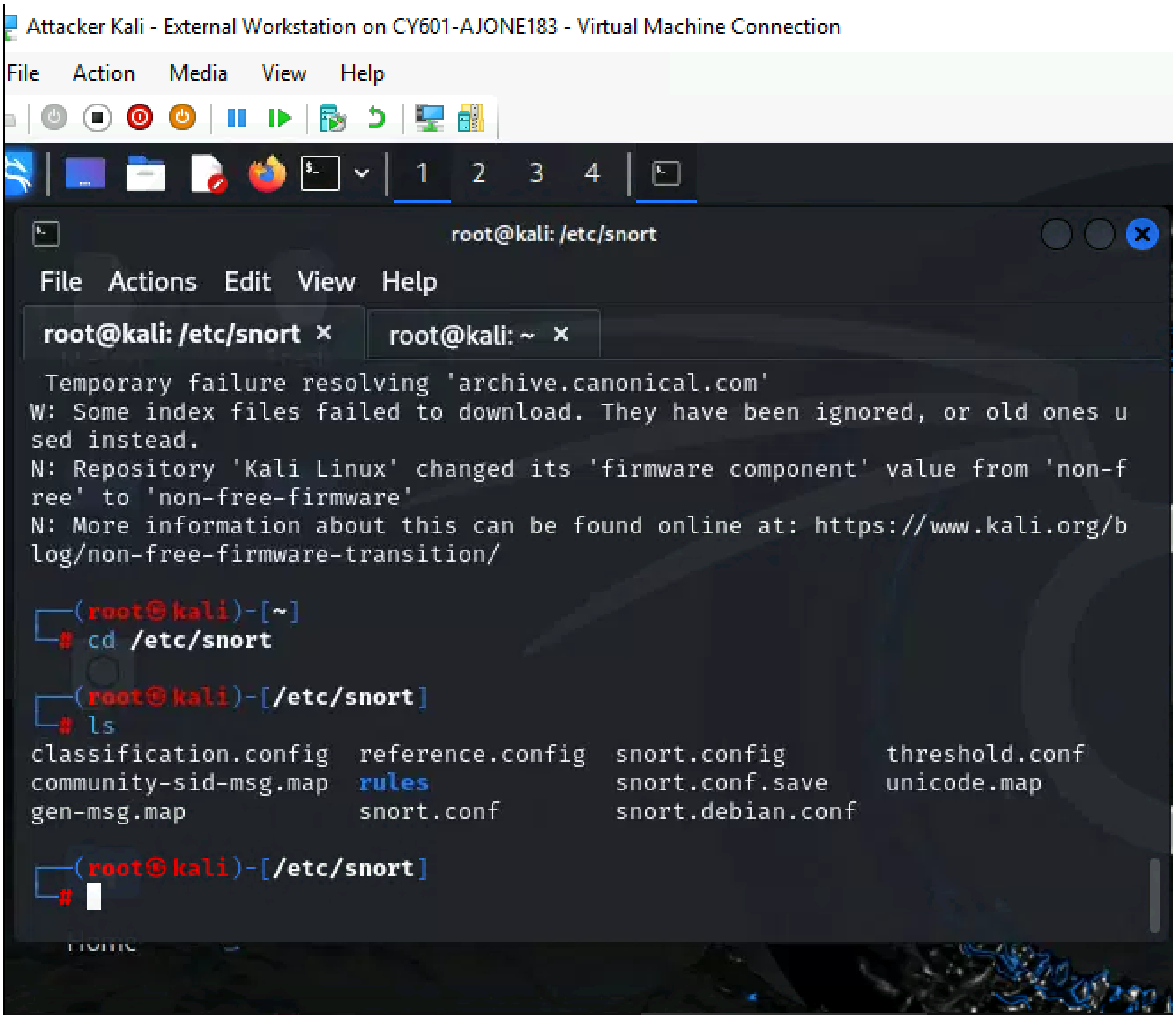
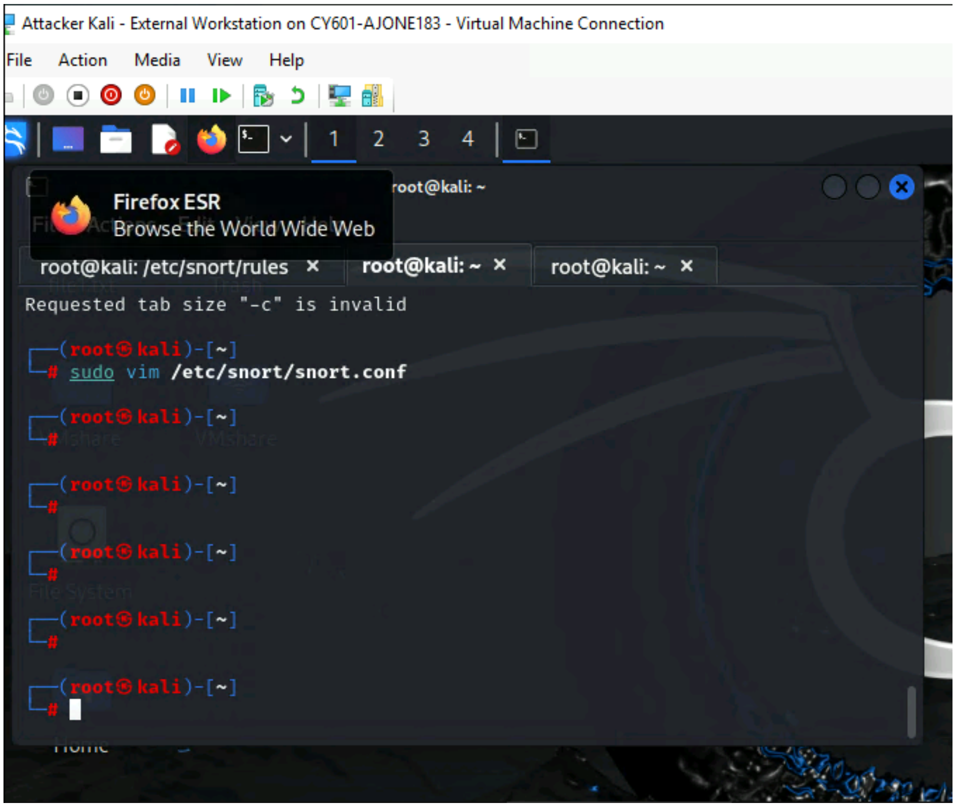
Task 1:

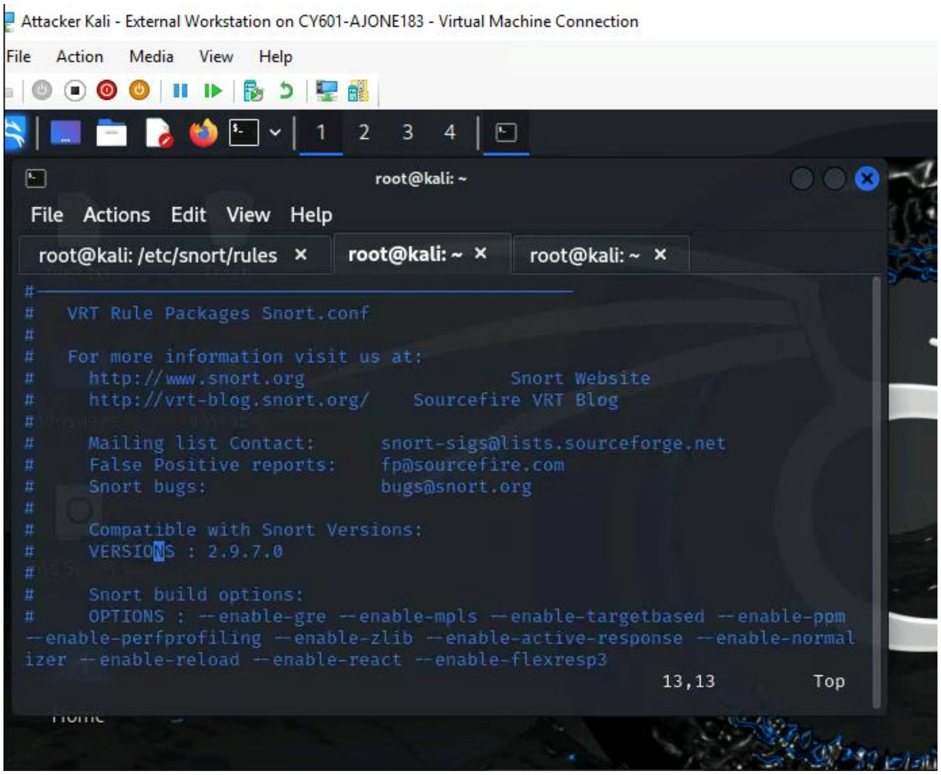

Attacker Kali - External Workstation on CY601-AJONE183 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
root@kali: /etc/snort
File Actions Edit View Help
root@kali: /etc/snort
root@kali: ~

```
 Temporary failure resolving 'archive.canonical.com'
W: Some index files failed to download. They have been ignored, or old ones u
sed instead.
N: Repository 'Kali Linux' changed its 'firmware component' value from 'non-f
ree' to 'non-free-firmware'
N: More information about this can be found online at: https://www.kali.org/b
log/non-free-firmware-transition/

┌──(root㉿kali)-[~]
└─# cd /etc/snort

┌──(root㉿kali)-[/etc/snort]
└─# ls
classification.config  reference.config  snort.config       threshold.conf
community-sid-msg.map  rules             snort.conf.save    unicode.map
gen-msg.map            snort.conf        snort.debian.conf

┌──(root㉿kali)-[/etc/snort]
└─# 
```

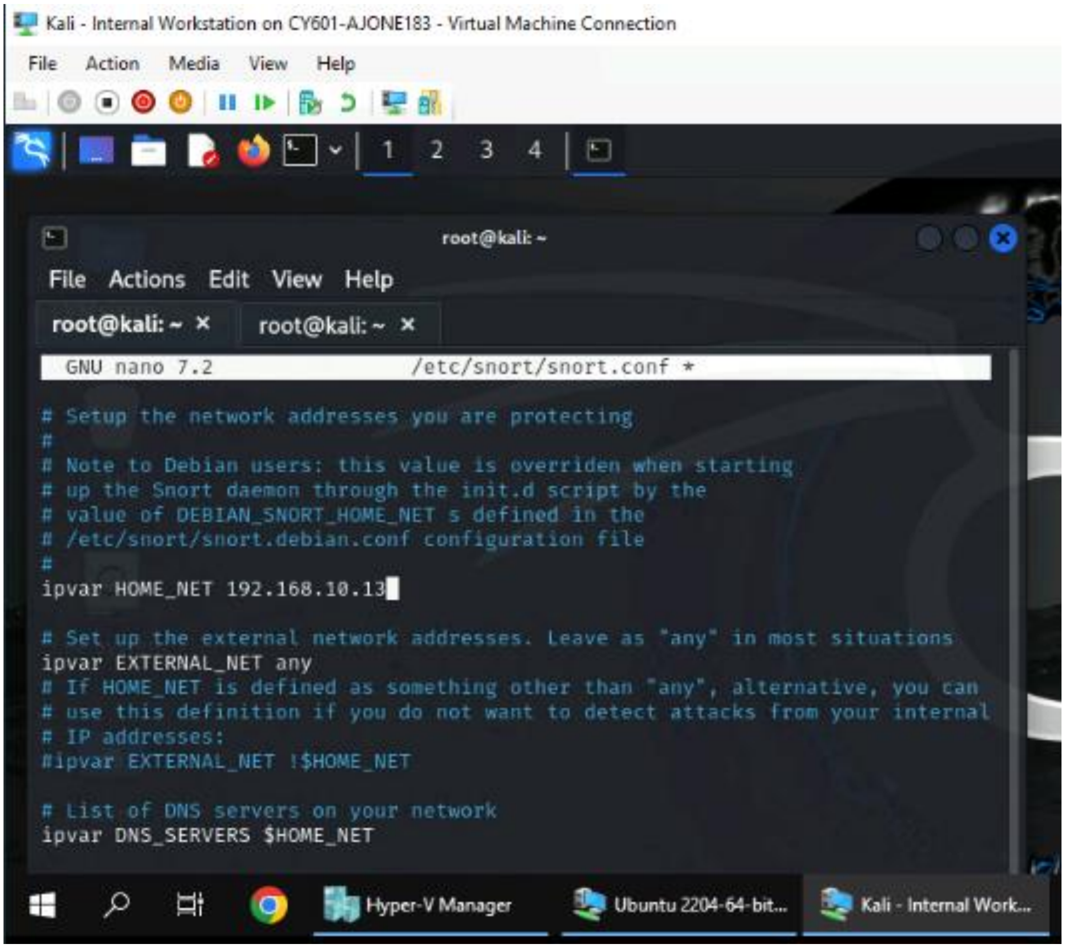
The command cd /etc/snort is used to move into the folder where Snort's settings are stored. To work with Snort's configuration files, I used the command cd /etc/snort. This command allowed me to access the folder where all the important files for Snort are kept. Inside this folder, I could find and make changes to the settings that control how Snort works. After entering the Snort folder, I used the command ls to list all the files inside. This command showed me the names of the files, including important ones like snort.conf, which contains the main settings for Snort.


Attacker Kali - External Workstation on CY601-AJONE183 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
root@kali: ~
Firefox ESR
Browse the World Wide Web
root@kali: /etc/snort/rules
root@kali: ~
root@kali: ~

```
Requested tab size "-c" is invalid

┌──(root㉿kali)-[~]
└─# sudo vim /etc/snort/snort.conf

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# 
```

