Name	**Akshat Biniwale**
UID	**2021300014**
Branch	**BE COMPS A**
Batch	**VI**
Subject	**Cryptography and System Security**
Experiment	9

Aim:

Configure and application of SNORT Intrusion Detection System

Objective:

- To configure and utilize Snort as a Network Intrusion Detection System (NIDS) to monitor and detect malicious activities such as SYN scans, UDP scans, and other network-based attacks.
- To write and implement custom Snort rules for identifying specific network attacks and analysing alerts generated during the intrusion detection process.

Theory:

Snort is an open-source tool for Intrusion Detection and Prevention System. It uses a series of rules that help define malicious network activities and uses those rules to find packets that match against them and generates alerts for users.

Snort has 3 primary uses:

1. A packet sniffer like tcpdump
2. A packet logger - which is useful for network traffic debugging
3. As a full-blown network intrusion prevention system

Features:

- Rules: To generate rules to identify various kinds of scans such as TCP scan, UDP scan, FIN scan, etc.
- Attack Detection: To detect network scanning attacks, DoS attack, malware attack, etc.

Procedure:

1. Download snort from their official website www.snort.org/downloads

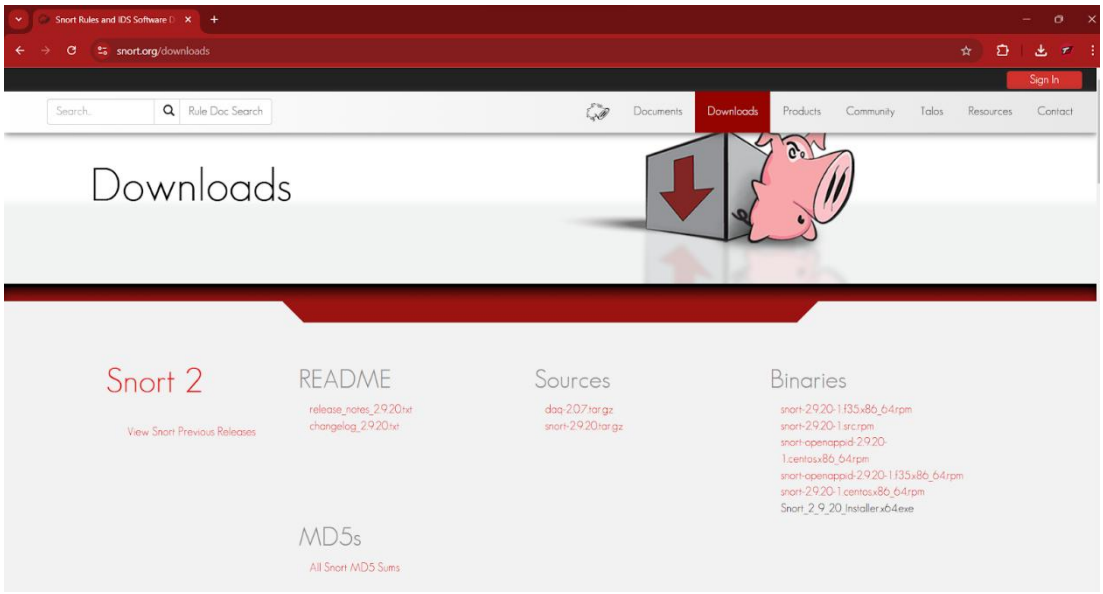

Fig 1.

