Jaelin Lazenberry

Phase 1 Final

Cybersecurity Track

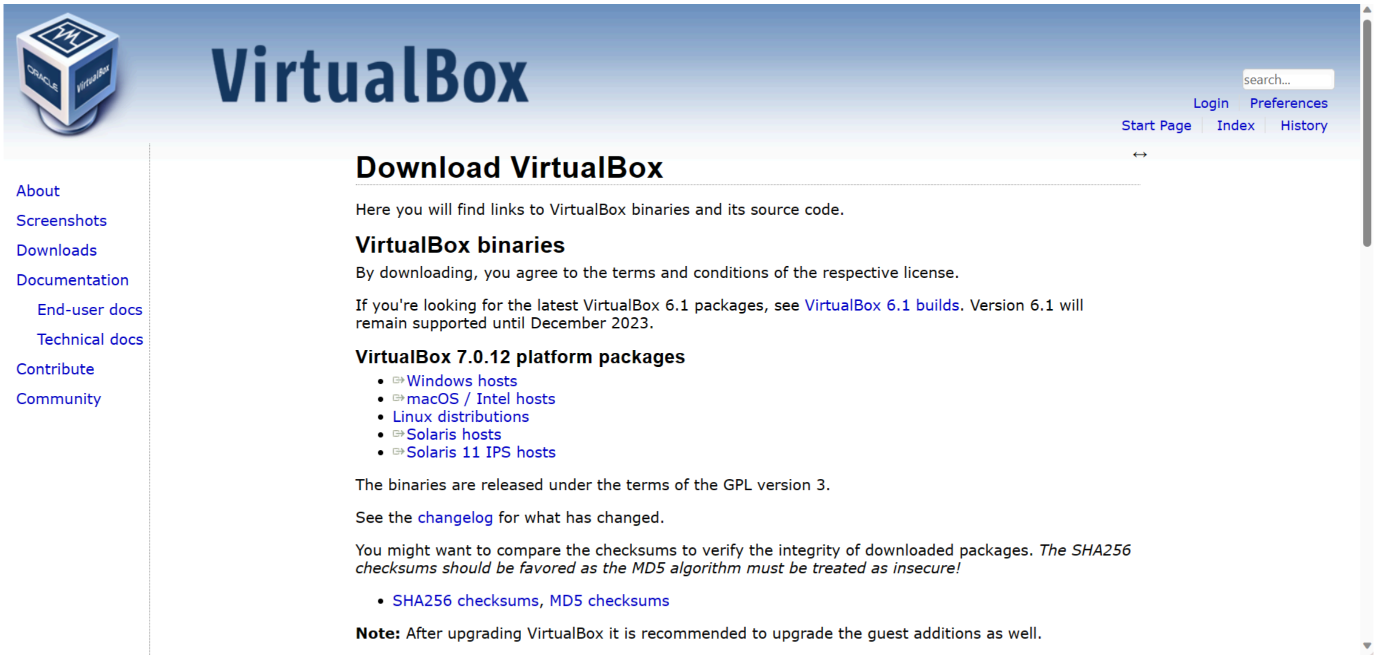
Introduction:

We want to feel safe, as it influences various aspects of an individual's physical, emotional, and psychological well-being. The feeling of security is essential to our lives and thankfully, we have cybersecurity professionals' who foster a sense of safety, on a daily basis. Ensuring a smooth operation, cyber professionals work to prevent unauthorized attacks, maintain privacy, security and the stability of our society. They are continuously adapting and developing innovative solutions to guarantee the privacy of people, organizations and businesses. The Phase 1 ethical hacking project provided us with an experience that gave us something to look forward to. Completing the hacking lab gave me hands-on experience working with the tools and softwares that most professionals use. I found the lab to be very rewarding, as it gave me insight on what a cybersecurity professional day entells.

The ethical hacking lab was a replication of a real life cybersecurity scenario but in a risk-free environment. I had the pleasure of using authentic cybersecurity tools and software commonly used in the industry. Virtualbox, Kali Linux, Pfsense, Snort, and Wazuh were the softwares I had decided to work with. The purpose of this lab was to launch an attack with my Kali machine against a vulnerable machine. In the event of the attack, my firewall and IDS/IPS Pfsense + Snort) should alert my SIEM tool (Wazuh) that an attack is taking place. This will indicate a successful project. The IDS/IPS alerting my SIEM tool means that my software was configured correctly .

Lab Setup :

To jumpstart my lab, I started by downloading Virtualbox and configuring its software. The primary use of Virtualbox is to support and operate multiple operating systems . Virtual box allows you to work, develop and experiment on multiple operating systems on a single device. I stored my supporting software here : (3 Kali Linux Virtual Machines, Pfsense+Snort, Wazuh).



Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

If you're looking for the latest VirtualBox 6.1 packages, see VirtualBox 6.1 builds. Version 6.1 will remain supported until December 2023.

VirtualBox 7.0.12 platform packages

- Windows hosts
- macOS / Intel hosts
- Linux distributions
- Solaris hosts
- Solaris 11 IPS hosts

The binaries are released under the terms of the GPL version 3.

See the changelog for what has changed.

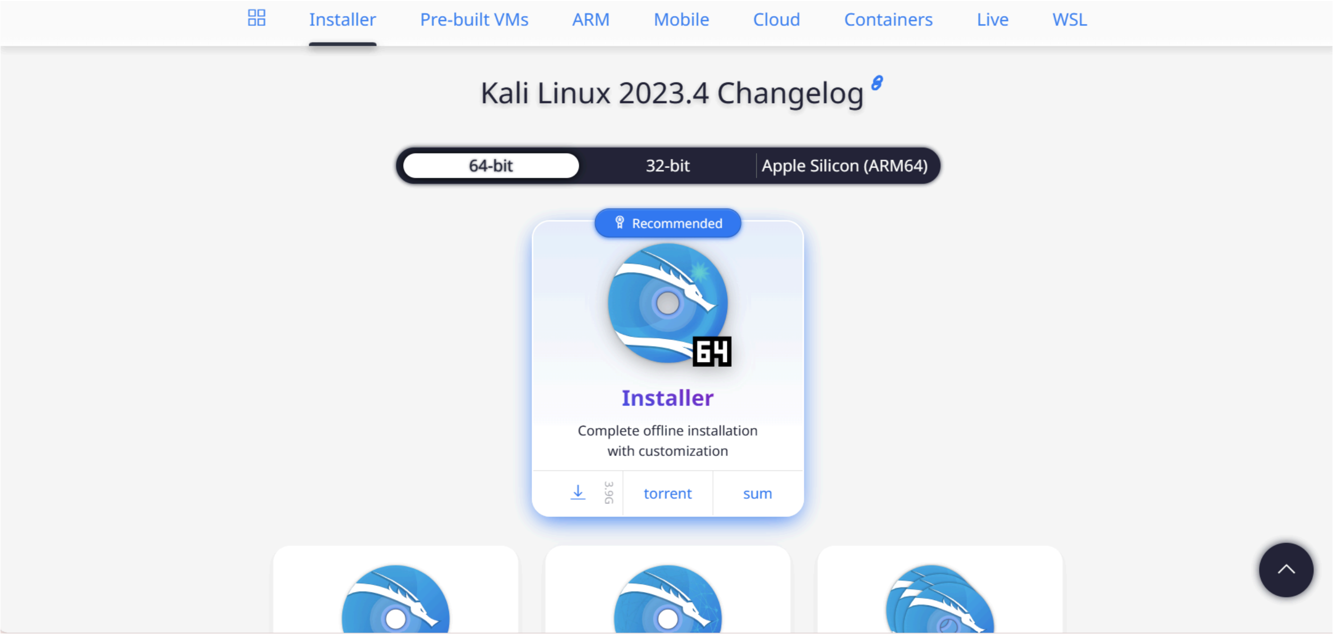
You might want to compare the checksums to verify the integrity of downloaded packages. *The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!*

