Maria Valencia

CSC 154

Lab 7

Lab 07 Security Systems

Exercise 7.1 Breach Report

In this task, I read the CrowdStrike 2023 Global Threat Report and briefly summarized its contents.

Step 1: Read and Report

I downloaded CrowdStrike 2023 Global Threat and read it while taking notes on any interesting facts I discovered.

After reading the report, it became clear to me that cyber threats will always be a cause of concern and companies should do their best to defend against these threats. Although there have been major shutdowns of ransomware, affiliates shifted to a new type of ransomware. It is safe to say that with the increase of these attacks despite the shutdowns, it will be a problem if we have technology, so we need to be able to make our networks impenetrable.

As noted in the report, 80% of the cyberattacks used identity-based techniques. So, identity protection should be a priority. Companies should focus on protecting against stolen credentials and enhance multifactor authentication. Another thing we should note is that since a lot of companies have gone remote or hybrid, there is a lot of use of the Cloud. There are adversaries that exploit this cloud infrastructure which makes it vulnerable to data leakage. There needs to be robust security measures implemented for these cloud services.

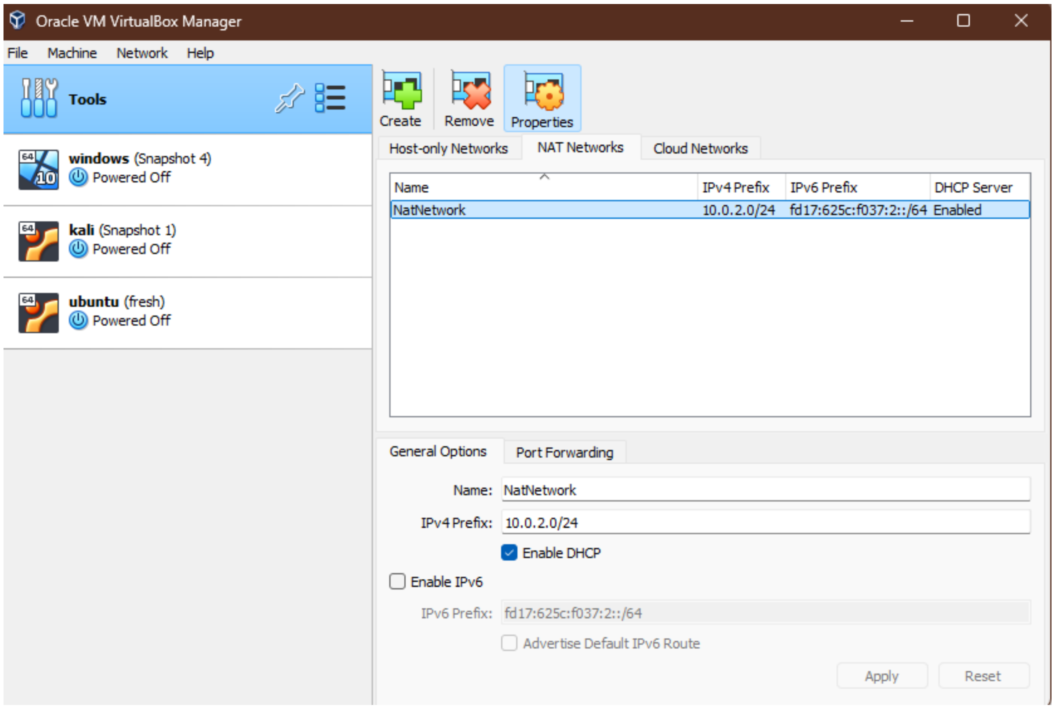
Just like technology keeps advancing and that means the cyberthreats keep advancing as well. Companies need to stay ahead of the game and learn to quickly adapt in order to protect themselves against evolving threats. If companies are able to understand the attackers and their tactics, it will be harder for the attacks to follow through. Having this knowledge as well as implementing more secure identity protection and cloud services, companies will be able much harder to break into.

Exercise 7.2 Nessus Vulnerability Scan

In this exercise, I used all three of my VMs in a NAT network and performed Nessus Vulnerability scans on the Windows and Ubuntu VMs from the Kali VM.

Step 1: Configure Network

Within VirtualBox, I selected “NAT networks” under the properties button and created a new NAT network that I will use for all my VMS. With all VMS powered off, I navigated to each VMs settings, selected NAT Network attachment and the name NatNetwork. Then I started each VM.



windows (Snapshot 4)
Powered Off

kali (Snapshot 1)
Powered Off

ubuntu (fresh)
Powered Off

Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork	10.0.2.0/24	fd17:625c:f037:2::/64	Enabled

Name: NatNetwork

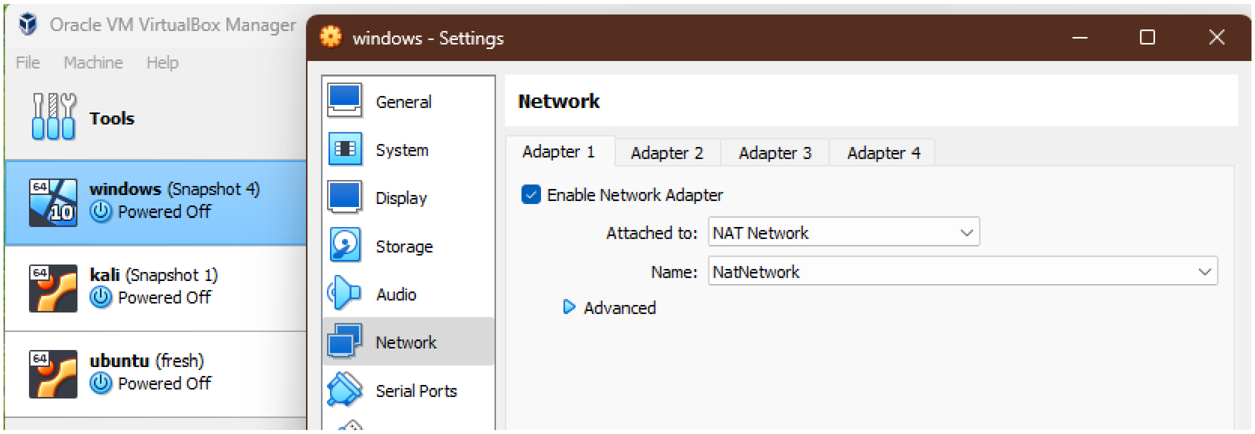
IPv4 Prefix: 10.0.2.0/24

☑ Enable DHCP

□ Enable IPv6

IPv6 Prefix: fd17:625c:f037:2::/64

□ Advertise Default IPv6 Route



windows (Snapshot 4) Powered Off

kali (Snapshot 1) Powered Off

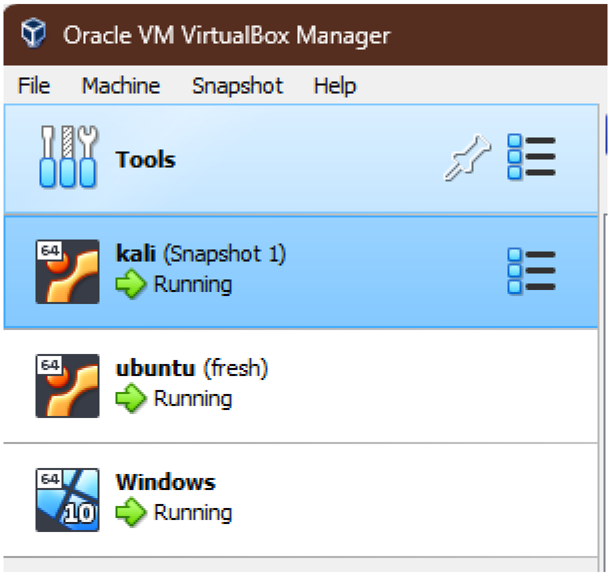
ubuntu (fresh) Powered Off

Network

☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork



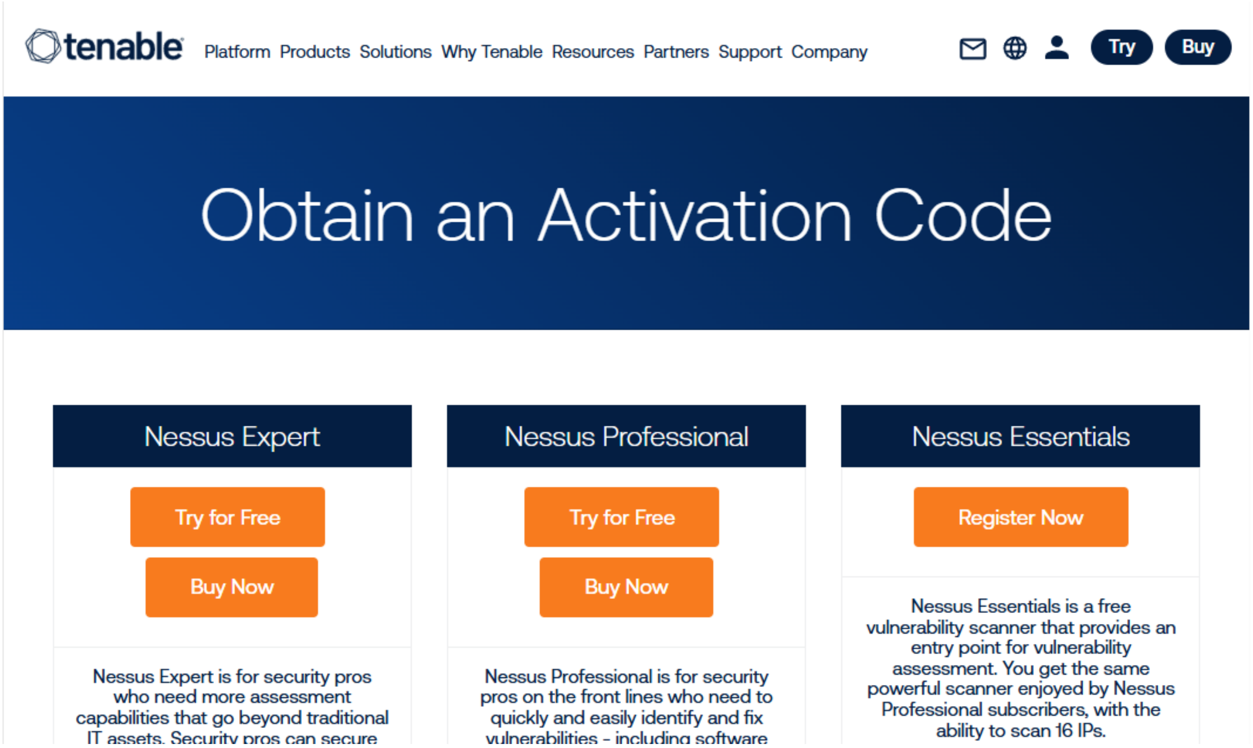
kali (Snapshot 1) Running

ubuntu (fresh) Running

Windows Running

Step 2: Obtain Activation Code

The Nessus Essentials product allows students a free activation code that can be used on up to 16 IP addresses. From your host machine, navigate to https://www.tenable.com/products/nessus/activation-code and select “Register Now” under the “Nessus Essentials” option.


tenable
Platform Products Solutions Why Tenable Resources Partners Support Company
Try
Buy
Try for Free
Buy Now
Try for Free
Buy Now
Register Now

Obtain an Activation Code

Nessus Expert

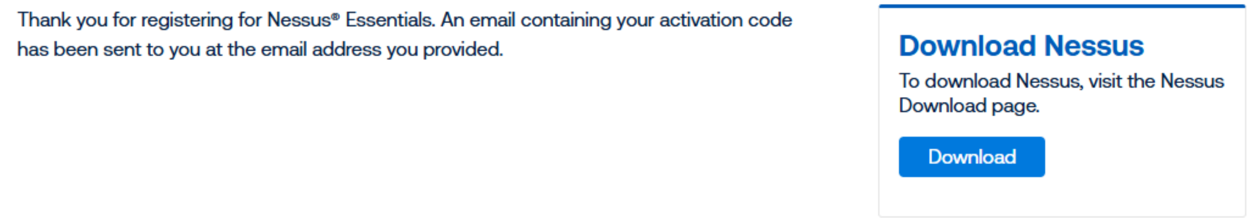
Nessus Expert is for security pros who need more assessment capabilities that go beyond traditional IT assets. Security pros can secure

Nessus Professional

Nessus Professional is for security pros on the front lines who need to quickly and easily identify and fix vulnerabilities - including software

Nessus Essentials

Nessus Essentials is a free vulnerability scanner that provides an entry point for vulnerability assessment. You get the same powerful scanner enjoyed by Nessus Professional subscribers, with the ability to scan 16 IPs.



