

# Symantec™ Infrastructure Security Principles

---

## Course Description

The Infrastructure Security Principles course provides an in-depth examination of the various methodologies and routes attackers use to compromise security by gaining access to hosts and networks. It includes four modular, half-day Instructor-led sessions that are tailored to address the organization's specific needs.

The **Introduction to Digital Security** session focuses on the business reasons motivating digital security, and the principles to be applied when developing any security strategy. Recent trends and incidents are discussed to gain a better understanding of the current state of digital technology.

The **Network Security** session focuses on security practices for digital networks. This session begins by examining the methodology employed by attackers against networks. An overview is provided of encryption technology and security-related cryptography applications, including demonstrations of cryptography best practices. The network attacks module describes examples of sniffing, man-in-the-middle, and denial of service attacks and countermeasures. Finally, a description of wireless networking, threats to wireless networks, and countermeasures to those threats closes out the session.

The **Windows Operating System Security** session and the **Linux Operating System Security** session both focus on securing computers running the Windows or Linux operating systems. Both sessions begin by defining the methodologies used when attacking hosts. Next, characteristics of each operating system and applications that are commonly exploited by attackers are evaluated. In the respective host access attacks module, demonstrations provide examples of password gathering, and cracking techniques, rootkit and Internet-based attacks and their countermeasures. Final discussions examine

the strategies for building hardened Windows and Linux hosts.

Symantec instructors have in-depth security expertise drawn from years of experience understanding and addressing infrastructure security strategy, design, implementation, and operations.

---

## Who Should Attend?

This course is designed for network and system administrators, architects, and those in information technology wishing to gain deeper insights into potential routes of compromise within hosts and networks.

---

## Learn How To:

- Apply the best-practice security principles to harden networks and hosts against attacks.
- Understand attackers' methodologies in order to deploy the most effective countermeasures.

## Course Outline

These sessions have both lecture and demonstrations.

### Session 1: Introduction to Digital Security

#### *Digital Security Business Imperatives*

- Business Drivers
- Technology Drivers
- Threat Drivers
- Regulatory Drivers

#### *Security Principles*

- Strategic Principles
- Design Principles
- Implementation Principles

### Session 2: Network Security

#### *Attack Methodology*

- Objective: Discover
- Objective: Attack
- Objective: Escalate
- Objective: Maintain

#### *Cryptography*

- Encryption
- Hashing
- Cryptography Threats
- Network Authentication

#### *Network Attacks and Countermeasures*

- Network Device Overview and Discovery Attacks
- Denial of Service Attacks
- Network Security Best Practices

#### *Risks Associated with 802.11 Wireless Networks*

- Introduction to Wireless Networks
- Discovering in Wireless Networks

- Attacking in Wireless Networks
- Wireless Network Design Best Practices

### Session 3: Windows Operating System Security

#### *Attack Methodology*

- Objective: Discover
- Objective: Attack
- Objective: Escalate
- Objective: Maintain

#### *Windows Host Attacks and Countermeasures*

- Introduction to Windows OS Security Concepts
- Windows Host Attacks
- Attacking Windows Hosts from the Internet
- Attacking Windows Hosts from User Applications

#### *Windows Host Hardening*

- Introduction to Host Hardening
- Windows Host Hardening Guidelines

### Session 4: Linux Operating System Security

#### *Attack Methodology*

- Objective: Discover
- Objective: Attack
- Objective: Escalate
- Objective: Maintain

#### *Linux Host Attacks and Countermeasures*

- Introduction to Linux OS Security Concepts
- Linux Host Attacks
- Attacking Linux Hosts from User Applications
- Linux Host Attacks and Countermeasures Summary

#### *Linux Host Hardening*

- Introduction to Host Hardening
- Linux Host Hardening Guidelines

## More information

### *Visit our website*

<http://ses.symantec.com/securitylearning>

### *To speak with a Security Learning Services Specialist*

US toll-free 866 271 8200

903 731 9110

### *About Symantec*

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

### *Symantec World Headquarters*

20330 Stevens Creek Blvd.

Cupertino, CA 95014 USA

408 517 8000

800 721 3934

[www.symantec.com](http://www.symantec.com)

