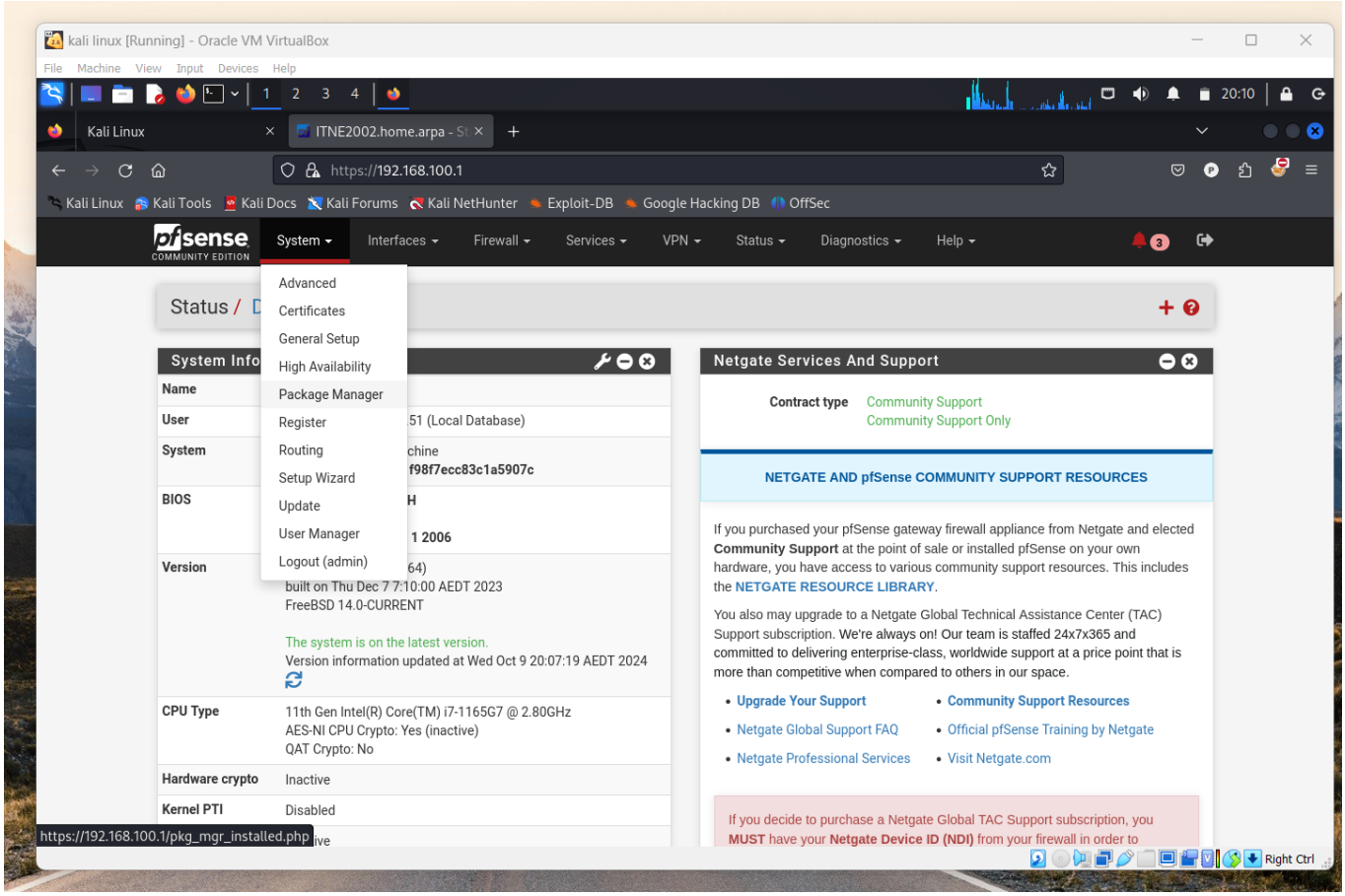
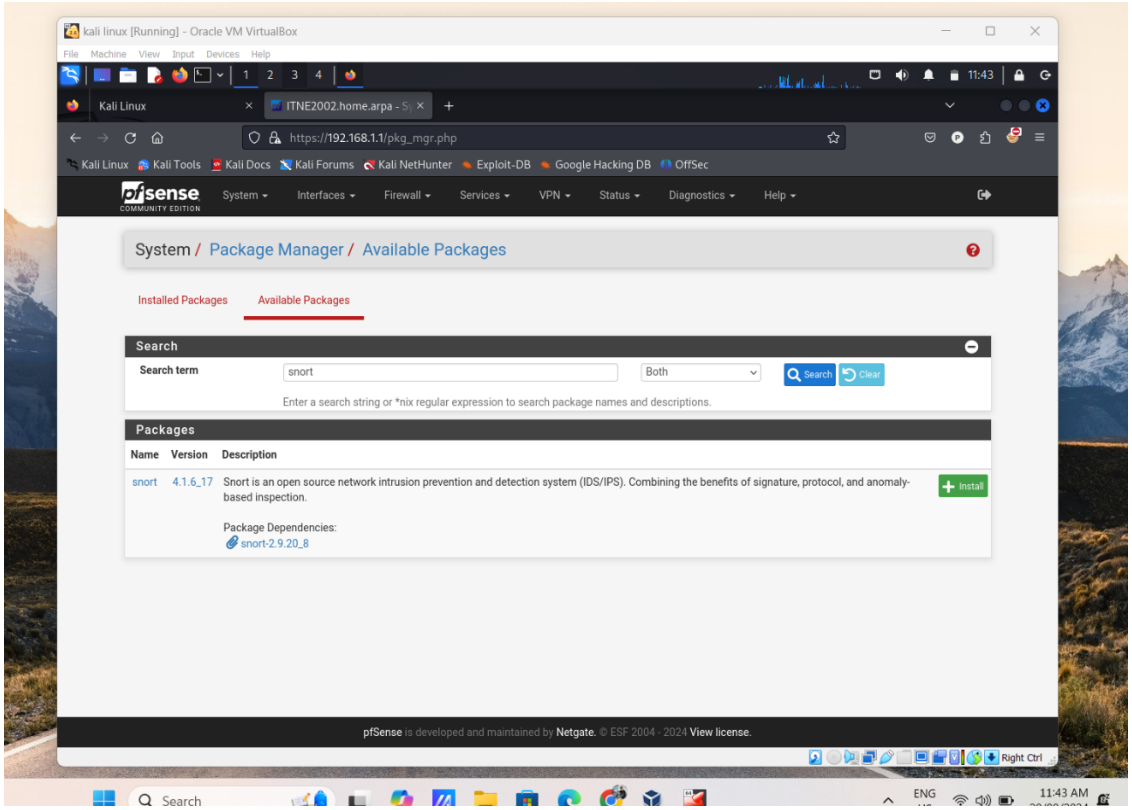
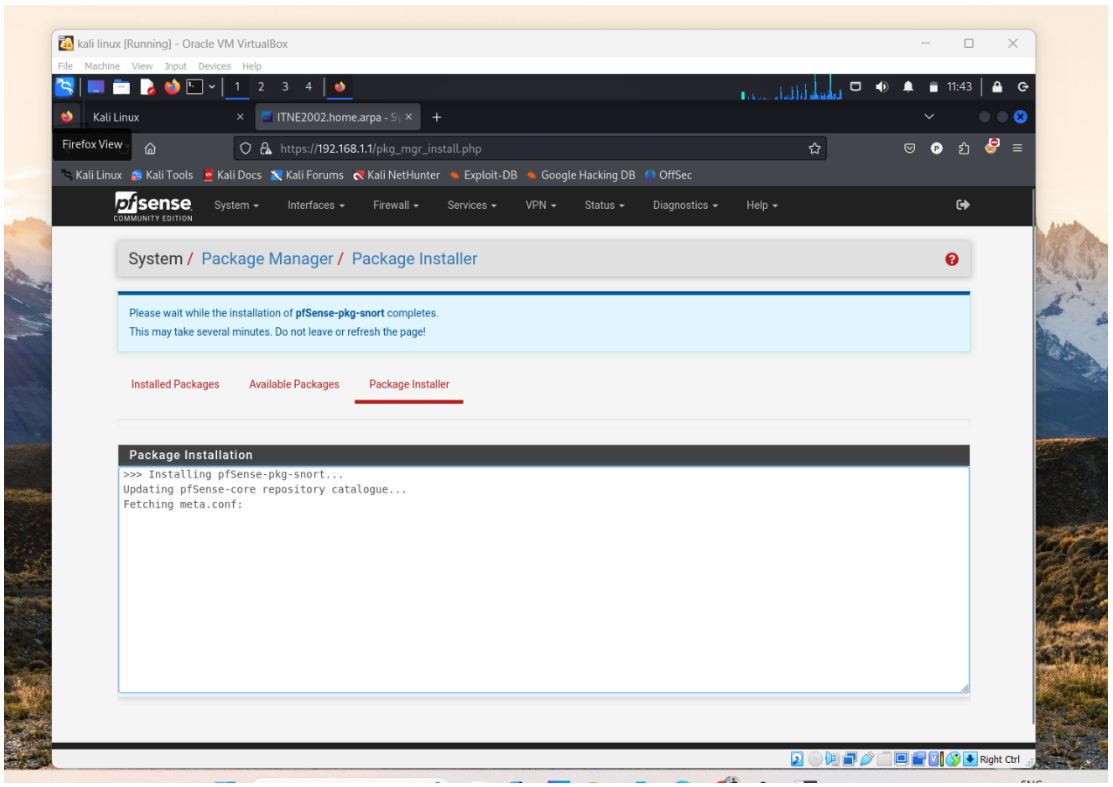
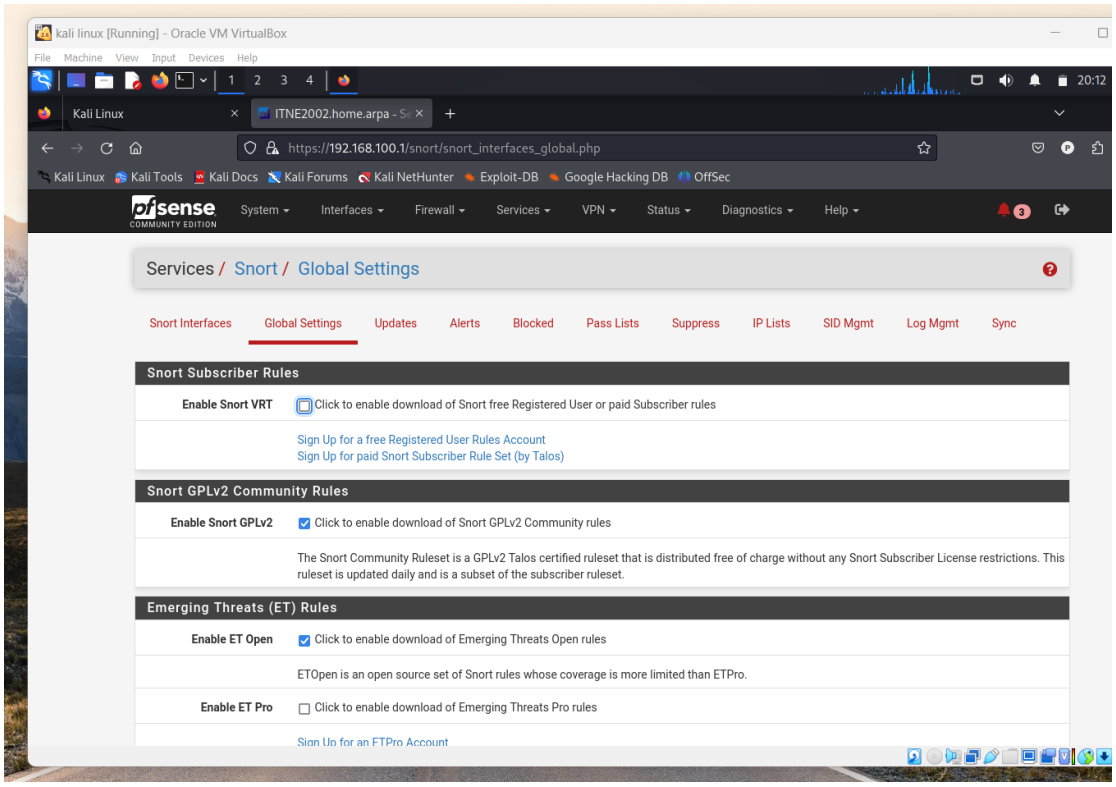
Table of Contents

