



Ethical Hacking

A Five-Day Course

To be successful in securing your information systems, you must understand the threats they face, such as malicious hackers who use numerous methods of attack to achieve their goal. Understanding the cunning, resourceful hackers is required to be able to stop them. We'll give you that understanding.

This instructor-led training provides detailed knowledge about the threats, business impact and security precautions available. You'll receive hands-on skills and immediately utilize them, by being immersed in the hacking process. You'll use hacker tools in a safe lab environment to learn how hackers perform malicious acts. At every step, we'll discuss why the hacker is able to succeed, and what can be done to prevent his success.

This course helps you understand that security is a business process and must be evaluated against the goals of and its financial impact on the business. You'll get a balanced view for implementing the appropriate security controls, both technologically and financially--and you'll have practical experience for your everyday work.

Course Contents

Who Hackers Are

- Hacker Motives
- What Hackers Do
- How Hackers Do What They Do

The Hacking Process

- Selecting the Target
- Gathering Information
- Identifying Systems
- Gaining Access
- Getting Credentials
- Acquiring Privileges
- Avoiding Detection
- Expanding His Realm
- Realizing His Goal

Security Process

- Inspection
- Protection
- Detection
- Reaction
- Reflection

Halting the Hacker

- Reducing Your Target Profile
- Limiting Information Disclosure
- Limiting Access
- Controlling Authentication
- Controlling Authorizations
- Increasing Monitoring

Who Should Attend

Managers with a technical background and those who are responsible for administering the security of systems and networks should attend this class. Additionally, anyone with an interest in understanding the hacking process will also benefit.

You'll need a good understanding of TCP/IP as well as administrative experience; scripting and programming experience is a plus. This is an intermediate level course.

What You'll Learn

- The ease with which systems are corrupted.
- How to think like a hacker in order to better protect your own systems.
- How to evaluate threats and identify the business impact and the security precautions available.

What You'll Do

- Examine the hacking process of
 - Gathering information
 - Scanning networks
 - Profiling systems
 - Gaining access
 - Acquiring authorizations
 - Avoiding detection
 - Expanding control
- Use hacker tools in a safe lab environment to learn how hackers perform malicious acts.
- Discuss why the hacker is able to succeed, and what can be done to prevent his success.

What You'll Take Home

- An understanding that security is a business process and has to be evaluated against the goals of and the financial impact on the business.
- A balanced view for implementing the appropriate security controls, both technologically and financially.
- Your personal copies of *Information Security: Protecting the Global Enterprise* and *Halting the Hacker: A Practical Guide to Computer Security*.