Identifying the Security Vulnerabilities of Company Web Sites by using Uniscan

Emin Borandag[#1], Fatih Yucalar[#2]

[#] *Department of Software Engineering, Manisa Celal Bayar University*
Manisa, Turkey

Abstract *— When it is said "Information Security", web applications and information systems are the first concepts which come to mind. Actually, the security concerns people. Although our mission seems to protect information such as a company's customer list, citizens' tax information or military secrets, the main objective is to make IT infrastructure of the systems more secure for the leveraging users. This paper aims to identify security vulnerabilities of the systems by focusing both social engineering and system side.*

Keywords — *Social Engineering, Uniscan, XSS, SQL Injection*

I. INTRODUCTION

Most of the attacks that we face with today are man-made and similarly, it is the users that they target, not the systems. When the attacks that can be considered as "successful" and result in significant security breaches are examined, it is seen that humans are the primary target. It has been also recorded that the systems targeted by attackers have plenty of technical vulnerabilities. Exploiting technical vulnerabilities requires a certain level of technical skills and resources.

On the other hand, it is easy to eliminate these technical vulnerabilities with a patch or an update to be published. Yet, the vulnerabilities targeted by social engineering attacks are not the kind of vulnerabilities that can be eliminated by "patching" or "updating" since they are man-made. Similarly, the exploitation of these vulnerabilities could be prevented by finding a security solution to the vulnerable system such as a firewall. However, it will not be possible to connect the person using the system to a firewall [1].

In the second chapter of this paper, the concept of social engineering, the steps taken, the target staff and the tools used for attack purposes will be mentioned. In the third chapter, topics such as the security of system and information will be discussed. The fourth chapter will explain the way the security system tests are made with by using Uniscan. The final chapter will show the results and offer recommendations

II. SOCIAL ENGINEERING

Social engineering is the art of obtaining information from people by using technology or not. The thought of obtaining information or taking advantage by deceiving people is not something new. It has continued for thousands of years and its existence will continue as long as people live. These types of attacks are now widely used in many areas. Today, telephone scams targeting people from the world of science, art and business could be great examples to this situation.

Companies are equipped with the state of the art technology as a measure to ensure the system security and to maintain reliable and continuous operation of intra-nets and servers. Although the system is technologically working behind solid walls, the staff that will use this system should not be ignored. During the recruitment process, employees should be trained about the in-house confidentiality of the information, how the in-house process will be handled, or who (which department in the company) may have access to information. In this context, social engineering attacks are the attacks aimed at people and collecting the necessary information by using people's weaknesses. Target's ignorance, lack of attention and personal weaknesses are made use of during these attacks (if research is done about the target prior to the attack).

These people play a role in the attack according to the opposite actor. Generally, these attackers either try to have friendly relationship with these people or try to impress them by acting like being from the opposite sex (usually the target is male) or make use of the superior-subordinate relationship. The reason why attackers choose these types of attacks is that they do not want to waste their time by attacking directly to the system and that they develop methods that yields fast results. The purpose of social engineering attacks is to obtain everything that could be used against them in any attack such as the corporate structure, network structure, customer list, personal information of employees or managers (address, telephone, identity number, personnel number etc.), extension numbers and passwords. Tragicomic, but sometimes you deliver your passwords to attackers yourself.

The distribution of computer related events happened in the United States between 2001 and 2010 is given.

When the crimes happened in the United States are examined, it could be observed that laptop thefts rank number one with 21% and hackings rank number two with 16% while hacking a web site

ranks number three with 13% among computer crimes. Stolen computers, medias and drivers have a rate of 32%. However, these theft incidents cannot be directly considered as Social Engineering attacks since it is uncertain whether these incidents were made for cyber crime or for money. However, "Hacking" and "Cheating" incidents, carried out by using social engineering techniques has a rate of 24%, which is very high in real terms [2].

Example:

Question: Does shutting down a computer count as the safest way for protection? Is it possible to steal information from your computer when you are not in the office?

Answer: I am afraid that is possible. The attacker may enter a series of commands by making the security officer, secretary, or housekeeper open the computer by using various social engineering techniques, either by coming to the office or by phone if you are not in the office. You have to take security measures against these types of attacks. The reason I will state in the following chapters that "everyone is responsible for the information security" in certain companies is that each staff member such as the security officer, the caretaker, the secretary or the IT specialist, is on the radar of the attacker.