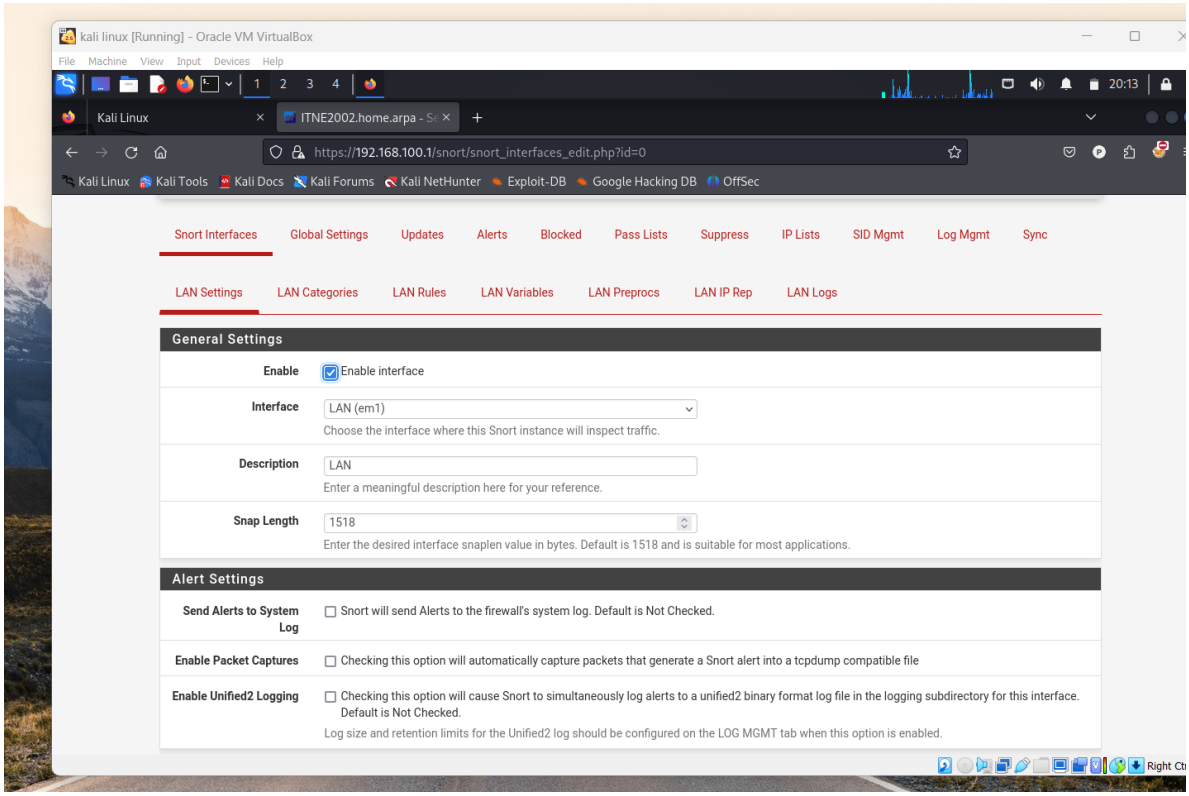
a. Configure Snort to detect local intrusions and attack the pfSense system through Kali Linux using ping sweep and attach the report.

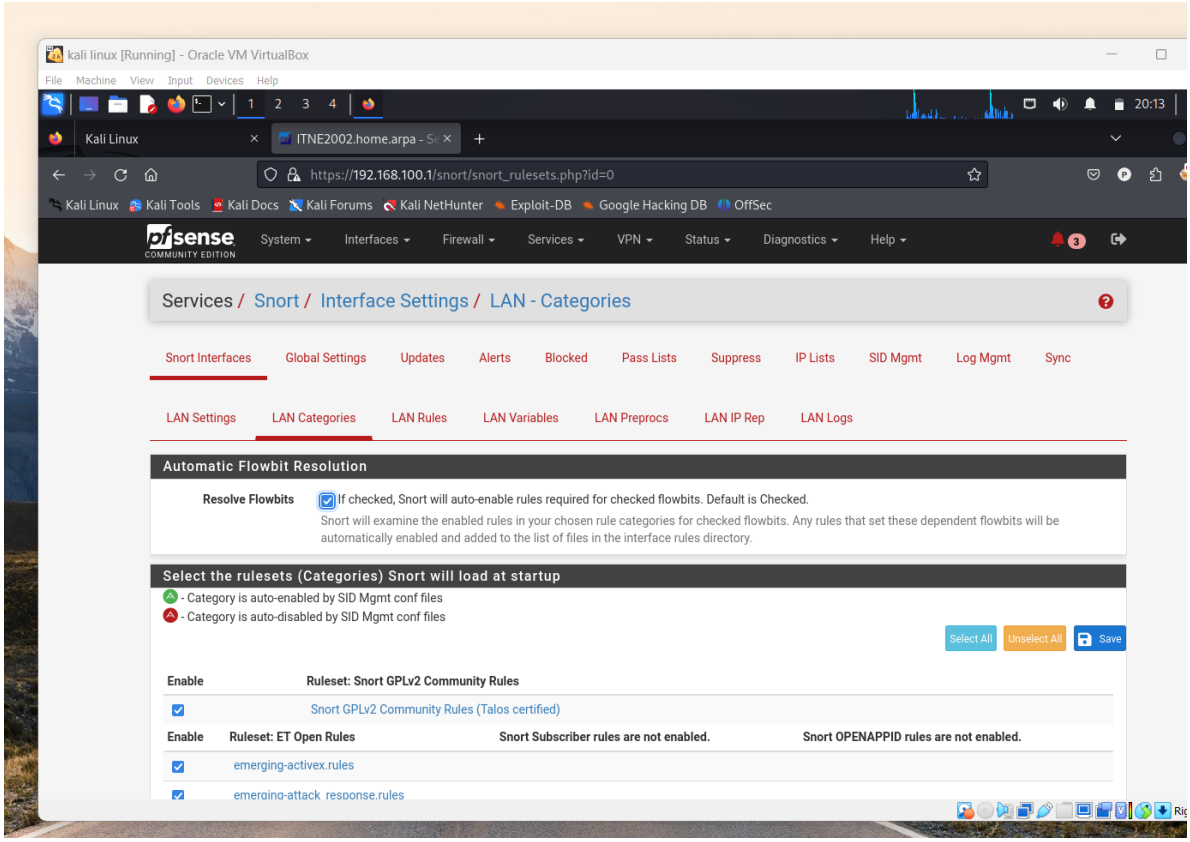


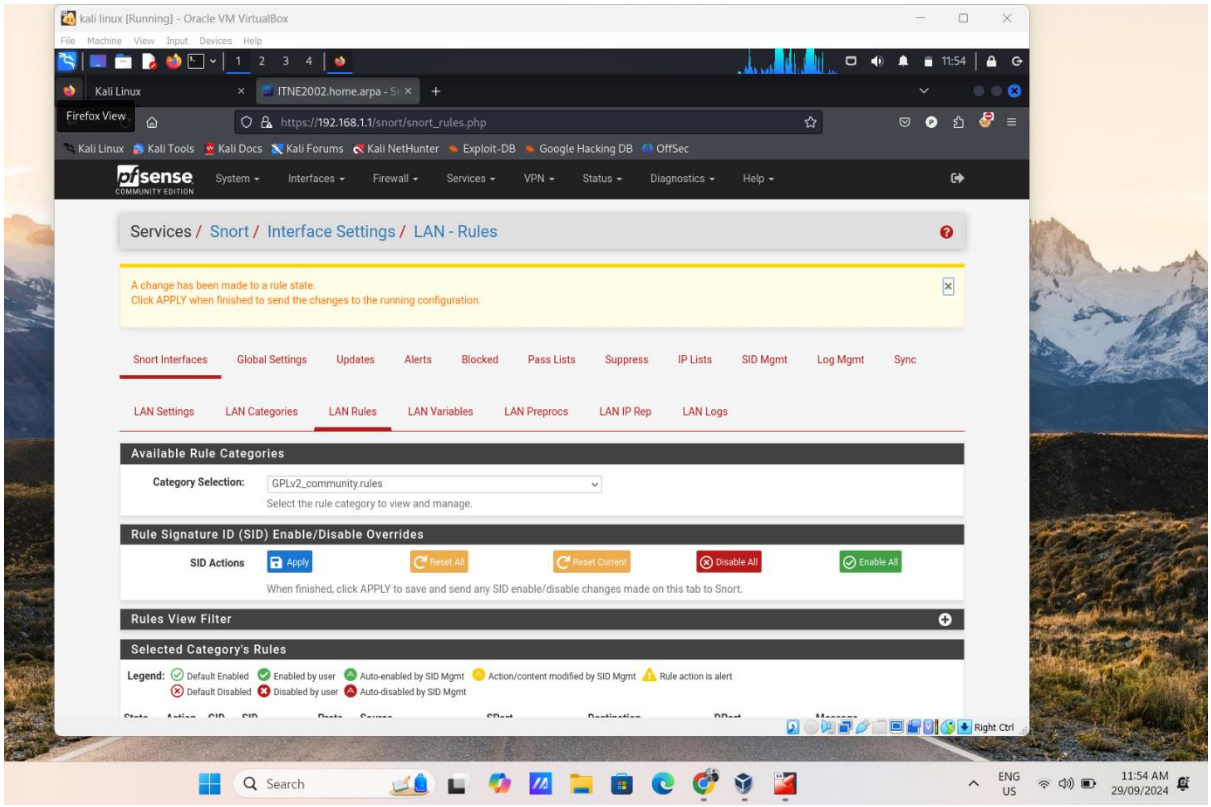

kali linux [Running] - Oracle VM VirtualBox
Kali Linux
ITNE2002.home.arpa
https://192.168.1.1/pkg_mgr.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
System / Package 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.
Package Dependencies:
snort-2.9.20_8
Install
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
Right Ctrl
Search
ENG
11:43 AM

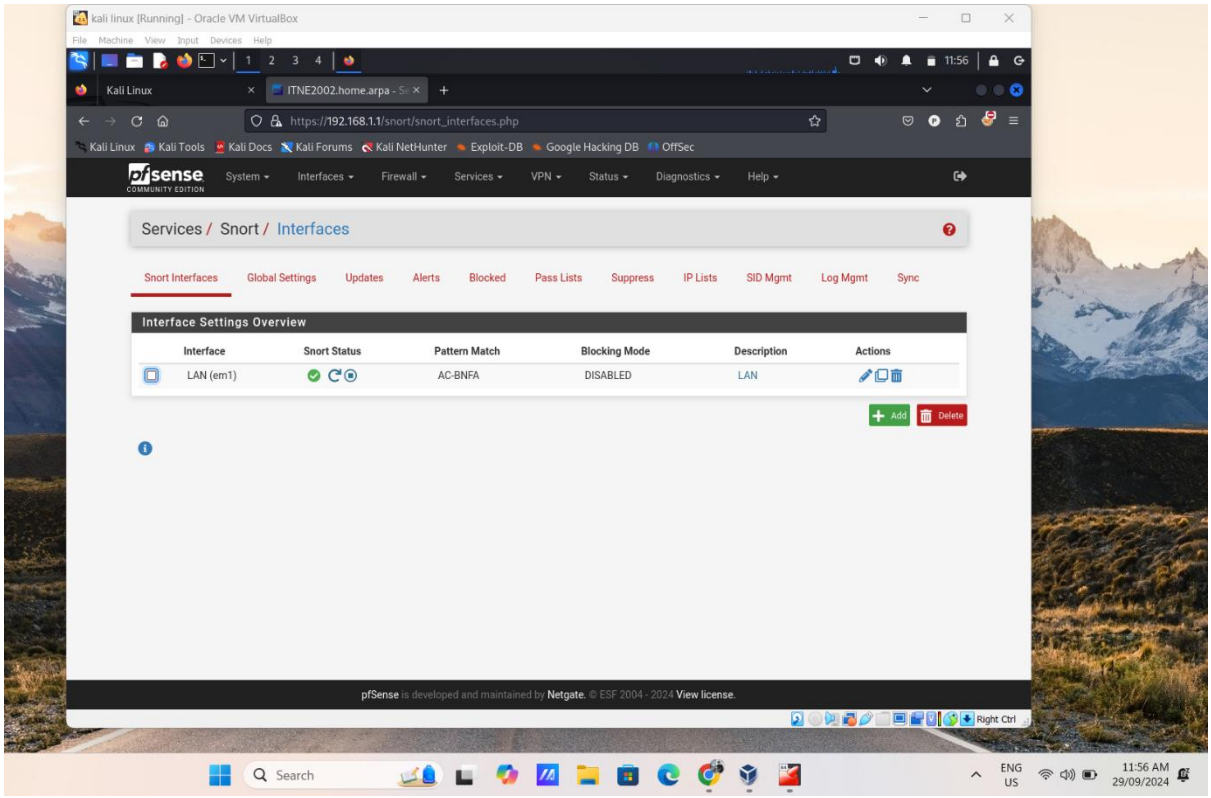

kali linux [Running] - Oracle VM VirtualBox
Kali Linux
ITNE2002.home.arpa
Firefox View
https://192.168.1.1/pkg_mgr_install.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
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:
Right Ctrl

