Ethical Hacking Training*

Aleksandr V. Dorofeev[1], Alexey S. Markov[2][0000-0003-0111-7377] and Yuri V. Rautkin[2]

[1] NPO Echelon, Moscow, Russia
a.dorofeev@npo-echelon.com
[2] Bauman Moscow State Technical University, Moscow, Russia
{a.markov, v.tsirlov}@bmstu.ru

Abstract. Topical issues of teaching students to information security are considered. It is concluded that security testing training is a fundamental factor in professional staff training. The well-known documents, techniques and tools for security testing are briefly reviewed. The need to accumulate training efforts on comprehensive solving of real-world problems is specified. A single platform for practical training is offered. A review of the original training course is given. It is concluded that the final stage of thematic training should be integrated with cyber exercises. The scheme of typical cyber exercises is considered. Recommendations for cyber exercises are given.

Keywords: IS-training, Information Security Audit, Cybersecurity Training, Cybersecurity Learning, Ethical Hacking.

1 Introduction

To protect your IT infrastructure from modern cyber threats, you need to constantly test the security of information systems. To assess the real level of security, you need to use the tools and approaches used by real attackers (ethical hacking) [1-4]. Future information security specialists should be proficient in ethical hacking methods, and such training should be carried out in higher educational institutions [5, 6].

Training to ethical hacking involves a number of problems, among which the main one is the lack of a unified security testing methodology based on the main technical aspects and adopted in the professional community. The other challenges include: the need to teach in the context of existing legal norms, maintain an up-to-date set of targeted vulnerable systems and test tools, and to constantly update teachers' knowledge and practical skills [7, 8]. Many courses devoted to this topic are aimed at studying only certain types of attacks and tools used for their implementation. The authors have developed and taught a course that takes into account the practical experience of security

testing projects to the maximum extent possible, which made it possible to focus teaching not only on the tools, but also on the methodology of comprehensive testing of information systems security.

2 Security Testing Methodology

It is obvious that the methodology of comprehensive security testing should include a description of the project phases and methods of conducting specific technical checks.

Regarding how to structure the phases of the security testing project, there are generally accepted methods, governed by such documents as: NSA IEM, NIST SP 800-115, BSI Penetration Testing Model [7-9]. The sequence of stages of the security testing project can be presented as follows:

- Determining the scope of the project;
- Collecting information about systems;
- Planning of specific checks;
- Performing checks;
- Analysis of the data received;
- Preparation of a report and formation of recommendations.

As to specific checks, it is worth paying attention to the presence of at least three conceptual approaches [10-13]:

A classic penetration test, which is the search and exploitation of the most dangerous vulnerabilities to demonstrate the possibility of hacking systems. The main advantage of the approach is detection of real attack vectors, and the main disadvantage is potential violating of the availability of services and systems.

Vulnerabilities scanning. Vulnerabilities scanning uses special software – vulnerability scanners. The scanner determines the versions of network services and checks to ensure that information about the published vulnerabilities is available in its constantly updated database. The main advantage is a high audit speed, the main disadvantage is “linear” logic of the scanner and inability to detect non-trivial attack vectors.

Configuration analysis. During the system configuration analysis, various system security settings are checked, for example, password policy, access rights to system resources, availability of installed updates etc. The main advantage is the possibility of finding vulnerabilities associated not only with errors in software development, but also because of errors made during administration.

The methods of specific technical checks should also be based on hacking methods used by real attackers. A potential sequence of their actions is shown in Fig. 1.

