

## **II. SOFTWARE MANUAL**

## **PURPOSE OF THE DOCUMENT**





The purpose of this document is to describe the functionality of Network Traffic Monitoring with Attack and Intrusion Detection System. 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. The aim of the project is to protect the network infrastructure of the organization by developing a software to monitor the network and detect malicious activities on it. In order to demonstrate the working of the software, different attacks have been developed 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 the administrator, whereas network traffic monitoring is the process of sniffing, reviewing, analysing and managing network traffic for any abnormality or process that can affect network performance, availability and/ or security.

## **CONTENTS**

	PURPOSE OF THE DOCUMENT	2
1	ICONS USED IN THE MANUAL	4
2	PRESENTATION OF THE SOLUTION	5
	2.1 Brief Description	5
	2.2 Descriptive Icons	5
	2.3 Project Players	5
	2.4 Support	6
	2.5 Referenced Documentation	6
	2.6 History of the Solution	7
3	CONNECTING TO THE APPLICATION	10
	3.1 Address	10
4	STRUCTURING OF THE APPLICATION	11
	4.1 Layout	11
	4.2 Menus	14
	4.3 Icons/Shortcuts	15
	4.4 Functionalities	15
	4.4.1 Functionalities Described	15
5	FUNCTIONS	17
	5.1 Screenshots	17
	5.2 Descriptions of Fields, Content	17
6	APPENDICES	19
	6.1 Appendix 1	19

## 1. ICONS USED IN THE MANUAL

Throughout this document, the pictograms below are used to underline points or important notions.

	Important information
	Good to know – Tricks
	Mandatory action
	Actions reserved for the user

## **2. PRESENTATION OF THE SOLUTION**

### **2.1 Brief Description**

The aim is to protect the network infrastructure of the organization by developing various tools to manage their network and club the tools under single software and also demonstrate the working of the tools by developing different attacks to crack into the network infrastructure. Companies 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 the system provides a network security environment to deal with the hazardous scenarios for the network infrastructure of the organization.

### **2.2 Descriptive Icons**



MAC-IP address association via ARP

### **2.3 Project Players**

Vyom Bhatia  
Maitraiye Saxena  
Shabad Sawhney  
Vivek Pathak

## 2.4 Support

+91 9999230611, +91 7838112069, +91 9717171504, +91 +91 8267873980

[bhatia.vyom25@gmail.com](mailto:bhatia.vyom25@gmail.com), [mitisaxena8@gmail.com](mailto:mitisaxena8@gmail.com), [shabadsawhney007@gmail.com](mailto:shabadsawhney007@gmail.com),  
[vivek18pathak@gmail.com](mailto:vivek18pathak@gmail.com)

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

## 2.5 Referenced Documentation

1. Joao B. D. Cabrerat B. Ravichandran and K. Raman Mehra *Statistical Traffic Modeling for Network Intrusion Detection*, 2001
2. J. B. D. Cabrera, Handran B., and R. K. Mehra. *Data Classification and Data Clustering Algorithms for intrusion detection on Computer Networks*. Technical Report AFRL-IS-TR-2000-51, Air Force Research Laboratory, Information Directorate, Rome, NY, April 2000.
3. Emerald Project. *EMERALD TCP Statistical Analyser 1998 Evaluation Results*, 1999. Available at <http://www.sdl.sri.com/emerald98-evalestat/index.html>
4. S. Floyd and V. Paxson. *Why we do not know how to simulate the Internet*, October 1999. Available at <http://www.aciri.org/floyd/papers.html>
5. Graf, R. Lippmann, R. Cunningham, D. Fried, K. Kendall, S. Webster, and M. Zissman. *Results of J998 Offline DARPA Intrusion Detection Evaluation*. December 1998. DARPA PI Meeting slides available at <http://videval.ll.mit.edu>
6. K. Kendall. *A database of computer attacks for the evaluation of detection systems*. Master's thesis, Massachusetts Institute of Technology, June 18, 1999