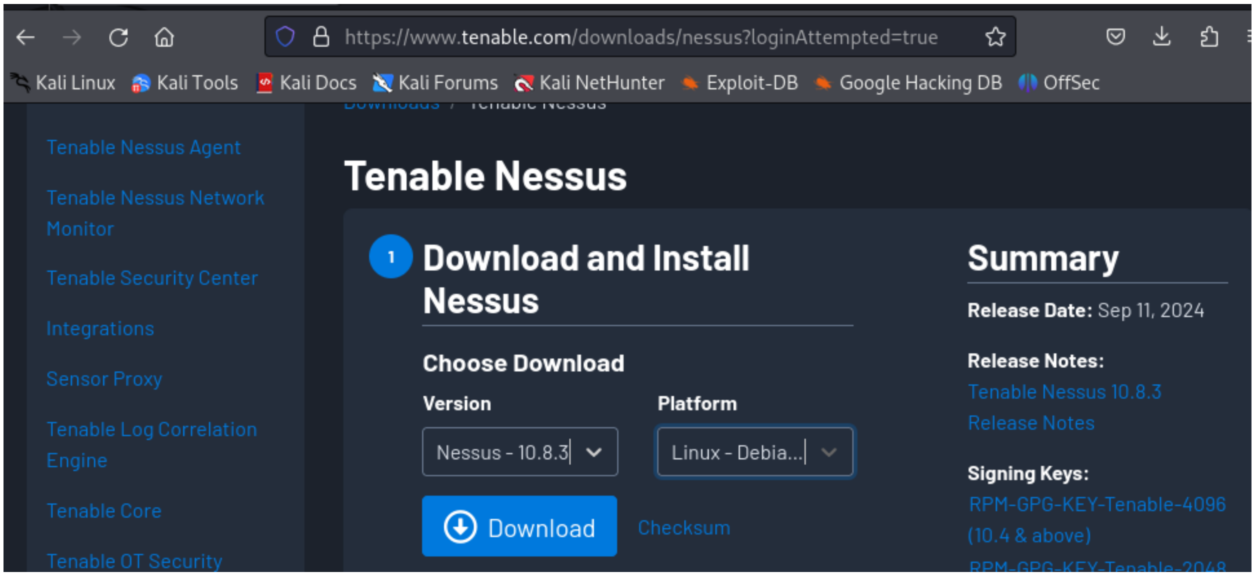
Thank you for registering for Nessus® Essentials. An email containing your activation code has been sent to you at the email address you provided.

Download Nessus

To download Nessus, visit the Nessus Download page.

Step 3: Download and Install Nessus

From my kali VM, I navigated to https://www.tenable.com/downloads/nessus?loginAttempted=true . I selected Linux Debian –amd64 and then pressed download and accepted the license agreement. With the Nessus DEB file downloaded to my downloads folder, I opened a terminal and changed directories to my downloads folder and installed the package.



Tenable Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.8.3

Platform: Linux - Debia...

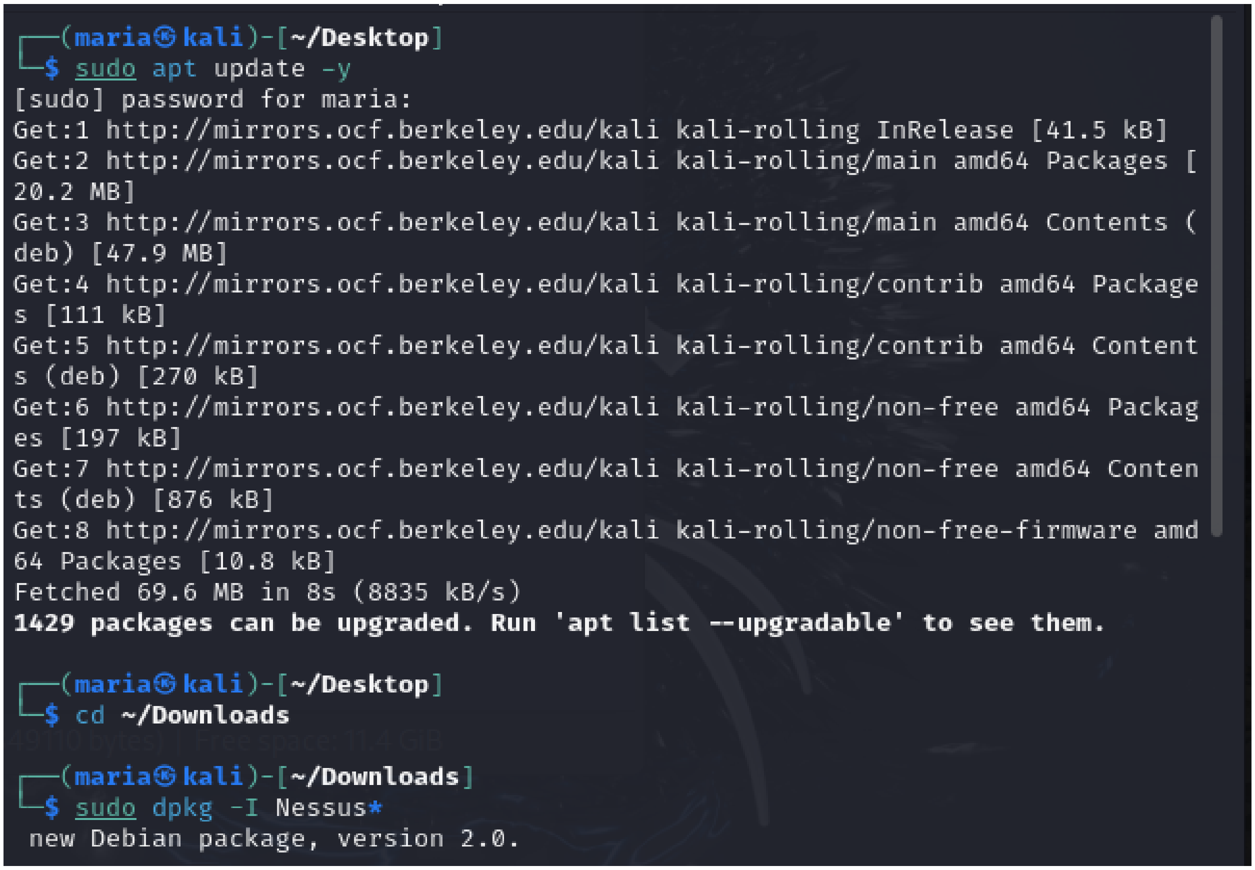
Summary

Release Date: Sep 11, 2024

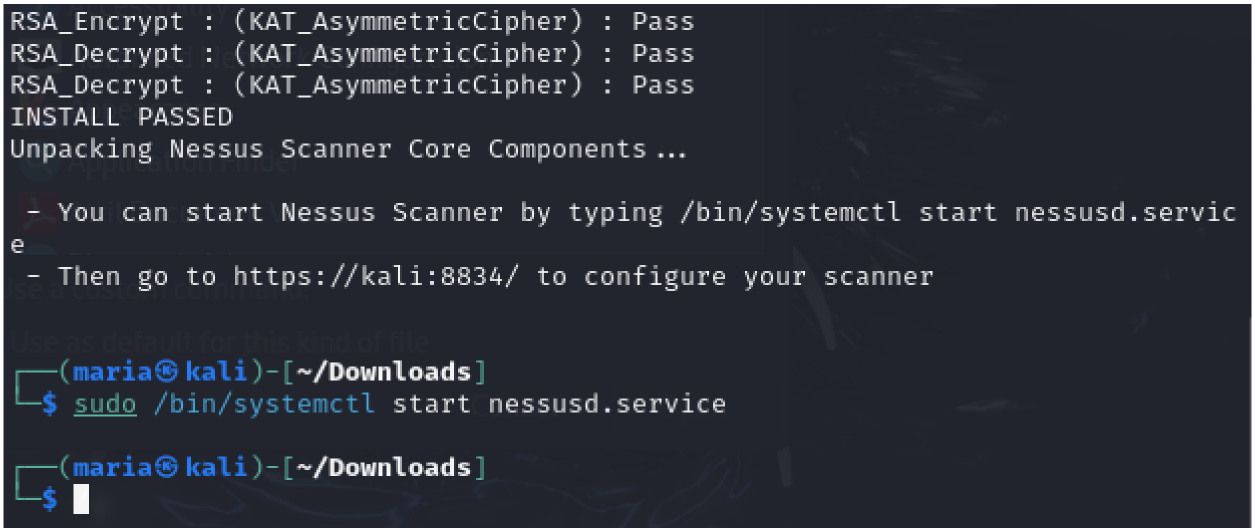
Release Notes: Tenable Nessus 10.8.3 Release Notes

Signing Keys: RPM-GPG-KEY-Tenable-4096 (10.4 & above)

RPM-GPG-KEY-Tenable-2048

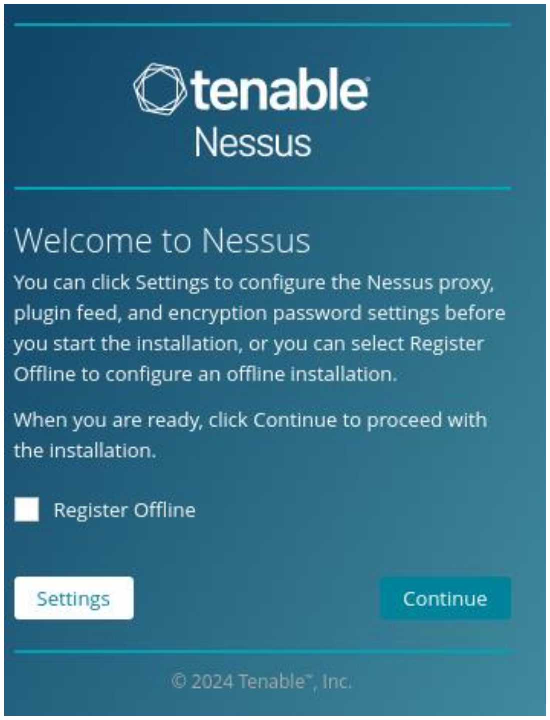


```
┌──(maria㉿kali)-[~/Desktop]
└─$ sudo apt update -y
[sudo] password for maria:
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling InRelease [41.5 kB]
Get:2 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 Packages [
20.2 MB]
Get:3 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 Contents (
deb) [47.9 MB]
Get:4 http://mirrors.ocf.berkeley.edu/kali kali-rolling/contrib amd64 Package
s [111 kB]
Get:5 http://mirrors.ocf.berkeley.edu/kali kali-rolling/contrib amd64 Content
s (deb) [270 kB]
Get:6 http://mirrors.ocf.berkeley.edu/kali kali-rolling/non-free amd64 Packag
es [197 kB]
Get:7 http://mirrors.ocf.berkeley.edu/kali kali-rolling/non-free amd64 Conten
ts (deb) [876 kB]
Get:8 http://mirrors.ocf.berkeley.edu/kali kali-rolling/non-free-firmware amd
64 Packages [10.8 kB]
Fetched 69.6 MB in 8s (8835 kB/s)
1429 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(maria㉿kali)-[~/Desktop]
└─$ cd ~/Downloads

┌──(maria㉿kali)-[~/Downloads]
└─$ sudo dpkg -I Nessus*
 new Debian package, version 2.0.
```



```
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.servic
e
 - Then go to https://kali:8834/ to configure your scanner


┌──(maria㉿kali)-[~/Downloads]
└─$ sudo /bin/systemctl start nessusd.service

┌──(maria㉿kali)-[~/Downloads]
└─$ 
```

I opened my browser within the Kali VM and went to “https://kali:8834” to access the Nessus console locally. Select Advanced and Accept the Risk and Continue if prompted



Welcome to Nessus

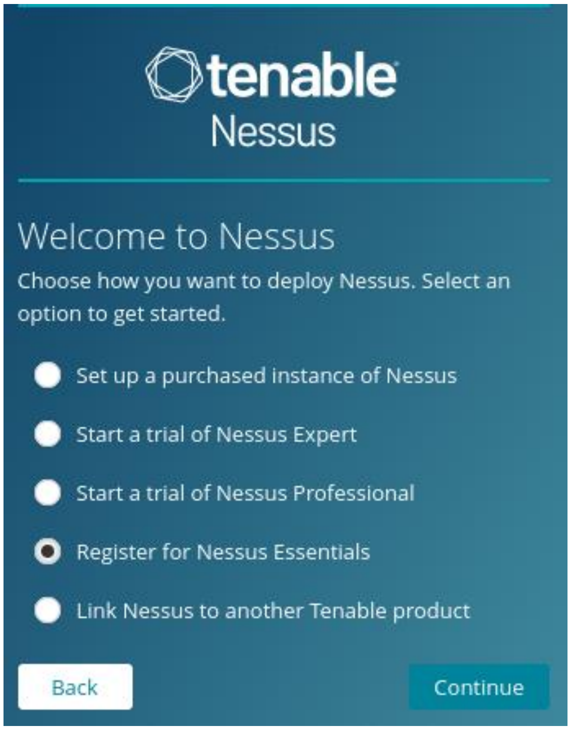
You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.