A. Staff Members on Social Engineer's Target

The attacker has a target group in your company for the attacks. Five of these target groups are given below [3].

- The employees who can be reached directly: These people are the ones who can contact customers or vendors directly. Technical service personnel or call center employees are in this group. Your employees in this position must be rigorously trained.
- Senior level employees: Employees who have privileged authority due to his position in the company are the people the mostly desired as a target by attackers. It would be harmful for the company if these employees, who have access to confidential information due to his position, are tricked into giving out information by attackers.
- Humanitarian employees: These people exceed their boundaries of authority to help and support their customers. Nonetheless, sometimes things can go wrong and a customer may turn out to be an attacker who wants to infiltrate your company. Employees should have certain authority boundaries and be reminded that they should act within the limits of their authority.
- Newly-hired employees: New employees, employees who have access to the system yet are not sure about how to use it, help desk workers or employees who may not differentiate between customers and attackers may create dangerous situations. These new employees ought to be well trained prior to being given access to the system and ought to be granted access authorization at the end of the trainings only if they are successful.
- Tricked or convinced employees: Active employees who lack commitment to the company or who consider leaving their job may be harmful to your company because of greediness or great promises made by the other person. Human resources or other employees in the company must report these people who exhibit negative behaviors to their supervisors.

B. Tools Used in Social Engineering Attacks

Attackers do not always use telephones or infiltrate a company in social engineering attacks. There are a number of tools that a social engineer can use according to his needs. For example, a USB Keylogger, which is too small to notice, may be installed between a senior employee's computer and his keyboard by an attacker who manages to enter the company physically. Of course, it involves some risks. He has to sneak in to take the USB Keylogger back and check the passwords saved. For instance, the attacker might give a senior employee a mouse, which acts as an audio surveillance tool, or a very expensive pen as a gift. Many tools like these are sold in the market. Anyone can buy them due to their low prices. Especially, larger companies and institutions need to take serious security measures against such tools shown in Fig. 1 [4].

Fig 1: The tools used in the attacks on social security.

C. Steps Taken in Social Engineering Attacks

Steps taken in social engineering attacks can be collected under four main headings: collecting information, building trust by building a relationship, taking advantage of the trust and making use of the information.

- Collecting information: This is the first step that a social engineer takes. He gets information from online, from newspapers even from you about the functioning of the company and about the arguments used in there. The reason he does this is because he wants to be able to give the right answers at short notice when a question is asked and use

these arguments frequently. This way, he can boost his credibility, thus access the information quickly.

- Building trust by building a good relationship: At this point, the attacker might try to build good relationships with his target both during working hours and out of office hours. He may prefer building a friendship based on trust at the office or may take advantage of the personal relationships developed out of office hours. Apart from all of these, he may convince your employee that he is an authorized person who can have access to the information or may introduce himself as a reliable source.
- Exploiting the trust: After obtaining enough information about the company, the attacker finds someone in the company who can give him the information he needs by winning his trust. At this stage, all he has to do is to gather the necessary information by asking the target the questions he has been prepared to ask.
- Making use of the information: The attacker checks the consistency of the information given by the victim. If he manages to obtain the information he needed, mission accomplished. The social engineer can start using this information in his favor as of this moment. If not, he goes back to the previous steps until the information he needs is given to him [5].

III. System Security

"Information security" has been one of the most controversial topics in a company. The concept of information security could be explained as a way to prevent the information from being acquired by undesired people or systems in all platforms by using the right technology properly with the right aim [6].

Companies ought to protect their information assets from damages. Company information security is based on preventing the information from being acquired by undesired people or systems in all platforms by using the right technology properly with the right aim. Increased risks, new regulations and compatibility obligations force people to create a solid "Information Management Security System" [7].

Since the system security is no longer network-based, end-to-end security becomes an inevitable solution as a measure. Therefore, solutions such as Firewall, which is a network-based security for companies, IPS, Web Security, End-user Security, Network Access Control, and Data Loss Prevention are regarded as essential components [8].

There are other attack methods deriving from certain vulnerabilities besides social engineering attacks mentioned above [9].

There are also some ready-made tools that businesses can use to secure their web sites. Uniscan, one of these tools, will be mentioned in the next chapter.

