I. USER MANUAL

CONTENTS

1. INTRODUCTION

The User Manual contains all essential information for the user to make full use of the information system. This manual includes a description of the system functions and capabilities, contingencies and alternate modes of operation, and step-by-step procedures for system access and use.

1.1 Purpose and Scope

The purpose of this document is to describe the functionality of Network Traffic Monitoring with Attack and Intrusion Detection System.

1.2 List of all the players who impacted the solution

Vyom Bhatia

MaitraiyeSaxena

ShabadSawhney

Vivek Pathak

1.3 Points of Contact

Our team can be contacted at any time

- +91 9999230611, +91 7838112069, +91 9717171504, +91 +91 8267873980
- bhatia.vyom25@gmail.com, mitisaxena8@gmail.com, shabadsawhney007@gmail.com, vivek18pathak@gmail.com

Our team will be in touch via e-mail through entire token validation period to avoid excessive telephony.

1.4 Project 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

1.5 Primary Business Functions

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.

1.6 Glossary

Msg	Message
Admin	Administrator
IP	Internet Protocol
DoS	Denial of Service
DDoS	Distributed Denial of Service

IDS	Intrusion Detection System
NIDS	Network Intrusion Detection System
ARP	Address Resolution Protocol

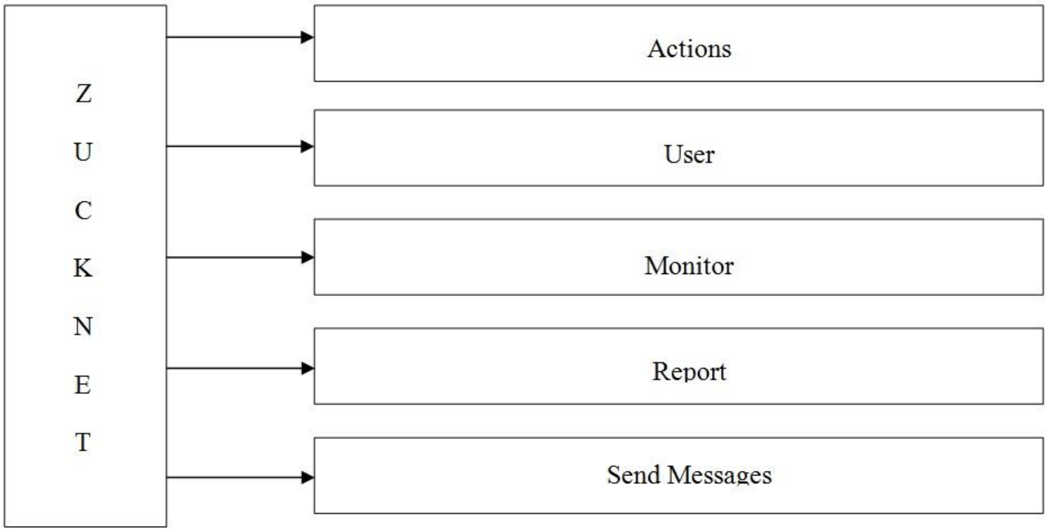
2. SYSTEM CAPABILITIES

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.

2.1 Purpose

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.

3. DESCRIPTION OF SYSTEM FUNCTIONS



There are 5 basic functions

- Actions
- Send message
- Monitor
- Users
- Report

3.1 Functions

3.1.1 Actions: Actions will contain refresh sub button that will help to refresh our IP systems scan.

3.1.2 Send Message and users: Send msg contains two sub buttons one for broadcasting amsg one for sending msg to particular user by admin. The button when clicked will pop up a window in which admin can type msg and send it to the user(s).

3.1.3 Monitor: Monitor will help the show the live traffic monitoring and also the unwanted traffic generated by an attacker.