- SHA256 checksums, MD5 checksums

Note: After upgrading VirtualBox it is recommended to upgrade the guest additions as well.

Next, I created a network of machines using virtualbox and configured them all to have ssh access. First, I needed to download my 64-bit Kali Linux Operating System that included the top 10 security tools. Kali is an open-source Debian-based distribution and contains industry specific modifications as well as several hundred tools. These tools are targeted towards various

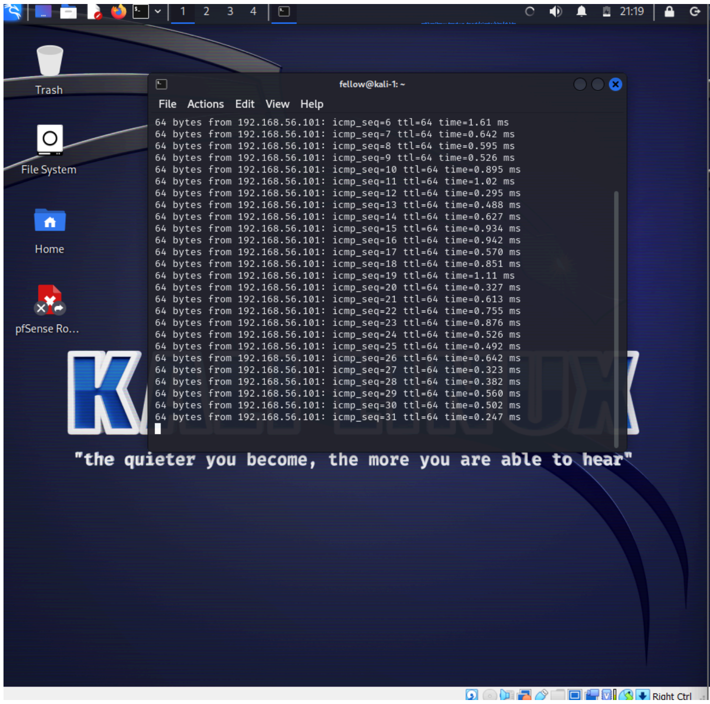
Information Security tasks, such as Penetration Testing, Security Research, Computer Forensics, Reverse Engineering, Vulnerability Management and Red Team Testing. Kali was downloaded using 2 gigabytes of RAM and 2 CPU. After completing my Kali Linux download , I went into the network settings to configure adapter 1 and 2. I configured adapter 1 to a NAT network (allows guests to connect to the Internet through host connection) . Adapter 2 will be assigned as a host-only network. The host machine was cloned 2 times. Both cloned Kali machines' names were changed to Kali_1 and Kali_2. Network interfaces were configured to set static ip addresses as 192.168.56.100 and 192.168.56.101 with a subnet mask of 255.255.255.0. SSH was enabled in both Kali terminals. I tested both Kali machines using their IP addresses and the ping command. All machines were set up successfully.



Kali Linux 2023.4 Changelog

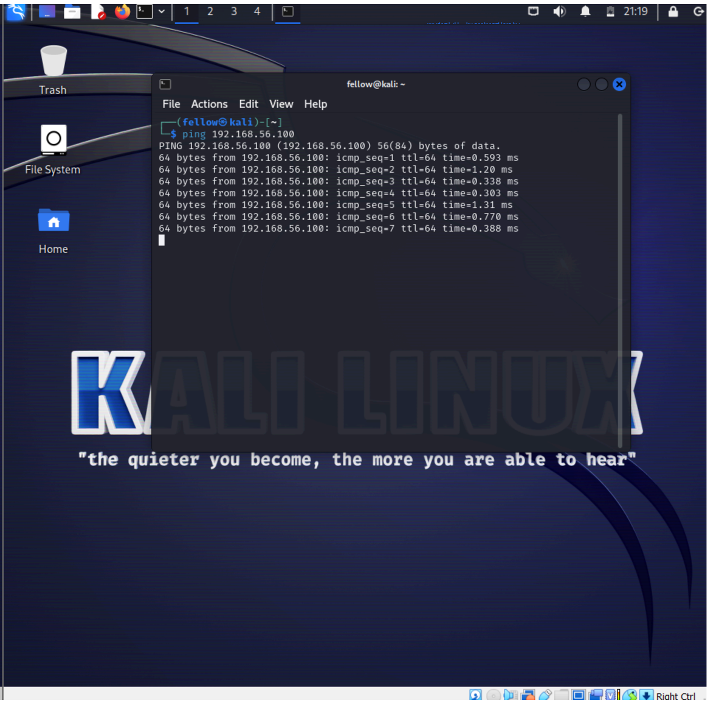
Installer

Complete offline installation with customization



1 2 3 4
21:19
Trash
File System
Home
pfSense Ro...
fellow@kali-1: ~
File Actions Edit View Help
"the quieter you become, the more you are able to hear"
Right Ctrl

