Threatbutt

Pentesting Ethics QRC

Professional Penetration Tester's Code of Ethics

Thou shalt Serve and Protect the Client:

1. Do not test the security of systems without explicit written permission of a client.
2. Maintain confidentiality. Do not discuss findings with third parties, do not implicate individuals and do not use prior findings or information to advertise to and attract new customers.
3. Act responsibly. Notify and assist the client immediately if you discover a high-risk vulnerability (personal injury, criminal offense, etc.)
4. Observe scope. Work with your client to precisely establish what you will pentest.
5. Include safety measures to protect the continuity of your client's business processes.
6. Be truthful to your client during acquisition, pentesting and reporting.
7. Uphold the law.

Thou shalt be Professional:

1. Maintain and expand your knowledge of the Security profession.
2. Be proficient with your toolset: know its functionalities, limitations and effects.
3. Do not use your toolset in production before having tested it in an isolated environment.
4. Do not pentest destructively.
5. Attempt to do offsite blackbox testing before continuing on-site, to maintain objectivity and prevent influence.
6. Use your head. Do not solely rely on your tools, but be insightful, creative and smart.
7. Act responsibly. Do not attack systems that you know to be highly vulnerable. Assist your client in securing these systems first.
8. Do not engage publicly in pentesting contests. It could expose a client's network and cause a breach of confidentiality.

Thou shalt prevent False Positives, False Negatives and Conflicts of Interest:

1. Prevent the client from interfering with your pentest. It should be a snapshot of the state of security at a given moment; actively changing the parameters could influence the results.
2. Attempt to limit the amount of people involved with or with knowledge of the pentest.

3. Be objective. Absence of proof does not mean proof of absence - charge for pentests that have not yielded any vulnerabilities.
4. Be truthful, but careful. If you cannot best meet your client's needs, say so. However, do not recommend another party as this might become a conflict of interest or otherwise be taken as a false positive/negative.

Other Considerations

The integrity of the pentester is of paramount importance. Ethical use of your knowledge and tools are key, as these could be considered illegitimate under other circmustances.

Pentesting provides only a momentary view into the state of security at a given time. Improving security should be done through a continuous process of monitoring, patching, testing and hardening systems, and the client should be made aware of this in your pentesting report.

Being truthful and honest to your client includes the duty not to withhold any information on your performance, that of any relevant products, systems or services; to accurately credit other parties, products or systems where credit is due; to be as precise as possible in stating claims or estimates. Furthermore, you must accept responsibility for your work and the work of others who operate under your supervision, including the possibility of limited liability for the results.

You shall uphold these ethics and this code of conduct; not doing so is a violation and incompatible with being a security professional.

Should you violate these principles, then you must contact your professional organization's board of ethics. If you violate the law, you must also contact the relevant authorities.

Version: 1.0
Date: December 1st 2015

References

- *"Penetration Testing Professional Ethics: A Conceptual Model and Taxonomy*", by Justin D. Pierce, Ashley G. Jones, Matthew J. Warren, Australasian Journal of Information Systems, Vol. 13 No. 2, May 2006
- *"BCS Code of Conduct"*, http://www.bcs.org/upload/pdf/conduct.pdf, retrieved 11-11-2015
- *"ACM Code of Ethics"*, http://www.acm.org/about/code-of-ethics, retrieved 11-11-2015
- Header image: *"Threatbutt Comprehensive Internet Hacking Protections"*, http://www.threatbutt.com/, retrieved 11-11-2015

A. Eijkhoudt