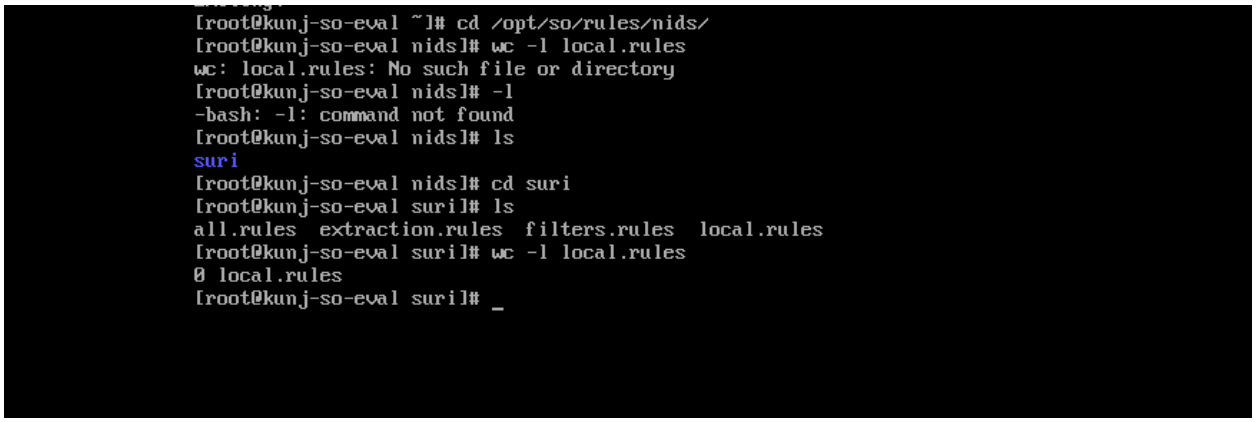
Name: Kunj Modi

ID: 100951290

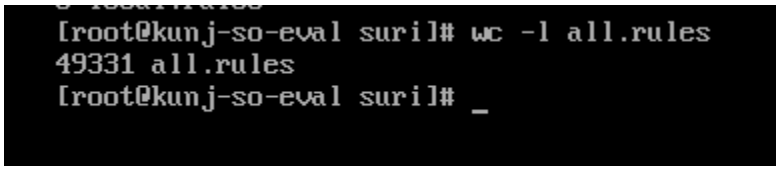
Scenario I – Detecting an attack on Security Onion VM(port 9595) by one linux based machine

a) What is the command to find the number of local rules? **[1 Mark]**
wc -l local.rules

b) How many rules are present in **local.rules**? **Attach the screenshot**. **[2 Marks]**
0

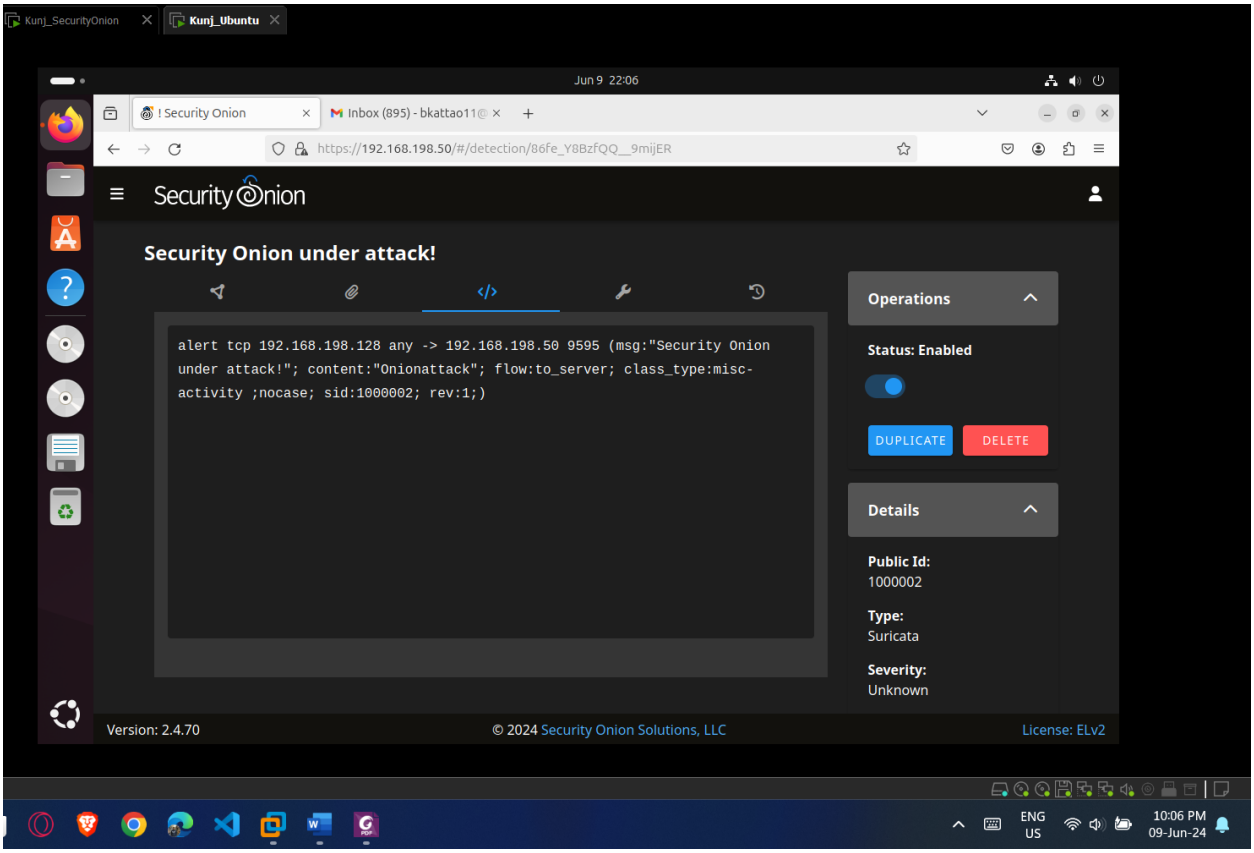


c) How many rules are present in **all.rules**? **Attach the screenshot**. **[2 Marks]**
49331



