Petar Kr. Boyanov, Zhaneta N. Savova,

IMPLEMENTATION OF CREDENTIAL HARVESTER ATTACK METHOD IN THE COMPUTER NETWORK AND SYSTEMS

Petar Kr. Boyanov[1], Zhaneta N. Savova[2]

[1] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", peshoaikido@gmail.com*
[2] *National Military University "Vasil Levski", Faculty of Artillery, Air Defense and Communications and Information Systems, Department „Communication Networks and Systems", zh.savova@mail.bg*

Abstract: In this paper some sophisticated implementation of credential harvester attack method in the computer network and systems is made.

Keywords: Credential Harvester, Cybersecurity, Footprinting, Government agencies, Information Security, Modern cyber-attacks, Social engineering, Vulnerability, Threat

Introduction

The cyberattacks cause the greatest damage to businesses, companies, organizations and individuals through unauthorized intrusion into the resources of computer and network systems [1], [2] regardless of the firewalls built in, IDS intrusion detection systems, anti-theft systems IPS penetrations, virtual local area networks, and virtual public networks. The types of social engineering attacks are Human and computer based attacks. Characteristic of human-based attacks is that the malicious perpetrator can be presented as a legitimate end user [12], a very important user, or as a technical support person [13]. In all three types, the masked abuser aims to gain access to confidential information about the company, company or organization [6], [7], [8], [9], [10]. It should be noted that this type of attack also includes techniques in which cybercriminals monitor and observe everything behind their victim. In this way, a cybercriminal can obtain the desired information only by gently spying and looking behind the back or shoulder of an organization employee. It is even more dangerous when it is behind the back of the system administrator who is responsible for all information security of the organization. The malicious perpetrator may also use Special Intelligence Means (CPCs) [15] for real-time audio and video calls. Another way a cybercriminal can get information about his victim is to search through trash cans to find letters, important documents, sketches, written passwords and usernames, projects, plans, and more. [12], [13], [14]. Disguising and presenting a cybercriminal as a legitimate representative of a large organization can also help him get information about his chosen victims, with the ultimate goal being, in most cases, financial fraud and demanding bribes in large sums of money [1], [2], [3], [5], [6, [7], [8].

Computer-based attacks are characterized by the fact that various malicious programs and software applications are used [9], [10] such as infected letters sent via e-mail, use of computer viruses, Trojans, etc. The types of computer-based attacks are [1], [2], [11], [14], [15], [16], [17], [18]:

• Send false emails [1].

• Pop-ups. These attacks use pop-ups that alert the average user to disconnect from the computer network [5] and need to re-enter their username and password [7]. The most commonly used email is a hyperlink that redirects to a fake web page requesting the introduction of personal information or downloading a malicious program such as a Trojan horse or spyware that keeps track of every key on the keyboard.

• Mobile-based cyberattacks. They are divided into:

• Publishing malicious applications. In these attacks, cybercriminals create malicious applications with attractive configurations similar to real trusted applications in a large online application store. Then, unwary ordinary users download these applications and are then infected by malware that sends all their personal information to the cybercriminal computer machine [1], [2], [6].

• Send fake short messages on mobile phones.

2. Phases and victims of social engineering

Social engineering is one of the most powerful and almost always successfully completed by cybercriminals. They are characterized by the following features:

• In most cases, people are most susceptible to different assumptions and influences and thus the cybercriminal can take advantage of this fact and get the information he or she wants.

• In computer practice, it is almost impossible to detect or detect attempts at social engineering.

• The fact is that no effective or almost no methods and means have been found so far to provide full protection from social engineering.

• In practice, there are neither hardware nor software protections against social engineering cyberattacks.

The phases that one must go through in order for an effective and successful social engineering cyberattack are:

• Finding a way to visit the victim organization. It is also possible to go to the trash can of the organization in order to search for and retrieve recorded passwords and employee usernames.

• Identify disgruntled or offended employees of the victim organization.

• Associate with certain employees of the organization to obtain more confidential information such as financial statements and bank accounts, telephone numbers, e-mails, social network profiles, future plans and projects of the organization, current and future products and services, etc. [1], [3].

The major victims of social engineering cyberattacks are:

• System administrators.

• Automated Information Systems and Networks Security Officers.

• Development and Operation Officers.

• Users as call center staff, receptionists, host organization.

• Technical managers for information problems in an organization or company.

• Ordinary users or customers of the company, company and organization.

• Representatives of large and small companies for software and hardware products and services.

