Penetration Testing Essentials Course Outline
(4 days)

The **Penetration Testing Essentials Course** is designed to provide practitioners with working knowledge of the cyber security challenges facing their environments. This knowledge is vital when managing the day to day running of all aspects of security risk for those environments.

This course is aimed at teaching students the basics of penetration testing to prepare them for the boot camp certification level course.

Who should attend?

- Those moving into the information security sector from a different sector.
- Those who would like to learn about penetration testing but not ready for an accreditation level course.
- Those who want to learn how adversaries target their companies.
- New graduates moving into transitioning in employment.
- Those who are retraining including those leaving military service.

…then this course is for you!

Pre-Requisites

There are no real pre-requisites to this course, however some skills are preferable such as:

- Basic knowledge of Microsoft Windows and Linux operating systems including navigation of file systems, installation and execution of applications and use of text editors.

If you are unsure on any of these skills or level please contact us to discuss them further.

What you will learn on this course

By the end of the course, you will be able to:

- Prepare a new penetration testing environment.
- Plan and prepare a penetration testing operation.
- Build and customise various VM's for attacking or testing.
- Install, deploy and customise penetration testing tools.

- Conduct operating system and technology reconnaissance.
- Scan and map target device or network.
- Obtain and maintain access to a target device or network.
- Perform escalation of privileges within a target network or device.
- Manage system logs and cover tracks when exiting target device or network.

Course Duration

The course consists of 4 days of classroom training. The course contains hands on exercises and examples of the hacking lifecycle to reinforce theory taught by our instructors.

Course Contents

Part 1: Performing basic OSINT and reconnaissance of a target network.
Part 2: Scanning of target network and completing a vulnerability assessment.
Part 3: Performing basic exploitation.
Part 4: Performing and maintaining privileged escalation.
Part 5: Covering tracks and exiting the target network.
Part 6: Completing a Capture the Flag style exercise to demonstrate skills covered in the first 5 part of the training course.

What training should follow on from this?

This course is a Level 2 Foundation course but it can be used as preparation for more focussed training such as the:

- Siker ICS405: Securing ICS course.
- EC-Council: Certified Ethical Hacker (CEH).
- GIAC Global Penetration Tester Professional (GPEN) certification.

For more information go to www.sikercyber.com