Kevin Cendana
Spring 2024
CSC 154

Lab 05 - Security Systems

Task 1

Executive Summary: Cybersecurity in 2024

Dear Team,

Diving into the CrowdStrike 2023 Global Threat Report, it's clear that we are up against some very sophisticated threats out there. Here's the breakdown on where problems stand and how we can brush up our defenses.

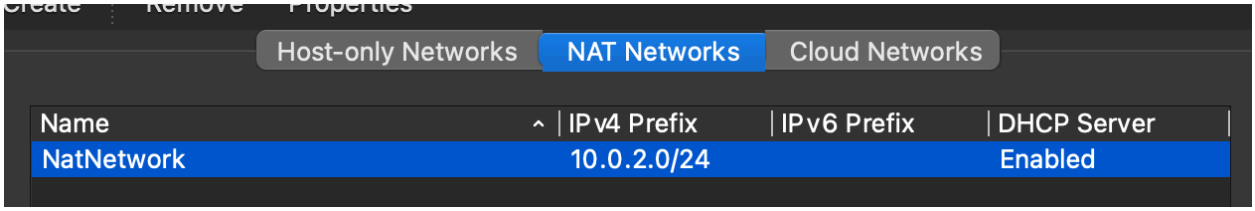
Report Summary:

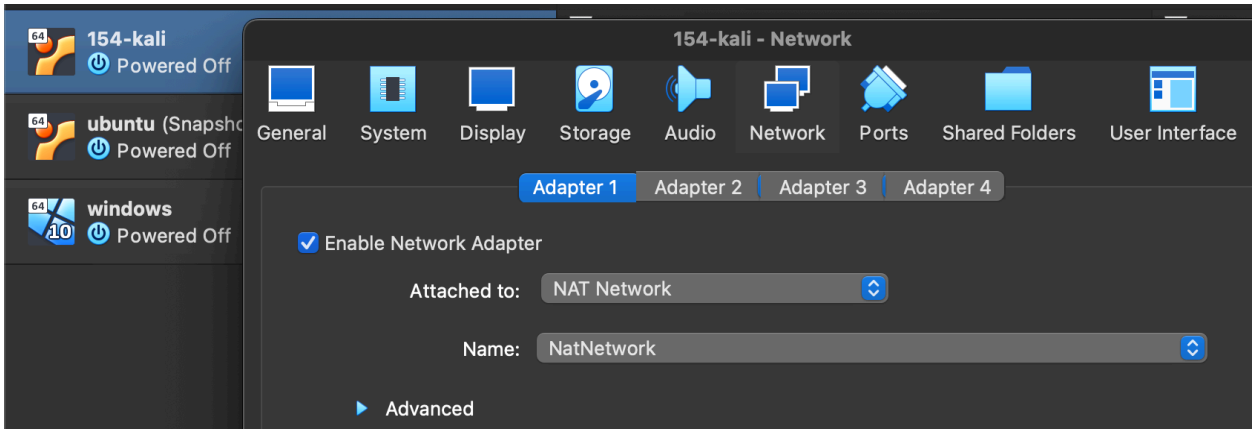
- It looks like the opposition is getting craftier with ransomware attacks. It is more than just a nuisance, as it is a serious threat to our data and the trust that our clients place in us.
- We're not just fighting off cybercriminals; there are entire countries out there trying to sneak a peek at our data for malicious reasons. This is especially true for companies in tech, healthcare, and government sectors, which are more at risk.Our report points out a shift towards attacks on cloud services and stealing identities. For example, there has been a sharp decline in malware based attacks since 2018, meaning our old security measures won't cut it anymore. We need to step up our game in protecting our cloud data and making sure only the right people can access our systems.
- Political and social issues are fueling more hacktivism, leading to targeted attacks. It's a reminder that we could be caught in the crossfire, even if we're not the intended target.
- We could invest in top-notch endpoint and cloud security. We need to see everything that's happening and stop threats in their tracks, whether they're coming at our laptops or floating around in the cloud.

- We've got to make sure only the right people can get into our systems. This means beefing up our identity protection with things like multi-factor authentication and keeping an eye out for any suspicious access attempts.
- We should get our hands on some solid threat intelligence so we know what we're up against. And if (or when) something does go wrong, having a quick-response plan will help us bounce back faster.

