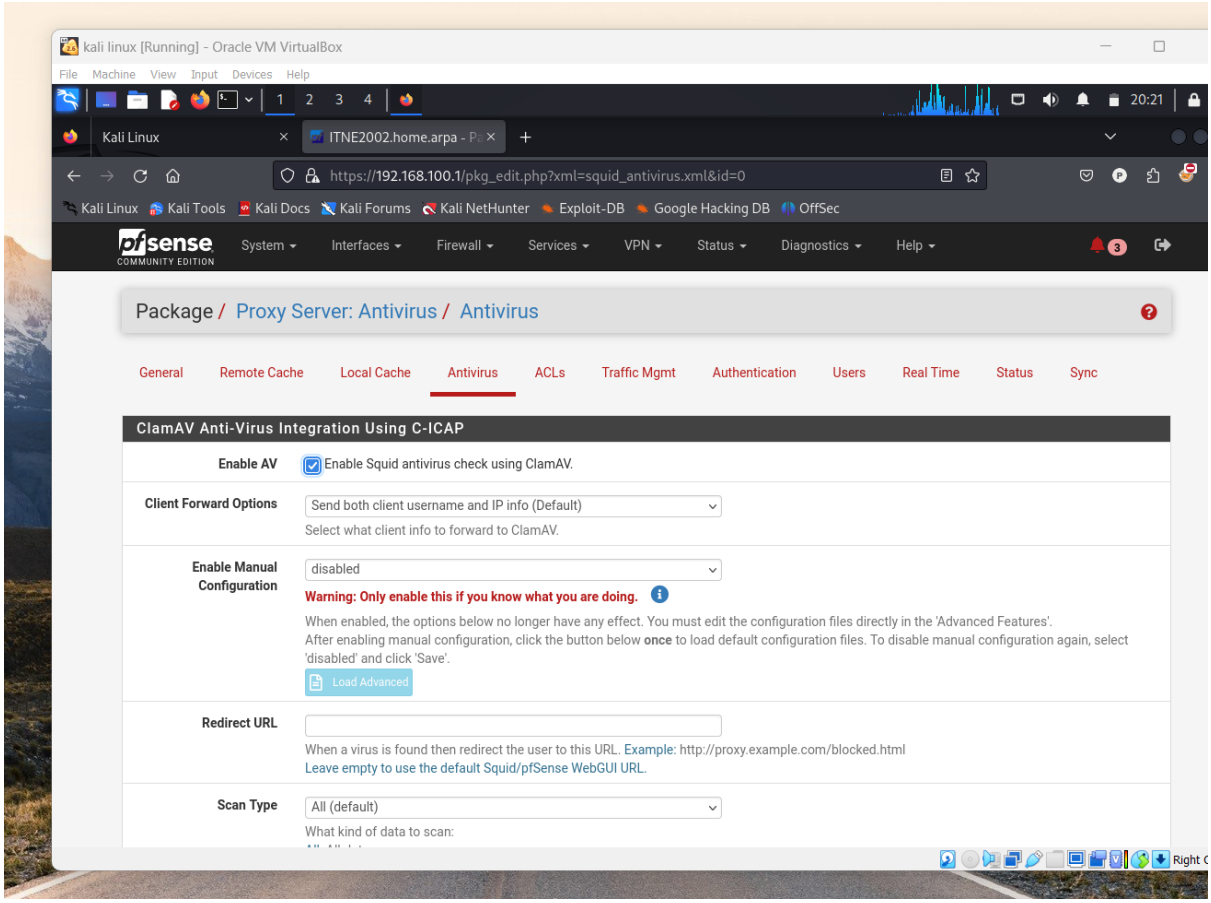

kali linux [Running] - Oracle VM VirtualBox
Kali Linux
ITNE2002.home.arpa
https://192.168.100.1/pkg_edit.php?xml=squid_nac.xml&id=0
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Package / Proxy Server: Access Control / ACLs
General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status Sync
Squid Access Control Lists
Allowed Subnets
Enter subnets that are allowed to use the proxy in CIDR format. All the other subnets won't be able to use the proxy.
Put each entry on a separate line.
When 'Allow Users on Interface' is checked on 'General' tab, there is no need to add the 'Proxy Interface(s)' subnet(s) to this list.
Unrestricted IPs
Enter unrestricted IP address(es) / network(s) in CIDR format. Configured entries will NOT be filtered out by the other access control directives set in this page.
Put each entry on a separate line.
Banned Hosts Addresses
Enter IP address(es) / network(s) in CIDR format. Configured entries will NOT be allowed to use the proxy.