3. Experiment

The experiment on a Local Area Network of 13 hosts in a computer lab at the Faculty of Technical Sciences at Konstantin Preslavsky University of Shumen is made. Similar lab is proposed in [4]. The operating system installed on the computer victim is Windows 10 Pro x64, version 1709, OS Build: 16299.371. The operating system installed on the attacking computer is Kali Linux 4.12.0-kali-amd64 #1 SMP Debian x86-64 GNU/Linux.

The purpose of the science experiment is to create a cloned site for stealing your username and password. The SET machine toolkit for this purpose will be used. This suite of tools was developed by TrustedSec in order to test the computer and network security of a particular host. This is shown on Fig. 1.

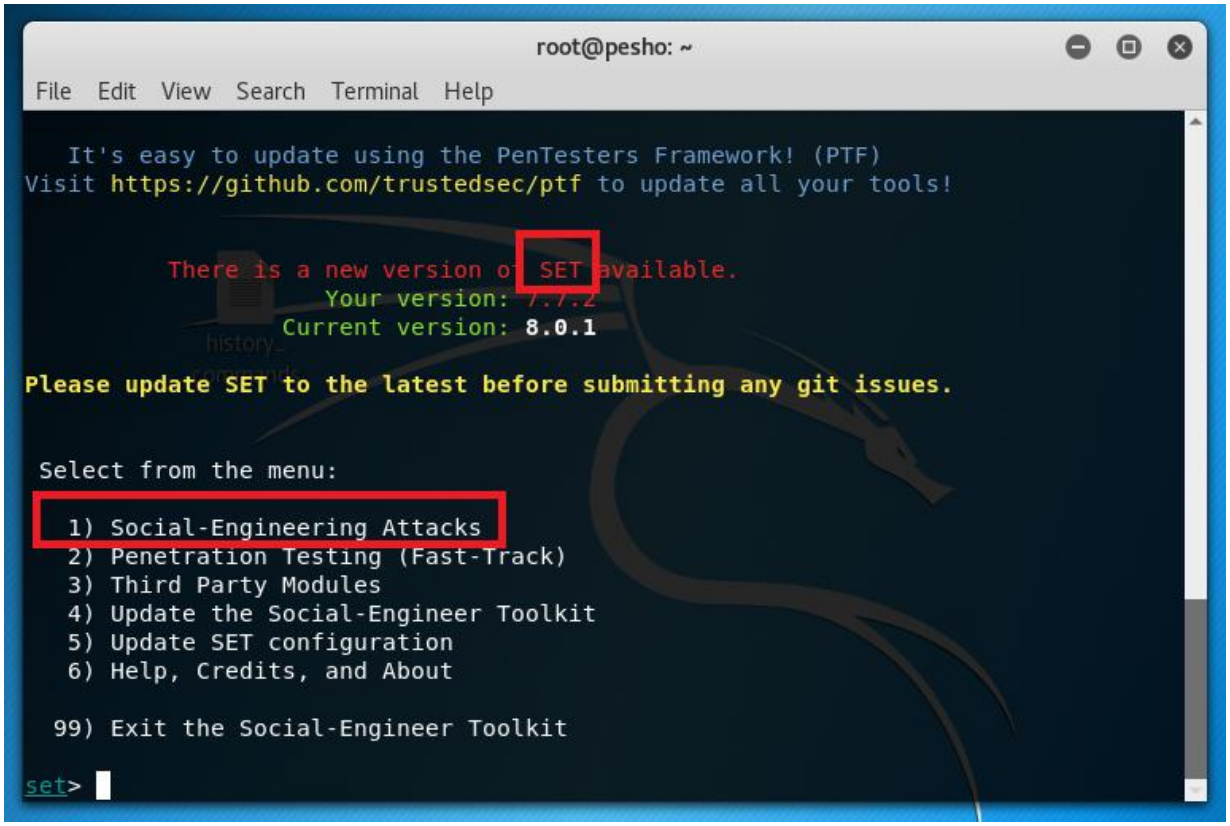


Figure 1. Initial screen of the toolbox SET

After the initialization of the toolbox the main menu is being visualized. Then menu number 1 with name "Social-Engineering Attacks" is selected. A new menu appears with possible attack vectors. It consists of 11 different attack vectors, which on Fig. 2 are shown.

