SNORT – Creating and Implementing Rules

I have now been tasked with writing rules to filter and detect certain data packets

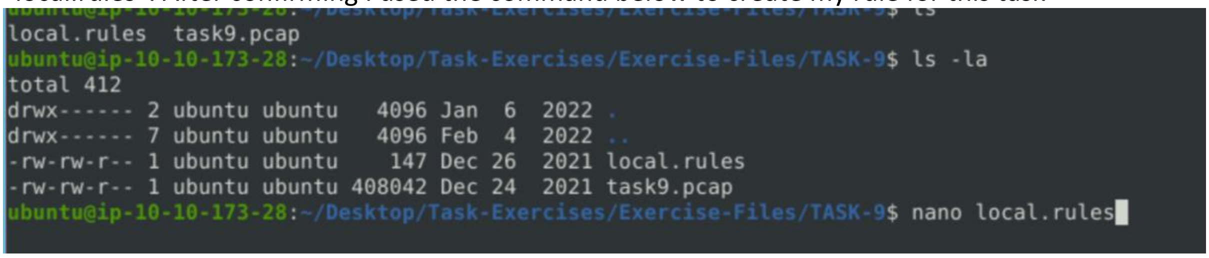
"Use the attached VM and navigate to the Task-Exercises/Exercise-Files/TASK-9 folder to answer the questions! Note that you can use the following command to create the logs in the current directory: -l .

Answer the questions below

Use "task9.pcap"."

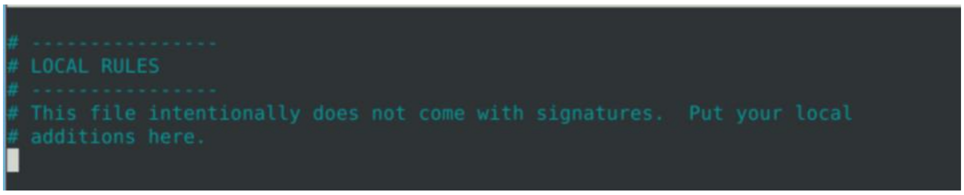
1.Write a rule to filter IP ID "35369" and run it against the given pcap file. What is the request name of the detected packet?
snort -c local.rules -A full -l . -r task9.pcap

First I made my way to the Task-9 folder and confirmed if I had permission to open the file "local.rules". After confirming I used the command below to create my rule for this task



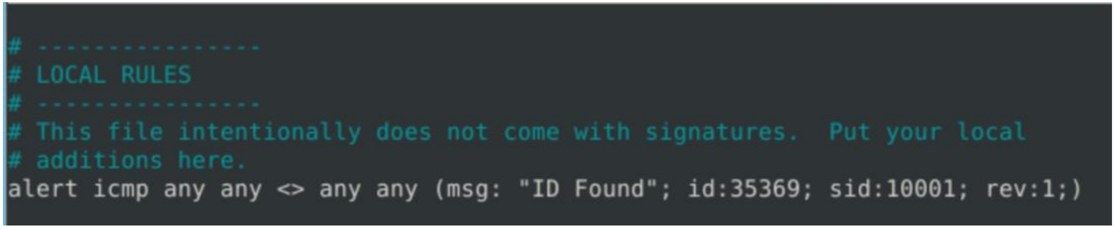
```
ubuntu@ip-10-10-173-28:~/Desktop/Task-Exercises/Exercise-Files/TASK-9$ ls
local.rules  task9.pcap
ubuntu@ip-10-10-173-28:~/Desktop/Task-Exercises/Exercise-Files/TASK-9$ ls -la
total 412
drwx------ 2 ubuntu ubuntu   4096 Jan  6  2022 .
drwx------ 7 ubuntu ubuntu   4096 Feb  4  2022 ..
-rw-rw-r-- 1 ubuntu ubuntu    147 Dec 26  2021 local.rules
-rw-rw-r-- 1 ubuntu ubuntu 408042 Dec 24  2021 task9.pcap
ubuntu@ip-10-10-173-28:~/Desktop/Task-Exercises/Exercise-Files/TASK-9$ nano local.rules
```

Local.rules



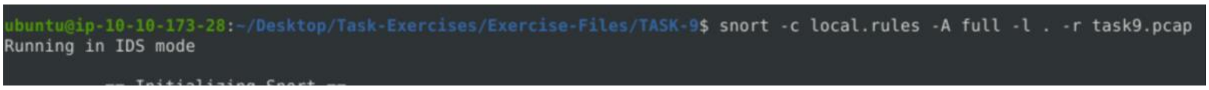
```
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
```

