Project Report on

Network Traffic Monitoring with Attack and Intrusion Detection System

Submitted by

Vyom Bhatia, Maitraiye Saxena, Shabad Sawhney, Vivek Kumar

Regn. No: 1081230004, 1081230005, 1081230006, 1081230008

Under the guidance of

Mr. Chiranjit Dutta

Assistant Professor

Department of Information technology

January 2016

DEPARTMENT OF INFORMATION TECHNOLOGY

SRMUNIVERSITY, NCR CAMPUS, MODINAGAR-201204

GHAZIABAD, UTTAR PRADESH

SRM UNIVERSITY NCR CAMPUS MODINAGAR

Department of Information Technology

Project Write-up (IT0420) Session: Jan- Jun, 2016

- Title
- Objective
- Introduction
- Technology/ Methodology
- Applications
- Expected Outcomes

TITLE

Network traffic monitoring with attack and intrusion detection system

OBJECTIVE

Our 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 we are providing a network security environment to deal with the hazardous scenarios for the network infrastructure of the organization

INTRODUCTION

Every organization, irrespective of its size depends on networking technologies. These networks hold the working of entire organization and thus is 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 of the business of the organization. Our 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.

TECHNOLOGY/METHODOLOGY

1) **Python 2.7 -** Python interpreters are available for installation on many operating systems, allowing Python code execution on a wide variety of systems.
2) **Operating System** - Both Windows and Linux operating systems will be required to create and run the software and simulate attacks.
3) **Virtual Environment** - Virtual Environment will be required to run multiple Operating Systems simultaneously to create a network infrastructure.

EXPECTED OUTCOMES

We are expecting the network traffic monitoring with attack and intrusion detection system to maintain logs of every aspect of the network infrastructure and logs can be manually analyzed in the graphical format by the administrator for security purposes. The logs can be maintained, stored and read by the administrator in case of breach of security.

SRM UNIVERSITY NCR CAMPUS MODINAGAR

Department of Information Technology

University Project Summary Table

(IT0420) Session: Jan- Jun, 2016

S.No.	**Project title**	**Network traffic monitoring with attack and intrusion detection system**
1	Team Members	Vyom Bhatia (1081230004) Maitraiye Saxena (1081230005) Shabad Sawhney (1081230006) Vivek Kumar Pathak (1081230008)
2	Objective	Our 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.
3	Application of previously acquired knowledge through courses	Computer Networks (IT0305) TCP/IP Technology (IT0405)
4	Realistic constraints	The software has to be configured according to the needs of the different networks and the actual scale of the organization keeps changing constantly
5	Standards to be followed	Wi-Fi standards (IEEE 802.11) Ethernet standards (IEEE 802.3) TCP/IP suite
6	Multi-disciplinary task involved	Information Technology Computer Science and Engineering

SRM UNIVERSITY NCR CAMPUS MODINAGAR

Department of Information Technology

University Project Synopsis Report

(IT0420) Session: Jan- Jun, 2016

This report includes the following.

1. Title
2. Abstract
3. Aim
4. Literature Survey
5. Project Plan
6. SRS
7. Existing problem
8. References

TITLE

Network traffic monitoring with attack and intrusion detection system

ABSTRACT

Every organization, irrespective of its size depends on networking technologies. These networks hold the working of entire organization and thus is 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 of the business of the organization. Our 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

AIM

Our 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 we are providing a network security environment to deal with the hazardous scenarios for the network infrastructure of the organization

LITERATURE SURVEY

Several information security techniques are available today to protect information systems against unauthorized use, duplication, alteration, destruction and virus attacks. An Intrusion Detection System (IDS) is a program that analyzes what happens or has happened during an execution and tries to find indications that the computer has been misused. There are abundant literatures on Intrusion detection system, and several IDS approaches have been proposed, since the origins of this technology, relevant works in this direction have been proposed to clarify the concepts of intrusion detection as a solution to the problem of providing a sense of security in computer systems. The basic idea is that intrusion behavior involves abnormal usage of the system. Different techniques and approaches have been used for latter developments. Some of the techniques used are statistical approaches, predictive pattern generation, expert systems, keystroke monitoring, state transition analysis, pattern matching, and data mining techniques.

PROJECT PLAN

Network traffic monitoring with attack and intrusion detection system mainly focuses on protecting the network infrastructure of the organization. But we are also demonstrating different attacks on network infrastructure for which we will be required to build the attack modules too.
We are planning to add more tools to make our attacking software a universal tool which can be used under mostly all scenarios so that we can get the attacked system out of the trouble.
We will start our software by coding the tools in python and will gradually develop a graphical use interface by using tkinter module of python.
We will add some other tools like Bluetooth attacks and key logger for expanding the horizon of our software.

The modules in location detection and security system are:

- Attack Module
- Network Intrusion Detection Module
- GUI

SOFTWARE REQUIREMENT SPECIFICATION (SRS)

Software requirements:

Number	Description	Alternatives (If available)
1	Python 3.5.1	Python 2.7.11
2	Tkinter	Turtle
3	VMWare	Oracle -Virtual Box
4	Windows XP or above	Any Linux flavour with python interpreter

Hardware requirements:

Number	Description	Alternatives (If available)
1	PC with minimum 2 GB hard-disk and 256 MB RAM	Not applicable
2	Wi-Fi enabled Router	Ethernet

EXISTING PROBLEMS

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 sniffing and DoS attacks. The administrator should also be notified about the active users and their activities on the network infrastructure.

REFERENCES

- A Summary of Network Traffic Monitoring and Analysis Techniques - Alisha Cecil
- http://www.mutisoftvirtualacademy.com
- http://www.researchpedia.info
- An Almamater survey on people's trust on internet security, 2015