2. Add NIDS rule for the attack by going to Administration –> Configuration –> idstools in your Security Onion Webinterface.

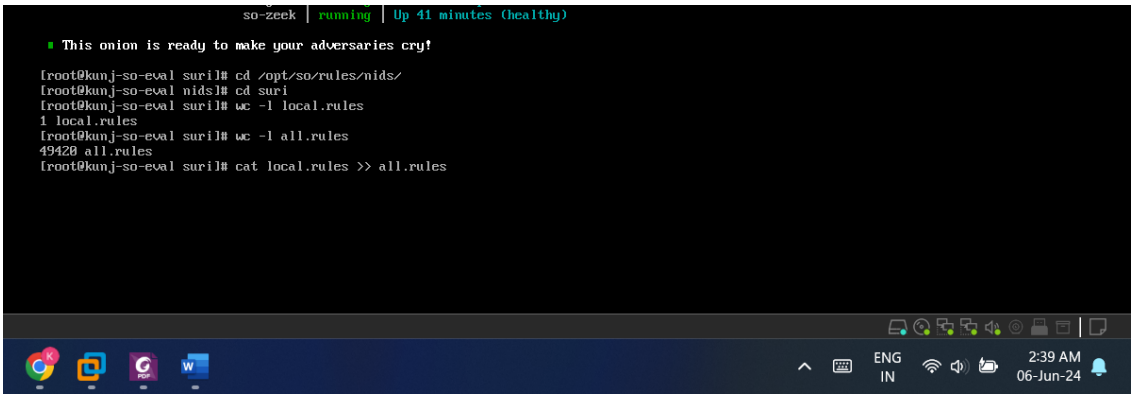
c) Add your new rule(s) and click the checkmark to save them. **The rule is** : alert tcp 192.168.198.128 any -> 192.168.198.50 9595 (msg: "Security Onion under Attack!"; content: "Onionattack"; flow:to_server; class_type:misc-activity; nocase; sid:1000001; rev:1;)



3. After addingAt Security Onion machine, (Switch to super user)

a) How many rules are present now in local.rules? Attach the screenshot. [2 Marks]

1



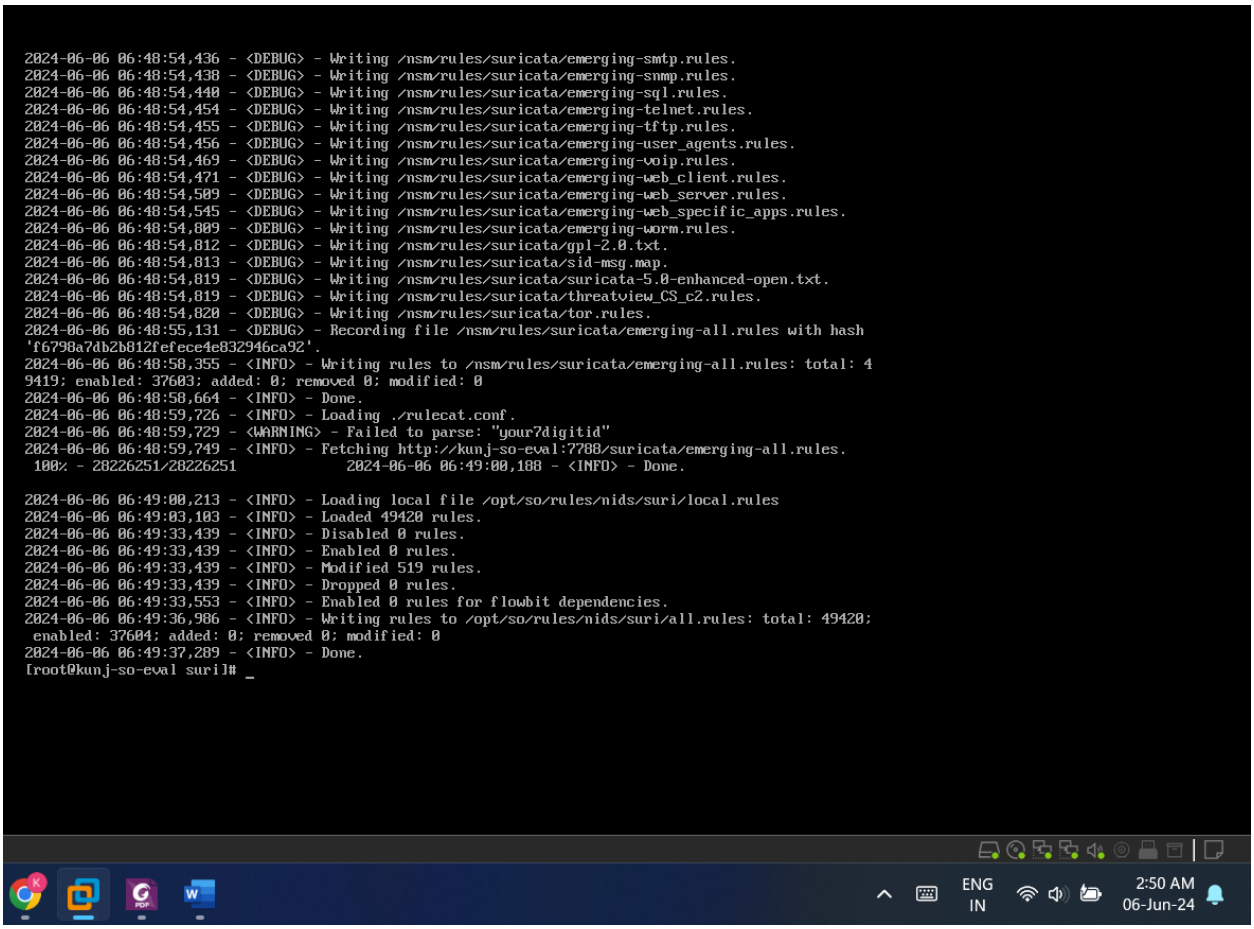
b) How many rules are present now in all.rules? Attach the screenshot. [2 Marks]