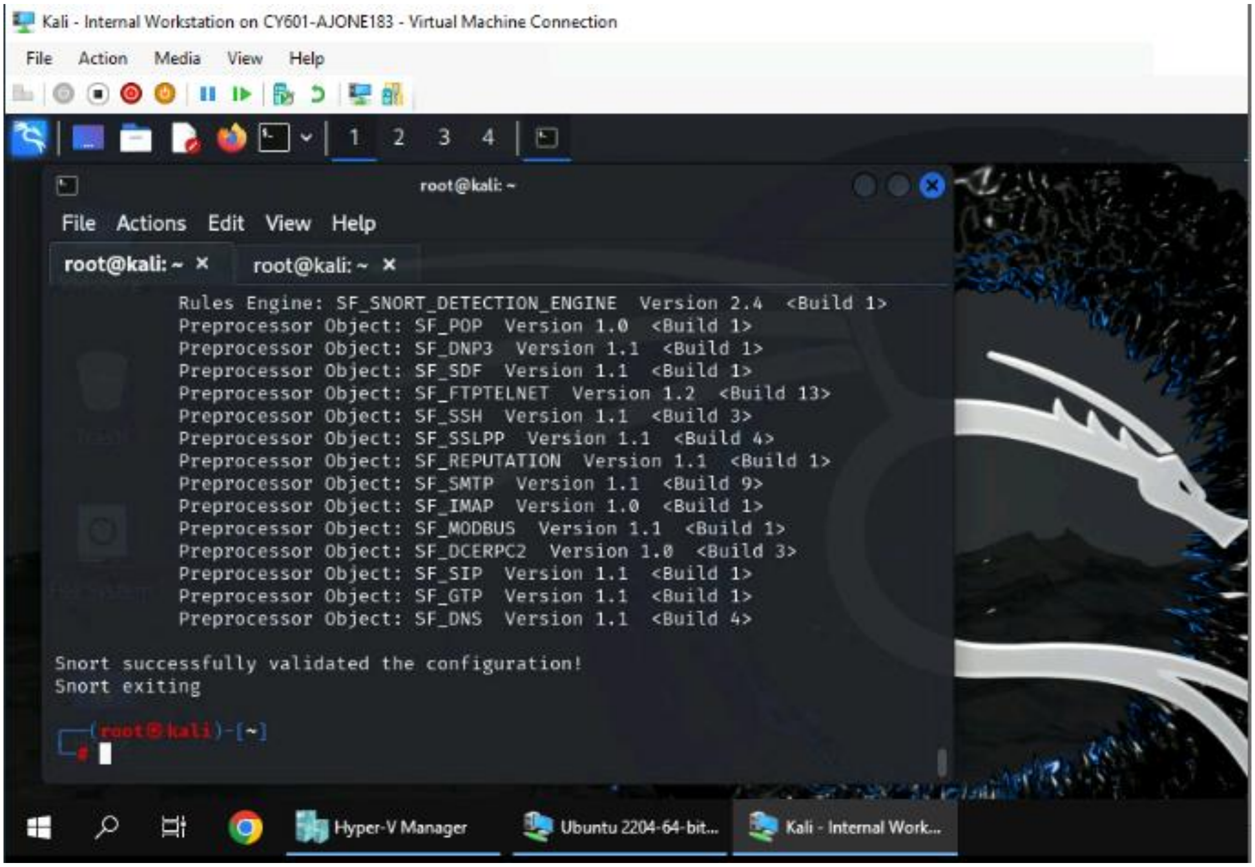

Attacker Kali - External Workstation on CY601-AJONE183 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
root@kali: ~
File Actions Edit View Help
root@kali: /etc/snort/rules
root@kali: ~
root@kali: ~

```
#--------------------------------------------------
#   VRT Rule Packages Snort.conf
#
#   For more information visit us at:
#     http://www.snort.org                   Snort Website
#     http://vrt-blog.snort.org/    Sourcefire VRT Blog
#
#     Mailing list Contact:      snort-sigs@lists.sourceforge.net
#     False Positive reports:    fp@sourcefire.com
#     Snort bugs:                bugs@snort.org
#
#     Compatible with Snort Versions:
#     VERSIONS : 2.9.7.0
#
#     Snort build options:
#     OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm
--enable-perfprofiling --enable-zlib --enable-active-response --enable-normal
izer --enable-reload --enable-react --enable-flexresp3
                                                          13,13         Top
```


Kali - Internal Workstation on CY601-AJONE183 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
root@kali: ~
File Actions Edit View Help
root@kali: ~ ×
root@kali: ~ ×
Hyper-V Manager
Ubuntu 2204-64-bit...
Kali - Internal Work...

```
 GNU nano 7.2                 /etc/snort/snort.conf *

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.10.13

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
```

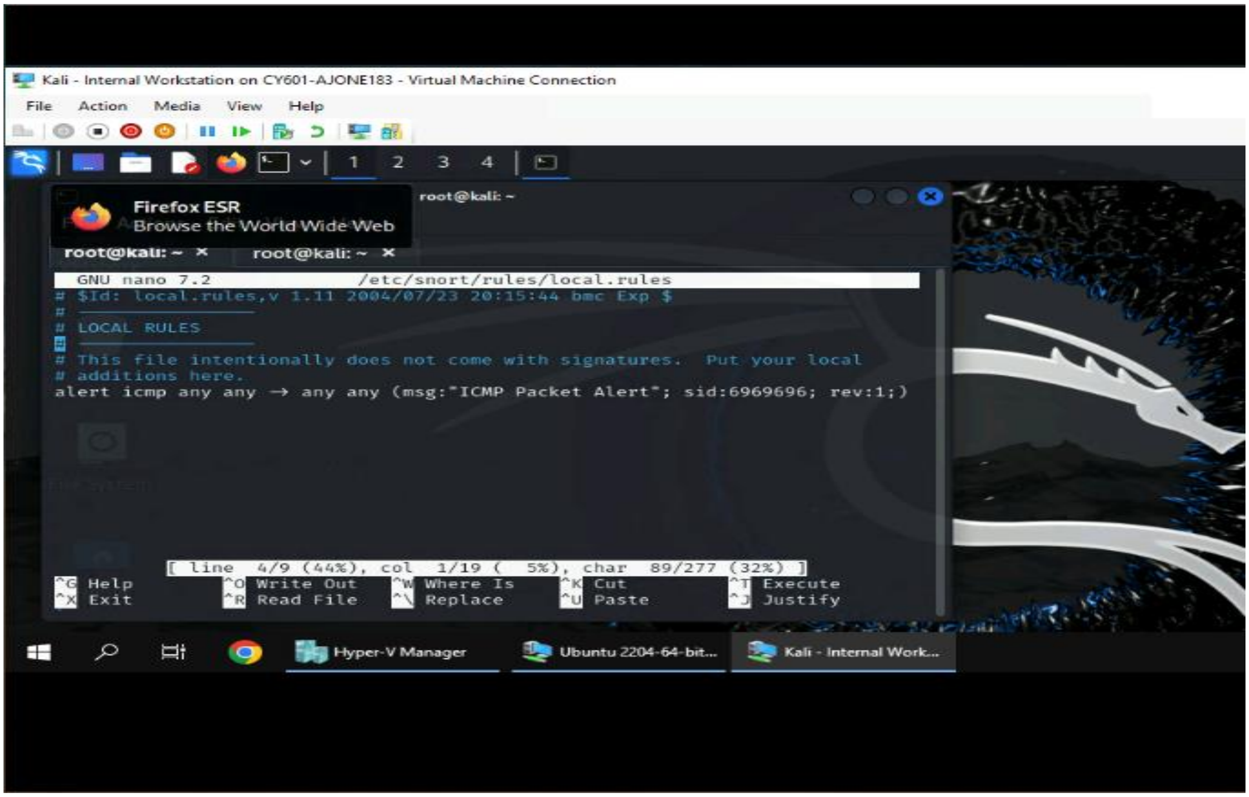
To edit the Snort configuration file, I used the command sudo vim /etc/snort/snort.conf. This opened the file with the necessary permissions since sudo gives root access. I also continued to run into the error of not connecting to the snort due to being on external kali. My next steps and updates and using the correct VM, thanks to cloudcomputing@odu.edu.


Kali - Internal Workstation on CY601-AJONE183 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
root@kali: ~
File Actions Edit View Help
root@kali: ~ ×
root@kali: ~ ×
Hyper-V Manager
Ubuntu 2204-64-bit...
Kali - Internal Work...

