
The ethics

The ethical vision of security testing constitutes rules of engagement that have to be followed by an auditor to present professional, ethical, and authorized practices. These rules define how the testing services should be offered, how the testing should be performed, determine the legal contracts and negotiations, define the scope of testing, prepare the test plan, follow the test process, and manage a consistent reporting structure. Addressing each of these areas requires careful examination and the design of formal practices and procedures must be followed throughout the test engagement. Some examples of these rules are discussed as follows:

- Offering testing services after breaking into the target system before making any formal agreement between the client and auditor is completely forbidden. This act of unethical marketing can result in the failure of a business and might have severe legal implications depending on the jurisdictions of a country.
- Performing a test beyond the scope of testing and crossing the identified boundaries without explicit permissions from a client is prohibited.
- Binding a legal contract that should limit the liability of a job unless any illegal activity is detected. The contract should clearly state the terms and conditions of testing, the emergency contact information, the statement of work, and any obvious conflicts of interest.
- The test plan concerns the amount of time that is required to assess the security of a target system. It is highly advisable to draw up a schedule that does not interrupt the production of business hours.
- The test process defines the set of steps that are required to be followed during the test engagement. These rules combine technical and managerial views to restrict the testing process with its environment and people.
- Scope definition should clearly define all the contractual entities and the limits imposed on them during the security assessment.
- Test results and reporting must be presented in a clear and consistent order. The report must mark all the known and unknown vulnerabilities and should be delivered confidentially to the authorized individual only.