7. Lee, S. J. Stolfo, and K. W Mok, *A data mining framework for building intrusion detection models*. In Proceedings of the IEEE Symposium on Security and Privacy, 1999
8. W Lee, S. J. Stolfo, and K. W. Mok. *Mining in a flow environment: Experience on network intrusion detection*. In Proceedings of the Conference on knowledge discovery and databases, 1999
9. Shaik Akbar Assoc. Profr, Dept. of C.S.E, SVIET, Nandamuru, Krishna Dist, Andhra Pradesh, India Dr.K.Nageswara Rao Prof & H.O.D, Dept. of C.S.E P.V.P.S.I.T, Vijayawada, Krishna Dist, Andhra Pradesh, India Dr.J.A.Chandulal Prof, Dept. of C.S.E GITAM University, Visakhapatnam, Andhra Pradesh, India, *Intrusion Detection System Methodologies Based on Data Analysis*, International Journal of Computer Applications (0975 – 8887) Volume 5– No.2, August 2010
10. Honeywell International Inc. *Method and system for monitoring and evaluating user activity in computer systems*, WO2004049251A2
11. Alcatel AlsthomCompagnieGeneraleD'electricite, *Facility for detecting intruders and suspect callers in a computer installation and a security system including such a facility*, US5621889

## 2.6 History of the Solution

### A. 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 networkbased 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.

#### B. Attack and 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. Attacks will also be detected. Attacks disturb the security infrastructure of the network. Security against 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) 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.

3) 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

4) DNS Spoofing: DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer).

5) MAC Flooding: MAC flooding is a technique employed to compromise the security of network switches. Switches maintain a MAC Table that maps individual MAC addresses on the network to the physical ports on the switch.

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.



### C. 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.

### **3. CONNECTING TO THE APPLICATION**

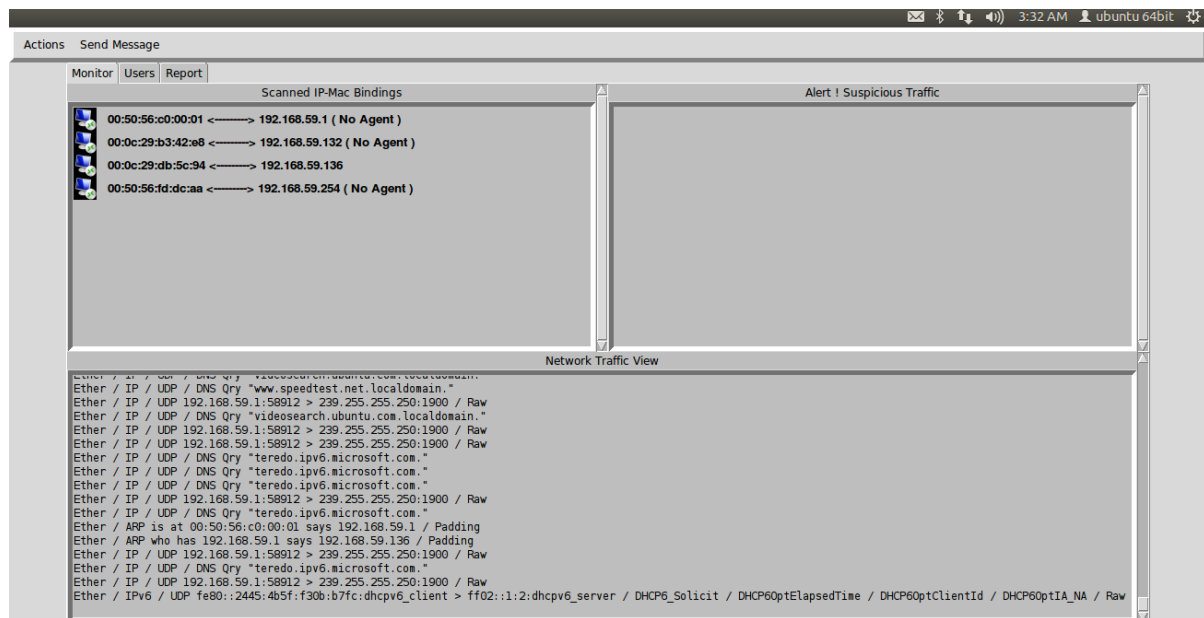
#### **3.1 Address**

You must connect to the application using the following address: <https://www.tinyurl.com/PIT1530>