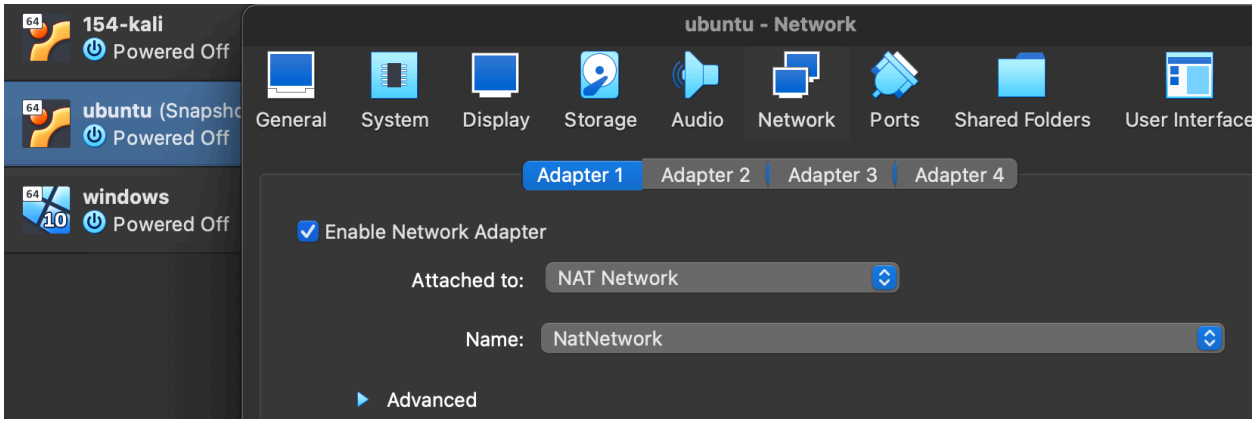
Task 2

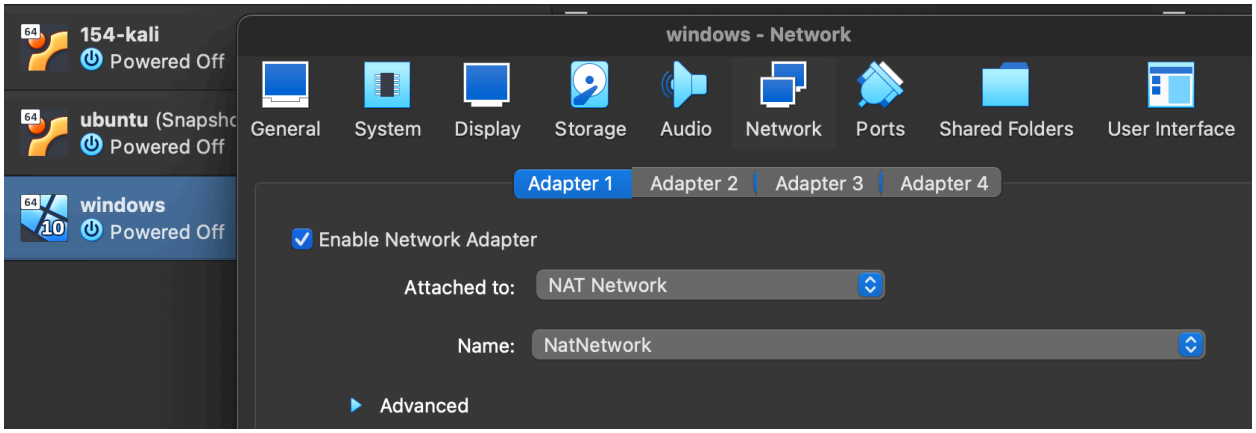
1) Created a new NAT Network in VirtualBox called "NatNetwork" with a subnet of 10.0.2.0/24. Then, I set each of my VMs (Windows, Ubuntu, and Kali) to use this NAT Network for their internet connection.





Kevin Cendana
Spring 2024
CSC 154





2) I visited the Tenable website on my host machine and registered for a free Nessus Essentials activation code using my CSUS email.