IV. Security Testing Using Uniscan

Uniscan is an open-source penetration testing tool written in perl. It can scan vulnerabilities on target web sites, folders and various security issues like XSS, LFI, RFI and SQL injection. Meanwhile, the administrator panel of the target web site can be found through directory check with Uniscan.

You can run Uniscan on Kali but you can also run it on Windows. If you are using Windows operating system, you can download and install Kali for Windows from the link given as a reference. In this way, you can run a "penetration test" on your Windows operating system for a web site [10]. To use Uniscan, open the terminal and type "uniscan".

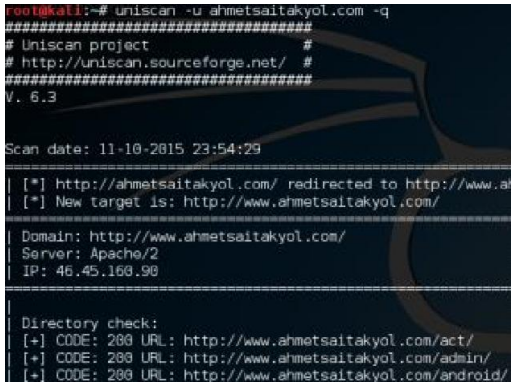

Fig 2: Running the program.

As seen in Fig. 2, the system gives different scanning options. For example, if you want to do a "–q Enable Directory Checks" on the target site, type "uniscan –u targetwebsite.com –q" in the terminal.

As shown in Fig. 2, when a directory check is performed on the web site, you have access to information such as admin panel and android related articles. The following Remaining test: 1194 gives the number of remaining index checks. It is also possible to find vulnerabilities on web sites through Uniscan scanning. The scanning options are given below:

uniscan –u targetwebsite.com With the –d command gives you XSS and RFI vulnerabilities in the system.

uniscan –u targetwebsite.com –s command gives other vulnerabilities in the system (SQL injection, XSS, RFI).

You can make a search with multiple inputs. See Fig. 3 for an example to that. You can type "uniscan –u targetwebsite.com – qweds" in terminal and run the command. This command respectively scans starting from "q" to "s".

q: Active Directory Control.
w: File Control.
e: shows URRobot.txt file.

d: scans XSS, RFI and Backup Files vulnerabilities in the system.

q: scans SQL injection, XSS and RFI vulnerabilities in the system.

Fig 3: Uniscan commands.

V. CONCLUSIONS

It is of utmost importance to ensure the data safety in the virtual environment since the information and data are transmitted to digital media. The most important issue is cyber attacks which threatens the information security of companies and organizations. As mentioned in the report, cyber attacks can be carried out using social engineering or the vulnerabilities on the system. Since social engineering based attacks constitute a major part of the attacks, it is possible to prevent them using the methods described in the report. Some ready-made security tools can be used to fix the system security vulnerabilities. A ready-made security tool such as "Uniscan" can be used to fix security vulnerabilities in web sites by using various commands.

REFERENCES

[1] (2017) Alper Basaran website [Online]. Available: http://alperbasaran.com

[2] (2017) Bilgi Güvenligi [Online]. Available: https://www.bilgiguvenligi.gov.tr/son-kullanici/index.php

[3] Kevin D., "*Aldatma Sanatı Yazar*:" Mitnick Yayınevi: ODTÜ Baskı. 2013

[4] (2017) Bilgimi Koruyorum [Online]. Available: http://www.bilgimikoruyorum.org.tr/?b320_"sosyal_muhendislik"

[5] (2015) Elektirik Mühendisleri Odasi [Online]. Available: http://www.emo.org.tr/ekler/288230da37dbf3cek.pdf

[6] G. Canbek, Ş. Sağıroğlu, "*Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri*", 2006.

[7] Ş.Sağıroğlu, "*Bilgisayar Güvenliğine Giriş Ders Notları*", Gazi Üniversitesi, 2012.

[8] A. Conklin, G. White, D. Williams, C. Cothren and R. Davis, "*CompTIA Security+ All-in-One Exam Guide*", Fourth Edition, McGraw-Hill Education, 2014.

[9] G.Erdoğan, Ş.Bahtiyar, "*Sosyal Ağlarda Güvenlik*", Akademik Bilişim, Anadolu Üniversitesi, Eskişehir, 2015.

[10] (2015) Uniscan Software [Online]. Available: http://sourceforge.net/projects/uniscan/