Service for Vulnerabilities Analysis and Security Assessment of Open Source Systems

Anastasiia Strielkina, Artem Tetskyi, Bogdan Selin, Oleksandr Solovyov, Dmitriy Uzun

***Abstract*—**The article describes the service for vulnerabilities analysis and security assessment of open source information systems. The article deals with determination of information security threats and vulnerabilities and actuality of protection sensitive information. The service that will help to improvement information security from cyber-attacks has been considered. The most valuable components of web-application penetration testing are shown. Also it is spoken in details about SQL-injections, brute-force, potential damage assessment model and device for anonymization. Operation principles of this device are described. The article can be used by information security specialists, network administrators and owners of web-resources and wireless networks.

***Keywords*—** anonymization, brute force, open source, penetration testing, damage assessment model.

I. Introduction

For today informatization is one of the priority development directions of all economic sectors. Almost each organization, commercial or governmental, has its own website and introduces all kinds of online services. Personal information of customers and employees, financial information and economic activity data are stored in electronic form. Therefore the task of ensuring security of web applications is becoming more important every year. Unfortunately, the developers of corporative information systems do not always follow the safety requirements [1] - due to lack of the necessary experience, or simply focusing on the development of other system purposes. The annual researches indicate that a large number of web applications contain high risk vulnerabilities, which may cause financial or reputational damage [2]. Exactly an attack against web applications is often the first step on the large companies' networks hacking and a publication of owner discrediting information on the official web sites serves as a weapon in the information war. All these suggest that the international community is in dire need of qualified information security specialists at the present time.

II. Topicality and Problems

The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit. And for today there is a rapid growth in the number of Internet resources, practically each organization has its own website. The functionality of sites varies, ranging from business card sites and ending with online stores, auctions, etc. Due to various content management systems, website creation does not require knowledge of programming languages and, especially, the knowledge of information security aspects. Therefore, the following problems occur:

1) Resource owners do not care about the security of their sites. Most of the owners begin to

A. Strielkina, National Aerospace University, Kharkov, Ukraine (e-mail: strelkina.anastasiya@hotmail.com).
A. Tetskyi, National Aerospace University, Kharkov, Ukraine (e-mail: artem.tetskiy@csn.khai.edu)
B. Selin, National Aerospace University, Kharkov, Ukraine (e-mail: selin.bv@gmail.com).
O. Solovyov, National Aerospace University, Kharkov, Ukraine (e-mail: extsand@gmail.com).
D. Uzun, National Aerospace University, Kharkov, Ukraine (e-mail dmitriy.d.uzun@gmail.com).

pay attention to security after attack on their site. If a site is, for example, an online store, the consequences of such an attack may carry substantial material damage. Other good example is PlayStation user data loss due to PlayStation Network service disabling in 2011. This hack has brought the loss to the company and caused the damage to users [1].

2) Not all developers have a sufficient knowledge level in the information security field. Topical example is the development of various plugins and modules for open source content management systems. Before the community or users will find a vulnerability in a component, that component will be already installed on some web-sites. Perhaps vulnerability will be closed in this component future releases, but there is a problem again - the resources owners do not follow the used software upgrading in a timely manner.

One of the main threats is cyber-attack on the target system.

Targeted cyber-attacks on resources often lead to the following consequences:

– the loss of important information can harm the competitiveness in the market (industrial and commercial espionage);

– the vulnerabilities presence in the system predetermines the potential financial loss (a denial of service, loss of profit, commercial espionage, fraud);

– loss of productivity.

III. Condition of the Problem and Existing Solutions

Thus, to prevent emergence/reduce risk of the aforementioned consequences is necessary to organize comprehensive protection against cyber-attacks.

There is a special testing to detect existing vulnerabilities in the studied system - penetration testing. This testing is a simulation of malicious attacks.

Conducting the penetration testing procedure is necessary to provide to user information about the real state of information security in the system.

Penetration tests are usually performed using manual or automated technologies to systematically compromise servers, endpoints, web applications, wireless networks, network devices, mobile devices and other potential points of exposure.

Providing of services for conducting penetration testing is not new. There are tools, methodologies and standards for penetration testing. Most of the necessary tools were assembled in the operating system Kali Linux [3], [4]. Kali Linux is a Debian Linux based Penetration Testing arsenal used by security professionals (and others) to perform security assessments. Kali offers a range of toolsets customized for identifying and exploiting vulnerabilities in systems.

It is also developed and actively applied testing methodology described in the OWASP Testing Guide. And Penetration Testing Execution Standard describes all the stages of testing.