3.1.4 Report: Report tab helps the user to graphically analyze the traffic in the network with the help of histograms.

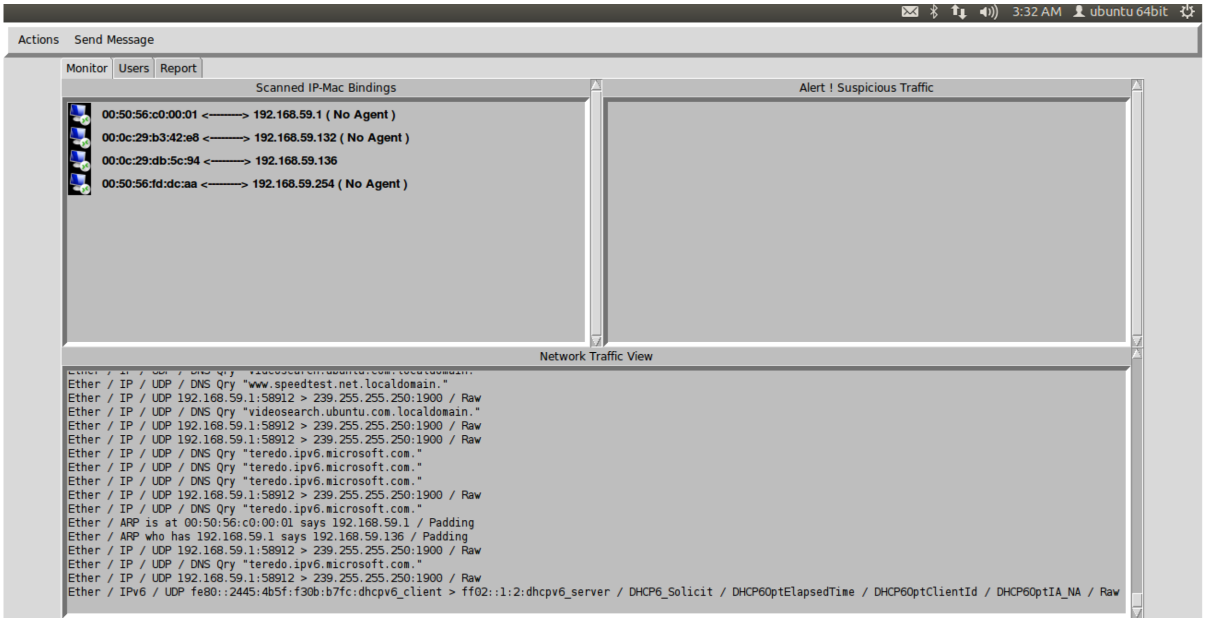
3.2 Detailed Description of Functions

This section provides a description of each function. Include the following, as appropriate:

- Initialization of the function
  - Click various tabs in the tool bar
- Execution options
  - Actions: Hit refresh button to refresh IP scan
  - Send message: (admin purpose only) allows to send message from one system to another
  - Monitor: Default tab
  - Report: Click on report tab to graphically analyze the histograms.

3.3 Results

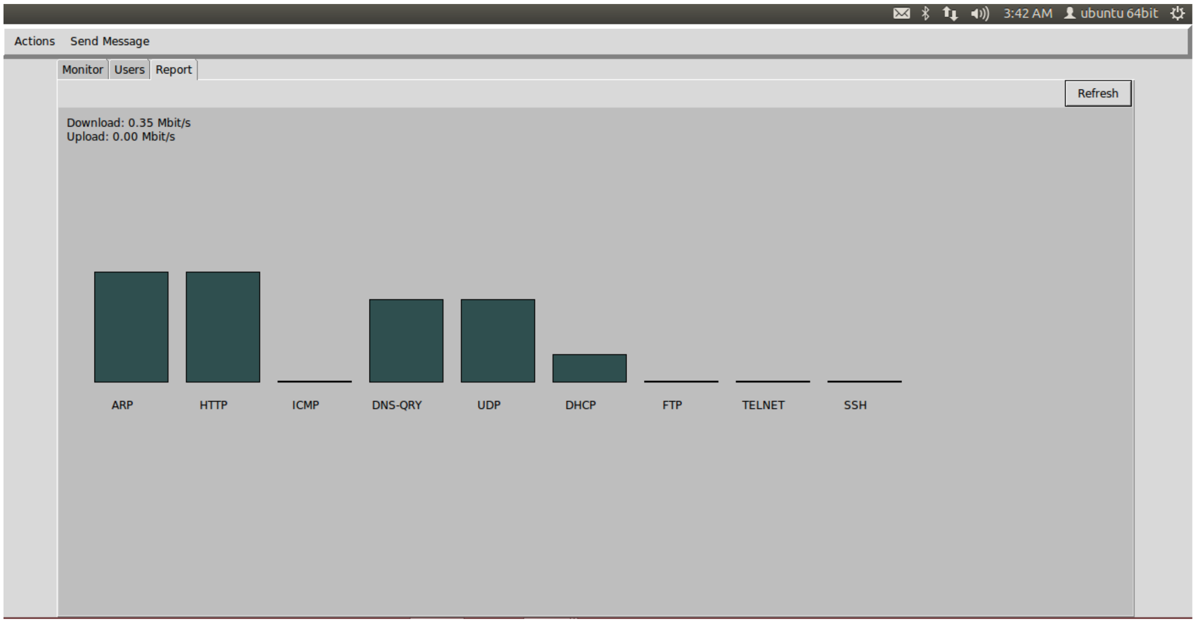
This section describes expected results of the function.