49420

c) Show the rule that gets added in local.rules at /opt/so/rules/nids/. . What is the command used? Attach the screenshot.

cat local.rules >> all.rules

d) Update rules: sudo so-rule-update



```
2024-06-06 06:48:54,436 - <DEBUG> - Writing /nsm/rules/suricata/emerging-smtp.rules.
2024-06-06 06:48:54,438 - <DEBUG> - Writing /nsm/rules/suricata/emerging-snmp.rules.
2024-06-06 06:48:54,440 - <DEBUG> - Writing /nsm/rules/suricata/emerging-sql.rules.
2024-06-06 06:48:54,454 - <DEBUG> - Writing /nsm/rules/suricata/emerging-telnet.rules.
2024-06-06 06:48:54,455 - <DEBUG> - Writing /nsm/rules/suricata/emerging-tftp.rules.
2024-06-06 06:48:54,456 - <DEBUG> - Writing /nsm/rules/suricata/emerging-user_agents.rules.
2024-06-06 06:48:54,469 - <DEBUG> - Writing /nsm/rules/suricata/emerging-voip.rules.
2024-06-06 06:48:54,471 - <DEBUG> - Writing /nsm/rules/suricata/emerging-web_client.rules.
2024-06-06 06:48:54,509 - <DEBUG> - Writing /nsm/rules/suricata/emerging-web_server.rules.
2024-06-06 06:48:54,545 - <DEBUG> - Writing /nsm/rules/suricata/emerging-web_specific_apps.rules.
2024-06-06 06:48:54,809 - <DEBUG> - Writing /nsm/rules/suricata/emerging-worm.rules.
2024-06-06 06:48:54,812 - <DEBUG> - Writing /nsm/rules/suricata/gpl-2.0.txt.
2024-06-06 06:48:54,813 - <DEBUG> - Writing /nsm/rules/suricata/sid-msg.map.
2024-06-06 06:48:54,819 - <DEBUG> - Writing /nsm/rules/suricata/suricata-5.0-enhanced-open.txt.
2024-06-06 06:48:54,819 - <DEBUG> - Writing /nsm/rules/suricata/threatview_CS_c2.rules.
2024-06-06 06:48:54,820 - <DEBUG> - Writing /nsm/rules/suricata/tor.rules.
2024-06-06 06:48:55,131 - <DEBUG> - Recording file /nsm/rules/suricata/emerging-all.rules with hash
'f6798a7db2b812fefece4e832946ca92'.
2024-06-06 06:48:58,355 - <INFO> - Writing rules to /nsm/rules/suricata/emerging-all.rules: total: 4
9419; enabled: 37603; added: 0; removed 0; modified: 0
2024-06-06 06:48:58,664 - <INFO> - Done.
2024-06-06 06:48:59,726 - <INFO> - Loading ./rulecat.conf.
2024-06-06 06:48:59,729 - <WARNING> - Failed to parse: "your?digitid"
2024-06-06 06:48:59,749 - <INFO> - Fetching http://kunj-so-eval:7788/suricata/emerging-all.rules.
 100% - 28226251/28226251            2024-06-06 06:49:00,188 - <INFO> - Done.

2024-06-06 06:49:00,213 - <INFO> - Loading local file /opt/so/rules/nids/suri/local.rules
2024-06-06 06:49:03,103 - <INFO> - Loaded 49420 rules.
2024-06-06 06:49:33,439 - <INFO> - Disabled 0 rules.
2024-06-06 06:49:33,439 - <INFO> - Enabled 0 rules.
2024-06-06 06:49:33,439 - <INFO> - Modified 519 rules.
2024-06-06 06:49:33,439 - <INFO> - Dropped 0 rules.
2024-06-06 06:49:33,553 - <INFO> - Enabled 0 rules for flowbit dependencies.
2024-06-06 06:49:36,986 - <INFO> - Writing rules to /opt/so/rules/nids/suri/all.rules: total: 49420;
 enabled: 37604; added: 0; removed 0; modified: 0
2024-06-06 06:49:37,289 - <INFO> - Done.
[root@kunj-so-eval suri]# _
```

i. What is the location (complete path) of the loading of local file?

