Cyber Security Penetration Testing Courses

What is Cyber Security Penetration Testing?

Cyber Security Penetration testing is a process of finding vulnerabilities in an application, system, or computer network so that they can be fixed before malicious hackers find them and exploit the flaws to break into the system. For the successful completion of a penetration test project, information security experts need to know how attackers think and what they do when they get a crack into a system or network.

Purpose of Penetration Testing

The primary goal of penetration testing is to carry out an authorized and systematic investigation by the concerned stakeholders of potential vulnerabilities in the system (application, network, etc.) with regard to planned changes, new installations, or additional operating environments. It provides real-time assessment of vulnerabilities at client sites without affecting their production environment.

Vulnerability assessment is a part of the penetration testing process, which attempts to identify and classify exploitable vulnerabilities that attackers can target. These vulnerabilities often relate to outdated software and systems that are not configured correctly or have known security flaws that the organization has failed to patch.

Content for Cyber Security Penetration Testing Courses

Cyber security penetration testing courses provide training on understanding vulnerabilities and how to find them, as well as techniques for exploiting security holes and writing proof-of-concept exploits. The course is designed for IT professionals looking to gain a better understanding of penetration testing.

Typically, the course will feature:

- Vulnerability Assessment
- Types of Penetration Testing
- Target Reconnaissance
- System Hacking
- Web Application Penetration Testing Ethical Hacking

Who Can Enroll in Cyber Security Penetration Testing Courses?

cyber security course in malaysia can be taken by anyone who is interested in learning the process of penetration testing. This includes IT professionals, application developers, or even hobby enthusiasts.

The course generally requires a basic understanding of computers and operating systems which would be useful during the lab sessions where students are given access to virtual machines on which they carry out penetration testing.

Duration of Cyber Security Penetration Testing Courses

The course generally takes a minimum of 40 hours to complete, which consists of both online and offline sessions on penetration testing techniques. The classes are conducted using a combination of video lectures, presentations, and hands-on lab exercises. Students work in a live laboratory environment with pre-installed hacking tools and techniques which provides a realistic experience.

Expert instructors guide students through the course modules using presentations, practical examples, and live demonstrations on the latest penetration testing techniques. Typically, the course is designed so that beginners can attend and learn with no prior knowledge of penetration testing while experienced candidates will find new information and ideas around old methodologies.

Conclusion

The need to secure systems and applications from malicious attacks has been growing at a fast pace. The next best thing after antivirus is penetration testing. Penetration testing is the only way you can know how attackers are targeting your data, what they are doing when they get in and how to avoid being a victim. There are many cyber security penetration testing courses available in the market.

cyber security course