www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-2, Issue-3, Oct- 2014
Research Paper

Int. J. Sci. Res. in Network Security and Communication
ISSN: 2321-3256

Delving into Security of Networks – Time's Need

Annie Singla[1*], Kamal Jain[2] and Ajay Gairola[3]

[1*]*Research Scholar, Disaster Mitigation & Management, IIT Roorkee, India*
[2]*Professor, Department of Civil Engineering, IIT Roorkee, India*
[3]*Head, Centre of Excellence in Disaster Mitigation & Management, IIT Roorkee, India*

[1]*anniesingla@yahoo.com*, [2]*kjain_us@yahoo.com*, [3]*garryfce@gmail.com*

Received: July/29/2014 Revised: Aug/10/2014 Accepted: Sep/25/2014 Published: Oct/30/2014

Abstract - Cyber space is an inevitable and indispensable place in every human being's life now. With the advent of Internet fad, the rapid digitization has taken place. But with the rapid digitization, there is a rapid increase in the occurrence of cyber disasters. Disasters are measured on two parameters – loss to life and property. In cyber disasters, there is a hell lot loss to money, zillions of people are getting affected on a daily basis and the loss of money is in billions of dollars in every disaster. They are bringing down the economy of the nation and people are also affecting on regular basis. Their privacy is being compromised. Due to the Internet fad, E-commerce, e-banking, online casinos are victimized. The vulnerability in the webpage of Gmail is found out during research study. The studies of vulnerability lead to cyber disasters using Phishing attacks through which the passwords were retrieved and accessed of various people. Users should be more aware as well as updated in terms of technology which can diminish these cyber disasters.

Keywords-Phishing Attack, DDoS

I. PREAMBLE

Cyber disasters are one of the most crucial problem which is being faced by nation on small as well as large scale. It is a continuous global concern. The total global direct cost of cybercrime has risen to US$113 billion in 2013 up from $110 billion in 2012 and the average cost per victim of cybercrime in 2013 is $298 which is up from $197 in 2012[1]. As the globalization has arose to a whole new different level due to Internet fad, it has caused more and more of brooding in terms of security. The rapid digitization which was man's quest has made humans stand on a very different platform where the Internet has become an indispensable part of a man's life as people are now constantly connected to one other whether locally, nationally or internationally. The lines between the personal and work lives have faded all the way now. The rapid digitization which has been a boon to the mankind has left certain vulnerable points in the network that it has catalyzed the cybercrime on an exponential increase.

National Research Council of USA said in 1991 that "*A modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.* The saying has come true as now cyber space has replaced bullets with bytes. There is no need of guns to harm a nation as one can sit millions of kilometers away and by giving some commands, a person can harm an entire nation. Some of the instructions are executed in less than 3 milliseconds. Now the automated disasters are considered in terms of a new time scale as the cyber-disasters are taking place in nanoseconds.

Corresponding Author: Annie Singla, anniesingla@yahoo.com
Research Scholar, Disaster Mitigation & Management, IIT Roorkee, India

II. NOTICEABLE CYBER DISASTERS

Companies, banks, e-commerce hubs rank cyber risk as the top risk to their operations [2]. The main threats which are related to the activities of cyber disasters can be grouped into the following categories:

- Intrusion for the monetary or other benefits.
- Interception for espionage.
- Manipulation of networks 3or information.
- Destruction of data.
- Misuse of the processing power
- Counterfeit items
- Tools and techniques for invasion [3].

Some of the noticeable cyber disasters which have happened are mentioned as follows:

- On the morning of Dec 30th, 2004, after The Great Sumatra Earthquake and Indian Ocean Tsunami of Dec 26, 2004, a major crisis and an embarrassment were created, when the Home Ministry issued a warning to the affected states of an earthquake and impending tsunami in the afternoon of the same day. Apparently an

individual in the United States was behind the hoax [4].

- In Oct'13, a cyber-disaster has led to a massive number of Adobe IDs and passwords fallen into the hands of attackers which comprised of certain information of 2.9 million customers. Among that data set were names of the customers, credit / debit card numbers which were encrypted as well as its expiration dates [5].
- On 28th Feb'14, World's biggest cyber-attack was detected as 360 million accounts, 1.25 billion email addresses were hacked and email addresses came from all the major providers including Microsoft, Google, and Yahoo, and that many non-profit organizations as well as almost all the Fortune 500 companies had been affected [6].
- In Feb'14, largest DDoS attack peaking at 400Gbps of traffic slows down the Internet [7].

III. OBJECTIVE OF THE STUDY

The email and password retrieval attacks are on the hike and recently so many cyber disasters have taken place in which the user ids and passwords are compromised. In view of this, the goal and objectives are focused in the research work.