00:50:56:c0:00:01 <---------> 192.168.59.1 (No Agent)
00:0c:29:b3:42:e8 <---------> 192.168.59.132 (No Agent)
00:0c:29:db:5c:94 <---------> 192.168.59.136
00:50:56:fd:dc:aa <---------> 192.168.59.254 (No Agent)

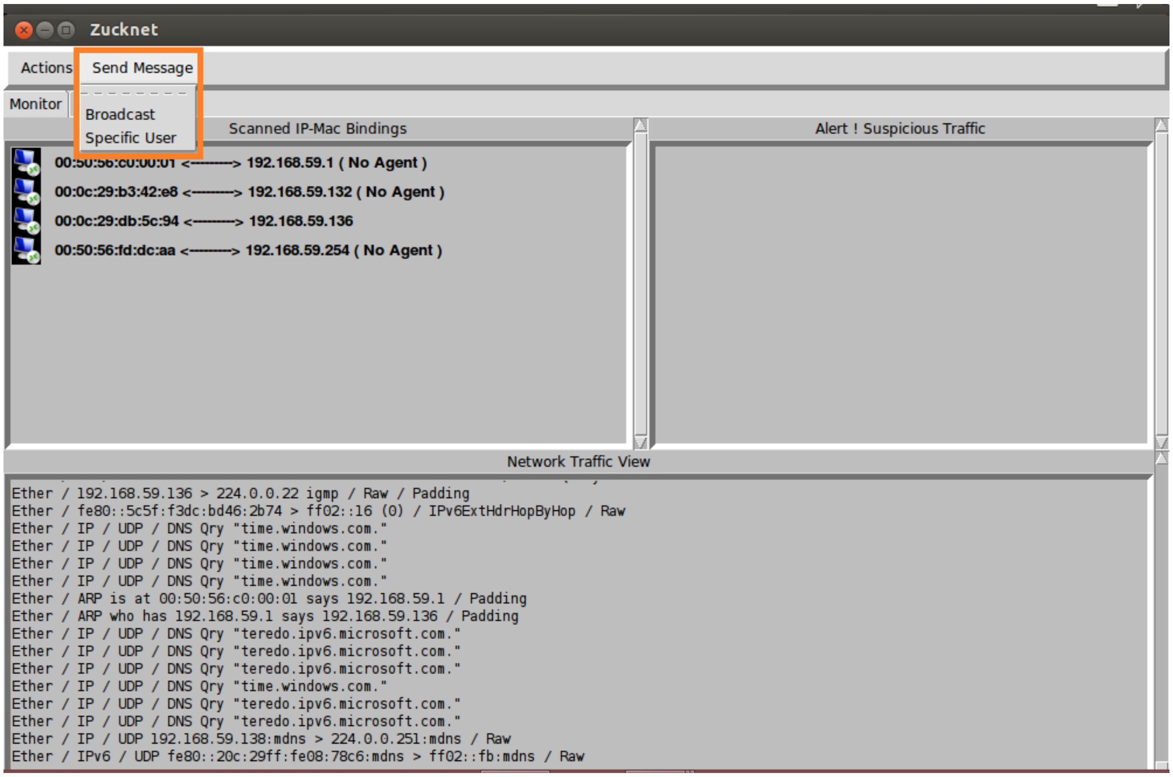
```
Ether / IP / UDP / DNS Qry "www.speedtest.net.localdomain."
Ether / IP / UDP 192.168.59.1:58912 > 239.255.255.250:1900 / Raw
Ether / IP / UDP / DNS Qry "videosearch.ubuntu.com.localdomain."
Ether / IP / UDP 192.168.59.1:58912 > 239.255.255.250:1900 / Raw
Ether / IP / UDP 192.168.59.1:58912 > 239.255.255.250:1900 / Raw
Ether / IP / UDP / DNS Qry "teredo.ipv6.microsoft.com."
Ether / IP / UDP / DNS Qry "teredo.ipv6.microsoft.com."
Ether / IP / UDP / DNS Qry "teredo.ipv6.microsoft.com."
Ether / IP / UDP 192.168.59.1:58912 > 239.255.255.250:1900 / Raw
Ether / IP / UDP / DNS Qry "teredo.ipv6.microsoft.com."
Ether / ARP is at 00:50:56:c0:00:01 says 192.168.59.1 / Padding
Ether / ARP who has 192.168.59.1 says 192.168.59.136 / Padding
Ether / IP / UDP 192.168.59.1:58912 > 239.255.255.250:1900 / Raw
Ether / IP / UDP / DNS Qry "teredo.ipv6.microsoft.com."
Ether / IP / UDP 192.168.59.1:58912 > 239.255.255.250:1900 / Raw
Ether / IPv6 / UDP fe80::2445:4b5f:f30b:b7fc:dhcpv6_client > ff02::1:2:dhcpv6_server / DHCP6_Solicit / DHCP6OptElapsedTime / DHCP6OptClientId / DHCP6OptIA_NA / Raw
```