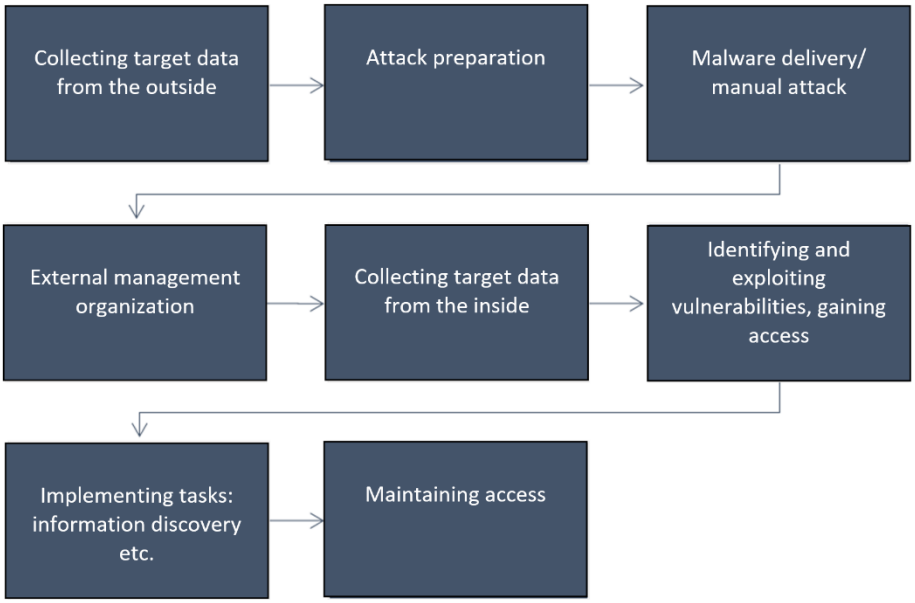

Fig. 1. Typical sequence of attacker's actions.

Analysis of the possibility of combining the well-known security testing methods and hacker approaches has allowed us to formulate a common integration testing methodology, which includes the following steps:

- Inventory of resources/search for testing goals;
- Vulnerability search (manual search, scanning, configuration analysis);
- Exploiting vulnerabilities and conducting attacks (penetration testing);
- Expansion of access (see Fig. 2).

The advantages of this approach are as follows [14, 15]:

- Identifying the maximum number of vulnerabilities and non-trivial attack vectors;
- Controlled risks of system malfunctions;
- Verification of vulnerabilities.

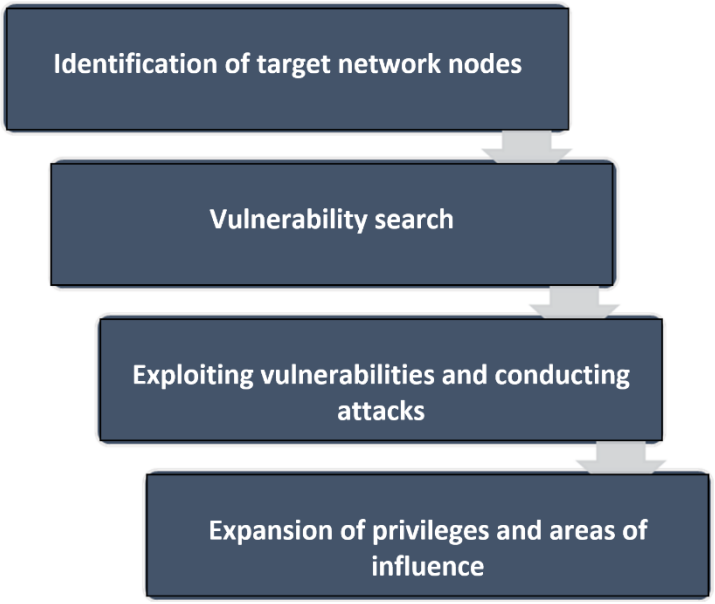

Fig. 2. Stages of comprehensive security testing.

3 Ethical Hacker Toolkit

Based on the practice of security testing projects, the following list of necessary tools can be generated:

- Port scanners;
- Vulnerability scanners;
- Web vulnerability scanners;
- Penetration testing frameworks, including exploit kits;
- Password guessing tools based on hash values obtained;
- Password guessing tools for network services;
- Network sniffers;
- utilities for Man-in-the-Middle attacks (for example, ARP-poisoning);
- Utilities to test wireless networks etc.

It should be noted that such a common class of security analysis tools as vulnerability scanners is just a small part of the complete set of tools of an ethical hacking specialist.

To implement a set of checks, Kali Linux environment is often used to launch a set of unix utilities. Unfortunately, its disadvantage is the absence of a unified report and a friendly shell focused on different levels of training and privileges of specialists [16-19]. These shortcomings can be eliminated by using the certified security analysis complex “Scanner-VS” [20], which allows you to perform the full scope of checks required from the uniform environment, taking into account the level of user training,

and to receive a unified report on the comprehensive audit of the system and network safety etc.