- Finding the vulnerability in thewebpage.
- Cracking the user ids and passwords of mail webpages.

IV. VULNERABILITY IN THE WEBPAGES

Despite of so many security checks, there exists a vulnerability gap in the homepage of Gmail/ Facebook which shows the password from asterisk form to textual format. Knowing about the vulnerability helps in accessing one's account leaks the confidential information.

A. Methodology

The steps followed for finding the vulnerability are as follows:

- Insert the username and password credentials in the Gmail homepage. (See Appendix, Fig 4.1)
- Select the Password.Inspect the element (See Appendix, Fig 4.2)
- There would be the coding details in which the type of password is passwd. (See Appendix : Fig 4.3)
- By changing it to text, it would display the password in textual/ readable form. (See Appendix, Fig 4.4 & 4.5)

This vulnerability makes the webpage of Google Mail vulnerable for the cyber disasters which further lead to the leakage of information if occurred on a large scale.

V. ACCESSING GMAIL/ FACEBOOK PASSWORDS

The method which is used during retrieval of Gmail/ Facebook passwords is Phishing attack. In this attack, the page of Gmail/Facebook is cloned i.e. it is absolutely same as that of the Gmail/ Facebook webpages. But the difference between real and cloned page is that when the victim enters his username and password credentials in real webpage, the homepage is opened. But in cloned webpage, the user still enters the username and password details in the homepage but the moment user enters his details, the confidential username and password are retrieved to the person sitting on the other end who cloned the site and moreover the password details are no more in asterisk form, they are retrieved in proper textual / readable form.

A. Platform used

Kali Linux is used as the platform.

B. Methodology

- Open the Social Engineering Toolkit in Kali Linux.
- Then choose Website Attack Vectors. (See Appendix : Fig 5.1)
- Choose Tabnabbing method. (See Appendix : Fig 5.2)
- After that, choose 'site cloner. (See Appendix : Fig 5.3)
- Then enter the IP address of one's own computer.
- The site would be cloned now. (See Appendix : Fig 5.4)
- Send the link of the cloned website to various people and whosoever would be entering the credentials, the password along with usernames would be retrieved to one's own computer. (See Appendix : Fig 5.5 & 5.6)

The yellow color in the snapshots depicts the password for the security reasons.

These types of attacks lead to the major cyber disasters specially related to the banking sector. Innocent people receive mails that your account needs to be verified, updated or the password of user is not in the database etc. These type of mails are nothing but the attacks which gives the password to the attacker without the knowledge of the user himself.

CONCLUSIONS

The use of all the utilities on Internet is inevitable. It is not possible to eliminate cyber disasters from cyber space because of the Internet fad. In remedy of the cyber disasters, people should be more aware about using Internet. They should not enter their confidential

credentials in the any webpage that comes to them. People should be more updated to save themselves from cyber disasters.

VI. REFERNCES

[1] Norton Report (2013). Available at <http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013> (Retrieved on May, 2014)

[2] Karnika Seth (8th May 2010). IT Act 2000 vs 2008-Implementation, Challenges, and the Role of Adjudicating Officers. Available at <http://catindia.gov.in/pdfFiles/IT_Act_2000_vs_2008.pdf > (Retrieved 29th May,2014)

[3] 2013- The Impact of Cyber Crime. Available at <http://resources.infosecinstitute.com/2013-impact-cybercrime/> (Retrieved on 23rd March,2014)

[4] EERI Special Earthquake Report — April 2005 global cyber war and crime: A conceptual framework * Bryan School of Business and Economics, The University of North Carolina at Greensboro, Bryan Building, Room: 368, P.O. Box 26165, Greensboro, NC 27402-6165, USA ,Received 14 December 2004; accepted 14 September 2005.

[5] Chris Welch(3rd October, 2013). Available at <http://www.theverge.com/2013/10/3/4800042/adobe-suffers-cyber-attack-millions-of-customers-affected)>. (Retrieved on 29th Nov, 2013).

[6] Kounteya Sinha (28th Feb, 2014). Available at <http://timesofindia.indiatimes.com/tech/tech-news/Worlds-biggest-cyberattack-detected-360-million-accounts-1-25-billion-email-addresses-hacked/articleshow/31133867.cms >. (Retrieved on 14th April, 2014).

[7] Steven Musil (February 11, 2014). Available at < http://news.cnet.com/8301-1009_3-57618762-83/record-breaking-ddos-attack-in-europe-hits-400gbps/> (Retrieved 23rd March,2014)

AUTHORS PROFILE

Annie Singla is a M-tech student in Disaster Mitigation & Management at Indian Institute of Technology Roorkee,India.