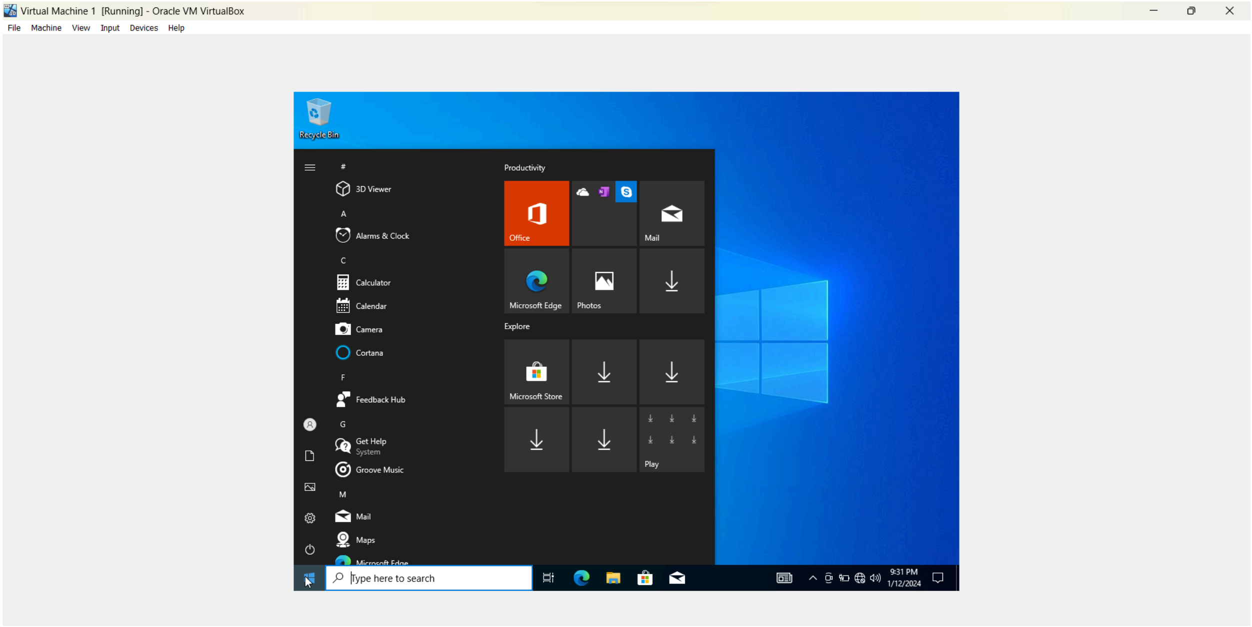
```
64 bytes from 192.168.56.101: icmp_seq=6 ttl=64 time=1.61 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=64 time=0.642 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=64 time=0.595 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=64 time=0.526 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=64 time=0.895 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=64 time=1.02 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=64 time=0.295 ms
64 bytes from 192.168.56.101: icmp_seq=13 ttl=64 time=0.488 ms
64 bytes from 192.168.56.101: icmp_seq=14 ttl=64 time=0.627 ms
64 bytes from 192.168.56.101: icmp_seq=15 ttl=64 time=0.934 ms
64 bytes from 192.168.56.101: icmp_seq=16 ttl=64 time=0.942 ms
64 bytes from 192.168.56.101: icmp_seq=17 ttl=64 time=0.570 ms
64 bytes from 192.168.56.101: icmp_seq=18 ttl=64 time=0.851 ms
64 bytes from 192.168.56.101: icmp_seq=19 ttl=64 time=1.11 ms
64 bytes from 192.168.56.101: icmp_seq=20 ttl=64 time=0.327 ms
64 bytes from 192.168.56.101: icmp_seq=21 ttl=64 time=0.613 ms
64 bytes from 192.168.56.101: icmp_seq=22 ttl=64 time=0.755 ms
64 bytes from 192.168.56.101: icmp_seq=23 ttl=64 time=0.876 ms
64 bytes from 192.168.56.101: icmp_seq=24 ttl=64 time=0.526 ms
64 bytes from 192.168.56.101: icmp_seq=25 ttl=64 time=0.492 ms
64 bytes from 192.168.56.101: icmp_seq=26 ttl=64 time=0.642 ms
64 bytes from 192.168.56.101: icmp_seq=27 ttl=64 time=0.323 ms
64 bytes from 192.168.56.101: icmp_seq=28 ttl=64 time=0.382 ms
64 bytes from 192.168.56.101: icmp_seq=29 ttl=64 time=0.560 ms
64 bytes from 192.168.56.101: icmp_seq=30 ttl=64 time=0.502 ms
64 bytes from 192.168.56.101: icmp_seq=31 ttl=64 time=0.247 ms
```



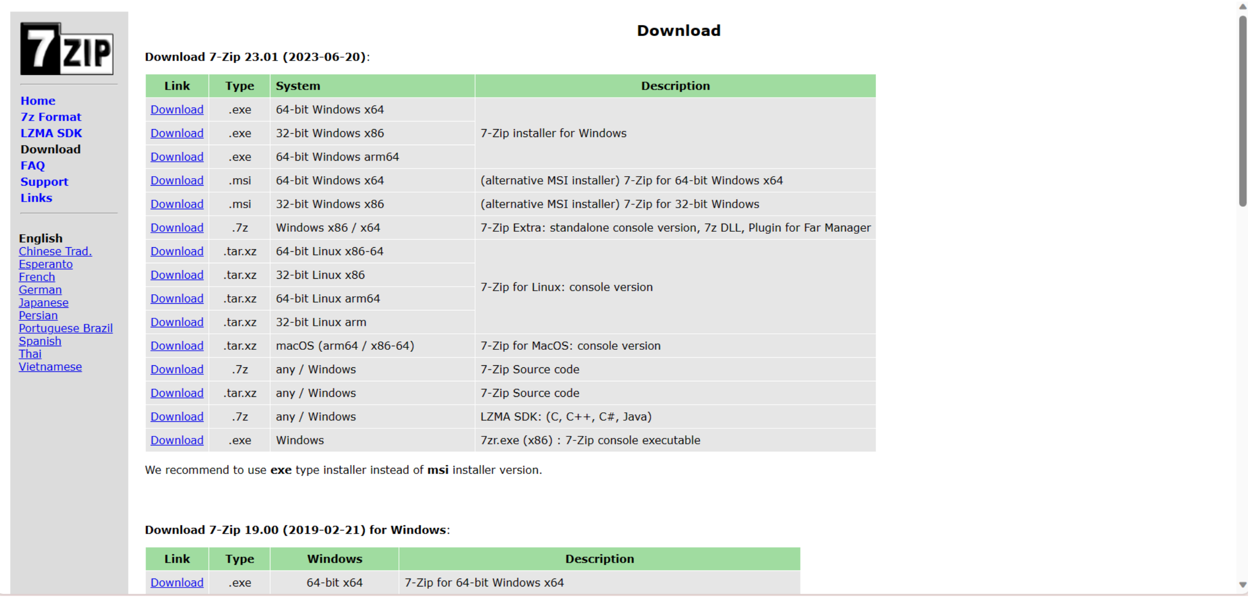
1 2 3 4
21:19
Trash
File System
Home
fellow@kali: ~
File Actions Edit View Help
"the quieter you become, the more you are able to hear"
Right Ctrl

```
┌──(fellow㉿kali)-[~]
└─$ ping 192.168.56.100
PING 192.168.56.100 (192.168.56.100) 56(84) bytes of data.
64 bytes from 192.168.56.100: icmp_seq=1 ttl=64 time=0.593 ms
64 bytes from 192.168.56.100: icmp_seq=2 ttl=64 time=1.20 ms
64 bytes from 192.168.56.100: icmp_seq=3 ttl=64 time=0.338 ms
64 bytes from 192.168.56.100: icmp_seq=4 ttl=64 time=0.303 ms
64 bytes from 192.168.56.100: icmp_seq=5 ttl=64 time=1.31 ms
64 bytes from 192.168.56.100: icmp_seq=6 ttl=64 time=0.770 ms
64 bytes from 192.168.56.100: icmp_seq=7 ttl=64 time=0.388 ms
```

I wanted to make my virtual lab unique by adding different types of software so I decided to install a Windows 10 Pro Virtual machine. I downloaded a media creation tool which generated a Windows ISO file. Once downloaded, you want to create the installation media and select ISO file. From there, I opened the software into my Virtual box and used 2 gigs and 1 CPU . Windows 10 virtual machine was successfully installed.



