«WHITE-HAT» HACKING

Uchkov A.K.

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Kaspiarovich N.G. – teacher

Different IT security vulnerabilities are discovered every day. Security specialists are working to fix them, but ethical hackers are those who are responsible for finding problems of systems. For safety of personal data and for keeping services running, this community needs to grow; it should also get more attention in media sphere.

In everyday life, the word «hacker» usually means «someone, who uses bugs or exploits to break into computer systems». But not all of them are malicious. They can be divided into two large groups: “white-hat” (or ethical hackers) and “black-hat”. Hackers from a first group use their skills to find security weaknesses in order to fix them before they can be exploited. Hackers from a second group are engaged in taking down networks, stealing data and compromising systems.

The history of “white hats” is actually just the history of hacking. Even the name “hacker” was not always associated with bad things. In early 1960’s, “hacking” meant “different ways to optimize systems and machines”. Hackers could be divided into groups only from 1970’s: one of the first ethical hacks was a “security evaluation” of Multics operation system, which belonged to the United States Air Force. Hackers’ goals were to gather all information that they could, and then to do maximum damage to the system. In result, they found “vulnerabilities in hardware security, software security and procedural security”. As hackers have become smarter and more persistent, it has become very important for companies to have strong defenses against them [1].

There are several reasons why just security specialists aren’t enough.

1. Cybersecurity teams and “white hats” have different knowledge: “white hats” know both about attacking and protecting the systems.

2. Hackers can give you a look from outside. Cybersecurity teams can work for one company for years, while “white-hat” hackers are often employed by different businesses to help assess and improve security, so they always work with different systems and use different techniques.

3. Hackers provide more precise testing. If a test is performed inside the company, there is a huge risk that information about the attack will leak to the security team members. If you want to test defenses in a really stressful situation, you should hire an attacking team from outside.

“White-hat” hackers have traditionally provided penetration testing services. They include different subtests, such as social engineering tests, where hackers try to get an employee or someone connected with the company to reveal sensitive information including passwords, business data, or other user data; or web application tests, where different software is used to assess the security vulnerability of web apps and software programs. Also, physical penetration tests, network services tests and wireless security tests are often performed [2].

However, there is one huge problem in testing it is time. While a team of “white-hats” is working with one security system for about a week, “black-hats” can gather information and find vulnerabilities for years before an attack.

Although “white-hats” don’t get really much attention in media, they still have their conferences, events and famous members of their community. One of the largest events is called Black Hat. It has been taking place for 22 years now. It gathers more than 3.5 thousand “white-hats” from more than 20 countries annually. It is supported by large IT companies, and it lasts 6 days [3].

Today, security and safety of personal data in particular have become very important. With the help of “white-hat” hackers, large and small companies can assure that they can recover after a real attack and protect user data. In media, we don’t hear about them a lot, but it doesn’t mean that their work is not important. If you are interested in the sphere of IT security, you might be interested in becoming a “white-hat” hacker.

References:

1. A history of ethical hacking [Electronic resource]. – Mode of access: https://staysafeonline.org/blog/history-ethical-hacking/. – Date of access: 16.04.2020.

2. Types of Penetration Techniques and Methods [Electronic resource]. – Mode of access:https://www.solarwindsmsp.com/blog/penetration-testing-methods. – Date of access: 16.04.2020.

3. Black Hat USA 2019 [Electronic resource]. – Mode of access: https://www.blackhat.com/us-19/. – Date of access: 16.04.2020