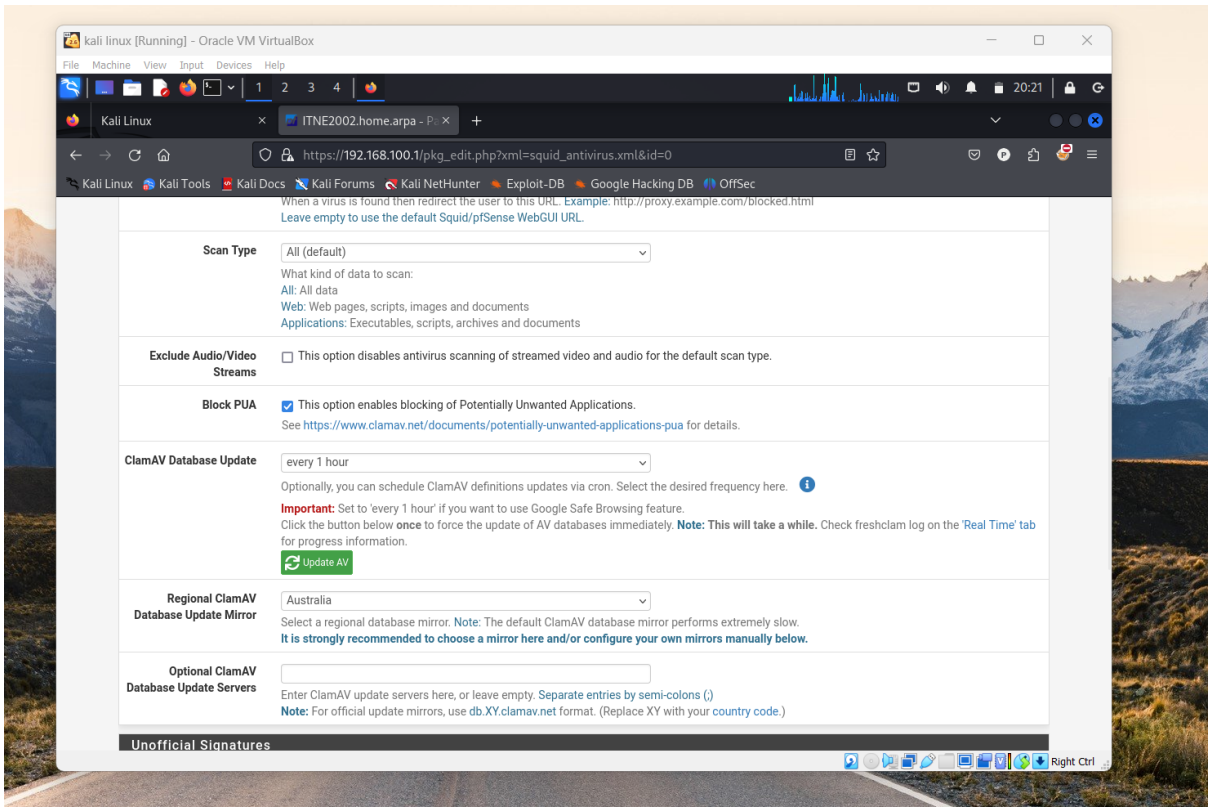

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
ITNE2002.home.arpa
https://192.168.100.1/pkg_edit.php?xml=squid_nac.xml&id=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Addresses
Enter IP address(es) / network(s) in CIDR format. Configured entries will NOT be allowed to use the proxy.
Put each entry on a separate line.
Whitelist
Destination domains that will be accessible to the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.
Blacklist
www.facebook.com
Destination domains that will be blocked for the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.
Block User Agents
Enter user agents that will be blocked for the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.
Block MIME Types (Reply Only)
Enter MIME types that will be blocked for the users that are allowed to use the proxy. Useful to block javascript (application/javascript).
Right Ctrl

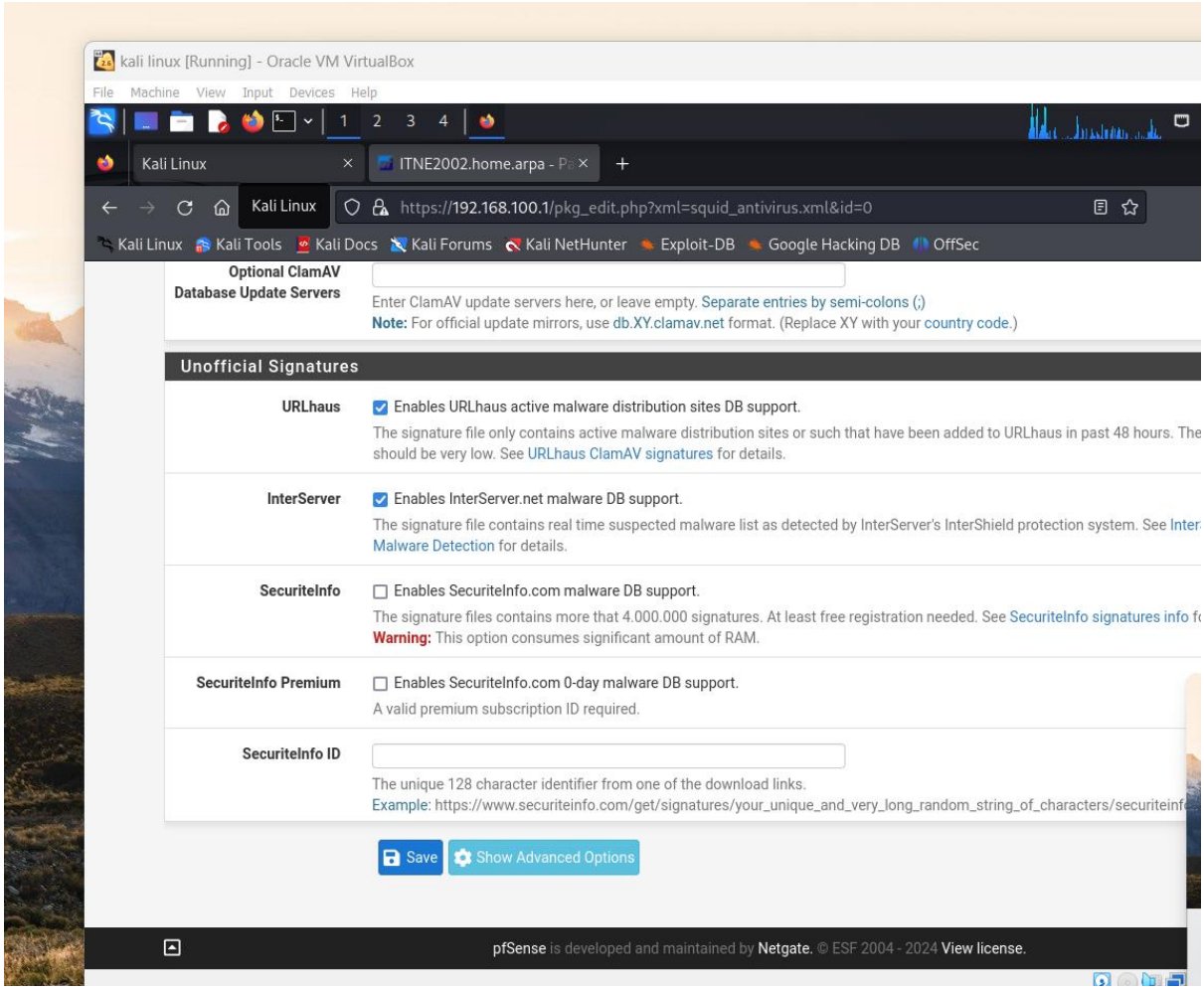

pr56333@student.vit.edu.au [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Command Prompt
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.
C:\Users\pr56333>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : home.arpa
Link-local IPv6 Address . . . . . : fe80::cc21:30f7:bdb2:82d9%7
IPv4 Address. . . . . : 192.168.100.101
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::a00:27ff:fef8:8cc6%7
C:\Users\pr56333>ping 192.168.100.1
Pinging 192.168.100.1 with 32 bytes of data:
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time=13ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.100.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 13ms, Average = 3ms
C:\Users\pr56333>
Windows 10 Enterprise Evaluation
Windows License valid for 79 days
Build 19041.vb_release.191206-1406
Type here to search
16°C
ENG
2:18 PM
9/10/2024
Right Ctrl


pr56333@student.vit.edu.au [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
www.facebook.com
https://www.facebook.com
Hmmm... can't reach this page
It looks like the webpage at https://www.facebook.com/ might be having issues, or it may have moved permanently to a new web address.
ERR_TUNNEL_CONNECTION_FAILED
Microsoft Edge
Type here to search
Live
ENG
2:19 PM
9/10/2024
Right Ctrl

