Open - Sec

THE SUCCESS OF AN ETHICAL HACKING/ PENTEST SERVICE

by Hernan Parodi*

*CEO, pentester, and red teamer of the Open-Sec team. He has experience on infrastructure tests, non conventional technology, and web/mobile applications. Focused on offensive security, he has completed numerous assessments identifying attack vectors that adversaries use to compromise critical infrastructure. He also performs penetration testing for applications in common sectors like payment methods or even health. (https://www.linkedin.com/in/hernanparodi/)

An Ethical Hacking/Pentest service has as a main objective to increase the security level of companies and institutions. Therefore, in addition to the professionalism required by the team of pentesters, the commitment of all the participants is necessary (company and pentesters).

The team of pentesters must have a constant training, experience in every type of test required (infrastructure, web and mobile applications, APIs, cloud, etc) and the respective rotation of the team depending on the specific test and specialities of every pentester, which guarantees a high quality service. For an effective selection, not only the certificates of the pentester should be considered - we know that cheating on these certifications like giving answers or supplantation is getting common nowadays - but, we should also check their clients history and validate, with them, the quality of service of the security company.

An Ethical Hacking/Pentest service is NOT only to inform the results that the automated tools can find, it is necessary to verify/eliminate false positives, realizing manual tests (which automated tools are not able to execute) and, more importantly, proposing specific recommendations with permanent accompaniment until the vulnerabilities are solved/mitigated, in order to protect the assets of the organization.

Finding and exploiting new vulnerabilities, in a certain way, it gives us satisfaction, not by criticizing or qualifying a development team or TI, but because it allows us to close gaps that we can anticipate to real attacks. As we can find new vulnerabilities (that we enjoy discovering and report), there are other vulnerabilities that keep on existing through the years even after being published or when the manufacturers have already released patches. I remember my first vulnerability encounter, more than 10 years ago, it was a SQLi that granted me access to a BD and with the obtained credentials, I could access the server. Nowadays, we keep on finding the same vulnerabilities and others similar to it that have been reported many years ago.

We need to have in mind that the objective is not to criticize the shortcomings of the organization, it is actually to come up with the best alternative of solution/mitigation to increase the security level and permanently follow the process of vulnerabilities resolution to avoid great losses against a real attack. When a company understands this objective - that the team of pentesters is on the company's side proposing solutions and not to judge - both at management and technical level,they are more open to tests and to the facilities that they can provide to the evaluation team.

Why is information required for the tests?

The Ethical Hacking/Pentest service has a limited time of execution and, on the other side of the coin, a real attacker has much more time (without limits) for investigation and performance. That is why to realize a service that can provide a big value to the organization, it is required to control the times of the service in an efficient way.

The tests must be realized with the knowledge of the environment of the systems and the facilities that the pentesters might require, which will allow an efficient evaluation of the security in the limited time of the service. This does not imply disabling the protection components, but to evaluate it in an orderly and gradual way, because, as an example, a WAF can reduce the attack surface, but it will not solve the vulnerabilities.

Now, many of the developers are using security by dark (the ones that include a type of additional encryption to reduce the surface of attack or even a low level “security companies”) arguing that since the communications/data is encrypted, they are already safe.

At not having the time or the level required to elude/solve the encryption, some “security companies” don’t report what they found and the client thinks that everything is safe, but there are many cases that we have found critical vulnerabilities (some of them typicals or very easy to exploit) in applications where they see the encryption as a solution for vulnerabilities.

Time is an important resource and we must manage it in the best way possible. For example: For a service of 2 weeks, it should only be established to this process (elude/solve the encryption)a maximum of 2 or 3 days and then there is an integral evaluation of the application; un máximo de 2 a 3 días y luego una evaluación integral de la aplicación; instead, if there is no facilities for the specific case, this first part can delay between 7 to 10 days, leaving less time for the revision of the application used. The encryption should be taken as an additional barrier, but not as a solution of codes with vulnerabilities.

To get success in an Ethical Hacking service, it is necessary to select an experienced team of pentesters and the commitment of the different areas of the organization that allow the development of a high quality service. Remember that the company you choose must not judge, but should actively participate in the process of testing and providing recommendations in order to anticipate and avoid losses in the company.