"Corelan Advanced Training" <3-day course, +10 hours/day>

The Corelan ADVANCED exploit development class is a fast-paced, mind-bending, hands-on course where you will learn advanced exploit development techniques from an experienced exploit developer.

REMARK : This training starts at 9:00 and will end around 22:00 PM. That means +10 hours each day (Dinner will be foreseen)

Instructor: Peter Van Eeckhoutte

"Offensive PowerShell for Red and Blue Teams" <3-day course>

Learn to attack and defense Windows environment with PowerShell and other built-in tools in this training. This class takes students from concepts to hands-on on latest red team techniques and focuses on minimum detection and functionality abuse while also discussing fingerprints and defenses against discussed attacks. This hands-on training gives you one-month access to a realistic lab containing fully patched machines, multiple domains and forests and latest Windows machines.

Instructor: Nikhil Mittal

"Malicious Documents for Blue and Red Teams" <3-day course>

For this anniversary edition of BruCON, our resident trainer Didier Stevens will teach you how to both analyse as well as create malicious files such as PDF, Word and Excel documents.
You'll learn how to analyse malicious files as well as create your own for Red team testing!

Instructor: Didier Stevens

"A Practical Approach to Malware Analysis and Memory Forensics" <3-day course>

Learn to analyze, hunt and investigate malware. Perform static, dynamic, code and memory analysis. Understand adversary tactics and techniques. Investigate code injection, rootkits, hooking techniques and much more. Join us for 3-day hands-on training on malware analysis and memory forensics at BruCON 0x0A

Instructor: Monnappa K A

"Practical IoT Hacking" <3-day course>

"Practical Internet of Things (IoT) Hacking" is a unique course which offers security professionals, a comprehensive understanding of the complete IoT Technology suite including, IoT protocols, sensors, client side, mobile, cloud and their underlying weaknesses. The extensive hands-on labs enable attendees to identify, exploit or fix vulnerabilities in IoT, not just on emulators but on real smart devices as well. Attendees will get a eXos - custom IoT security Testing VM, Complete Lab manual and slides.

Instructor: Aseem Jakhar and Arun Magesh

"Windows Kernel Exploitation Advanced" <3-day course>

This training is the upgraded version of Windows Kernel Exploitation Foundation course.
In this course we will use Windows 10 RS2 x64 for all the labs. This course starts with the changes in Windows 10 RS2, Internals, hands-on fuzzing of Windows kernel mode drivers.

Instructor: Ashfaq Ansari

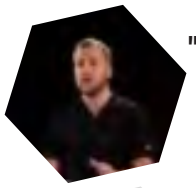
"Post Exploitation Adversary Simulations - Network Data Exfiltration Techniques" <3-day course>

The training class has been designed to present students modern and emerging tools and techniques available for network data exfiltration, testing and bypassing DLP/IDS/IPS/FW systems, protocol tunneling, hiding, pivoting and generating malicious network events. Highly technical content and only a hands-on practical approach guarantees that the usage of this transferred knowledge & technologies in real production environments will be easy, smooth and repeatable. Become confident that your network security / SOC environment really works!

Instructor: Leszek Miś

When: 1 - 3 October 2018
Where: Ghent

Prices: €1,400– €1,700
More information: www.brucon.org



"Threat Hunting in Industrial Control System Environments with Open Source Tools" <2-day course>

Industrial Control System environments contain purpose-driven network and hosts devices related to the production goal of the industrial environment. Due to the unique nature of production environments, IT approaches to threat hunting do not map well to OT environments. Within this training, we will share our approach to hunting in industrial control system environments using only open source tools.

Instructor: Daniel Michaud-Soucy and Marc Seitz

"Thinking Behind Enemy Lines – Actionable Threat Intelligence Tools and Technique" <2-day course>

In this course, which will include both lectures and hands on training, we will learn how to look beyond the malware itself in order to dig information on the infrastructure and actor behind it. We will understand the adversary's intents, way of thinking and the risk it poses against our threat model, to develop the best protections and mitigations.

Instructor: Irena Damsky

"Offensive Whiteboard Hacking for Penetration Testers" <2-day course>

With this training we will teach you how to use threat modeling as an offensive weapon. Traditional threat modeling looks at the attacker, the asset and the system. With offensive threat modelling we look at the defender to understand his tactics and expose weaknesses. You will be challenged to perform practical threat modelling in groups of 3 to 4 people covering the different stages of offensive threat modelling on applications, IOT devices and a nuclear facility.

Feedback from a Black Hat 2017 training attendee:
"I feel that this course is one of the most important courses to be taken by a security professional."

Instructor: Sebastien Deleersnyder and Steven Wierckx

HACKING FOR B33R

BRUCON

0X0A

When: 1 - 3 October 2018
Where: Ghent

Prices: €1,400– €1,700
More information: www.brucon.org