Seminar Report

On

A general purpose framework or architecture for testing security device on high speed network.

By

Bedse Tanuja Parag

**TCOA-09**

Under the guidance

Of

Prof. Archana Kollu





**Department of Computer Engineering**

**Dr. D. Y. Patil Unitech Society’s**

**Dr. D. Y. Patil Institute of Technology**

**Sant Tukaram Nagar, Pimpri, Pune-18**

**Affiliated to Savitribai Phule Pune University, Pune**

**[2018-2019]**

Department of Computer

Engineering,

Dr. D. Y. Patil Institute of Technology, Pimpri, Pune.



**CERTIFICATE**

This is to certify that **Aditya Diliprao Kulkarni** from **Third Year Department of computer Engineering** has successfully completed his seminar work **titled “Study of Machine Learning and Deep Learning for network analysis of intrusion detection”**at **Dr. D. Y. Patil Institute of Technology and Engineering, Pimpri** in the partial fulfillment of the Bachelor’s Degree in Engineering.

Prof. Archana Head of the DepartmentPrincipal

Kollu

# Acknowledgement

I would like to express my deep gratitude to professor Archana Kollu for their patient guidance, enthusiastic encouragement and useful critiques of this research work, Also for their advice and assistance in keeping my progress on schedule. I would also like to thanks all the authors, writers and technical experts whose Research papers, Books and Websites were used in order to fulfill my seminar report work.

# Table of Contents

|  |  |  |
| --- | --- | --- |
| **S.R no.** | **Description** | **Page no.** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# List of figures

|  |  |  |
| --- | --- | --- |
| **S.R.no** | **Description** | **Page no.** |
|  |  |  |
|  |  |  |
|  |  |  |

# Abstract

The need of security appliance is an increasing availability of high throughput networks in high speed networks. Testing these security appliance by considering their performance and effectiveness depends on testing tool that can achieve by increasing the capabilities of device and network.

In modern high security equipment current tools are not capable of achieving demands of flexibility and performance. To fulfill these demands we can used the architecture of general purpose network testing framework as prototype. This framework is high adaptable and can achieve high throughput.

## Keywords:

Security, Networks, Testing, Framework

# Objectives

* To understand General purpose network testing framework as prototyping implementation used in network testing.
* Understand the architecture of high speed networks.
* To understand concept of security devices, internet traffic generator and simulators.

# Introduction

A General purpose network testing tools are classified into three categories and the tools are security testing tools, traffic generator, and network simulators.

Security testing is used to identify the threats and helps to detect all possible security risks in the system. Security testing tool are designed to detect vulnerabilities in the device under test.

For instance W3af(web application attack and audit framework) is open source web application security scanner.W3af provide vulnerability scanner and exploitation tool for web application. Sqlmap focusing on SQL injection and database takeover. bestorm and metasploit consist of many attack pattern and types .

All these programs create harmful traffic. To analyze it harmful traffic testing tool is needed. Traffic generator create traffic flows or data sources in communication network. example packETH ,DITG are used to create real traffic. packETH is GUI packet generator tool for ethernet. Distrubed internet traffic generator is used to produce traffic at packet level. Network simulators Ns-3 and Netsim emulate real networks with all components and traffic flows in virtual environment. Simulators support network protocols , traffic loads and distribution.

Network device in general purpose framework are classified into three categories: security device, service devices and forwarding device. Security devices are system that detect harmful traffic and collect statistical information about processed packet. The main purpose of Security devices is to protect against both outgoing and incoming harmful tarffic.

Service device is used as webservers and file transfer servers. Servers must be transfer synthically correct data at client side and handle response from the DUT. Forwarding device are network routers or switches that forward and reroute packet at specified bandwidth.

Testing framework work on operating system that support hardware. A highly modular framework allows easy extensibility, exchangeability and removability of specific future implementation.

General purpose network framework (GPNTF) has bidirectional synchronized client server communication flow. GPNTF provided mixing flow of all types of protocols and communication pattern with harmful traffic.

