**WIRESHARK (TASK 10)**

*Project report (CA3) submitted in fulfilment of the requirements for the Degree of*

**BACHELOR OF TECHNOLOGY**

**in**

# COMPUTER SCIENCE AND ENGINEERING

By

# SAMAKSH BANSAL

## (11912543)

## Roll No. 35

SUBJECT

# INT301 – OPEN-SOURCE TECHNOLOGIES



**School of Computer Science and Engineering**

Lovely Professional University

Phagwara, Punjab (India)

Month April Year 2023

**LIST OF CONTENTS**

Page No.

1. Introduction

1.1 Objective of the project 3

1.2 Description of the project 3

1.3 Scope of the project 3

2. System Description

2.1 Target system description 4

2.2 Assumptions and Dependencies 4

2.3 Functional/Non-Functional Dependencies 5

2.4 Data set used in support of your project. 5

3. Analysis Report

3.1 System snapshots and full analysis report 6

4. GitHub Link 11

5. Reference/ Bibliography 12

1. **INTRODUCTION**
   1. **OBJECTIVE OF THE PROJECT**

In this project, the objective is to inspect HTTP traffic and retrieve the username and password from the BSNL website using an appropriate tool. The project aims to demonstrate how an attacker can exploit the security vulnerabilities in the website and gain access to sensitive information.

* 1. **DESCRIPTION OF THE PROJECT**

The project involves the use of Wireshark, a popular network protocol analyzer tool, to capture and analyze HTTP traffic between the user's computer and the BSNL website. The tool will allow us to inspect the packets and extract the username and password sent by the user to the website.

The project will focus on identifying the security weaknesses in the website's login process that allow an attacker to intercept and steal the user's credentials. It will involve analyzing the HTTP packets for any unencrypted data and looking for patterns that indicate the username and password.

* 1. **SCOPE OF THE PROJECT:**

The scope of the project is limited to the BSNL website and its login process. The project will not involve any actual hacking or exploitation of the website's security vulnerabilities. Instead, it will focus on demonstrating how an attacker can use Wireshark to intercept and retrieve sensitive information from the website's traffic.

The project will provide insights into the importance of secure website design and the use of encryption to protect sensitive user data. It will also demonstrate the need for users to be cautious when entering their credentials on websites and the importance of using strong and unique passwords.

1. **SYSTEM DESCRIPTION**

2.1 **TARGET SYSTEM DESCRIPTION:**

The target system for this project is the BSNL website's login process. The website uses HTTP protocol to transmit data between the user's computer and the website's servers. The login process involves the user entering their username and password into a form on the website, which is then transmitted to the server for authentication.

**2.2 ASSUMPTIONS AND DEPENDENCIES:**

The assumptions for this project include:

1. The user is using an unsecured Wi-Fi network, which can be intercepted by an attacker.
2. The website does not use any encryption or security protocols to protect the user's credentials during transmission.
3. The user's computer is not infected with any malware that can intercept and steal their credentials.
4. The dependencies for this project include:
5. Wireshark, the network protocol analyzer tool used to capture and analyze the website's traffic.
6. An internet connection to access the BSNL website.
7. A web browser to access the BSNL website and enter the login credentials.

2.3 **FUNCTIONAL/NON-FUNCTIONAL DEPENDENCIES:**

1. The functional dependencies for this project include:
2. The ability of Wireshark to capture and analyze HTTP traffic between the user's computer and the BSNL website.
3. The user's ability to access the BSNL website and enter their login credentials.
4. The non-functional dependencies for this project include:
5. The speed and reliability of the user's internet connection.
6. The compatibility of Wireshark with the user's operating system and hardware.

**2.4 DATA SET USED IN SUPPORT OF YOUR PROJECT:**

This project focuses on capturing and analyzing live HTTP traffic between the user's computer and the BSNL website, without the need for a specific data set. The main objective is to extract the username and password from the traffic, and to demonstrate the techniques used through sample data. The process involves analyzing the data packets sent and received during the login process and identifying the relevant fields containing the login credentials. The project aims to provide insight into the vulnerabilities present in HTTP traffic, and to raise awareness about the importance of secure communication protocols in online transactions.

1. **ANALYSIS REPORT**
   1. **SYSTEM SNAPSHOTS AND FULL ANALYSIS REPORT**

1.

Graphical user interface, text, application, Word

Description automatically generated

2.

Graphical user interface, text, application

Description automatically generated

3.

Graphical user interface, text, application, email

Description automatically generated

4.

Graphical user interface, application

Description automatically generated

5.

A screenshot of a computer

Description automatically generated

6.

Graphical user interface, application

Description automatically generated

7.

Graphical user interface, application, table

Description automatically generated

8.

Graphical user interface, application, table

Description automatically generated

9.

Text

Description automatically generated

10.

Text

Description automatically generated

1. **GITHUB LINK**

* **LINK:**

<https://github.com/SamakshBansal/InspectingHTTPusingWireShark>

1. **REFERENCE AND BIBLOGRAPHY**
2. Wireshark - Go deep. (n.d.). Retrieved March 26, 2023, from <https://www.wireshark.org/>
3. BSNL. (n.d.). Retrieved March 26, 2023, from <https://www.bsnl.co.in/>
4. M. M. Adeel Arif, N. M. Arif, & A. H. Malik. (2017). Security assessment of web applications: An insight into OWASP top 10 vulnerabilities. Journal of King Saud University - Computer and Information Sciences, 29(4), 512-525.
5. Shobha, B. R., & Shylaja, B. S. (2015). Analysis of web application security vulnerabilities using OWASP. Procedia Computer Science, 45, 697-706.
6. OWASP Top Ten Project. (n.d.). Retrieved March 26, 2023, from <https://owasp.org/www-project-top-ten/>
7. HTTP/1.1: Authentication. (n.d.). Retrieved March 26, 2023, from <https://tools.ietf.org/html/rfc7235#section-4>
8. Singh, S., & Singh, S. P. (2013). Web application security: A review of the state of the art. International Journal of Computer Applications, 78(8), 10-15.