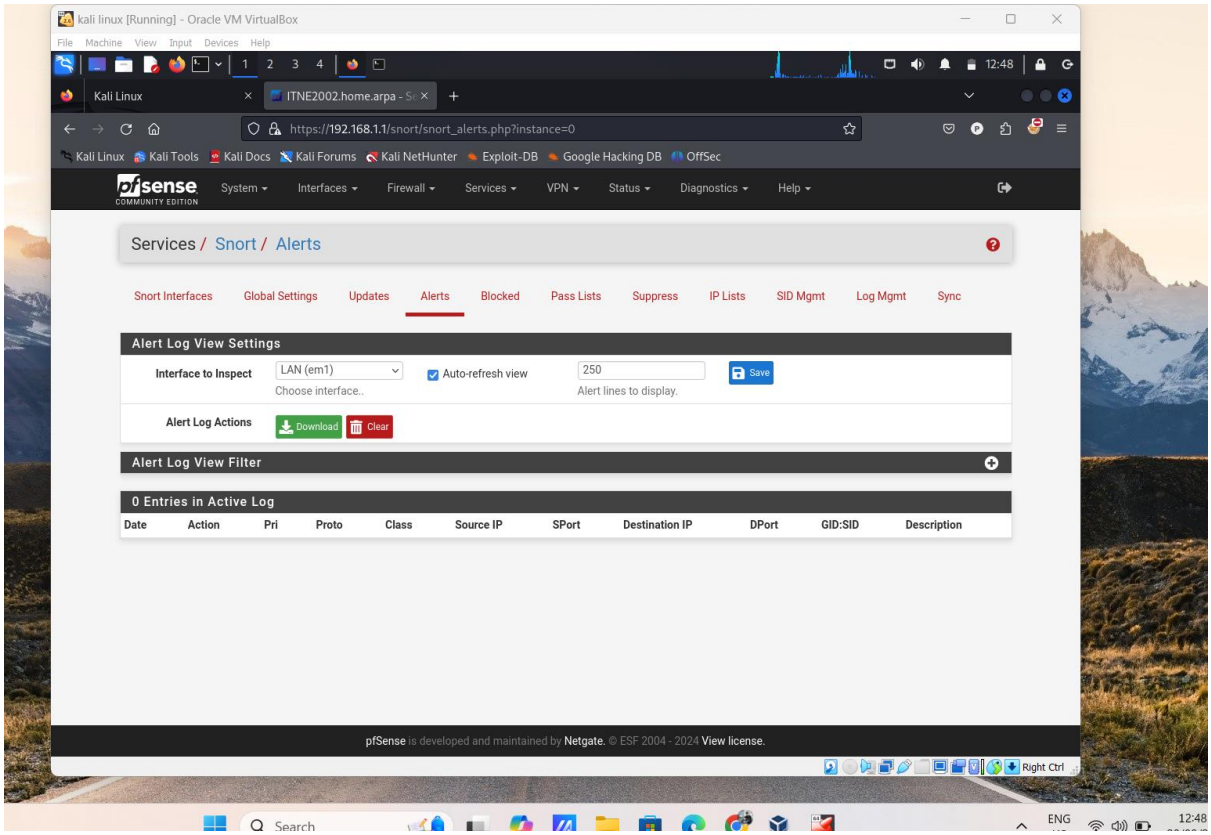

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
20:12
Kali Linux
ITNE2002.home.arpa - Se
https://192.168.100.1/snort/snort_interfaces_global.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System 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

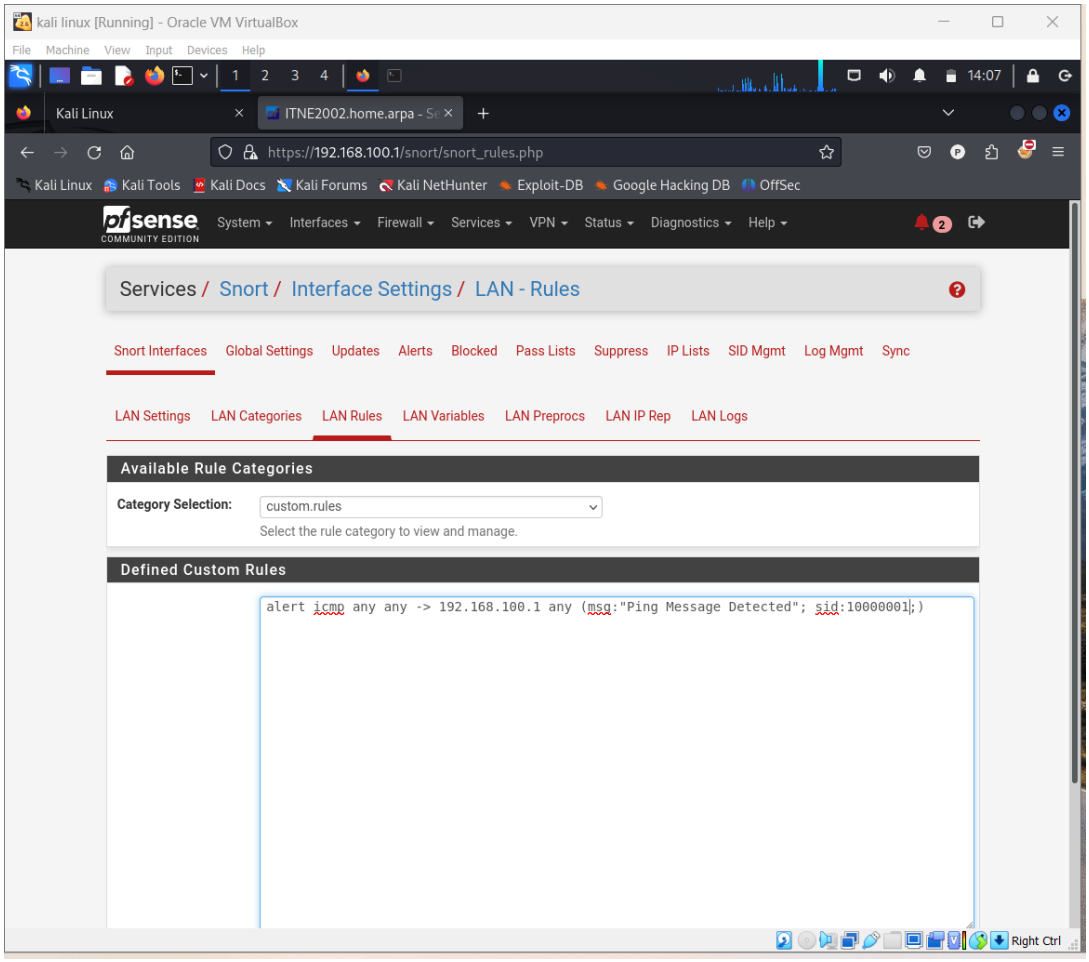

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
20:13
Kali Linux
ITNE2002.home.arpa - Se
https://192.168.100.1/snort/snort_interfaces_edit.php?id=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Snort Interfaces Global Settings 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
emerging-attack_response.rules

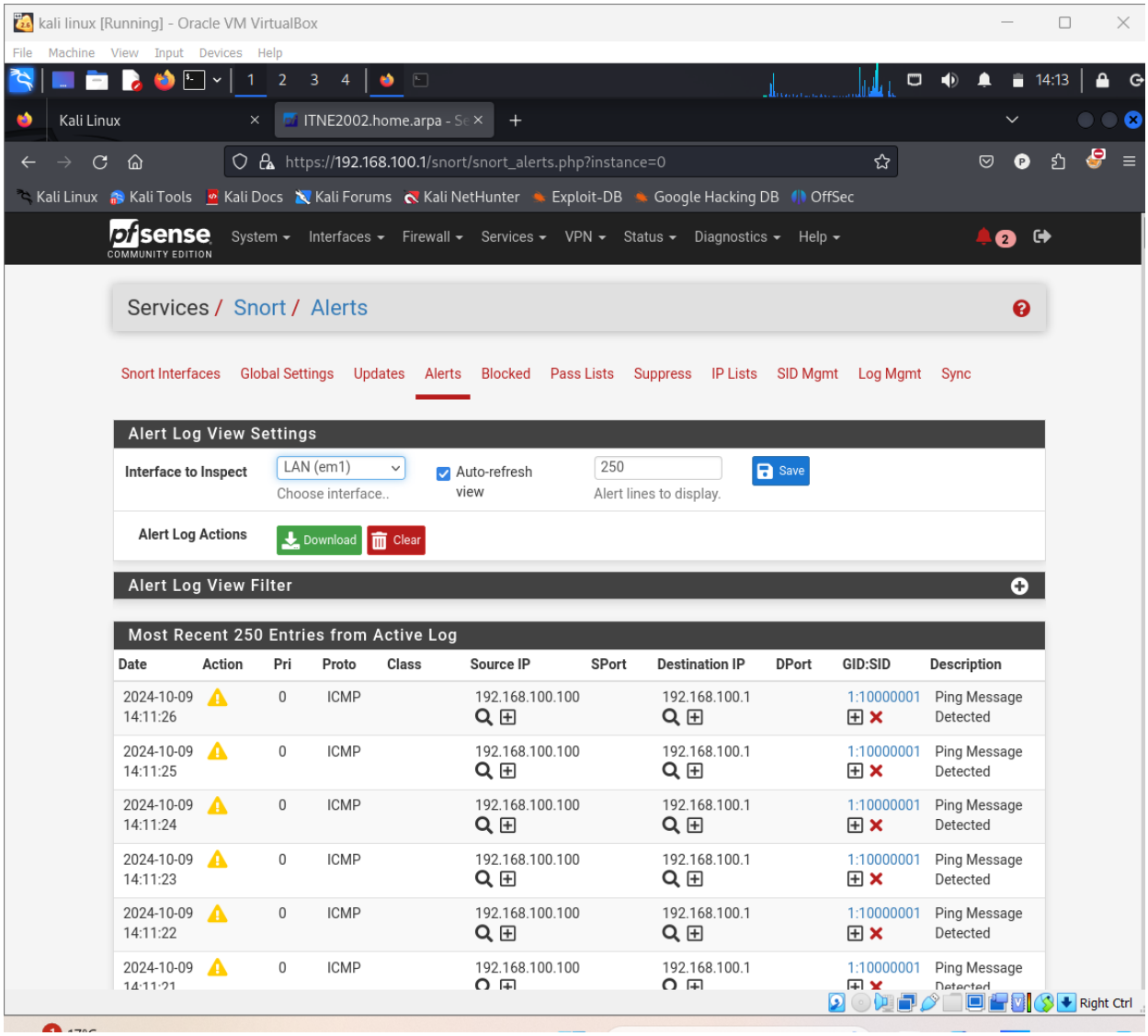

kali linux [Running] - Oracle VM VirtualBox
Kali Linux
Firefox View
ITNE2002.home.arpa
https://192.168.1.1/snort/snort_rules.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics 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

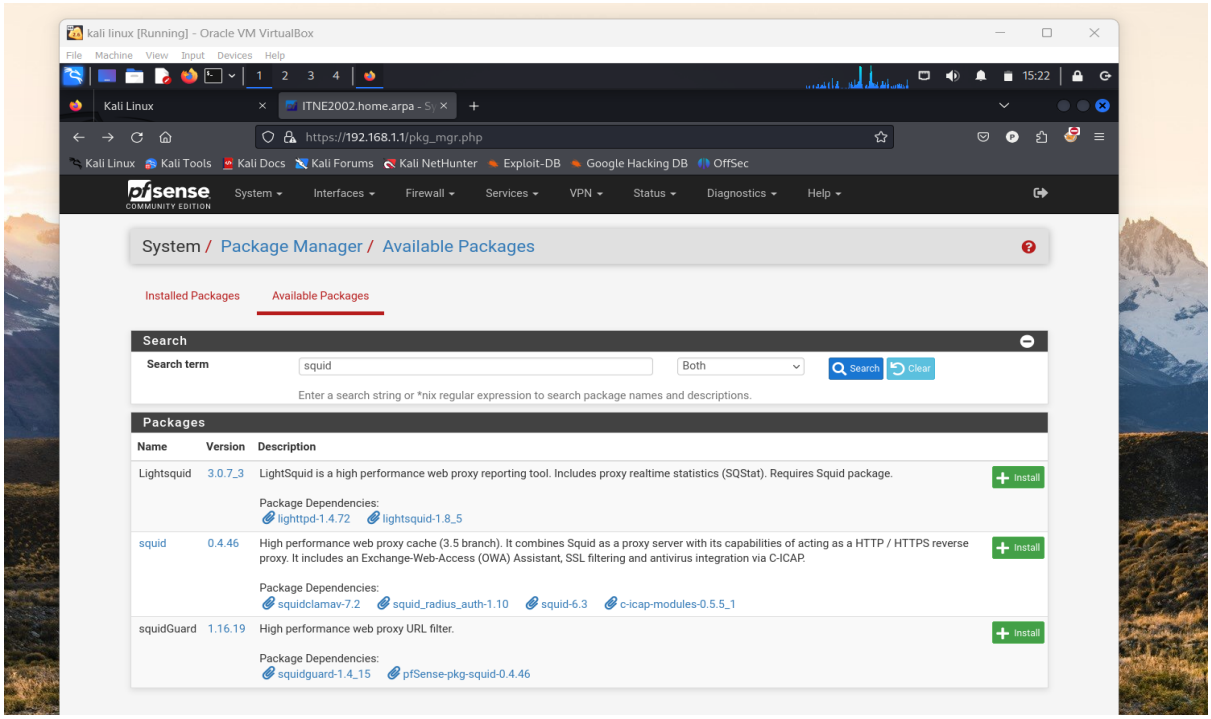

kali linux [Running] - Oracle VM VirtualBox
Kali Linux
ITNE2002.home.arpa
https://192.168.1.1/snort/snort_alerts.php?instance=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics 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