When you are ready, click Continue to proceed with the installation.

□ Register Offline

Step 4: Configure Nessus

Now that Nessus is installed and running in the Kali VM, I pressed continue. I selected Register for Nessus Essentials and then continue.

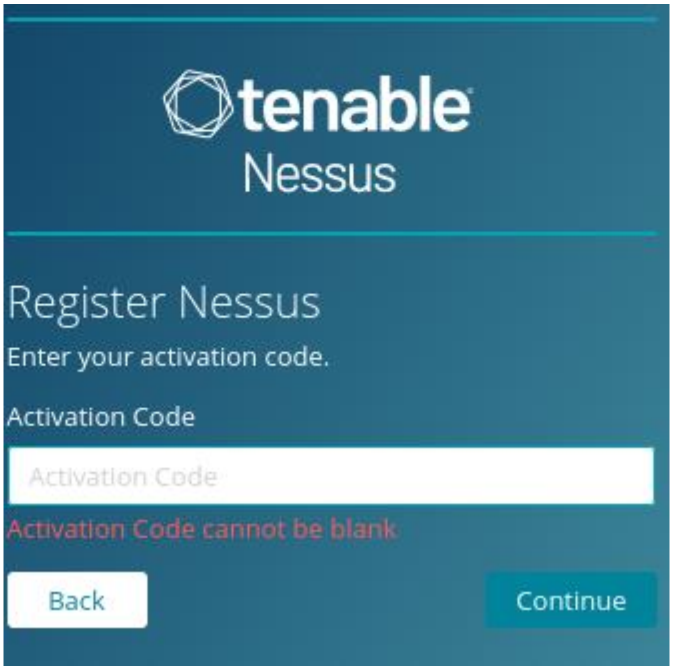


Welcome to Nessus

Choose how you want to deploy Nessus. Select an option to get started.

- ○ Set up a purchased instance of Nessus
- ○ Start a trial of Nessus Expert
- ○ Start a trial of Nessus Professional
- ● Register for Nessus Essentials
- ○ Link Nessus to another Tenable product

I then pressed the skip section because I already have an activation code. I entered my activation code and pressed continue.



Register Nessus

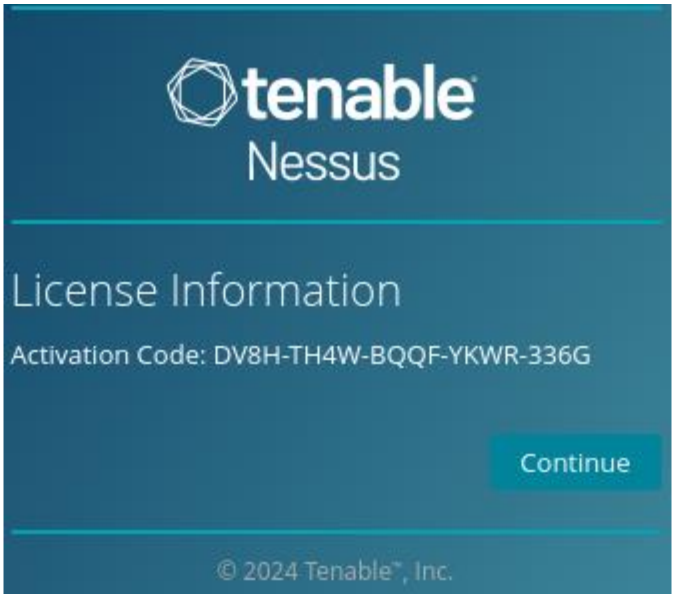
Enter your activation code.

Activation Code

Activation Code

Activation Code cannot be blank

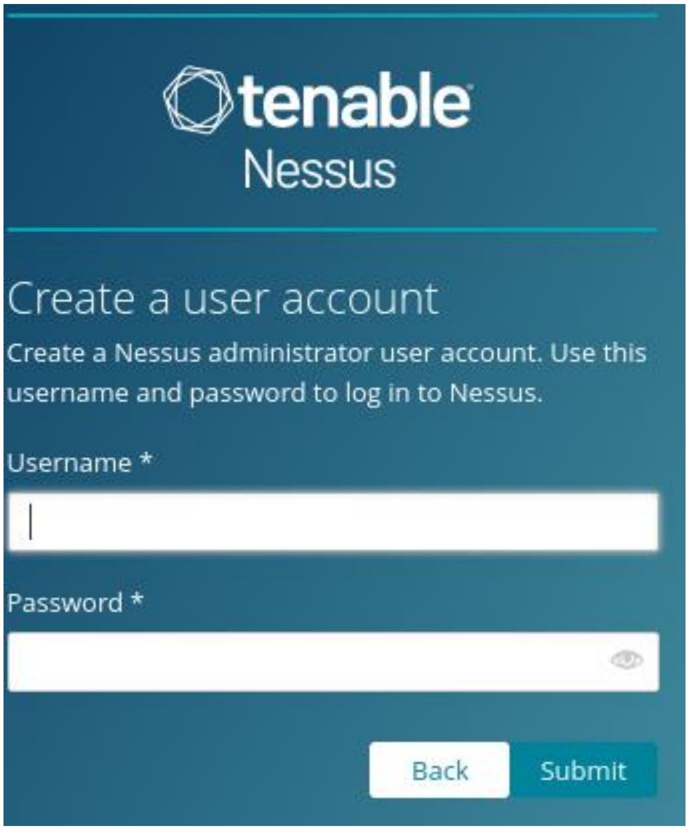
Then I pressed continue again after being presented with the license information.



License Information

Activation Code: DV8H-TH4W-BQQF-YKWR-336G

I then entered a username and password and submitted. Nessus is now downloading the plugins and data.



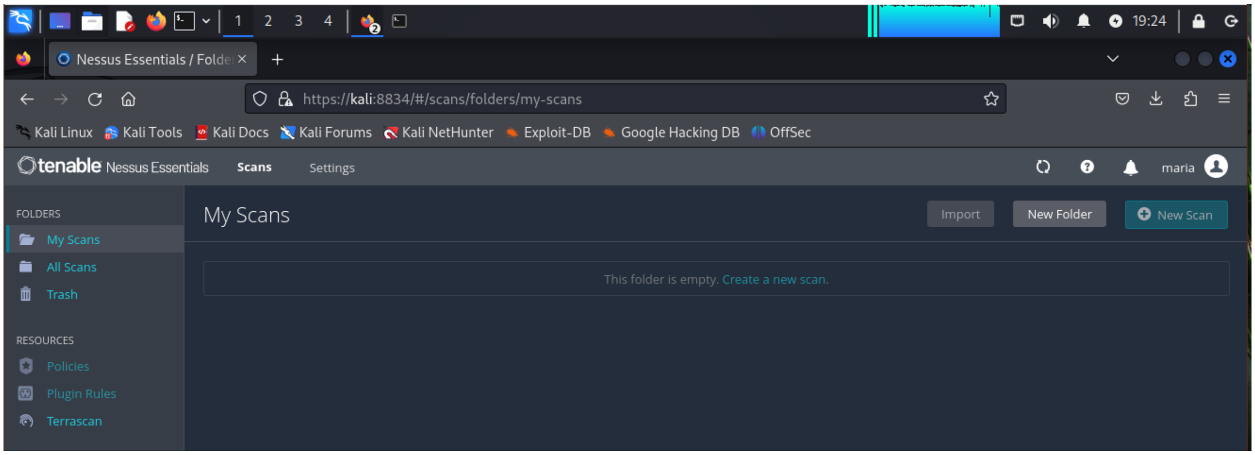
Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

Password *

Plugin and feed data will continue to download in the background which may take 1-2 hours to complete. It is complete when the +new scan button is no longer greyed out.

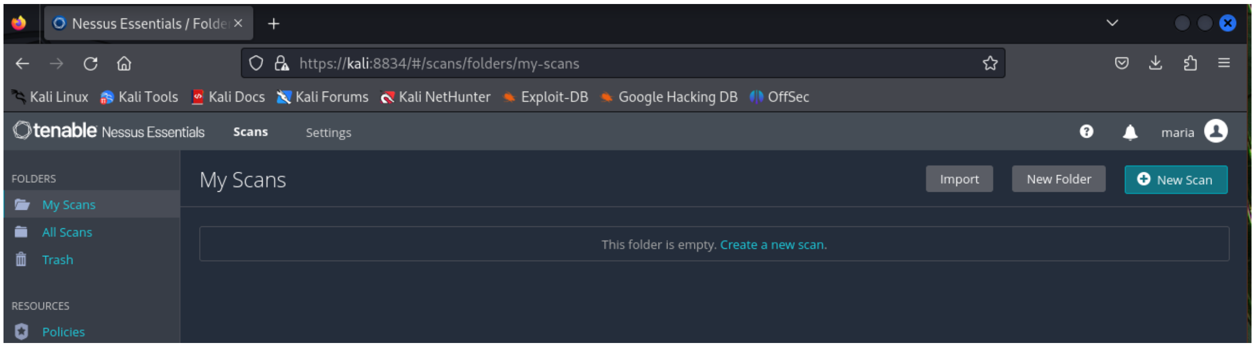


https://kali:8834/#/scans/folders/my-scans

This folder is empty. Create a new scan.

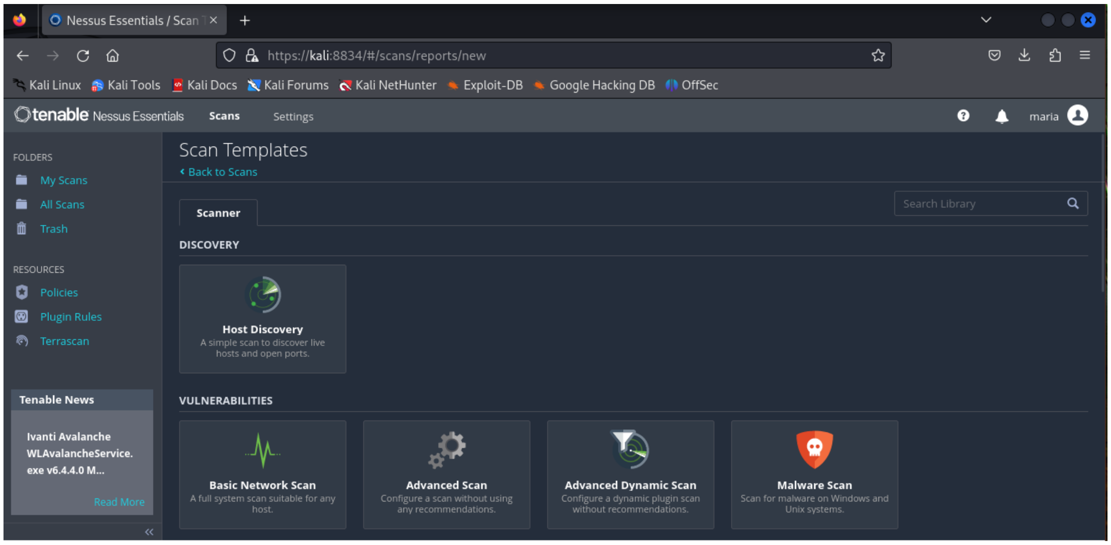
Step 5: Create and launch Scan

With the Nessus running and logged in on the kali VM, I press the new scan button. I then Selected the basic network scan under the vulnerabilities section. Under the Settings tab, Basic menu section, select General. Name the scan “Initial-Maria" and enter the Targets as 10.0.2.0/24. Then press the Save button at the bottom of the form.



https://kali:8834/#/scans/folders/my-scans

This folder is empty. Create a new scan.



Scan Templates

Ivanti Avalanche WLAvalancheService.exe v6.4.4.0 M...

DISCOVERY

Host Discovery A simple scan to discover live hosts and open ports.

