
General penetration testing framework

Kali Linux is a versatile operating system that comes with a number of security assessment and penetration testing tools. Deriving and practicing these tools without a proper framework can lead to unsuccessful testing and might produce unsatisfied results. Thus, formalizing the security testing with a structured framework is extremely important from a technical and managerial perspective.

The general testing framework presented in this section will constitute both the black box and white box approaches. It offers you a basic overview of the typical phases through which an auditor or penetration tester should progress. Either of these approaches can be adjusted according to the given target of assessment. The framework is composed of a number of steps that should be followed in a process at the initial, medial, and final stages of testing in order to accomplish a successful assessment. These include the following:

- Target scoping
- Information gathering
- Target discovery
- Enumerating target
- Vulnerability mapping
- Social engineering
- Target exploitation
- Privilege escalation
- Maintaining access
- Documentation and reporting

Whether applying any combination of these steps with the black box or white box approaches, it is left to the penetration tester to decide and choose the most strategic path according to the given target environment and its prior knowledge before the test begins. We will explain each stage of testing with a brief description, definition, and its possible applications. This general approach may be combined with any of the existing methodologies and should be used as a guideline rather than a penetration testing catch-all solution.

Target scoping

Before starting the technical security assessment, it is important to observe and understand the given scope of the target network environment. It is also necessary to know that the scope can be defined for a single entity or set of entities that are given to the auditor. The following list provides you with typical decisions that need to be made during the target scoping phase:

- What should be tested?
- How should it be tested?
- What conditions should be applied during the test process?
- What will limit the execution of the test process?
- How long will it take to complete the test?
- What business objectives will be achieved?

To lead a successful penetration testing, an auditor must be aware of the technology under assessment, its basic functionality, and its interaction with the network environment. Thus, the knowledge of an auditor does make a significant contribution towards any kind of security assessment.

Information gathering

Once the scope is finalized, it is time to move into the reconnaissance phase. During this phase, a pentester uses a number of publicly available resources to learn more about his or her target. This information can be retrieved from Internet sources such as:

- Forums
- Bulletin boards
- Newsgroups
- Articles
- Blogs
- Social networks

- Commercial or non-commercial websites

Additionally, the data can also be gathered through various search engines, such as Google, Yahoo!, MSN Bing, Baidu, and others. Moreover, an auditor can use the tools provided in Kali Linux to extract the network information about a target. These tools perform valuable data mining techniques to collect information through DNS servers, trace routes, Whois database, e-mail addresses, phone numbers, personal information, and user accounts. As more information is gathered, the probability of conducting a successful penetration test is increased.

Target discovery

This phase mainly deals with identifying the target's network status, operating system, and its relative network architecture. This provides you with a complete image of the interconnected current technologies or devices and may further help you in enumerating various services that are running over the network. By using the advanced network tools from Kali Linux, one can determine the live network hosts, operating systems running on these host machines, and characterize each device according to its role in the network system. These tools generally implement **active** and **passive** detection techniques on the top of network protocols, which can be manipulated in different forms to acquire useful information such as operating system fingerprinting.

Enumerating target

This phase takes all the previous efforts forward and finds the open ports on the target systems. Once the open ports have been identified, they can be enumerated for the running services. Using a number of port scanning techniques such as full-open, half-open, and stealth scan can help determine the port's visibility even if the host is behind a firewall or **Intrusion Detection System** (**IDS**). The services mapped to the open ports help in further investigating the vulnerabilities that might exist in the target network's infrastructure. Hence, this phase serves as a base for finding vulnerabilities in various network devices, which can lead to a serious penetration. An auditor can use some automated tools given in Kali Linux to achieve the goal of this phase.

Vulnerability mapping

Up until the previous phase, we have gathered sufficient information about the target network. It is now time to identify and analyze the vulnerabilities based on the disclosed ports and services. This process can be achieved via a number of automated network and application vulnerability assessment tools that are present under the Kali Linux OS. It can also be done manually but takes an enormous amount of time and requires expert knowledge. However, combining both approaches should provide an auditor with a clear vision to carefully examine any known or unknown vulnerability that may otherwise exist on the network systems.

Social engineering

Practicing the art of deception is considerably important when there is no open gate available for an auditor to enter the target network. Thus, using a human attack vector, it is still possible to penetrate the target system by tricking a user into executing malicious code that should give backdoor access to the auditor. Social engineering comes in different forms. This can be anybody pretending to be a network administrator over the phone forcing you to reveal your account information or an e-mail phishing scam that can hijack your bank account details. Someone imitating personnel to get into a physical location is also considered social engineering. There is an immense set of possibilities that could be applied to achieve the required goal. Note that for a successful penetration, additional time to understand human psychology may be required before applying any suitable deception against the target. It is also important to fully understand the associated laws of your country with regards to social engineering prior to attempting this phase.

Target exploitation

After carefully examining the discovered vulnerabilities, it is possible to penetrate the target system based on the types of exploits that are available. Sometimes, it may require additional research or modifications to the existing exploit in order to make it work properly. This sounds a bit difficult but might get easier when considering a work under advanced exploitation tools, which are already provided with Kali Linux. Moreover, an auditor can also apply client-side exploitation methods mixed with a little social engineering to take control of a target system. Thus, this phase mainly focuses on the target acquisition process. The process coordinates three core areas, which involve pre-exploitation, exploitation, and post-exploitation activities.

Privilege escalation

Once the target is acquired, the penetration is successful. An auditor can now move freely into the system, depending on his or her access privileges. These privileges can also be escalated using any local exploits that match the system's environment, which, once executed, should help you attain super-user or system-level privileges. From this point of entry, an auditor might also be able to launch further attacks against the local network systems. This process can be restricted or non-restricted depending on the given target's scope. There is also a possibility of learning more about the compromised target by sniffing the network traffic, cracking passwords of various services, and applying local network spoofing tactics. Hence, the purpose of privilege escalation is to gain the highest-level access to the system that is possible.

Maintaining access

Sometimes, an auditor might be asked to retain access to the system for a specified time period. Such activity can be used to demonstrate illegitimate access to the system without performing the penetration testing process again. This saves time, cost, and resources that are being served to gain access to the system for security purposes. Employing some secret tunneling methods, which make a use of protocol, proxy, or end-to-end connection strategy that can lead to establishing a backdoor access, can help an auditor maintain his or her footsteps into the target system as long as required. This kind of system access provides you with a clear view on how an attacker can maintain his or her presence in the system without noisy behavior.

Documentation and reporting

Documenting, reporting, and presenting the vulnerabilities found, verified, and exploited will conclude your penetration testing activities. From an ethical perspective, this is extremely important because the concerned managerial and technical team can inspect the method of penetration and try to close any security loopholes that may exist. The types of reports that are created for each relevant authority in the contracting organization may have different outlooks to assist the business and technical staff understand and analyze the weak points that exist in their IT infrastructure. Additionally, these reports can serve the purpose of capturing and comparing the target system's integrity before and after the penetration process.