***Features of GPNTF***

* support for arbitrary client and server flows.
* Ethernet as layer-2 protocol.
* IPv4 and IPv6 as layer-3 protocol.
* UDP and TCP as layer-4 protocol.
* XMPP (Extensible messaging and presence protocol)as layered-7 protocol.
* Bidirectional client-server communication support.
* **Architecture of framework:**

Framework is run in three modes

1. Network client
2. Network server
3. Controller for administration purpose.

Framework can be configured by configuration file which is used

to stored statistical information.

Running in client mode framework diverse real network

client with fields of application.

Client mode contain three main module:

* Task processing module:read client parameter from file to generate requested flow
* Packet builder module :generate required packet and dispatch returned packets
* Client state machine module :connect new state machine handling new protocol.
* Running in server mode, Framework simulates the behavior of real network server. The server mode contain same mode as client. The task processing mode open user requested server socket and processing incoming client request. Client state machine module is used to connect new protocol state machines to main module. Controller is used to send the configuration file to client or Server.

**Literature survey**

1. sqlmap - “Automatic SQL injection and database takeover tool,” (M. Stampar,16 April 2017)

2. “A flexible overlay network simulation framework,”

( B. Heep and S. Krause *2007* IEEE Global Internet Symposium, May 2007,)

3. Security device W3af-”Open Source Web Application Security Scanner”

(M.Stamper,16 April 2017)

**Design Details**

**Technology**

**Conclusion**

A concept for testing framework that enables tester to test more efficiently and to make it easy to document also share test cases for network equipment performance evaluation and also transformed theoretical architecture to proved design goals of a dynamic testing framework.

**References**

1.D-ITG,‘DistributedInternetTrafficGenerator’, http://traffic.comics.unina.it/software/ITG/,

2.OSTINATO.http://ostinato.org/,

3. packETH.<http://packeth.sourceforge.net/packnet/Home.html>.

4. w3af - Open Source Web Application Security Scanner.,

5. I. Baumgart B. Heep S. Krause "Oversim: A flexible overlay network simulation framework" 2007 IEEE Global Internet Symposium pp. 79-84 May 2007.

6.beStorm.,http://www.beyondsecurity.com/bestorm.html.

7. B. Guimaraes M. Stampar sqlmap - Automatic SQL injection and database takeover tool; http://sqlmap.org/,  
8. I. Raicu C. Dumitrescu M. Ripeanu I. Foster "The design performance and use of diperf: An automated distributed performance evaluation framework" Journal of Grid Computing vol.4no.3pp.287-3092006.   
  
9. metasploit. http://metasploit.org/  
10. Steve McCanne ns-3,ns-3,htttp://nsnam.org/  
11. D. Stingl C. Gross J. Rckert L. Nobach A. Kovacevic R. Steinmetz "Peerfactsim.kom: A simulation framework for peer-to-peer systems" 2011 International Conference on High Performance Computing Simulation pp. 577-584 July 2011.   
  
12.TETCOS,NetSIM,http://tetcos.com/.  
  
13. G. Tsouloupas M. D. Dikaiakos GridBench: A Workbench for Grid Benchmarking Berlin Heidelberg:Springer Berlin Heidelberg pp. 211-225 2005. http://dx.doi.org/

**Plagiarism check report**

|  |  |
| --- | --- |
| **Seminar Report Documentation** | |
| **Report Code:**TE-CS-Seminar 2018-2019 | **Report No:**TCOA-09 |
| **Report Title:** A general purpose framework or architecture for testing security device on high speed network. | |
| **Address:**Dr. D. Y. Patil Institute of Technology, Sant Tukaram Nagar, Pimpri, Pune, Pin-411018, M.S.India. | |
| **Address:** Sant Tukaram Nagar,Pimpri, Pune-411018.  **E-mail:**[tanujabedse1998@gmail.com](mailto:tanujabedse1998@gmail.com)  **Cell-no:** 9420129783 | |
| **Year:** 2018-2019  **Branch:** Computer Engineering | |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Type of Report:**  Final | **Report checked by:** | **Report checked**  **Date:** | **Guide’s complete**  **Name:**  Prof. Archana Kollu | **Total copies:**  2 |   **Keywords:** Security,Networks,Testing,Framework. | |