Downloading Pfsense was the next step in setting up my hacking lab. Having an IDPS installed was put in place to monitor the network's traffic for abnormal activity and potential threats. The AMD 64-bit version of Pfsense was downloaded and configured to act as a firewall/router for my network. Pfsense was extracted using 7zip . Using 7zip for the Pfsense software created a new folder that contained a gunzipped version of the file. The software was uploaded and configured as a BSD file type and as the 64-bit version. 2 gigabytes of RAM and 2 CPUs of memory was used for Pfsense download. Adapter 1 was set as a NAT network, Adapter 2 and 3 were both set as internal networks. After going through the installation steps, I had to unmount the pfsense installation and reboot the software. Failing to remove the ISO file from the virtual box before rebooting would lead us back to the initial steps of the installation process. The IP address of Pfsense was 192.168.20.9 and I entered it in my web browser in Kali to access it.



Download

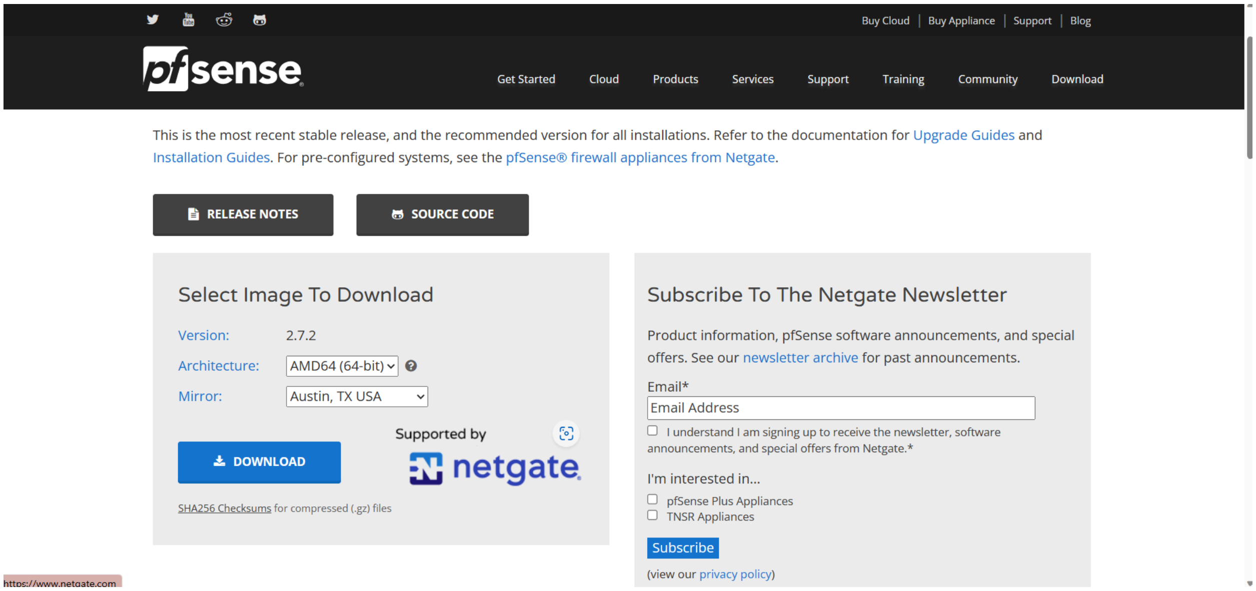
Download 7-Zip 23.01 (2023-06-20):

Link	Type	System	Description
Download	.exe	64-bit Windows x64	7-Zip installer for Windows
Download	.exe	32-bit Windows x86	
Download	.exe	64-bit Windows arm64	
Download	.msi	64-bit Windows x64	(alternative MSI installer) 7-Zip for 64-bit Windows x64
Download	.msi	32-bit Windows x86	(alternative MSI installer) 7-Zip for 32-bit Windows
Download	.7z	Windows x86 / x64	7-Zip Extra: standalone console version, 7z DLL, Plugin for Far Manager
Download	.tar.xz	64-bit Linux x86-64	7-Zip for Linux: console version
Download	.tar.xz	32-bit Linux x86	
Download	.tar.xz	64-bit Linux arm64	
Download	.tar.xz	32-bit Linux arm	
Download	.tar.xz	macOS (arm64 / x86-64)	7-Zip for MacOS: console version
Download	.7z	any / Windows	7-Zip Source code
Download	.tar.xz	any / Windows	7-Zip Source code
Download	.7z	any / Windows	LZMA SDK: (C, C++, C#, Java)
Download	.exe	Windows	7zr.exe (x86) : 7-Zip console executable

We recommend to use **exe** type installer instead of **msi** installer version.

Download 7-Zip 19.00 (2019-02-21) for Windows:

Link	Type	Windows	Description
Download	.exe	64-bit x64	7-Zip for 64-bit Windows x64



This is the most recent stable release, and the recommended version for all installations. Refer to the documentation for Upgrade Guides and Installation Guides. For pre-configured systems, see the pfSense® firewall appliances from Netgate.

Select Image To Download

Version:	2.7.2
Architecture:	AMD64 (64-bit)
Mirror:	Austin, TX USA

SHA256 Checksums for compressed (.gz) files

Subscribe To The Netgate Newsletter

Product information, pfSense software announcements, and special offers. See our newsletter archive for past announcements.

