STUDENT ACTIVITY 3.3_A_KEY: NETWORK ISOLATION

MTA Course: 98-367 Security Fundamentals
Topic: Network Isolation
File name: SecurityFund_SA_3.3_A_Key

Lesson Objective

3. 3_A: Understand network isolation. *This objective may include but is not limited to:* VLANs; routing; honeypot; perimeter network; NAT; VPN; IPsec; Server and Domain Isolation.

Resources, software, and additional files needed for this lesson

- None

Directions to the student

Identify the scenarios in which you might deploy Windows Server® 2003 Routing and Remote Access NAT to include connecting a business or home to the Internet.

Connecting a Business or Home to the Internet

In a typical deployment that uses Windows Server 2003 Routing and Remote Access NAT, a small- or medium-sized business (or home office) assigns private IPv4 addresses to its computers and installs a Routing and Remote Access NAT-enabled router. The computers on the private network cannot gain access to the Internet directly because they have reusable private addresses. Instead, they gain access to the Internet through the NAT-enabled router.

The NAT-enabled router has both a private interface and a public interface, the public IPv4 address of the latter provided by a local ISP. When a client computer sends a request out to a resource on the Internet, the request is sent initially to the NAT-enabled router, which translates the request packets, forwards them to the Internet resource, accepts responses from the Internet resource, retranslates the packets, and then returns the response to the client.

Another example in which NAT technology can provide access to the Internet is the case of a small ISP that serves home users who have dial-up connections. In this case, the NAT-enabled router is located at the ISP. Whenever the customer dials in, the ISP assigns a private IPv4 address to the customer's computer. When the customer requests access to a server on the Internet, the NAT-enabled router at the ISP translates the outgoing request and, later, the incoming response.