Most of web applications testing methodologies are based on OWASP (Fig. 1) [5], [6].

Thereby the procedure for penetration testing should follow the steps described below [7].

1) Research information about the target system. Computers that can be accessed over the internet must have an official IP address. Freely accessible databases provide information about the IP address blocks assigned to an organization.
2) Scan target systems for services on offer. An attempt is made to conduct a port scan of the computer(s) being tested, open ports being indicative of the applications assigned to them.
3) Identify systems and applications. The names and version of operating systems and applications in the target systems can be identified by “fingerprinting”.
4) Researching vulnerabilities. Information about vulnerabilities of specific operating systems and applications can be researched efficiently using the information gathered.
5) Exploiting vulnerabilities. Detected vulnerabilities can be used to obtain unauthorized

access to the system or to prepare further attacks.

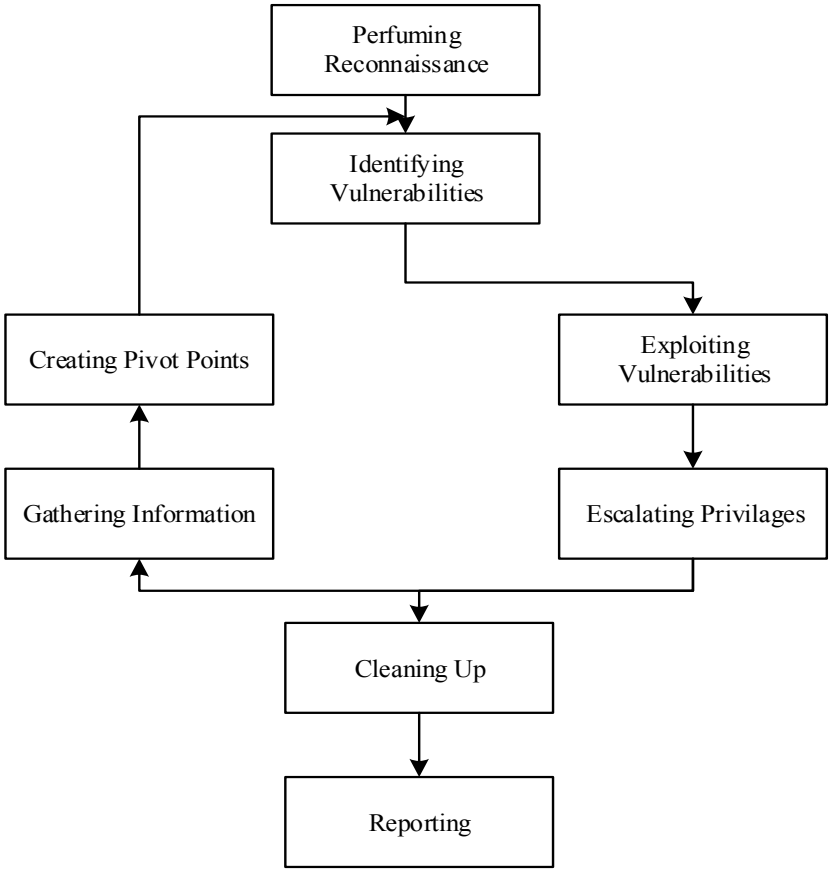

Fig. 1. OWASP testing methodology

Client goals that can be attained by penetration testing can be divided into four categories:

1) Improving security of technical systems.
2) Identifying vulnerabilities.
3) Having IT security confirmed by an external third party.
4) Improving security of organizational and personnel infrastructure.

The result of an IT penetration test should therefore be more than just a list of existing vulnerabilities; ideally it should also suggest specific solutions for their elimination.

So penetration verification is a reliable method for information security, which confirms the breaking possibility not only theoretically, but also empirically. Penetration testing can provide valuable insight into company's risk exposure, including resistance to real world-style attacks, level of sophistication required to compromise systems, countermeasures that mitigate risk, attack detection and incident response etc.

There are companies that provide penetration testing services in Ukraine for today:

– "Active Audit Agency";
– "FireEye";
– "AMI";
– "Berezha Security".

The main drawback of these companies is the price for provided services.

So it is necessary to have a service that provides penetration testers with an acceptable price / performance ratio.

IV. Obtained Results

Service for vulnerabilities analysis and security assessment of open source systems is a comprehensive solution in the field of cyber security that will help to eliminate security breaches (identify and prevent cyber-attacks at every stage of invasion), protect valuable information and ensure data confidentiality with the help of technology, intelligence, knowledge and skills of the project team.

The service is based on open source software and does not contain proprietary software.