Kamal Jain, Professor, Indian Institute of Technology Roorkee, India.

Ajay Gairola, Professor, Indian Institute of Technology Roorkee, India

APPENDIX

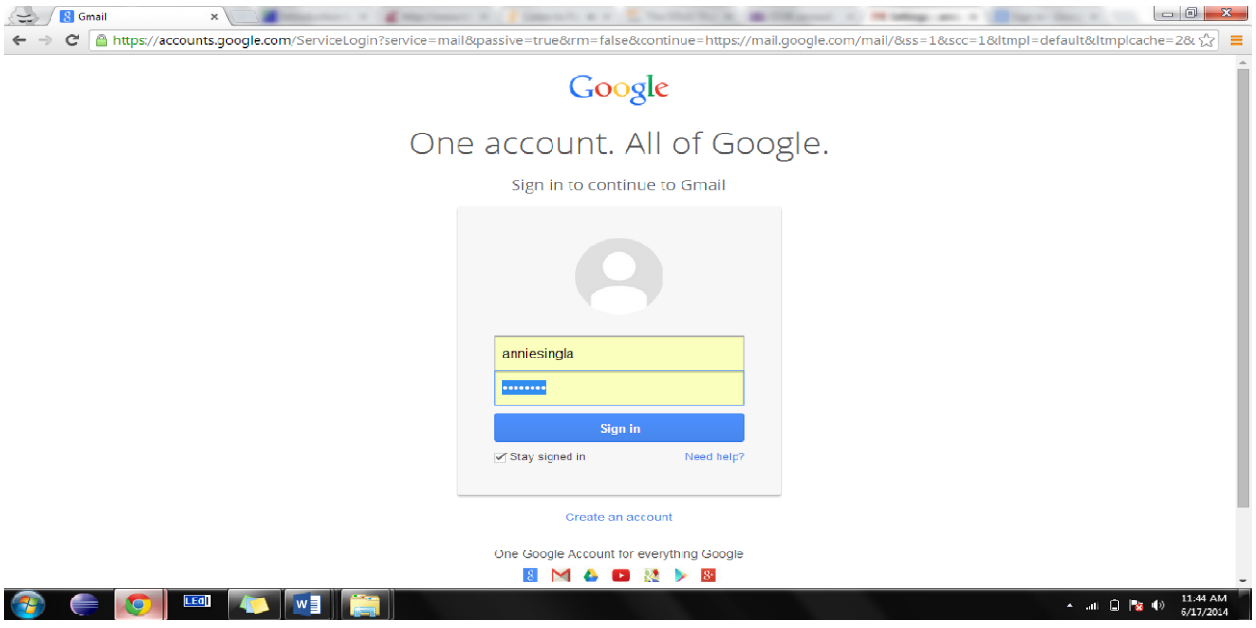

Fig 4. 1 : Insertion of password credentials

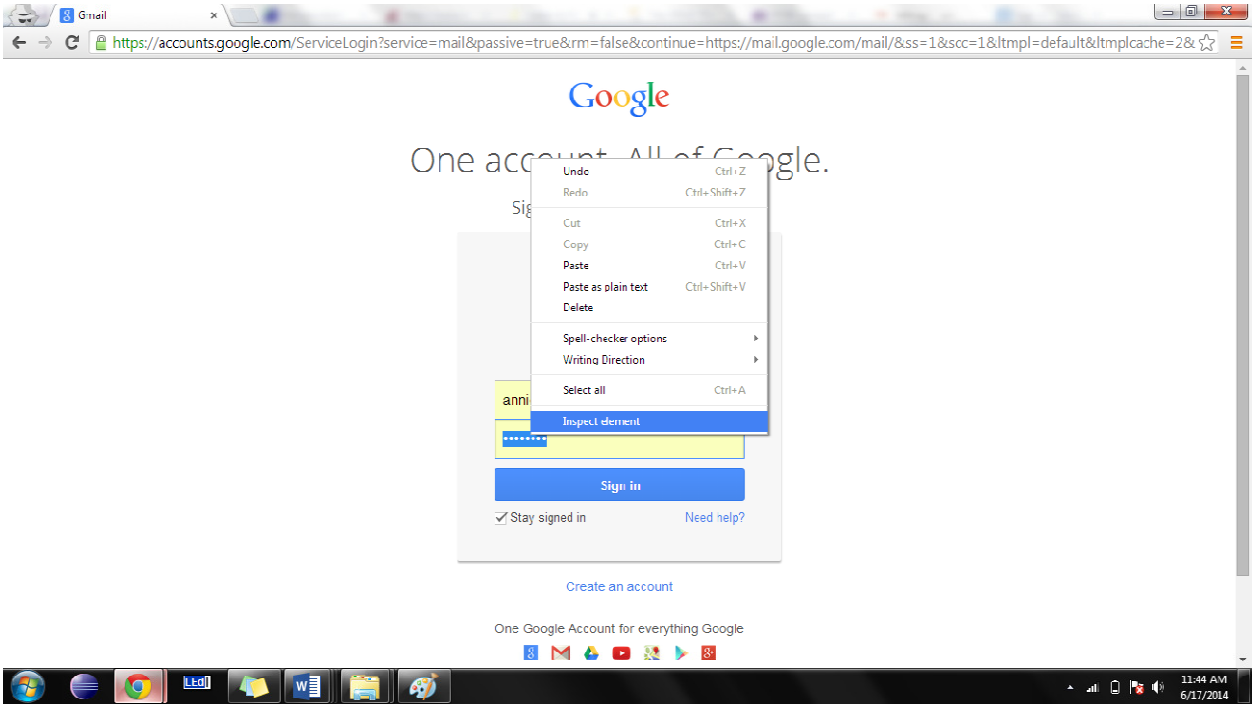

Fig 4. 2: Inspect Element of password