`/etc/suricata/suricata.yaml`

ii. How many total rules loaded?

1

iii. What is the location(complete path) where the local files are written or merged?

/opt/so/rules/nids

iv. Justify your answer with screenshot.

```
2024-06-06 06:48:54,436 - <DEBUG> - Writing /nsm/rules/suricata/emerging-smtp.rules.
2024-06-06 06:48:54,438 - <DEBUG> - Writing /nsm/rules/suricata/emerging-snmp.rules.
2024-06-06 06:48:54,440 - <DEBUG> - Writing /nsm/rules/suricata/emerging-sql.rules.
2024-06-06 06:48:54,454 - <DEBUG> - Writing /nsm/rules/suricata/emerging-telnet.rules.
2024-06-06 06:48:54,455 - <DEBUG> - Writing /nsm/rules/suricata/emerging-tftp.rules.
2024-06-06 06:48:54,456 - <DEBUG> - Writing /nsm/rules/suricata/emerging-user_agents.rules.
2024-06-06 06:48:54,469 - <DEBUG> - Writing /nsm/rules/suricata/emerging-voip.rules.
2024-06-06 06:48:54,471 - <DEBUG> - Writing /nsm/rules/suricata/emerging-web_client.rules.
2024-06-06 06:48:54,509 - <DEBUG> - Writing /nsm/rules/suricata/emerging-web_server.rules.
2024-06-06 06:48:54,545 - <DEBUG> - Writing /nsm/rules/suricata/emerging-web_specific_apps.rules.
2024-06-06 06:48:54,809 - <DEBUG> - Writing /nsm/rules/suricata/emerging-worm.rules.
2024-06-06 06:48:54,812 - <DEBUG> - Writing /nsm/rules/suricata/gpl-2.0.txt.
2024-06-06 06:48:54,813 - <DEBUG> - Writing /nsm/rules/suricata/sid-msg.map.
2024-06-06 06:48:54,819 - <DEBUG> - Writing /nsm/rules/suricata/suricata-5.0-enhanced-open.txt.
2024-06-06 06:48:54,819 - <DEBUG> - Writing /nsm/rules/suricata/threatview_CS_c2.rules.
2024-06-06 06:48:54,820 - <DEBUG> - Writing /nsm/rules/suricata/tor.rules.
2024-06-06 06:48:55,131 - <DEBUG> - Recording file /nsm/rules/suricata/emerging-all.rules with hash
'f6798a7db2b812fefece4e832946ca92'.
2024-06-06 06:48:58,355 - <INFO> - Writing rules to /nsm/rules/suricata/emerging-all.rules: total: 4
9419; enabled: 37603; added: 0; removed 0; modified: 0
2024-06-06 06:48:58,664 - <INFO> - Done.
2024-06-06 06:48:59,726 - <INFO> - Loading ./rulecat.conf.
2024-06-06 06:48:59,729 - <WARNING> - Failed to parse: "your?digitid"
2024-06-06 06:48:59,749 - <INFO> - Fetching http://kunj-so-eval:7788/suricata/emerging-all.rules.
 100% - 28226251/28226251             2024-06-06 06:49:00,188 - <INFO> - Done.

2024-06-06 06:49:00,213 - <INFO> - Loading local file /opt/so/rules/nids/suri/local.rules
2024-06-06 06:49:03,103 - <INFO> - Loaded 49420 rules.
2024-06-06 06:49:33,439 - <INFO> - Disabled 0 rules.
2024-06-06 06:49:33,439 - <INFO> - Enabled 0 rules.
2024-06-06 06:49:33,439 - <INFO> - Modified 519 rules.
2024-06-06 06:49:33,439 - <INFO> - Dropped 0 rules.
2024-06-06 06:49:33,553 - <INFO> - Enabled 0 rules for flowbit dependencies.
2024-06-06 06:49:36,986 - <INFO> - Writing rules to /opt/so/rules/nids/suri/all.rules: total: 49420;
 enabled: 37604; added: 0; removed 0; modified: 0
2024-06-06 06:49:37,289 - <INFO> - Done.
[root@kunj-so-eval suri]# _
```

---

4. Perform the following steps in first Ubuntu / Centos machine: [1 + 1 + 2 Marks]

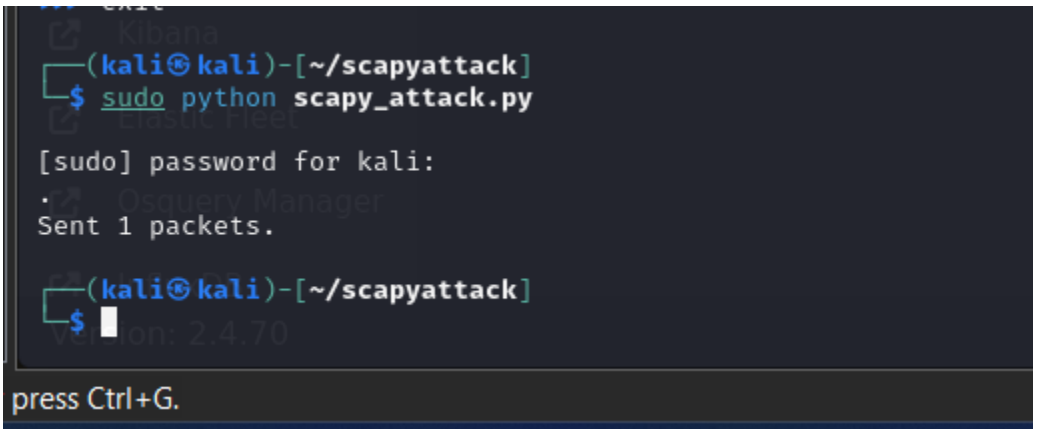
a) What is the version of python?
Python 3.11.7

