Title: Installation and Configuration of Snort for Network Security and Safeguarding Against Cyber Threats

DATE:4TH MAY2023

Objective:

The aim of this report is to provide a guide for installing and configuring Snort, a highly regarded network intrusion detection system (IDS). We will demonstrate the functionality of Snort by generating an ICMP attack using the "ping" command and present a screenshot of an alert generated by Snort for the ICMP attack.

Requirements:

To follow this guide, you will need a Linux-based operating system (such as Ubuntu) with administrative privileges. Snort can be downloaded and installed from the official Snort website.

Procedure:

1. Download and Install Snort:

a. Visit the official Snort website and locate the download page.

b. Download the suitable version of Snort compatible with your Linux distribution.

c. Open the terminal and navigate to the directory where the Snort package is downloaded.

d. Utilize the appropriate command to extract the files from the package.

2. Configure Snort:

a. Navigate to the extracted Snort directory using the terminal.

b. Execute the command that generates the Snort configuration file.

c. Customize the configuration file according to the specifications of your network environment and specific requirements.

3. Activate Snort in IDS Mode:

a. Run the command that initiates Snort in IDS mode with the configured rules.

b. Snort will start monitoring network traffic and issuing alerts for suspicious activities.

4. Generate ICMP Attack:

a. Open a separate terminal window.

b. Employ the "ping" command with an increased packet size to simulate an ICMP attack. For instance:

ping -s 65535 <target IP address>

5. Monitor Snort Alerts:

a. Return to the terminal where Snort is running.

b. Observe the real-time alerts generated by Snort.

c. Take note of any alerts related to the ICMP attack.

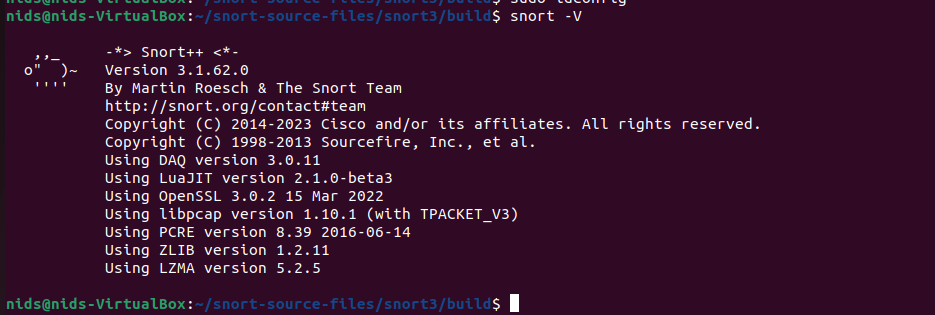
Results Analysis:

By following the outlined steps, Snort is successfully installed, configured, and operating in IDS mode. As a demonstration, we generated an ICMP attack using the "ping" command with a larger packet size. Snort promptly detected and issued an alert for the ICMP attack, highlighting its ability to recognize and respond to network threats.