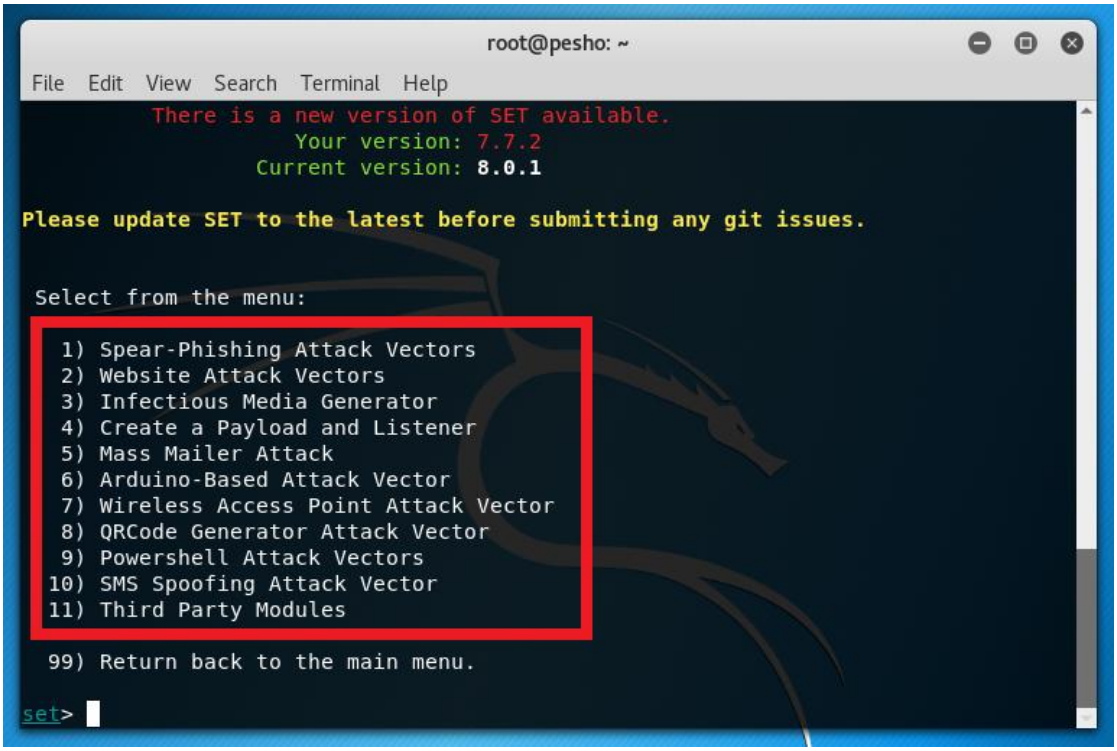


Figure 2. The attacking vectors

Menu „Website Attack Vectors" consists of the following attacking methods:

1) Java Applet Attack Method;
2) Metasploit Browser Exploit Method;
3) Credential Harvester Attack Method;
4) Tabnabbing Attack Method;
5) Web Jacking Attack Method;
6) Multi-Attack Web Method;
7) Full Screen Attack Method;
8) HTA Attack Method.

The most appropriate attacking method is Credential Harvester Attack Method. It will utilize web cloning of a web site that has a username and password field and harvest all the information posted to the website. The next menu displays three options (shown on Fig. 3).