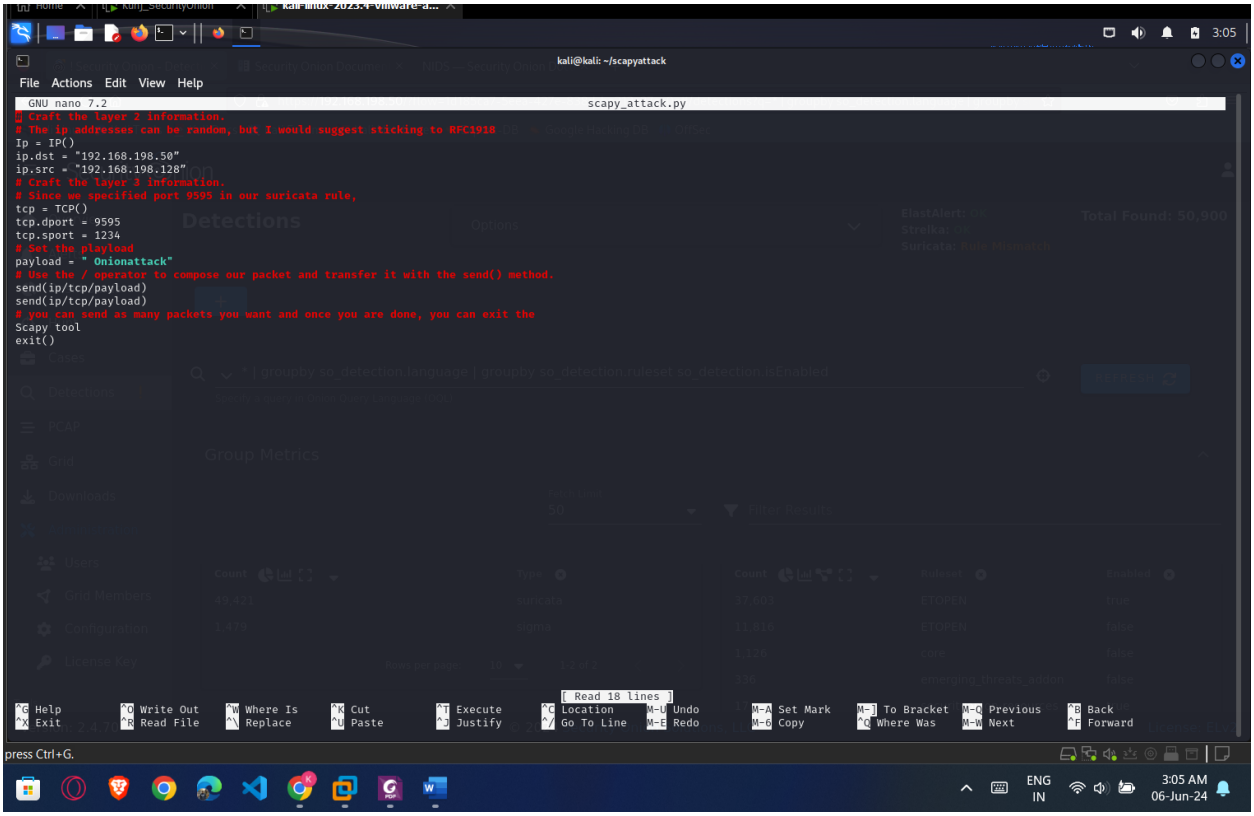
b) What is the ip address of inet Interface?
192.168.198.128