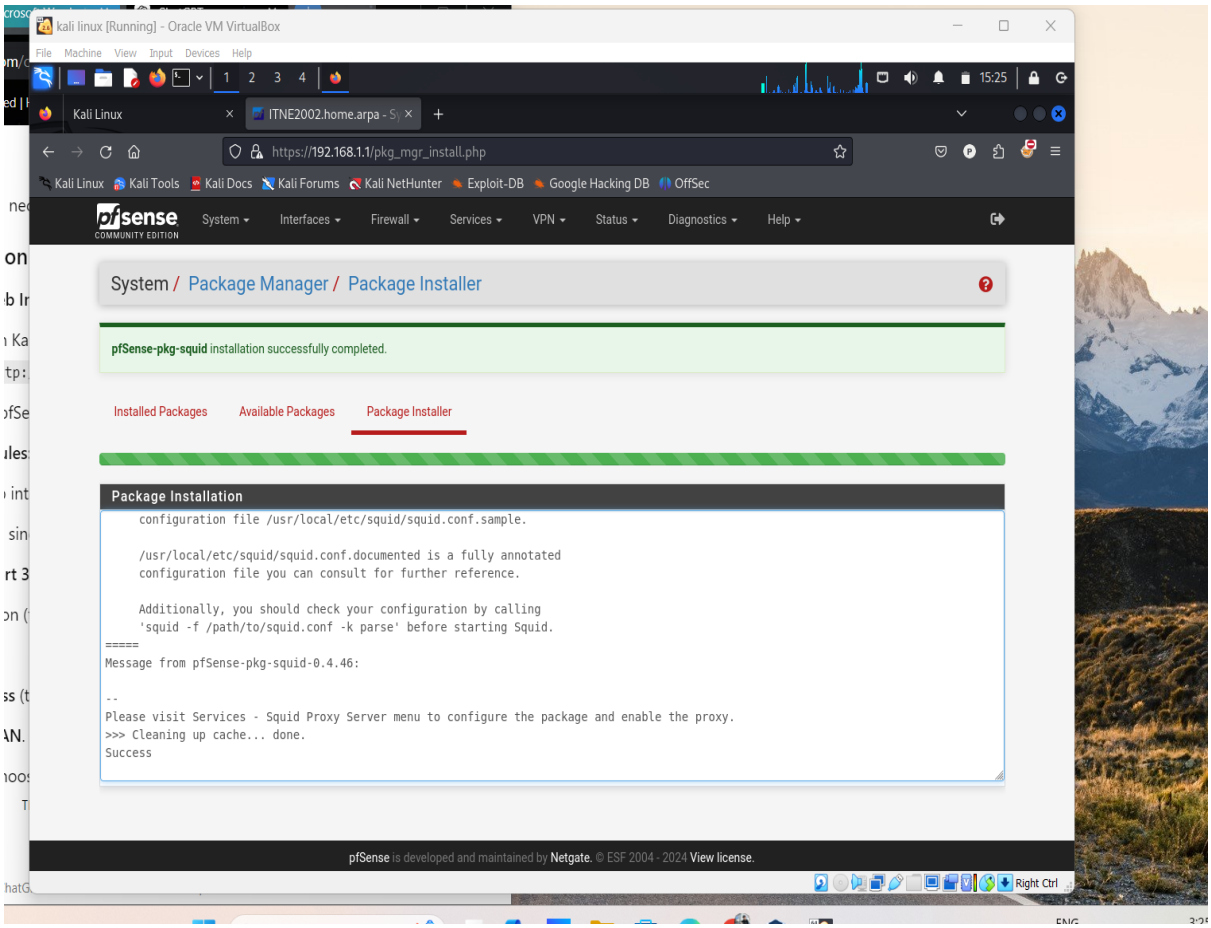


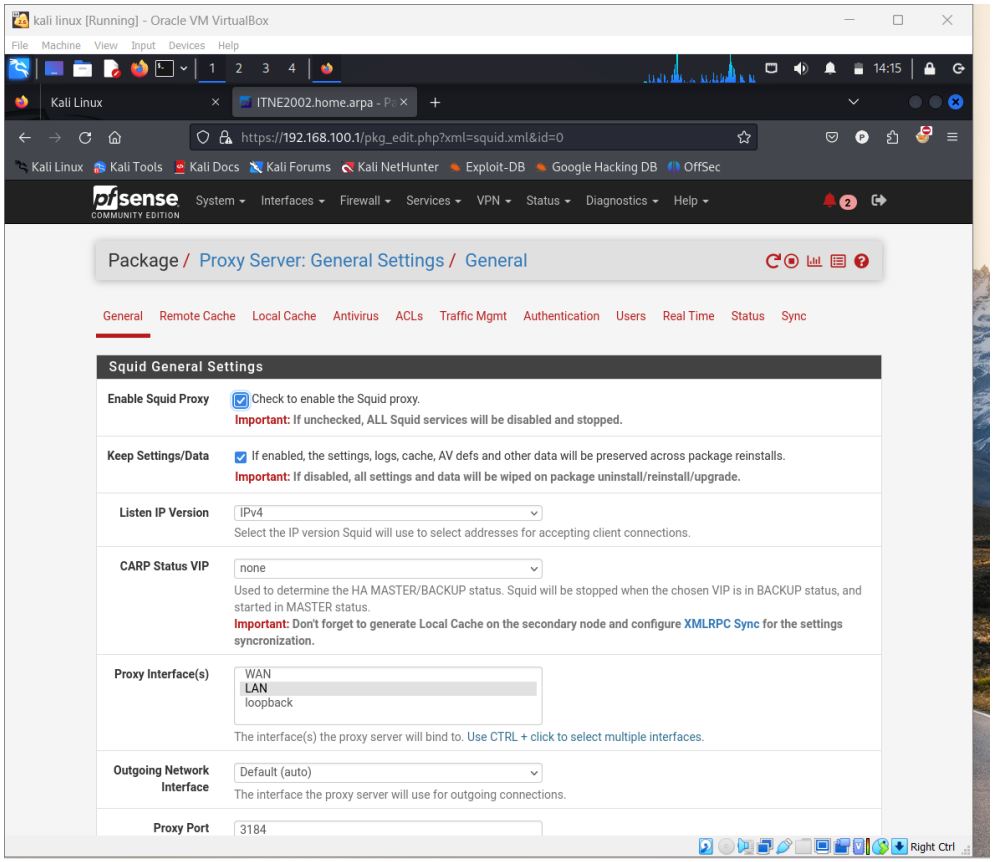

```
Nmap done: 256 IP addresses (3 hosts up) scanned in 1.80 seconds

┌──(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
```

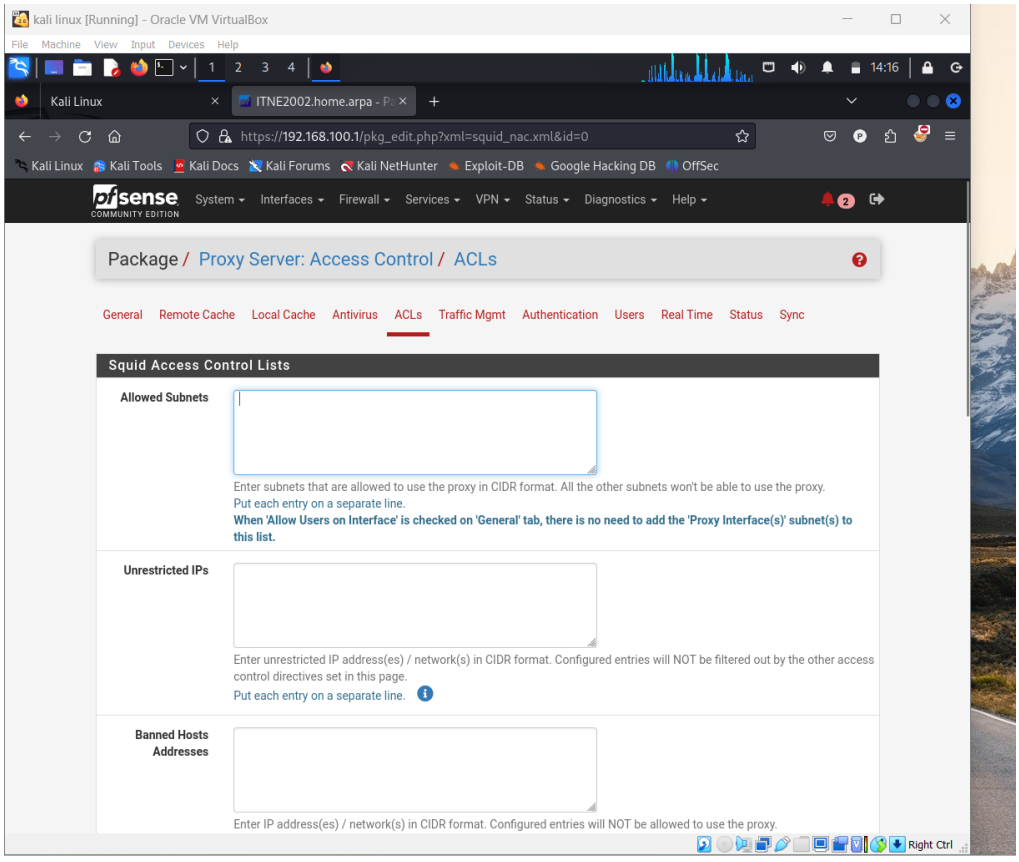

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
ITNE2002.home.arpa - Se
https://192.168.100.1/snort/snort_alerts.php?instance=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces 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

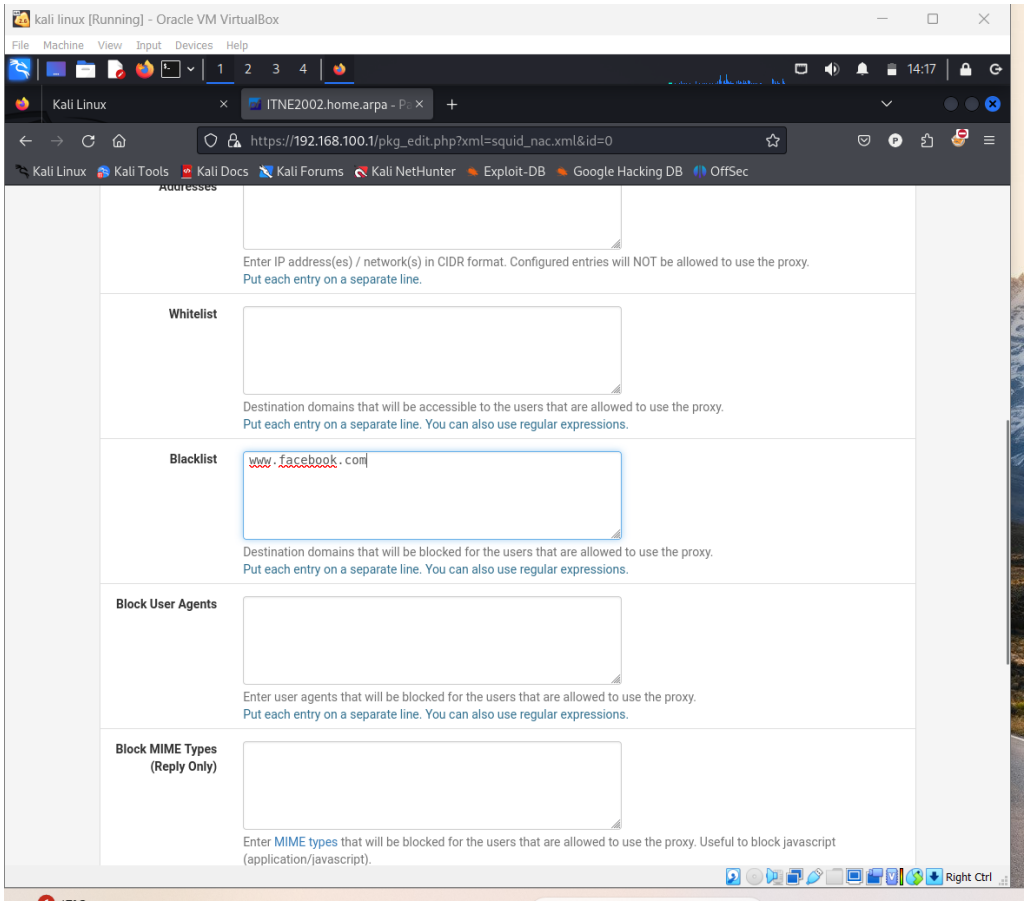
b. Use Squid to block (blacklist) www.facebook.com and attempt to access Facebook from the Windows 10 VM. Attach the output of the Windows.