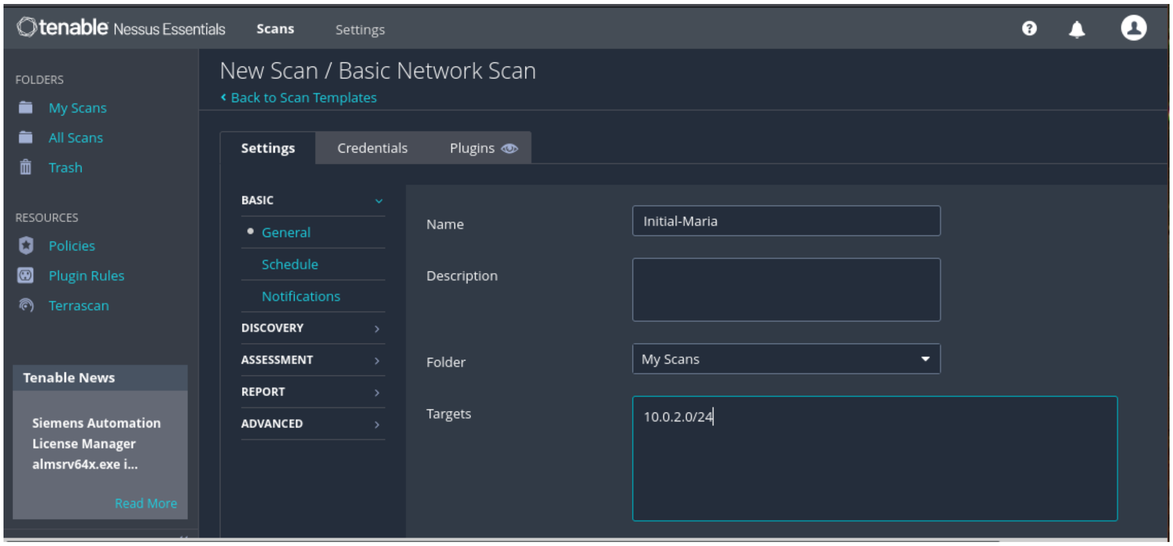
VULNERABILITIES

Basic Network Scan A full system scan suitable for any host.

Advanced Scan Configure a scan without using any recommendations.

Advanced Dynamic Scan Configure a dynamic plugin scan without recommendations.

Malware Scan Scan for malware on Windows and Unix systems.



New Scan / Basic Network Scan

Siemens Automation License Manager almsrv64x.exe i...

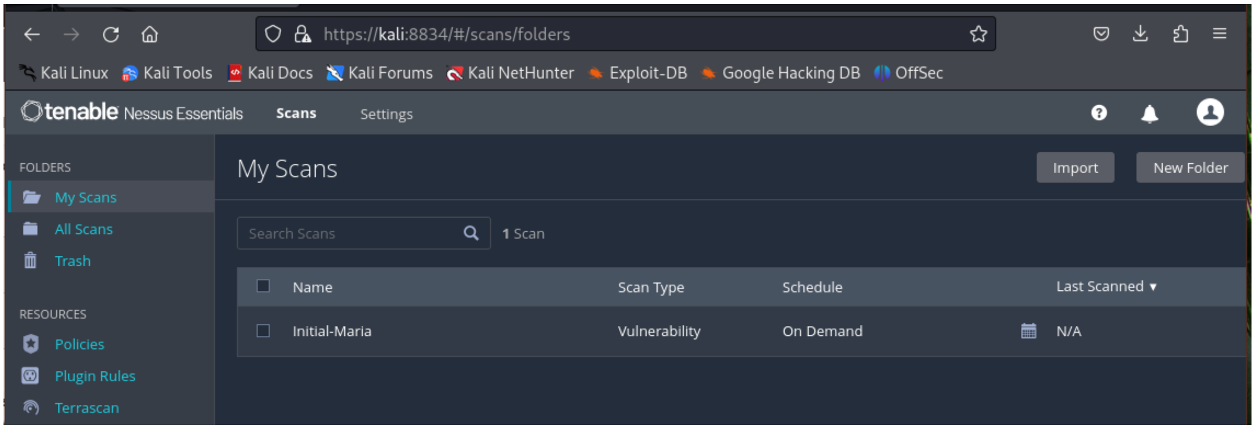
Name: Initial-Maria

Description:

Folder: My Scans

Targets: 10.0.2.0/24

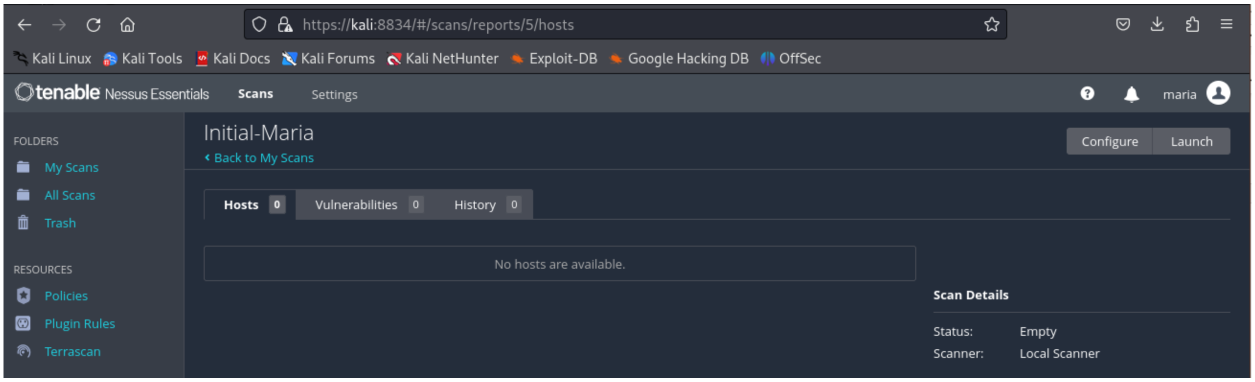
I observed the scan configurations are now listed under my scans. I clicked the name to open more options and pressed launch in the upper right corner. I observed the scan show status running.



My Scans

1 Scan

Name	Scan Type	Schedule	Last Scanned ▾
Initial-Maria	Vulnerability	On Demand	N/A



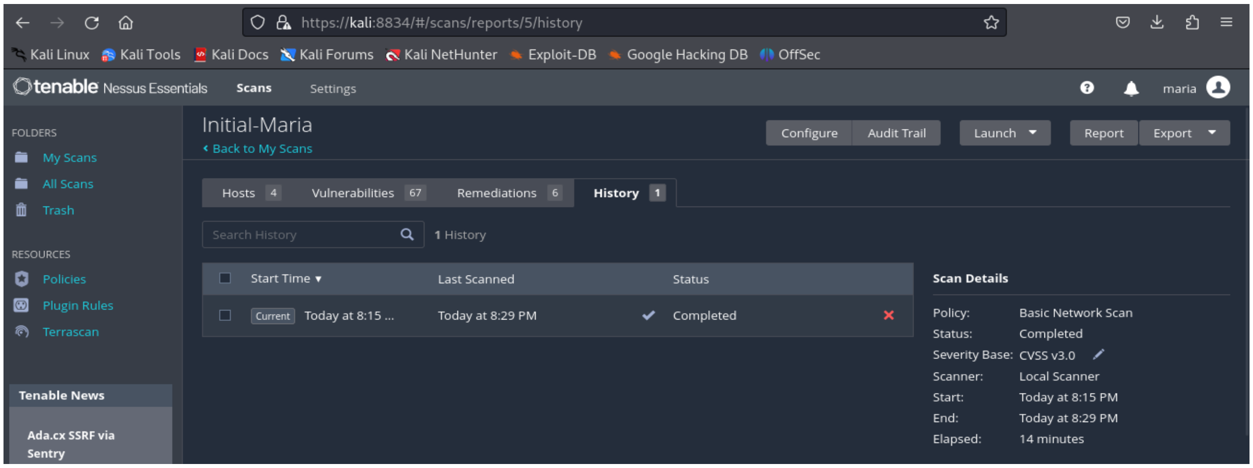
No hosts are available.

Scan Details

Status:	Empty
Scanner:	Local Scanner

Step 6: Analyze Results

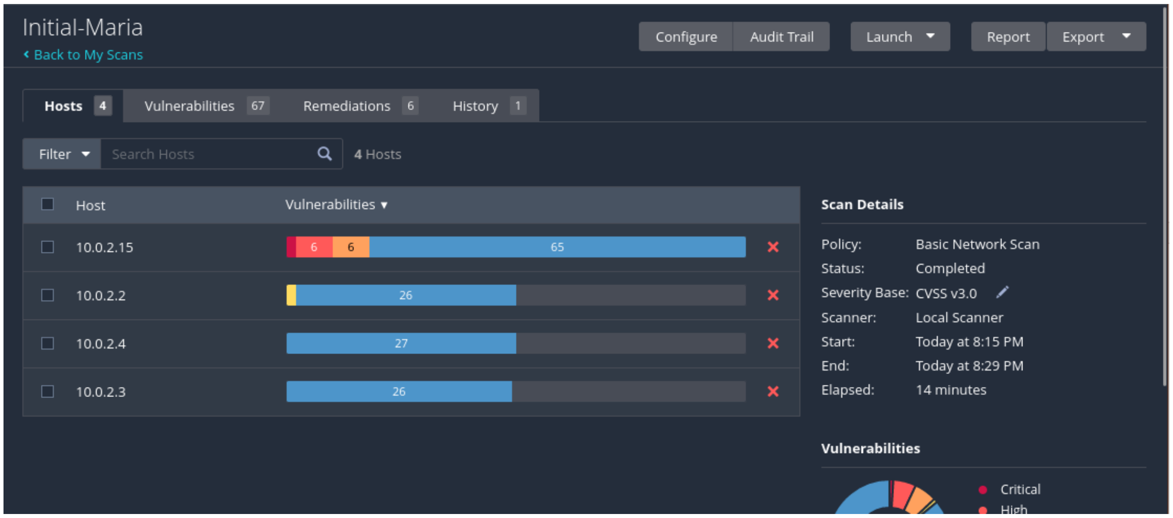
Now that the scan was completed, I explored the Hosts and Vulnerabilities tab. The vulnerabilities are listed in order of severity. I explored further details on one of the items by clicking on the vulnerability.



☐	Start Time ▾	Last Scanned	Status	
☐	Current Today at 8:15 ...	Today at 8:29 PM	✓ Completed	✕

Scan Details

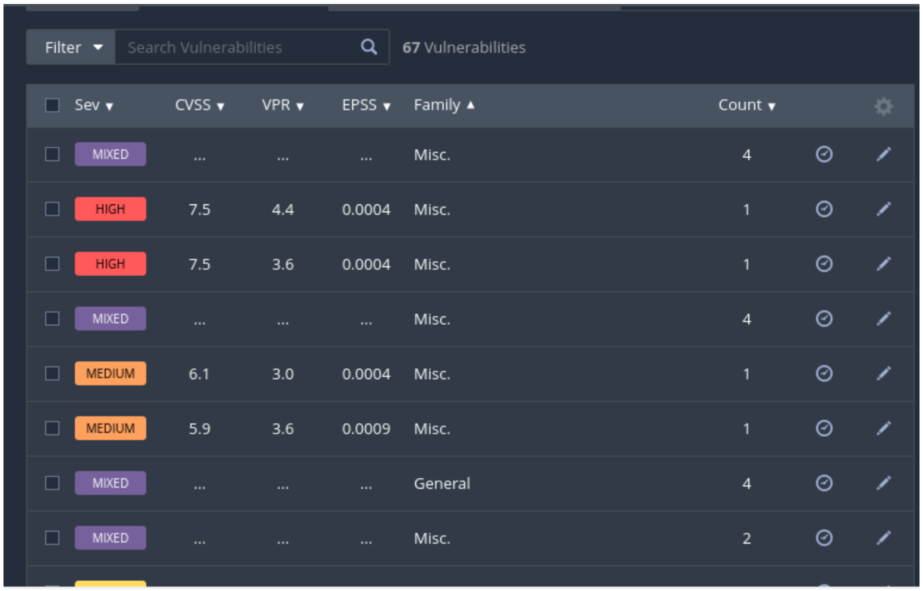
Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:15 PM
End:	Today at 8:29 PM
Elapsed:	14 minutes



☐	Host	Vulnerabilities ▾	
☐	10.0.2.15	6 6 65	✕
☐	10.0.2.2	26	✕
☐	10.0.2.4	27	✕
☐	10.0.2.3	26	✕