The implementation of actions is carried out both from a position of an insider and external potential attacker and involves active using of security vulnerabilities.

A. Web-Vulnerabilities

According [8] to describe web-application penetration testing can be used Markov processes.

In general, the description of the web-application penetration testing as graph is shown on Fig. 2

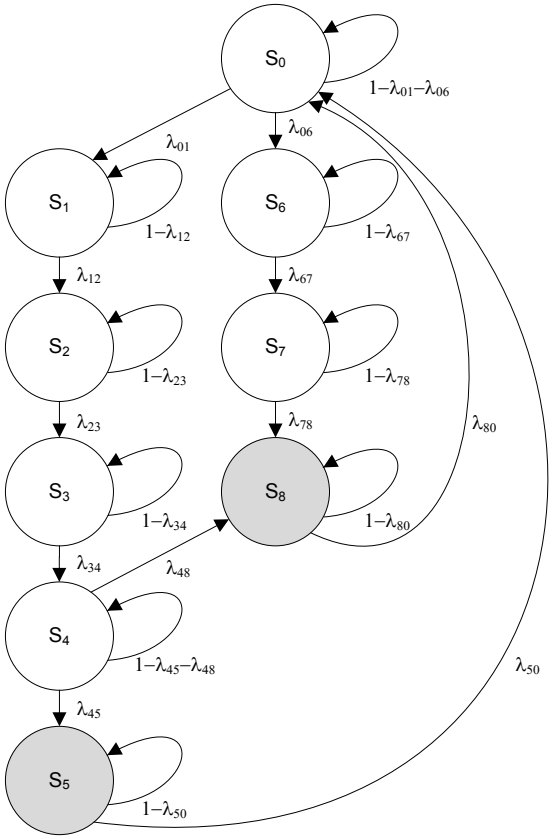

Fig. 1 State graph for web-applications testing

Meanings of the states graph that is shown on Figure 1 are:

S_0 – initial state without any concrete knowledge;

S_1 – content management system and its version are known;

S_2 – all vulnerabilities identifiers are known;

S_3 – critical vulnerabilities identifiers are known;

S_4 – exploits for critical vulnerabilities are exist;

S_5 – vulnerability exploitation (excluding SQL-injection);

S_6 – paths to data processing scripts are known;

S_7 – the scripts without input data sanitization are found;

S_8 – SQL-injection exploitation.

Table I shows the transition probabilities for the graph shown on figure 1.

TABLE I
THE TRANSITION PROBABILITIES FOR THE GRAPH

from \ *to*	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
S_0	$1-\lambda_{01}-\lambda_{06}$	λ_{01}					λ_{06}		
S_1		$1-\lambda_{12}$	λ_{12}						
S_2			$1-\lambda_{23}$	λ_{23}					
S_3				$1-\lambda_{34}$	λ_{34}				
S_4					$1-\lambda_{45}-\lambda_{48}$	λ_{45}			λ_{48}
S_5	λ_{50}					$1-\lambda_{50}$			
S_6							$1-\lambda_{67}$	λ_{67}	
S_7								$1-\lambda_{78}$	λ_{78}
S_8	λ_{80}								$1-\lambda_{80}$

In Table I λ_{ij} is a probability of transition from state S_i to state S_j.

For example, it is possible to go into state S8 by two ways:

1) By finding vulnerable page with CVE-ID from the state S4;
2) By testing all pages from the state S7.

This graph may be expanded with new vulnerabilities by adding new columns for appropriate vulnerabilities.

Also during the research the methods of getting the database contents using SQL-injections have been identified experimentally. Fig. 3 shows these methods.

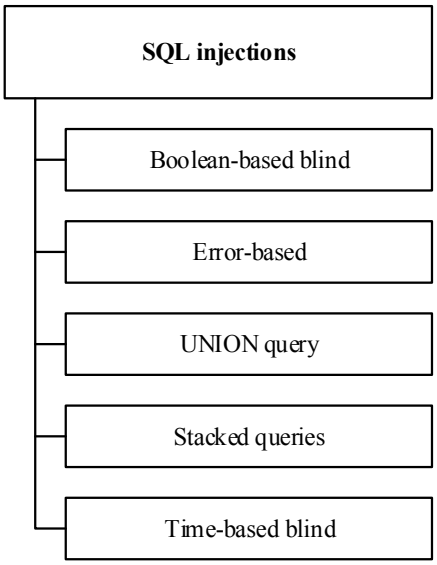

Fig. 3. Varieties of SQL-injections

1) Boolean-based blind SQL injection.