Email*

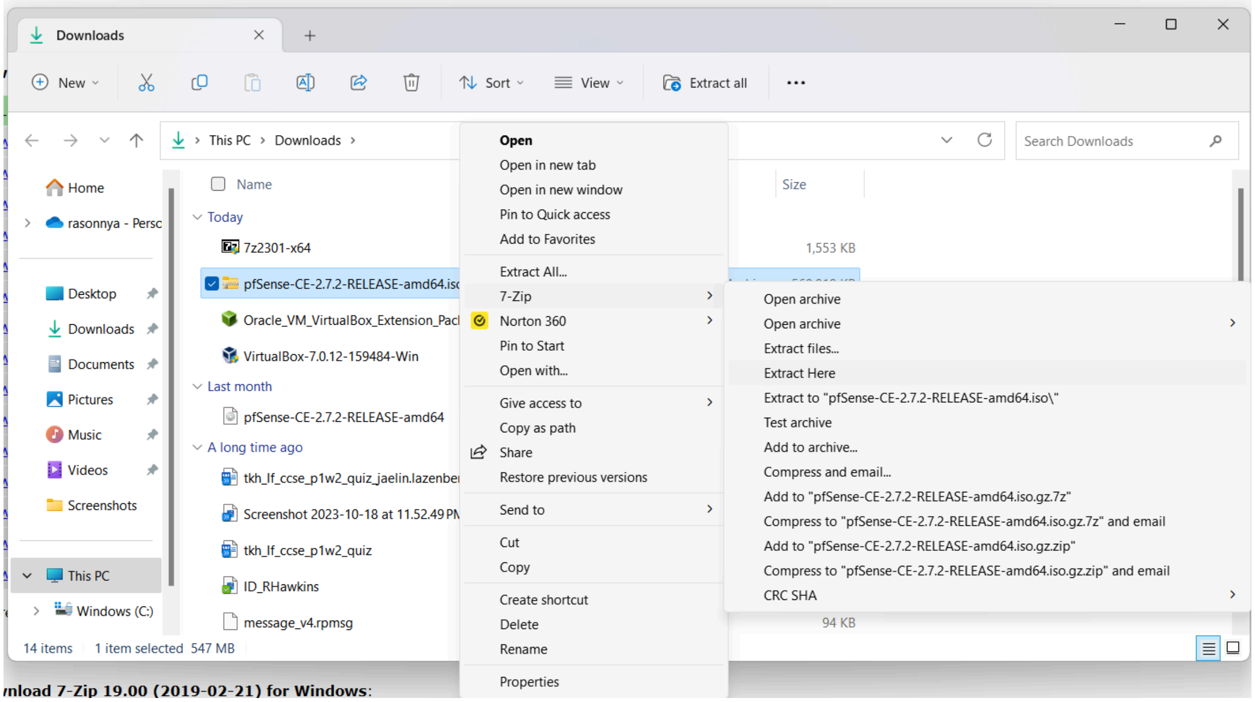
Email Address

□ I understand I am signing up to receive the newsletter, software announcements, and special offers from Netgate.*

I'm interested in...

□ pfSense Plus Appliances
□ TNSR Appliances

(view our privacy policy)



Name	Size
7z2301-x64	1,553 KB
pfSense-CE-2.7.2-RELEASE-amd64.isc	
Oracle_VM_VirtualBox_Extension_Pacl	
VirtualBox-7.0.12-159484-Win	
pfSense-CE-2.7.2-RELEASE-amd64	
tkh_lf_ccse_p1w2_quiz_jaelin.lazenbe	
Screenshot 2023-10-18 at 11.52.49 PM	
tkh_lf_ccse_p1w2_quiz	
ID_RHawkins	
message_v4.rpmsg	94 KB

Extract to "pfSense-CE-2.7.2-RELEASE-amd64.iso\"

Add to "pfSense-CE-2.7.2-RELEASE-amd64.iso.gz.7z"

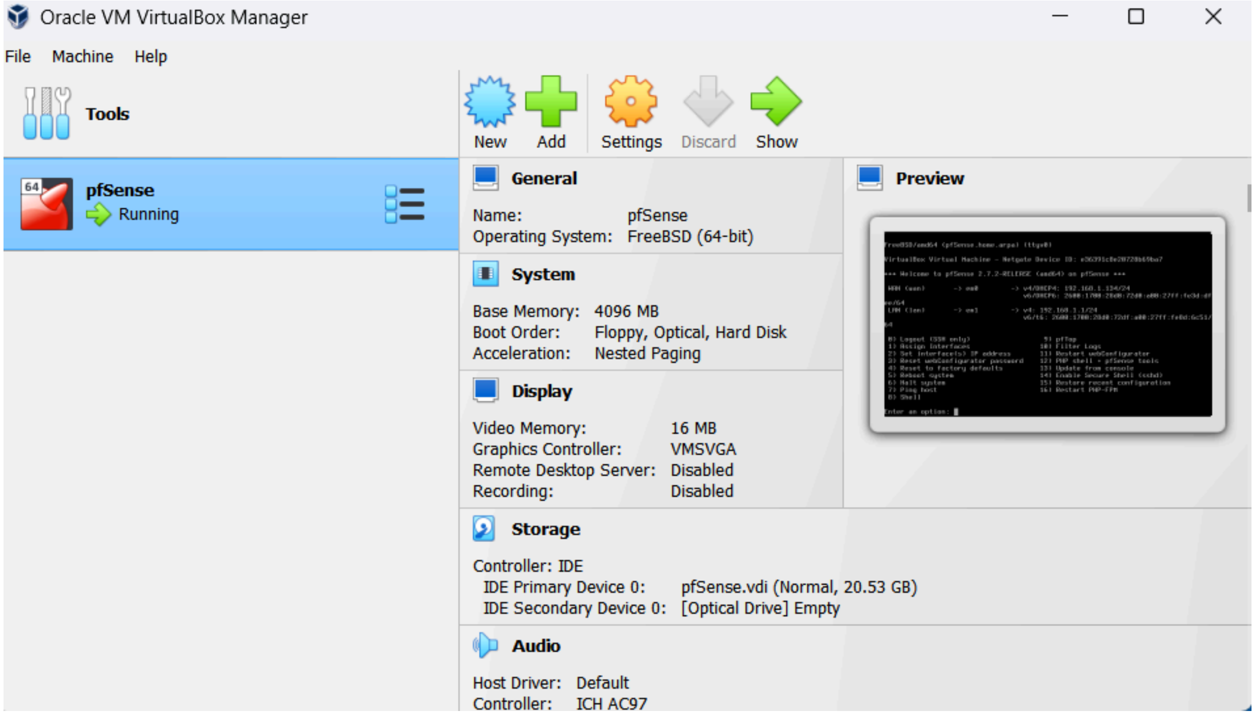
Compress to "pfSense-CE-2.7.2-RELEASE-amd64.iso.gz.7z" and email

Add to "pfSense-CE-2.7.2-RELEASE-amd64.iso.gz.zip"

Compress to "pfSense-CE-2.7.2-RELEASE-amd64.iso.gz.zip" and email

14 items 1 item selected 547 MB

nload 7-Zip 19.00 (2019-02-21) for Windows:



Name: pfSense
Operating System: FreeBSD (64-bit)

Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging

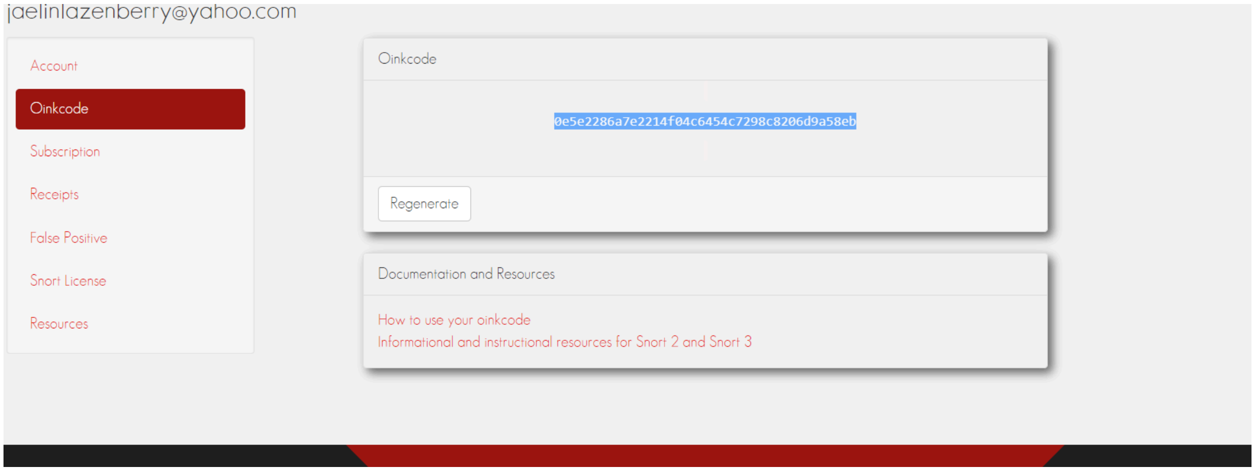
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Controller: IDE
IDE Primary Device 0: pfSense.vdi (Normal, 20.53 GB)
IDE Secondary Device 0: [Optical Drive] Empty

Host Driver: Default
Controller: ICH AC97

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: e36391c8e28728b69ba7

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.134/24
                                  v6/DHCP6: 2600:1700:28d0:72d0:a00:27ff:fe3d:df
ee/64
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24
                                  v6/t6: 2600:1700:28d0:72df:a00:27ff:fe8d:6c51/
64

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

After a successful Pfsense install, Snort was added onto my IDPS. A Security Information and Event Management (SIEM) tool such as Snort is often integrated with an Intrusion Detection and Prevention System (IDPS) to enhance overall cybersecurity capabilities. Snort can correlate events and logs from different security devices, including the IDPS. This correlation helps in identifying patterns and potential security incidents that may go unnoticed when analyzing individual logs. Accessing my Pfsense, I was able to go through the package manager and install my Snort onto my IDPS. When configuring Snort's settings I was asked to enter my oinkcode. From there I was able to edit global settings and WAN settings and rules.



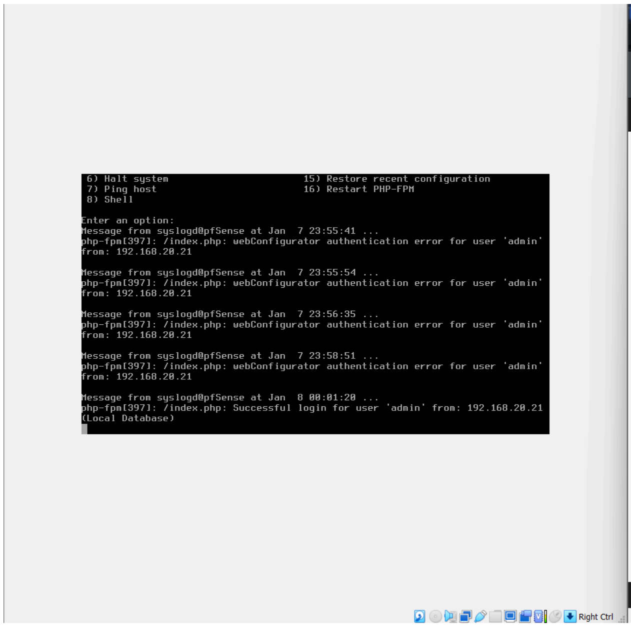
jaelinlazenberry@yahoo.com

Oinkcode

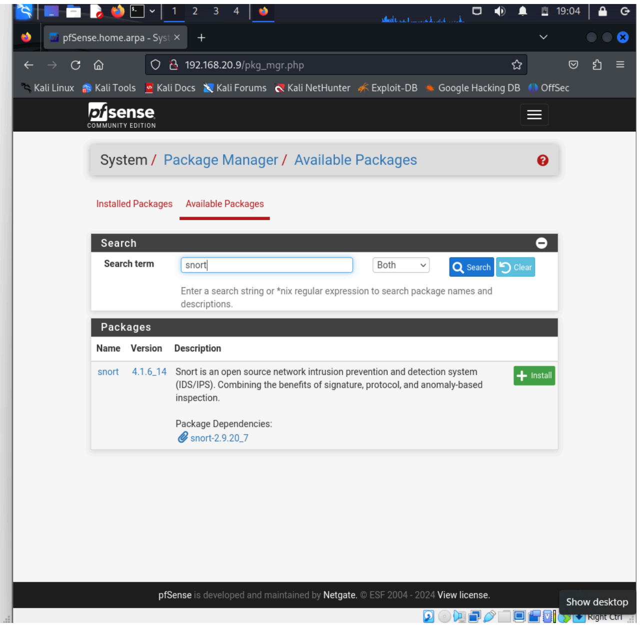
0e5e2286a7e2214f04c6454c7298c8206d9a58eb

Documentation and Resources

How to use your oinkcode
Informational and instructional resources for Snort 2 and Snort 3



```
 6) Halt system                    15) Restore recent configuration
 7) Ping host                      16) Restart PHP-FPM
 8) Shell

Enter an option:
Message from syslogd@pfSense at Jan  7 23:55:41 ...
php-fpm[397]: /index.php: webConfigurator authentication error for user 'admin'
from: 192.168.20.21

Message from syslogd@pfSense at Jan  7 23:55:54 ...
php-fpm[397]: /index.php: webConfigurator authentication error for user 'admin'
from: 192.168.20.21

Message from syslogd@pfSense at Jan  7 23:56:35 ...
php-fpm[397]: /index.php: webConfigurator authentication error for user 'admin'
from: 192.168.20.21

Message from syslogd@pfSense at Jan  7 23:58:51 ...
php-fpm[397]: /index.php: webConfigurator authentication error for user 'admin'
from: 192.168.20.21

Message from syslogd@pfSense at Jan  8 00:01:20 ...
php-fpm[397]: /index.php: Successful login for user 'admin' from: 192.168.20.21
(Local Database)
```



