Network Traffic Monitoring with Attacks and Intrusion Detection System

Vivek Kumar Pathak[#1], Shabad Sawhney[#2], Vyom Bhatia[#3], Maitraiye Saxena[#4]

[#]*Department of Information Technology, SRM University, Delhi- NCR Campus,*
Ghaziabad, U.P., India

[1]vivek18pathak@gmail.com
[2]shabadsawhney007@gmail.com
[3]bhatia.vyom25@gmail.com
[4]mitisaxena8@gmail.com

Abstract— Every organization, irrespective of its size depends on networking technologies. These networks hold the working of entire organization and thus are very important part of the organization. Being the backbone of the business, it is vulnerable to attacks from crackers and rival organizations to gain unauthorized information or to cause harm to the business of the organization. Our aim is to protect the network infrastructure of the organization by developing a software to monitor the network and detect malicious activities on it. We also demonstrate the working of the software by developing different attacks to crack into the network infrastructure. 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 an administrator, whereas network traffic monitoring is the process of reviewing, analysing and managing network traffic for any abnormality or process that can affect network performance, availability and/or security.

Keywords— **Network, Network Security, IDS (intrusion detection system), Network Traffic Monitoring.**

I. Introduction

A. *Statement of Problem*

Security is a big issue for all networks in today’s environment. Intruders can attack the system by any means to get unauthorized data or affect the performance of the network. With networking technologies and services evolving rapidly, accurate network traffic monitoring is required to ensure the security and optimize the efficiency of our networks.

B. *Intrusion Detection System*

The purpose of the IDS is to detect certain well known intrusion attacks on the host system and display warnings to the user and also store information regarding the IP addresses and allow the traffic based on that information.

C. *Network Traffic Monitoring*

Network Traffic Monitor is a network analytic tool that examines network usage and provides a display of its statistics [1]. The purpose of the application is monitoring the IP traffic within the network and report to the administrator in case of abnormality. Network traffic monitoring and measurement is increasingly regarded as an essential function for understanding and improving the performance and security of the network infrastructure.

II. Literature Survey

A. *Basic Terminology*

1) Intrusion: An unauthorised entry into a network or a system, frequently synonymous with an information technology security incident.

2) Network Traffic: Incoming and outgoing packets generating traffic.

3) Attacks: Any method, process, or means used to maliciously attempt to compromise network security.

B. *Need*

Any network is vulnerable to attacks from crackers and rival organizations to gain unauthorized information or to cause harm to the business of the organization. Here arises a need to protect the network from such attacks and create a safe environment where the data and all the internal working of the organisation are safeguarded.

C. *NIDS*

Network based Intrusion Detection System (NIDS) is a system which monitors network intrusion. Intrusion may be detected by techniques like anomaly detection, signature pattern matching etc [2].

D. *Network Traffic Monitoring*

Network Traffic Monitoring Network Traffic Monitor is a network analytic tool that examines a network usage and provides a display of its statistics [3]. The main purpose of the application is monitoring the IP traffic between your local area network and Internet. Network Monitor is a network diagnostic tool that monitors local area networks and provides a graphical display of network statistics. Network administrators can use these statistics to perform routine trouble- shooting tasks, such as locating a server that is down, or that is receiving a disproportionate number of work requests. The process by which Network Monitor collects this information is called capturing.

III. DESCRIPTION OF MODULES

A. *Attack Module*

Attacks are developed in the project for the purpose of demonstration of NIDS. Attacks disturb the security infrastructure of the network. Following attacks have been incorporated:

1) DoS: A denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

2) DDoS: Distributed Denial of Service is a type of DoS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.

3) SYN Flood: A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

4) Brute Force Attack: A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data

5) Slowloris: Slowloris is a type of denial of service attack invented by Robert "RSnake" Hansen which allows a single machine to take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports.