2. Follow the setup wizard and install snort

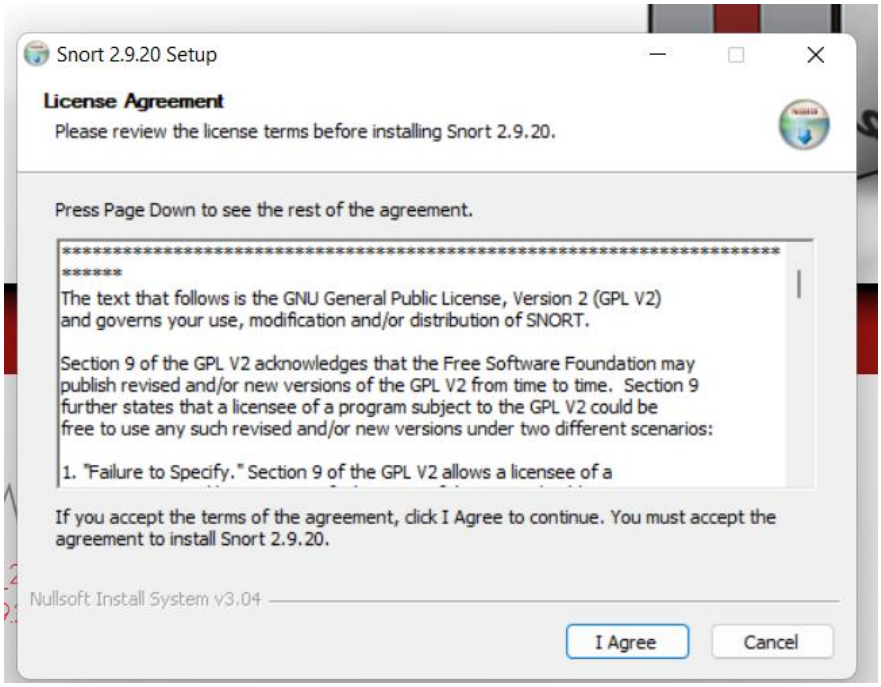

Fig 2.

3. Go to C:/Snort/bin folder and check if snort is properly installed using the -V flag. If snort is properly installed it will show the version of Snort.

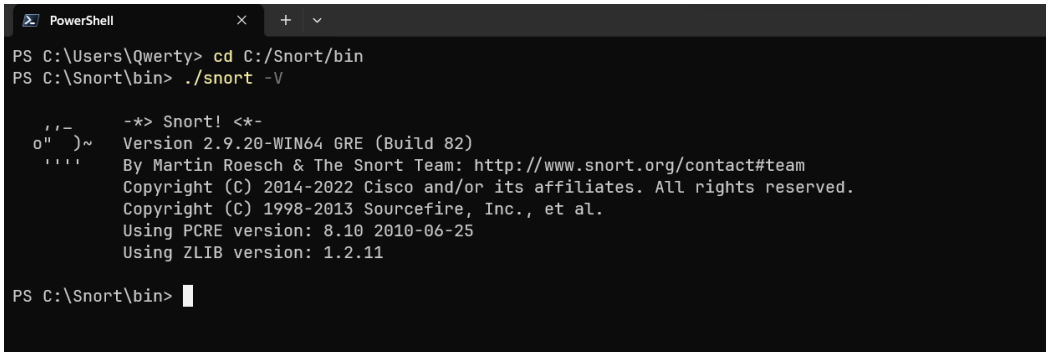

Fig 3.

4. Login in Snort to download Snort rules

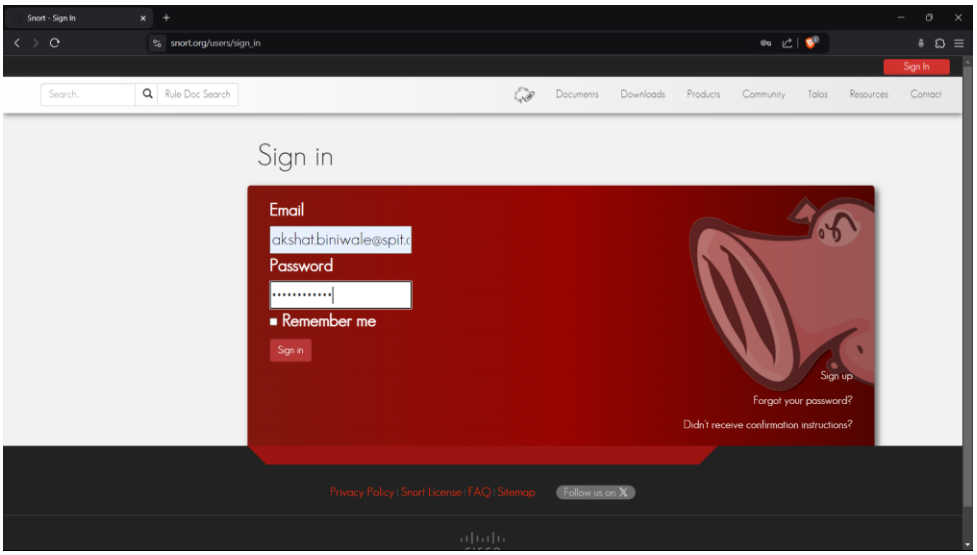

Fig 4.