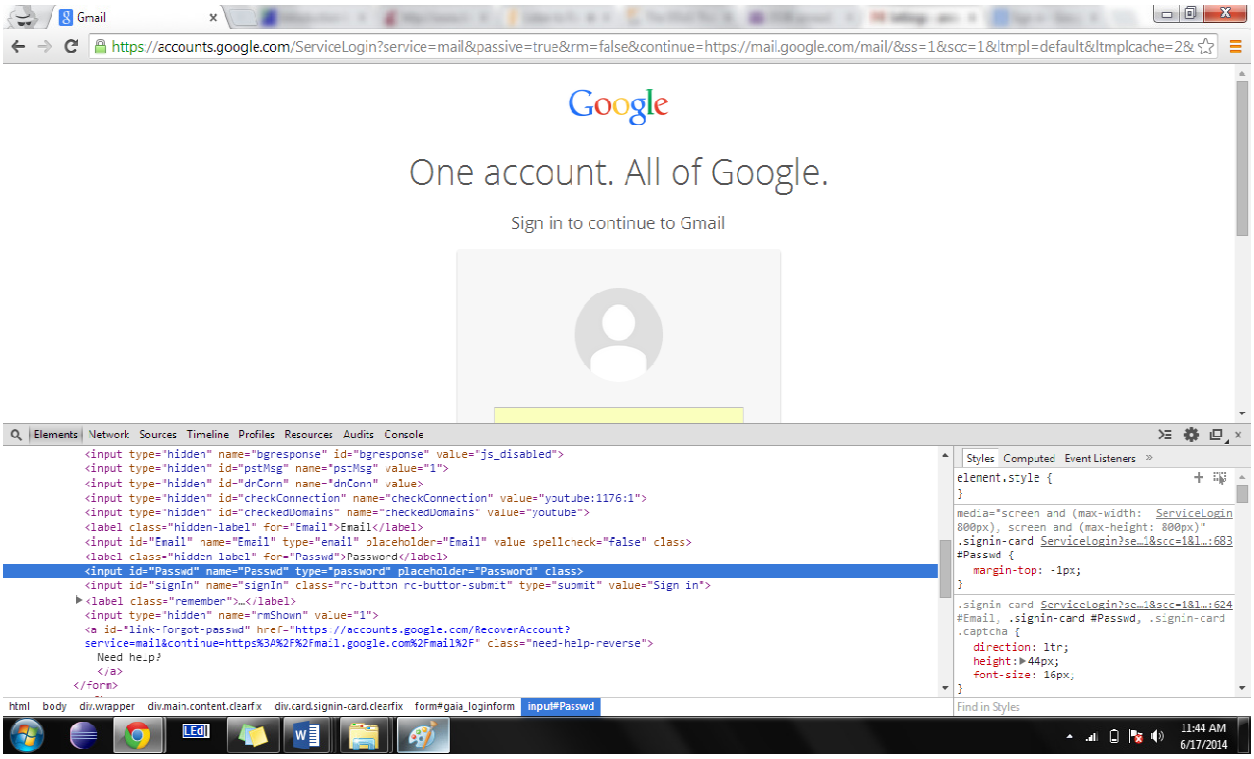

Fig 4. 3: Password details coding

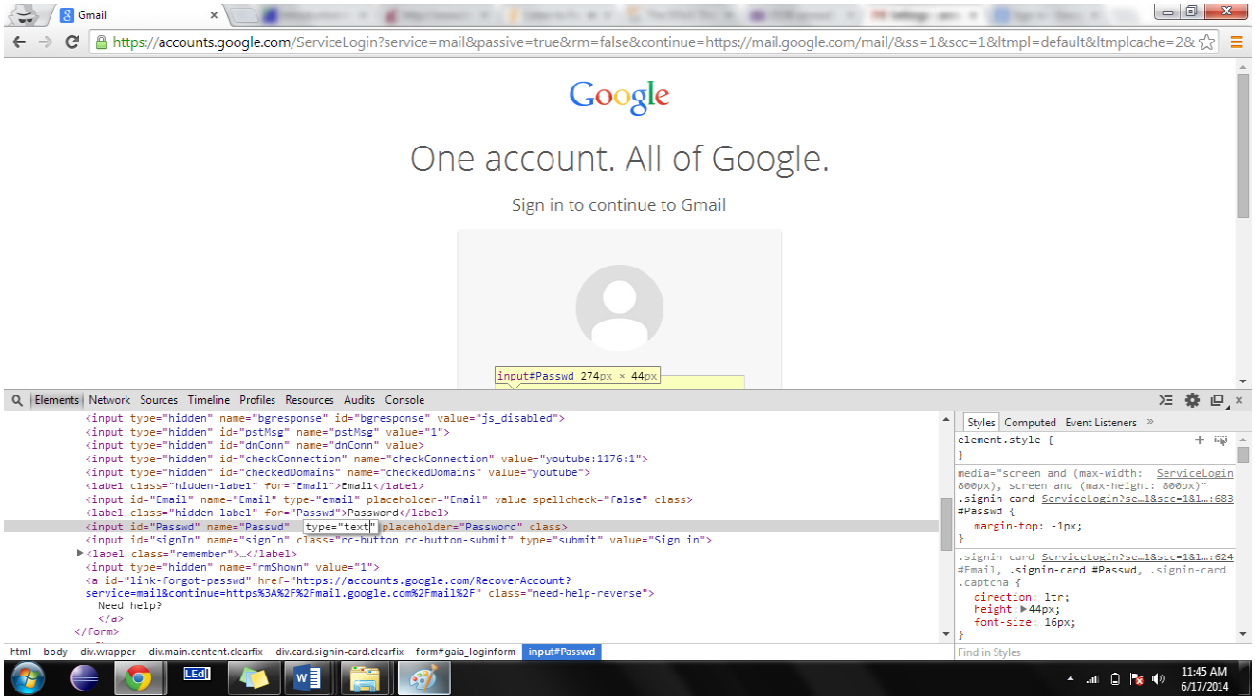

Fig 4. 4: changing the " type= text "

