5 pen testing rules of engagement: What to consider while performing Penetration testing

Penetration testing and **ethical hacking** are proactive ways of testing web applications by performing attacks that are similar to a real attack that could occur on any given day. They are executed in a controlled way with the objective of finding as many security flaws as possible and to provide feedback on how to mitigate the risks posed by such flaws.

Security-conscious corporations have implemented integrated penetration testing, vulnerability assessments, and source code reviews in their software development cycle. Thus, when they release a new application, it has already been through various stages of testing and remediation.

When planning to execute a penetration testing project, be it for a client as a professional penetration tester or as part of a company's internal security team, there are aspects that always need to be considered before starting the engagement.

This article is an excerpt from the book Web Penetration testing with Kali Linux – Third Edition, written by Gilberto Najera-Gutierrez, Juned Ahmed Ansari.

Rules of Engagement for Pen testing

Rules of Engagement (**RoE**) is a document that deals with the manner in which the penetration test is to be conducted. Some of the directives that should be clearly spelled out in RoE before you start the penetration test are as follows:

- The type and scope of testing
- Client contact details
- Client IT team notifications
- Sensitive data handling
- Status meeting and reports

Type and scope of Penetration testing

The type of testing can be black box, white box, or an intermediate gray box, depending on how the engagement is performed and the amount of information shared with the testing team.

There are things that can and cannot be done in each type of testing. With **black box testing**, the testing team works from the view of an attacker who is external to the organization, as the penetration tester starts from scratch and tries to identify the network map, the defense mechanisms implemented, the internet-facing websites and services, and so on.

Even though this approach may be more realistic in simulating an external attacker, you need to consider that such information may be easily gathered from public sources or that the attacker may be a disgruntled employee or ex-employee who already possess it. Thus, it may be a waste of time and money to take a black box approach if, for example, the target is an internal application meant to be used by employees only.

White box testing is where the testing team is provided with all of the available information about the targets, sometimes even including the source code of the applications, so that little or no time is spent on reconnaissance and scanning. A gray box test then would be when partial information, such as URLs of applications, user-level documentation, and/or user accounts are provided to the testing team.

Gray box testing is especially useful when testing web applications, as the main objective is to find vulnerabilities within the application itself, not in the hosting server or network. Penetration testers can work with user accounts to adopt the point of view of a malicious user or an attacker that gained access through social engineering.

When deciding on the scope of testing, the client along with the testing team need to evaluate what information is valuable and necessary to be protected, and based on that, determine which applications/networks need to be tested and with what degree of access to the information.

Client contact details

We can agree that even when we take all of the necessary precautions when conducting tests, at times the testing can go wrong because it involves making computers do nasty stuff. Having the right contact information on the client-side really helps. A penetration test is often seen turning into a **Denial-of-Service** (**DoS**) attack. The technical team on the client side should be available 24/7 in case a computer goes down and a hard reset is needed to bring it back online.

Penetration testing web applications has the advantage that it can be done in an environment that has been specially built for that purpose, allowing the testers to reduce the risk of negatively affecting the client's productive assets.

Client IT team notifications

Penetration tests are also used as a means to check the readiness of the support staff in responding to incidents and intrusion attempts. You should discuss this with the client whether it is an announced or unannounced test. If it's an announced test, make sure that you inform the client of the time and date, as well as the source IP addresses from where the testing (attack) will be done, in order to avoid any real intrusion attempts being missed by their IT security team. If it's an unannounced test, discuss with the client what will happen if the test is blocked by an automated system or network administrator. Does the test end there, or do you continue testing? It all depends on the aim of the test, whether it's conducted to test the security of the infrastructure or to check the response of the network security and incident handling team. Even if you are conducting an unannounced test, make sure that someone in the escalation matrix knows about the time and date of the test. Web application penetration tests are usually announced.

Sensitive data handling

During test preparation and execution, the testing team will be provided with and may also find sensitive information about the company, the system, and/or its users. Sensitive data handling needs special attention in the RoE and proper storage and communication measures should be taken (for example, full disk encryption on the testers' computers, encrypting reports if they are sent by email, and so on). If your client is covered under the various regulatory laws such as the **Health Insurance Portability and Accountability Act** (**HIPAA**), the **Gramm-Leach-Bliley Act** (**GLBA**), or the European data privacy laws, only authorized personnel should be able to view personal user data.

Status meeting and reports

Communication is key for a successful penetration test. Regular meetings should be scheduled between the testing team and the client organization and routine status reports issued by the testing team. The testing team should present how far they have reached and what vulnerabilities have been found up to that point. The client organization should also confirm whether their detection systems have triggered any alerts resulting from the penetration attempt. If a web server is being tested and a WAF was deployed, it should have logged and blocked attack attempts. As a best practice, the testing team should also document the time when the test was conducted. This will help the security team in correlating the logs with the penetration tests.

WAFs work by analyzing the HTTP/HTTPS traffic between clients and servers, and they are capable of detecting and blocking the most common attacks on web applications.

To build defense against web attacks with Kali Linux and understand the concepts of hacking and penetration testing, check out this book Web Penetration Testing with Kali Linux – Third Edition.