Startup Scan with MAC IP Address binding and Live Traffic Monitoring



Download: 0.35 Mbit/s
Upload: 0.00 Mbit/s

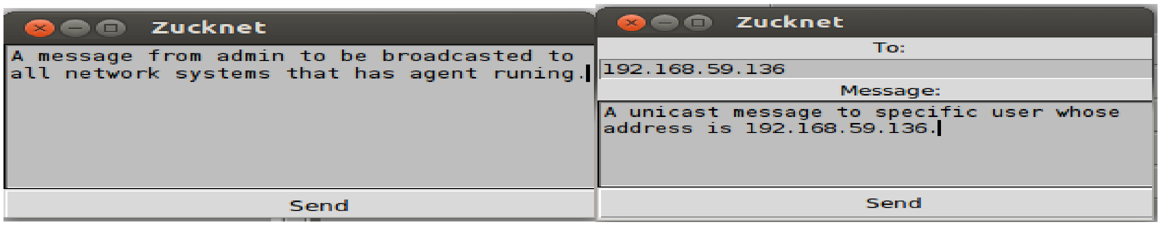
Report Histogram for Manual Analysis



00:50:56:c0:00:01 <---------> 192.168.59.1 (No Agent)
00:0c:29:b3:42:e8 <---------> 192.168.59.132 (No Agent)
00:0c:29:db:5c:94 <---------> 192.168.59.136
00:50:56:fd:dc:aa <---------> 192.168.59.254 (No Agent)

```
Ether / 192.168.59.136 > 224.0.0.22 igmp / Raw / Padding
Ether / fe80::5c5f:f3dc:bd46:2b74 > ff02::16 (0) / IPv6ExtHdrHopByHop / Raw
Ether / IP / UDP / DNS Qry "time.windows.com."
Ether / IP / UDP / DNS Qry "time.windows.com."
Ether / IP / UDP / DNS Qry "time.windows.com."
Ether / IP / UDP / DNS Qry "time.windows.com."
Ether / ARP is at 00:50:56:c0:00:01 says 192.168.59.1 / Padding
Ether / ARP who has 192.168.59.1 says 192.168.59.136 / Padding
Ether / IP / UDP / DNS Qry "teredo.ipv6.microsoft.com."
Ether / IP / UDP / DNS Qry "teredo.ipv6.microsoft.com."
Ether / IP / UDP / DNS Qry "teredo.ipv6.microsoft.com."
Ether / IP / UDP / DNS Qry "time.windows.com."
Ether / IP / UDP / DNS Qry "teredo.ipv6.microsoft.com."
Ether / IP / UDP / DNS Qry "teredo.ipv6.microsoft.com."
Ether / IP / UDP 192.168.59.138:mdns > 224.0.0.251:mdns / Raw
Ether / IPv6 / UDP fe80::20c:29ff:fe08:78c6:mdns > ff02::fb:mdns / Raw
```

