binsec GmbH
Solmsstraße 41
60486 Frankfurt am Main

Overview of penetration testing

As a penetration tester, you will face the exciting challenge of performing security analyses of IT systems. Penetration testing arose more or less as a kind of countermeasure on behalf of IT security in an arms race against attackers. Potential clients ask us or hire us to identify vulnerabilities in their IT systems in order to subsequently reinforce them. But which technologies do we need to review in detail?

A pioneer in the security of web applications is the non-profit organisation Open Web Application Security Project (OWASP). In the OWASP TOP 10 project, the ten most common vulnerabilities in web applications are listed. (`https://owasp.org/www-project-top-ten/`).

The results from our penetration test should be noted down in a final report. This report constitutes the document that our client will be holding in his or her hands. And this is why we need to pay special heed to the reporting aspect. If we have identified a vulnerability, the client's management will have to make a decision on how to deal with the presented risk. In the best case scenario, the hole will be patched by software developers or IT administrators. This means that our report must be geared towards persons with a lot of IT knowledge as well as those with little IT knowlegede. This is generally accomplished by splitting the document into a management overview and a technical report. Both list all identified vulnerabilities, but they are distinguished by the author's intent. The management overview should highlight the risk of the vulnerabilities, whilst the detailed descriptiong of a vulnerability should comprise the following aspects in the technical report:

- Description of the vulnerability
- Description of the effects
- Proof of concept
- Recommendation

Challenge: Identify two vulnerabilities of the OWASP TOP 10 in one of their web applications of your choice (s. `https://owasp.org/www-project-vulnerable-web-applications-directory/`), write a final pentest report and send this encrypted with GPG by e-mail to ds@binsec.com. The corresponding public key is stored on a publicly accessible key server for this purpose.

Hints:

1. You need at least one attacker system and one target system for the above scenario.
2. You can create all servers with VirtualBox. Since the servers need to reach each other and programs need to be installed, the VBox setting "Nat-Network" is suitable as network configuration.
3. You may use Kali Linux for the attacker machine. Kali Linux is a free penetration testing and security auditing Linux distribution (derived from Debian, based on Debian testing), which includes more than 300 penetration testing tools and pre-installed services. The ISOs or the pre-built VMs can be downloaded from `https://www.kali.org/downloads/`. An introduction to Kali Linux is available from `https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf`.
4. The report could be structered as follows:
   - Cover sheet
   - Table of contents
   - Preamble
   - Management overview
   - Technical report