Task 4: Setting Up an Intrusion Detection System Using Snort on Windows 11

In this task, I successfully set up an Intrusion Detection System (IDS) using Snort on a Windows 11 machine. Snort is a powerful open-source tool that monitors network traffic and detects suspicious activities. Below are the steps I followed to configure Snort.

Step 1: Install Required Software

1. I downloaded and installed the following software:
    - **Snort**: The IDS software.
    - **WinPcap/Npcap**: Packet capture libraries required for Snort to monitor network traffic.
2. I ensured all installations were completed without errors.

Step 2: Configure Snort Rules

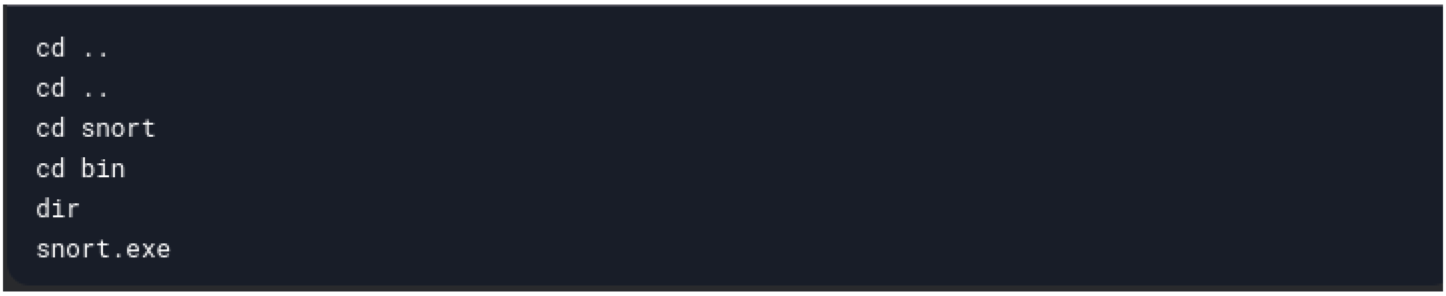
1. After installing Snort, I checked the rules directory located at C:\Snort\rules.
2. Since the directory was empty, I downloaded the Snort rules from the official Snort website (the same site where I downloaded Snort).
3. I extracted the rules into the C:\Snort\rules directory.

Step 3: Organize Snort Files

1. I navigated to C:\Snort\etc.
2. I moved all the contents of the etc folder into the C:\Snort\bin folder for easier access.

Step 4: Verify Snort Installation

1. I opened Command Prompt and used the following commands to navigate to the Snort directory:



```
cd ..
cd ..
cd snort
cd bin
dir
snort.exe
```

2) Snort ran without errors, confirming the installation was successful. I exited Snort by pressing Ctrl + C.

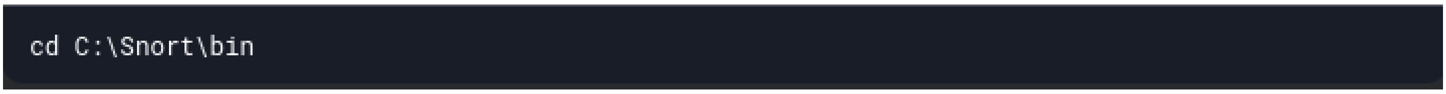
Step 5: Modify Snort Configuration File

1. I opened the snort.conf file located in C:\Snort\etc using Notepad++.
2. I made the following changes:
   - Replaced the IP address in the configuration file with my system's IP address.
   - Updated the rule paths to point to the correct directories on my C drive (e.g., C:\Snort\rules).
3. I saved the changes and closed the editor.

Step 6: Test Snort Configuration

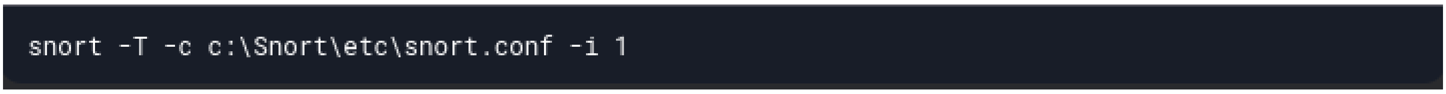
1) I opened Command Prompt as an administrator.

2) I navigated to the bin directory:



```
cd C:\Snort\bin
```

3) I ran the following command to test the configuration:

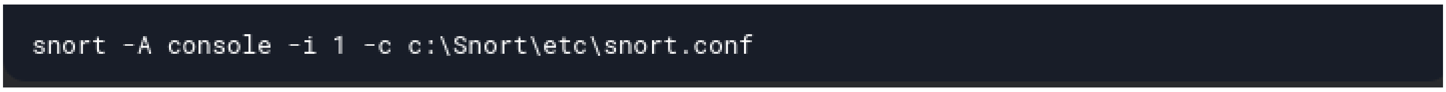


```
snort -T -c c:\Snort\etc\snort.conf -i 1
```

4) The absence of errors confirmed that Snort was successfully configured.

Step 7: Set Up Alert Rules

1) To enable alerts for suspicious network activities, I ran the following command:



```
snort -A console -i 1 -c c:\Snort\etc\snort.conf
```

2) This command started Snort in intrusion detection mode, and any suspicious activity was logged and displayed in the console.

Conclusion

By following these steps, I successfully set up an Intrusion Detection System using Snort on Windows 11. Snort now monitors my network traffic and alerts me to any suspicious activities. I plan to regularly update the Snort rules to ensure the system remains effective against the latest threats.