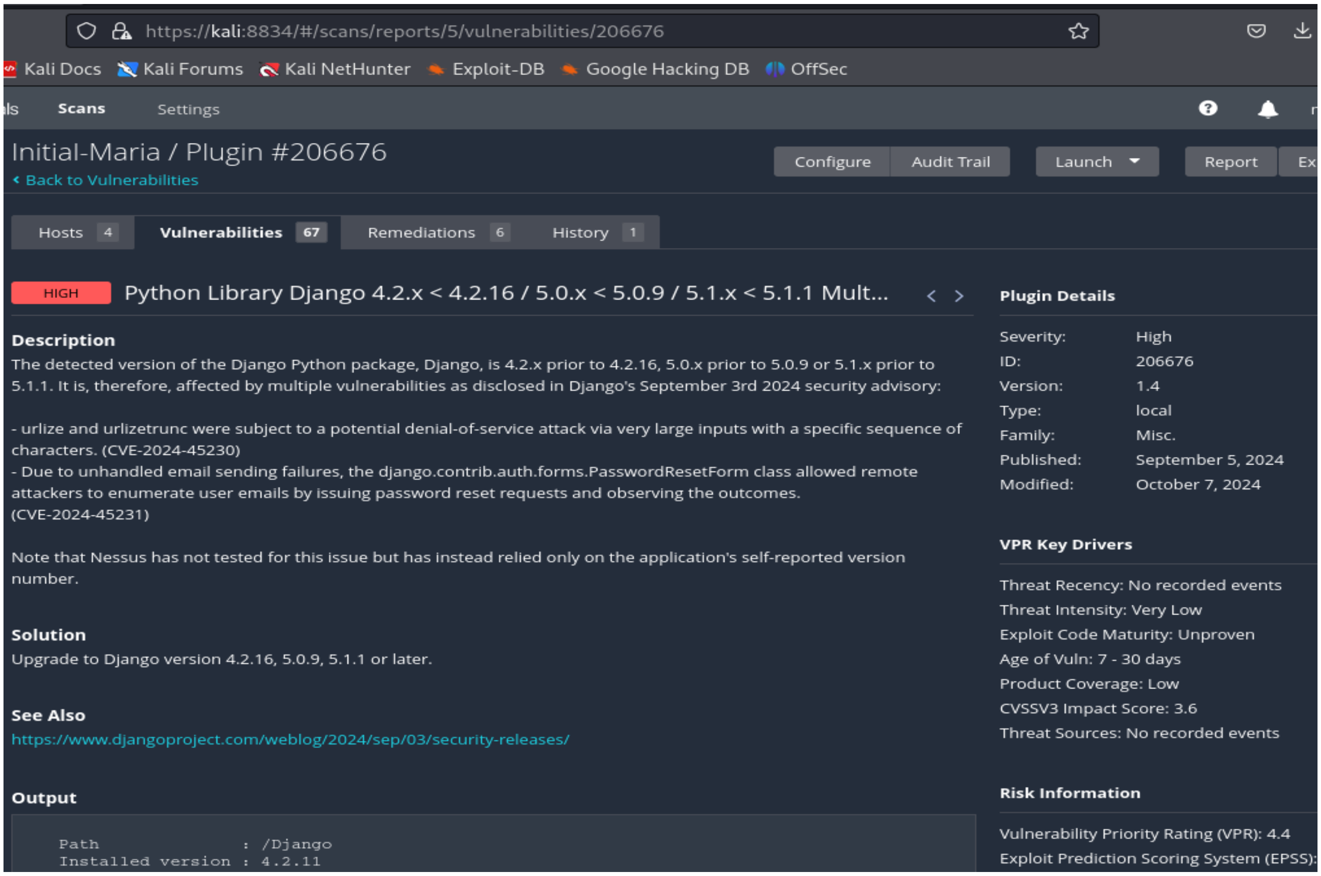
Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:15 PM
End:	Today at 8:29 PM
Elapsed:	14 minutes



67 Vulnerabilities

☐ Sev	CVSS	VPR	EPSS	Family	Count
☐ MIXED	...	...	...	Misc.	4
☐ HIGH	7.5	4.4	0.0004	Misc.	1
☐ HIGH	7.5	3.6	0.0004	Misc.	1
☐ MIXED	...	...	...	Misc.	4
☐ MEDIUM	6.1	3.0	0.0004	Misc.	1
☐ MEDIUM	5.9	3.6	0.0009	Misc.	1
☐ MIXED	...	...	...	General	4
☐ MIXED	...	...	...	Misc.	2



Initial-Maria / Plugin #206676

‹ Back to Vulnerabilities

HIGH Python Library Django 4.2.x < 4.2.16 / 5.0.x < 5.0.9 / 5.1.x < 5.1.1 Mult...

Description

The detected version of the Django Python package, Django, is 4.2.x prior to 4.2.16, 5.0.x prior to 5.0.9 or 5.1.x prior to 5.1.1. It is, therefore, affected by multiple vulnerabilities as disclosed in Django's September 3rd 2024 security advisory:

- urlize and urlizetrunc were subject to a potential denial-of-service attack via very large inputs with a specific sequence of characters. (CVE-2024-45230)
- Due to unhandled email sending failures, the django.contrib.auth.forms.PasswordResetForm class allowed remote attackers to enumerate user emails by issuing password reset requests and observing the outcomes. (CVE-2024-45231)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Django version 4.2.16, 5.0.9, 5.1.1 or later.

See Also

https://www.djangoproject.com/weblog/2024/sep/03/security-releases/

Output

```
    Path              : /Django
    Installed version : 4.2.11
```

Plugin Details

Severity:	High
ID:	206676
Version:	1.4
Type:	local
Family:	Misc.
Published:	September 5, 2024
Modified:	October 7, 2024

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 7 - 30 days
Product Coverage: Low
CVSSV3 Impact Score: 3.6
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 4.4
Exploit Prediction Scoring System (EPSS):

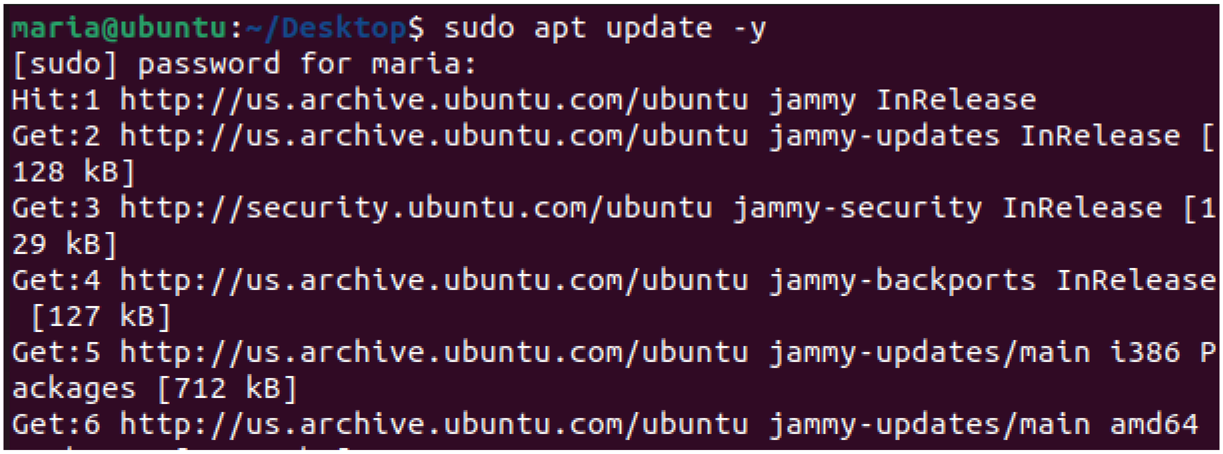
The Nessus vulnerability report indicated that the Django Python Library in use has known security vulnerabilities. They advised me to upgrade to a more secure version. Nessus flagged this as a high severity vulnerability which means it requires action. To fix this issue, we must upgrade Django to the appropriate patched version. To check which version is installed, use the “python -m django –version" and then upgrade it using “pip install –upgrade “django>=VERSION”. Doing this should fix the vulnerability.

Exercise 7.3 Snort Detection

In this task, I used Snort to analyze a packet capture from malware-traffic-analysis.net

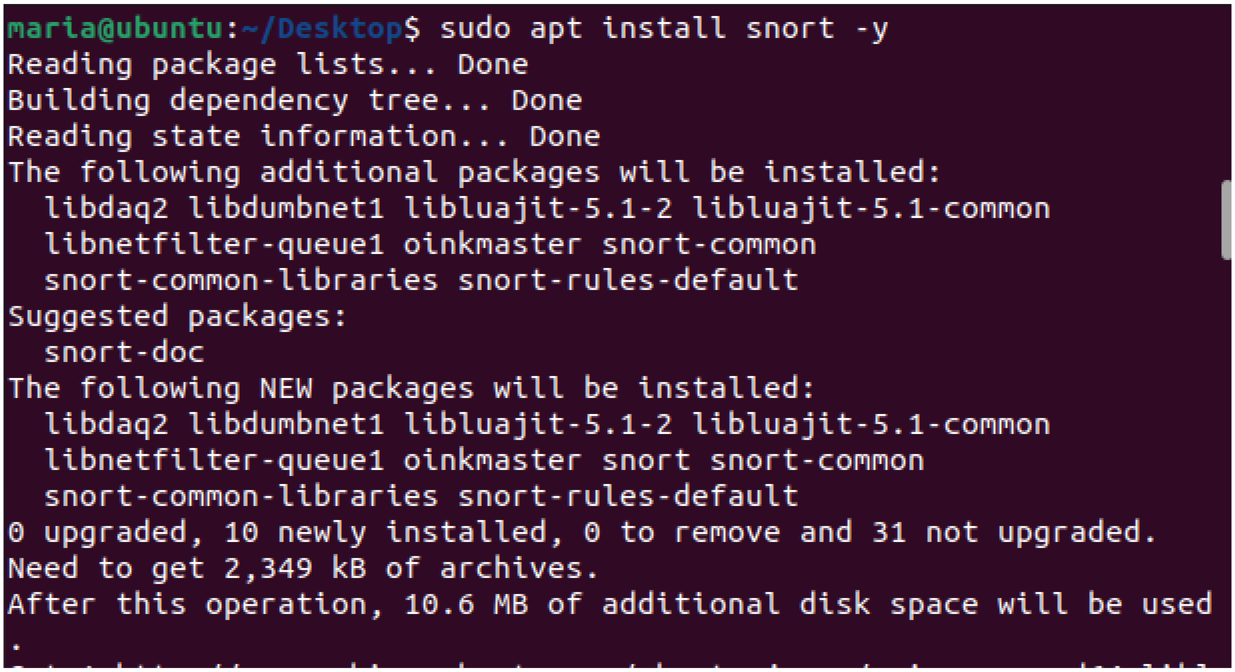
Step 1: Install Snort

On my Ubuntu VM with Bridge Adapter network mode, I logged in and opened a terminal. I applied any updates on my system with the following command.

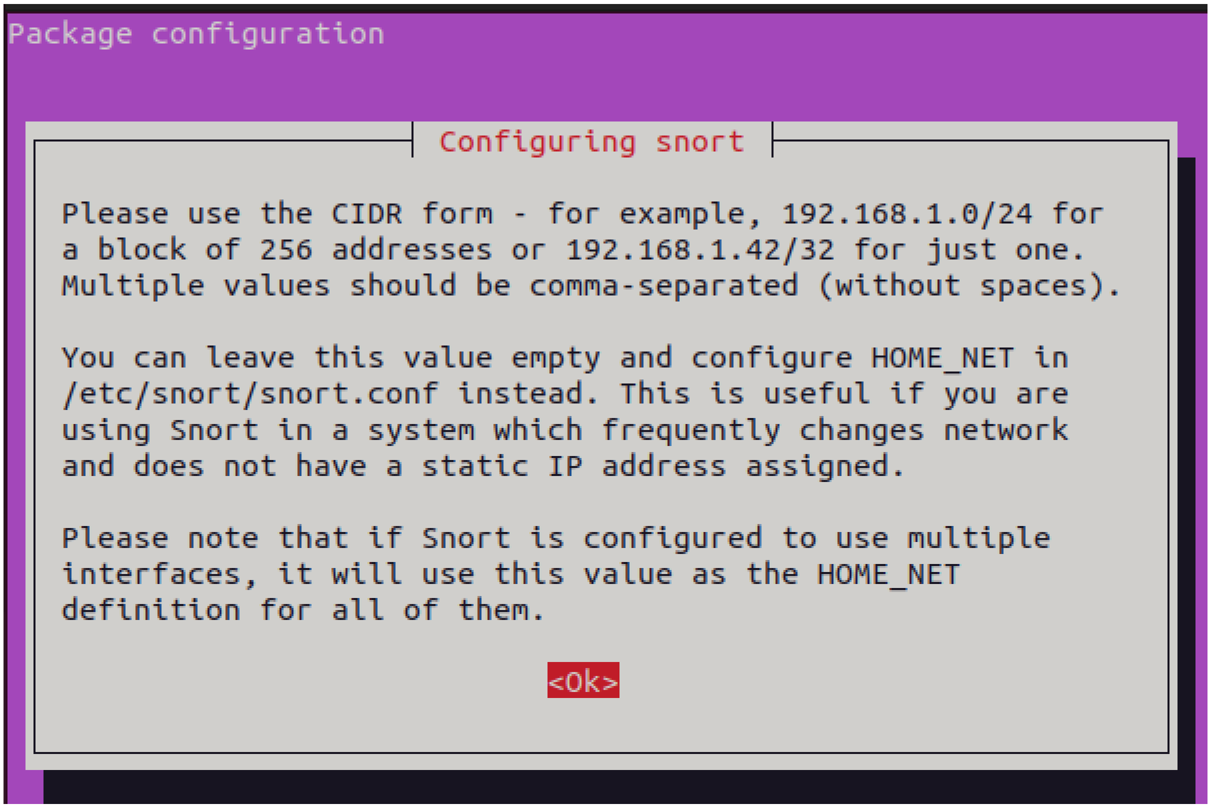


```
maria@ubuntu:~/Desktop$ sudo apt update -y
[sudo] password for maria:
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [
128 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [1
29 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
 [127 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu jammy-updates/main i386 P
ackages [712 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64
```

Then, I installed snort using apt and accepted default Snort network configuration.