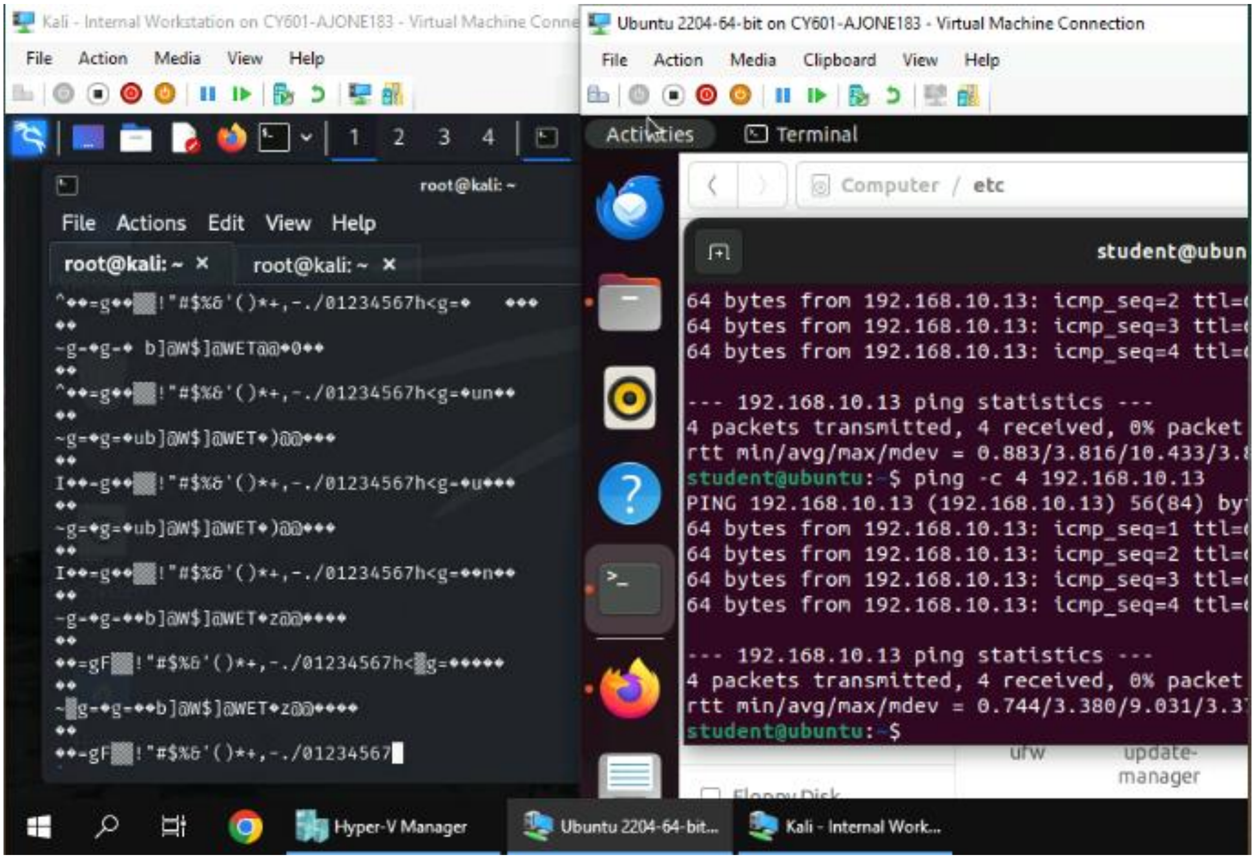
```
          Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
          Preprocessor Object: SF_POP  Version 1.0  <Build 1>
          Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
          Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
          Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
          Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
          Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
          Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
          Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
          Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
          Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
          Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
          Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
          Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
          Preprocessor Object: SF_DNS  Version 1.1  <Build 4>

Snort successfully validated the configuration!
Snort exiting

┌──(root㉿kali)-[~]
└─# 
```

Snort is successfully configured.

Task 2:


Kali - Internal Workstation on CY601-AJONE183 - Virtual Machine Connection
File Action Media View Help
Firefox ESR
Browse the World Wide Web
root@kali: ~
root@kali: ~
root@kali: ~
Hyper-V Manager
Ubuntu 2204-64-bit...
Kali - Internal Work...

```
  GNU nano 7.2                /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp any any → any any (msg:"ICMP Packet Alert"; sid:6969696; rev:1;)




              [ line  4/9 (44%), col  1/19 (  5%), char  89/277 (32%) ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```


Kali - Internal Workstation on CY601-AJONE183 - Virtual Machine Conne
File Action Media View Help
root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali: ~
Ubuntu 2204-64-bit on CY601-AJONE183 - Virtual Machine Connection
File Action Media Clipboard View Help
Activities
Terminal
Computer / etc
student@ubun
ufw
update-manager
Floppy Disk
Hyper-V Manager
Ubuntu 2204-64-bit...
Kali - Internal Work...

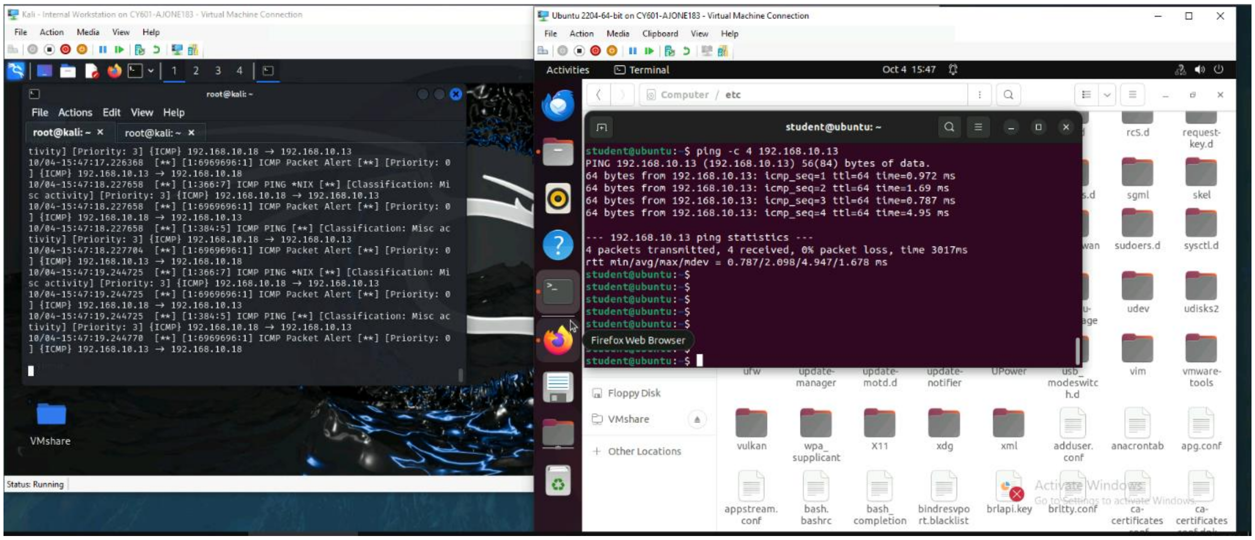
```
^••=g••▒!"#$%&'()*+,-./01234567h<g=•   •••
••
~g-•g-• b]@W$]@WET@@•0••
••
^••=g••▒!"#$%&'()*+,-./01234567h<g=•un••
••
~g=•g=•ub]@W$]@WET•)@@•••
••
I••-g••▒!"#$%&'()*+,-./01234567h<g-•u•••
••
~g=•g=•ub]@W$]@WET•)@@•••
••
I••-g••▒!"#$%&'()*+,-./01234567h<g=••n••
••
-g-•g-••b]@W$]@WET•z@@••••
••
••=gF▒!"#$%&'()*+,-./01234567h<▒g=•••••
••
~▒g-•g-••b]@W$]@WET•z@@••••
••
••-gF▒!"#$%&'()*+,-./01234567
```