B. *Network Traffic Monitoring Module*

Network traffic monitoring is the process of reviewing, analysing and managing network traffic for any abnormality or process that can affect network performance, availability and/or security. It is a network management process that uses various tools and techniques to study computer network-based communication/data/packet traffic. The key objective behind network traffic monitoring is to ensure availability and smooth operations on a computer network. Network monitoring incorporates network sniffing and packet capturing techniques in monitoring a network. Network traffic monitoring generally requires reviewing each incoming and outgoing packet [4].

C. *Intrusion Detection Module*

Intrusion detection is a process that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.

D. *Integration and User Interface*

Graphical user interface is used to combine various tools used for attacking and managing the network under a single roof, using tkinter.

IV. Platform Used

A. *Python 2.7*

Python interpreters are available for installation on many operating systems, allowing Python code execution on a wide variety of systems.

B. *Virtual Environment*

Virtual Environment is required to run multiple Operating Systems simultaneously to create a network infrastructure. VMWare is a popular software used for creating a virtual environment.

V. Implementation

To implement our network monitoring system, we run the agent in the windows machine and monitor the agent through a program running in Ubuntu. The agent will keep reporting to the monitoring program through socket connection.

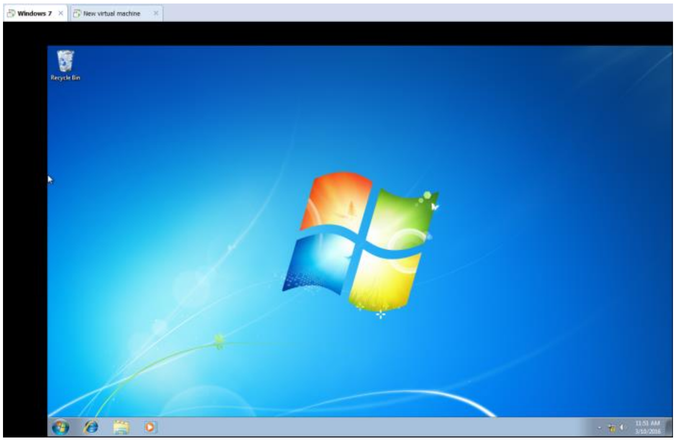


Fig. 1. *Windows running on virtual environment Specification- RAM: 512 MB, HD space: 6GB*

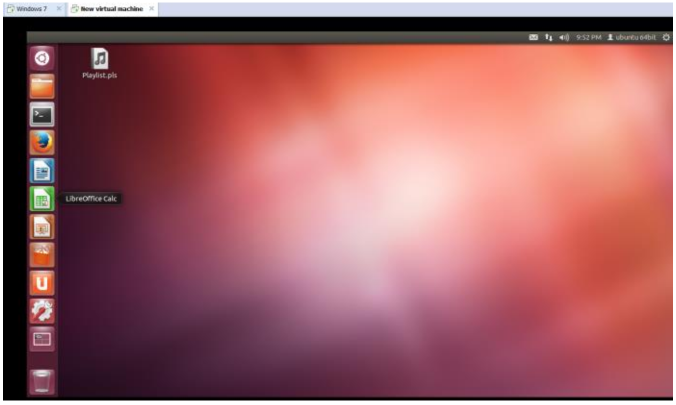
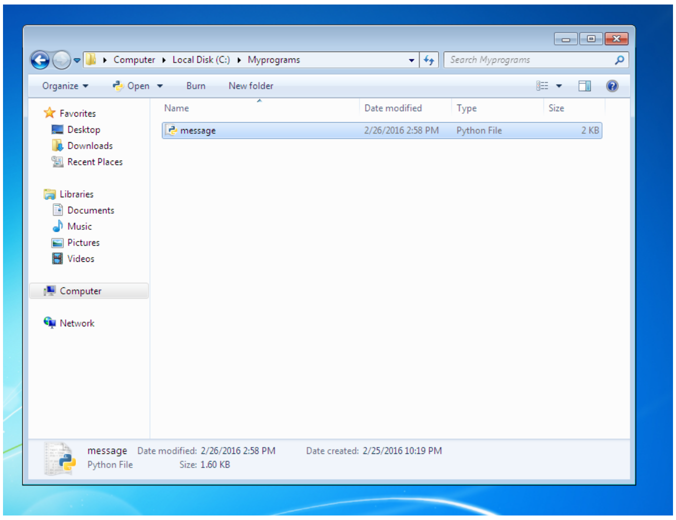