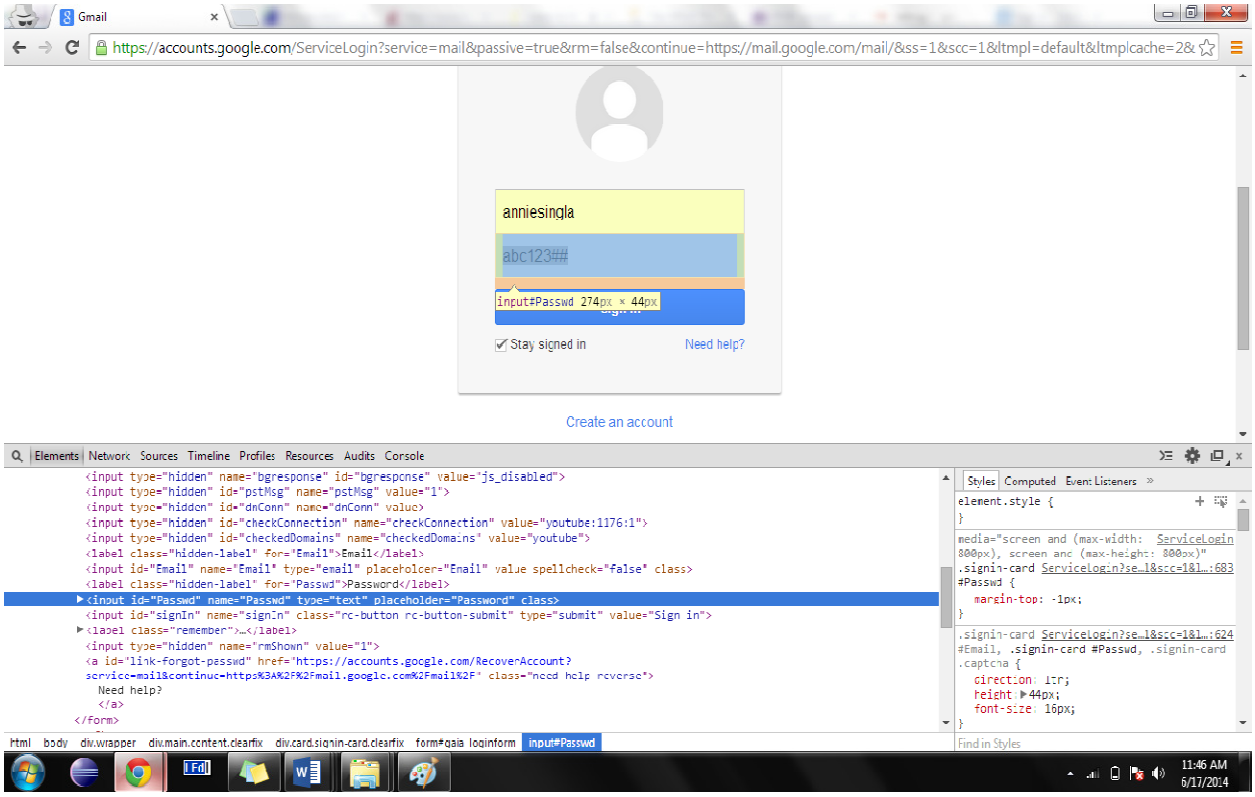

Fig 4. 5: Visibility of password in textual form

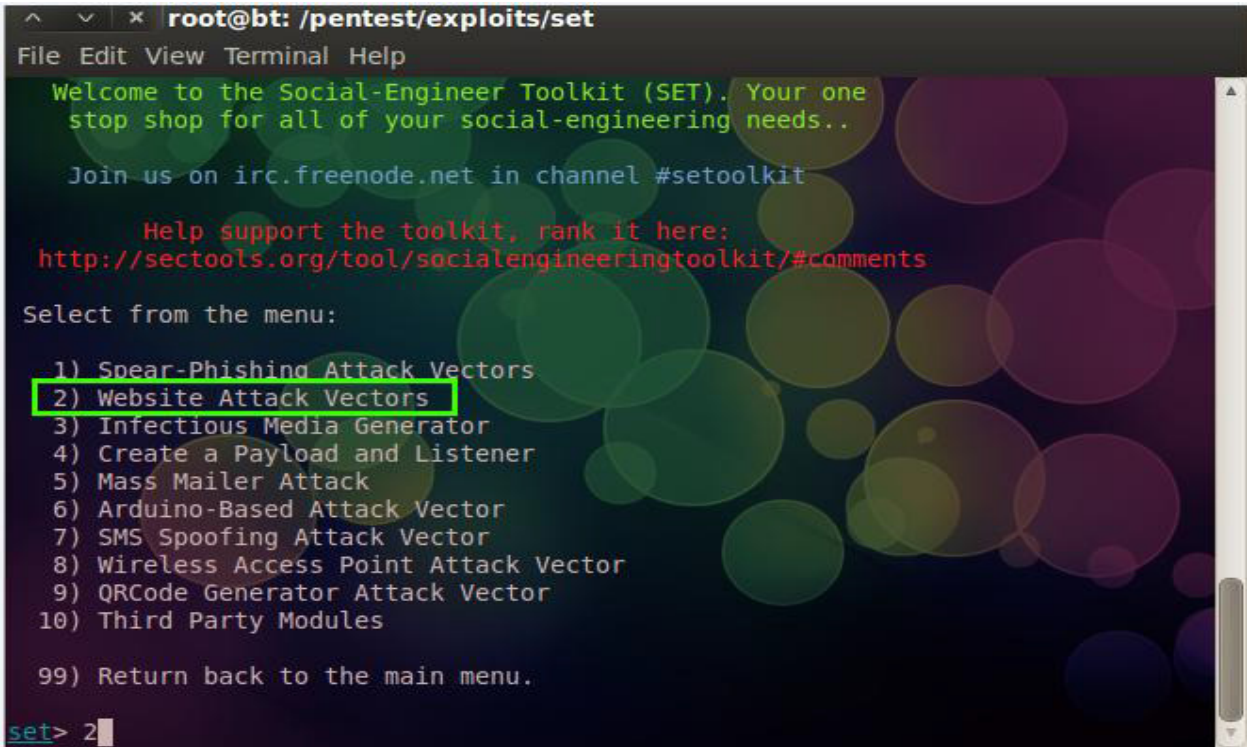