```
64 bytes from 192.168.10.13: icmp_seq=2 ttl=
64 bytes from 192.168.10.13: icmp_seq=3 ttl=
64 bytes from 192.168.10.13: icmp_seq=4 ttl=

--- 192.168.10.13 ping statistics ---
4 packets transmitted, 4 received, 0% packet
rtt min/avg/max/mdev = 0.883/3.816/10.433/3.
student@ubuntu:~$ ping -c 4 192.168.10.13
PING 192.168.10.13 (192.168.10.13) 56(84) by
64 bytes from 192.168.10.13: icmp_seq=1 ttl=
64 bytes from 192.168.10.13: icmp_seq=2 ttl=
64 bytes from 192.168.10.13: icmp_seq=3 ttl=
64 bytes from 192.168.10.13: icmp_seq=4 ttl=

--- 192.168.10.13 ping statistics ---
4 packets transmitted, 4 received, 0% packet
rtt min/avg/max/mdev = 0.744/3.380/9.031/3.3
student@ubuntu:~$
```

To access the local Snort rules file, I used the following command sudo nano /etc/snort/rules/local.rules. This command opens the local.rules file using the nano text editor with superuser privileges, allowing me to modify the rule set. Alert: This specifies the action that Snort should take when it matches this rule. In this case, it will generate an alert when the rule conditions are met. ICMP: This indicates that the rule applies specifically to ICMP (Internet Control Message Protocol) packets. ICMP is used for error messages and operational information in the network layer, such as the ping command. Any any -> any any: The first any any refers to the source of the packet. It means that the rule will match ICMP packets from any source IP address and any source port. The arrow -> indicates the direction of the traffic being monitored, meaning from the source to the destination. (msg:"ICMP Packet Alert"; sid:6969696; rev:1;): This part specifies additional options for the rule: msg:"ICMP Packet Alert": This is the message that will be logged when the rule triggers, allowing administrators to understand the context of the alert. Sid:6969696: This is the Snort ID (SID) for the rule, which must be unique among all rules. It helps identify the rule in logs and alerts. rev:1: This indicates the revision number of the rule. It can be incremented when changes are made to the rule.

To test the newly added rule, I generated ICMP traffic by pinging the IP address of my Snort instance from an Ubuntu machine. I executed the following command: ping -c 4 192.168.10.13

Task 3:



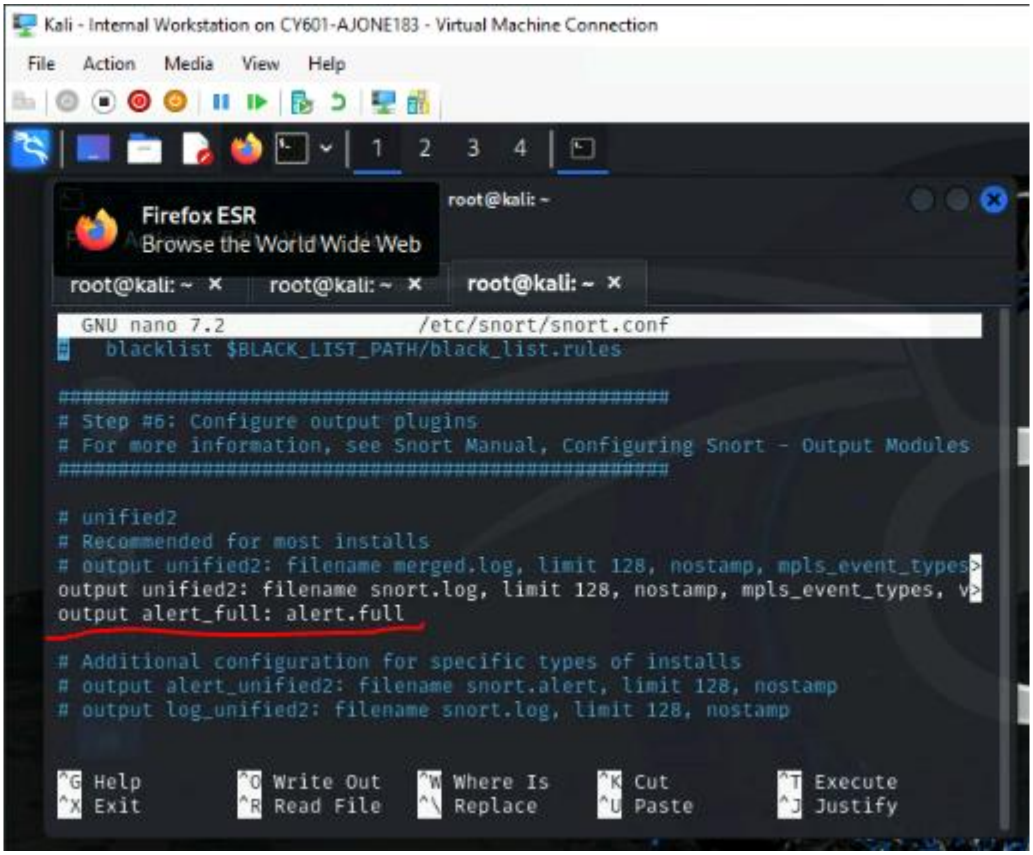
```
tivity] [Priority: 3] {ICMP} 192.168.10.18 → 192.168.10.13
10/04-15:47:17.226368  [**] [1:6969696:1] ICMP Packet Alert [**] [Priority: 0
] {ICMP} 192.168.10.13 → 192.168.10.18
10/04-15:47:18.227658  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Mi
sc activity] [Priority: 3] {ICMP} 192.168.10.18 → 192.168.10.13
10/04-15:47:18.227658  [**] [1:6969696:1] ICMP Packet Alert [**] [Priority: 0
] {ICMP} 192.168.10.18 → 192.168.10.13
10/04-15:47:18.227658  [**] [1:384:5] ICMP PING [**] [Classification: Misc ac
tivity] [Priority: 3] {ICMP} 192.168.10.18 → 192.168.10.13
10/04-15:47:18.227704  [**] [1:6969696:1] ICMP Packet Alert [**] [Priority: 0
] {ICMP} 192.168.10.13 → 192.168.10.18
10/04-15:47:19.244725  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Mi
sc activity] [Priority: 3] {ICMP} 192.168.10.18 → 192.168.10.13
10/04-15:47:19.244725  [**] [1:6969696:1] ICMP Packet Alert [**] [Priority: 0
] {ICMP} 192.168.10.18 → 192.168.10.13
10/04-15:47:19.244725  [**] [1:384:5] ICMP PING [**] [Classification: Misc ac
tivity] [Priority: 3] {ICMP} 192.168.10.18 → 192.168.10.13
10/04-15:47:19.244770  [**] [1:6969696:1] ICMP Packet Alert [**] [Priority: 0
] {ICMP} 192.168.10.13 → 192.168.10.18
```

```
student@ubuntu:~$ ping -c 4 192.168.10.13
PING 192.168.10.13 (192.168.10.13) 56(84) bytes of data.
64 bytes from 192.168.10.13: icmp_seq=1 ttl=64 time=0.972 ms
64 bytes from 192.168.10.13: icmp_seq=2 ttl=64 time=1.69 ms
64 bytes from 192.168.10.13: icmp_seq=3 ttl=64 time=0.787 ms
64 bytes from 192.168.10.13: icmp_seq=4 ttl=64 time=4.95 ms