The method is based on the selection of the code table symbol number by adding structures using operators AND/OR. A feature of this method is that the information obtained from the database is not displayed. Binary search algorithm is used, so to get a single character an average of 7 database queries should be executed. For the Unicode characters it need more requests because code range becomes wider. Therefore, due to low speed and high load on the server, this method is not suitable for obtaining large amounts of data.

2) Error-based SQL injection.

This method is based on the fact that the contents of the cell is included in the error text

generated by the database server as a result of an incorrect request. With a single query it is possible to get the contents of a single cell. This method is possible only when the script displays an error returned by the database server. Using MySQL database in PHP the following construction exists:

mysql_query("...") or die(mysql_error());

It is important to prevent error messages displaying in the browser.

3) UNION query SQL injection.

This method is classic and the easiest for understanding injection of SQL-code. The principle is to combine two SELECT queries with the operator UNION. The peculiarity is that the number of columns in queries should be the same. If the result of the query is processed in a cycle, then one query can get contents of several columns in the table (depending on the number of columns in the first query).

4) Stacked queries SQL injection.

The principle of this method is using multiple queries to the database, separated by semicolons. It is the most dangerous injection type because requests may occur to insert/update/delete records. Therefore, using of stacked queries in PHP + MySQL is prohibited for safety reasons.

5) Time-based blind SQL injection.

This method is a modification of the first method, because similar principle to obtain information is used. In the «Boolean-based blind» method a sign of fulfillment of the condition is the withdrawal of the correct result, in this method such feature is the implementation of a time delay in a database query..

By comparing the time of query with the correct parameter with the time of a query with a parameter that contains the SQL-code, it can be concluded that the condition was performed in the modified SQL-query. Delay is produced using the SLEEP(). The presence of these delays is the additional drawback of this method.

As a result of research the methods of getting contents of the database were identified, these methods are confirmed by the sources [9]. The SQL-injection should not only compromise the database, but also gain full access to the server (at the confluence of certain circumstances). To prevent this kind of attack it is strongly recommended to avoid the simple concatenation of parameters in queries, instead using the appropriate drivers (for example, PDO in PHP to work with MySQL).

During the research penetration testing has been conducted of such large web-sites:

1) Internet-shop "Tehnomaster".
2) Internet-shop "Mobilluck".
3) The conference "Dessert" site.
4) National Aerospace University “KhAI” site.
5) Computer systems and networks department (NAU “KhAI”) site.

A vulnerability was detected on one of the sites via which was held SQL-injection, which led to the the database compromising, that stores information about employees. Also in the database stored the password in an unencrypted form, so it was accessed to the admin panel.

B. Hardware and Software System for Anonymization

One of the main components of penetration tester secure work is the anonymity of his activities. For this purpose it is necessary to have networking device-anonymizer that allows access to the Internet regardless of reception and transmission device settings and furthermore provides anonymous access to the Internet. This device may be useful not only to penetration tester, but also for secure Internet surfing, safe data transferring and to bypass censorship in places where Internet access is limited.

This device is based on microcomputer, additional standardized equipment (i.e. case for microcomputer, microSD memory card, Wi-Fi adapter, power source, Ethernet cable), open source operating system and a set of additional services (i.e. DNS, Gateway, Router, DHCP client, ISC DHCP server, Hostapd, service Tor and etc.).

After configuring the microcomputer, additional equipment and the operating system components (services) can be obtained anonymous access to the Internet.

This device encrypts all web traffic, not just the traffic that arrives from one program. That is, there is no need to download additional software or set up accounts, register. It is only necessary to connect the device to the Ethernet interface and user can connect to an anonymous Wi-Fi network.

Anonymizer operating principle can be divided into levels (Fig. 4).The first level is the network gateway, which is needed to convert the protocols among different network model levels. This layer functions as router - receives a signal from the network cable, converts into the protocol that is required and sends it to the recipient address. Also there is the Domain Name System (DNS) on the first level which is responsible for converting network nodes domain names into IP addresses. The second and third levels are Dynamic Host Configuration Protocol (DHCP), responsible for IP addresses distribution among clients, which are connected to the access point. The fourth level is a service (daemon) Hostapd, which is designed for server access points, security configuration and authentication that is for conversion the microcomputer to the access point. Thus, at this stage, devices can connect to the configured access point. The fourth level is the service Tor that is responsible for traffic anonymization that passes through the access point by using a technology "onion routing" that encrypts the data and sends a lot of time through a large number of servers, each of which removes one layer of encryption. The sixth level is responsible for connecting end users to the access point and further access to the Internet through the configured access point on the microcomputer.