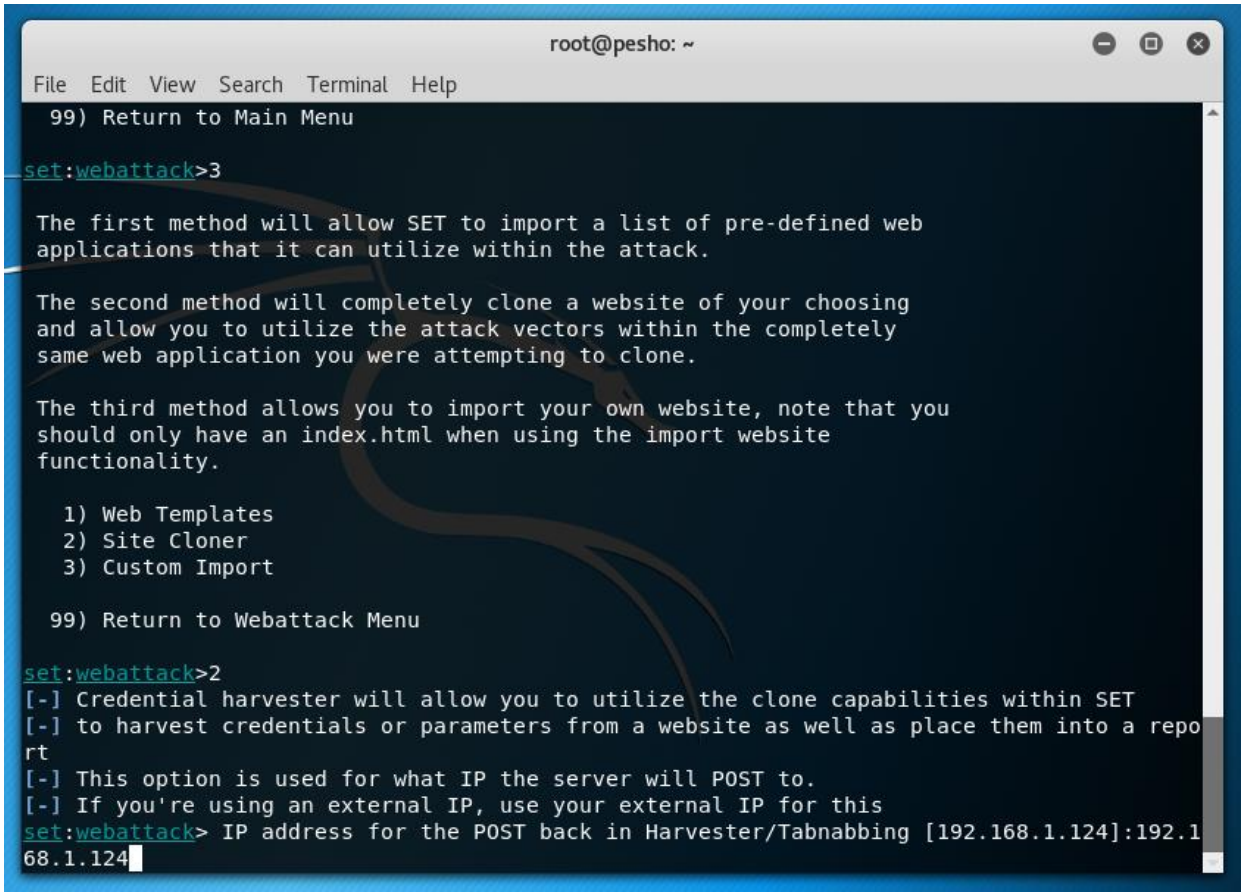


Figure 3. The menu of Credential Harvester Attack

After selecting "Site Cloner" the program asks for the IP address that the cloned site will contact when it is opened on the victim's computer. The IPv4 address of the attacking machine is 192.168.1.124. If this attack is carried out over the Internet, the public IP address is entered. When using a public network and a router, the port to be used for the connection will need to be routed from the router to the attacker's private address.

The last parameter that must be entered is a web page that will clone. The URL of the cloned web site will be - https://twitter.com/login. This is shown on Fig. 4.