--- 192.168.10.13 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3017ms
rtt min/avg/max/mdev = 0.787/2.098/4.947/1.678 ms
student@ubuntu:~$
student@ubuntu:~$
student@ubuntu:~$
student@ubuntu:~$
student@ubuntu:~$
student@ubuntu:~$
```

Kali - Internal Workstation on CY601-AJONE183 - Virtual Machine Connection
Ubuntu 2204-64-bit on CY601-AJONE183 - Virtual Machine Connection
root@kali: ~
student@ubuntu: ~
Oct 4 15:47
Computer / etc
Firefox Web Browser
VMshare
Status: Running

I verified that Snort generated alerts for the UDP packets based on the rule I created. I checked the terminal running Snort for any alerts or messages indicating the detection of UDP traffic.

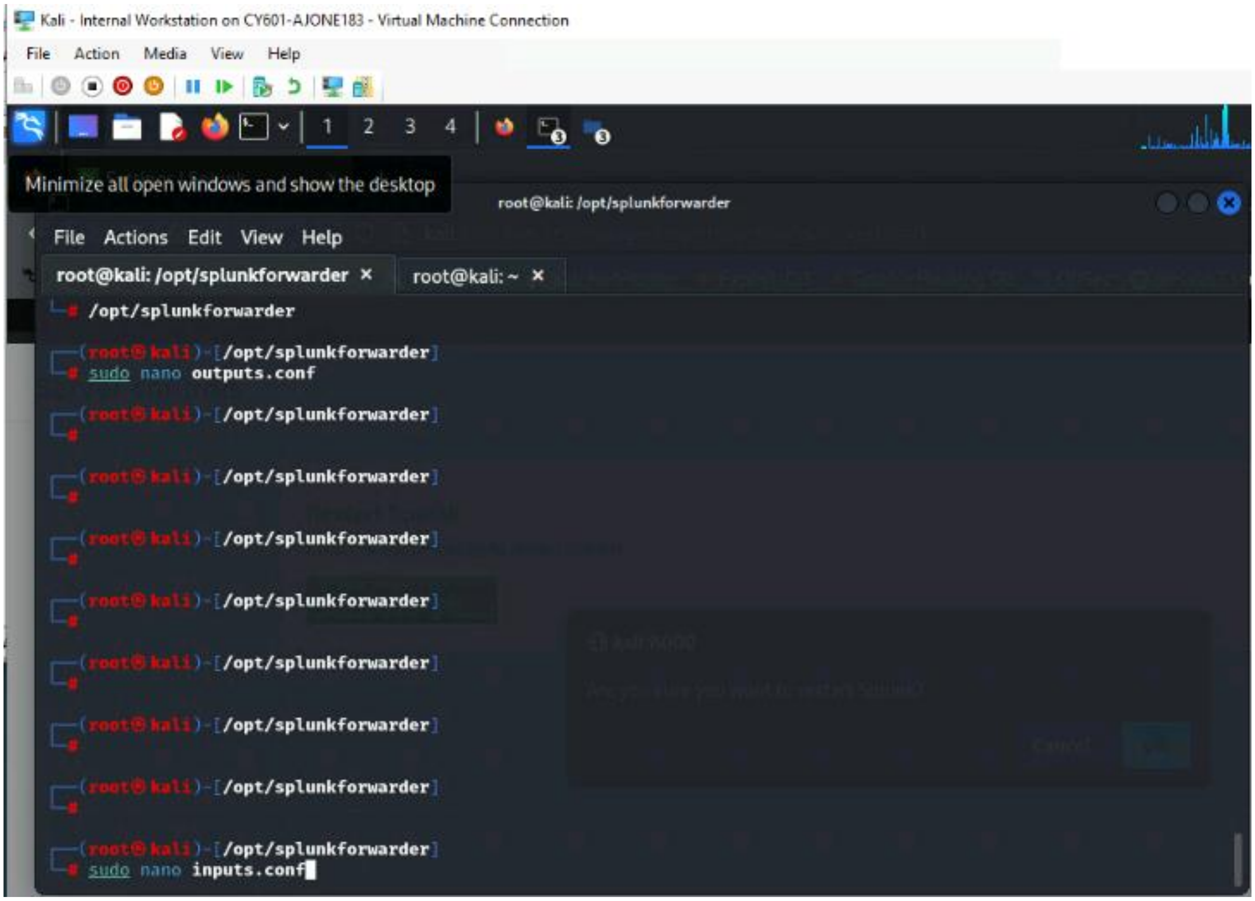
Task 4:



```
  GNU nano 7.2                  /etc/snort/snort.conf
#   blacklist $BLACK_LIST_PATH/black_list.rules

###################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
###################################################

# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types>
output unified2: filename snort.log, limit 128, nostamp, mpls_event_types, v>
output alert_full: alert.full

# Additional configuration for specific types of installs
# output alert_unified2: filename snort.alert, limit 128, nostamp
# output log_unified2: filename snort.log, limit 128, nostamp


^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```

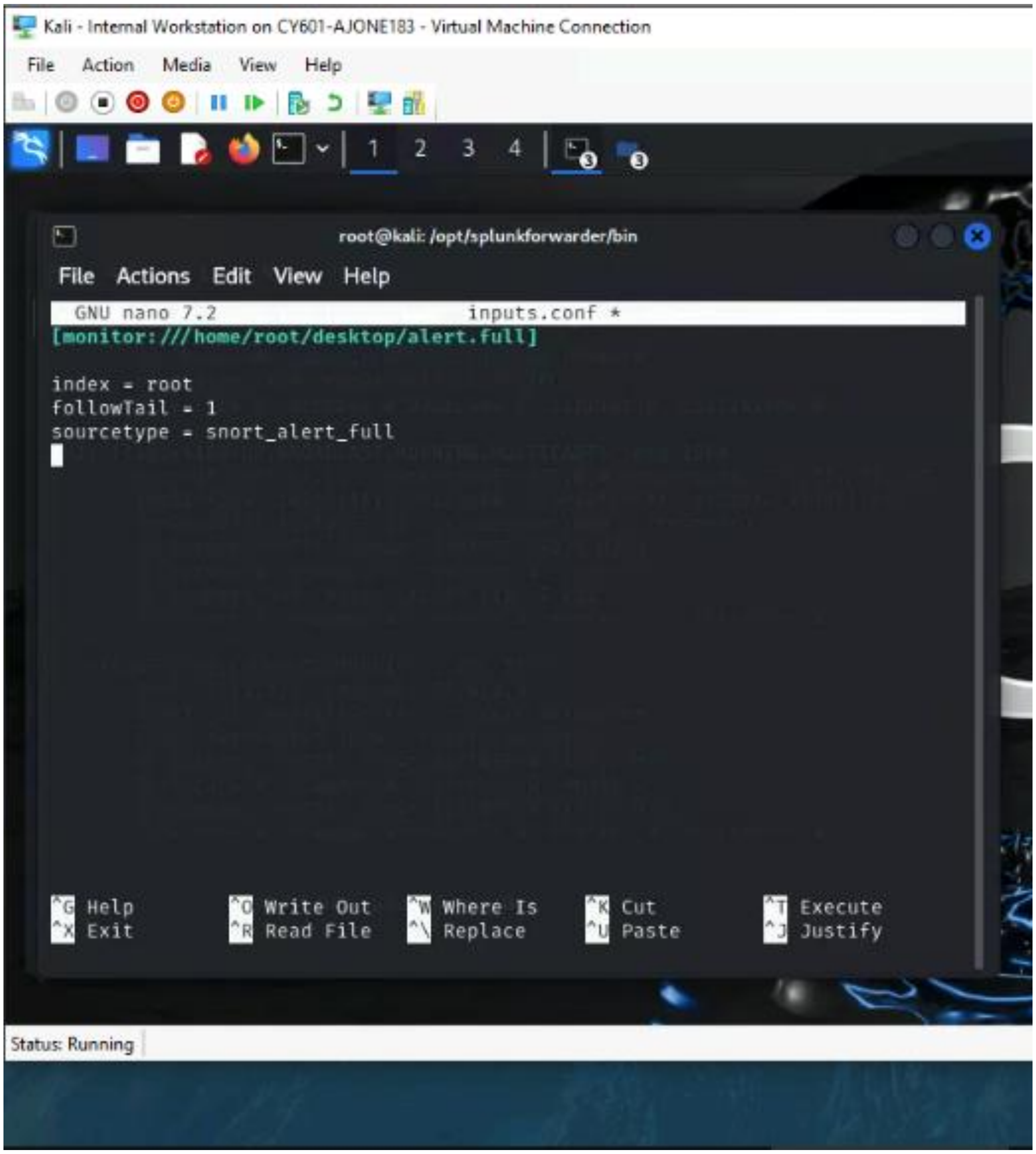
Kali - Internal Workstation on CY601-AJONE183 - Virtual Machine Connection
File
Action
Media
View
Help
Firefox ESR
Browse the World Wide Web
root@kali: ~

