Komodo CONSULTING
making security simple

THE 7 MISTAKES OF EXTERNAL PENETRATION TESTING

THE 7 MISTAKES OF EXTERNAL PENETRATION TESTING

Penetration Testing (PT) has become standard for global enterprises and SMB's trying to reduce the risk of a security breach by evaluating the security level of their systems or trying to identify security vulnerabilities in their applications. For best results, and in order to avoid conflicts of interest, it is also standard to use external contractors to conduct the testing. However, by giving external contractors authorization and access to internal systems, organizations risk being harmed by the very people hired to protect them. In this white paper we outline what your external penetration team should *not* be doing and what you can do to protect your organization.

1. PENETRATE OUT-OF-SCOPE APPLICATIONS

Since penetration teams are given access to networks and applications, they can use this to "go beyond" the scope of the test. In other words, they can try and penetrate applications without prior authorization. This could compromise organizational systems that were not in the original scope of the penetration test, potentially resulting in unintended detrimental results.

To avoid this, a penetration test must have a clear, preliminary scoping procedure that defines what should and should not be tested as part of the project.

2. USE UNAUTHORIZED TOOLS

An external pentest team can create or install a tool containing a backdoor that may expose your organization to risks. While automated scanning tools, off-the-shelf exploits, and hacking platforms are legitimate tools in the hands of a white-hat hacker, they are not always handled with care.

Make sure to assess and approve all tools used throughout the test to make sure they were created by credible sources. Also, only hire an external pentesting company with a reputation for using tools that come from a trusted community and a legitimate source.

3. IGNORE THE BUSINESS LOGIC OF THE SYSTEM

Whenever an application penetration test is conducted, pentesters often look for common vulnerabilities such as XSS, SQL Injections, buffer overflows, and others. This is very important; However, they do not always check for vulnerabilities whilst taking into consideration the

application's business logic. Sometimes, understanding this logic requires research and considerable knowledge of fields outside pentesters' expertise such as finance, banking, insurance, etc. In these cases, pentesters often fail to recognize serious security vulnerabilities that can arise from manipulating the business processes.

It is therefore essential that pentesters have a good understanding of the business logic behind the application. This is something that needs to be dealt with in the advance training of your pentesters, to make sure they grasp at least the essentials of your applications' business logic, in order to allow them to effectively test their flaws.

4. INTERFERE WITH PRODUCTION SYSTEMS

The attack arsenal of an experienced pentester is usually excellent. Today, the number of security tools, exploits, scanners and frameworks is larger than ever before. However, not all pentesters launching these tools on your systems have a good understanding of how to use them responsibly. All too often, a security tool will cause the system to crash or behave unpredictably. When this happens on production systems, the results can lead to severe financial loss.

It is vital to establish the scope and boundaries of the pentest and to validate that the testing team can act accordingly under these circumstances in order to avoid costly downtimes of production systems.

5. STOP AFTER FIRST SUCCESSFUL PENETRATION

It is not uncommon for pentesters to discover a critical vulnerability bug in the very early stages of the test, often leading to a complete takeover of the server or data. Some testers believe that once a "game-ending" vulnerability has been discovered, the test is over since they managed to completely compromise the system. This approach is incorrect as 9 times out of 10 the goal of the test is not to show that an attacker can gain *complete* access to the system, but to find as many vulnerabilities as possible!

Make sure that your testers do not stop after discovering the first high-risk issue or after gaining access to the system. They might miss other critical vulnerabilities that won't be mitigated unless discovered.

6. MISUNDERSTAND THE RISK OF CERTAIN VULNERABILITIES

After the pentest is said and done, it is time to write the final report. Most penetration reports contain an assessment of the risk of each vulnerability — usually low, medium, high or critical. Some pentesting companies exaggerate the risk they assign to each vulnerability in order to emphasize their achievements.

In other cases, a risk may be underestimated. For example, say a client is PCI DSS-compliant and a bug is found in his system, which exposes a single credit card number. We might assign a vulnerability of "low" or "medium" *if* we were trying to examine the risk of a single credit card number being exposed. But, since this vulnerability breaches the PCI- compliance, it has a huge professional impact on the client's reputation and should be flagged as "high".

To accurately assess the risk of vulnerability, make sure your testers take into account factors such as the probability of a successful attack, the value of the vulnerability to the attacker, and the business impact of the bugs found.

7. PUBLISH SENSITIVE TESTING RESULTS

The results of a successful pentest on a system can be a very strong marketing tool for the pentesting company as it culminates many hours of hard work and research. Often, exposed vulnerabilities also raise curiosity in the security community. Since most pentests reveal sensitive information about the organization, such as discovered internal networks, IP addresses, and security bugs, most organizations would not knowingly reveal these results to the general public.

For this reason, it is vital that the pentest provider contractually guarantees that no information regarding the pentesting will ever be published or exposed to unauthorized parties — whether deliberately or accidentally.

In conclusion, while pentesting is a common and necessary practice for many organizations, it is essential to understand the pitfalls and how to avoid them. If any of the above behaviors are demonstrated by your pentesting company, it might be time to reconsider your contractor.

ABOUT KOMODO

Komodo Consulting enables companies to align their business and regulatory requirements and adapt to the ever-changing challenges of the Information and Cyber security fields.

Utilizing proprietary tools and techniques and an expert approach, we provide our customers with a full range of cyber security services including Application Security, Incident Response, Training, Penetration Testing through to Cyber Security Strategy, Risk Assessments and more. Our expertise revolves around secure software development as well as standards, regulations and best practices of the security industry, with a fresh and updated view of the Cyber Arena.

The company was founded in 2011 by a team of security professionals with decades of solid, hands-on experience. Our team's members include military computer unit graduates, the Intelligence Corps (8200) graduates, as well as computer science graduates from leading universities.