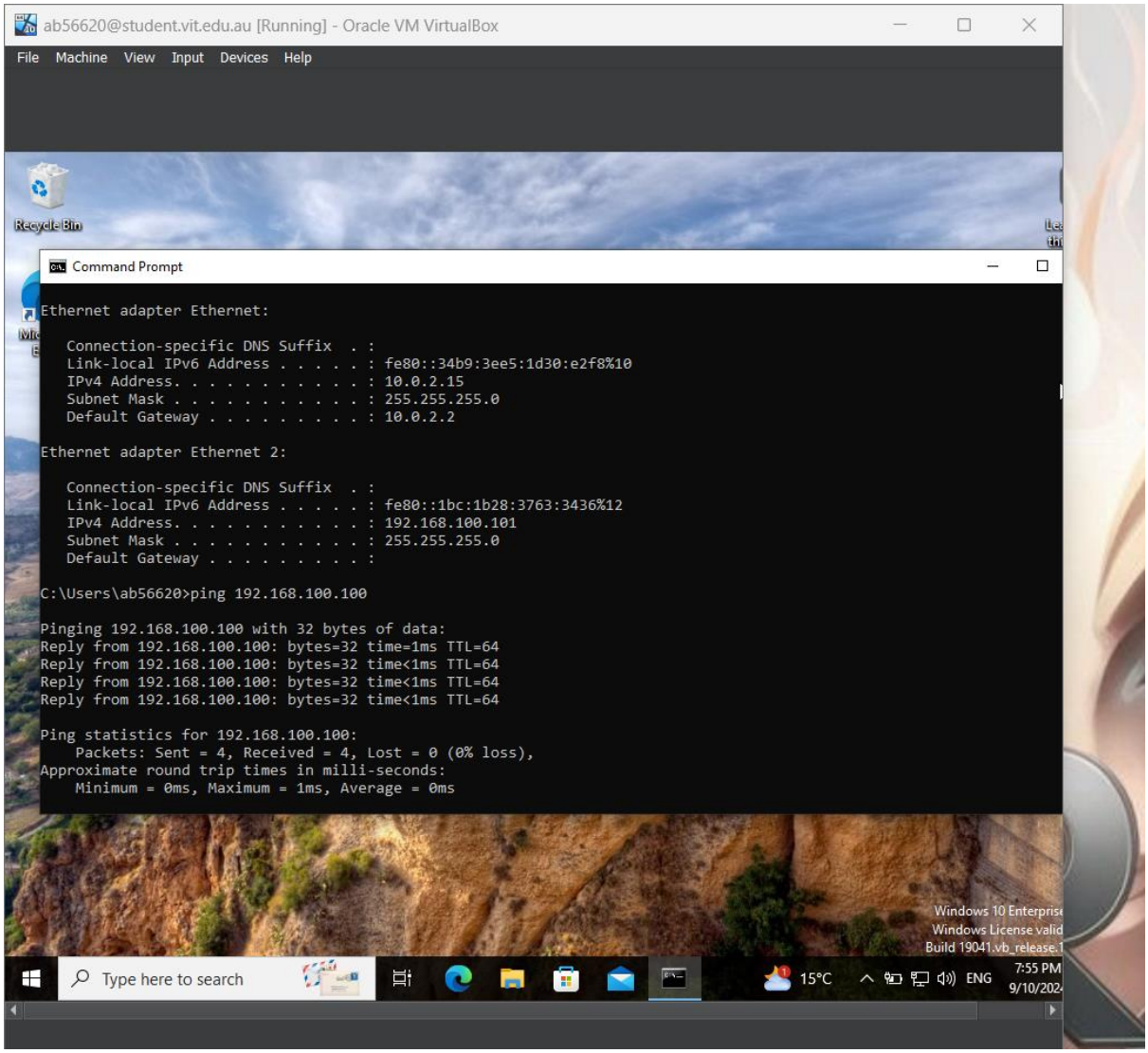
c. Installing ClamAV

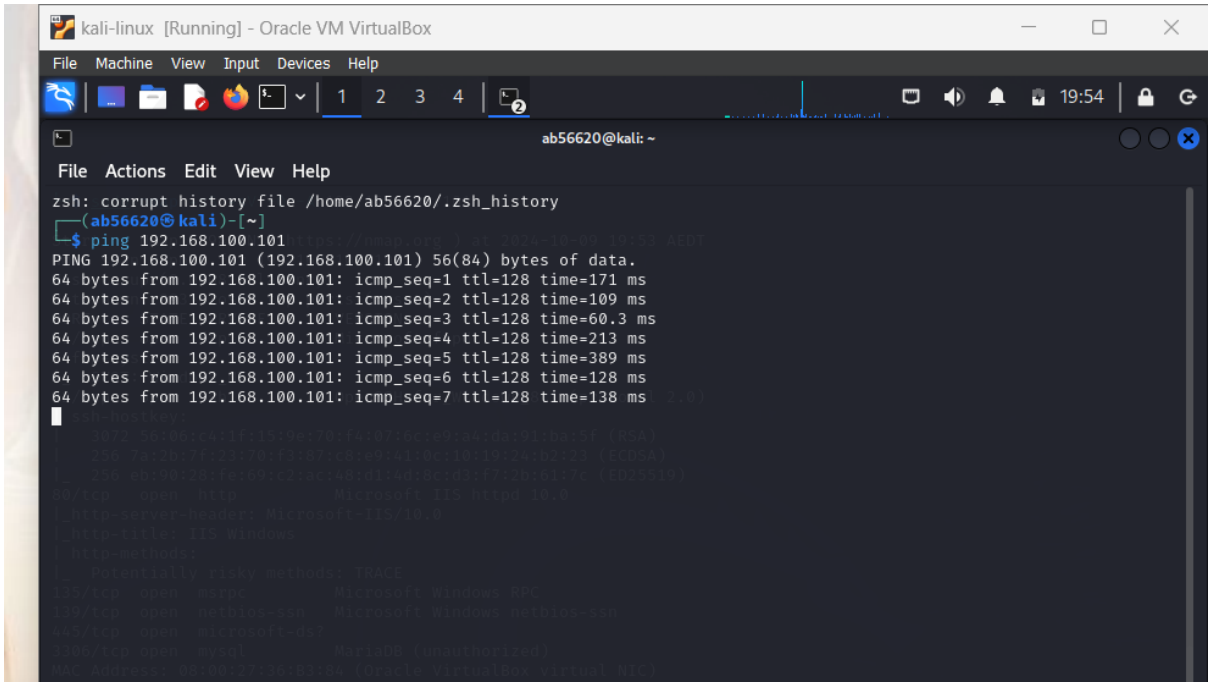


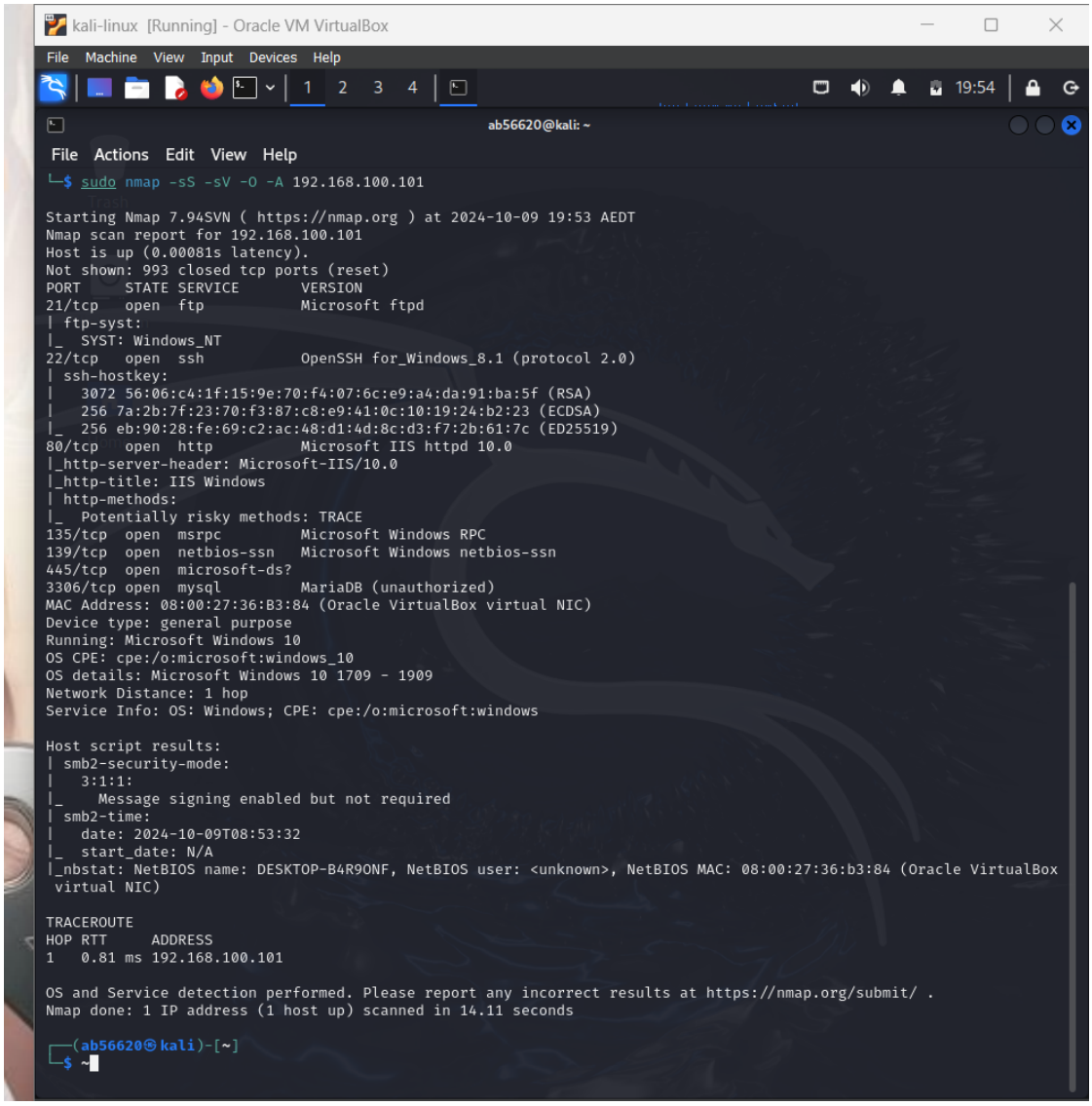



kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
ITNE2002.home.arpa - Pa
https://192.168.100.1/pkg_edit.php?xml=squid_antivirus.xml&id=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Optional ClamAV Database Update Servers
Enter ClamAV update servers here, or leave empty. Separate entries by semi-colons (;)
Note: For official update mirrors, use db.XY.clamav.net format. (Replace XY with your country code.)
Unofficial Signatures
URLhaus
Enables URLhaus active malware distribution sites DB support.
The signature file only contains active malware distribution sites or such that have been added to URLhaus in past 48 hours. The
should be very low. See URLhaus ClamAV signatures for details.
InterServer
Enables InterServer.net malware DB support.
