

## **MCSA Security + Certification Program**

12 credit hours

270 hours to complete certifications

**Tuition: \$4500**

Information technology positions are high-demand occupations that support virtually all industries. The 12-week MCSA SECURITY + certification program is designed to help new IT professionals become competent in Microsoft network operating systems (MCSA) as well as Security +. Modules are not in chronological order.

Successfully completing this course will meet the requirements for **DoD 8570: IAT Level II and IAM Level I**.

**A+ The first two days will familiarize students with the principles of hardware and A+ certification.**

### **Security +**

Students will learn about IT industry-wide security topics, including communication security, infrastructure security, cryptography, access control, authentication, external attack, and operational and organization security. Other topics included in this course are protocols used in Linux, UNIX, and Windows 2000 in addition to the TCP/IP suite component protocols, and Ethernet operations. Students will gain knowledge in capturing, analyzing, and generating IP traffic, how to exploit protocol weaknesses and examine defensive solutions. Packet filtering, password policies, and file integrity checking are also covered.

## **Microsoft Vista**

Candidates for this exam operate in medium to very large computing environments that use Windows XP Professional as a desktop operating system. They have a minimum of one year of experience implementing and administering any desktop operating system in a network environment.

Students will study and practice the following skills:

- **Perform and troubleshoot an attended installation of Windows Vista.**
- **Configure and manage file systems.**
- **Manage and troubleshoot drivers and driver signing.**
- **Troubleshoot cache credentials.**
- **Configure, manage, and troubleshoot Internet Explorer security settings.**

## **Microsoft 70-290: Managing and Maintaining a Microsoft Windows Server Environment**

This part of the MCSA certification is intended for IT professionals who work in the complex computing environment of medium to large companies. An individual with this credential will administer client and network operating systems in environments that have the following characteristics: 250 to 5,000 or more users; three or more physical locations; three or more domain controllers; network services and resources such as messaging, database, file and print, proxy server, firewall, Internet, intranet, remote access, and client computer management. Network administrators will connect branch offices and individual users in remote locations to the corporate network and connecting corporate networks to the Internet.

Students will study and practice the following skills:

### **Managing and Maintaining Physical and Logical Devices**

Manage basic disks and dynamic disks.

Monitor server hardware. Tools might include Device Manager, the Hardware

Troubleshooting Wizard, and appropriate Control Panel items.

Optimize server disk performance.

Implement a RAID solution.

Defragment volumes and partitions.

Troubleshoot server hardware devices.

Diagnose and resolve issues related to hardware settings.

Diagnose and resolve issues related to server hardware and hardware driver upgrades.

Install and configure server hardware devices.

Configure driver signing options.

Configure resource settings for a device.  
Configure device properties and settings.

### **Managing Users, Computers, and Groups**

Manage local, roaming, and mandatory user profiles.  
Create and manage computer accounts in an Active Directory environment.  
Create and manage groups.  
Identify and modify the scope of a group.  
Find domain groups in which a user is a member.  
Manage group membership.  
Create and modify groups by using the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in.  
Create and modify groups by using automation.  
Create and manage user accounts.  
Create and modify user accounts by using the Active Directory Users and Computers MMC snap-in.  
Create and modify user accounts by using automation.  
Import user accounts.  
Troubleshoot computer accounts.  
Diagnose and resolve issues related to computer accounts by using the Active Directory Users and Computers MMC snap-in.  
Reset computer accounts.  
Troubleshoot user authentication issues.

### **Managing and Maintaining Access to Resources**

Configure access to shared folders.  
Manage shared folder permissions.  
Troubleshoot Terminal Services.  
Diagnose and resolve issues related to Terminal Services security.  
Diagnose and resolve issues related to client access to Terminal Services.  
Configure file system permissions.  
Verify effective permissions when granting permissions.  
Change ownership of files and folders.  
Troubleshoot access to files and shared folders.

### **Managing and Maintaining a Server Environment**

Monitor and analyze events. Tools might include Event Viewer and System Monitor.  
Manage software update infrastructure.  
Manage software site licensing.  
Manage servers remotely.  
Manage a server by using Remote Assistance.  
Manage a server by using Terminal Services remote administration mode.  
Manage a server by using available support tools.  
Troubleshoot print queues.

Monitor system performance.

**Monitor file and print servers. Tools might include Task Manager, Event Viewer, and System Monitor.**

Monitor disk quotas.

Monitor print queues.

Monitor server hardware for bottlenecks.

Monitor and optimize a server environment for application performance.

Monitor memory performance objects.

Monitor network performance objects.

Monitor process performance objects.

Monitor disk performance objects.

Manage a Web server.