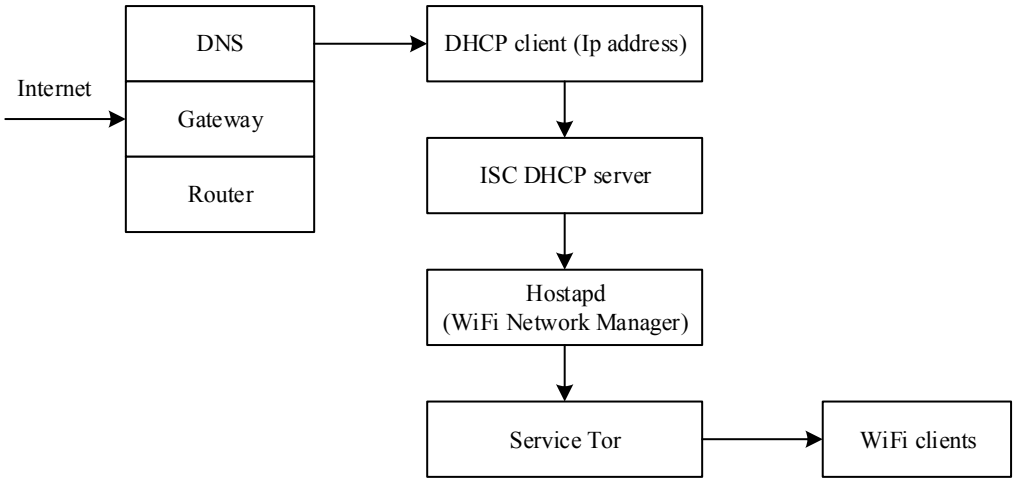

Fig. 4 Anonymizer operating principle

During the implementation of access to the Internet resources could leak user personal data (location, other personal information), and the using of the above described device allows to hide all the data.

C. Distributed Brute Force

For today one of the most common vulnerabilities is a possibility of making automated selection of the credentials and passwords (Brute Force Attack). A disadvantage that allows exploiting this vulnerability exposed almost 70% of the systems that ranks the second place in

the ranking of vulnerabilities after the "Cross-Site Scripting» (Cross-site Scripting, XSS) by rating of Positive Technologies [10].

An exhaustive search or so-called "brute force" is so common among hackers because it is suitable for attacks on almost any system because it can be used against practically any existing encryption method. More often, this method is used in cases when other weaknesses cannot be found in the system because despite the fact that brute force gives an absolute guarantee to solve the problem, it requires enormous time and (or) computing resources. This is due to the fact that the complexity of exhaustive search depends on the number of all possible solutions and may require exponential time operation. For example, using the alphabet of Latin letters and numbers of one register and speed of selection of 100 000 passwords per second on selection passphrase of 6 characters 6 hours, and the phrase from 8 characters - 11 months are required. Here are examples those shows the time required for password guessing using a processor i7 3840QM 4x3.8 GHz ~ 4700 pmk/s:

– 8-digit password: $\frac{10^8}{4700 \cdot 3600} = 5.91$ hours;

– 8-character password: $\frac{26^8}{4700 \cdot 3600 \cdot 24} = 514$ days;

– 10-digit password: $\frac{10^{10}}{4700 \cdot 3600 \cdot 24} = 24.6$ days;

– 10-character password: $\frac{26^{10}}{4700 \cdot 3600 \cdot 365 \cdot 24} = 952$ years.

The calculation was performed according to the formula:

$$T = \frac{d^c}{p \cdot t}, \quad (1)$$

where T – the result, time required for guessing a password; d – number of characters in the dictionary; c – number of characters in the password; p – speed of computing which gives the device; t – the number of seconds in an hour, hours in the day and so on (for a more convenient time display).

These numbers can instill that this method is ineffective, especially in order to ensure the best protection can be used alphabet of more characters (for example, Latin letters of both registers, numbers and special characters). However, human nature is such that the users (even privileged) too lazy to remember a complex password consisting of more than 8 characters, especially when it is not meaningful phrase and a random set of letters and numbers. According to the analysis conducted by Positive Technologies [11], about 52% of users of Russian companies is used as a password only numbers, only 18% use the Latin lowercase letters and the same percent of people use Latin letters in lowercase + numbers. As for the length of a passphrase, only about 15% of users have more than 8 characters, 25% of use 8 characters long, and about 50% of the users' passphrase have 6-7 characters or less. This statistic is not much more different for network or web resources for administrators. In addition, frequently used passwords are recording in the dictionaries, attacks which are much more effective.