Fig 5. 1: Website Attack Vectors

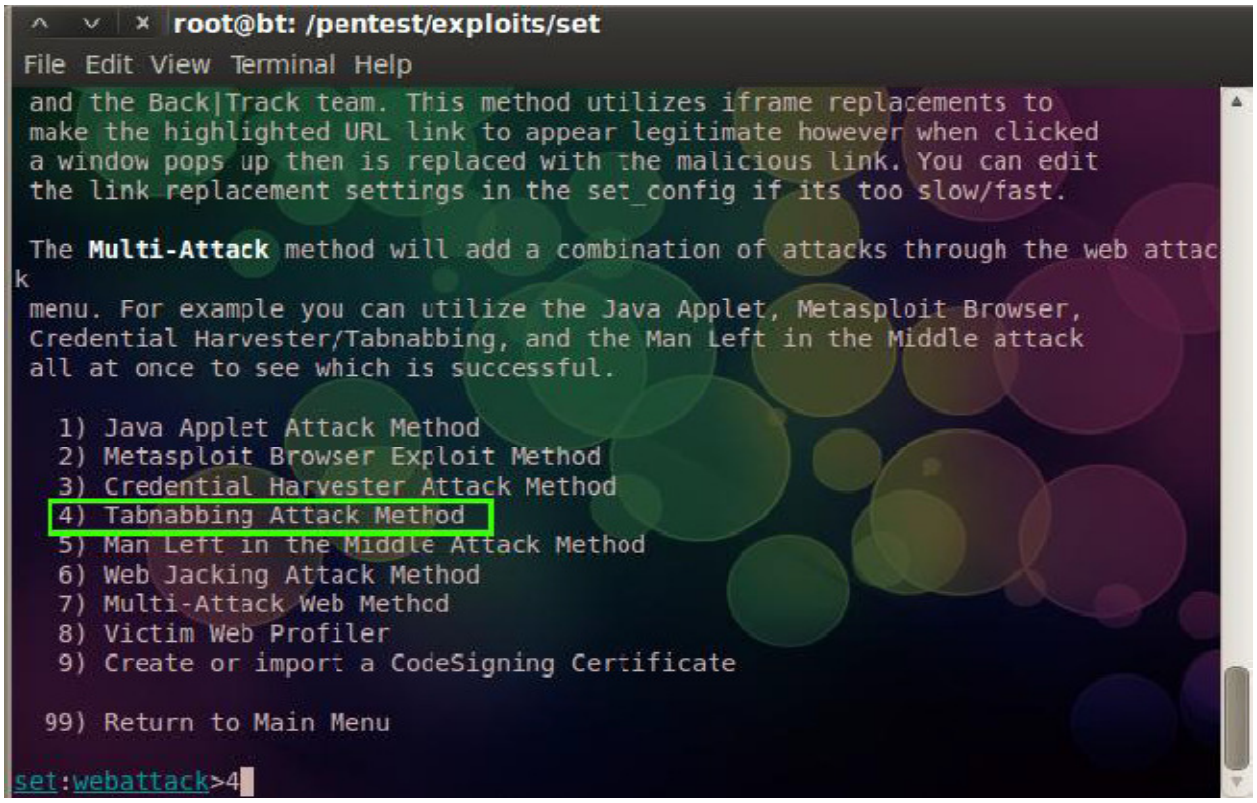

Fig 5. 2: Tabnabbing Attack Method

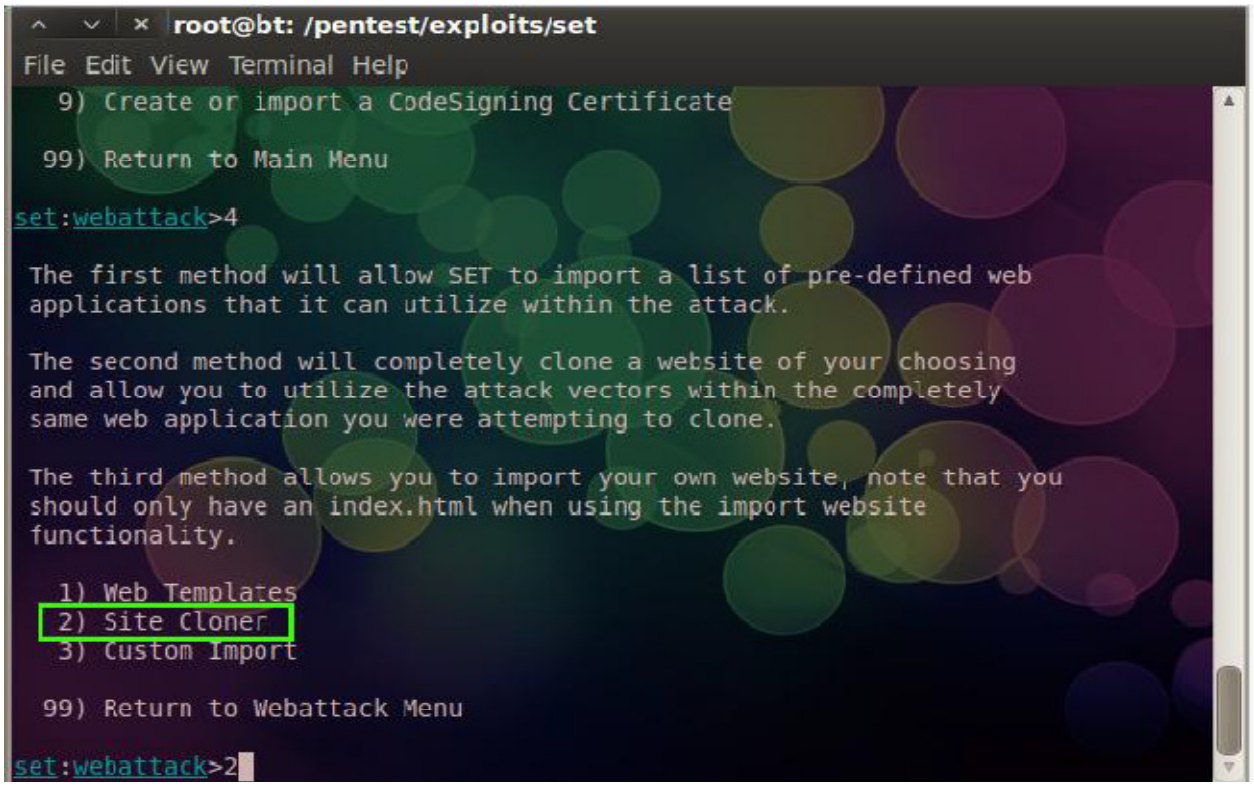