4 Training Course Structure

Based on a comprehensive approach to security, we have developed the structure of our training course, including the following 8 sections:

- Chapter 1. Introduction to the penetration testing.
- Chapter 2. Intelligence Gathering.
- Chapter 3. Vulnerability Analysis.
- Chapter 4. Exploitation.
- Chapter 5. Exploitation of Web-applications.
- Chapter 6. Social engineering.
- Chapter 7. Maintaining access.

5 Description of the Training Course Sections

5.1 Introduction to the Penetration Testing

In the very first section of the course, students get acquainted with the basic concepts (vulnerability, APT, exploit, payload etc.), comprehensive testing methods, documenting penetration testing results. This section of the course examines the structure of the penetration test report: the chapters “Summary for Management”, “Project Scope” and chapters with descriptions of detected vulnerabilities. The descriptions of vulnerabilities contain subsections: finding – risk – recommendation [14]. The “finding” subsection describes what kind of vulnerability has been detected and in which system, and demonstrates the possibility of its exploitation with appropriate screenshots. The “risk” subsection describes the situation that can occur if potential attackers exploit this vulnerability. For the proper assessment, testers need to find out the criticality of the compromised resource. In the “recommendation” subsection, security testing experts give advice on how to correct the situation.

Throughout all other sections of the course, students develop and supplement the report on vulnerabilities detected in the course of laboratory work.

5.2. Intelligence Gathering

This section analyses methods of collecting and analysing information to identify the purposes for which security testing will be conducted. Students perform laboratory work to find network nodes on the Internet related to a particular organization (using whois service, various queries to DNS servers), as well as to identify nodes during internal security testing (scanning of network ports, tracing of network routes). This section also teaches to Structured Analysis Techniques, which are used for efficient

information retrieval [21]. It also considers the use of search engine operators for the targeted information retrieval on the Internet.

5.3. Vulnerability Analysis

The third section of the course covers two approaches to vulnerability search: manual and automated (using vulnerability scanners) search [15].

Manual search for vulnerabilities involves determining the software version and the list of vulnerabilities known for this version of the product. You can find out the version of the software product in a number of ways. For example, many network services, when accessing them, demonstrate a so-called banner containing version data. Sometimes the version can be determined analytically. For example, you can find a press release of a developer or integrator company that created an Internet portal to be hacked by an attacker. The press release often contains all the necessary information about the technologies used, and comparing the release date of this news with the information about the release dates of the corresponding product allows you to easily determine which versions were used. Performing the appropriate laboratory work, students master the methods of analysis and comparison of data obtained using techniques mastered in the previous section of the course (port scanning and search for information on the Internet).

Vulnerability search can be automated using special vulnerability scanners. Students perform laboratory work to search for vulnerabilities using a vulnerability scanner, learn how to choose and form scanning policies correctly, as well as apply scanning modes with and without an administrative account. An equally important skill that is developed within the framework of this section is the ability to interpret scanning results.

5.4. Exploitation

In the fourth section of the course students learn techniques of exploiting vulnerabilities, as well as a number of common attacks. Metasploit Framework is used as the main tool for exploiting vulnerabilities in the laboratory [22, 23]. In addition to exploiting vulnerabilities, students learn such attack methods as password guessing and traffic interception using ARP-poisoning.

Students gain practical experience in both bruteforce and dictionary attacks. In the first case, passwords are generated based on the set rules [24, 25]. Dictionary attacks allow you to try your luck and check if the user is using a common password. Recent password leaks clearly show that many users prefer to choose keyboard passwords (such as qwerty, qazwsxedc), phone numbers, dates, names etc. Students learn how to create password dictionaries using analytical methods.

5.5. Exploitation of Web-applications

Exploitation of vulnerabilities in web applications is considered in a separate section. The main attacks related to web applications are considered: Cross Site Scripting - CSS and SQL injection. In the case of CSS, the script is implemented on the website pages,

which is executed in the user's browser when viewing the page. This can happen, for example, due to an error of the programmer, who did not implement the correct filtering of data entered by the user, for example, when a user posts a message on the forum. SQL injection consists in the fact that due to an error in the data filtering or web application architecture, an attacker can directly interact with the application database via SQL commands through the web interface.