5. Download the rules of the correct installed version, here 2.9.20

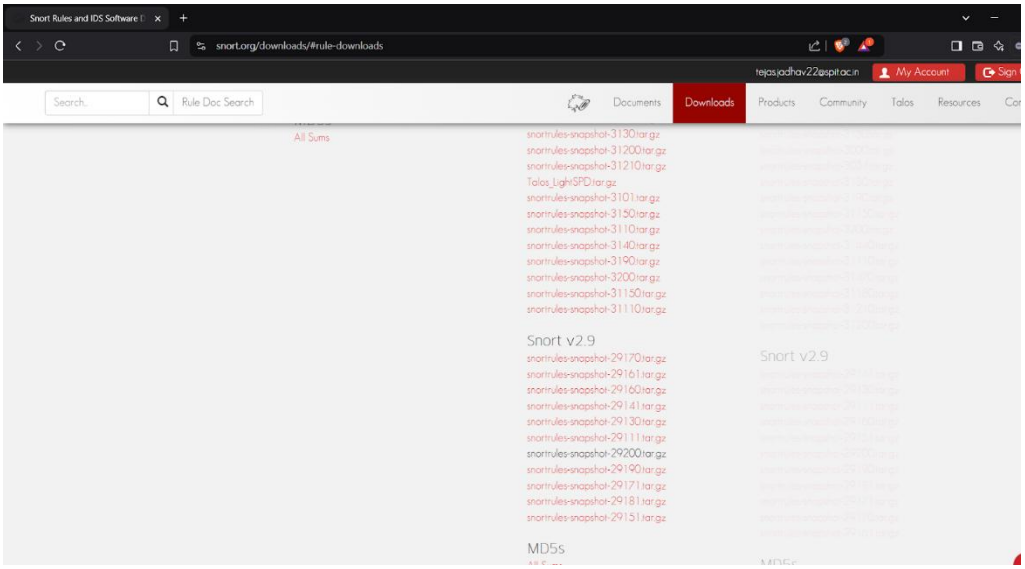

Fig 5.

6. Edit the snort.conf File:

   - Navigate to C:\Snort\etc\snort.conf and configure:
     - Network variables like $HOME_NET and $EXTERNAL_NET.
     - Paths for rules, preproc_rules, and log files.
     - Include custom rule files (e.g., local.rules).
   - Define paths for white.list and black.list if using reputation-based detection.

7. Create and Add Custom Rules:

   - Open local.rules in the Snort rules directory.
   - Add custom rules to detect various attacks, such as SYN scans or ICMP packets.

8. Run Snort and Test Setup:

   - Use the -W option to list available interfaces, then specify the correct one with -i.
   - Run Snort in IDS mode with the command:
     - snort -i <interface_number> -c C:\Snort\etc\snort.conf -A console
   - Perform network scans or attacks from another machine using tools like Nmap and verify that alerts are generated in the console or log files.

Screenshots:

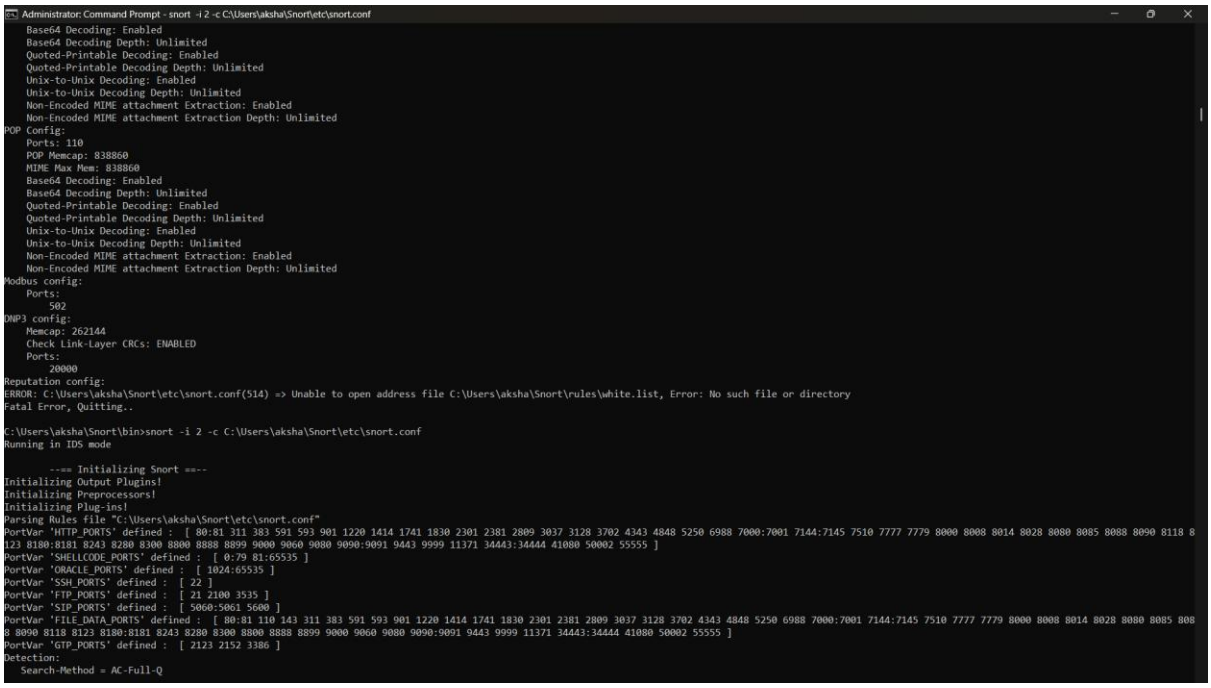

Fig 6.

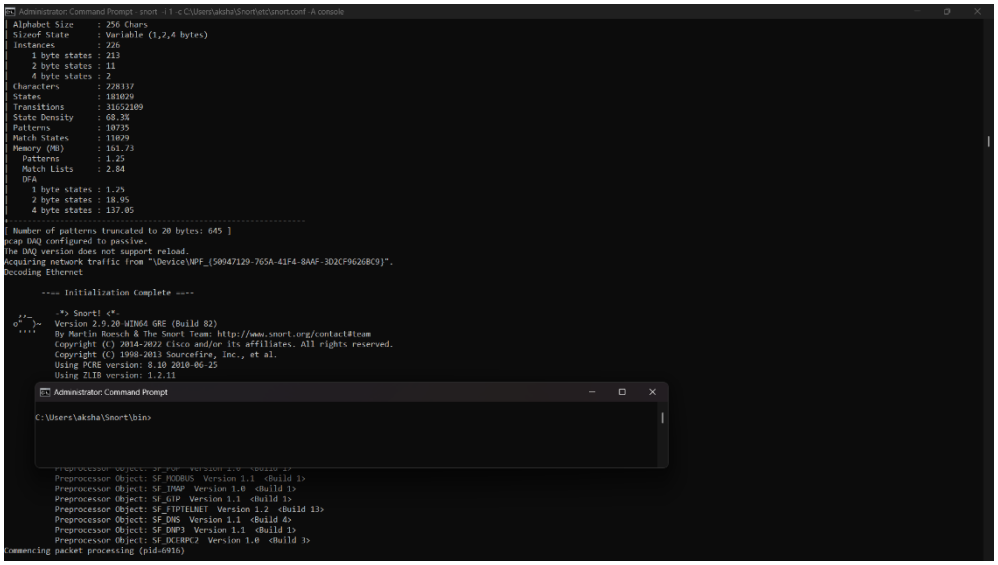

Fig 7.