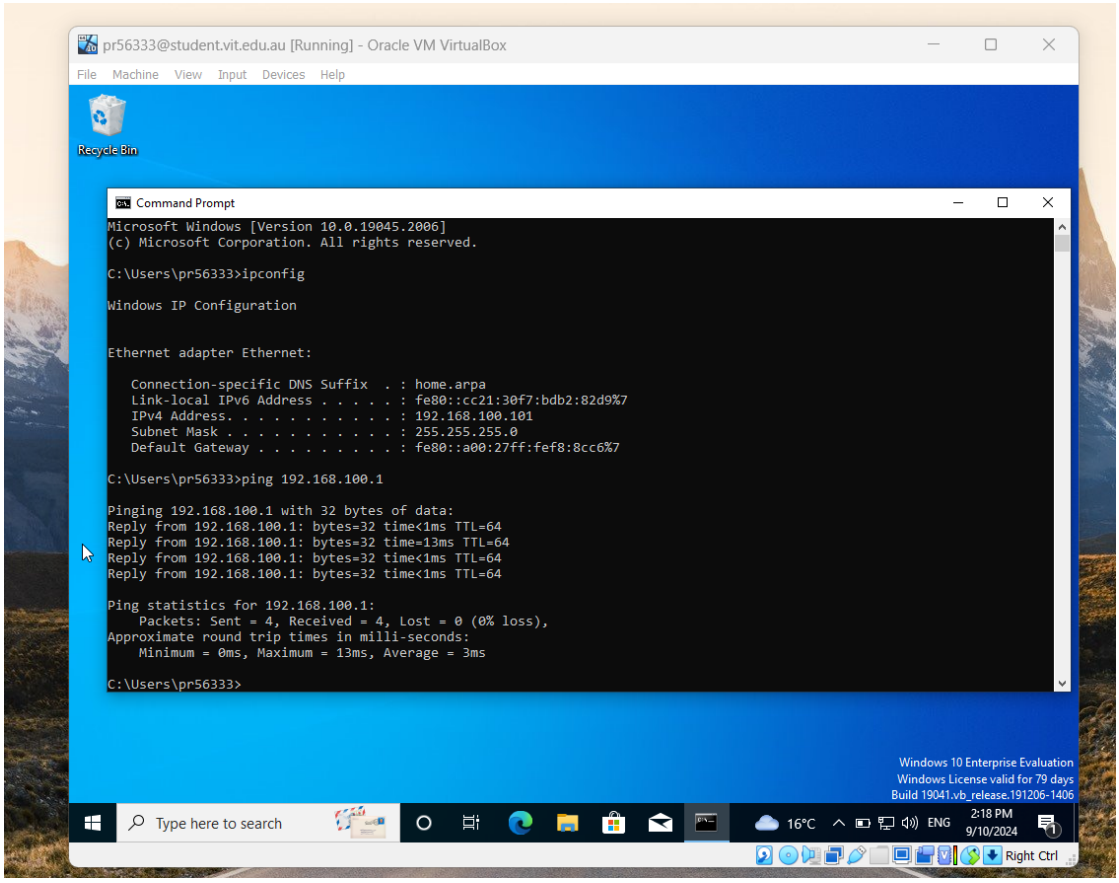


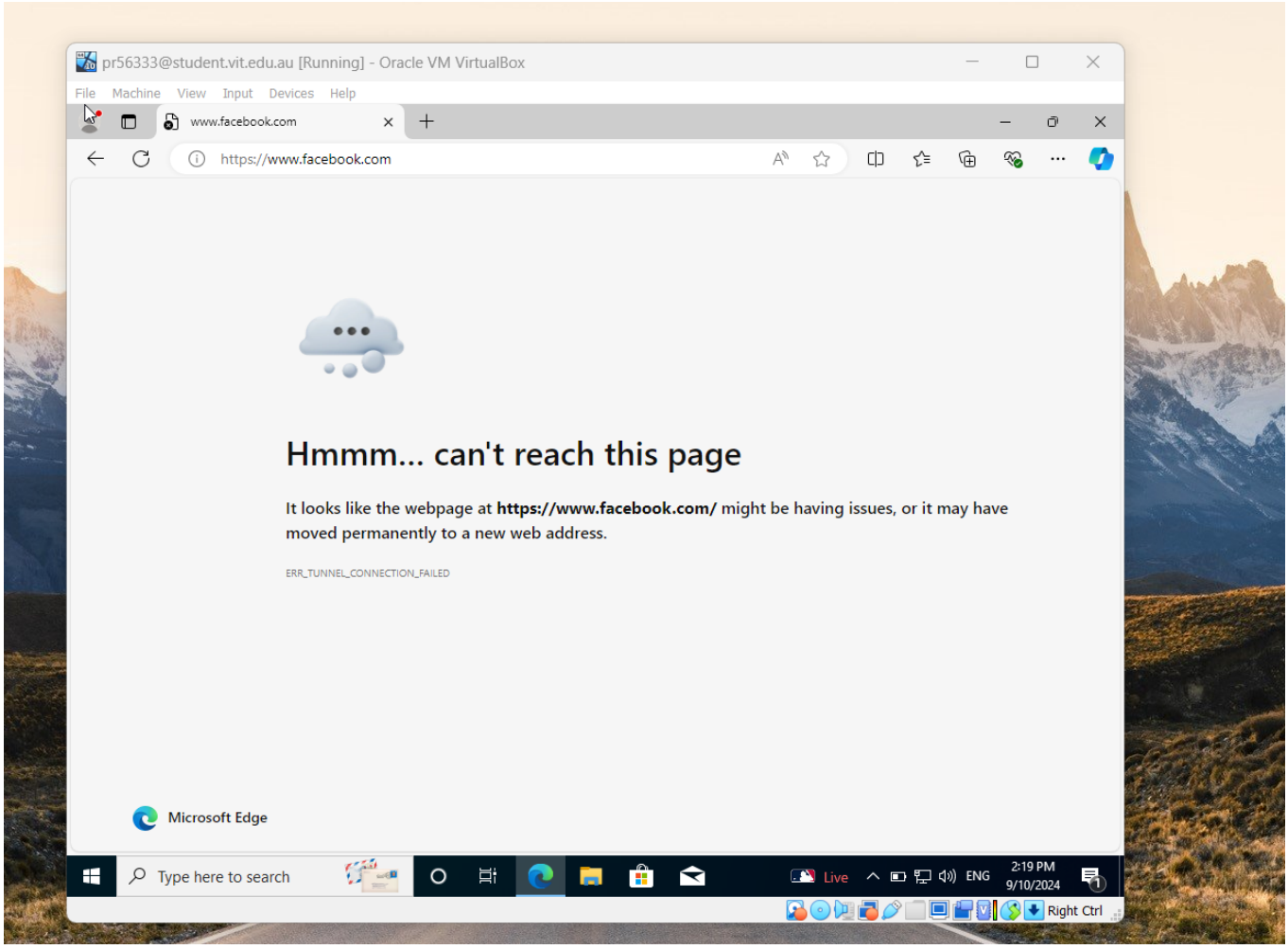



kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
ITNE2002.home.arpa
https://192.168.100.1/pkg_edit.php?xml=squid.xml&id=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
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
Right Ctrl

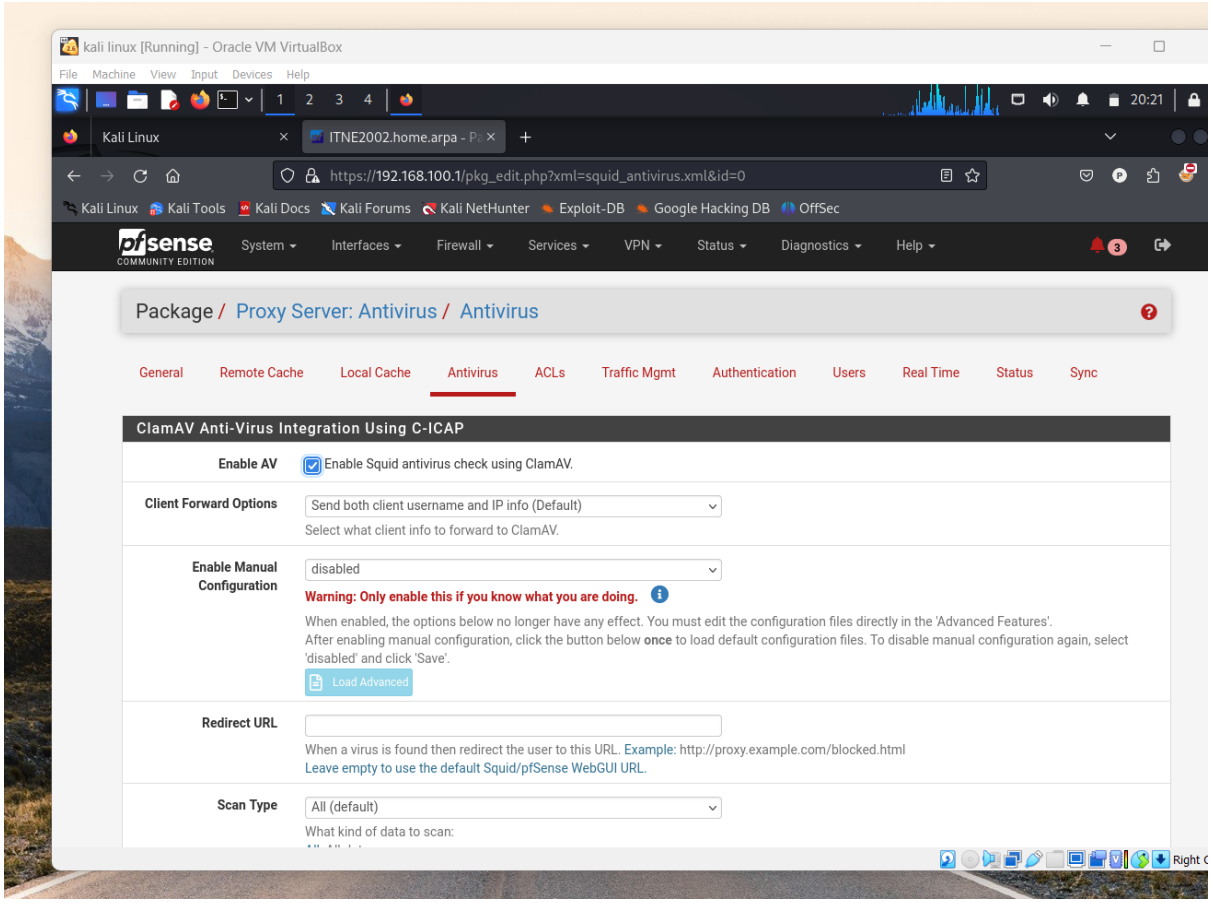

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
ITNE2002.home.arpa
https://192.168.100.1/pkg_edit.php?xml=squid_nac.xml&id=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces 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.
Right Ctrl

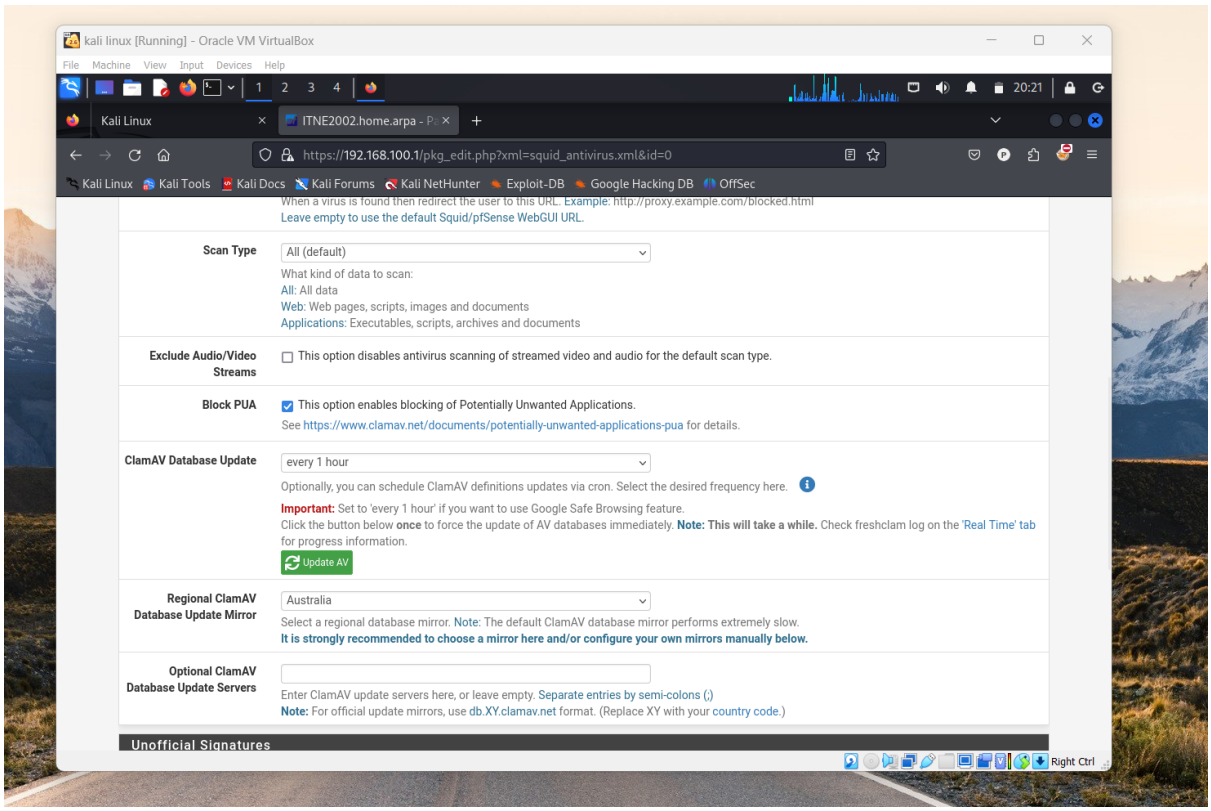

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
ITNE2002.home.arpa - Pf
https://192.168.100.1/pkg_edit.php?xml=squid_nac.xml&id=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Addresses
Enter IP address(es) / 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

