Hacking Training

Practical, Hands-On, Lab-Based Hacking.

WE HACK.
WE TEACH.

NOT SO SECURE
A Claranet Group Company

claranet cyber security

75% Hands-on Learning in Our Modern Hack Lab

Updated Regularly to Include Trending Techniques

Written by BlackHat Trainers and Available Globally

For more information contact
T: 415 659 1543
contact@notsosecure.com

Hacking 101

This course will teach you the foundations of pen testing and how to find and exploit vulnerabilities. This introductory course will train attendees in understanding pen testing, and provide background information, risks and vulnerabilities associated with different systems.

Attendees will gain understanding in the following topics:

- Understand different network topologies and addressing schemes
- Understand the properties and security of common network protocols and the network protocol stacks.
- How to fingerprint, enumerate and exploit common windows and linux misconfigurations and vulnerabilities.
- Differentiate between types of wireless standards and understand the benefits and risks associated with these standards.
- How to exploit common web application security flaws.

Students will get access to an online training platform which will be used to practice the concepts taught during the course.

SCAN TO FIND OUT MORE

The Art of Hacking Bootcamp

Master the Art of Hacking by building your hands-on skills in a sophisticated hack-lab with material that is delivered on the world conference stage; certified, accredited, continually updated and available globally.

This introductory / intermediate class brings together both infrastructure hacking and web hacking into a 5-day "Art of Hacking" class designed to introduce the fundamentals of penetration testing.

This hands-on class was written to address the market need around the world for a real practical experience that focuses on what knowledge and tools are really needed when conducting a penetration test. The variety of tools used are the key tools that should be in any penetration tester's kit bag and are those used by our very own penetration testers.

Updated Regularly To Include Trending Techniques

One of the best classes I've taken in a long time. The content was on point and kept me engaged. I'm new to Cyber Security after 25 years in App Development and very pleased with what I have learned

Delegate, Black Hat USA

SCAN TO FIND OUT MORE

Infrastructure Hacking

Introduction into infrastructure testing. Gain practical experience using professional tools. Leave with the basis to take your testing knowledge forward into more advanced infrastructure topics.

Part of The Art of Hacking

This is an entry-level infrastructure security and testing class and is a pre-requisite for our Advanced Infrastructure Hacking class. This class familiarizes the attendees with the basics of network hacking. A number of tools and techniques will be taught during this 3-day class, If you would like to step into the world of ethical hacking / pen testing this is the right class for you.

This class familiarizes the attendees with a wealth of hacking tools and techniques. The class starts from the very basic and gradually builds up to the level where attendees not only use the tools and techniques to hack various components involved in infrastructure hacking, but also walk away with a solid understanding of the concepts on which these tools work.

Introduction into key tools that build a must have pen tester kit.

SCAN TO FIND OUT MORE

Web Hacking

Introduction into web application hacking. Practical in focus, teaching how web application security flaws are discovered. Covering leading industry standards and approaches.

Part of The Art of Hacking

This entry-level class familiarizes the attendees with the basics of web and application hacking. A number of tools and techniques will be taught during the 2 day class. If you would like to step into the world of ethical hacking / pen testing with a focus on web applications, then this is the right class for you.

The class starts from the very basic and then gradually builds up to a level where attendees can use the tools and techniques to hack various components involved in web application hacking. The class covers the industry standards such as OWASP Top 10, PCI DSS and contains numerous real life examples to help the attendees understand the true impact of these vulnerabilities.

Written by leading BlackHat trainers & world renowned penetration testers.

SCAN TO FIND OUT MORE

Specialist Offensive Classes

Advanced Infrastructure Hacking

Covering the latest relevant exploits. Teaching a wide variety of offensive hacking techniques. Written by real pen testers with a world conference reputation (BlackHat, AppSec, OWASP, Defcon etc).

This fast-paced class teaches the audience a wealth of advanced hacking techniques to compromise various operating systems and networking devices. The class will cover advanced penetration techniques to achieve exploitation and will familiarize delegates with hacking of common operating systems, networking devices and much more.

Whether you are pen testing, red teaming, or hoping to gain a better understanding of managing vulnerabilities in your environment, understanding advanced techniques for infrastructure devices and systems is critical.

While prior pen testing experience is not a strict requirement, a prior use of common hacking tools such as Metasploit is recommended for this class.