The signature file contains real time suspected malware list as detected by InterServer's InterShield protection system. See Inter
Malware Detection for details.
SecuriteInfo
Enables SecuriteInfo.com malware DB support.
The signature files contains more that 4.000.000 signatures. At least free registration needed. See SecuriteInfo signatures info f
Warning: This option consumes significant amount of RAM.
SecuriteInfo Premium
Enables SecuriteInfo.com 0-day malware DB support.
A valid premium subscription ID required.
SecuriteInfo ID
The unique 128 character identifier from one of the download links.
Example: https://www.securiteinfo.com/get/signatures/your_unique_and_very_long_random_string_of_characters/securiteinf
Save
Show Advanced Options
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

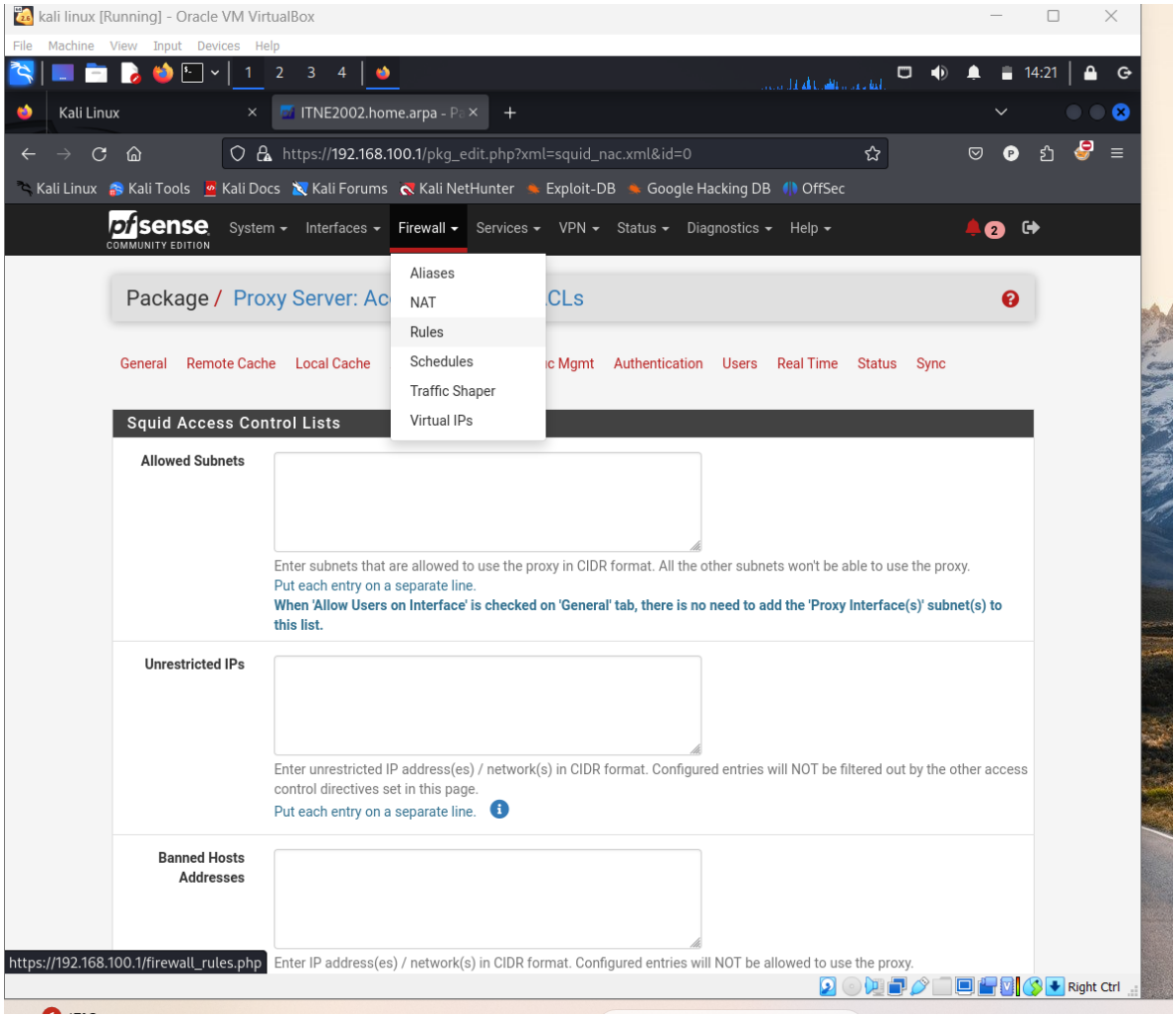
d. Scan windows 10 using Kali using Nmap and then provide a complete report on open ports and fix those.