Once opened I wrote the following rule to filter out the IP ID "35369" as requested above.



```
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert icmp any any <> any any (msg: "ID Found"; id:35369; sid:10001; rev:1;)
```

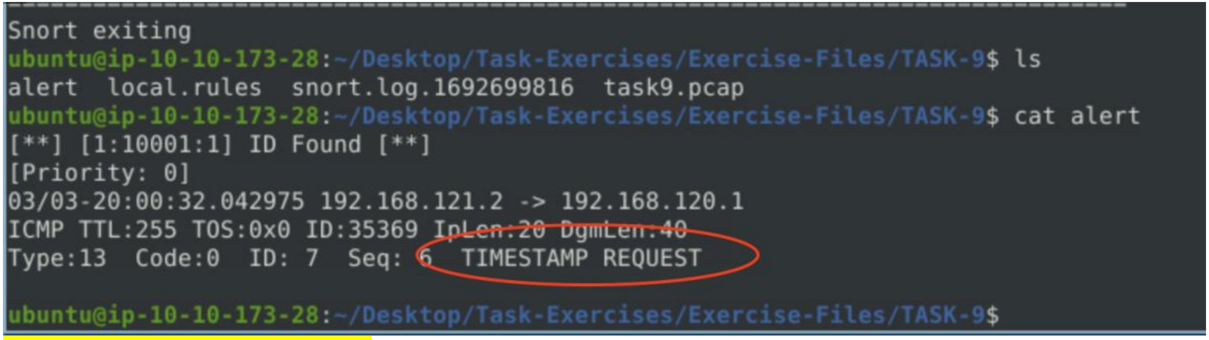
Then once saved I ran the command snort -c local.rules -A full -l . -r task9.pcap



```
ubuntu@ip-10-10-173-28:~/Desktop/Task-Exercises/Exercise-Files/TASK-9$ snort -c local.rules -A full -l . -r task9.pcap
Running in IDS mode

        --== Initializing Snort ==--
```

Once finished I checked to see if the “alert” file was saved within the directory and then opened it. “what is the request name for the detected packet?” As seen below circled the answer to the question above is “TIMESTAMP REQUEST”



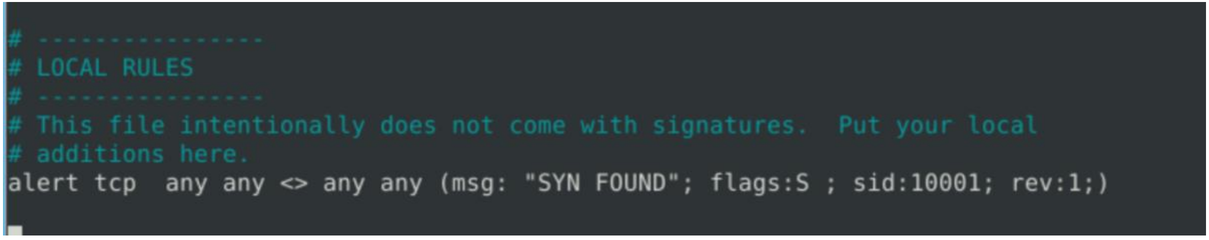
```
Snort exiting
ubuntu@ip-10-10-173-28:~/Desktop/Task-Exercises/Exercise-Files/TASK-9$ ls
alert  local.rules  snort.log.1692699816  task9.pcap
ubuntu@ip-10-10-173-28:~/Desktop/Task-Exercises/Exercise-Files/TASK-9$ cat alert
[**] [1:10001:1] ID Found [**]
[Priority: 0]
03/03-20:00:32.042975 192.168.121.2 -> 192.168.120.1
ICMP TTL:255 TOS:0x0 ID:35369 IpLen:20 DgmLen:40
Type:13  Code:0  ID: 7  Seq: 6  TIMESTAMP REQUEST

ubuntu@ip-10-10-173-28:~/Desktop/Task-Exercises/Exercise-Files/TASK-9$
```

Answer: TIMESTAMP REQUEST

2.Create a rule to filter packets with Syn flag and run it against the given pcap file. What is the number of detected packets?

I modified the rule, saved the file, ran the command snort -c local.rules -A full -l . -r task9.pcap and the total of detected packets was 1.



