Innopolis University

SYSTEM AND NETWORKING ENGINEERING

Secure of Systems and Networks

Lecturer:

Rasheed Hussain

Project

Automated Socio-Technical Testing

Project Team:

1. Nikita Mokhnatkin
2. Niyaz Kashapov
3. Sergey Grebennikov

Submission Date : January 22, 2019

Abstract

In the current state of Information Technologies, each serious software and information system includes a very efficient information security system. Companies increase the level of information security by using new technologies, methodologies, and implementation of new solutions and software products. The hacking process becomes harder and complicated, requires more resources to theft a confidential information. And more often, hackers use another vulnerable part of the companies - employees of the companies. Over the past 5 years, incidents involving phishing and social engineering have become more relevant and frequent. And companies need methods and tools to test and find employees with low digital literacy, whom increases the probability of the violation of information security. The goal of the project is to create a solution for conducting social and technical testing of the company's employees.

Contents

1 Introduction

Each information system consists of three main parts: Technologies, Personel, Processes. Often companies spend big money on new technologies and protection of computer equipment. Computers can be protected as efficiently as possible, however, employees themselves can become a threat to information security. Socio-technical testing is aimed at testing and protecting employees and companies from security threats.

Sberbank's Cybersecurity Department found more than 600 domain names are used for providing phishing attacks, and more than 1300 sites that have distributed malicious software. Kaspersky's "Antiphishing" system prevented 46,557,343 attempts to switch to phishing pages.Phishing and social engineering are closely related to socio-technical testing.

The companies are interested in testing of employees. And this procedure is provided by outsourcing companies. But these companies test personnel manually: collect information, analysis data, perform tests, send messages, aggregate results. These companies test personnel manually: collect information, analyze data, perform tests, send messages, aggregate results. Thus, security tests take a long time and require a lot of resources. The testing process disrupts the normal business process, which creates additional chores and problems for companies.

The main problem of socio-technical testing is a large amount of material and time resources. The solution to this problem is the automation of testing processes. This reduces costs and increases efficiency.

2 Related Work

To date, almost all companies use manual testing of personnel. During testing, various tools are used, including the well-known "Social Engineering Toolkit (SET)", which is part of Kali Linux. There are companies specializing in protection against phishing, but they do not conduct targeted testing. For example, PhishMe. There are companies specializing in protection against phishing, but they do not conduct targeted testing. For example, PhishMe. The company may specialize only in education without identifying problem areas. For example, Abiroy company.

SafeStack Company attempted to develop AVA in 2015. AVA is a system for socio-technical testing of companies, also named "A Security Scanner for Human Vulnerabilities". Project was shown on the BlackHat 2015 conference. But the project is not completed and was closed at the end of 2015.

Large companies, like a Cisco and Qiwi, has its own socio-technical testing tools for inside testing of employees. These systems are very specific, and tests employees only from several sides of social engineering. Often, medium and small businesses test employees during the information security audit time, but in that case, social engineering testing is done manually. And the cost of these tests is very high.

3 Methodology

The term "social engineering" is sociological, but in the field of information security, the term was distributed by security adviser Kevin Mitnick, who argued: "The human factor is the most vulnerable place in any corporate system." [1]

Methods of social engineering are based on ways to access confidential data or motivation for action using technical or non-technical resources. But these methods were used long before the popularization of the term by Mitnick and before the computer era. For example, a group of researchers from doctors and nurses from three hospitals in the Midwest conducted a study in which psychologists on the phone were represented by doctors and asked nurses to inject a deadly dose of the drug to the patient. Despite the fact that nurses knew what they were doing, in 95% of cases, they unquestioningly performed the team (they were stopped by assistants at the entrance to the ward). [2]

All techniques of social engineering are

based on cognitive distortions[1]. These behavioral errors are used by social engineers to create attacks aimed at obtaining confidential information, often with the consent of the victim.

So, one of the simple examples is the situation in which a certain person enters the building of the company and hangs on the information bureau an advertisement looking like official with information about changing the telephone number of the Internet service provider's reference service. When employees call this number, an attacker can request personal passwords and identifiers to gain access to confidential information.

There are several threats related to social engineering: threats related to the phone; threats associated with e-mail; and threats related to the use of instant messaging. The phone is still one of the most popular ways of communication within and between organizations, hence it is still an effective tool for social engineers. Many employees receive dozens and even hundreds of e-mails every day through corporate and private mail systems. Of course, with such a flow of correspondence it is impossible to give due attention to each letter. Instant messaging is a relatively new way of transferring data, but it has already gained wide popularity among corporate users. Because of the speed and ease of use, this way of communication opens up wide possibilities for carrying out various attacks.

Specialists in social engineering identify the following basic protective methods for organizations:

- developing a classification policy that takes into account those seemingly innocuous types of data that can lead to important information;
- securing the protection of customer information by encrypting data or using access control;
- training employees skills to recognize the social engineer, manifestations of suspicion when dealing with people they do not know personally;
- the ban on personnel exchanging passwords or using a common one;
- a ban on the provision of information from the department with secrets to someone who does not know personally or is not confirmed in any way;
- use of special confirmation procedures for all who request access to confidential information;

The strongest protective method of social engineering is qualified personnel and suggest identifying weak employees with automated socio-technical analysis. This testing method allows to identify the vulnerability in the organization and take timely action.