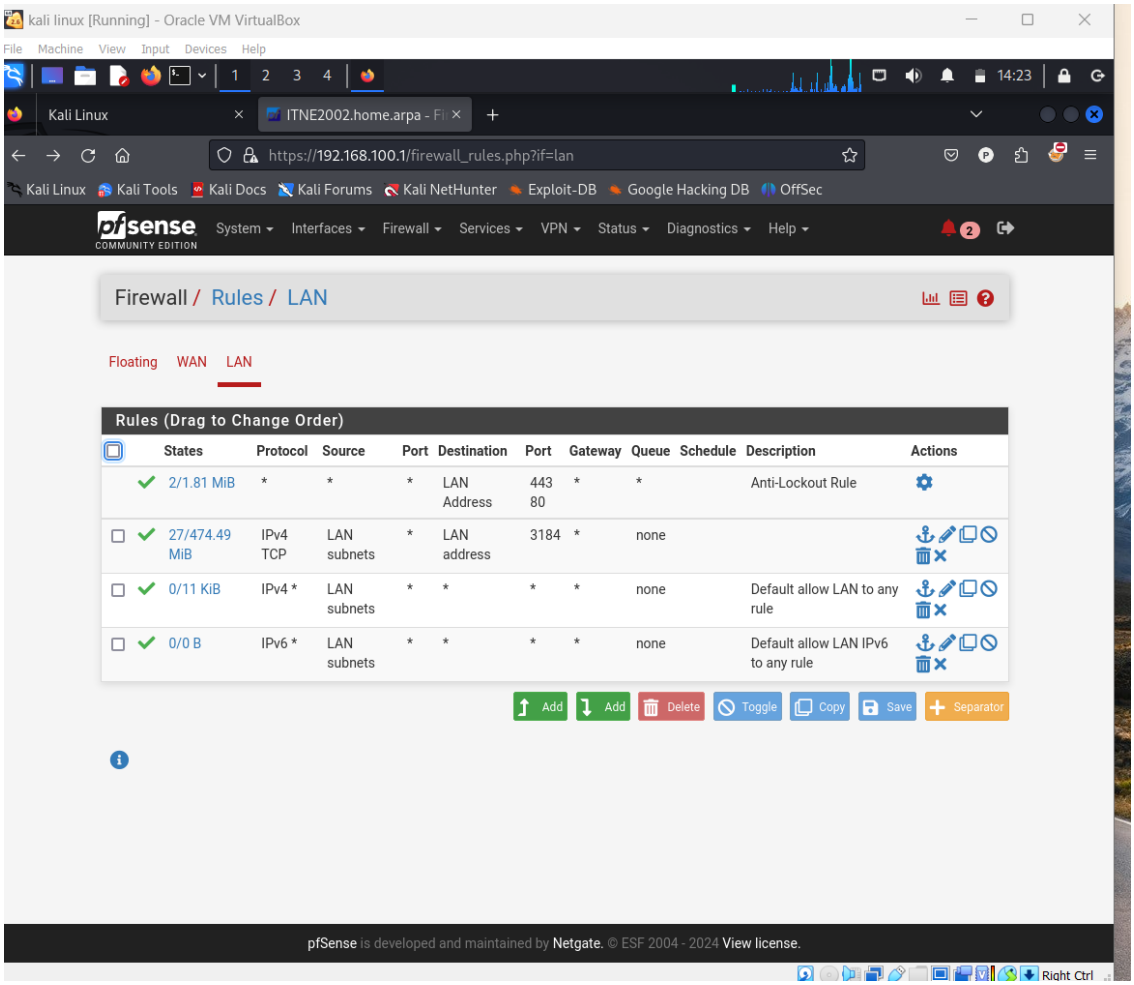


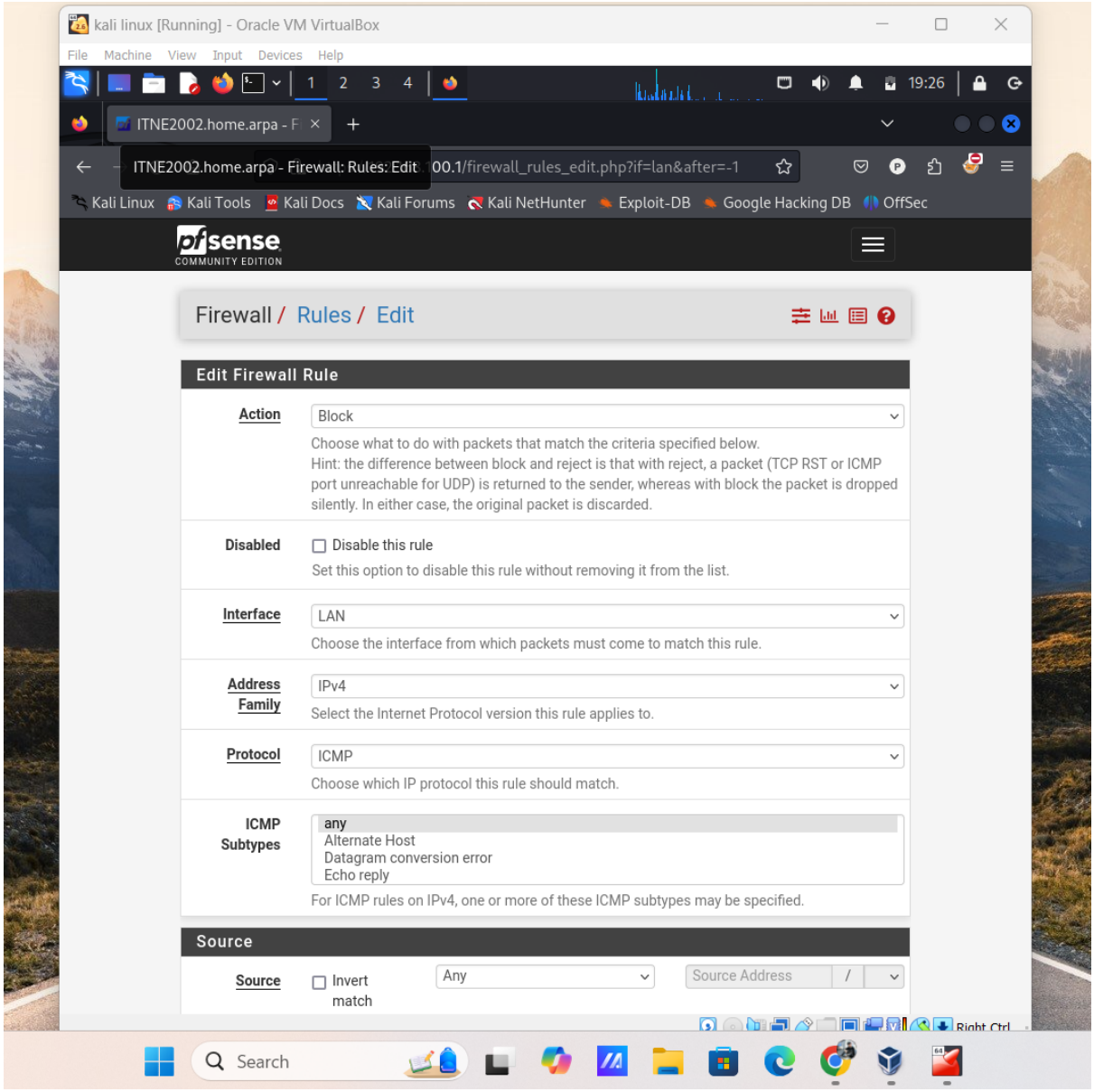

kali-linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
19:54
ab56620@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/ab56620/.zsh_history
(ab56620㉿kali)-[~]
$ ping 192.168.100.101
PING 192.168.100.101 (192.168.100.101) 56(84) bytes of data.
64 bytes from 192.168.100.101: icmp_seq=1 ttl=128 time=171 ms
64 bytes from 192.168.100.101: icmp_seq=2 ttl=128 time=109 ms
64 bytes from 192.168.100.101: icmp_seq=3 ttl=128 time=60.3 ms
64 bytes from 192.168.100.101: icmp_seq=4 ttl=128 time=213 ms
64 bytes from 192.168.100.101: icmp_seq=5 ttl=128 time=389 ms
64 bytes from 192.168.100.101: icmp_seq=6 ttl=128 time=128 ms
64 bytes from 192.168.100.101: icmp_seq=7 ttl=128 time=138 ms

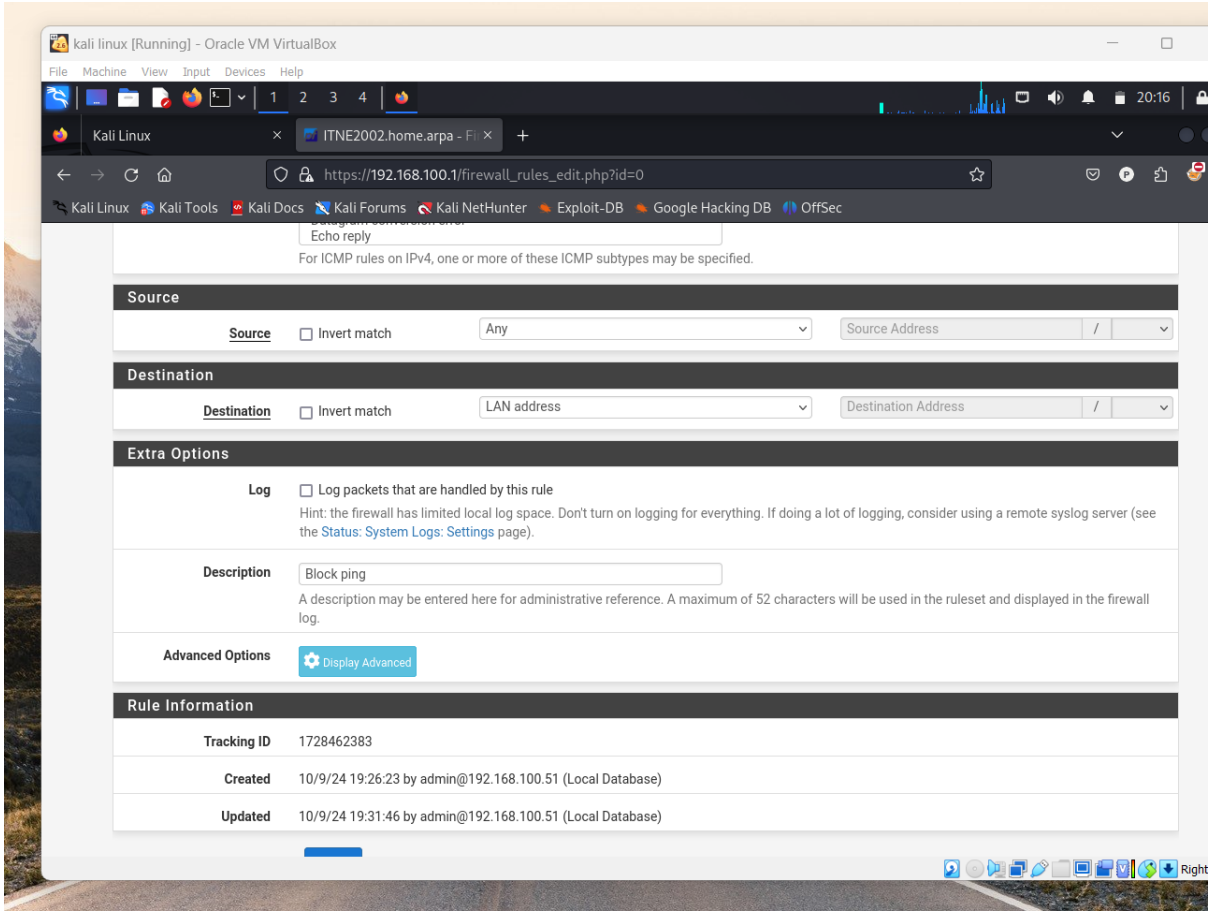

kali-linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
19:54
ab56620@kali: ~
File Actions Edit View Help
$ sudo nmap -sS -sV -O -A 192.168.100.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-09 19:53 AEDT
Nmap scan report for 192.168.100.101
Host is up (0.00081s latency).
Not shown: 993 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
| ftp-syst:
|_ SYST: Windows_NT
22/tcp open ssh OpenSSH for_Windows_8.1 (protocol 2.0)
| ssh-hostkey:
| 3072 56:06:c4:1f:15:9e:70:f4:07:6c:e9:a4:da:91:ba:5f (RSA)
| 256 7a:2b:7f:23:70:f3:87:c8:e9:41:0c:10:19:24:b2:23 (ECDSA)
|_ 256 eb:90:28:fe:69:c2:ac:48:d1:4d:8c:d3:f7:2b:61:7c (ED25519)
80/tcp open http Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows
| http-methods:
|_ Potentially risky methods: TRACE
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
3306/tcp open mysql MariaDB (unauthorized)
MAC Address: 08:00:27:36:B3:84 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
| smb2-time:
| date: 2024-10-09T08:53:32
|_ start_date: N/A
|_nbstat: NetBIOS name: DESKTOP-B4R9ONF, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:36:b3:84 (Oracle VirtualBox virtual NIC)
TRACEROUTE
HOP RTT ADDRESS
1 0.81 ms 192.168.100.101
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.11 seconds
(ab56620㉿kali)-[~]
$