Real world challenges from local privilege escalation to network exploitation (VLAN, VOIP, VPN included), cloud attacks and more

SCAN TO FIND OUT MORE

Advanced Web Hacking

The class allows attendees to practice some neat, new and ridiculous hacks which affected real life products and have found a mention in real bug-bounty programs.

This fast-paced class, gives attendees an insight into Advanced Web Hacking, the team has built a state of the art hacklab and recreated security vulnerabilities based on real life Pen Tests and real bug bounties seen in the wild.

Some of the highlights of the class include:

Modern JWT, SAML, oauth bugs

Core business logic issues

Practical cryptographic flaws.

RCE via Serialisation, Object, OGNL and template injection.

Exploitation over DNS channels

Advanced SSRF, HPP, XXE and SQLi topics.

Serverless exploits

Web Caching issues

Attack chaining and real life examples.

Updated Regularly To Include Trending Techniques

SCAN TO FIND OUT MORE

Hacking and Securing Cloud infrastructure

Brand new for 2019, this 2-day course cuts through the mystery of Cloud Services (including AWS, Azure and G-Cloud) to uncover the vulnerabilities that lie beneath.

In order to manage vulnerabilities in a Cloud environment, understanding relevant hacking techniques, and how to protect yourself from them, is critical. This course covers both the theory as well as a number of modern techniques that may be used to compromise various Cloud services and infrastructure, along with the tools and skills required to defend against them.

Who should attend?
Cloud Administrators, Developers, Solutions Architects, DevOps Engineers, SOC Analysts, Penetration Testers, Network Engineers, security enthusiasts and anyone who wants to take their skills to next level.

Prior pentest experience is not a strict requirement, however, some knowledge of Cloud Services and a familiarity with common command line syntax will be greatly beneficial.

SCAN TO FIND OUT MORE

Specialist Defensive Classes

AppSec for Developers

Covers latest industry standards such as OWASP Top 10. Thorough guidance on security best practices (like HTTP header such as CSP, HSTS header etc.). References to real world analogy for each vulnerability.

Application security is a top concern for us and the best way to battle it out is to nip it in the bid during the development stage itself. This class is geared towards those who wish to understand OWASP Top 10 and want to avoid breaches like that of Equifax in 2017 with good references to vulnerabilities found on popular websites like Google, Facebook, Twitter, Paypal etc...

A highly-practical class that targets web developers, pen testers, and anyone else who would like to learn about writing/ auditing secure code against security flaws. The class covers a variety of best the security practices and in-depth approaches.

Hack lab access after course completion

SCAN TO FIND OUT MORE

DevSecOps

This class will give the audience a holistic approach in assessing and securing web applications in an automated fashion within the existing CI/CD pipeline.

Modern enterprises are implementing the technical and cultural changes required to embrace DevOps methodology. DevSecOps extends DevOps by introducing security early into the SDLC process, thereby minimizing the security vulnerabilities and enhancing the software security posture. In this workshop we will show how this can be achieved through a series of live demonstrations and practical examples.

As part of this workshop attendees will receive a state-of-the-art DevSecOps tool-chest comprising of various open-source tools and scripts to help the DevOps engineers in automating security within the CI/CD pipeline. While the workshop uses Java/J2EE framework, the workshop is language agnostic and similar tools can be used against other application development frameworks.

Attendees will receive a state-of-the-art DevSecOps Tool-Chest

SCAN TO FIND OUT MORE

AppSecOps

AppSecOps is a course to help you understand and mitigate application security vulnerabilities in your DevOps environment.This will help in closing the security loopholes at a very early stage of the SDLC process.

This class is geared towards understanding what application security vulnerabilities are, their trends and to gain an insight into the impact through practical demonstrations.

This will cover how to fix/avoid them by discussing various strategies, best practices , code snippets and tools (Hackers/application security tester's view) and how to inject Security into your DevOps pipeline to automate security and develop a DevSecOps pipeline

This class is for those who wish to learn about application security vulnerabilities and understand more about their impact.

A holistic approach for identification of security bugs and then integrating the security into your devops pipeline to automate the process of fixing and triaging the bugs

SCAN TO FIND OUT MORE

SCAN TO DOWNLOAD A PDF VERSION OF THIS BOOKLET

www.notsosecure.com