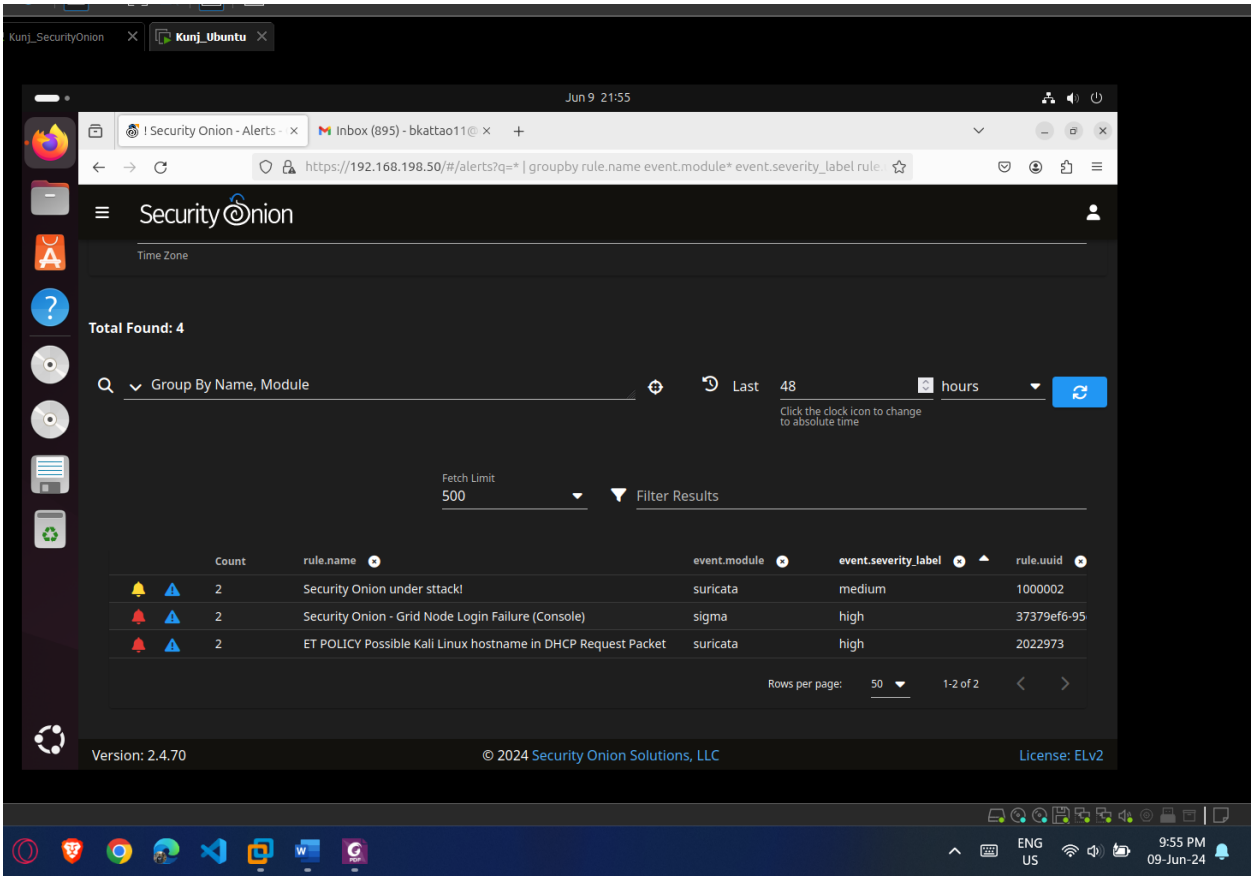
e)

```
┌──(kali㉿kali)-[~]
└─$ pip install scapy

Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: scapy in /usr/lib/python3/dist-packages (2.5.0)

┌──(kali㉿kali)-[~]
```

 # Craft the layer 2 information.
 # The ip addresses can be random, but I would suggest sticking to RFC1918
Ip = IP()
ip.dst = "192.168.198.50”
ip.src = "192.168.198.128”
 # Craft the layer 3 information.
 # Since we specified port 9595 in our suricata rule,
tcp = TCP()
tcp.dport = 9595
tcp.sport = 1234
 # Set the playload
payload = " Onionattack"
 # Use the / operator to compose our packet and transfer it with the send() method.
send(ip/tcp/payload)
send(ip/tcp/payload)
 # you can send as many packets you want and once you are done, you can exit the Scapy tool
exit()




kali@kali: ~/scapyattack
File Actions Edit View Help
GNU nano 7.2
scapy_attack.py
# Craft the layer 2 information.
# The ip addresses can be random, but I would suggest sticking to RFC1918
Ip = IP()
ip.dst = "192.168.198.50"
ip.src = "192.168.198.128"
# Craft the layer 3 information.
# Since we specified port 9595 in our suricata rule,
tcp = TCP()
tcp.dport = 9595
tcp.sport = 1234
# Set the payload
payload = " Onionattack"
# Use the / operator to compose our packet and transfer it with the send() method.
send(ip/tcp/payload)
send(ip/tcp/payload)
# you can send as many packets you want and once you are done, you can exit the
Scapy tool
exit()
[Read 18 lines]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous ^B Back
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-W Next ^F Forward
press Ctrl+G.
3:05 AM
06-Jun-24


Kunj_SecurityOnion
Kunj_Ubuntu
Jun 9 21:55
Security Onion - Alerts
Inbox (895) - bkattao11@
https://192.168.198.50/#/alerts?q=* | groupby rule.name event.module* event.severity_label rule
Security Onion
Time Zone
Total Found: 4
Group By Name, Module
Last 48 hours
Click the clock icon to change to absolute time
Fetch Limit 500
Filter Results
Count rule.name event.module event.severity_label rule.uuid
2 Security Onion under sttack! suricata medium 1000002
2 Security Onion - Grid Node Login Failure (Console) sigma high 37379ef6-95
2 ET POLICY Possible Kali Linux hostname in DHCP Request Packet suricata high 2022973
Rows per page: 50 1-2 of 2
Version: 2.4.70
© 2024 Security Onion Solutions, LLC
License: ELv2
9:55 PM
09-Jun-24

Answer the following: [12 Marks]

a) network.data.decoded: " Onionattack

b) observer.name : "Suricata"

c) rule.category: "misc-activity"

d) rule.metadata.policy: none

e) rule.name : "Security Onion under attack!