Kevin Cendana
Spring 2024
CSC 154

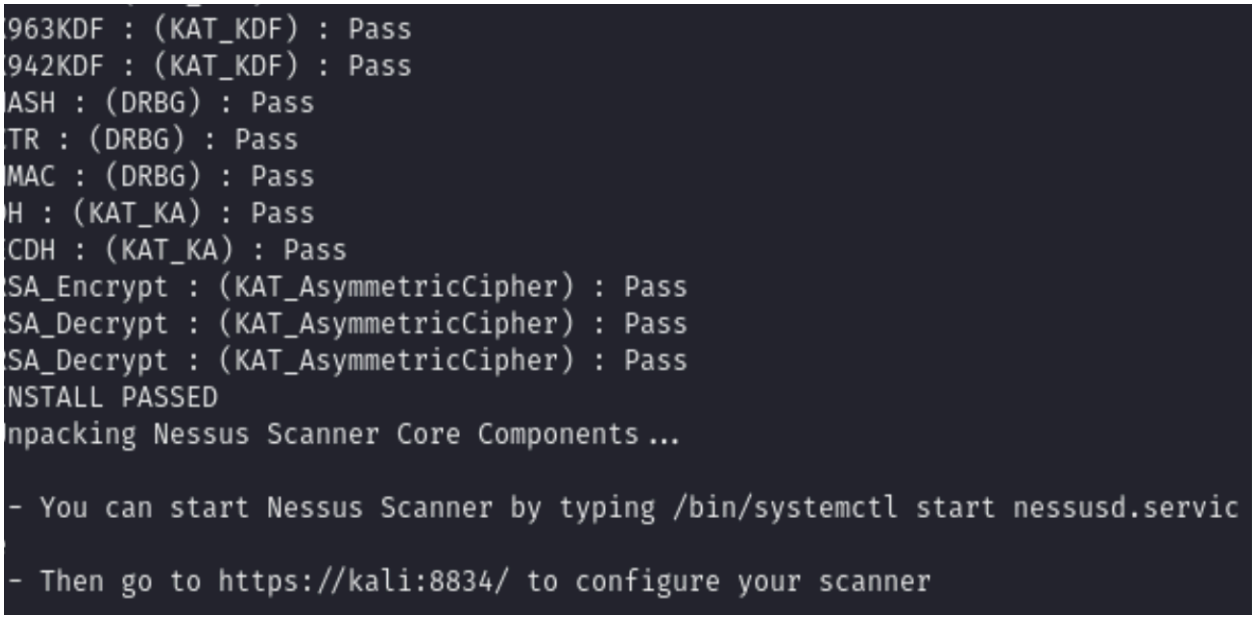
Welcome To Nessus Essentials

Welcome to Nessus Essentials and congratulations on taking action to secure your network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your network protected.

If you're looking for more advanced capabilities, such as live results and configuration checks – as well as the ability to scan unlimited IPs, check out Nessus Professional. To learn more view the Nessus Professional datasheet.

Activating Your Nessus Essentials License

Your activation code for Nessus Essentials is:

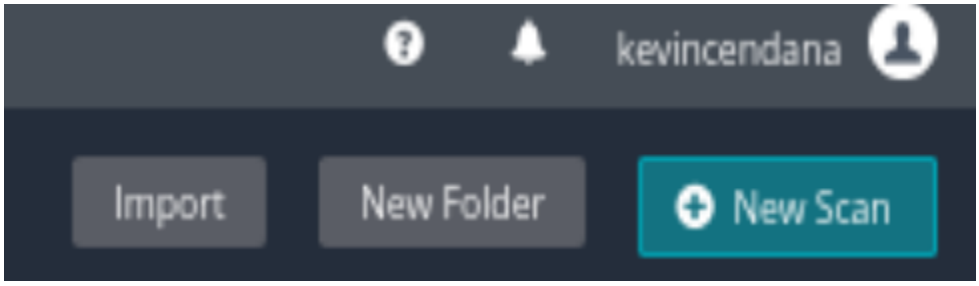


3) On my Kali VM, I downloaded the Nessus package for Debian and installed it using the terminal. After the installation, I started the

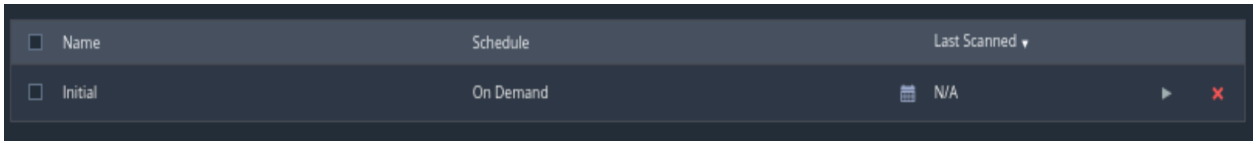
Nessus service and opened the Nessus console in my browser.