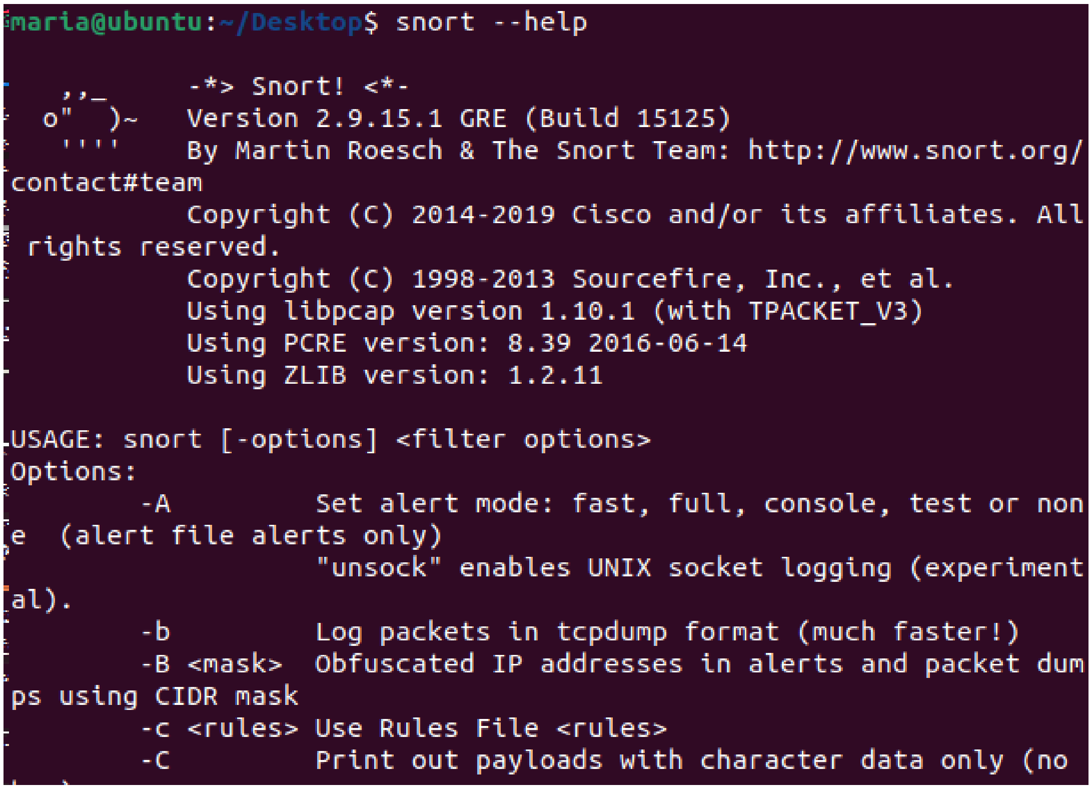


```
maria@ubuntu:~/Desktop$ sudo apt install snort -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common
  libnetfilter-queue1 oinkmaster snort-common
  snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common
  libnetfilter-queue1 oinkmaster snort snort-common
  snort-common-libraries snort-rules-default
0 upgraded, 10 newly installed, 0 to remove and 31 not upgraded.
Need to get 2,349 kB of archives.
After this operation, 10.6 MB of additional disk space will be used
.
```



```
Package configuration

                     Configuring snort

  Please use the CIDR form - for example, 192.168.1.0/24 for
  a block of 256 addresses or 192.168.1.42/32 for just one.
  Multiple values should be comma-separated (without spaces).

  You can leave this value empty and configure HOME_NET in
  /etc/snort/snort.conf instead. This is useful if you are
  using Snort in a system which frequently changes network
  and does not have a static IP address assigned.

  Please note that if Snort is configured to use multiple
  interfaces, it will use this value as the HOME_NET
  definition for all of them.

                           <Ok>
```

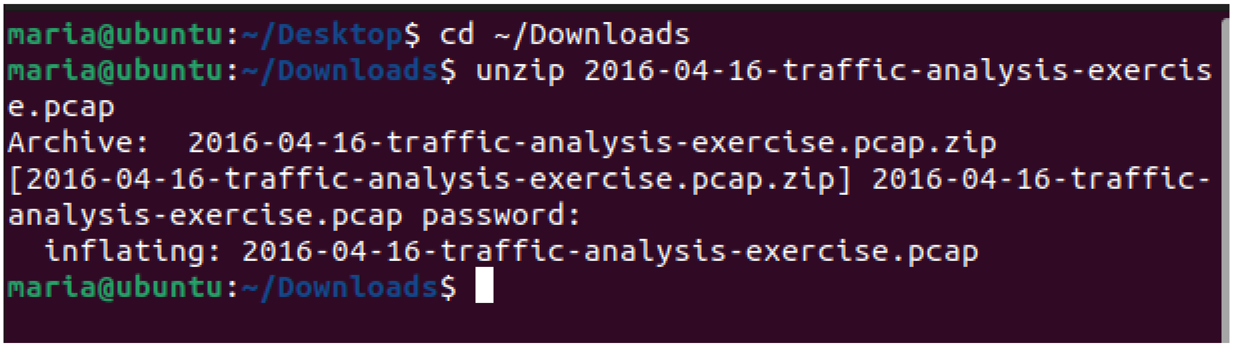
I confirmed snort was installed using the command below.



```
maria@ubuntu:~/Desktop$ snort --help

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/
contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All
 rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

USAGE: snort [-options] <filter options>
Options:
        -A         Set alert mode: fast, full, console, test or non
e  (alert file alerts only)
                   "unsock" enables UNIX socket logging (experiment
al).
        -b         Log packets in tcpdump format (much faster!)
        -B <mask>  Obfuscated IP addresses in alerts and packet dum
ps using CIDR mask
        -c <rules> Use Rules File <rules>
        -C         Print out payloads with character data only (no
```

Step 2: Download Malicious PCAP

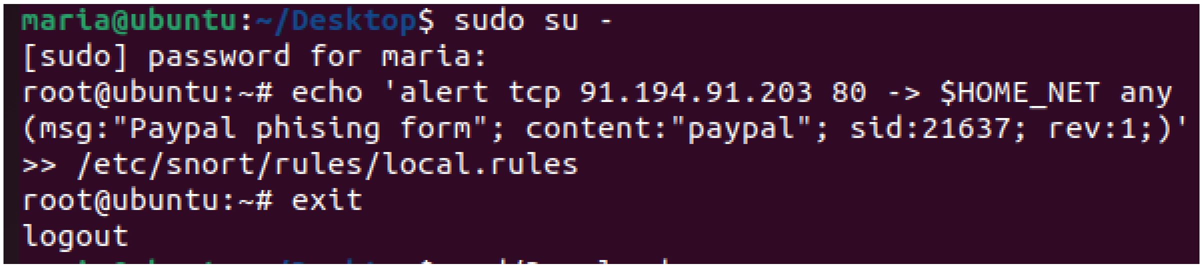
Within the Ubuntu VM, I downloaded the accompanying file and unzipped it.



```
maria@ubuntu:~/Desktop$ cd ~/Downloads
maria@ubuntu:~/Downloads$ unzip 2016-04-16-traffic-analysis-exercis
e.pcap
Archive:  2016-04-16-traffic-analysis-exercise.pcap.zip
[2016-04-16-traffic-analysis-exercise.pcap.zip] 2016-04-16-traffic-
analysis-exercise.pcap password:
  inflating: 2016-04-16-traffic-analysis-exercise.pcap
maria@ubuntu:~/Downloads$ 
```

Step 3: Create Custom Rule

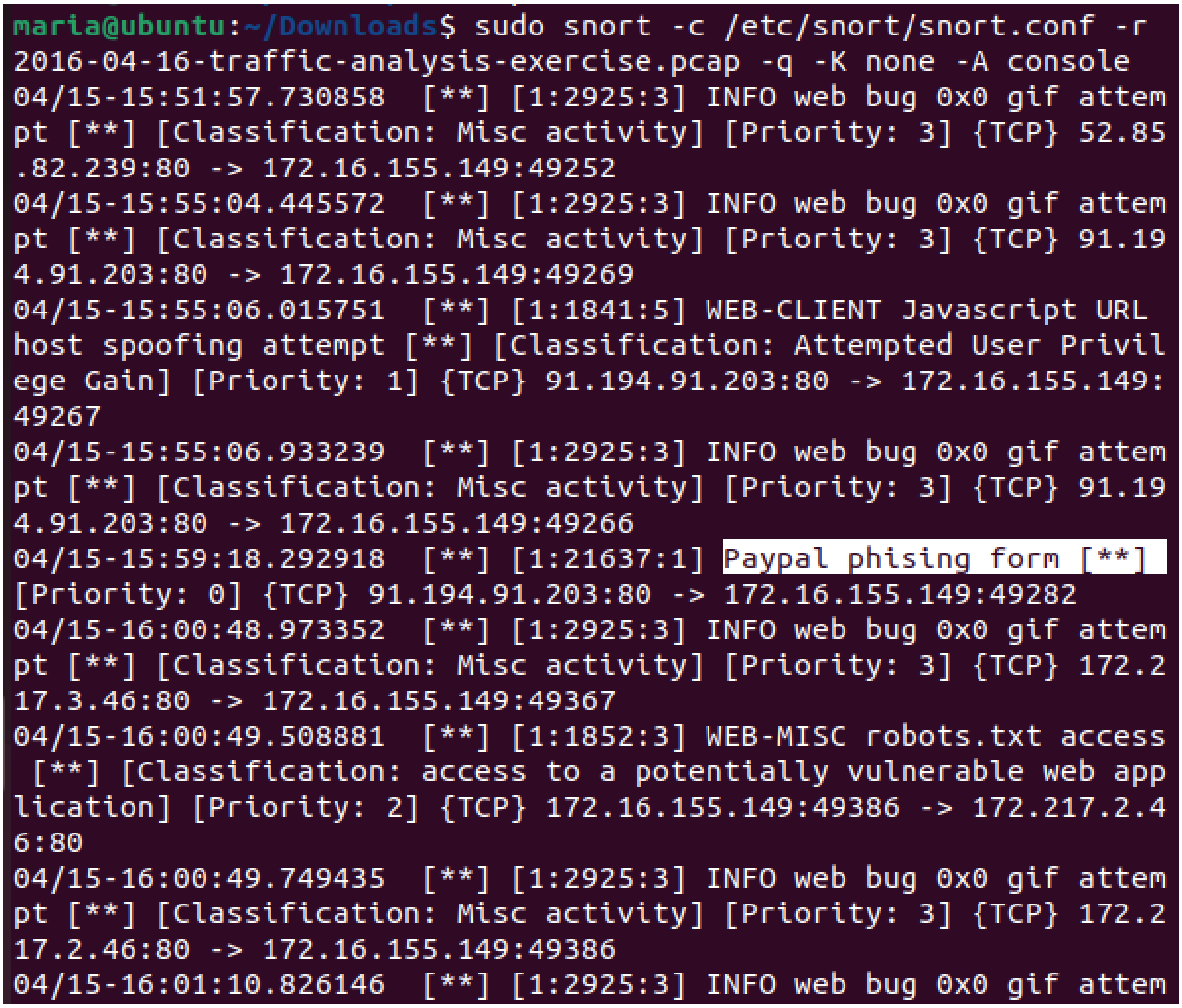
I created a custom rule to detect if a known malicious webserver has been accessed and credential form submitted. I switched user to root, then echo the rule to the local.rules file and exited the root terminal.



```
maria@ubuntu:~/Desktop$ sudo su -
[sudo] password for maria:
root@ubuntu:~# echo 'alert tcp 91.194.91.203 80 -> $HOME_NET any
(msg:"Paypal phising form"; content:"paypal"; sid:21637; rev:1;)'
>> /etc/snort/rules/local.rules
root@ubuntu:~# exit
logout
```

Step 4: Analyze the PCAP

I ran Snort against the unzipped PCAP file in my downloads folder and observed the paypal rule was triggered.