## 4. STRUCTURING OF THE APPLICATION

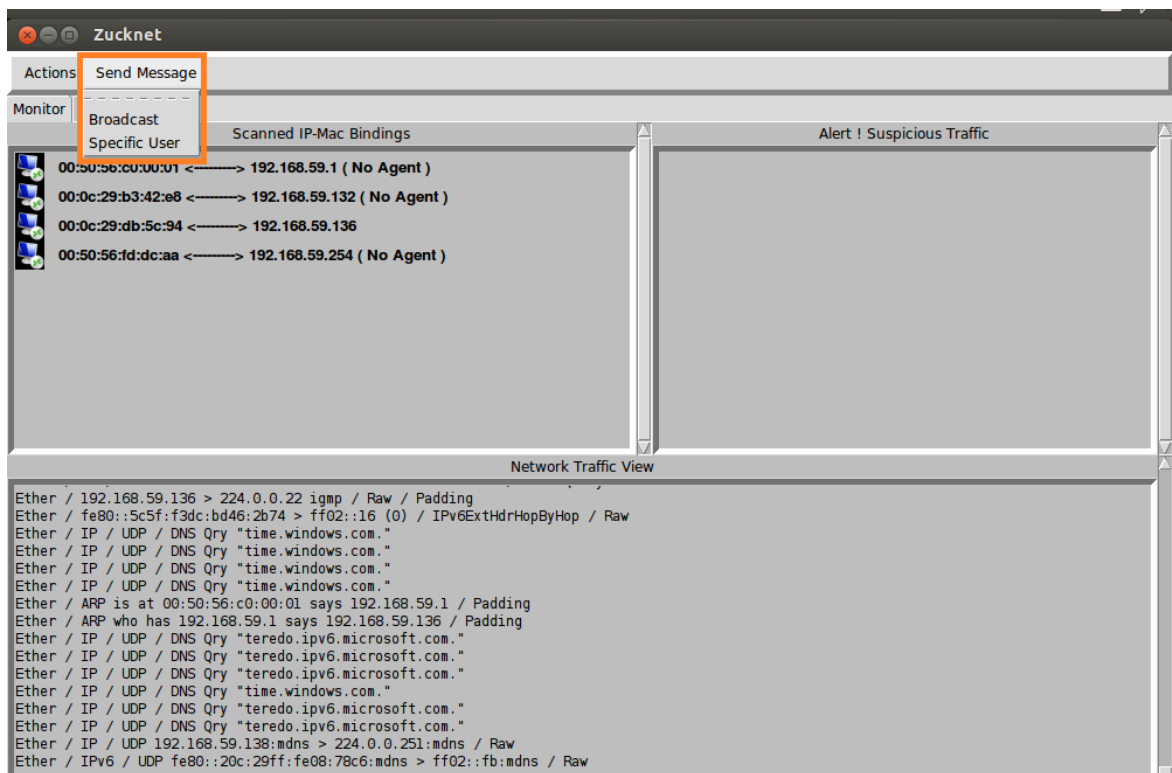
## 4.1 Layout



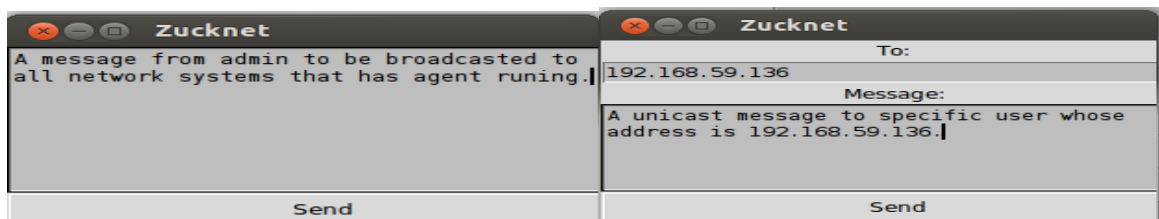
## Startup Scan with MAC IP Address binding and Live Traffic Monitoring



