Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

Experiment No. : 12

Date: _____

Title : SNORT and studing the logs.

Problem Definition : Study network security by installing an IDS, SNORT and study the logs.

Pre-requisite : IDS

Theory :

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.[1]

IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

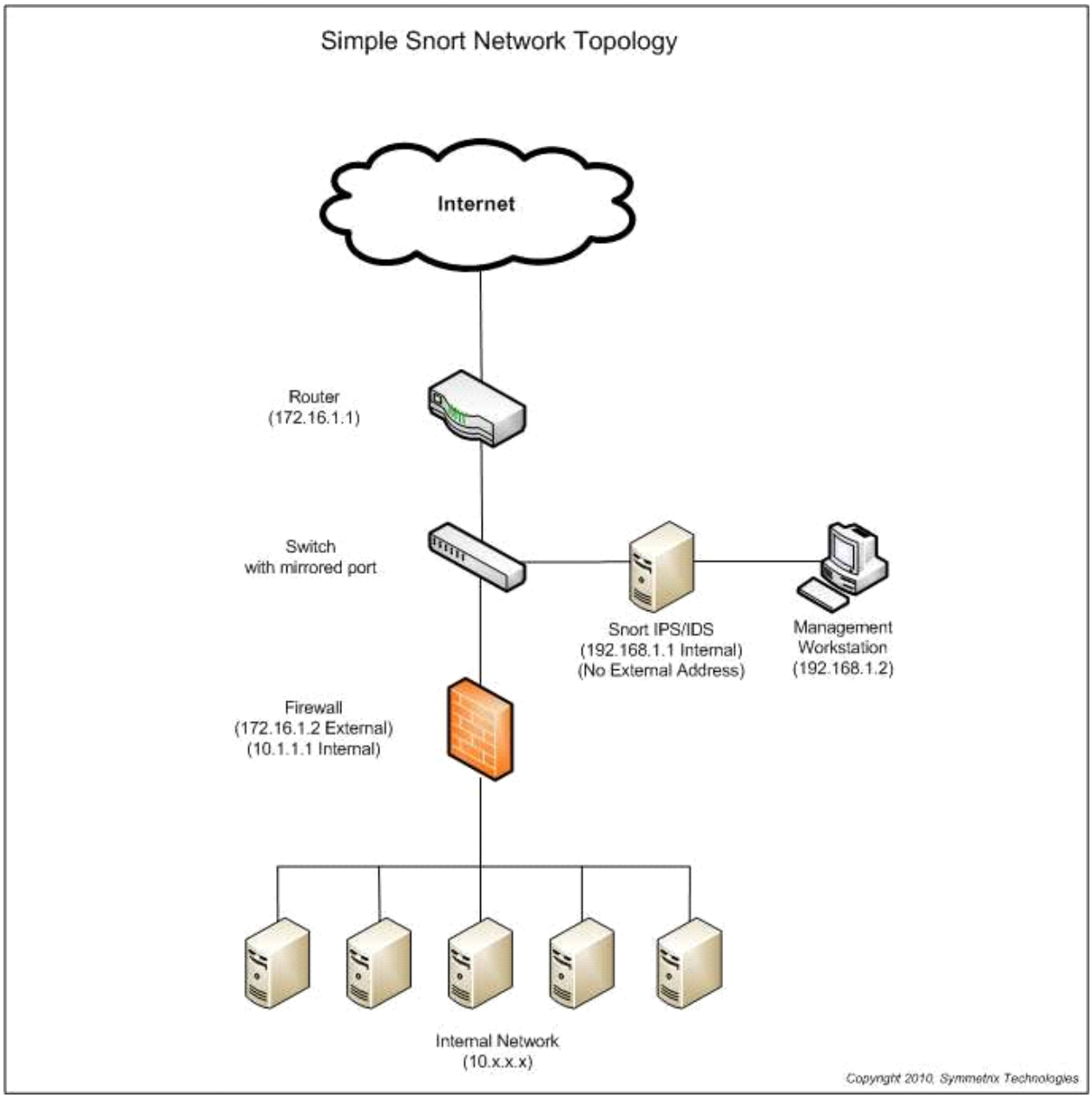
SNORT
Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) created by Martin Roesch in 1998. Snort is now developed by Sourcefire, of which Roesch is the founder and CTO. In 2009, Snort entered InfoWorld's Open Source Hall of Fame as one of the "greatest [pieces of] open source software of all time".

Snort's open source network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching, and content matching. These basic services have many purposes including application-aware triggered quality of service, to de-prioritize bulk traffic when latency-sensitive applications are in use.

The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans.

Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the

program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.



Procedure/ Algorithm :

Snort Installation:

Results :

References :

1. http://en.wikipedia.org/wiki/Snort_(software)
2. http://www.informit.com/articles/article.aspx?p=101171&seqNum=2
3. *https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids*
4. *2. https://www.techopedia.com/definition/3988/intrusion-detection-system-ids*
5. *3. https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799*
6. *4. http://searchmidmarketsecurity.techtarget.com/definition/Snort*

Lab practice (optional) :

Questions (Short, Long, MCQs) (optional) :

Experiment No. : 10

Date: _____

Title :

Problem Definition :

Pre-requisite :

Theory :

Procedure/ Algorithm :