

## Assignment 3: Snort Hands-On Practical


### Instructions:

Carefully follow the steps below after watching the **Snort lesson video** on the LMS.

### What you need to do

1. **Watch the full Snort lesson video** on the LMS.
2. Attempt **all the tasks (Task 1 to Task 11)**. Each task has questions — ensure you answer all of them.
3. After completion, take a **screenshot of the Snort Overview and Congratulations Pages** that shows:
  - All tasks (Task 1–11) as completed (each with a checkmark).
  - The congratulations message after you're done with the 11 tasks.





Congratulations on completing Snort!!! 🎉

Points earned 🏆 232	Completed tasks 📋 11	Room type 👤 Walkthrough	Difficulty 📊 Medium	Streak 🔥 1
------------------------	-------------------------	----------------------------	------------------------	---------------

[📧 Leave Feedback](#) [Next](#)

## Configuration Tasks

- From task 9, open the local.rules file in your Snort configuration directory and add your details as comments at the top of the file in this format:  
# Email address: [your\\_altschool\\_email@example.com](#)  
# AltSchool ID: ALT/ID/2025



```
modifying the local rules
user@ubuntu$ sudo gedit /etc/snort/rules/local.rules

That is your "local.rules" file.

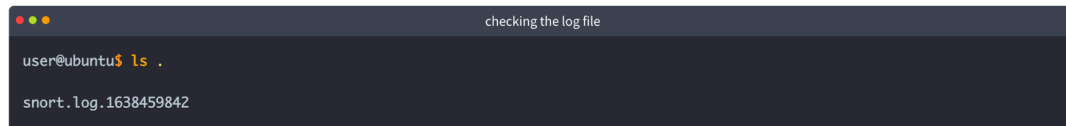
local.rules
/etc/snort/rules

1
2 # -----
3 # LOCAL RULES
4 # -----
5 # This file intentionally does not come with signatures. Put your local
6 # additions here.
7
8 alert icmp any any <- any any (msg: "ICMP Packet Found"; sid: 1000001; rev:1;)
9
10
```

## Task 6 - Special Instruction

- Navigate to the directory that contains your snort.logXXXXX file. Inside that directory:
  - Create a **new file** named with your AltSchool ID.
  - Then run the **ls .** command and take a screenshot showing the file you just created.

Now, let's check the generated log file. **Note that the log file names will be different in your case.**



```
checking the log file
user@ubuntu$ ls .
snort.log.1638459842
```

As you can see, it is a single all-in-one log file. It is a binary/tcpdump format log. This is what it looks like in the folder view.

Name	Size
snort.log.1638459842	6.3 kB

## Submission Format

6. Create a **2-page document** that includes:
  - The screenshot of the overview page (with all tasks ticked).
  - The screenshot showing your **local.rules** comment entries from Task 9
  - The ls . output showing your AltSchool ID file from Task 6.
7. Upload the document to Drive and copy the link. Give permission for anyone with the link to view the document.
8. Submit the link using this [link](#).

**Deadline:** 11:55 PM, 19 April 2025.

## Reminders

- Double-check that every task is marked as complete before taking your overview screenshot.
- Do not share the document with me. Just add the permission for it to be viewed by anyone with the link
- Make sure your AltSchool email and ID are written correctly in the **local.rules** file.