4 Project Goals

The main goal of the project is to study various testing methods and realize them as an automated system for socio-technical testing.

The system must be usability. List of "victims" for testing would be provided from different sources. Active directory, LDAP or simple CSV file for example. It helps allows to exclude of extra work.

Another goal is to automate the process of collecting, analyzing and generating results. Socio-technical testing should provide estimated, objective and measurable information about the security of the company's personnel. Also that information should be represented inconvenient kind to easy and fast analysis.

5 Results and Analysis

The result of this project is the software solution, based on the web-server. A devel-

[1]Cognitive distortion is the concept of cognitive science, meaning systematic deviations in behavior, perception and thinking, conditioned by subjective beliefs (prejudices) and stereotypes, social, moral and emotional causes, failures in the processing and analysis of information, and physical limitations and peculiarities of the structure of the human brain.

oped product is consist of four main part:

- Main logic – Those modules responsible for proceed attacks to users. Frequency of attacks, types of attacks and send malware to users via e-mail and social networks.
- Collector – Those modules responsible to collect interact information from users.
- Front-end – Those modules represent all collected information to graphs and reports. Also it provides a web interface for administrator of test.
- Data storage – Database that store all data that necessary for system.

5.1 Data and Platform

by Sergey Grebennikov

Amazon Web Services was used as a computing platform for LAMP[2] web services stack, that is suitable for building dynamic web sites and web applications. The testing environment is a dynamic website with a user-friendly interface. The user simply needs to upload information about employees, where, in addition to basic information, the e-mail, phone number and social network account are also required. All data should be uploaded by using the CSV file format, which can be made by any editor, but for convenience it is preferable to use Excel or Calc office suites. After uploading files using a PHP script, the data is sent to a database containing four tables for storing, processing, and logging events. This data is used by the main logic module and collector to generate a report on the work performed. The report can be presented as a visual graph or as a table.

5.2 Main Logic module

by Nikita Mokhnatkin

Main module fully implemented on Python 3. The first function is a planning of test. The test have feature "intensity". That feature are changing a frequency of sending different tests to users. It provides a possibility to adjust intensity and quantity of test that will be sent to users. If the head of customer company wants to get results fast or to get quality results. After intensity was chosen the application randomly select a victim from victims list. Then it selects a type of attack. There are 6 main types of attack:
1) Fake mail
2) Phishing bank page
3) Bat-script that veiled like a photo
4) Malware in .PDF
5) Malware in .exe file
6) Social network message
Then that type of attack sends to the client with a special message with link or file that contains an identifier that refers to special user ID and event ID. The message looks like letters from support or security services but contains links or some attachments with malware files.

5.3 Collector

by Niyaz Kashapov

Apache Server with PHP page is a collector for incoming events. Each of the types of attack contain 'GET' request to server in the following form:

```
http://ip-address/info.php?id=21&event=5
```

This request contains two parameters - the first one is the identification number of the target user, and the second one is event's weight.The weight of the event allows you to determine what type of attack has worked and allows you to assess the severity of the

[2]The names of the original four open-source components: the **L**inux operating system, the **A**pache HTTP Server, the **M**ySQL relational database management system (RDBMS), and the **P**HP programming language.

attack. All requests are stored in the Test table of the database. Also, each event writes to the database with a current time. It is required to evidence of the event.

5.4 Front-end

by Niyaz Kashapov and Sergey Grebennikov

All results are stored in the MySQL database. But this is not a readable form of information. It is necessary to represent this information in a more useful form. Results module is a part of Front-end. To get table form, simple PHP code is used. All information is got from the database to the HTML table. The VivaGraph.js library is used to build a graph. All collected information is transformed into the JSON form, and after that are sent to the HTML page. JavaScript code draws a graph with employees. The color of the employee in the graph shows the level of vulnerability.

The Graph and Table allow showing all picture of vulnerable employees in the company. The results obtained during the work can form the basis for the development of the Security Awareness Program, which is maximally focused on the problem areas identified during testing and can also be useful for testing the effectiveness of the current Customer Awareness Program.

The system has the main page, that allows controlling the testing process. User or administrator should upload the CSV file with information about employees. After the uploading, the testing process is started by pushing the next button. The testing process runs for 1 to 15 days, depending on the number of employees.

After the testing time, the user can query the results in one of the two ways (Table or Graph) by pushing one of the buttons.

6 Conclusion

The developed application provides basic tools for testing the employees inside the company. Preparing visual interpretation of results that show the weakest users in the structure. Also it easily scalable for new tests or types of attacks. That application allows evaluating a level of knowledge of employees in basic information security and ecology of information. Furthermore, that application can help to develop new educational programs for reducing risks to catch a malware or data leak by unintentional users actions.

The solution is based on open source software and allows you to effectively test the company and get an objective assessment of employee awareness. The testing procedure is of low cost in comparison with competitors. Also, it can be carried out along with a regular audit of information security without any disturbing of business-processes.

7 References

[1] "Kevin Mitnick sentenced to nearly four years in prison; computer hacker ordered to pay restitution to victim companies whose systems were compromised" (Press release). United States Attorney's Office, Central District of California. August 9, 1999. Archived from the original on June 13, 2013.

[2] Influence: The Psychology of Persuasion, Revised Edition by Robert B. Cialdini