192.168.20.9/pkg_mgr.php

System / Package Manager / Available Packages

Search

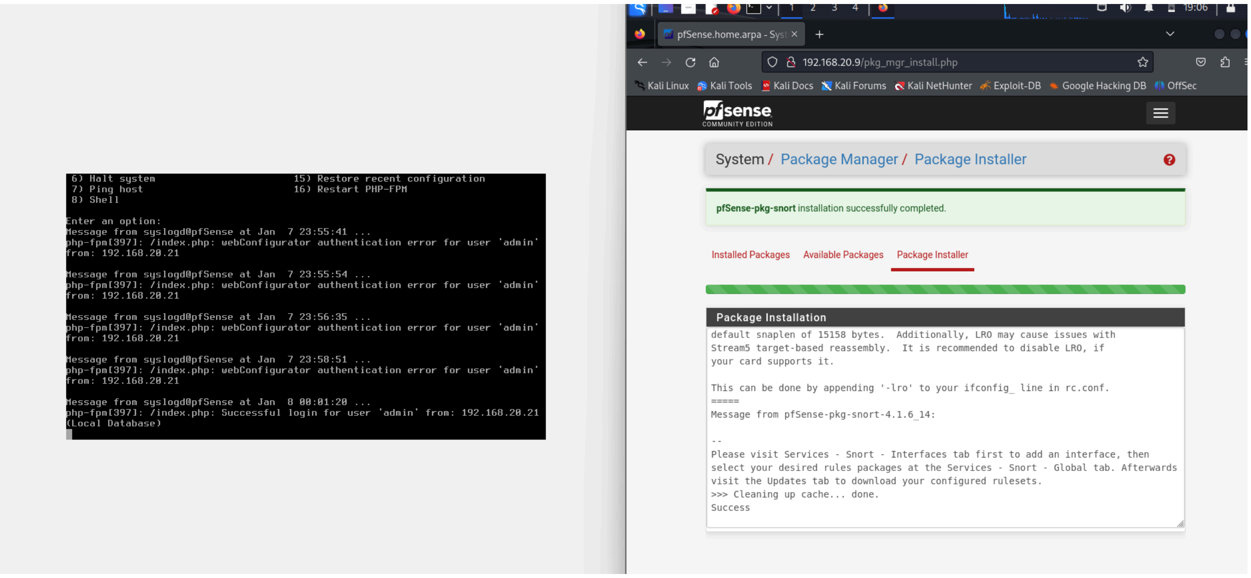
Search term: snort   Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
snort	4.1.6_14	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_7

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.



```
 6) Halt system                        15) Restore recent configuration
 7) Ping host                          16) Restart PHP-FPM
 8) Shell

Enter an option:
Message from syslogd@pfSense at Jan  7 23:55:41 ...
php-fpm[397]: /index.php: webConfigurator authentication error for user 'admin'
from: 192.168.20.21

Message from syslogd@pfSense at Jan  7 23:55:54 ...
php-fpm[397]: /index.php: webConfigurator authentication error for user 'admin'
from: 192.168.20.21

Message from syslogd@pfSense at Jan  7 23:56:35 ...
php-fpm[397]: /index.php: webConfigurator authentication error for user 'admin'
from: 192.168.20.21

Message from syslogd@pfSense at Jan  7 23:58:51 ...
php-fpm[397]: /index.php: webConfigurator authentication error for user 'admin'
from: 192.168.20.21

Message from syslogd@pfSense at Jan  8 00:01:20 ...
php-fpm[397]: /index.php: Successful login for user 'admin' from: 192.168.20.21
(Local Database)
```

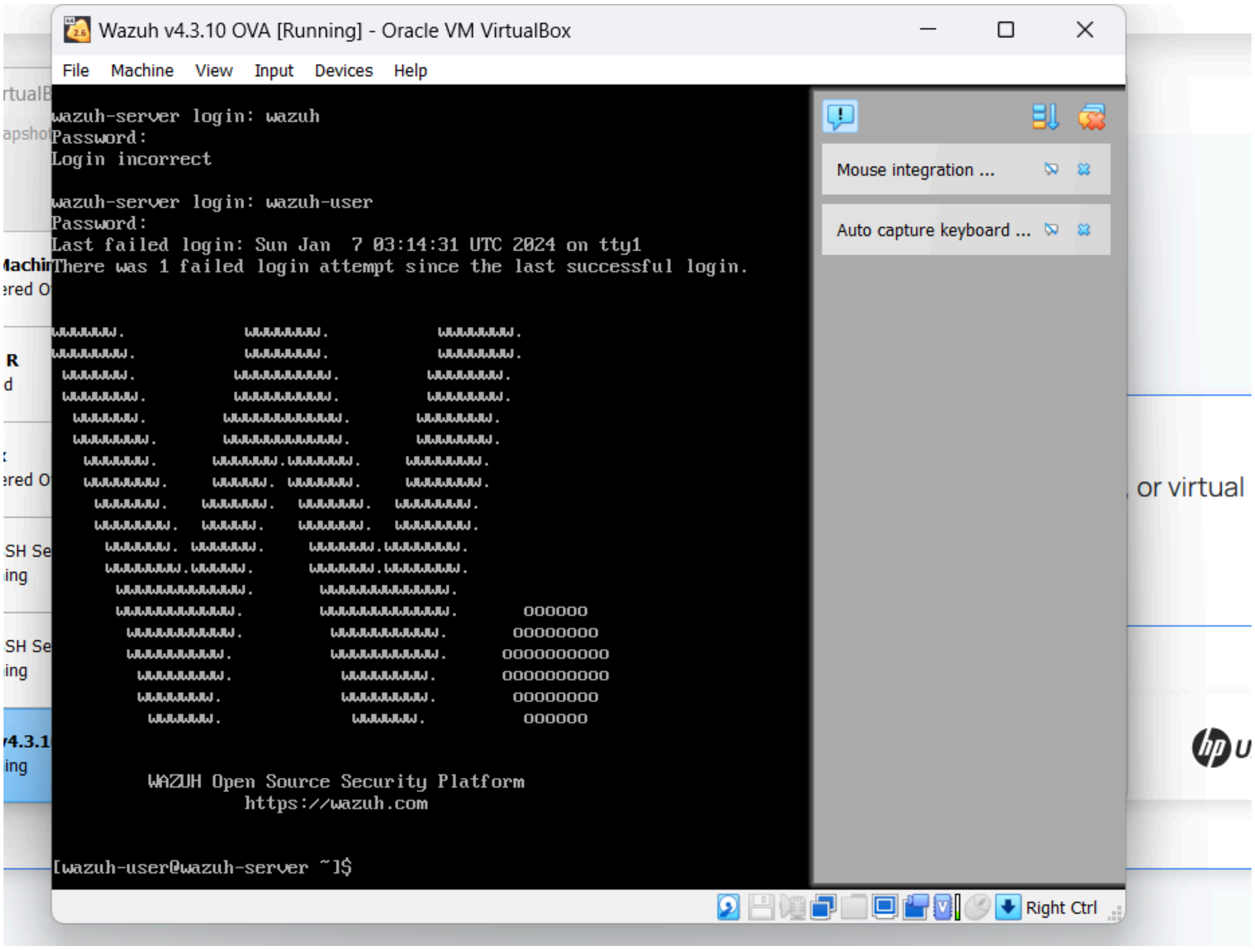
System / Package Manager / Package Installer

pfSense-pkg-snort installation successfully completed.

