

Advanced Hacking Training

Penetration Testing

Have you ever wondered why Microsoft's Active Directory is such a favored target of the world wide hacking community? Are you curious how to circumvent certain security protocols, like e.g. WiFi? Would you like to learn how to attack computer networks while also learning how to defend against said attacks?

In this advanced Hacking training using pen-testing and red-teaming techniques, you will find out.

Goals After completing this training, you will

- thoroughly understand the security architecture of the Microsoft secure authentication subsystem.
- have applied standard tools and techniques, such as Buffer Overflow, Malware generation, XSS attacks among others,
- be able to assess and exploit the security flaws of computer systems and networks.

Structure The training builds upon not only theoretical parts, but also emphasizes practical parts and thus consists of

- *lectures*, which presents technical topics,
- *many practical exercises*, to support the individual understanding, *extended project*, to deepen the gained knowledge and practice the covered techniques beyond the initial training session (Capture the Flag scenario).

Prerequisites For a successful participation, we recommend basic knowledge of computer sciences, a laptop to access the lab environment and a working internet connection.

Join us in following this fascinating path and find out how deep the rabbit hole goes.

For more information, please get in

contact@cryptosolutions.de