APPLICATION PENETRATION TEST AND ITS NECESSITY IN 2021

Pohorila V. M.
National Aviation University, Kyiv
Supervisor – Martyniuk H. V., PhD., associate professor

A modern site is a system with a complex architecture, containing on average 20 vulnerabilities that can be exploited by attackers. 62% of sites are subject to medium to high risk vulnerabilities [1]. On the corporate website or on the website of the state department, it is necessary to ensure protection against distortion, destruction of publicly available information or blocking access to it.

Pentest (penetration testing) - penetration testing, analysis of network infrastructure, company servers or applications for vulnerabilities [3]. The purpose of this analysis is to find vulnerabilities and compose possible attack vectors, simulating the actions of a real attacker.

There are several types of penetration testing that can be used to gauge and pinpoint these vulnerabilities [3]:

- Whitebox - code and infrastructure audit.
- Graybox - the organizational structure is provided to the team prior to testing.
- Blackbox - the pentester has no information about the organization of information protection.
- The “Red Team” principle is the variant most close to the real scenario.

There are several sub-categories and variations when it comes to the types of penetration testing a company can use to audit the security of a business’s infrastructure. The five most common are Network Service Tests, Web Application Tests, Client Side Tests, Wireless Network Tests, and Social Engineering Tests [2].

Searching for vulnerabilities in an organization's WIFI network includes [3]:

1. Pentest of Web applications - search for vulnerabilities on the sites of the organization.
2. Load testing - checking the readiness of the network infrastructure in the event of a DDOS attack on the organization.
3. Testing of social networks of employees - verification of compliance by employees of the organization with adherence to internal security protocols.

Not every service can be called a "pentest". Recently, a situation has developed on the market that a number of software vendors and integrators offer vulnerability scanner reports as a pentest. Sometimes, they do not even carry out manual verification (check) of the found vulnerabilities.

As a result, in essence, a simple service is sold as more expensive. A full-fledged penetration test is not only an automated scan using existing vulnerability scanners (although this is one of the testing stages) or a manual check for vulnerabilities, for example, of a website; it is rather a complete analysis of the IT infrastructure for security. It is important not only to run the scanner, it is important to understand what problems in the current infrastructure may be and how an attacker can take advantage of them.

What is hidden under the white hood? Differences between a penetration test and a real hacker attack in its limitations [4]:

1. Law. It is logical that all actions are carried out only by agreement and on the basis of an agreement and permits from the customer. Black hackers don't ask permission

2. Time. Black hackers are not limited in time, they can follow the "victim" for years, revealing new security holes.

3. The budget. Black hackers can invest heavily in offensive tools, including the purchase of exclusive exploits (0-day, malware). White hackers are limited by customer budgets.

4. Depth of penetration. It is clear that black hackers are not limited by anything, including the ability to gain access to all systems that they can “hack”. Ethical hackers have limitations - a list of systems that can be accessed.

With the advent of the popularity of crowdsourcing, it was decided to supplement the pentest with this fashionable approach using bug bounty programs. These programs work all over the world, customers are the largest international companies, the executors are white hackers around the world. Idea - the customer places an application on the platform for testing his company or product, specifies the limitations and the amount of remuneration for the vulnerabilities found, the contractor looks for vulnerabilities and, if successful, receives a reward. A special case of bug bounty has also appeared - bug bash, a time-limited event, usually within the framework of a large conference with the same conditions (reward for “hacking” a product).

The penetration testing market is growing. According to some studies, it will reach $ 3.2 billion by 2023 [4]. The increasing demand for Internet of Things (IoT) security and the growing Bring Your Own Device (BYOD) trend are expected to drive growth in the penetration testing market in the coming years.

In conclusion, I can add that at this time, pentest is an integral part of the life of every Internet resource or application. Do not be afraid to test your resources and infrastructure - this is one of the most effective and secure ways to identify problems in the security of your corporate information system. And remember, the security of the entire information system is determined by the security of the weakest link.

References:

1. PENTESTS OF SITES AND WEB-APPLICATIONS [Electronic resource]. – Electronic magazine. Access mode: https://amonitoring.ru/service/pentest/web/

2. Randy Lindberg. Types of Penetration Testing for 2021 [Electronic resource]. – Electronic magazine. – November 10, 2020 – Access mode: https://www.rivialsecurity.com/blog/types-of-penetration-testing

3. Cryptoperty. What is pentest? [Electronic resource]. – Electronic magazine. – May 04, 2020 – Access mode: https://itsecforu.ru/2020/05/04/chto-takoe-pentest/

4. 10Guards. Pentest: what is hidden under the white hood?. [Electronic resource]. – Electronic magazine. – December 18, 2019 – Access mode: https://10guards.com/ru/articles/pentest-under-the-white-hood/