Package Installation

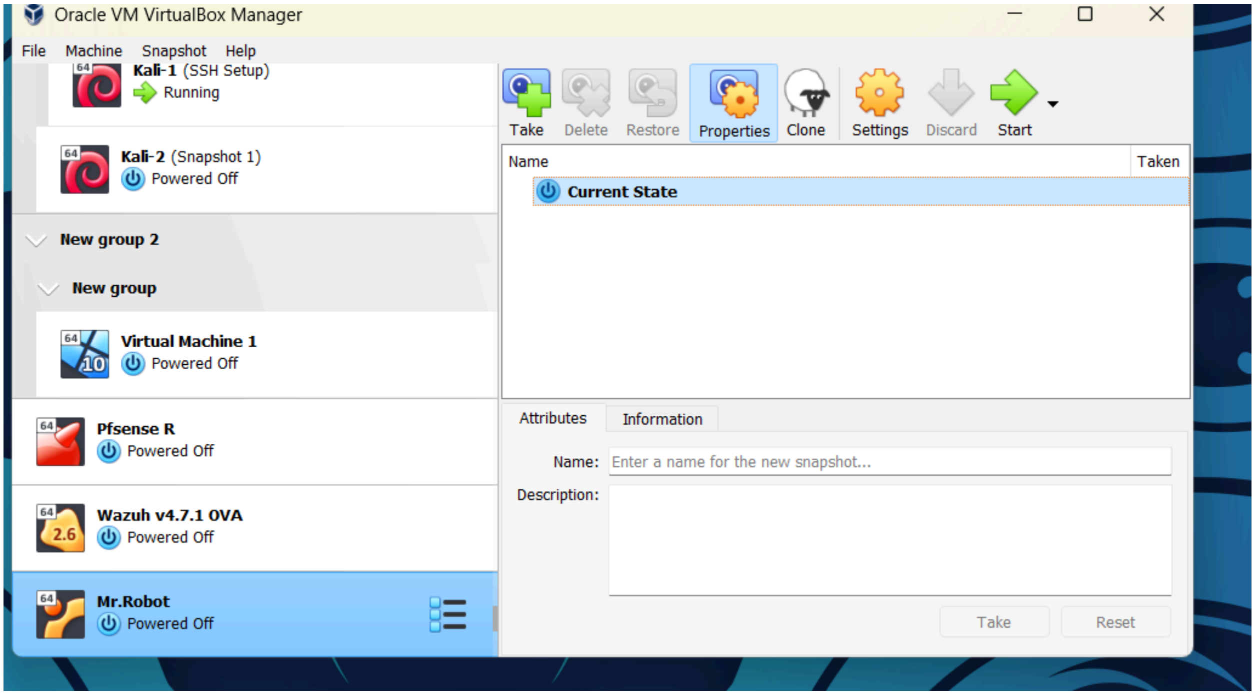
```
default snaplen of 15158 bytes.  Additionally, LRO may cause issues with
Stream5 target-based reassembly.  It is recommended to disable LRO, if
your card supports it.

This can be done by appending '-lro' to your ifconfig_ line in rc.conf.
=====
Message from pfSense-pkg-snort-4.1.6_14:

--
Please visit Services - Snort - Interfaces tab first to add an interface, then
select your desired rules packages at the Services - Snort - Global tab. Afterwards
visit the Updates tab to download your configured rulesets.
>>> Cleaning up cache... done.
Success
```

Installing Wazuh, I opened up Virtualbox and imported the download using expert mode. I used 2 Gigs for Wazuh and enabled the adapter as a NAT network. After starting my machine, I received an IP address of a192.168.1.136. I used my Kali browser to visit the address and was successful. SIEM solutions allow organizations to efficiently collect and analyze log data from all of their digital assets in one place. This gives them the ability to recreate past incidents or analyze new ones to investigate suspicious activity and implement more effective security processes.


Wazuh v4.3.10 OVA [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Mouse integration ...
Auto capture keyboard ...
Right Ctrl

```
wazuh-server login: wazuh
Password:
Login incorrect

wazuh-server login: wazuh-user
Password:
Last failed login: Sun Jan  7 03:14:31 UTC 2024 on tty1
There was 1 failed login attempt since the last successful login.


wwwwww.           wwwwwww.          wwwwwww.
wwwwwww.          wwwwwww.          wwwwwww.
 wwwwww.         wwwwwwwww.        wwwwwww.
 wwwwwww.        wwwwwwwww.        wwwwwww.
  wwwwww.       wwwwwwwwwww.      wwwwwww.
  wwwwwww.      wwwwwwwwwww.      wwwwwww.
   wwwwww.     wwwwww.wwwwww.    wwwwwww.
   wwwwwww.    wwwww. wwwwww.    wwwwwww.
    wwwwww.   wwwwww.  wwwwww.  wwwwwww.
    wwwwwww.  wwwww.   wwwwww.  wwwwwww.
     wwwwww. wwwwww.    wwwwww.wwwwwww.
     wwwwwww.wwwww.     wwwwww.wwwwwww.
      wwwwwwwwwwww.      wwwwwwwwwwww.
      wwwwwwwwwwww.      wwwwwwwwwwww.      oooooo
       wwwwwwwwww.        wwwwwwwwww.      oooooooo
       wwwwwwwwww.        wwwwwwwwww.     oooooooooo
        wwwwwwwww.         wwwwwwwww.     oooooooooo
        wwwwwwwww.         wwwwwwwww.      oooooooo
         wwwwwww.           wwwwwww.        oooooo


         WAZUH Open Source Security Platform
                  https://wazuh.com


[wazuh-user@wazuh-server ~]$
```

Lastly, I had to download my virtual machine that served as the victim machine. Vulnhub is where I downloaded my vulnerable machine called Mr.Robot. Once Mr.Robot was downloaded I uploaded the file onto my virtual box and set its network to internal. The purpose of this vulnerable machine is to practice and enhance their skills in identifying and exploiting vulnerabilities. The vulnerable machine serves as a simulated target that participants can attempt to compromise using ethical hacking techniques.



In conclusion, Ethical hacking labs play a crucial role in cybersecurity education and training. A project like this provides cybersecurity professionals with a safe and controlled environment that allows us to continue to enhance our skills. Engaging in practices like the ethical lab, helps students gain deeper knowledge of attack vectors, vulnerabilities and exploitation techniques. All of my tools were successfully installed and configured. I was not able to fully complete an attack on my vulnerable machine due to my own difficulties of not understanding how to make it come all together. I enjoyed downloading and configuring the software but somehow became lost. I didn’t get fully through my project and although it's unfortunate, I learned information that’s essential for securing systems and networks effectively. I was able to play around with my IDPS and SIEM tool and see real-time alerts. Overall the lab proved to be effective. I was able to achieve skill development, vulnerability discovery, understanding attack vectors and real world application. Since ethical hacking labs are designed for learning purposes, individuals can make mistakes and learn from them without the risk of legal consequences. These labs contribute to building a skilled and ethical cybersecurity workforce.This fosters a culture of continuous learning and improvement. Hacking labs contribute significantly to the education and training of cybersecurity professionals, preparing them for the challenges they may face in the field.