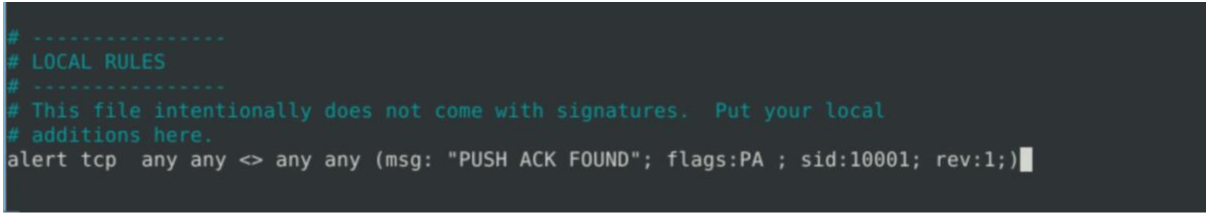
```
# ---------------
# LOCAL RULES
# ---------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert tcp  any any <> any any (msg: "SYN FOUND"; flags:S ; sid:10001; rev:1;)
```

Answer: 1

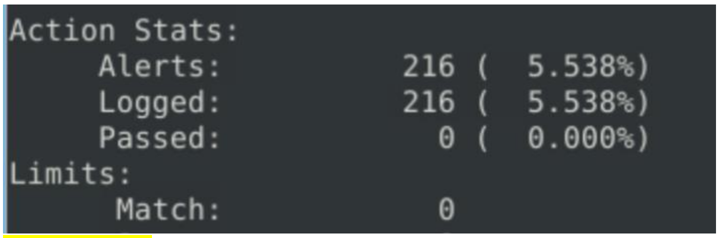
Clear the previous log and alarm files and deactivate/comment out the old rule.

3.Write a rule to filter packets with Push-Ack flags and run it against the given pcap file. What is the number of detected packets?

I modified the rule, saved the file, ran the command snort -c local.rules -A full -l . -r task9.pcap and the total of detected packets was 216



```
# ---------------
# LOCAL RULES
# ---------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert tcp  any any <> any any (msg: "PUSH ACK FOUND"; flags:PA ; sid:10001; rev:1;)
```



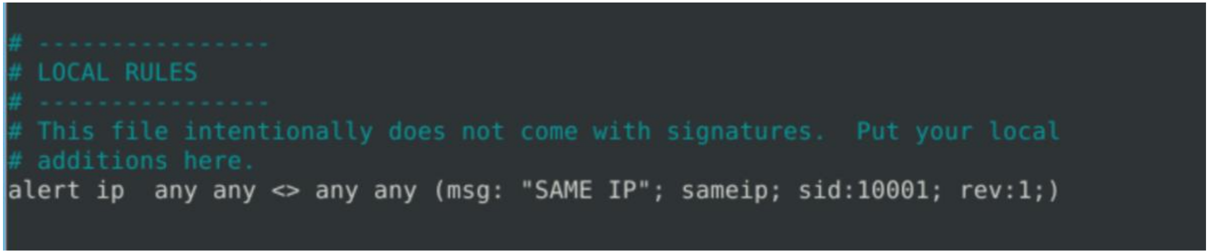
```
Action Stats:
     Alerts:          216 (  5.538%)
     Logged:          216 (  5.538%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
```

Answer: 216

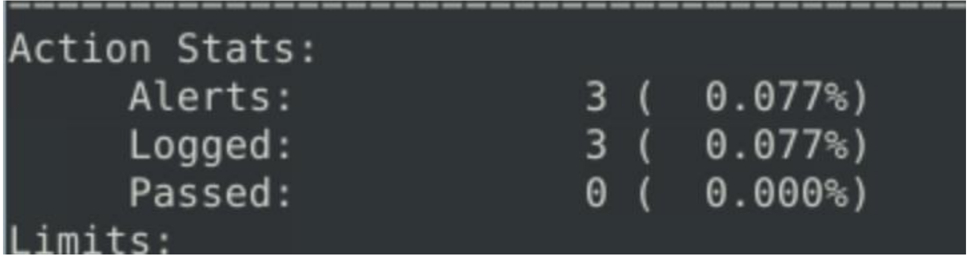
Clear the previous log and alarm files and deactivate/comment out the old rule.

4.Create a rule to filter packets with the same source and destination IP and run it against the given pcap file. What is the number of detected packets?

I modified the rule, saved the file, ran the command snort -c local.rules -A full -l . -r task9.pcap and the total of detected packets was 3 which was incorrect.