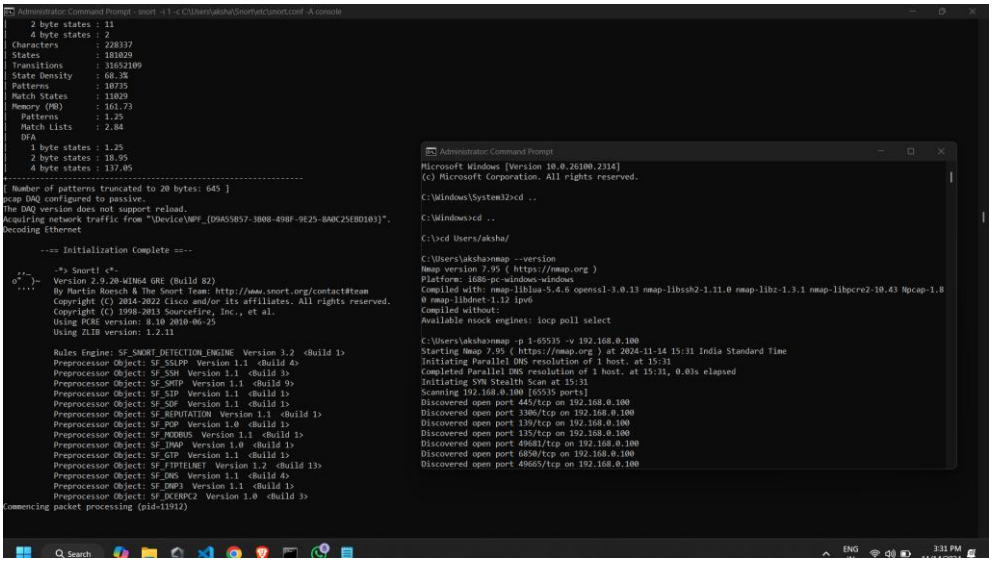

Fig 8.

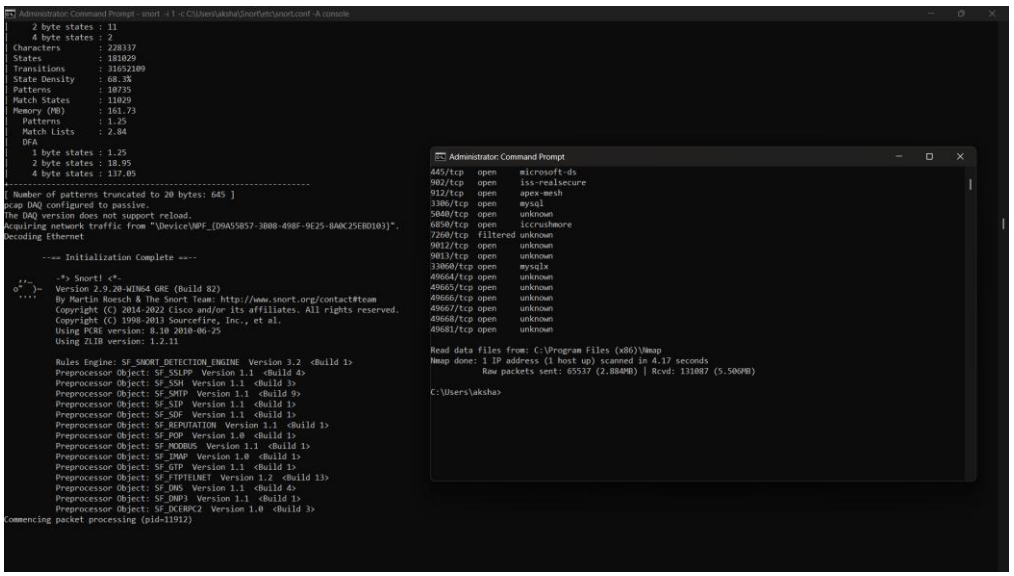

Fig 10.