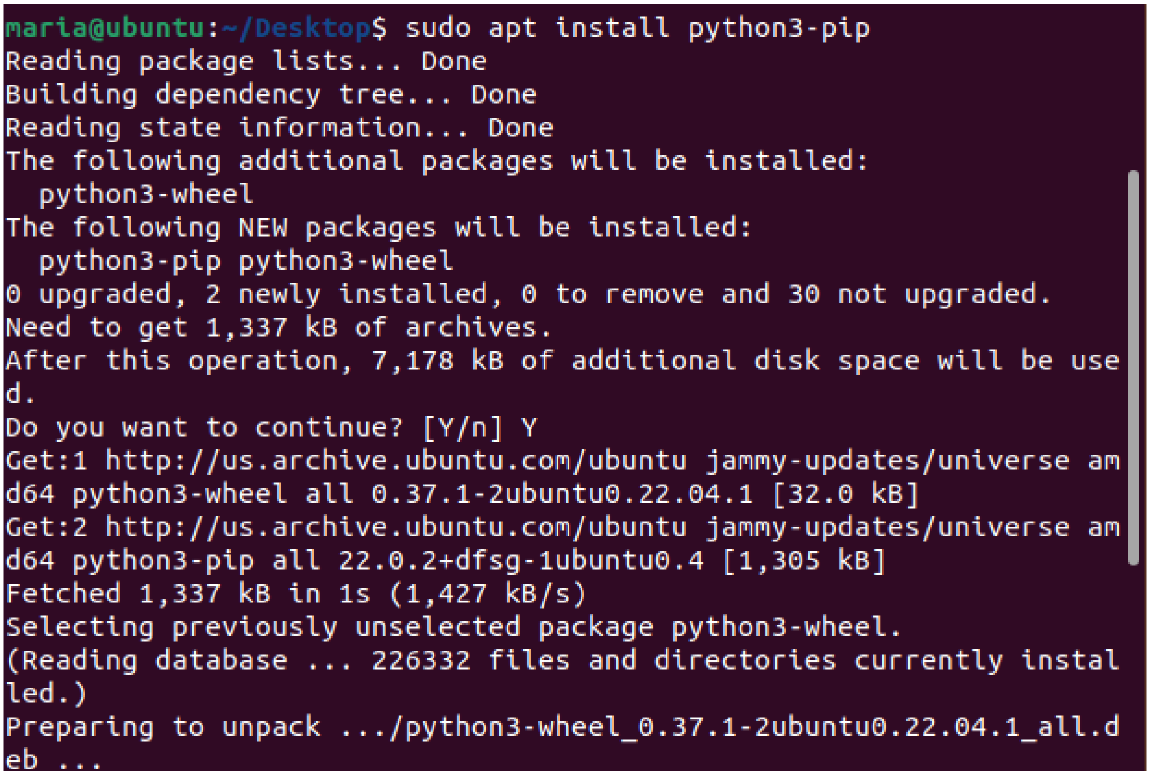
```
maria@ubuntu:~/Downloads$ sudo snort -c /etc/snort/snort.conf -r
2016-04-16-traffic-analysis-exercise.pcap -q -K none -A console
04/15-15:51:57.730858  [**] [1:2925:3] INFO web bug 0x0 gif attem
pt [**] [Classification: Misc activity] [Priority: 3] {TCP} 52.85
.82.239:80 -> 172.16.155.149:49252
04/15-15:55:04.445572  [**] [1:2925:3] INFO web bug 0x0 gif attem
pt [**] [Classification: Misc activity] [Priority: 3] {TCP} 91.19
4.91.203:80 -> 172.16.155.149:49269
04/15-15:55:06.015751  [**] [1:1841:5] WEB-CLIENT Javascript URL
host spoofing attempt [**] [Classification: Attempted User Privil
ege Gain] [Priority: 1] {TCP} 91.194.91.203:80 -> 172.16.155.149:
49267
04/15-15:55:06.933239  [**] [1:2925:3] INFO web bug 0x0 gif attem
pt [**] [Classification: Misc activity] [Priority: 3] {TCP} 91.19
4.91.203:80 -> 172.16.155.149:49266
04/15-15:59:18.292918  [**] [1:21637:1] Paypal phising form [**]
[Priority: 0] {TCP} 91.194.91.203:80 -> 172.16.155.149:49282
04/15-16:00:48.973352  [**] [1:2925:3] INFO web bug 0x0 gif attem
pt [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.2
17.3.46:80 -> 172.16.155.149:49367
04/15-16:00:49.508881  [**] [1:1852:3] WEB-MISC robots.txt access
 [**] [Classification: access to a potentially vulnerable web app
lication] [Priority: 2] {TCP} 172.16.155.149:49386 -> 172.217.2.4
6:80
04/15-16:00:49.749435  [**] [1:2925:3] INFO web bug 0x0 gif attem
pt [**] [Classification: Misc activity] [Priority: 3] {TCP} 172.2
17.2.46:80 -> 172.16.155.149:49386
04/15-16:01:10.826146  [**] [1:2925:3] INFO web bug 0x0 gif attem
```

Exercise 7.4 MySQL Honeypot

In this exercise, i used opensource Python honeypots to create a honeypot running on my ubuntu VM in Bridged Adapter network mode. I then attacked the Ubuntu VM from my Kali VM also in Bridge Adapter network mode.

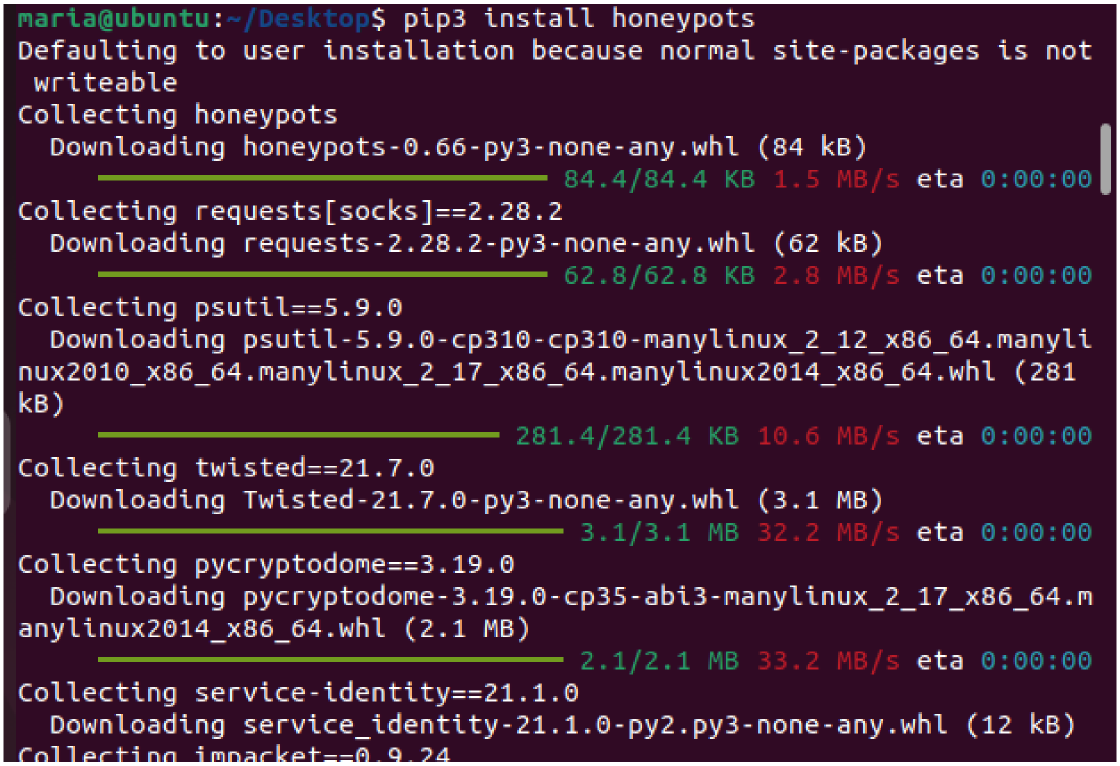
Step 1: Install honeypots

From my Ubuntu VM, I installed python3-pip.



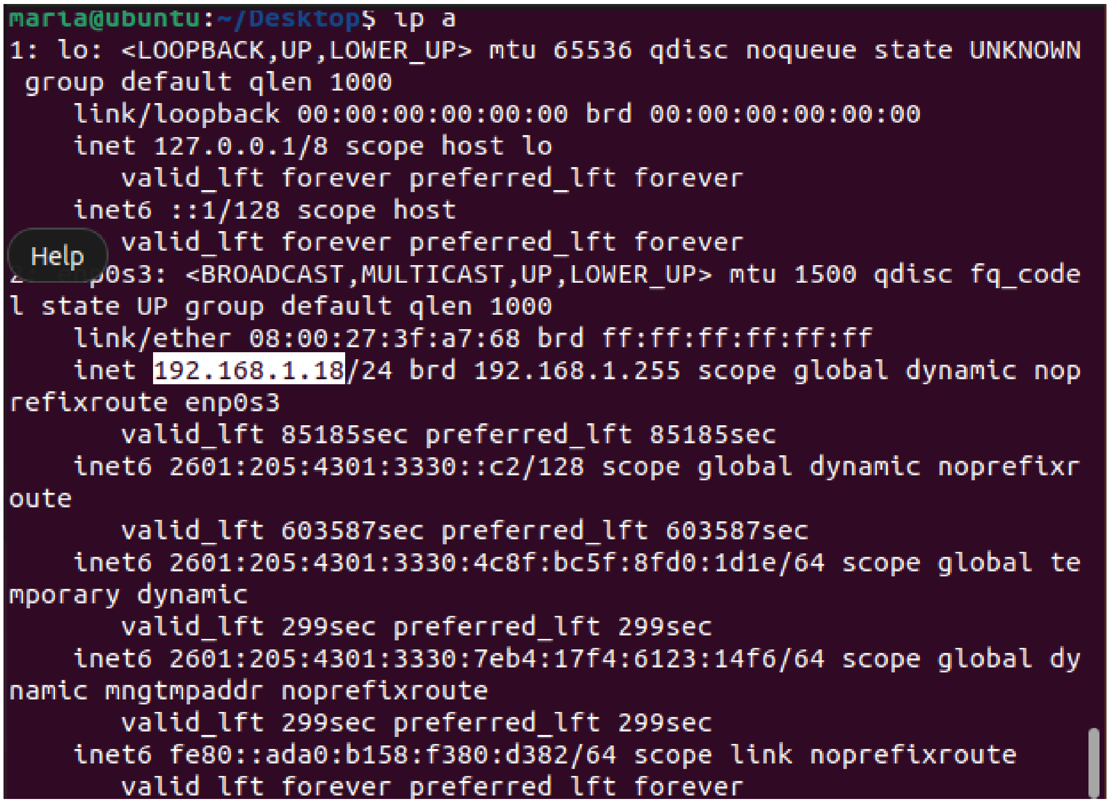
```
maria@ubuntu:~/Desktop$ sudo apt install python3-pip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-wheel
The following NEW packages will be installed:
  python3-pip python3-wheel
0 upgraded, 2 newly installed, 0 to remove and 30 not upgraded.
Need to get 1,337 kB of archives.
After this operation, 7,178 kB of additional disk space will be use
d.
Do you want to continue? [Y/n] Y
Get:1 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe am
d64 python3-wheel all 0.37.1-2ubuntu0.22.04.1 [32.0 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe am
d64 python3-pip all 22.0.2+dfsg-1ubuntu0.4 [1,305 kB]
Fetched 1,337 kB in 1s (1,427 kB/s)
Selecting previously unselected package python3-wheel.
(Reading database ... 226332 files and directories currently instal
led.)
Preparing to unpack .../python3-wheel_0.37.1-2ubuntu0.22.04.1_all.d
eb ...
```