In your snort.conf file, add the following line to ensure Snort outputs full alerts to a file named alert.full: output alert_full: alert.full



Kali - Internal Workstation on CY601-AJONE183 - Virtual Machine Connection
File Action Media View Help
Minimize all open windows and show the desktop
root@kali: /opt/splunkforwarder
File Actions Edit View Help
root@kali: /opt/splunkforwarder
root@kali: ~

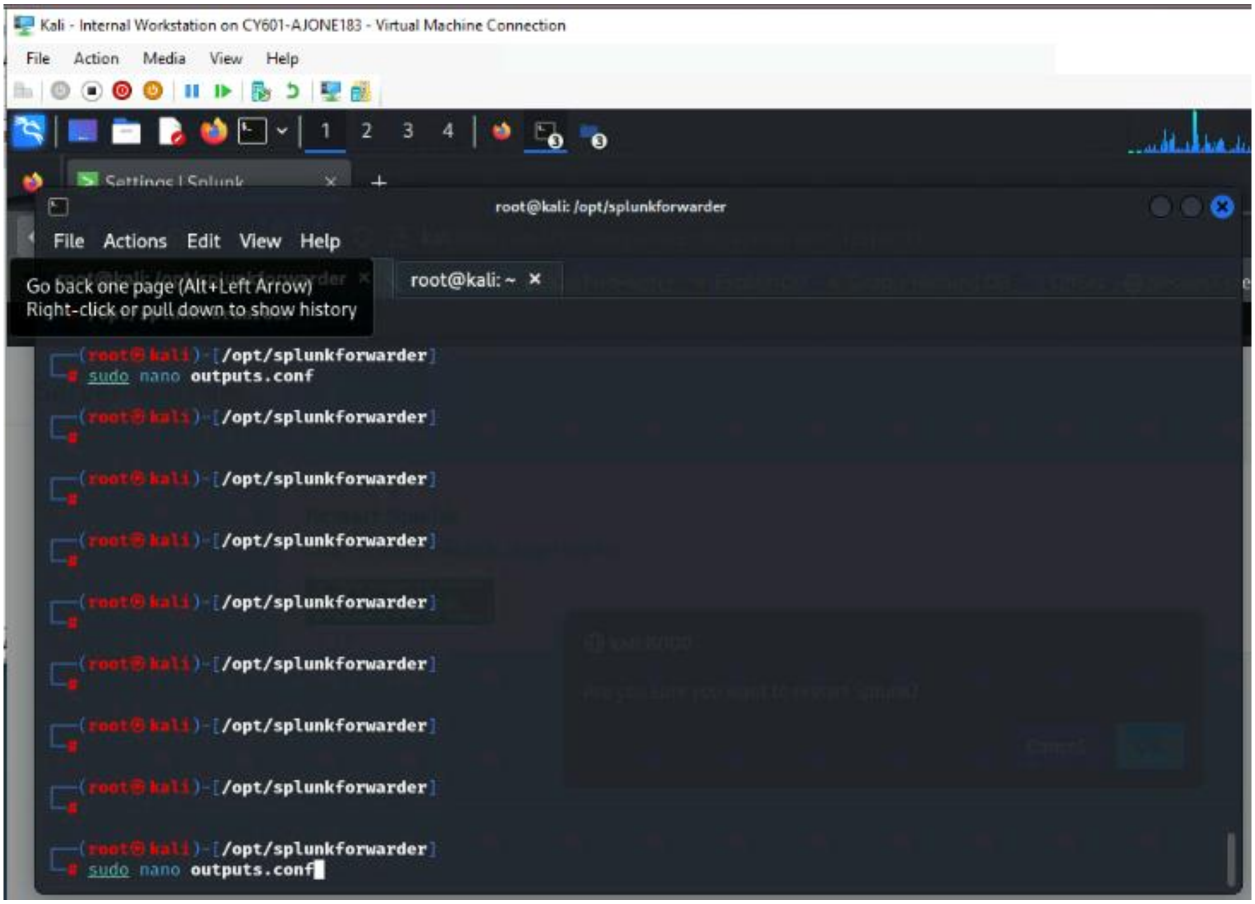
```
└─# /opt/splunkforwarder

┌──(root㉿kali)-[/opt/splunkforwarder]
└─# sudo nano outputs.conf

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─# sudo nano inputs.conf
```


Kali - Internal Workstation on CY601-AJONE183 - Virtual Machine Connection
File Action Media View Help
root@kali: /opt/splunkforwarder/bin
File Actions Edit View Help
Status: Running

```
  GNU nano 7.2                       inputs.conf *
[monitor:///home/root/desktop/alert.full]

index = root
followTail = 1
sourcetype = snort_alert_full
```