Manage Internet Information Services (IIS).

Manage security for IIS.

**Managing and Implementing Disaster Recovery**

Perform system recovery for a server.

Implement Automated System Recovery (ASR).

Restore data from shadow copy volumes.

Back up files and System State data to media.

Configure security for backup operations.

Manage backup procedures.

Verify the successful completion of backup jobs.

Manage backup storage media.

Recover from server hardware failure.

Restore backup data.

Schedule backup jobs.

**Microsoft 70-291: Implementing, Managing, and Maintaining a Windows Server Network Infrastructure**

This part of the MCSA certification measures an individual's ability to implement, manage, and maintain a Windows Server 2003 network infrastructure.

Students will study and practice the following skills:

**Implementing, Managing, and Maintaining IP Addressing**

Configure TCP/IP addressing on a server computer.

Manage DHCP.

- Manage DHCP clients and leases.
- Manage DHCP Relay Agent.
- Manage DHCP databases.
- Manage DHCP scope options.
- Manage reservations and reserved clients.

### **Troubleshoot TCP/IP addressing**

- Diagnose and resolve issues related to Automatic Private IP Addressing (APIPA).
- Diagnose and resolve issues related to incorrect TCP/IP configuration.

### **Troubleshoot DHCP.**

- Diagnose and resolve issues related to DHCP authorization.
- Verify DHCP reservation configuration.
- Examine the system event log and DHCP server audit log files to find related events.
- Diagnose and resolve issues related to configuration of DHCP server and scope options.
- Verify that the DHCP Relay Agent is working correctly.
- Verify database integrity.

### **Implementing, Managing, and Maintaining Name Resolution**

Install and configure the DNS Server service.

- Configure DNS server options.
- Configure DNS zone options.
- Configure DNS forwarding.

### **Manage DNS.**

- Manage DNS zone settings.
- Manage DNS record settings.
- Manage DNS server options.

**Monitor DNS. Tools might include System Monitor, Event Viewer, Replication Monitor, and DNS debug logs.**

### **Implementing, Managing, and Maintaining Network Security**

#### **Install and configure software update infrastructure.**

- Install and configure software update services.
- Install and configure automatic client update settings.
- Configure software updates on earlier operating systems.

**Monitor network protocol security.** Tools might include the IP Security Monitor Microsoft Management Console (MMC) snap-in and Kerberos support tools.

**Troubleshoot network protocol security.** Tools might include the IP Security Monitor MMC snap-in, Event Viewer, and Network Monitor.

## **Implementing, Managing, and Maintaining Routing and Remote Access**

### **Configure Routing and Remote Access user authentication.**

- Configure remote access authentication protocols.
- Configure Internet Authentication Service (IAS) to provide authentication for Routing and Remote Access clients.
- Configure Routing and Remote Access policies to permit or deny access.

### **Manage remote access.**

- Manage packet filters.
- Manage Routing and Remote Access routing interfaces.
- Manage devices and ports.
- Manage routing protocols.
- Manage Routing and Remote Access clients.

### **Manage TCP/IP routing.**

- Manage routing protocols.
- Manage routing tables.
- Manage routing ports.

### **Implement secure access between private networks.**

### **Troubleshoot user access to remote access services.**

- Diagnose and resolve issues related to remote access VPNs.
- Diagnose and resolve issues related to establishing a remote access connection.
- Diagnose and resolve user access to resources beyond the remote access server.

### **Troubleshoot Routing and Remote Access routing.**

- Troubleshoot demand-dial routing.
- Troubleshoot router-to-router VPNs.

### **Maintaining a Network Infrastructure**

Monitor network traffic. Tools might include Network Monitor and System Monitor.

### **Troubleshoot connectivity to the Internet.**

### **Troubleshoot server services.**

- Diagnose and resolve issues related to service dependency.



- Use service recovery options to diagnose and resolve service-related

## Instructor Bio

Mr. Vy Nguyen has 12 years of experience teaching college courses in server networks and operating systems. Mr. Nguyen taught students the skills and knowledge necessary to support end users who run Windows NT, Windows XP, and Windows 200x operating systems in a corporate, small business, or home environment. In this role, he has prepared students to pass the Microsoft certification exams.

As a professional Network Engineer for more than 20 years, Mr Nguyen has provided extensive technical leadership in multiple areas including managing a team consisting of engineers, scientists, and contractors in the formulation and development of a complex simulation. This was used to assess electromagnetic launchers, conduct trade studies, and perform parametric studies. Mr. Nguyen manages technical staff, computer technicians, and application programmers in planning and coordinating computer production and application development. He has also mentored IT support contractors (TAMS) in the computer security and system administration for secure Windows Server systems.