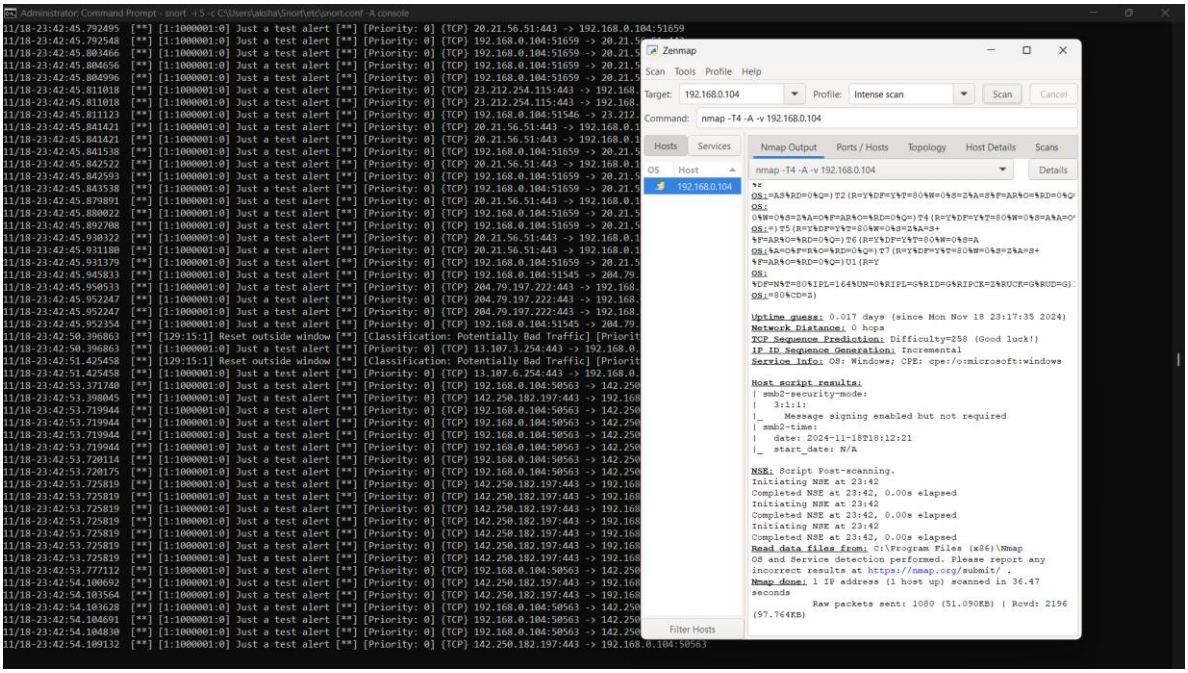

Fig 11.

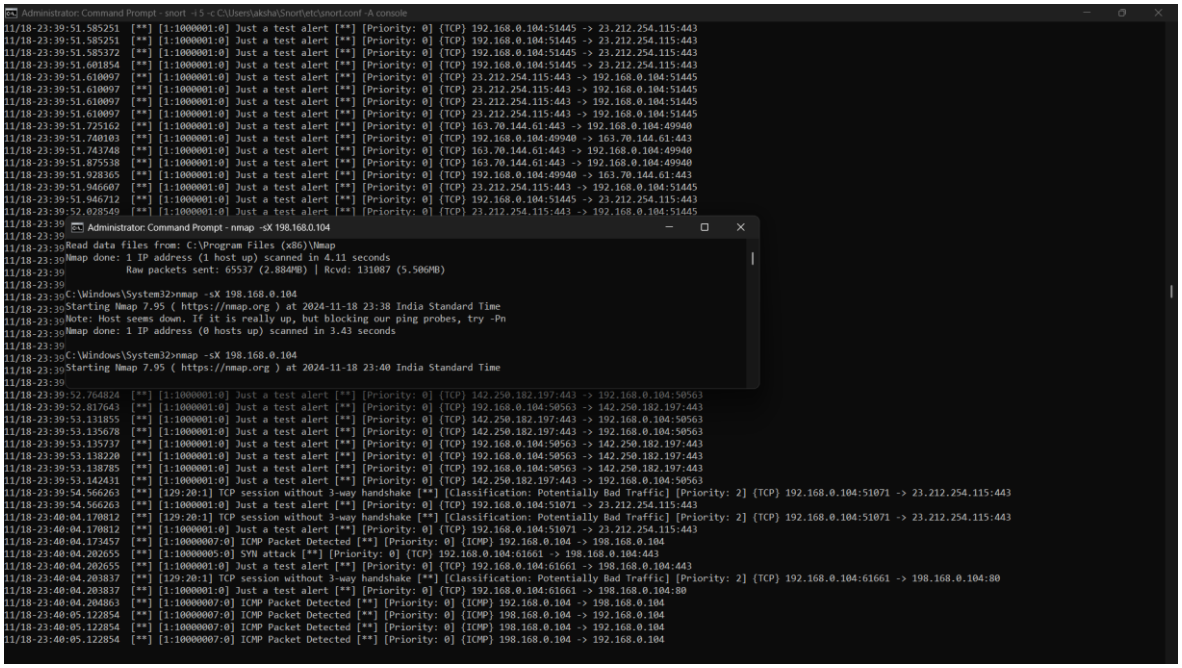

Fig 12.

Conclusion:

This experiment demonstrated the effectiveness of Snort in detecting network intrusions, such as an Nmap OS scan attack, showcasing its utility as a powerful intrusion detection system (IDS). Snort provides real-time monitoring and alerts to help secure networks against potential threats.

- Snort can successfully detect reconnaissance attacks like Nmap OS scans, helping to prevent further exploitation.
- Configuring Snort rules enhances its accuracy and adaptability to diverse attack scenarios.