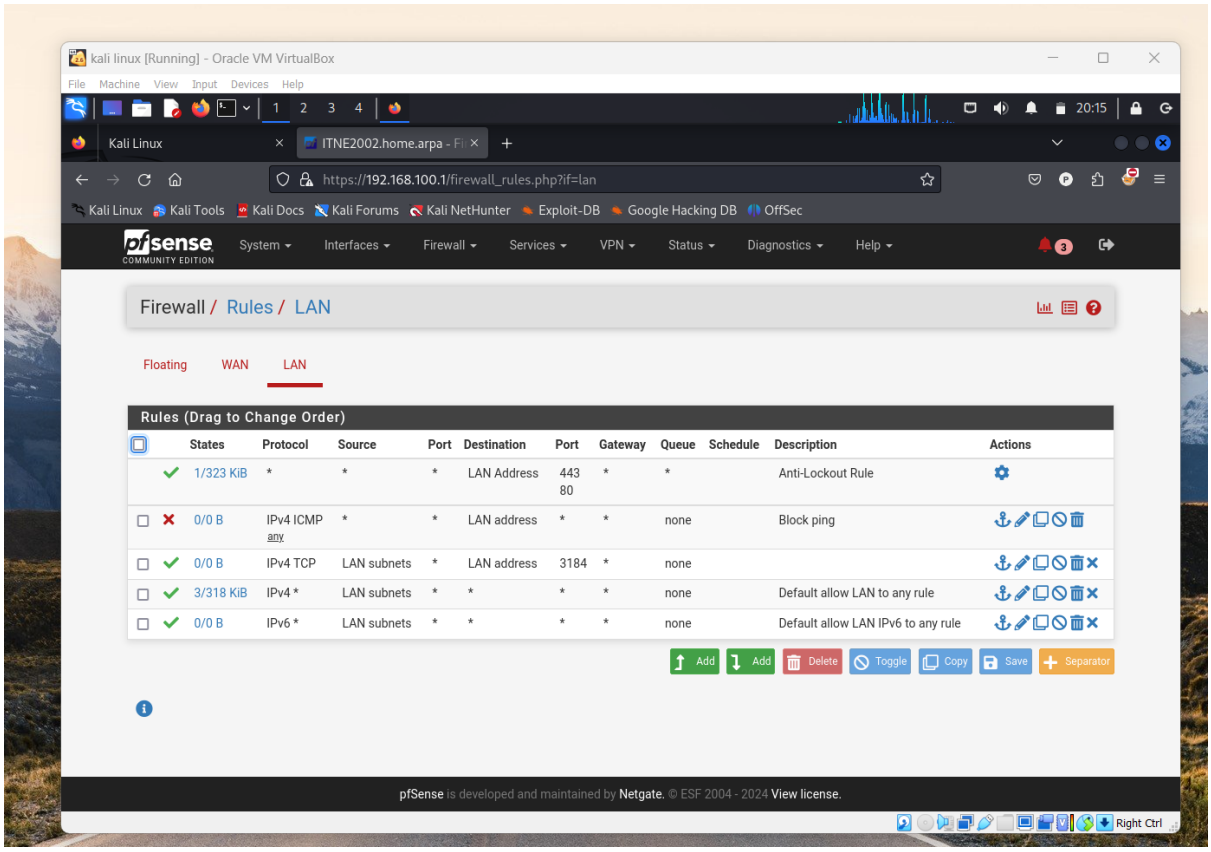
e. Configure firewall in pfSense

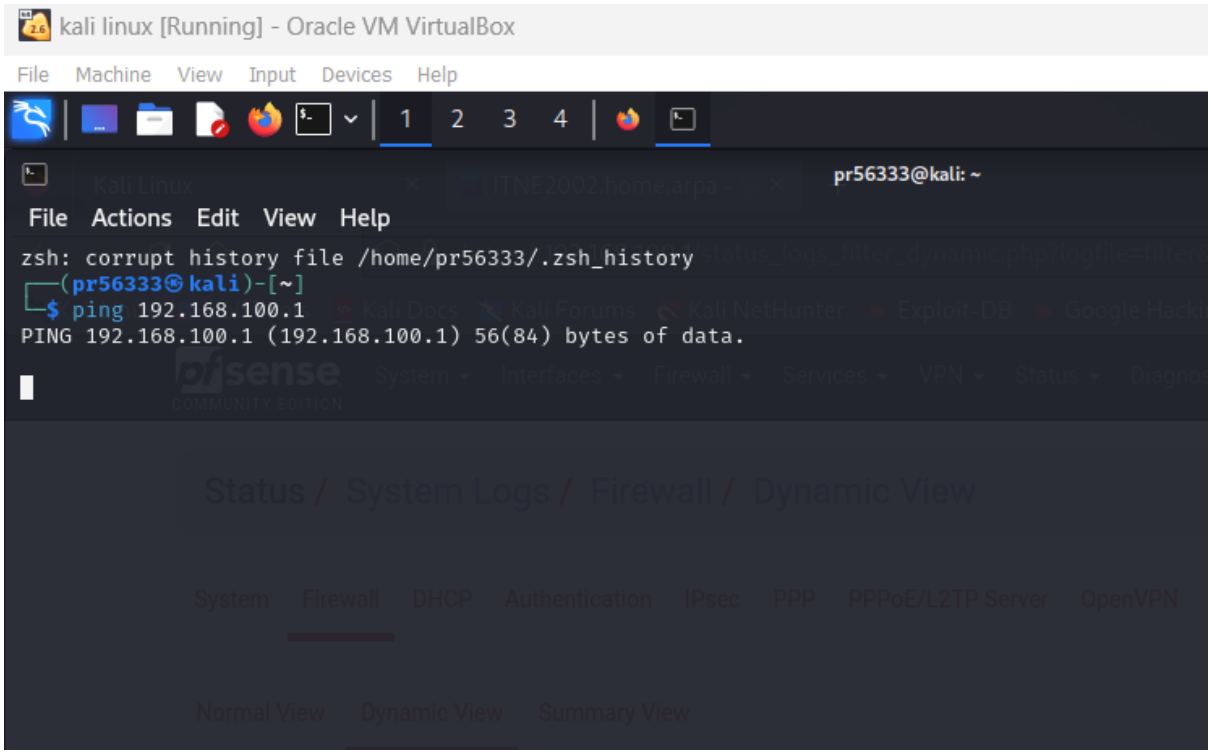


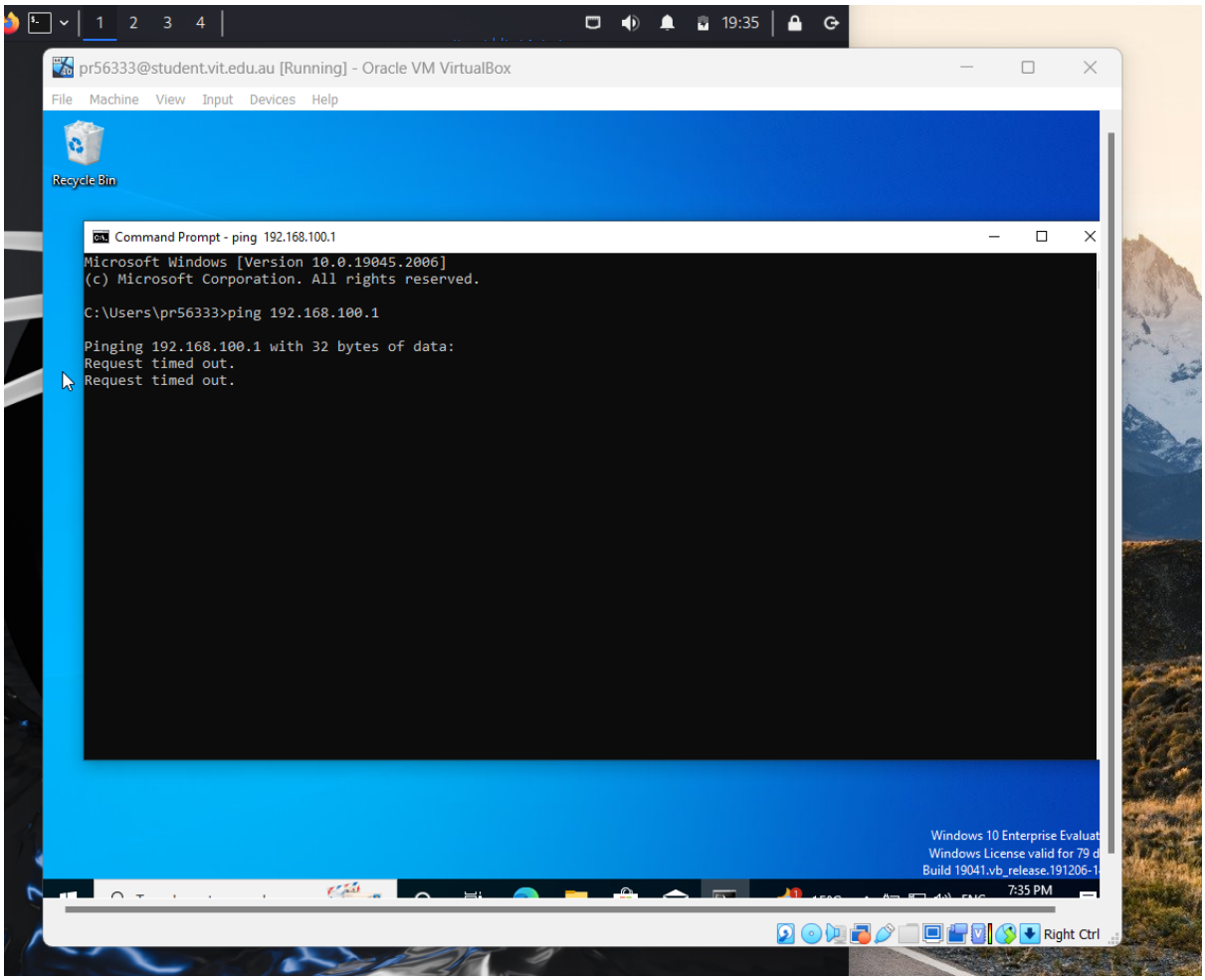

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
ITNE2002.home.arpa - Fi
https://192.168.100.1/firewall_rules.php?if=lan
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Firewall / Rules / LAN
Floating WAN LAN
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions
2/1.81 MiB * * * LAN Address 443 80 * * Anti-Lockout Rule
27/474.49 MiB IPv4 TCP LAN subnets * LAN address 3184 * none
0/11 KiB IPv4 * LAN subnets * * * * none Default allow LAN to any rule
0/0 B IPv6 * LAN subnets * * * * none Default allow LAN IPv6 to any rule
Add Add Delete Toggle Copy Save Separator
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Right Ctrl


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ITNE2002.home.arpa - Firewall: Rules: Edit
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
Firewall / Rules / Edit
Edit Firewall Rule
Action
Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
LAN
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
ICMP
Choose which IP protocol this rule should match.
ICMP Subtypes
any
Alternate Host
Datagram conversion error
Echo reply
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.
Source
Source
Invert match
Any
Source Address
Search


kali linux [Running] - Oracle VM VirtualBox
https://192.168.100.1/firewall_rules_edit.php?id=0
Echo reply
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.
Source
Source
Invert match
Any
Source Address
Destination
Destination