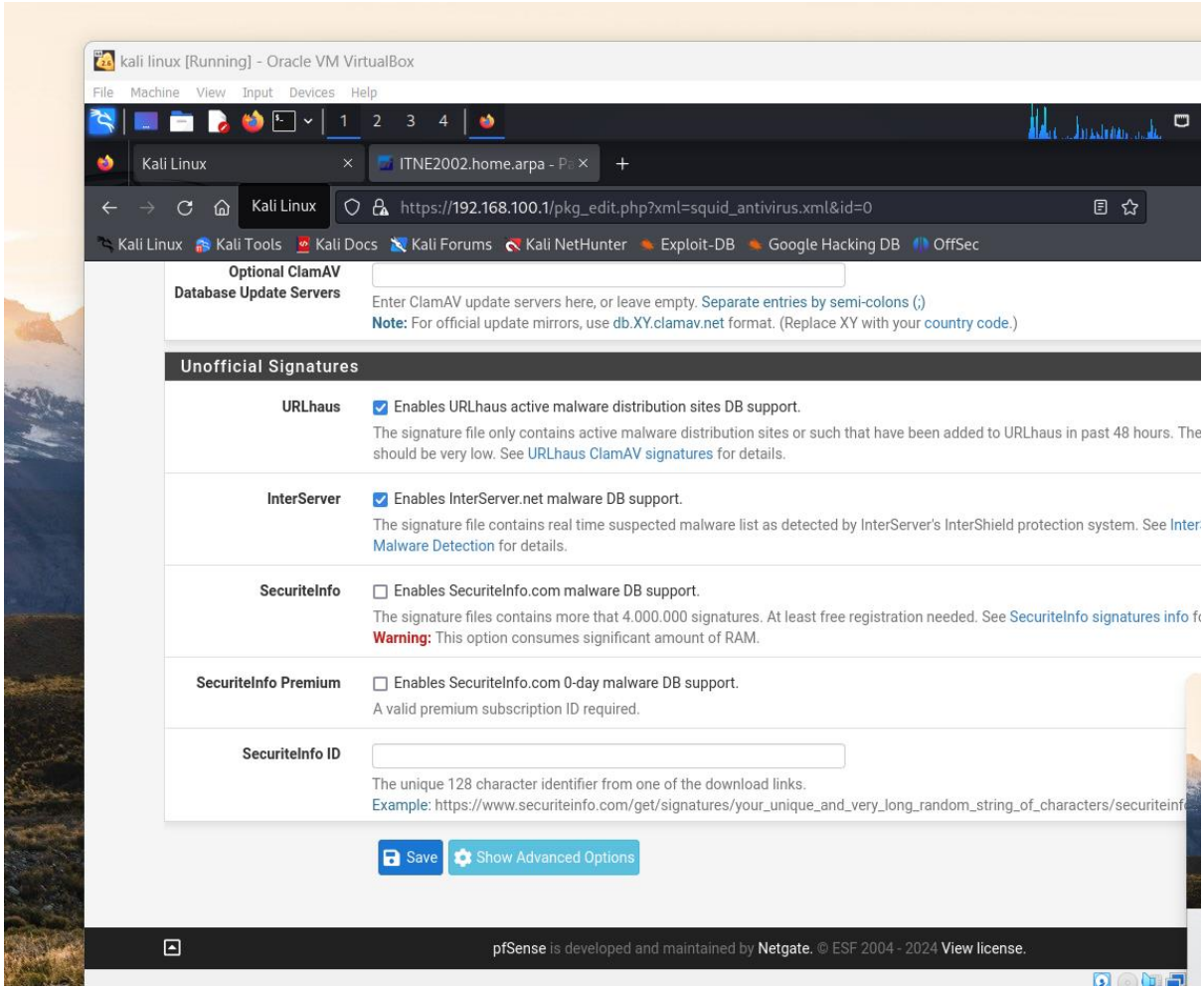

pr56333@student.vit.edu.au [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Command Prompt
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.
C:\Users\pr56333>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific 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

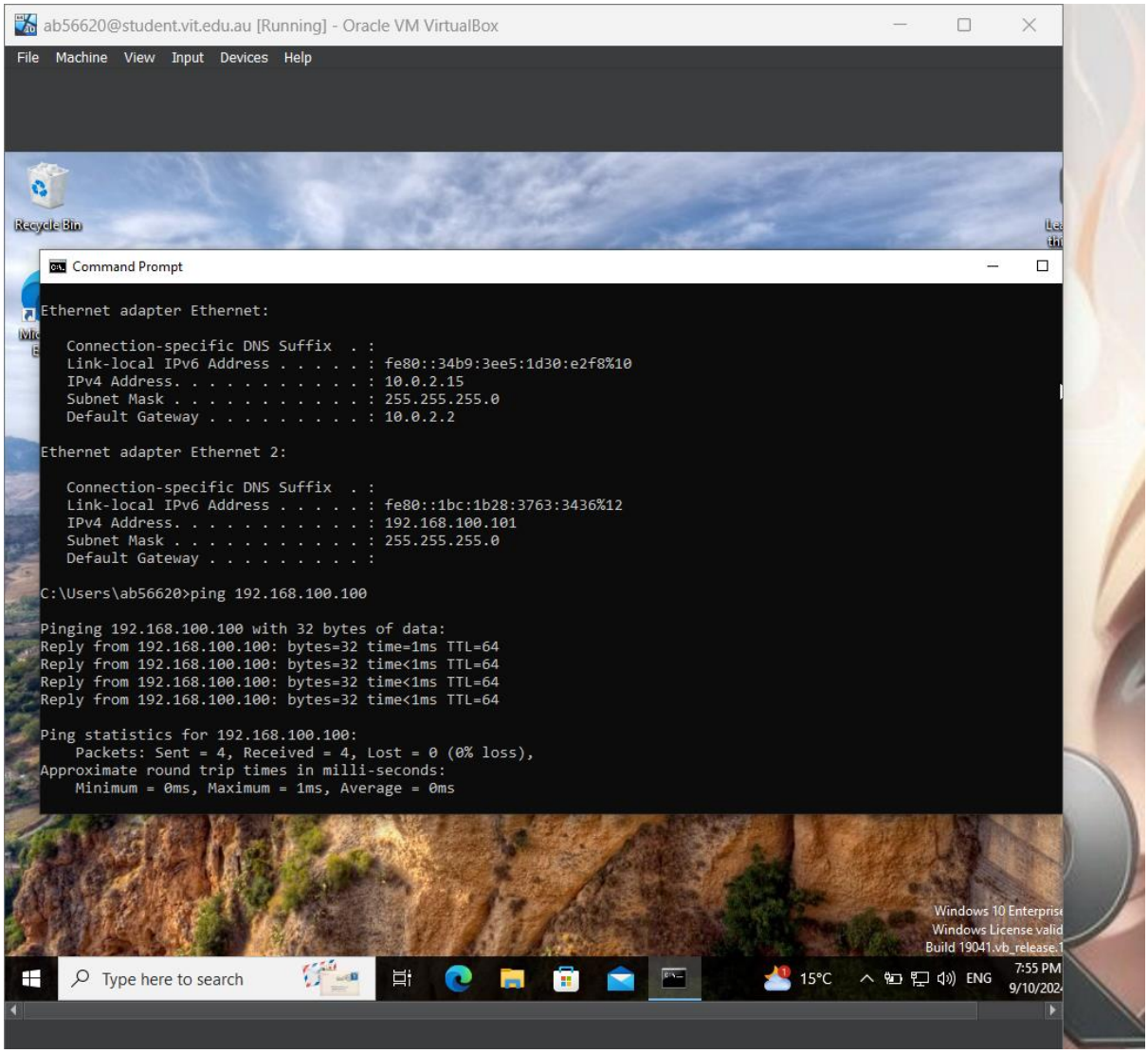
c. Installing ClamAV

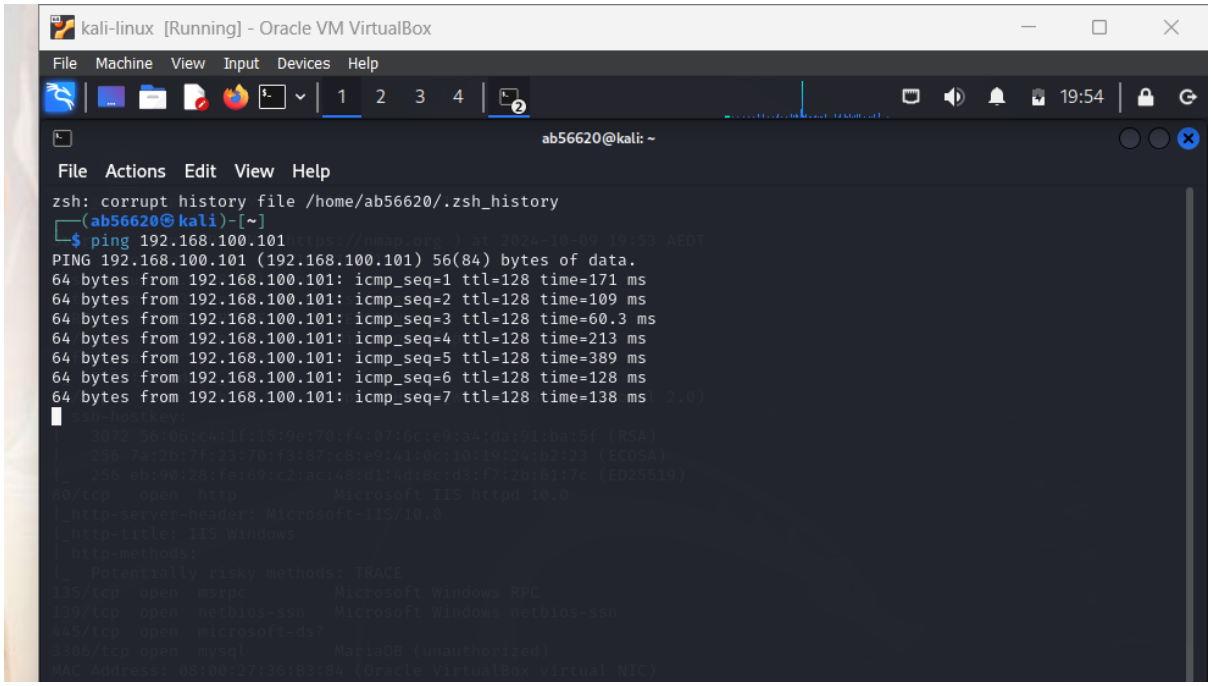


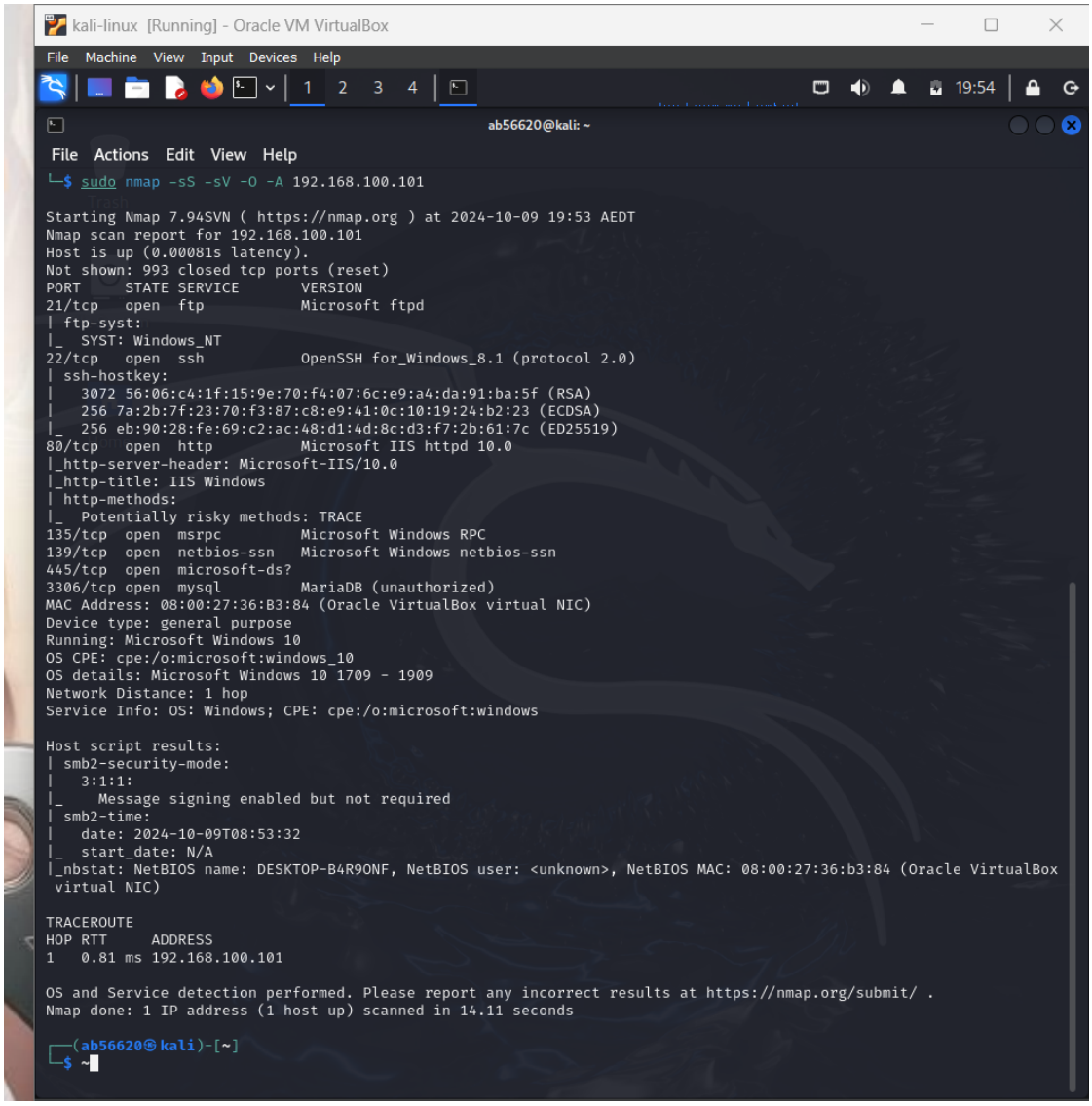



kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
ITNE2002.home.arpa - Pa
https://192.168.100.1/pkg_edit.php?xml=squid_antivirus.xml&id=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Optional ClamAV Database Update 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.