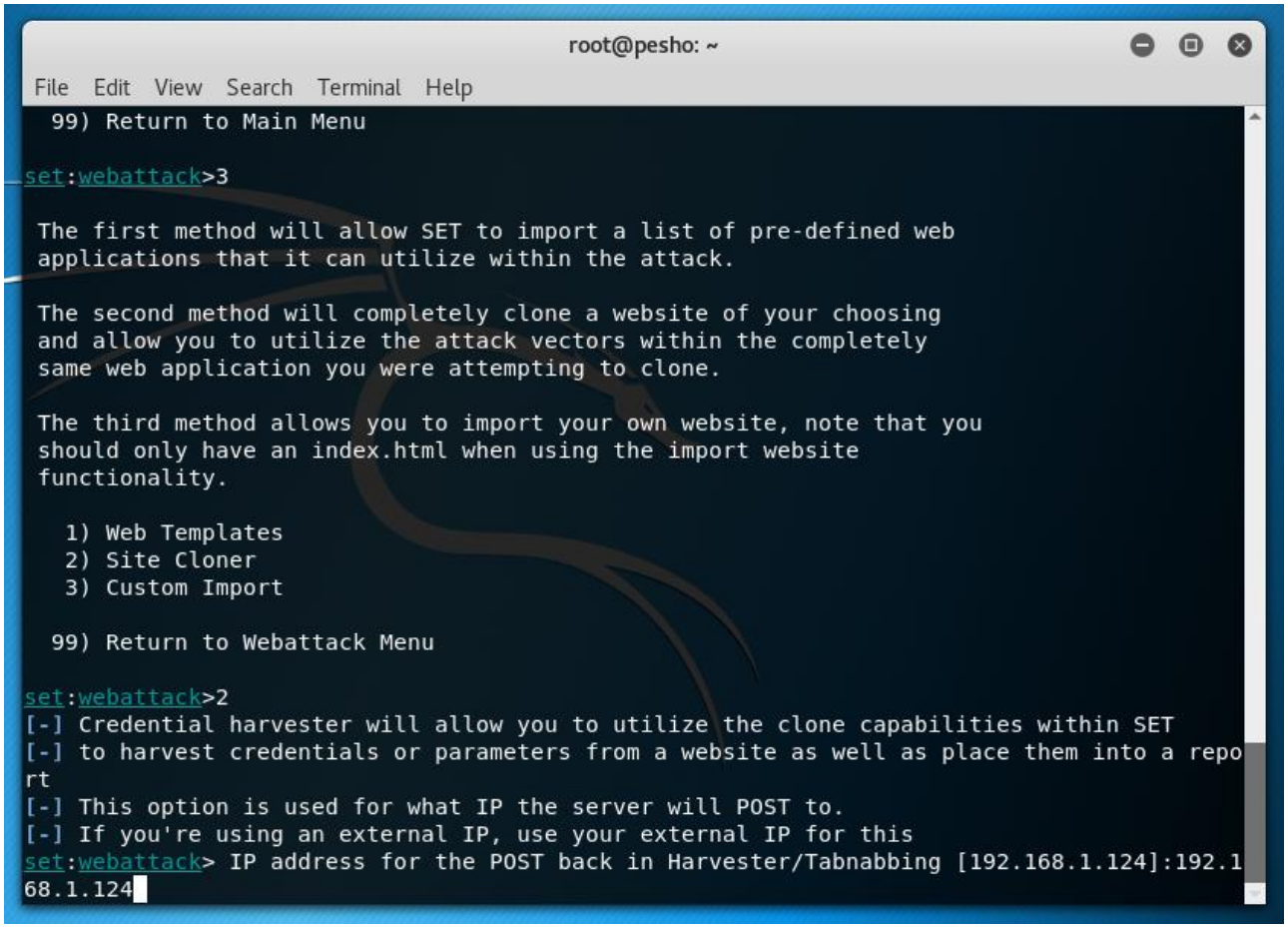


Figure 4. Credential harvester parameters

After that the Credential harvester vector is running on port 80 and clones the web site https://twitter.com/login. When everything is configured, then the victim computer is expected to enter their data on the cloned website and this is shown on Fig. 5.

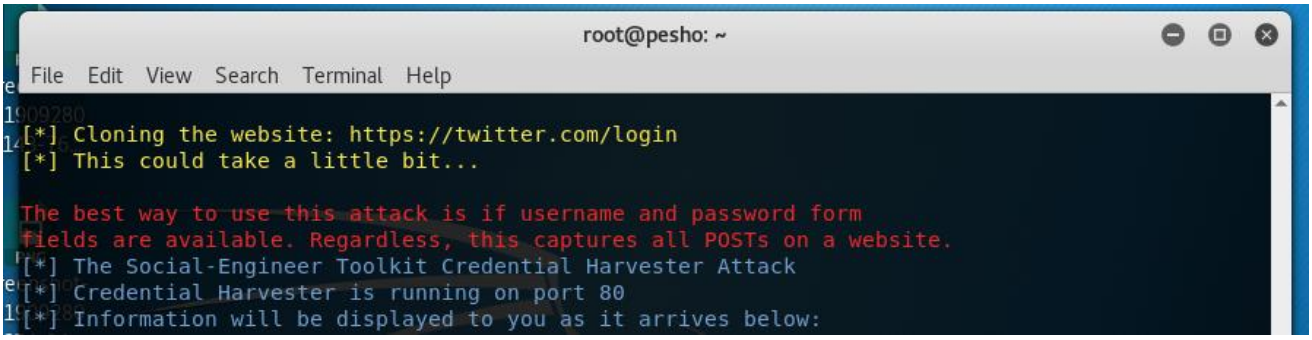


Figure 5. The configured parameters of the Credential harvester vector attack

When the victim's computer enters its information, then it will appear on the screen in plain text format. After that the victim will be redirected to the official Twitter web page. The victim

Fig. 6 illustrates the loading the Twitter cloned web site with IPv4 address of the attacking machine. Fig. 7 shows the process of entering the username and password of the victim with working operating system Windows 10 Pro x64. The victim's web browser Google Chrome version 77.0.3865.90 is used.