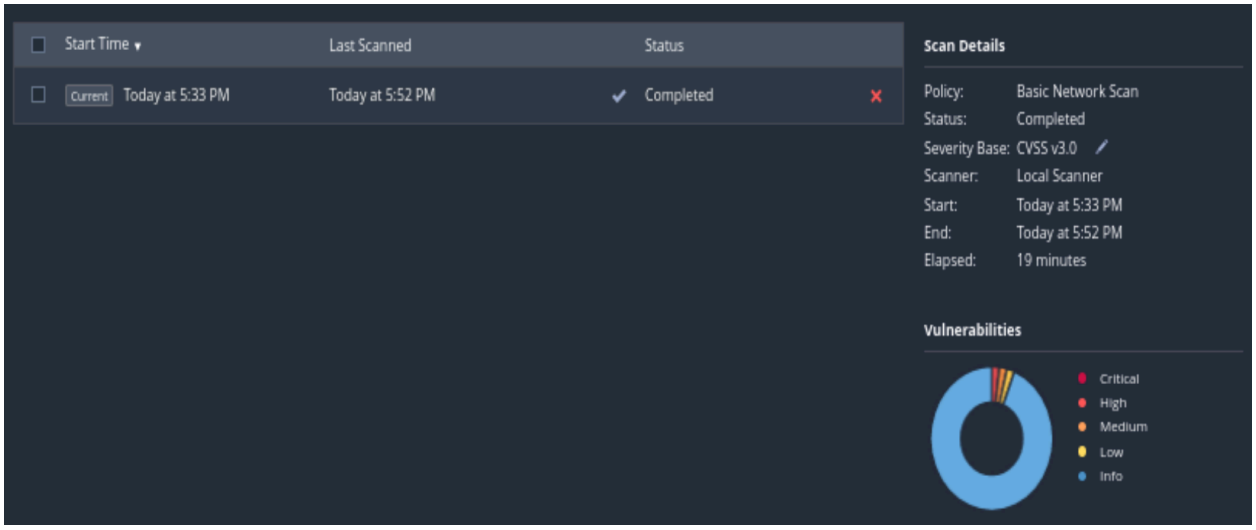
4) I registered Nessus Essentials with the activation code I received earlier and set up my username and password. Nessus then started

downloading plugins and data. This took like, about 2 hours?



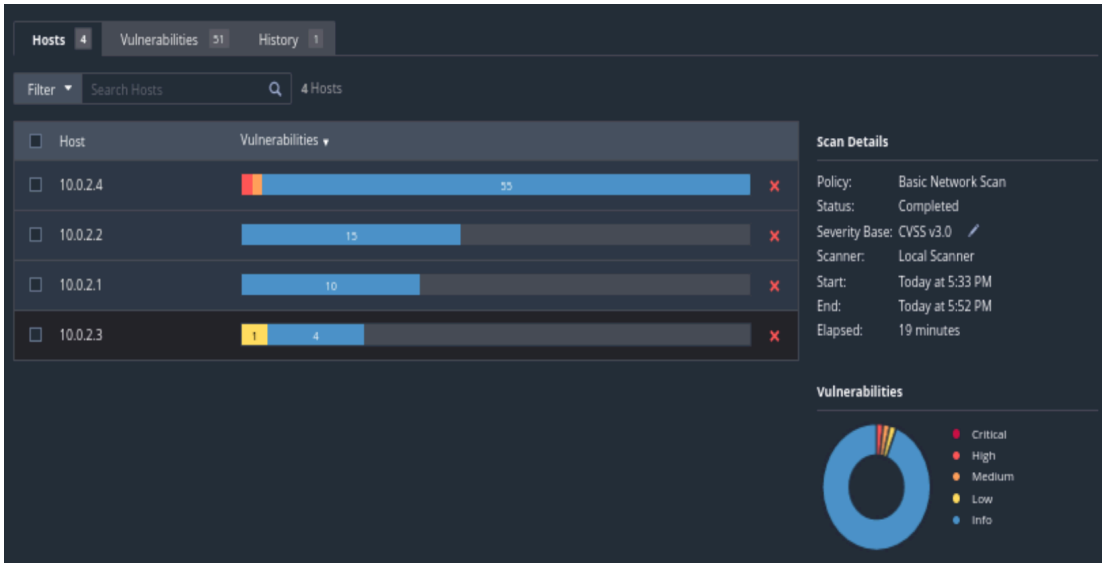
5) After logging into Nessus, I created a new scan named "Initial" targeting the 10.0.2.0/24 network. I launched the scan and waited about ~40 minutes for it to complete (slow laptop / network maybe?)