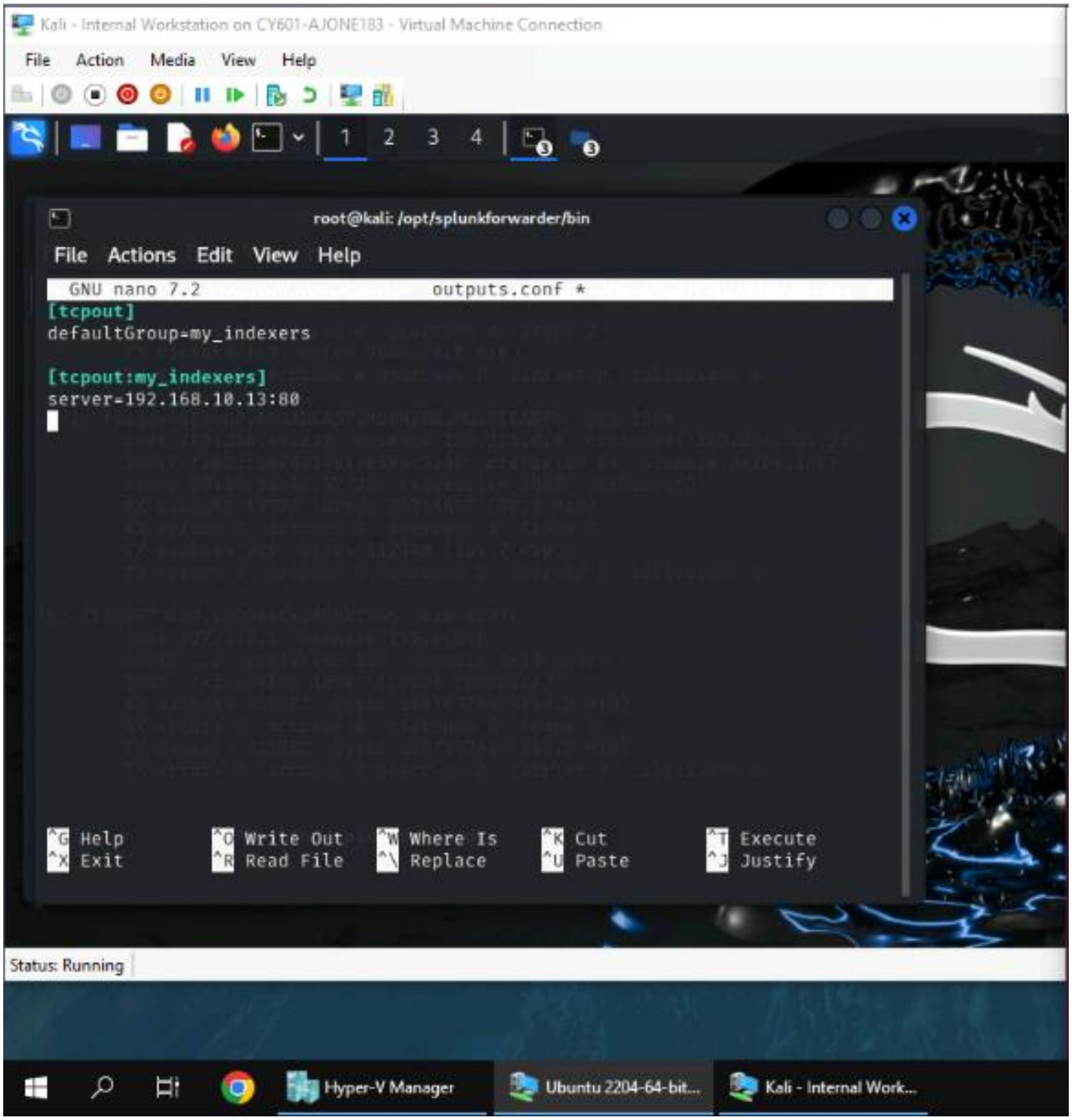
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste
^T Execute
^J Justify

Input: To open the inputs.conf file with a text editor I used the command sudo nano inputs.conf and added the following lines to monitor the alert.full file with the correct file path.



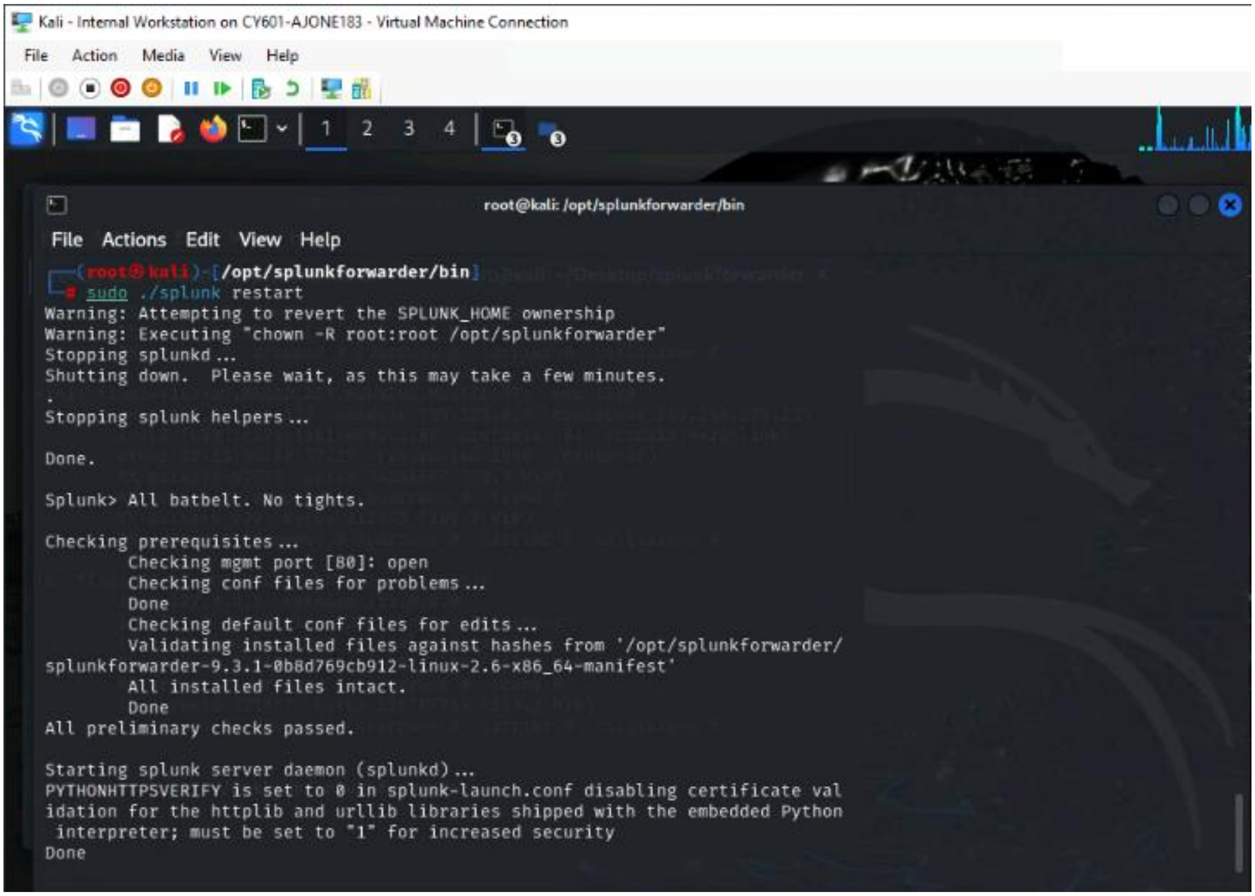
Kali - Internal Workstation on CY601-AJONE183 - Virtual Machine Connection
File Action Media View Help
Settings | Splunk
root@kali: /opt/splunkforwarder
File Actions Edit View Help
Go back one page (Alt+Left Arrow)
Right-click or pull down to show history
root@kali: ~

```
┌──(root㉿kali)-[/opt/splunkforwarder]
└─# sudo nano outputs.conf

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─#

┌──(root㉿kali)-[/opt/splunkforwarder]
└─# sudo nano outputs.conf
```



```
  GNU nano 7.2                            outputs.conf *
[tcpout]
defaultGroup=my_indexers

[tcpout:my_indexers]
server=192.168.10.13:80
```

Output: I configured the forwarder to send data to the Splunk server. I replaced the following IP address/port.



Kali - Internal Workstation on CY601-AJONE183 - Virtual Machine Connection
File
Action
Media
View
Help
1
2
3
4
root@kali: /opt/splunkforwarder/bin
File
Actions
Edit
View
Help

```
┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─# sudo ./splunk restart
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R root:root /opt/splunkforwarder"
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
.
Stopping splunk helpers...

Done.

Splunk> All batbelt. No tights.

Checking prerequisites...
        Checking mgmt port [80]: open
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/
splunkforwarder-9.3.1-0b8d769cb912-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate val
idation for the httplib and urllib libraries shipped with the embedded Python
 interpreter; must be set to "1" for increased security
Done
```

Restart: After making the changes I saved the new information and used the command sudo ./spunk restart to apply all the changes. This command forces the Splunk Forwarder to reload its configuration and begin monitoring the alert.full file for new Snort alerts.