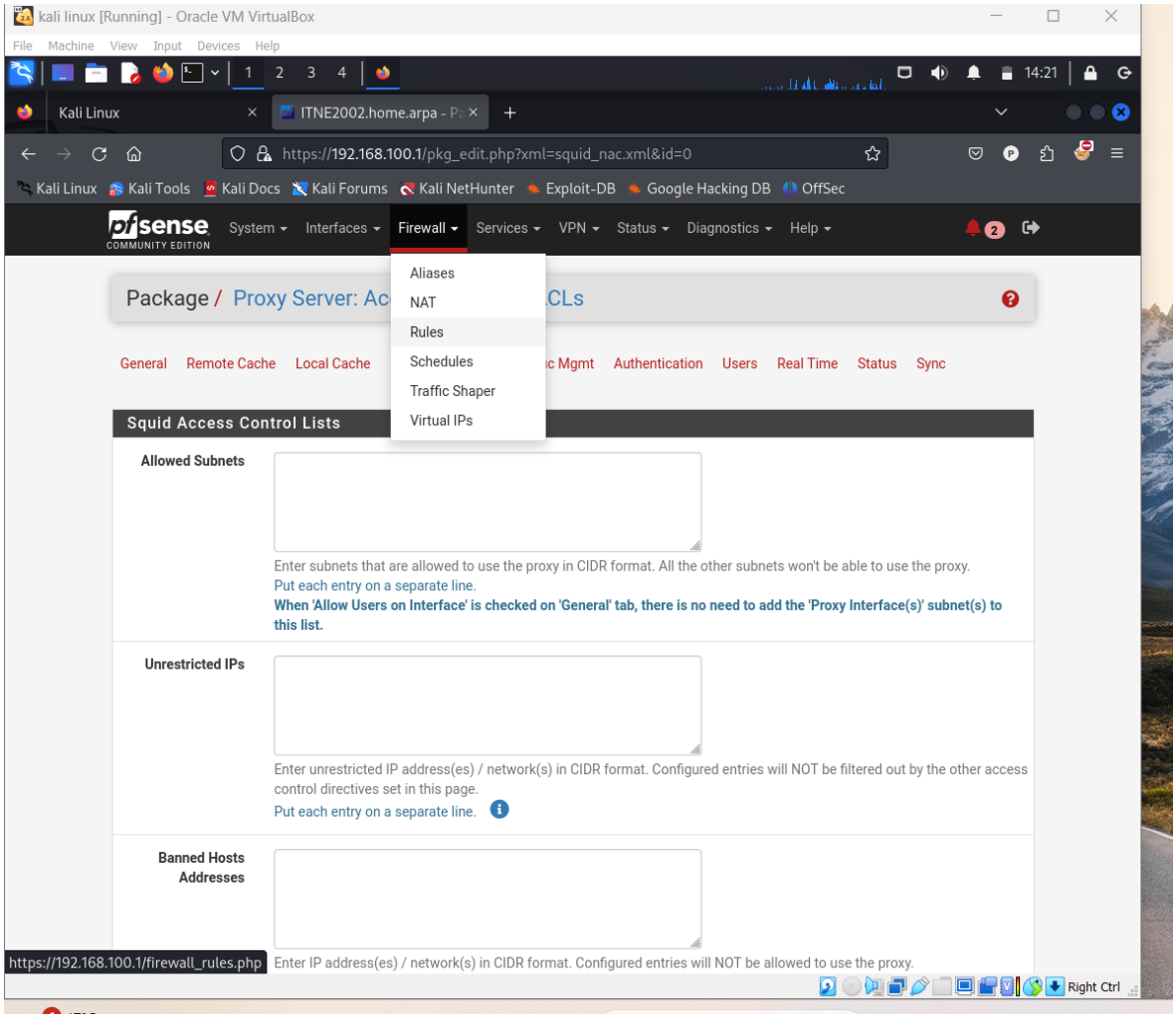
d. Scan windows 10 using Kali using Nmap and then provide a complete report on open ports and fix those.

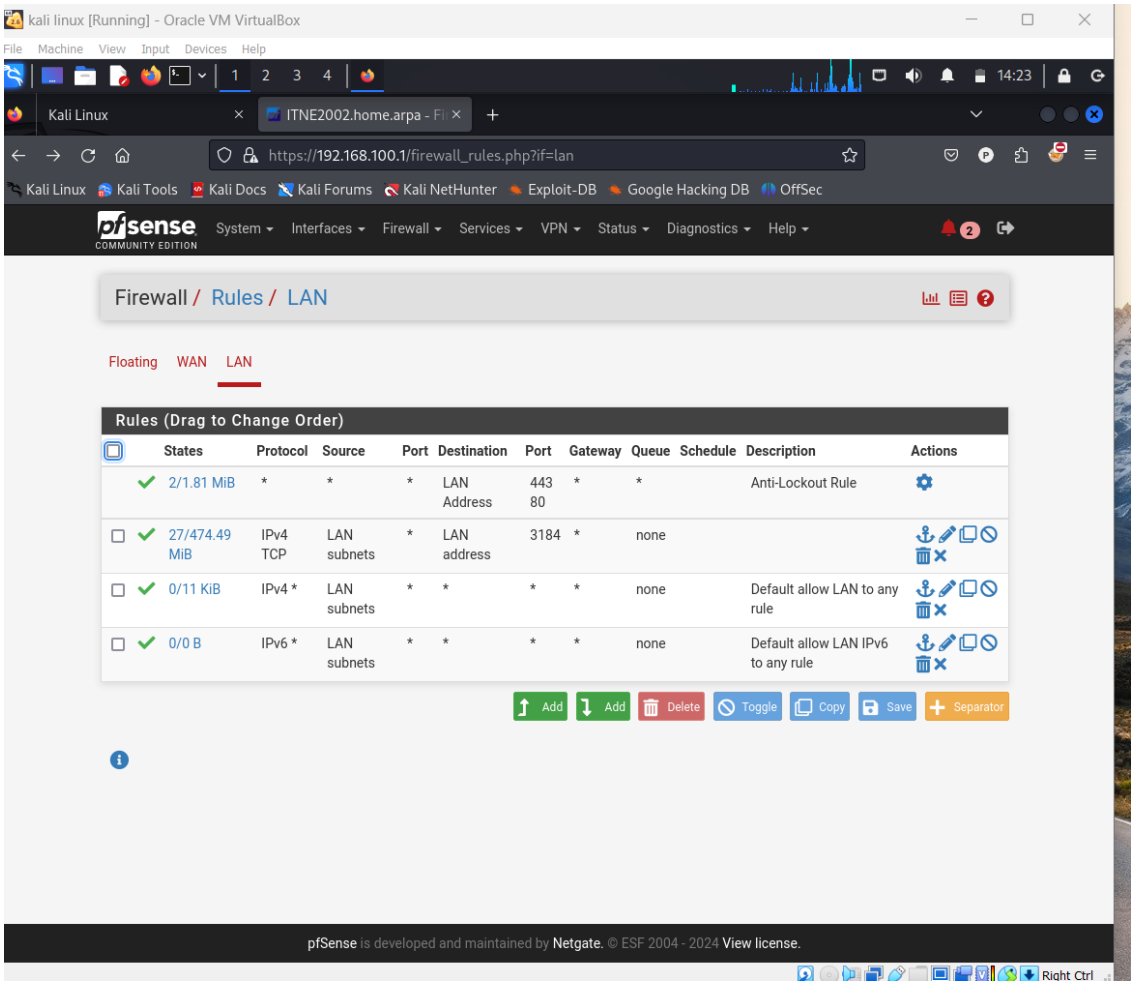


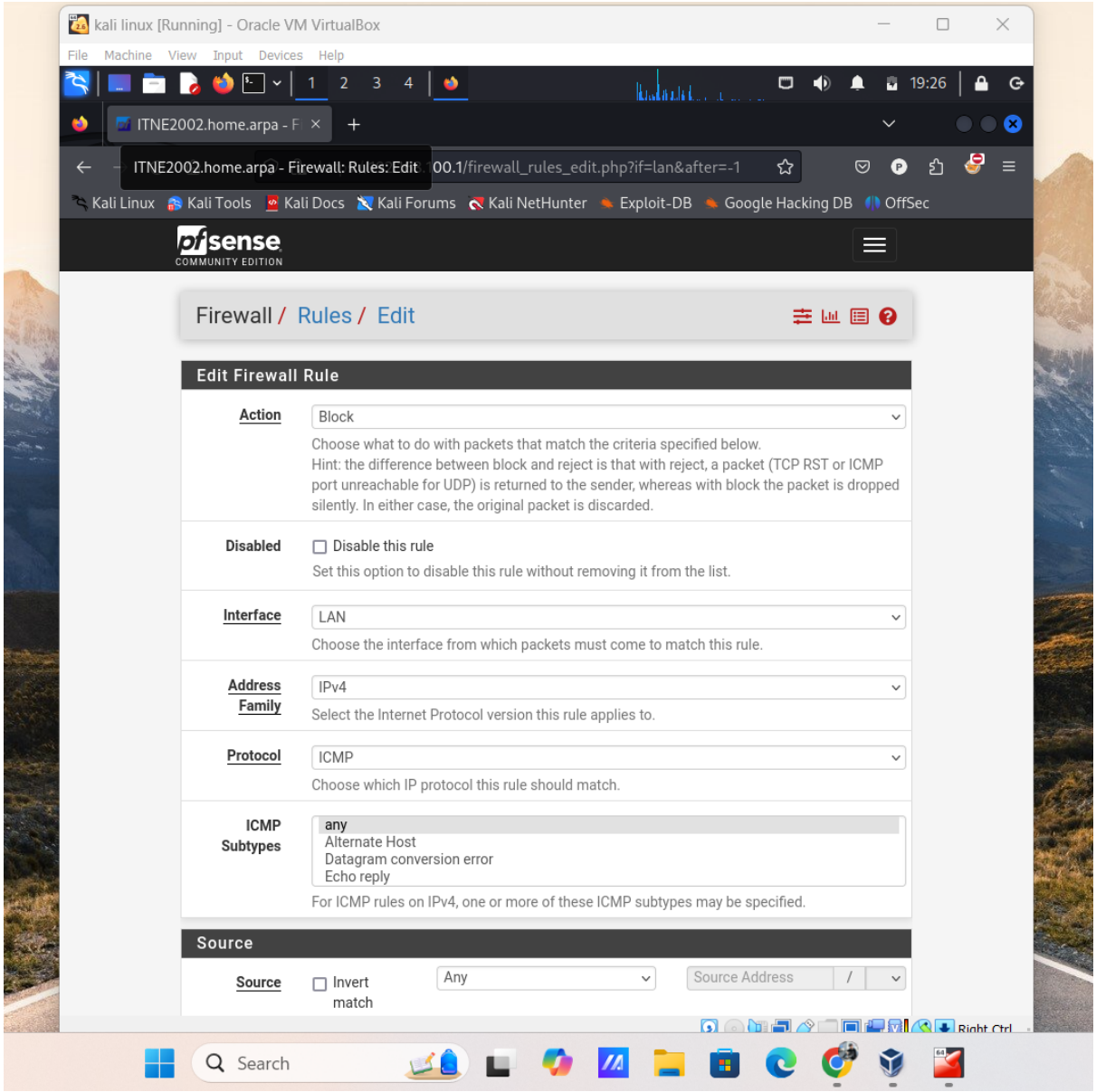

kali-linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
19:54
ab56620@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/ab56620/.zsh_history
(ab56620㉿kali)-[~]
$ ping 192.168.100.101
PING 192.168.100.101 (192.168.100.101) 56(84) bytes of data.
64 bytes 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