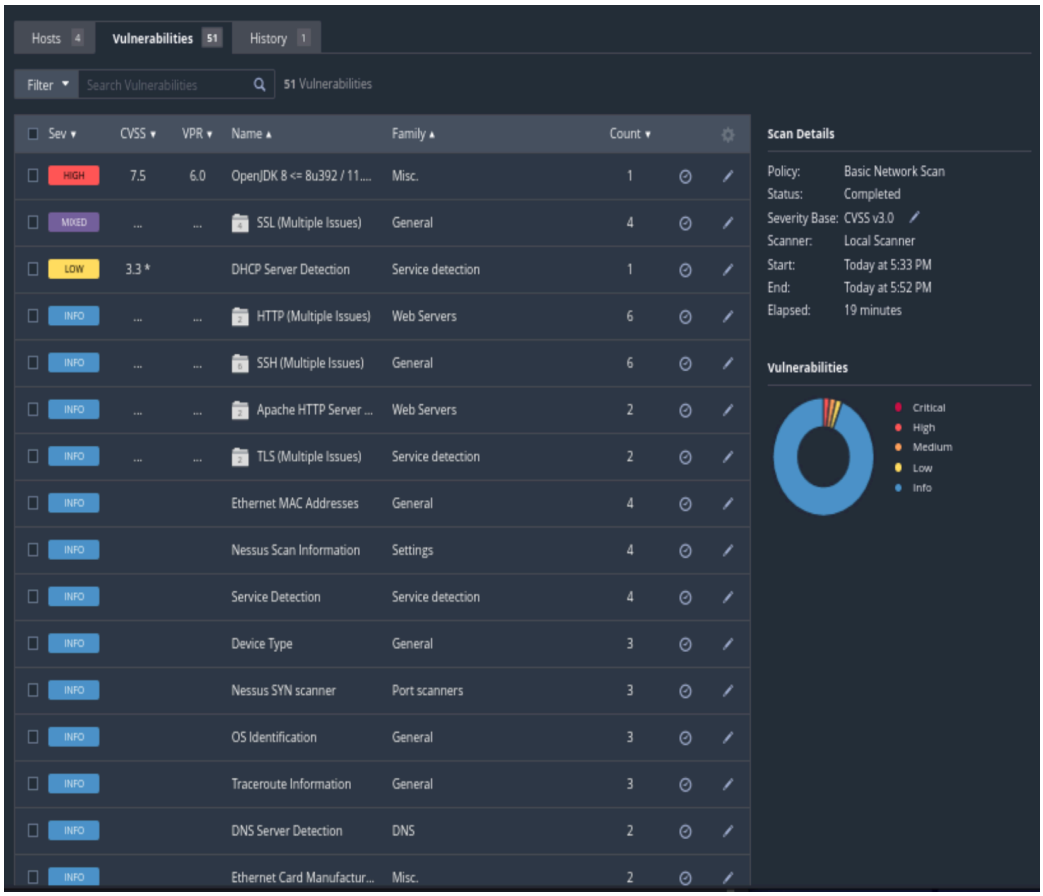


6) Once the scan finished, I explored the Hosts and Vulnerabilities tabs to see what was found. I focused on a few vulnerabilities listed by severity and looked into the details of one to understand it better. I saw one warning of “high” severity, which seemed to be caused by

having an outdated Java JDK file, which posed a security issue.