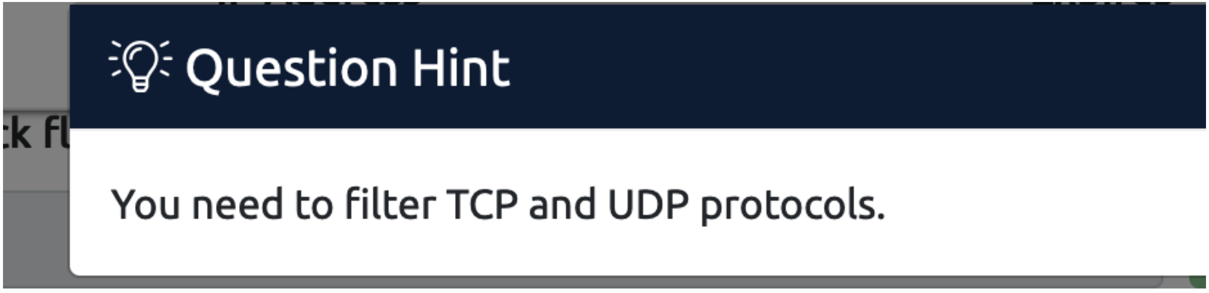


```
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert ip  any any <> any any (msg: "SAME IP"; sameip; sid:10001; rev:1;)
```



```
=======================================
Action Stats:
     Alerts:                 3 (   0.077%)
     Logged:                 3 (   0.077%)
     Passed:                 0 (   0.000%)
Limits:
```

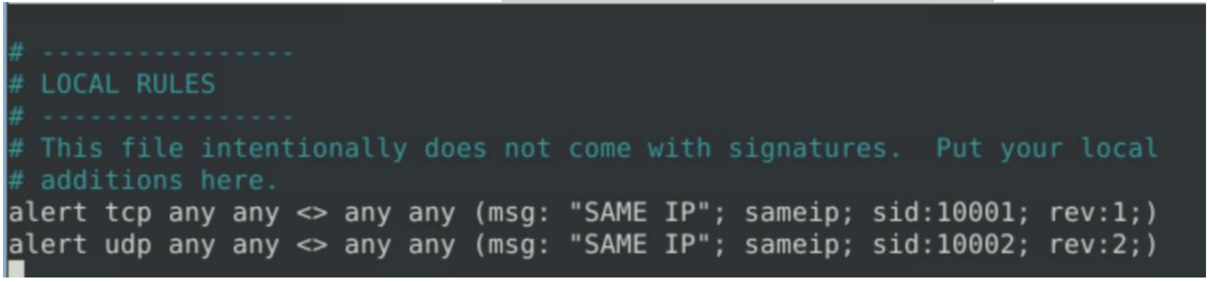
I was unsure of what went wrong and checked the “hint” section



Question Hint

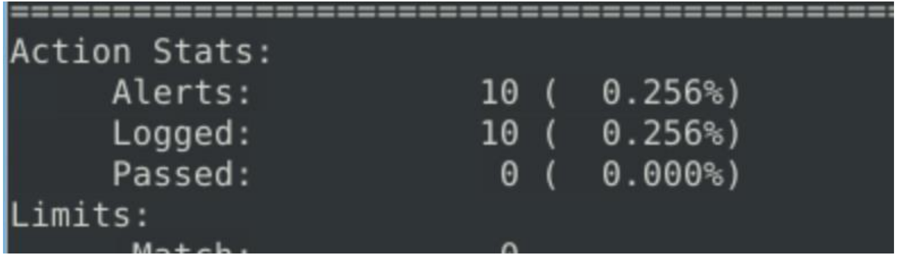
You need to filter TCP and UDP protocols.

It was then I realised that I needed 2 rules to run simultaneously. So I added the following rule to the original and then executed the command snort -c local.rules -A full -l . -r task9.pcap.



```
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
alert tcp any any <> any any (msg: "SAME IP"; sameip; sid:10001; rev:1;)
alert udp any any <> any any (msg: "SAME IP"; sameip; sid:10002; rev:2;)
```

This time the correct alerts of detected packets was revealed



```
=======================================
Action Stats:
     Alerts:                10 (   0.256%)
     Logged:                10 (   0.256%)
     Passed:                 0 (   0.000%)
Limits:
     Match:                  0
```

Answer: 10

5.Case Example - An analyst modified an existing rule successfully. Which rule option must the analyst change after the implementation?

Due to the previous question where I had to add another rule to the “local.files” the answer to the question is rev

Answer: rev