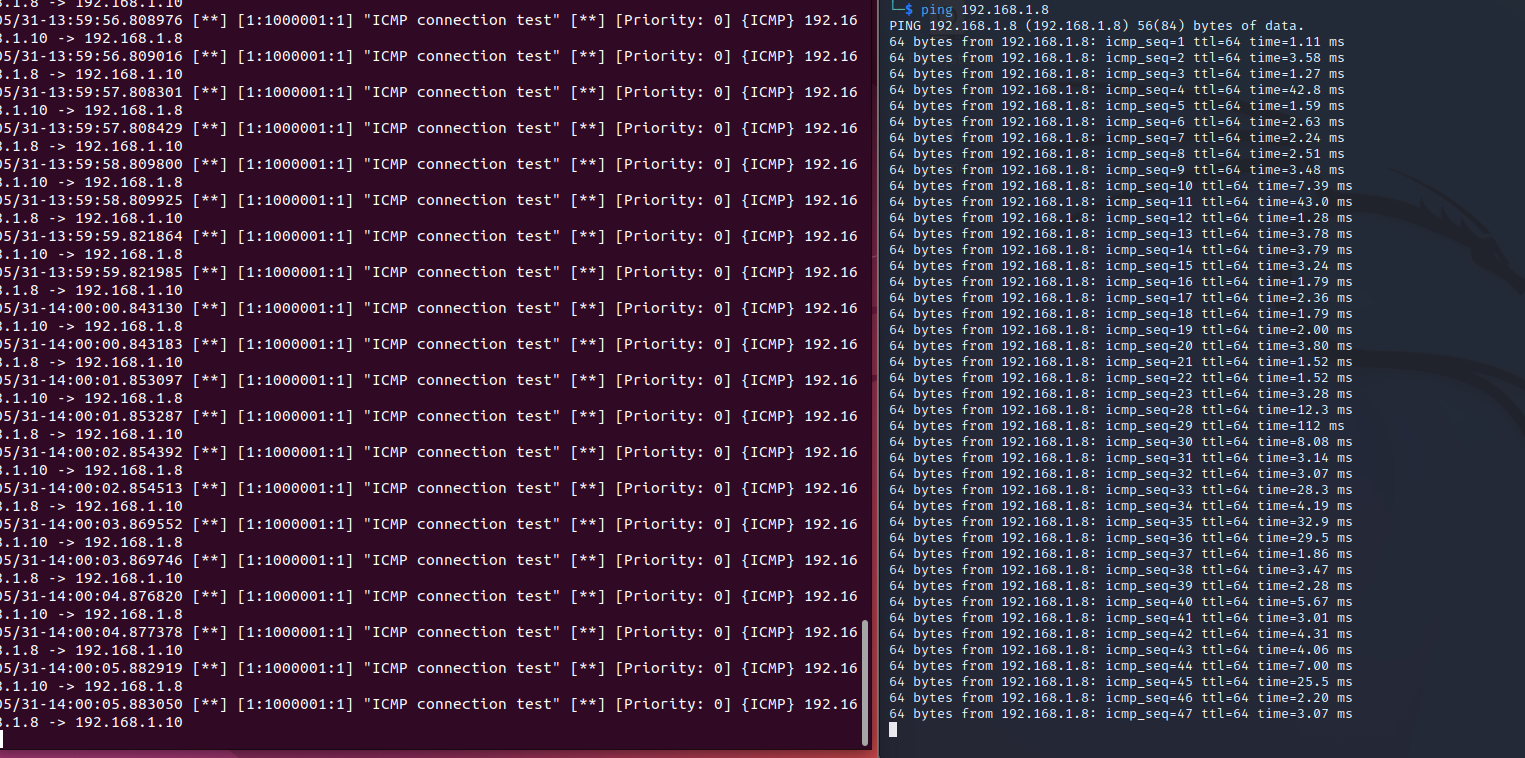
The provided screenshot showcases an alert captured by Snort, clearly indicating the detection of the ICMP attack. This serves as evidence of Snort's proficiency in monitoring network traffic, analyzing packets, and generating alerts for potentially malicious activities.

Demonstrate:

Download and Install Snort from official website the installation method is by the source method from cloning of github and with the configuration



Log generated by snort IDS (ICMP )



Conclusion:

Snort stands as a potent network intrusion detection system, playing a critical role in enhancing network security and defending against cyber threats. By following the step-by-step instructions in this report, users can successfully install and configure Snort, leveraging its capabilities to monitor network traffic, identify suspicious activities, and generate alerts for potential threats.

The demonstration of generating an ICMP attack using the "ping" command and capturing the corresponding Snort alert underscores its effectiveness in identifying and responding to network-based attacks. This underscores the value of Snort in fortifying network security and providing early detection of cyber threats.

Future Scope:

In the future, further advancements can be made to expand Snort's rule set, enabling it to detect and respond to an even broader array of network attacks. Additionally, integration of Snort with complementary security tools and technologies can enhance the overall network defense strategy, bolstering the security posture against evolving cyber threats.

Reference: https://zaeemjaved10.medium.com/installing-configuring-snort-2-9-17-on-windows-10-26f73e342780