Another argument convincing of the danger of brute force attacks is increasing at huge rates computing power and bandwidth of the network connection. One of the methods to increase the efficiency of the exhaustive search is solutions becoming more common based on the computing power of the GPU (GPGPU). The newest graphics processor allows increasing the speed of password guessing tenfold. Using (1) and speed of password selection on GPGPU AMD 7990 ~ 220 kh/s (kh = 1000 pmk):

– 8-digit password: $\frac{10^8}{220000 \cdot 60} = 7.5$ minutes;

– 8-character password: $\frac{26^8}{220000 \cdot 3600} = 10.9$ days;

– 10-digit password: $\frac{10^{10}}{220000 \cdot 3600} = 12.6$ hours;

– 10-character password: $\frac{26^{8}}{220000 \cdot 3600 \cdot 24 \cdot 365} = 20.3$ years.

The difference is obvious, but even the use of this method requires a huge time-consuming, if the passphrase is quite complicated. Therefore, to improve the efficiency of brute force attacks often use distributed computing: in this case the set of keys splits into subsets that are processed parallel on multiple machines. Attackers can create a cluster from the n-th number of GPGPU and (or) CPU and perform calculations on it. Fig. 5 shows this graphically.

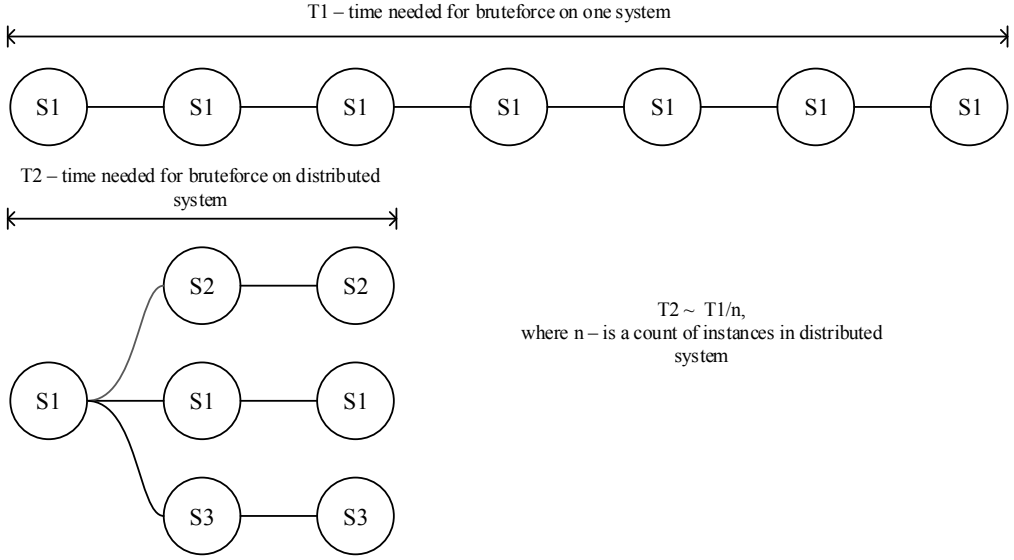

Fig. 5 Simple graphical view of brute force time decreasing with distributed system using

In this case, time required to compute the passphrase will decrease, respectively, as many times as many instances is used in a distributed system (on the condition that they have the same computing power).

Using (1) approximate time of the key calculation using the cluster of 40 AMD 7990 ~ 10000 kh/s is:

– 8-digit password: $\frac{10^{8}}{10000000 \cdot 60} = 10$ seconds;

– 8-character password: $\frac{26^{8}}{10000000 \cdot 3600} = 5.8$ hours;

– 10-digit password: $\frac{10^{10}}{10000000 \cdot 3600} = 16$ minutes;

– 10-character password: $\frac{26^{10}}{10000000 \cdot 3600 \cdot 24 \cdot 365} = 163$ days.

According to this principle hackers often create a botnets, a network of infected unsuspecting PCs users, by means of which produces a distributed brute force attack on web resources. This type of attack is most advantageous for the attacker, both in terms of efficiency, as the botnet can total tens of thousands of infected machines that give a huge amount of computing power, and in terms of financial costs - no need to establish and maintain computing cluster.