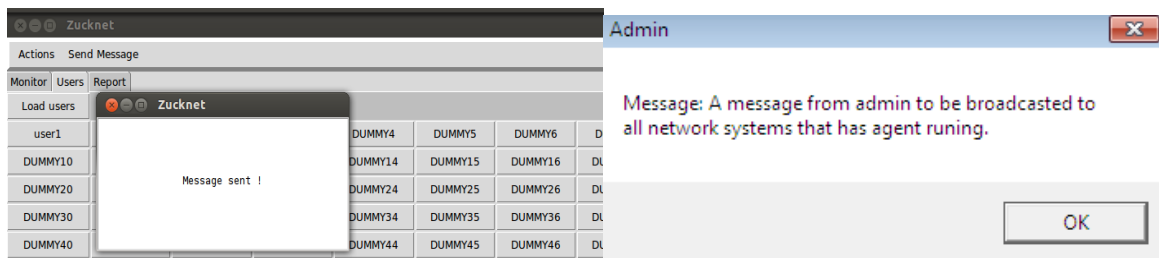
## Report Histogram for Manual Analysis



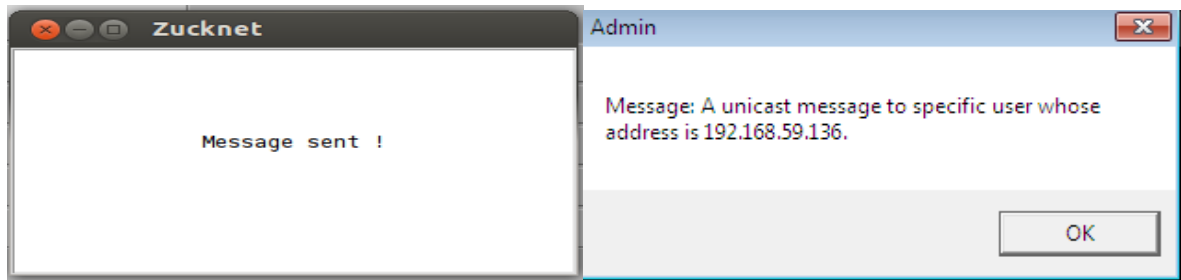
Send Message Tab



Broadcast and Unicast a Message



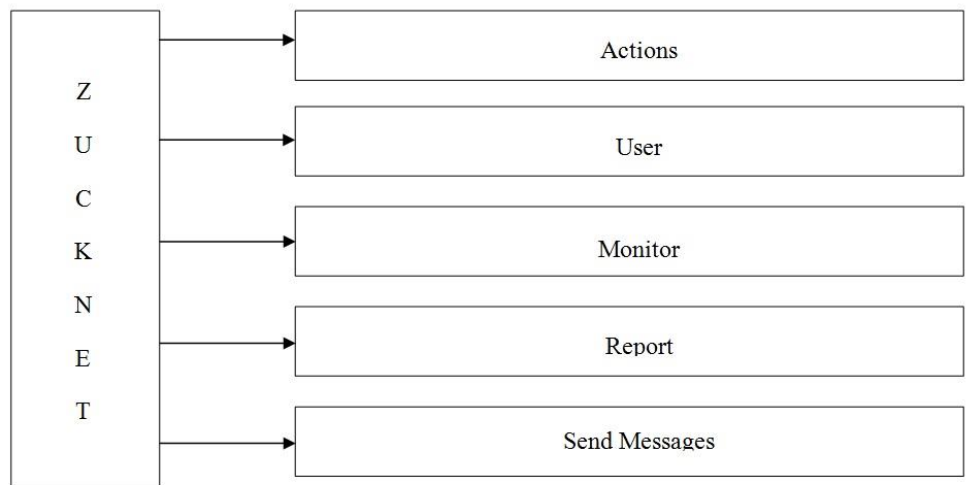
Broadcast Message Sent and Received




Unicast Message Sent and Received

The main program Zucknet has following 5 tabs, actions, send message, monitor, users and report.

## 4.2Menus





**1) Actions:** Actions will contain refresh sub button that will help to refresh our IP systems scan

Send Message and users: Send msg contains two sub buttons one for broadcasting a msg 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). 