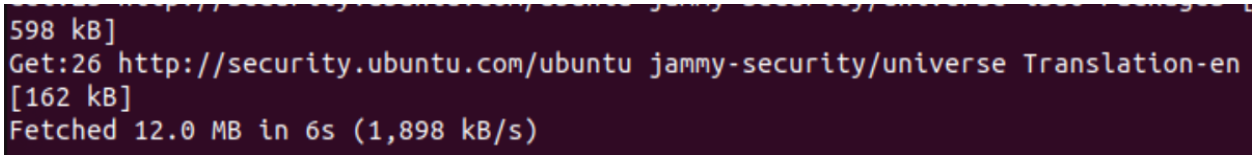
Kevin Cendana
Spring 2024
CSC 154

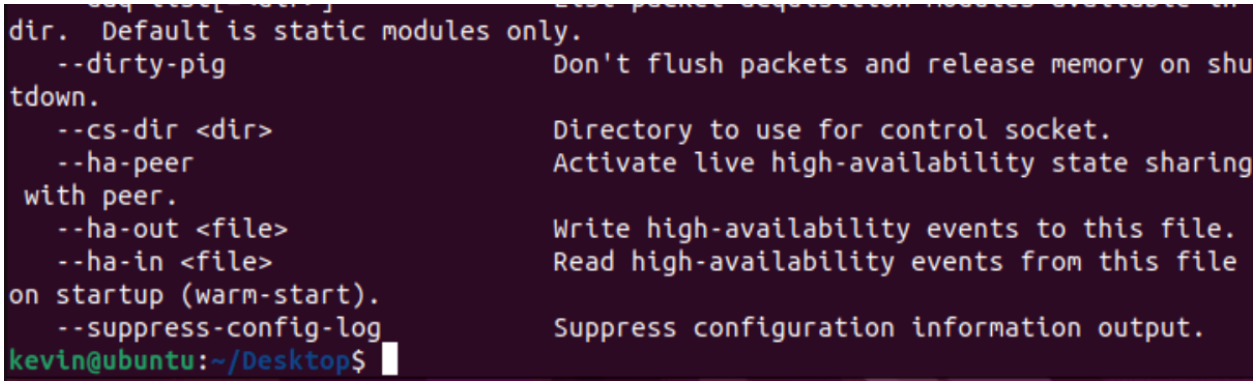


Kevin Cendana
Spring 2024
CSC 154

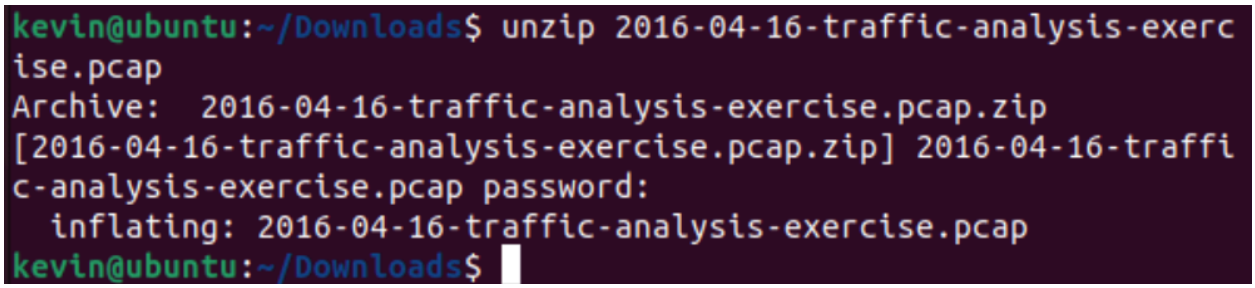
Task 3

1) I installed Snort on my Ubuntu VM, which was set up with a Bridge Adapter network mode. After the installation, I confirmed Snort was installed correctly by running its help command.





2) I tried to download the zipped PCAP file from malware-traffic-analysis.net to my Ubuntu VM but I ended up going to Canvas instead. I unzipped it using the password "infected".



3) I created a custom Snort rule to detect access to a known malicious webserver. I added this rule to the local.rules file, aiming to catch any Paypal phishing attempts. I got some errors at first and had to repeat

this step and edit the rules with nano, but I got it working!