Fig 5. 3: Cloning of site

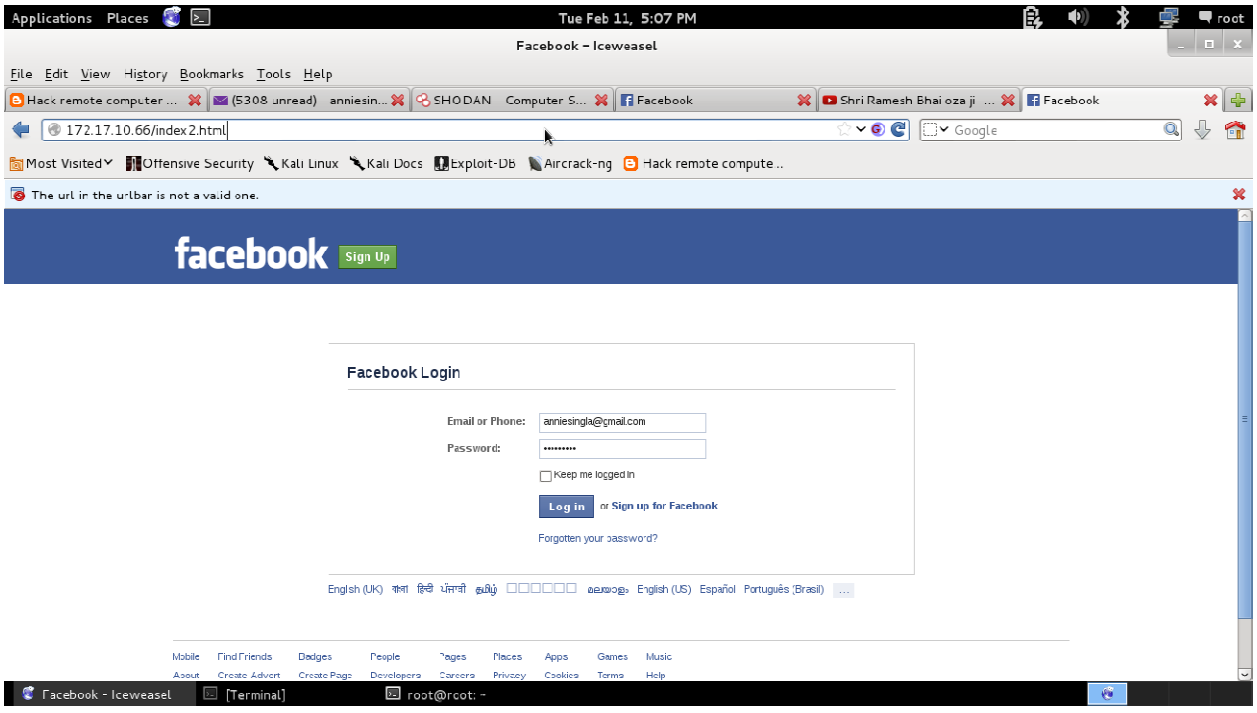

Fig 5. 4: The cloned web page

Fig 5. 5: Password Retrieval 1

Fig 5. 6: Password Retrieval 2