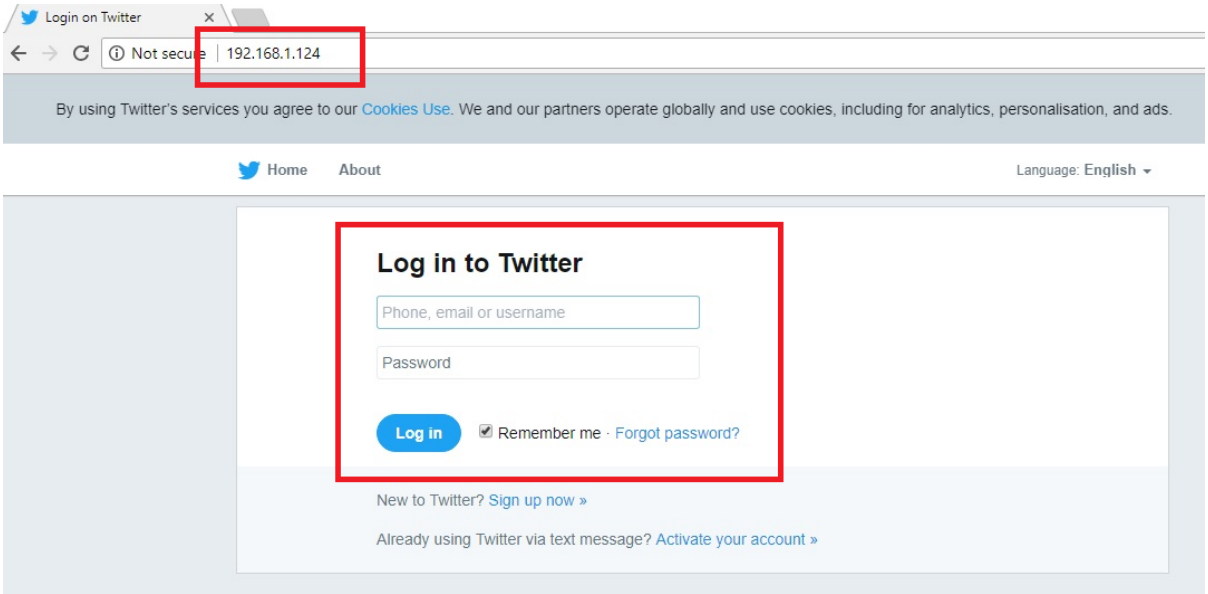


Figure 6. The Loading the Twitter cloned web site

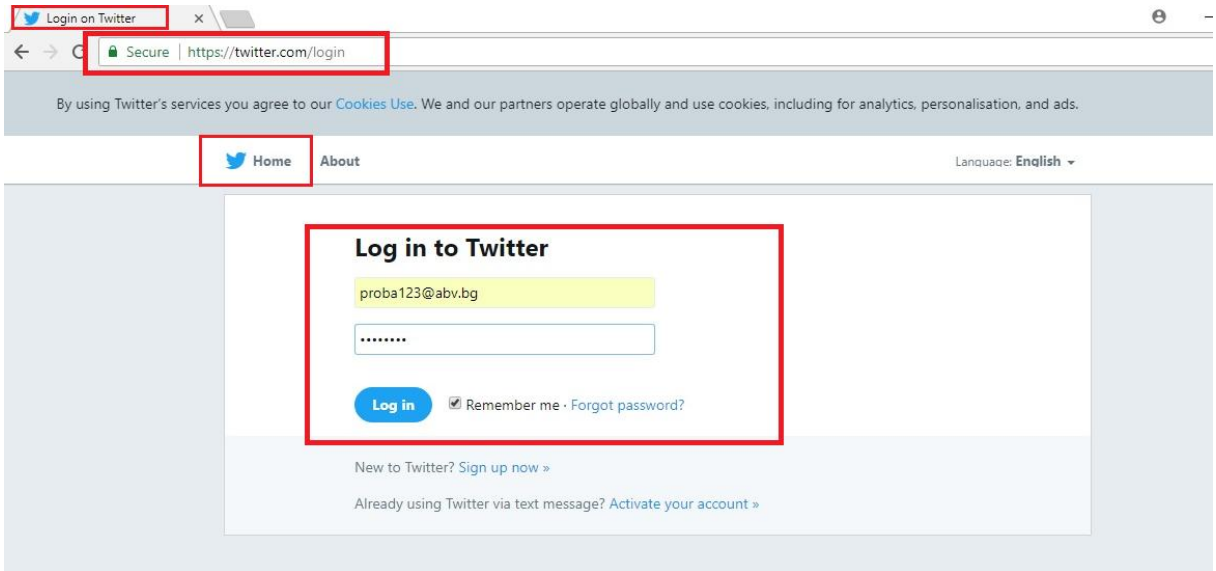
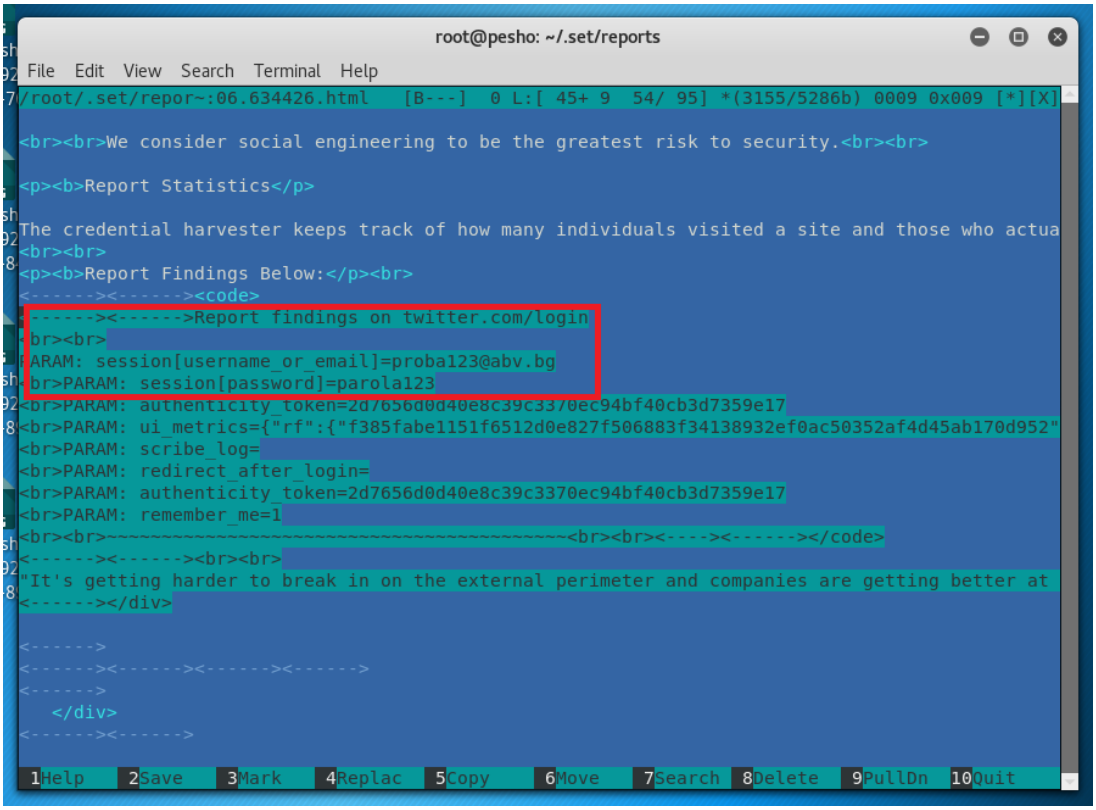