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

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

### 4.3 Icons/Shortcuts

	MAC-IP address association via ARP
 [CTRL]+[ALT]+T	Open terminal in linux

### 4.4 Functionalities

#### 4.4.1 Functionalities Described

##### **A. 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 networkbased 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.

##### **B. Attack and 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. . Attacks will also be detected. Attacks disturb the security infrastructure of the network. Security against 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) 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.

3) 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

4) DNS Spoofing: DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer).

5) MAC Flooding: MAC flooding is a technique employed to compromise the security of network switches. Switches maintain a MAC Table that maps individual MAC addresses on the network to the physical ports on the switch.

### **C. 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.



## 5. FUNCTION

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.

### 5.1 Screenshots

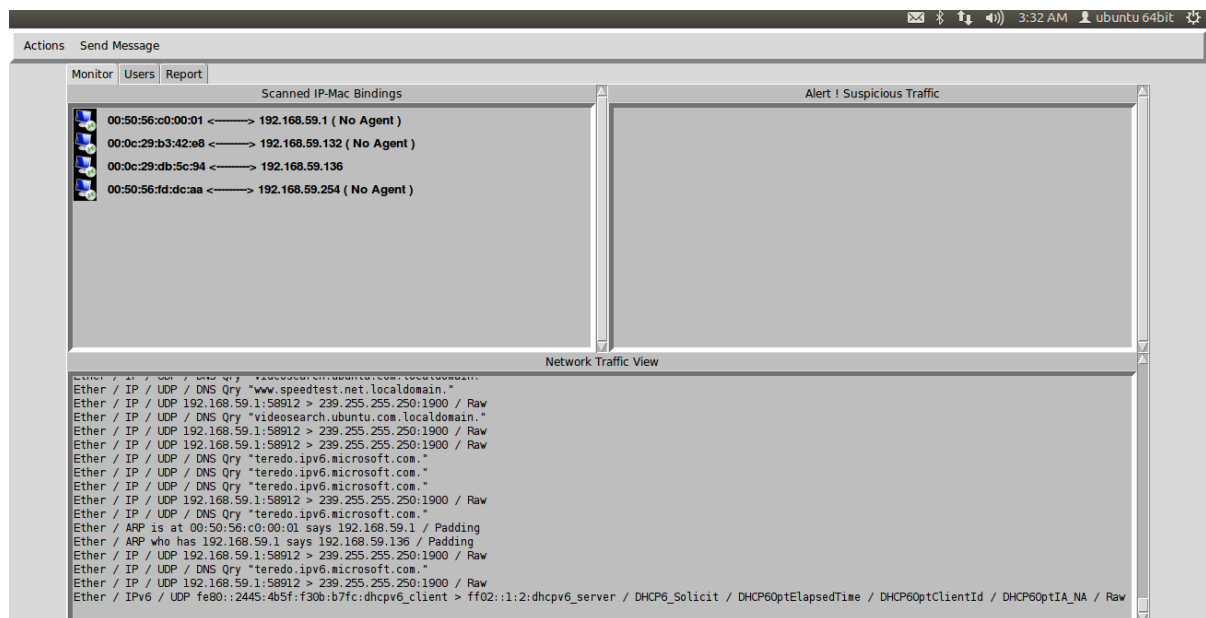



Figure 5.3. Startup Scan with MAC IP Address binding and Live Traffic Monitoring

### 5.2 Description of Fields, Content

1) Actions: Actions will contain refresh sub button that will help to refresh our IP systems scan

Send Message and users: Send msg contains two sub buttons one for broadcasting a msg 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). 

- 2) Monitor: Monitor will help the show the live traffic monitoring and also the unwanted traffic generated by an attacker.
- 3) Report: Report tab helps the user to graphically analyze the traffic in the network with the help of histograms.

## 6. APPENDICES

### 6.1 Appendix 1

Address	4
Brief Description	2
Description of Field Contents	8
Descriptive Icons	2
Functionalities	5
History of the Solution	3
Icons and shortcuts	5
Layout	4
Menu	5
Referenced Documentation	3
Screenshot	6
Support	2
Project Players	2

**End of document**