Professional And Ethical Standards

pentestlab.blog/category/general-lab-notes/page/6

January 8, 2013

Every penetration tester that works for the information security industry must have ethics that will help him to serve his client better and to avoid any illegal activities.Of course for this reason penetration testing companies are requiring from their penetration testers to sign the NDA (Non-disclosure agreement) in order to protect their clients and align with the current laws depending the location as the legal framework can be different from country to country.

However the penetration tester must be aware of the current laws and must remain fully ethical and professional at all times as the information security industry is not that big and a potential mistake can mark your career.So according to my personal opinion the following are some of the ethical standards that a penetration tester must have:

- Serve and protect the client and uphold the security profession
- Never take personal copies of client's data
- Never perform unauthorized testing
- Don't discuss findings with unauthorized people
- Don't publish vulnerabilities without permission
- Test everything in scope and never go outside
- Observe all legal requirements
- Act with integrity
- Avoid conflicts of interest
- Avoid FUD
- Avoid hubris
- Protect client's data (encryption etc.)
- Don't associate with black-hat hackers