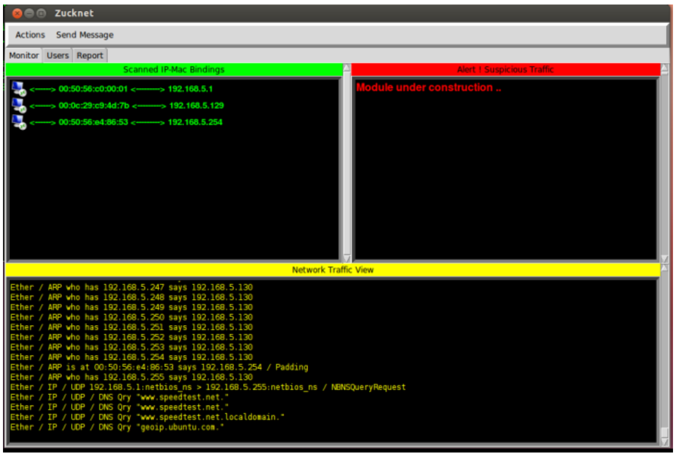
Fig. 2. *Ubuntu running on virtual environment. Widows and Ubuntu run simultaneously. Specification- RAM 1512 MB, HD space: 20GB*



Name	Date modified	Type	Size
message	2/26/2016 2:58 PM	Python File	2 KB

message Date modified: 2/26/2016 2:58 PM Date created: 2/25/2016 10:19 PM
Python File Size: 1.60 KB

Fig. 3. *Windows running agent program message.py*

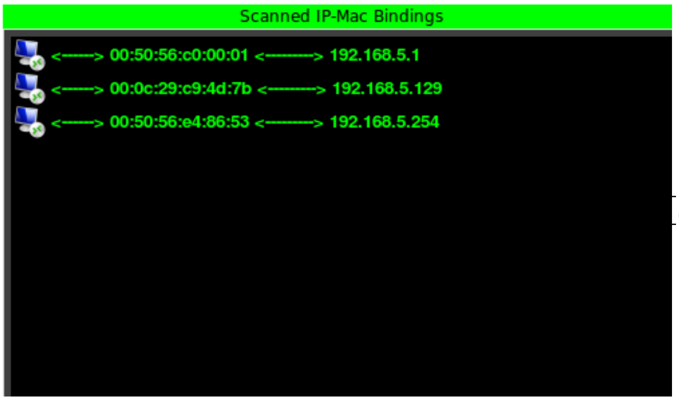


```
<——> 00:50:56:c0:00:01 <———> 192.168.5.1
<——> 00:0c:29:c9:4d:7b <———> 192.168.5.129
<——> 00:50:56:e4:86:53 <———> 192.168.5.254
```

Module under construction ..