Send Message Tab

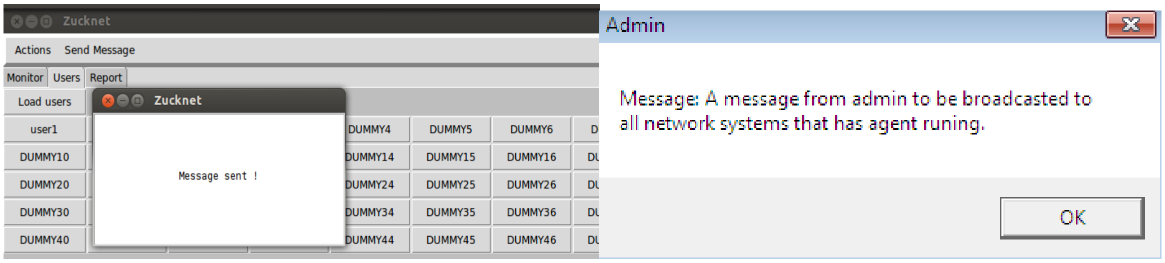


A message from admin to be broadcasted to all network systems that has agent runing.

To: 192.168.59.136

Message: A unicast message to specific user whose address is 192.168.59.136.

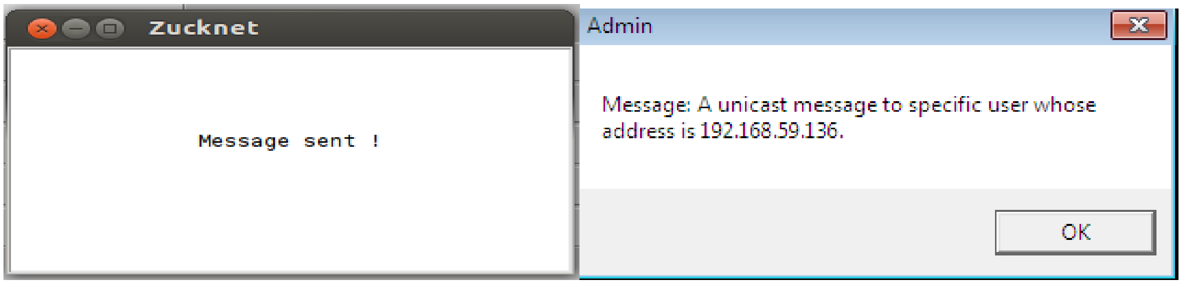
Broadcast and Unicast a Message



Message sent !

Message: A message from admin to be broadcasted to all network systems that has agent runing.

Broadcast Message Sent and Received



Message sent !

Message: A unicast message to specific user whose address is 192.168.59.136.

Unicast Message Sent and Received

4. OPERATING INSTRUCTIONS

This section provides detailed, step-by-step system operating instructions.

4.1 Initiate Operation

You need to install python from python.org to run our software on your platform. If you are using any Linux based operating system, the python will be pre-installed in your OS. For further details about installing python for your OS, refer the installation documentation at https://www.python.org/

- Download our programs from http://www.tinyurl.com/PIT1530
- Copy them into the python folder
- For windows, run command prompt as an administrator and type “python production3.py”
- For Linux, open terminal and type “sudo python production3.py”
- Terminal will prompt for root password
- Enter root password

4.2 Maintain Operation

Do not close either the command prompt/ terminal or the running windows for maintaining the operation.

4.3 Terminate and Restart Operation

This section defines procedures for normal and unscheduled termination of the system operations and should define how to restart the system.

- Press Ctrl+C in command prompt/ terminal to terminate the operation.

Refer section 4.1 to initiate the process again.

5. ERROR HANDLING

This section should address error message and help facilities.

The only known bug that we came across is when we run the program in Ubuntu OS platform which stops live traffic monitoring from happening. If you encounter any such problem, refer section 4.3 to restart operations.

5.1 Help Facilities

- +91 9999230611, +91 7838112069, +91 9717171504, +91 +91 8267873980
- bhatia.vyom25@gmail.com, mitisaxena8@gmail.com, shabadsawhney007@gmail.com, vivek18pathak@gmail.com

Our team will be in touch via e-mail through entire token validation period to avoid excessive telephony.

End of document