Similarly lately, after the spread of cloud computing a rent of needed for brute force attacks computing resources become more popular. Since the essence of cloud easily scalable them quite easy to use and profitable - 200 entities Amazon EC2 ~ 10000 kh/s and using (1):

– 8-digit password: $\frac{10^{8}}{10000000 \cdot 60} = 10$ seconds;

– 8-character password: $\frac{26^{8}}{10000000 \cdot 3600} = 5.8$ hours;

– 10-digit password: $\frac{10^{10}}{10000000 \cdot 3600} = 16$ minutes;

– 10-character password: $\frac{26^{10}}{10000000 \cdot 3600 \cdot 24 \cdot 365} = 163$ days.

There is even online service WPACracker, based on 400 entities Amazon EC2, which provides services to hack WPA-key by a downloaded "file handshake".

All of these attacks can be applied by hackers to penetrate into the corporate wireless networks to steal confidential information or for unauthorized access to other password-protected infrastructures.

Described service provides services of testing to penetrate the enterprise wireless network in order to verify a cryptographic strength of passphrase, professionalism and integrity of the enterprise information network administrator, fulfillment security standards of employees, etc.

The software that used for testing is the free open source software, such as pyrit, which specializes in automated brute force attacks on wireless networks and allows integrating into a cluster any number of computers of any power, whether they support or not GPGPU technology (from this depends only on increase in power) through the Internet. This allows saving money by combining together the computing resources available to the team of developers and not having to buy additional equipment. As one more software means serves also open source software hascat, which is based solely on the use of distributed computing on clusters of GPGPU. This software is used to recover passwords of the intercepted hash functions and can be used in the expansion of service and acquisition of additional processing power, as it is well amenable to parallelization on a large number of clusters of GPGPU.

D. Potential Damage Assessment Model

It is possible to use the methods of game theory to assess the potential damage [12].

The basic concepts of game theory are:

– the game is a mathematical model of conflict;

– the parties involved in the conflict are called players;

– the move is the player choice one of the courses of action;

– the player strategy is a set of rules that determines the behavior of the player at the move;

– the goal of game theory is to develop methods to determine the optimal strategy for each player [13].

In the present study are considered two players - the attacker and the security administrator. The relationship between these players is determined as the payoff matrix (Table II). In drawing up the matrix of the game can be assumed that the attacker aims to inflict the greatest possible

TABLE II
TABLE OF THE MATRIX GAME

	y_1	y_2	y_3	...	y_m
x_1	a_{11}	a_{12}	a_{13}	…	a_{1m}
x_2	a_{21}	a_{22}	a_{23}	…	a_{2m}
x_3	a_{31}	a_{32}	a_{33}	…	a_{3m}
...	…	…	…	…	…
x_n	a_{n1}	a_{n2}	a_{n3}	…	a_{nm}

damage to the attacked computer system. The purpose of the security administrator in the matrix game is to allow the attacker to inflict the least damage at the lowest cost of the means of protection.

As the attacker strategy we mean string $x_i(i = \overline{1,n})$ of the matrix, and as the security administrator strategy – columns $y_j(j = \overline{1,m})$. To the attacker strategy can be attributed various types of attacks on the computer

system, and to the strategy administrator – protection means of computer information. The parameter a_{ij} is a result of the game. As this parameter can be regarded, for example, the annual loss to all combinations variants of $x_i(i = \overline{1,n})$ and $y_j(j = \overline{1,m})$. For this is necessary to compare each attack with each protection method and to determine the damage that can be suffered in this case. Purchase, installation and use of protective equipment can require additional costs, which should also contribute to the damage in the calculations.

Assume also are known the following parameters: *n* – the number of attacks types; *m* – the number of protection means; $S_j(j = \overline{0,m})$ – the cost of protection means; *D* – the value of alleged damage; $p_{ij}^{(p)}(i = \overline{1,n}, j = \overline{1,m})$ – the probability of attack x_i reflection using protection means y_j, i.e. probability of protection against attack; $p_{ij}^{(a)}$– the probability of the attack x_i; $p_{ij}^{(d)}$ – the probability of damage during an attack x_i using protection means y_j.

The condition for the effective protection is a rule: the cost of protection means should be less than the cost of the losses incurred in the successful implementation of attack.