f) rule.rule: alert tcp 192.168.198.128 any -> 192.168.198.50 9595 (msg:"Security Onion under attack!"; content:"Onionattack"; flow:to_server; class_type:misc-activity; nocase; sid: 1000002; rev:1;)

g) rule.uuid : 1000002

h) source.ip : "192.168.198.128"

i) source.port : 1234

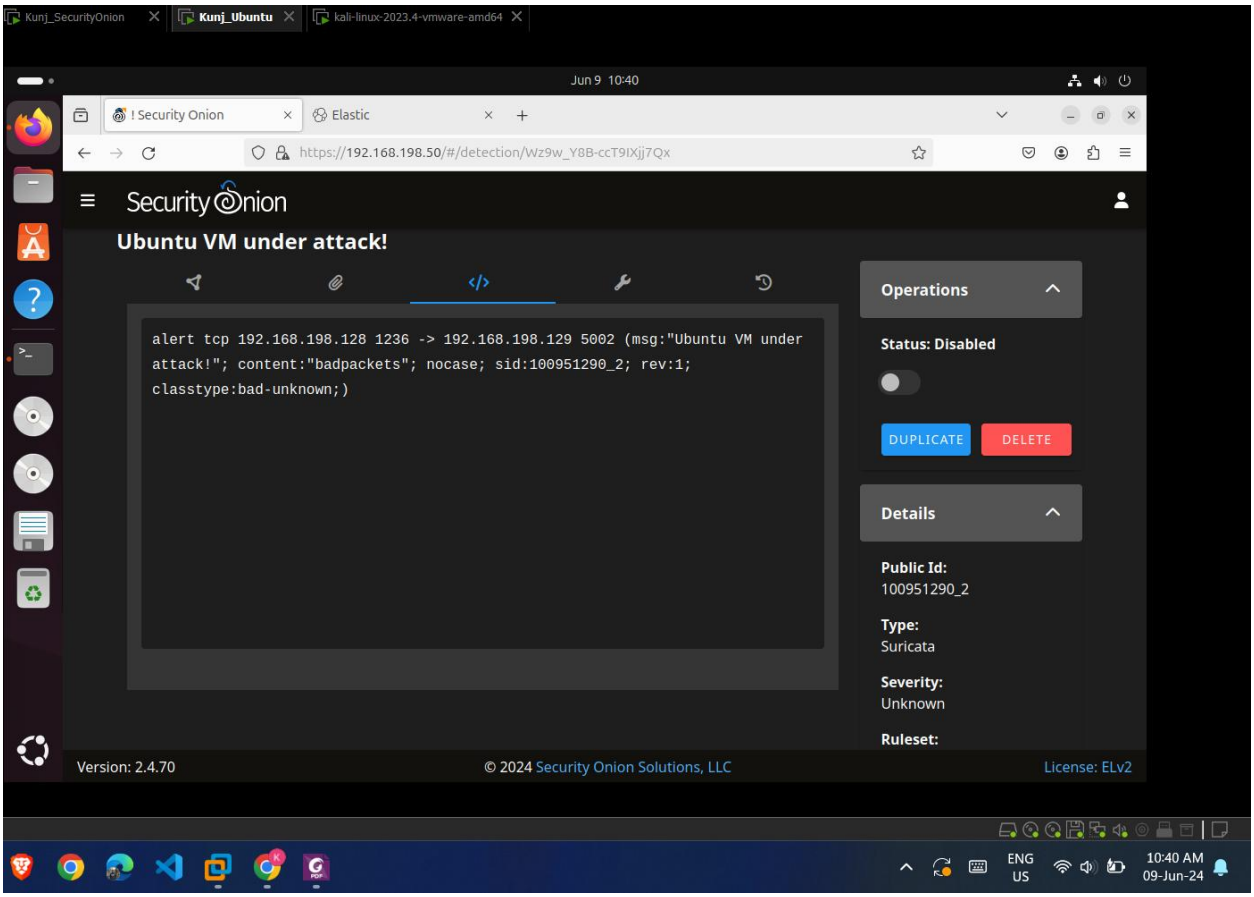
j) destination.ip: "192.168.198.50"

k) destination.port : 9595

l) event.severity: medium

Scenario II – Detecting an attack on one linux based machine from another linux
based machine by Security Onion

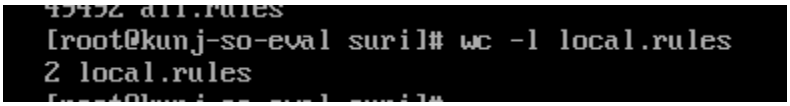
c)



3. At Security Onion machine, (Switch to super user)

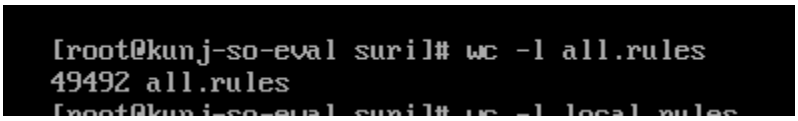
a. How many rules are now present in local.rules? Attach the screenshot. [2 Marks]

1(this is old screenshot I have reperformed this step)



b. How many rules are now present in all.rules? Attach the screenshot. [2 Marks]