Invert match
LAN address
Destination Address
Extra Options
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description
Block ping
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options
Display Advanced
Rule Information
Tracking ID
1728462383
Created
10/9/24 19:26:23 by admin@192.168.100.51 (Local Database)
Updated
10/9/24 19:31:46 by admin@192.168.100.51 (Local Database)


kali linux [Running] - Oracle VM VirtualBox
https://192.168.100.1/firewall_rules.php?if=lan
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / LAN
Floating
WAN
LAN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
1/323 KiB * * * LAN Address 443 80 * * Anti-Lockout Rule
0/0 B IPv4 ICMP any * * LAN address * * none Block ping
0/0 B IPv4 TCP LAN subnets * LAN address 3184 * none
3/318 KiB IPv4 * LAN subnets * * * * none Default allow LAN to any rule
0/0 B IPv6 * LAN subnets * * * * none Default allow LAN IPv6 to any rule
Add
Add
Delete
Toggle
Copy
Save
Separator
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
pr56333@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/pr56333/.zsh_history
(pr56333㉿kali)-[~]
$ ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.


1 2 3 4
19:35
pr56333@student.vit.edu.au [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Command Prompt - ping 192.168.100.1
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.
C:\Users\pr56333>ping 192.168.100.1
Pinging 192.168.100.1 with 32 bytes of data:
Request timed out.
Request timed out.
Windows 10 Enterprise Evaluat
Windows License valid for 79 d
Build 19041.vb_release.191206-1
7:35 PM
Right Ctrl