Since the probability of using at least one protection means equals 1, draw up the following inequality:

$$1 \times S_j \le p_{ij}^{(d)} \times D, \qquad i = \overline{1,n},\ j = \overline{1,m}. \tag{2}$$

Represent the probability of damage $p_{ij}^{(d)}$ as probability of protection $p_{ij}^{(p)}$ and the probability of the attack $p_{ij}^{(a)}$:

$$p_{ij}^{(d)} = \left(1 - p_{ij}^{(p)}\right) \times p_{ij}^{(a)}, \qquad i = \overline{1,n},\ j = \overline{1,m}. \tag{3}$$

Substituting (3) into (2), we obtain:

$$S_j \le \left(1 - p_{ij}^{(p)}\right) \times p_{ij}^{(a)} \times D, \qquad i = \overline{1,n},\ j = \overline{1,m}. \tag{4}$$

Dividing both sides of (4) to the expression in the right-hand side of this inequality, we obtain:

$$\frac{S_j}{\left(1-p_{ij}^{(p)}\right)\times p_{ij}^{(a)}\times D} \le 1, \qquad i = \overline{1,n},\ j = \overline{1,m}. \tag{5}$$

Denote in (5) left-hand side as λ_{ij} and call as a coefficient of effective protection:

$$\lambda_{ij} = \frac{S_j}{\left(1-p_{ij}^{(p)}\right)\times p_{ij}^{(a)}\times D}, \qquad i = \overline{1,n},\ j = \overline{1,m}. \tag{6}$$

According to (5) the condition of the effective protection is the ratio:

$$\lambda_{ij} \le 1, \qquad i = \overline{1,n},\ j = \overline{1,m}. \tag{7}$$

This condition is necessary to use with the Wald's maximin model [14]-[16].That is, the matrix of game is complemented by a string, each element of which has a minimum value of the gain in the strategy. The optimum for this criterion considered to be that strategy when

choosing minimum value is the maximum payoff. The chosen strategy in this way eliminates the risk.

Thus, after developing the game matrix and analyzing its values, it is possible to assess in advance the cost of each decision for the protection of computer information and choose the most effective variants to ensure security for the entire range of attacks.

V. Conclusion

The article describes security problems because of cyber-threats, the service for vulnerability analysis and security assessment of open source systems.

The proposed service has some advantages over other services that provide penetration testing services. This service can offer a lower price in the implementation of testing services at the required quality, as it is possible due to lower costs of doing business by a small group of individual entrepreneurs. Also the use of software with open source has a positive effect on the cost price.

The article gives examples of hacking techniques, which are based on exhaustive search on (brute force) and SQL-injections. Also state graph for web-applications testing was presented. And the device for anonymization operating principle was described. In addition, were established interconnections and proposed a quantitative method for assessing potential damage after implementation of attack.

Ways of further investigations are improvement of testing methods, review of application source code to detect backdoors, improvement of anonymization device using such techniques as I2P and VPN, conducting simulation experiments and analysis of results obtained to develop recommendations to prevent potential damage and attacks.

References

[1] "PlayStation Network Restoration Begins", PlayStation Network / PSN News. United Kingdom: Sony. 2011-05-17. Retrieved 2011-10-20.

[2] *2015 Trustwave Global Security Report*, Trustwave Holdings, Inc, 2015.

[3] J. Muniz, A. Lakhani, “Web Penetration Testing with Kali Linux”. Packt Publishing Ltd, Birmingham B3 2PB, UK, 2013.

[4] R. W. Beggs, “Mastering Kali Linux for Advanced Penetration Testing”. Packt Publishing Ltd, Birmingham B3 2PB, UK, 2014.

[5] *OWASP Application Security Verification Standard*, 2014.

[6] *OWASP TESTING GUIDE* v3.0, 2013.

[7] *Study: A Penetration Testing Model,* Federal Office for Information Security, Germany.

[8] S.Abraham, S. Nair, *Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains,* Journal of Communications Vol. 9, No. 12, December 2014.

[9] J. Clarke, *SQL Injection Attacks and Defense*, Justine Clarke, Syngress Publishing, Inc., 576 p., 2009.

[10] *Statistics of web application vulnerabilities*, Positive Technologies, 2013.

[11] *Analysis of the problems of password protection in Russian companies*, Positive Technologies, 2013.

[12] K. Hausken, “Probabilistic Risk Analysis and Game Theory. Risk Analysis”, Vol 22, No1, 2002.

[13] G. Owen, “Game Theory”, 2nd edition, Academic Press, 1982.

[14] A. Wald, “Contributions to the theory of statistical estimation and testing hypotheses”, The Annals of Mathematics, 10(4), 299-326, 1939.

[15] A. Wald. “Statistical decision functions which minimize the maximum risk”, The Annals of Mathematics, 46(2), 265-280, 1945.

[16] A. Wald, “Statistical Decision Functions”, John Wiley, NY, 1950.

Co-funded by the Tempus Programme of the European Union

This publication is the result of the project implementation:
TEMPUS CERES: Centers of Excellence for young RESearchers.
Reg.no.544137-TEMPUS-1-2013-1-SK-TEMPUS-JPHES