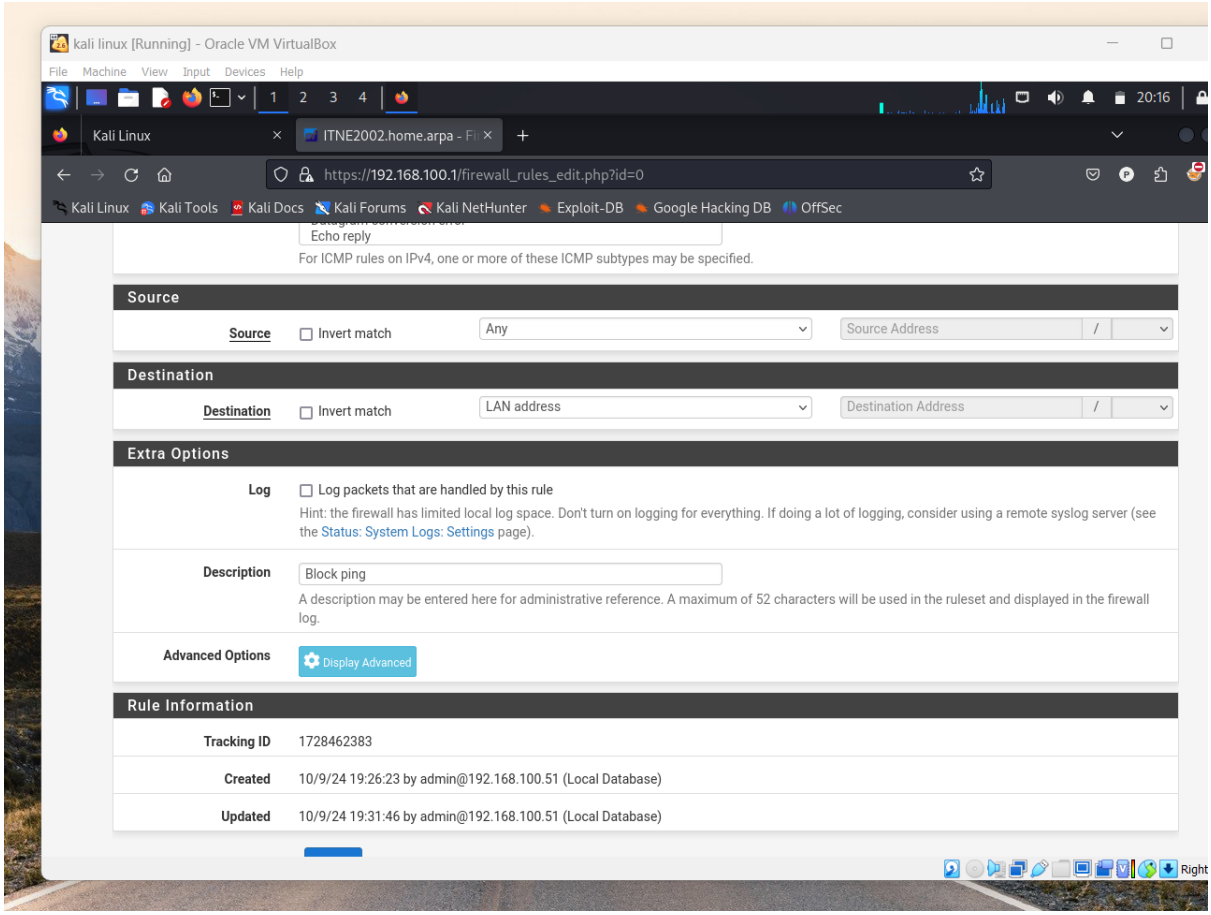

kali-linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
19:54
ab56620@kali: ~
File Actions Edit View Help
$ sudo nmap -sS -sV -O -A 192.168.100.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-09 19:53 AEDT
Nmap scan report for 192.168.100.101
Host is up (0.00081s 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)-[~]
$ ~

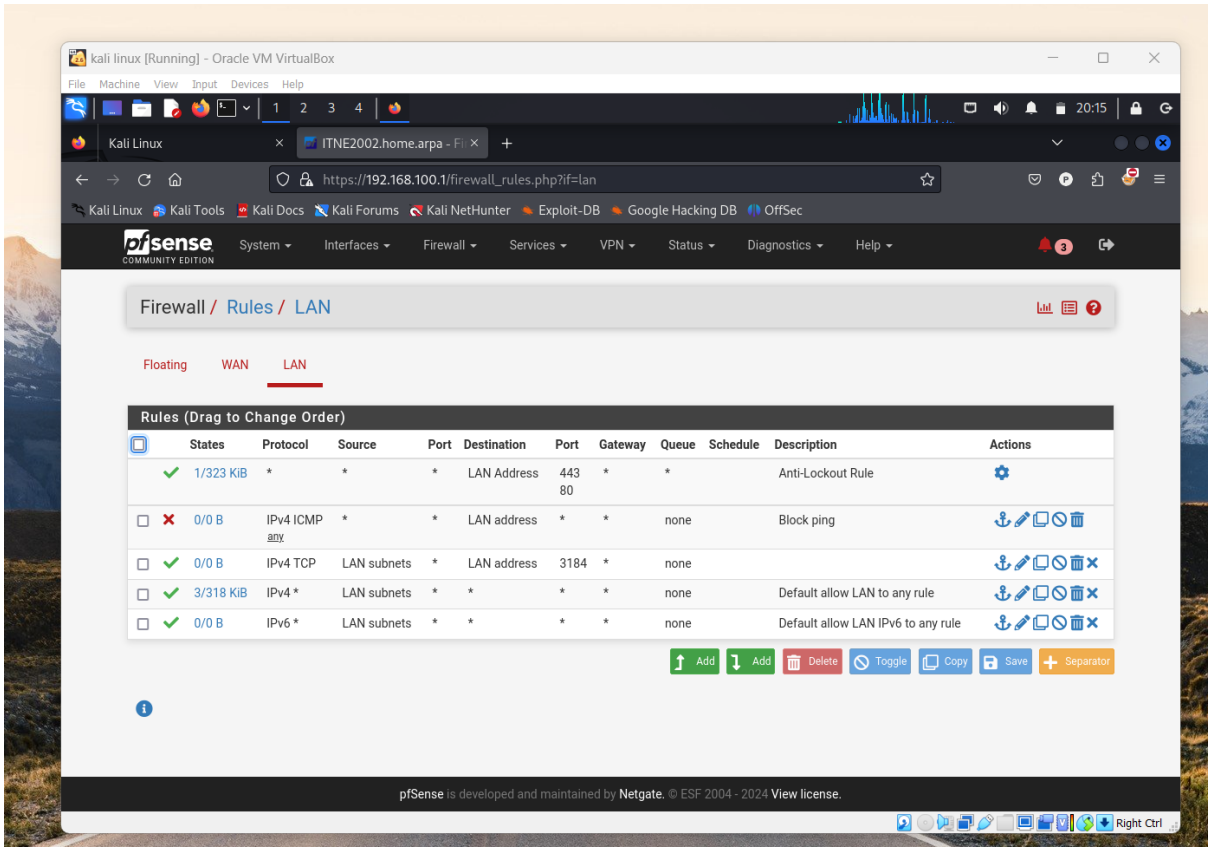
e. Configure firewall in pfSense

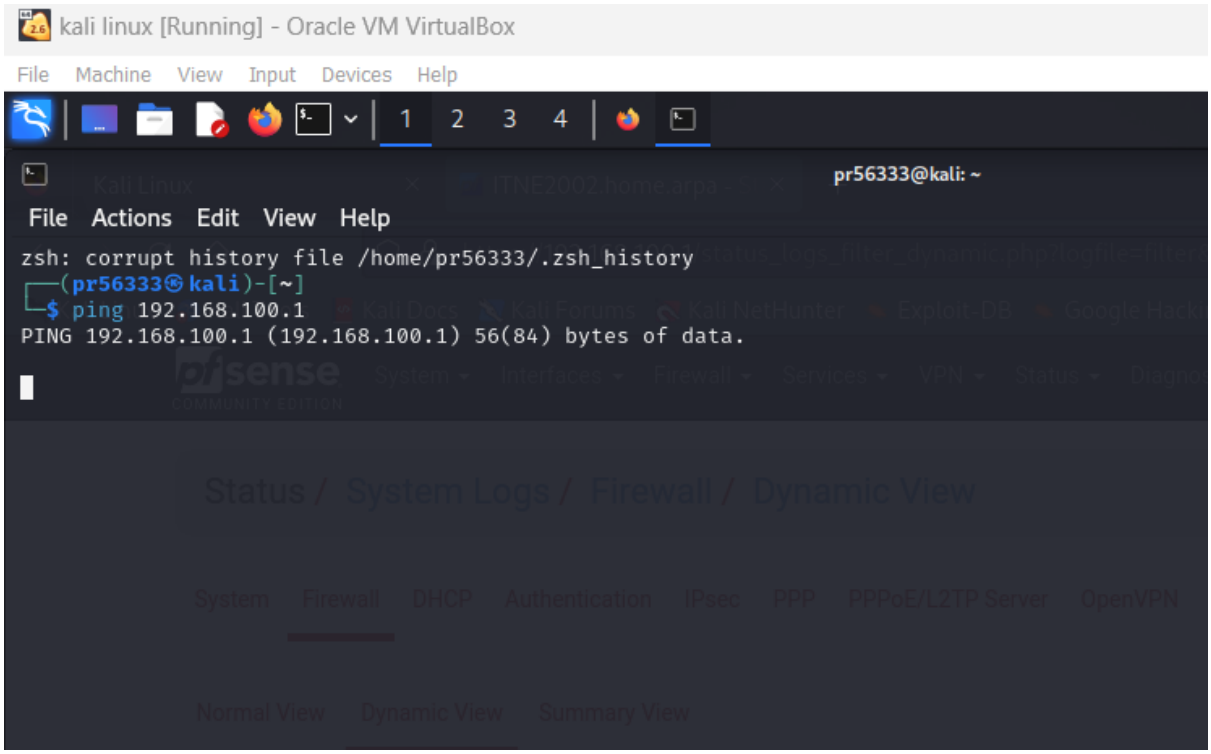


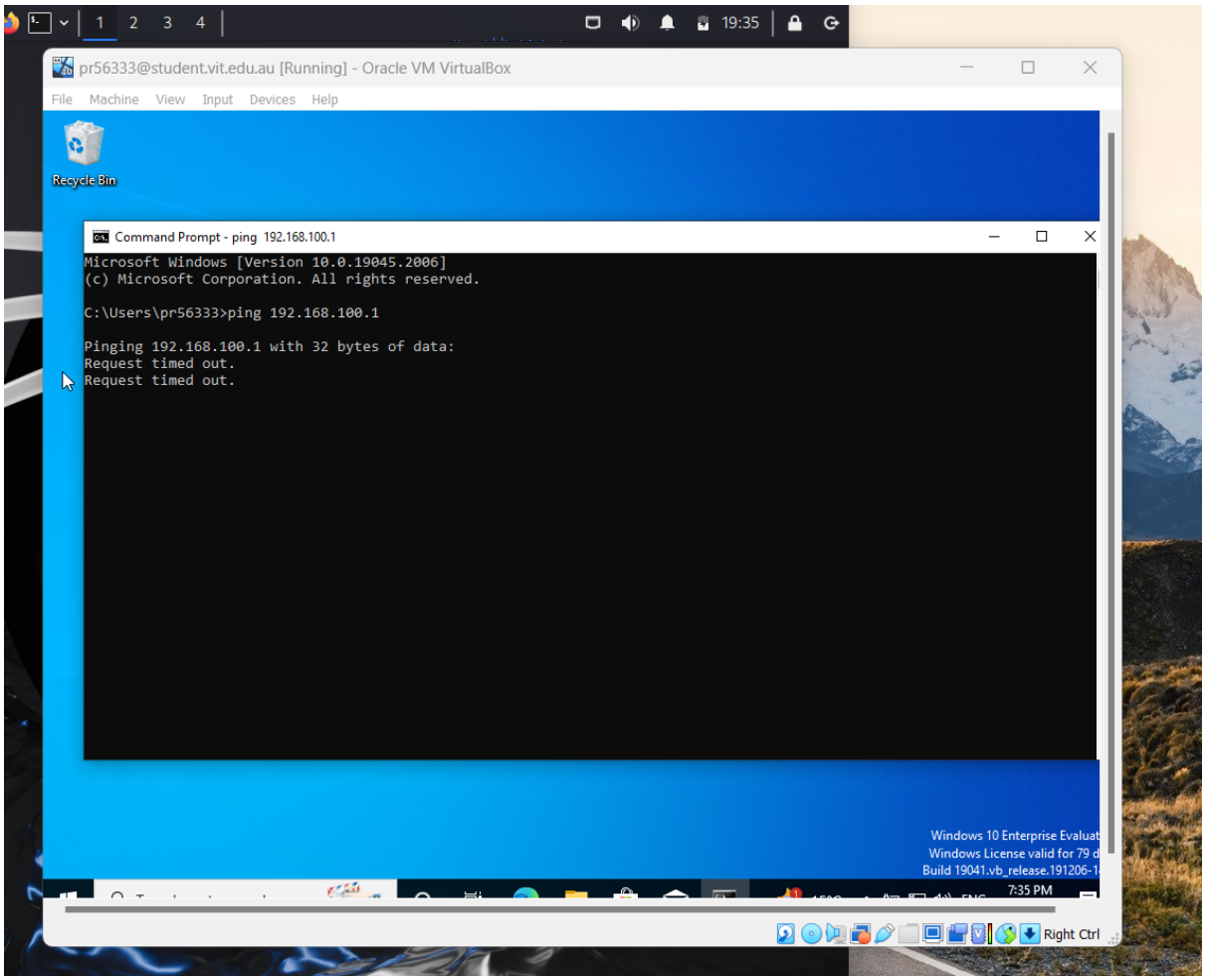

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
14:23
Kali Linux
ITNE2002.home.arpa - Fi
https://192.168.100.1/firewall_rules.php?if=lan
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces 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
File Machine View Input Devices Help
Kali Linux
ITNE2002.home.arpa - Fi
https://192.168.100.1/firewall_rules_edit.php?id=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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