49492



c. Update rules: sudo so-rule-update

d. Show the rule that gets added in local.rules at /opt/so/rules/nids/. . What is the command used? Attach the screenshot. [1+2 Marks]

sudo tail -n 20 local.rules

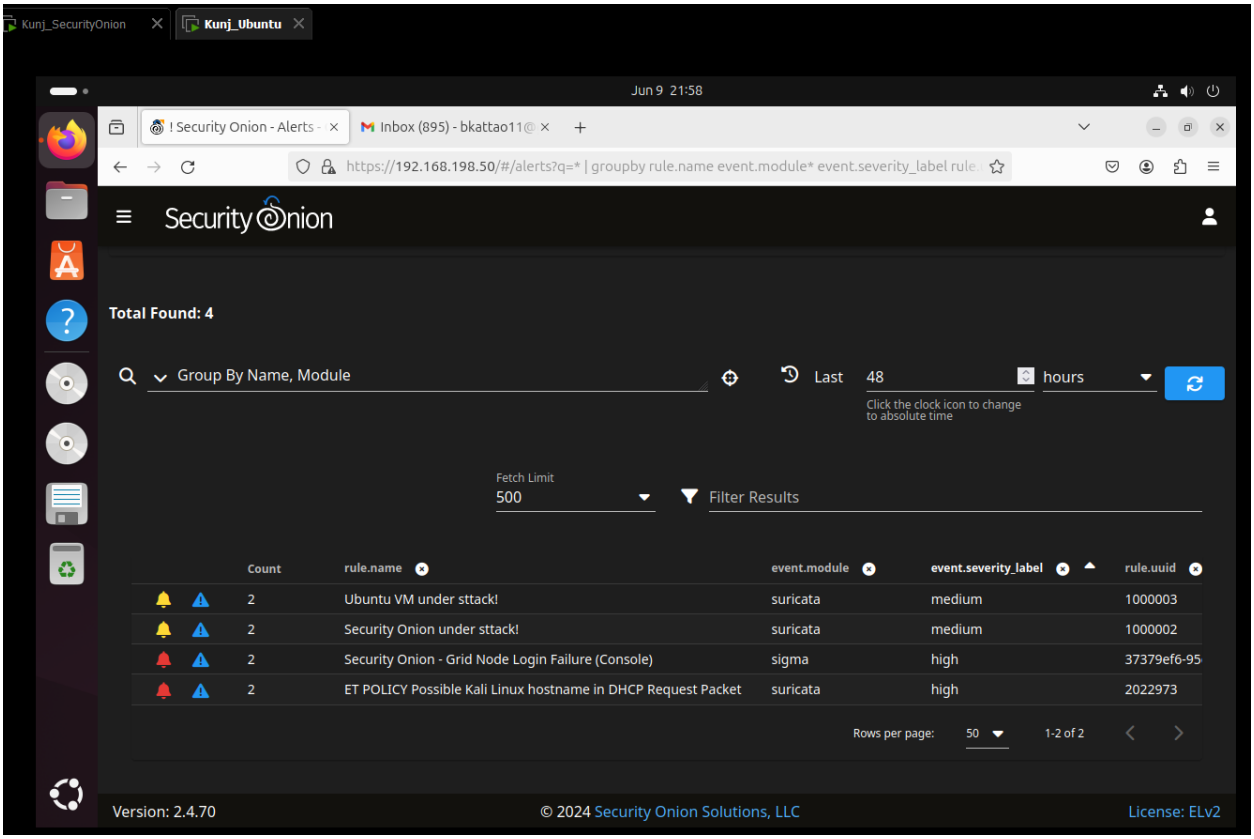
```
[root@kunj-so-eval suri]# sudo tail -n 20 local.rules
# Add your custom Suricata rules in this file.
alert tcp 192.168.198.128 any -> 198.168.198.50 9595 (msg: "Security Onion under Attack!"; content:
"Onionattack"; flow:to_server; class_type:misc-activity; nocase; sid:100951290; rev:1;)
alert tcp 192.168.198.128 1236 -> 192.168.198.129 5002 (msg:"Ubuntu VM under attack!"; content:"badp
ackets"; nocase; sid:100951290_2; rev:1; classtype:bad-unknown;)[root@kunj-so-eval suri]#
```

4. C)

```
Home | Kunj_SecurityOnion | Kunj_Ubuntu | kali-linux-2023.4-vmware-a...
kali@kali: ~/part2_so
File  Actions  Edit  View  Help
  GNU nano 7.2                                                part2_script.py
from scapy.all import *
# Craft the layer 2 information.
# The ip addresses can be random, but I would suggest sticking to RFC1918
Ip = IP()
ip.dst = "192.168.198.129"
ip.src = "192.168.198.128"

# Craft the layer 3 information.
# Since we specified port 9595 in our suricata rule,
tcp = TCP()
tcp.dport = 5002 #( This has to be 5002 because you mentioned your suricata rule)
tcp.sport = 1236 #( You can mention any source port other than assigned ports)
# Set the playload
payload = " Onionattack"
# Use the / operator to compose our packet and transfer it with the send() method.
# Define the source and destination IP addresses and ports
send(ip/tcp/payload)
send(ip/tcp/payload)
send(ip/tcp/payload)
send(ip/tcp/payload)


# you can send as many packets you want and once you are done, you can exit the Scapy tool
exit()
```

```
[06/09/24] kunj [11:17:56 AM] -[~]sudo python3 part2_script.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.

[06/09/24] kunj [11:18:00 AM] -[~]
```

5)



Answer the following:**[12 Marks]**

a) network.data.decoded: "badpackets"
b) observer.name: "Suricata"
c) rule.category: "bad-unknown"
d) rule.metadata,policy : none
e) rule.name : "Ubuntu VM under attack!"
f) rule.rule: alert tcp 192.168.198.128 1236 -> 192.168.198.129 5002 (msg:"Ubuntu VM under attack!"; content:"badpackets"; nocase; sid:100951290_2; rev:1; classtype:bad-unknown;)
g) rule.uuid: 1000003
h) source.ip: "192.168.198.128"
i) source.port: 1236
j) destination.ip: "192.168.198.129"
k) destination.port : 5002
l) event.severity : medium