5.6. Social Engineering

The sixth section of the course addresses social engineering techniques aimed at provoking users to take actions that are beneficial for attackers. In the course of laboratory work, students learn phishing attack techniques and exploitation methods for vulnerabilities in the application software used by users.

5.7. Maintaining Access

The final section of the course is devoted to expanding the zone of influence and maintaining comfortable access to the infrastructure under test, simulating similar actions by attackers.

Expansion of the zone of influence is discussed using the following two examples. In the course of the laboratory work, students gain access to a web server at the operating system level. This access allows them to find configuration files of web applications running on the server and extract passwords from them to access databases hosted on other servers. The second example is related to obtaining user passwords and verifying their validity to other systems deployed in the test infrastructure.

In the laboratory work, devoted to creating comfortable access to the target system, students learn how to implement a backdoor in the installation deb package based on Metasploit Framework components.

6 Description of a Vulnerable Training System

The course uses a specialized Linux build, containing vulnerable network services, Metasploitable 2. Metasploitable 2 contains more than 200 vulnerabilities in such services as FTP server, Web server, Postgres, MySQL, IRC, VNC etc. The build also contains vulnerable Web applications like DVWA.

7 Ethical Hacking Development: Cyber Exercises

The next step in ethical hacking development is cyber exercises involving creation of a virtual infrastructure to be protected by one team of students and to be attacked by the other. Let us look at Locked Shields drills conducted by the NATO Cooperative Cyber Defence Centre of Excellence as open examples of such cyber exercises.

Let us start with Locked Shields cyber drills that were conducted in 2013. The organizers of the exercises have created a virtual infrastructure that includes about 400

nodes. The infrastructure is called Gamenet. Each team of defenders (Blue team) received a network of 34 machines, including a router, firewalls, Linux and Windows workstations, domain controllers, file, mail, DNS and web servers, and database servers.

It should be noted that the protected systems were as close to the reality as possible, and the organizers of exercises prepared the following points:

- A few patches were missing on the operating systems, the application software was mainly vulnerable;
- Two backdoors were introduced in advance, which started to access the management servers at the appointed time;
- The network had a connected vulnerable laptop of the contractor's specialist.

Each protected infrastructure was also accessed by a representative of the organizing team (White Team), who acted as a "blonde", imitating a curious user who clicks on all the links in the emails received and opens all attachments.

The attackers (Red Team) were armed with full knowledge of the target IT infrastructure, as well as the tools used during the cyber attacks: Kali Linux and Metasploit. Attackers were divided into groups by the following specializations: workstations, Web and DBMS, networks etc. The team of "Reds" was assigned 20 tasks, which had to be performed in stages during the exercise. Examples of tasks: to change the content of an important Web page, organize denial of service, get administrative access, introduce malicious code, get access to certain emails, receive a specific report, replace a video file etc. The duration of the active phase of the exercise was 3 days.

Such cyber exercises following the ethical hacking course will help to consolidate the acquired skills of security testing in practice.

8 Conclusion

The main factors of successful training of students in ethical hacking are the following: the availability of methods, an appropriate set of vulnerable systems and tools for security testing. In our opinion, we have managed to create a practical course on ethical hacking, which allows students to master the key skills required by information security specialists. Cyber exercises are the logical continuation of such training, which is the subject of our further research.

The proposed training course and the support platform were tested for a long time in the Echelon training course, as well as in the framework of the international thematic Olympiad-contest Echelon Defence.