Figure 7. Entering the username and password of the victim

The possible found username or email is "proba123@abv.bg" and possible found password is "parola123". The fetched information is saved as a report file. The content of the generated report file is shown on Fig. 8.

NOTE: All of the scientific experiments and studies in this paper were conducted in a specialized computer lab at the Faculty of Technical Sciences at the Konstantin Preslavsky University of Shumen, consisting of several hosts. Everything illustrated and explained in this paper is for research purposes and the authors are not responsible for any misuse.



```
/root/.set/repor~:06.634426.html   [B---]  0 L:[ 45+ 9  54/ 95] *(3155/5286b) 0009 0x009 [*][X]

<br><br>We consider social engineering to be the greatest risk to security.<br><br>

<p><b>Report Statistics</p>

The credential harvester keeps track of how many individuals visited a site and those who actua
<br><br>
<p><b>Report Findings Below:</p><br>
<------><------><code>
------><------>Report findings on twitter.com/login
br><br>
ARAM: session[username_or_email]=proba123@abv.bg
br>PARAM: session[password]=parola123
<br>PARAM: authenticity_token=2d7656d0d40e8c39c3370ec94bf40cb3d7359e17
<br>PARAM: ui_metrics={"rf":{"f385fabe1151f6512d0e827f506883f34138932ef0ac50352af4d45ab170d952"
<br>PARAM: scribe_log=
<br>PARAM: redirect_after_login=
<br>PARAM: authenticity_token=2d7656d0d40e8c39c3370ec94bf40cb3d7359e17
<br>PARAM: remember_me=1
<br><br>~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~<br><br><----><------></code>
<------><------><br><br>
"It's getting harder to break in on the external perimeter and companies are getting better at
<------></div>

<------>
<------><------><------><------>
<------>
   </div>
<------><------>
```

Figure 8. The content of the generated report

Conclusion

Automated Information Systems and Networks Security Officers and the Security Administrator must take and take the following security actions, such as:

- Mandatory periodic change of employee passwords.
- Blocking an employee's user account if more than three or more unsuccessful attempts have been made. The blocking time can be set for 1 day.
- Use of special machines for destroying Schroeder documents. This way, the cybercriminal will not be able to find any stored sheets of paper in the organization's trash cans.
- Mandatory employee identification through unique ID cards, fingerprints, special uniforms, hand bracelets, eye retina scanners, and more.
- When there is an open day at the organization, there is a need for special staff to monitor all guests what they are doing and where they are going.
- Compulsory undergraduate special training courses for employees and signing special documents to ensure that they understand and comply with information security policies. In case the employee does not comply with the regulated internal rules, he is liable to criminal liability according to the Criminal Code and the Criminal Procedure Code of the Republic of Bulgaria.

