## Penetration testing is a challenging job. If you ask an experienced pentester about their work, they will tell you about the endless hours they spend doing their jobs, before they succeed and finish their task. But it’s not always as easy, and many a times they have to perform the process repeatedly, whether due to a small configuration mistake while exploiting a vulnerability or being unable to find a main target.

## In reality, it’s quite a journey to master the job of penetration testing. It includes sevteral failures before you achieve the much-deserved success. In fact, it is through this process that experts are able to acquire most of their knowledge.

## Let’s have a look at five common mistakes penetration testers make.

## Forgetting about Professional Ethics

## The basic difference between a hacker and ethical hacker is legality. Carrying out a penetration test not only requires a high-level of technical ability, it also needs you to follow professional ethics. It’s very common during this type of work to gain access to confidential or sensitive information. This could include security breach details that can potentially expose a corporation to real attacks. Hence, a good penetration tester should be able to handle the aspects of privacy, confidentiality and legality in a serious manner.

## However, it is not uncommon where professionals may use abusive tactics such as reporting exploited vulnerabilities to potential customers or executing unsolicited intrusion tests and then asking for payment to fix the problems. This is against professional ethics and must be avoided.

## Conducting a Test Without Getting Proper Authorization

## As a penetration tester, you still need to follow the rules. Work only for what you are authorized to. As a pentester, you may feel eager to demonstrate your ability and knowledge and may lose focus on the real objectives. However, it’s important to follow the scope of assessment and consider what type of tests can be performed, the time window of execution and assets that should not be touched.

## Not Keeping the Evidence

## An important part of pentesting is to collect and adequately store evidence during intrusion testing, as it forms the basis of your final report. Many times, penetration testers forget to keep important information as evidence. For instance, the vulnerabilities that were successfully exploited, a timestamp, activities that can be performed or the number of unsuccessful tries. This information is collectively important to build a fact-based report.

## Exclusively Relying on Tools

## Tools can make a pentester’s life easier. But relying solely on tools is not enough to become a skilled tester. In most of the cases, even the best solution will require a skilled professional to define what to scan and how to build context-specific exploit. They must know the concept behind an intrusion test.

## Not Developing Report Writing Skills

## The final step of a pentest is to write a comprehensive report of each activity performed along with the findings. An experienced professional should not only use automated tools to create a report but also be able to create meaningful reports related to their client’s business context.

We at Aardwolf Security have a professional penetration testing team with years of experience in the industry. Get in touch with us today to hire our penetration testing services.