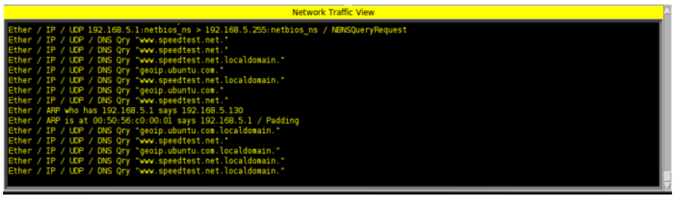
```
Ether / ARP who has 192.168.5.247 says 192.168.5.130
Ether / ARP who has 192.168.5.248 says 192.168.5.130
Ether / ARP who has 192.168.5.249 says 192.168.5.130
Ether / ARP who has 192.168.5.250 says 192.168.5.130
Ether / ARP who has 192.168.5.251 says 192.168.5.130
Ether / ARP who has 192.168.5.252 says 192.168.5.130
Ether / ARP who has 192.168.5.253 says 192.168.5.130
Ether / ARP who has 192.168.5.254 says 192.168.5.130
Ether / ARP is at 00:50:56:e4:86:53 says 192.168.5.254 / Padding
Ether / ARP who has 192.168.5.255 says 192.168.5.130
Ether / IP / UDP 192.168.5.1:netbios_ns > 192.168.5.255:netbios_ns / NBNSQueryRequest
Ether / IP / UDP / DNS Qry "www.speedtest.net."
Ether / IP / UDP / DNS Qry "www.speedtest.net."
Ether / IP / UDP / DNS Qry "www.speedtest.net.localdomain."
Ether / IP / UDP / DNS Qry "geoip.ubuntu.com."
```

Fig. 4. Linux running production2.py which is our monitoring system



```
<------> 00:50:56:c0:00:01 <---------> 192.168.5.1
<------> 00:0c:29:c9:4d:7b <---------> 192.168.5.129
<------> 00:50:56:e4:86:53 <---------> 192.168.5.254
```

Fig. 5. *Interface snap: ARP to associate the IP address to MAC addresses*



```
Ether / IP / UDP 192.168.5.1:netbios_ns > 192.168.5.255:netbios_ns / NBNSQueryRequest
Ether / IP / UDP / DNS Qry "www.speedtest.net."
Ether / IP / UDP / DNS Qry "www.speedtest.net."
Ether / IP / UDP / DNS Qry "www.speedtest.net.localdomain."
Ether / IP / UDP / DNS Qry "geoip.ubuntu.com."
Ether / IP / UDP / DNS Qry "www.speedtest.net.localdomain."
Ether / IP / UDP / DNS Qry "geoip.ubuntu.com."
Ether / IP / UDP / DNS Qry "www.speedtest.net."
Ether / ARP who has 192.168.5.1 says 192.168.5.130
Ether / ARP is at 00:50:56:c0:00:01 says 192.168.5.1 / Padding
Ether / IP / UDP / DNS Qry "geoip.ubuntu.com.localdomain."
Ether / IP / UDP / DNS Qry "www.speedtest.net."
Ether / IP / UDP / DNS Qry "geoip.ubuntu.com.localdomain."
Ether / IP / UDP / DNS Qry "www.speedtest.net.localdomain."
Ether / IP / UDP / DNS Qry "www.speedtest.net.localdomain."
```

Fig. 6. *Interface snap: Live Traffic monitoring*

VI. CONCLUSION

Intrusion Detection System on any network is capable of detecting malicious activities. In such a case the administrator of a network would be able to track the source system which is trying to attack. Network monitoring devices also notify the administrator in case of an attack. The administrator is also notified about the active users and their activities on the network infrastructure. Organisations may employ some white hat or ethical hackers to conduct some methods in order to breach the security of the organization but in mind they are not always driven by the same motivation, no matter the end goal. So we provide a network security environment to deal with the hazardous scenarios for the network infrastructure of the organization.

REFERENCES

[1] Amit Kumar, Harish Chandra Maurya, Rahul Misra (April 2013). "A Research Paper on Hybrid Intrusion Detection System". International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958

[2] Brajesh Patel, Amrita Anand (August 2012). “An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols”. International Journal of Advanced Research in Computer Science and Software Engineering. ISSN: 2277 1285

[3] Radha S. Shirbhate, Pallavi A. Patil (January 2012). “Network Traffic Monitoring Using Intrusion Detection System”. International Journal of Advanced Research in Computer Science and Software Engineering. ISSN: 2277 1284

[4] Python Programming Training, 2012. Author: Mike McMillan