References

1. Linko Nikolov, Krasimir Slavyanov, „*On the contemporary cybersecurity threats*“, I st CONFSEC 2017, 11-14.12.2017, Borovets, ISSN Print: 2603-2945, ISSN Online: 2603-2953, стр. 142-144; url: http://confsec.eu/sbornik/2-2017.pdf.
2. Linko G. Nikolov, Ognyan M. Fetfov, Angela R. Borisova, „SECURITY CONCERNS IN JAVASCRIPT CODING“, MATTEX 2018, Volume 2, part 2, CONFERENCE PROCEEDING, v. 2, pp. 27 – 31, SECTION Communication and Computer Technologies, ISSN: 1314-3921

3. Linko G. Nikolov, „*Wireless network vulnerabilities estimation*“, International Scientific Journal “Security & Future”, Vol. 2 (2018), Issue 2, pg(s) 80-82; WEB ISSN 2535-082X; PRINT ISSN 2535-0668
4. Nikolov, L., Slavyanov, V. Network infrastructure for cybersecurity analysis. International scientific conference 2018, “Vasil Levski” National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2018, ISSN 2367-7902.
5. Савова, Ж., Богданов, Р., *Анонимна система за комуникации в киберпространството, използваща протокол TOR*, Сборник научни трудове на научна конференция на Факултет „А, ПВО и КИС” „Новата парадигма за сигурност в киберпространството” Шумен 2014, стр. 259-265, ISBN 978-954-9681-49-9.
6. Савова, Ж., Богданов, Р., *Оценка на изчислителната сложност на алгоритмите за генериране на големи прости числа за целите на криптографията*, Сборник научни трудове на Научна конференция „Проблеми на информационната сигурност”, гр. Шумен, 2010, ISSN 1314-0647.
7. Савова, Ж., Богданов, Р., *Приложение на недвоичните псевдослучайни последователности в криптографията*, Сборник научни трудове Немус'2012. Институт по отбрана Проф. „Цветан Лазаров”, 2012, ISSN 1312-2916.
8. Досев, Н., Петров, В., *Съвременни тенденции и аспекти на информационната сигурност в автоматизираните информационни системи и мрежи (АИС/М)*, Научна конференция с международно участие MATTEX 2018 , Шуменски университет „Епископ Константин Преславски“, Университетско издателство, Сб. научни трудове том 2, част 1, стр. 85¸95, ISBN 1314-3921.
9. Фетфов, О., Боянов, П., Ташева, Ж., Трифонов, Т., *Анализ на съвременните видове уязвимости и експлойти в компютърните мрежи и системи*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско идателство „Епископ Константин Преславски“, ISSN 1311-834X, Vol. VI E, 2016, с. 112-122.
10. Savov, I., Edin pogled varhu sashtnostta na kiberprestapleniyata, spisanie „Politika i sigurnost”,VUSI, 2017, ISSN 2535-0358, s. 36-47.
11. Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.
12. Камарашев, Г., Димитрова, С., *Финансовия мениджмънт като елемент на военната логистика*, Trans&Motauto 2005 с.37-41.
13. Kamarashev, G., Dimitrova, S., *Outsourcing as a part of the management of resources for security and defense*, SIBIU 2011, pp.643-647.
14. Kamarashev, G., Dimitrova, S., A*spects of defence and security resource allocattion*, Sibiu 2007.
15. Kamarashev, G., Banabakova, V., *Acquisition – theoretical and practical aspects of application in the defense system*, Brno 2005 с.30-37.
16. Parashkevanova, G., Tsankov, Ts., *CERT Bulgaria*. Научна конференция с международно участие „Киберсигурността в информационното общество“, НВУ „Васил Левски“, Шумен, 2017.
17. Parashkevanova, G., Tsankov, Ts., *Cybercrime as the main contemporary threat to large organizations*, Conference proceedings Mattex 2016, ISSN 1314-3921.
18. Tsankov, Ts., Denev D. R., *Use in Internet of Protocols Transport Layer Security and its now-deprecated predecessor Secure Sockets Layer*. Annual of Konstantin Preslavski University of Shumen, Vol. VIII E, 2018.