clarified security
we break security to bring clarity

Hands-on Hacking Essentials (HOHE) v5

Hands-on Hacking Essentials is an ***eye-opening*** training for IT specialists, system administrators and security practitioners, a much needed "***shock therapy***" for most.

Training duration: ***2 days*** of pure hacking and feeling "1337"

Group size: ***12 participants*** maximum

Trainers:

Taavi Sonets (in English or Estonian upon demand)

James Dodd (in English)

Karl Kristjan Raik (in English or Estonian upon demand)

Target audience: System admins, information security specialists & -managers and any other IT personnel that is not afraid of the shell or command prompt.

Contents of the training: (HOHE v5, updated January 2019)

Day One (introductions, essential attack phases, concepts attack vectors and tools):

- Introduction
- Kali Linux intro (participant's attack platform)
- Reconnaissance and information gathering
- Targets (a mix of Windows and Linux workstations and servers)
- Remote exploitation attacks
- Privilege escalation attacks
- Attack tool-sets and attack automation (incl. Metasploit Framework and meterpreter)
- "Jumping the (fire)wall" with targeted client-side attacks

Day Two (putting it all together in one training scenario):

- **„Network Takeover" scenario with Kali Linux and Armitage** – a whole day hands-on hacking scenario that walks participants through a small company network takeover scenario from an attacker's perspective.
- Mostly Armitage along with other tools on Kali Linux will be used for attacking, making it easy to track and visualize how the victim network reveals itself as participants hack deeper into the network.
- A brief reconnaissance followed by a targeted client-side attack gains your foothold. Pivoting your attacks through the initial compromised workstation and following up with local privilege escalation, scanning, password hash dumping, pass-the-hash and other attacks will deliver you the rest of the subnet. Credential and additional information harvesting, traffic capturing, data ex-filtration, steganography tools, PHP shells and other trickery will be used to compromise the rest of the subnets to find and steal steal the intellectual property you are after. We will also explain weaknesses in Windows credential handling by using tools such as Mimikatz and WCE (fairly popular tools among APT attackers) to dump plain-text passwords from any Windows

version. Towards the end you will also use AV evasion tools and techniques to defeat or bypass common defense tools.

- ❑ Your targets network consists of Windows 10 and various Linux based firewall and server distributions.
- ❑ **Feedback and training wrap-up**

Training methods: Trainers will engage participants with lectures, live attack demonstrations and practical examples followed by individual hands-on exercise scenarios. Training is interactive, practical, and besides active participation also full of attack stories that help to change the perspective and understanding of real life security threats.

Ideology of this training: The main differences between hacking and penetration testing are the intent and (imposed) limitations. Therefore, the **idea behind this training is to see practical information security from the attacker's or "opposing team's" point of view and to deliver first-hand experience or running attacks**.

Although this training is highly technical and extensively hands-on, all scenarios are built so that with the help of hints or even full HOWTO's from the scoring server, everyone can complete all exercises regardless of prior 1337 skills or experience level with various operating system.

Everyone will walk through the phases of an attack until successfully 0wning various systems and services. There are plenty of attack scenarios to play through and to complete scored objectives. Since the expected participants' skill and experience level is varying to a large degree, we cover a mix of *nix and Windows world and focus on explaining key concepts and on showing real attacks even to those who have never compiled or launched any exploits before.

Intended outcome: During the 2 day hands-on training experience the participants should form a good understanding of current attacker tool-set, attack types and methods. By experiencing the attacker mindset and point of view via hands-on exercises the participants not only will gain much higher appreciation for attack threats, but will be much more alert and better prepared for their own IT systems defense.

Delivery: We can deliver on-site at group pricing anywhere in the world where good broadband connection is available. Ask us for the group pricing or for times and locations of our public courses. Public groups are currently available directly or via partners in: ***Estonia***, ***Finland***, ***Sweden***.