References

1. Lane, E.: Hacking with Python: Beginner's Guide to Ethical Hacking, Basic Security, Penetration Testing, and Python Hacking. CreateSpace Independent Publishing Platform (2017).
2. Petrenko, A.S., Petrenko, S.A., Makoveichuk, K.A., Chetyrbok, P.V.: Protection Model of PCS of Subway from Attacks Type «Wanna cry», «Petya» and «Bad rabbit» IoT. In: Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus 2018). IEEE, pp. 945 – 949 (2018). DOI: 10.1109/EIConRus.2018.8317245.
3. Thompsons, J.: Hacking: Hacking For Beginners Guide On How To Hack, Computer Hacking, And The Basics Of Ethical Hacking. CreateSpace Independent Publishing Platform (2017).
4. Walker, M.: CEH Certified Ethical Hacker All-in-One Exam Guide: 3rd Ed. McGraw-Hill Education (2016). 525 p.
5. Petrenko, S.A., Petrenko, A.S., Makoveichuk, K.A.: Problem of Developing an Early-Warning Cybersecurity System for Critically Important Governmental Information Assets. In: CEUR Workshop Proceedings. 2081, pp. 112-117 (2017).
6. Sheremet, I.A.: Directions of a New Level Education to Counter Cyberthreats in Financial Sphere. Voprosy kiberbezopasnosti [Cybersecurity issues]. 4, pp. 69-74 (2017). DOI: 10.21681/2311-3456-2016-5-3-7.
7. BSI - Study A Penetration Testing Model. A Penetration Testing Modul. BSI, https://bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf, last accessed 2019/08/08.
8. Rogers, R., Fuller, E., Miles, G., Hoagberg, M., Schack, T., Dykstra, T., Cunningham, B., Little, C.: Network Security Evaluation Using the NSA IEM. Syngress (2005).
9. Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A.: Technical Guide to Information Security Testing and Assessment. NIST. SP 800-115, pp. 1-80 (2008). DOI: 10.6028/NIST.SP.800-115.
10. Allsopp, W.: Advanced Penetration Testing: Hacking the World's Most Secure Networks. John Wiley & Sons (2017).
11. Dorofeev, A.V., Rautkin, Y.V. Applied Aspects of Security Testing. In: CEUR Workshop Proceedings. 2081, pp. 49-53 (2017).
12. Kim, P.: The Hacker Playbook 2: Practical Guide to Penetration Testing. CreateSpace Independent Publishing Platform (2015).
13. Shatob, R.: Step by Step Guide to Penetration Testing. Tellwell Talent (2019).
14. Markov, A., Barabanov, A., Tsirlov, V.: Models for Testing Modifiable Systems. In Book: Probabilistic Modeling in System Engineering, by ed. A.Kostogryzov. IntechOpen. Chapter 7, pp. 147-168 (2018). DOI: 10.5772/intechopen.75126.
15. Markov, A.S., Fadin, A.A., Tsirlov, V.L.: Multilevel Metamodel for Heuristic Search of Vulnerabilities in The Software Source Code. International Journal of Control Theory and Applications. 9, 30, pp. 313-320 (2016).
16. Dieterle, D.W.: Basic Security Testing with Kali Linux 2. CreateSpace Independent Publishing Platform (2016).
17. Hertzog K., O'Gorman J.: Kali Linux Revealed: Mastering the Penetration Testing Distribution. Offsec Press (2017).
18. Schultz, C.P., Perciaccante, B.: Kali Linux Cookbook: Effective penetration testing solutions: 2nd Ed. Packt Publishing (2017).

19. White, A.K.: Hacking: The Underground Guide to Computer Hacking, Including Wireless Networks, Security, Windows, Kali Linux and Penetration Testing. CreateSpace Independent Publishing Platform (2017).
20. Scaner-VS. NPO Echelon, http://scaner-vs.ru/trial, last accessed 2019/08/08.
21. Dorofeev, A.V., Markov, A.S., Tsirlov, V.L.: Social Media in Identifying Threats to Ensure Safe Life in a Modern City. Communications in Computer and Information Science. 674, pp. 441-449 (2016). DOI: 10.1007/978-3-319-49700-6_44.
22. Heriyanto, T., Allen, L., Ali, S.: Assuring Security by Penetration Testing. Packt Publishing (2014).
23. Jaswal, N.: Metasploit Bootcamp: The fastest way to learn Metasploit Paperback. Packt Publishing (2017).
24. Markov, G., Sharunov, V.: Mail Service Password Security. In: CEUR Workshop Proceedings. 2081, pp. 79-82 (2017).
Picolet, J. Hash Crack: Password Cracking Manual. CreateSpace Independent Publishing Platform (2017).