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

4) I ran Snort against the unzipped PCAP file and saw that my custom Paypal phishing rule was triggered. This confirmed that the malicious traffic was successfully detected with our rule.

```
04/15-15:55:06.015751  [**] [1:1841:5] WEB-CLIENT Javascript URL host spoofing a
ttempt [**] [Classification: Attempted User Privilege 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 attempt [**] [Classi
fication: Misc activity] [Priority: 3] {TCP} 91.194.91.203:80 -> 172.16.155.149:
49266
04/15-15:59:18.292918  [**] [1:21637:1] Paypal phishing 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 attempt [**] [Classi
fication: Misc activity] [Priority: 3] {TCP} 172.217.3.46:80 -> 172.16.155.149:4
9367
04/15-16:00:49.508881  [**] [1:1852:3] WEB-MISC robots.txt access [**] [Classifi
cation: access to a potentially vulnerable web application] [Priority: 2] {TCP}
172.16.155.149:49386 -> 172.217.2.46:80
04/15-16:00:49.749435  [**] [1:2925:3] INFO web bug 0x0 gif attempt [**] [Classi
fication: Misc activity] [Priority: 3] {TCP} 172.217.2.46:80 -> 172.16.155.149:4
9386
04/15-16:01:10.826146  [**] [1:2925:3] INFO web bug 0x0 gif attempt [**] [Classi
fication: Misc activity] [Priority: 3] {TCP} 72.167.2.1:80 -> 172.16.155.149:493
95
04/15-16:01:10.888641  [**] [1:2925:3] INFO web bug 0x0 gif attempt [**] [Classi
fication: Misc activity] [Priority: 3] {TCP} 172.217.3.46:80 -> 172.16.155.149:4
9367
kevin@ubuntu:~/Downloads$
```

Task 4

1) I installed python3-pip on my Ubuntu VM and then used it to install the honeypots module. I checked my IP address, noting it down for later use from my Kali VM.

Kevin Cendana
Spring 2024
CSC 154

```
  Consider adding this directory to PATH or, if you prefer to suppress this warn
ing, use --no-warn-script-location.
Successfully installed Automat-22.10.0 Jinja2-3.1.3 MarkupSafe-2.1.5 PySocks-1.7
.1 Werkzeug-3.0.1 attrs-23.2.0 blinker-1.7.0 cffi-1.16.0 charset-normalizer-3.3.
2 click-8.1.7 constantly-23.10.4 cryptography-42.0.5 dnspython-2.6.1 flask-3.0.2
 honeypots-0.65 hyperlink-21.0.0 impacket-0.9.24 incremental-22.10.0 itsdangerou
s-2.1.2 ldap3-2.9.1 ldapdomaindump-0.9.4 paramiko-3.1.0 psutil-5.9.0 psycopg2-bi
nary-2.9.3 pyOpenSSL-24.1.0 pyasn1-0.5.1 pyasn1-modules-0.3.0 pycparser-2.21 pyc
ryptodome-3.19.0 pycryptodomex-3.20.0 requests-2.28.2 scapy-2.4.5 service-identi
ty-21.1.0 twisted-21.7.0 typing-extensions-4.10.0 zope.interface-6.2
```

```
kevin@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:c3:66:fc brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 328sec preferred_lft 328sec
    inet6 fe80::d970:dce9:be36:adb1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
kevin@ubuntu:~$
```

2) I set up a MySQL honeypot on port 3306 using the honeypots module. Everything started up correctly, and the terminal was ready to log any incoming connections.

```
kevin@ubuntu:~$ python3 -m honeypots --setup mysql:3306
[INFO] For updates, check https://github.com/qeeqbox/honeypots
[WARNING] Using system or well-known ports requires higher privileges (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", "password": "te
st", "server": "mysql_server", "src_ip": "0.0.0.0", "src_port": "3306", "status"
: "success", "timestamp": "2024-03-18T02:36:40.928701", "username": "test"}
[INFO] servers mysql running...
[INFO] Everything looks good!
```

3) From my Kali VM, I attempted to connect to the MySQL honeypot on my Ubuntu VM using the mysql client. When I checked back on my Ubuntu VM, I saw the connection attempt logged, indicating the honeypot was working as expected.

Kevin Cendana
Spring 2024
CSC 154

```
┌──(kevin㉿kali)-[~]
└─$ mysql -h 10.0.2.15 -u test -ptest
ERROR 1040 (08004): Too many connections
```

```
[INFO] Everything looks good!
{"action": "connection", "dest_ip": "0.0.0.0", "dest_port": "3306", "server": "m
ysql_server", "src_ip": "10.0.2.4", "src_port": "51566", "timestamp": "2024-03-1
8T02:58:39.534591"}
{"action": "login", "dest_ip": "0.0.0.0", "dest_port": "3306", "password": "test
", "server": "mysql_server", "src_ip": "10.0.2.4", "src_port": "51566", "status"
: "success", "timestamp": "2024-03-18T02:58:39.539785", "username": "test"}
```