clarified security
we break security to bring clarity

Hands-on Hacking Advanced (HOHA)

Hands-on Hacking Advanced (HOHA) is a follow-up course to our Hands-on Hacking Essentials (HOHE) training.

Training duration: 3 days of pure hacking and feeling "1337"

Group size: ***10 participants*** maximum

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

Pre-requisites: Prior HOHE participation is required to take this course to ensure minimum same level of participants

Trainer: (in English or Estonian upon demand)

- **Taavi Sonets**

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. Everyone will walk through the phases of an attack until successfully owning 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.

Training objectives: During the 3 days hands-on training experience the participants should build upon HOHE training in understanding of current attacker tool-sets, attack types and methods. By experiencing the attacker mindset and point of view via hands-on exercises the participants will use Cobalt Strike and other tools from Red Teaming perspective in order to understand what it takes in terms of individual skills to be a red team member with a bit of team-working towards the end.

Intended outcome: During the 3 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.

clarified security
we break security to bring clarity

Schedule
Day 1

Warm-up scenario - we introduce and use advanced features of Cobalt Strike, learn to create and deliver client-side attacks that are not recognized as malicious neither by the user nor various security products. Since all participants are expected to have completed our HOHE (Hands-on Hacking Essentials) course, we pick up speed fast and there is no time for much "spoon feeding".
Devmoon – a company "Network Takeover " scenario of "almost" fully patched and properly configured networks. We gain initial foothold by taking over end-user computers and also by compromising servers. We escalate privileges and spread deeper into the network via different pivoting techniques, such as SSH tunneling, SMB and DNS beacons, proxy tunneling and VPN pivoting.

Day 2

Devmoon – a company "Network Takeover " scenario (continues)
Instead of hoping for missing patches we elevate our privileges to root/SYSTEM in a fully patched Linux and Windows environments. We utilize different elevation techniques, detect weak or badly configured services and "hidden" features of daily used applications.
Devmoon – a company "Network Takeover " scenario (continues)
We spread further and take ultimate control by attacking the Domain Controller thanks to evil-usage of PowerShell, brute forcing different services such as SSH and FTP, exploiting advances "shellshock"-like vulnerabilities and creating malicious yet real documents.

Day 3

Devmoon – a company "Network Takeover " scenario (continues)
We finish mopping up our APT (Advanced Persistent Threat) style rampage of our hypothetical victim company Devmoon in order to move to the next topic.
Introduction to exploit development
There are many in-depth exploitation courses, but our goal is to get you going in just half a day in a very easy-to-understand way, hands-on. No previous programming experience is needed, we start from absolute zero! We learn how to find a buffer overflow vulnerability and write our own first buffer overflow exploit code. We use debuggers to look for issues within applications, identify application crashes using fuzzing techniques, generate reliable and undetectable shell-code and at the end we will write our (potentially first) working exploit.
We finish the course with the final feedback round, re-iterate what we learned in the process and ask your opinion of the course to continuously improve the content and learning experience.

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***.