After it was installed, I installed the honeypots module.



```
maria@ubuntu:~/Desktop$ pip3 install honeypots
Defaulting to user installation because normal site-packages is not
 writeable
Collecting honeypots
  Downloading honeypots-0.66-py3-none-any.whl (84 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 84.4/84.4 KB 1.5 MB/s eta 0:00:00
Collecting requests[socks]==2.28.2
  Downloading requests-2.28.2-py3-none-any.whl (62 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 62.8/62.8 KB 2.8 MB/s eta 0:00:00
Collecting psutil==5.9.0
  Downloading psutil-5.9.0-cp310-cp310-manylinux_2_12_x86_64.manyli
nux2010_x86_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl (281
kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━ 281.4/281.4 KB 10.6 MB/s eta 0:00:00
Collecting twisted==21.7.0
  Downloading Twisted-21.7.0-py3-none-any.whl (3.1 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 3.1/3.1 MB 32.2 MB/s eta 0:00:00
Collecting pycryptodome==3.19.0
  Downloading pycryptodome-3.19.0-cp35-abi3-manylinux_2_17_x86_64.m
anylinux2014_x86_64.whl (2.1 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.1/2.1 MB 33.2 MB/s eta 0:00:00
Collecting service-identity==21.1.0
  Downloading service_identity-21.1.0-py2.py3-none-any.whl (12 kB)
Collecting impacket==0.9.24
```

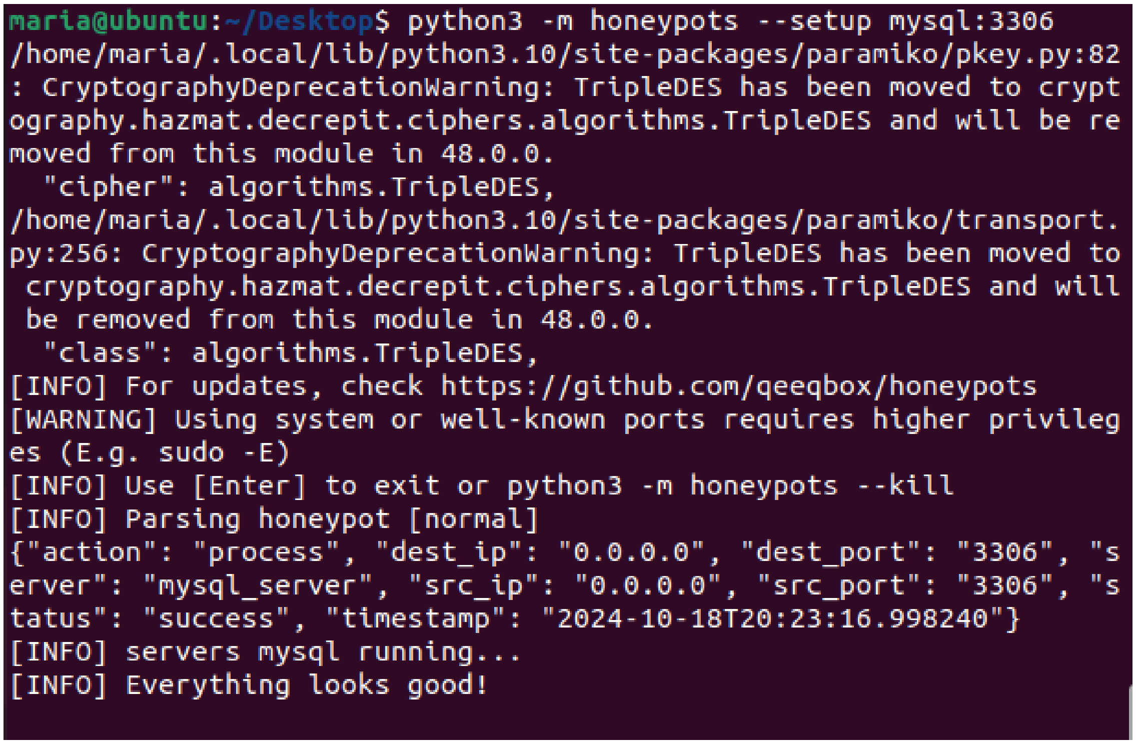
I then checked my IP address.



```
maria@ubuntu:~/Desktop$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
 group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_code
l state UP group default qlen 1000
    link/ether 08:00:27:3f:a7:68 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.18/24 brd 192.168.1.255 scope global dynamic nop
refixroute enp0s3
       valid_lft 85185sec preferred_lft 85185sec
    inet6 2601:205:4301:3330::c2/128 scope global dynamic noprefixr
oute
       valid_lft 603587sec preferred_lft 603587sec
    inet6 2601:205:4301:3330:4c8f:bc5f:8fd0:1d1e/64 scope global te
mporary dynamic
       valid_lft 299sec preferred_lft 299sec
    inet6 2601:205:4301:3330:7eb4:17f4:6123:14f6/64 scope global dy
namic mngtmpaddr noprefixroute
       valid_lft 299sec preferred_lft 299sec
    inet6 fe80::ada0:b158:f380:d382/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Step 2: Setup MySQL Honeypot

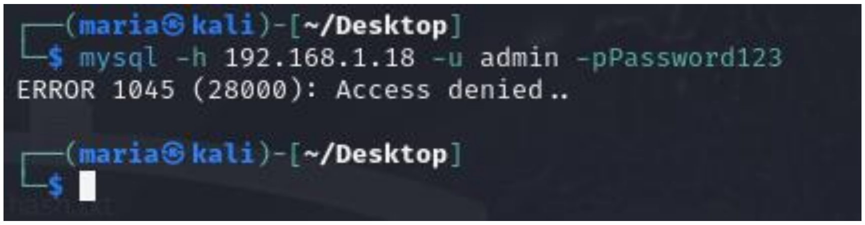
In this step, I set up a MySQL honeypot running on port 3306.



```
maria@ubuntu:~/Desktop$ python3 -m honeypots --setup mysql:3306
/home/maria/.local/lib/python3.10/site-packages/paramiko/pkey.py:82
: CryptographyDeprecationWarning: TripleDES has been moved to crypt
ography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be re
moved from this module in 48.0.0.
  "cipher": algorithms.TripleDES,
/home/maria/.local/lib/python3.10/site-packages/paramiko/transport.
py:256: CryptographyDeprecationWarning: TripleDES has been moved to
 cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will
 be removed from this module in 48.0.0.
  "class": algorithms.TripleDES,
[INFO] For updates, check https://github.com/qeeqbox/honeypots
[WARNING] Using system or well-known ports requires higher privileg
es (E.g. sudo -E)
[INFO] Use [Enter] to exit or python3 -m honeypots --kill
[INFO] Parsing honeypot [normal]
{"action": "process", "dest_ip": "0.0.0.0", "dest_port": "3306", "s
erver": "mysql_server", "src_ip": "0.0.0.0", "src_port": "3306", "s
tatus": "success", "timestamp": "2024-10-18T20:23:16.998240"}
[INFO] servers mysql running...
[INFO] Everything looks good!
```

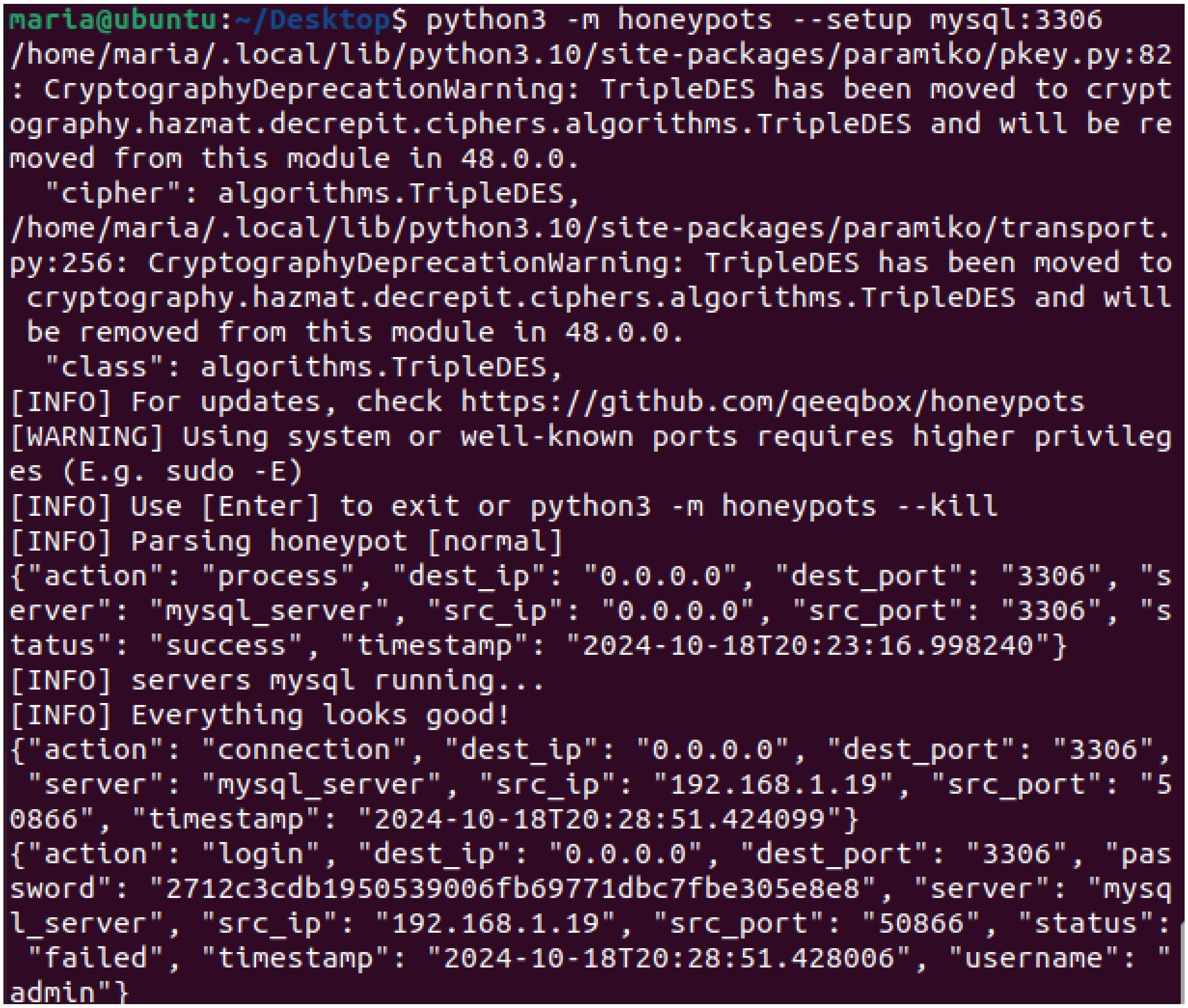
Step 3: Attack the MySQL Port

From my Kali VM I launched a terminal and made a connection to my Ubuntu VM using the mysql client.



```
┌──(maria㉿kali)-[~/Desktop]
└─$ mysql -h 192.168.1.18 -u admin -pPassword123
ERROR 1045 (28000): Access denied..

┌──(maria㉿kali)-[~/Desktop]
└─$ 
```

I returned to my Ubuntu VM and observed that the attack was registered!



```
maria@ubuntu:~/Desktop$ python3 -m honeypots --setup mysql:3306
/home/maria/.local/lib/python3.10/site-packages/paramiko/pkey.py:82
: CryptographyDeprecationWarning: TripleDES has been moved to crypt
ography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be re
moved from this module in 48.0.0.
  "cipher": algorithms.TripleDES,
/home/maria/.local/lib/python3.10/site-packages/paramiko/transport.
py:256: CryptographyDeprecationWarning: TripleDES has been moved to
 cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will
 be removed from this module in 48.0.0.
  "class": algorithms.TripleDES,
[INFO] For updates, check https://github.com/qeeqbox/honeypots
[WARNING] Using system or well-known ports requires higher privileg
es (E.g. sudo -E)
[INFO] Use [Enter] to exit or python3 -m honeypots --kill
[INFO] Parsing honeypot [normal]
{"action": "process", "dest_ip": "0.0.0.0", "dest_port": "3306", "s
erver": "mysql_server", "src_ip": "0.0.0.0", "src_port": "3306", "s
tatus": "success", "timestamp": "2024-10-18T20:23:16.998240"}
[INFO] servers mysql running...
[INFO] Everything looks good!
{"action": "connection", "dest_ip": "0.0.0.0", "dest_port": "3306",
 "server": "mysql_server", "src_ip": "192.168.1.19", "src_port": "5
0866", "timestamp": "2024-10-18T20:28:51.424099"}
{"action": "login", "dest_ip": "0.0.0.0", "dest_port": "3306", "pas
sword": "2712c3cdb1950539006fb69771dbc7fbe305e8e8", "server": "mysq
l_server", "src_ip": "192.168.1.19", "src_port": "50866", "status":
 "failed", "timestamp": "2024-10-18T20:28:51.428006", "username": "
admin"}
```