STUDENT ACTIVITY 3.2_KEY: NETWORK ACCESS PROTECTION

MTA Course: 98-367 Security Fundamentals
Topic: Network Access Protection
File name: SecurityFund_SA_3.2_Key

Lesson Objective

3.2: Network Access Protection. *This objective may include, but is not limited to:* purpose of NAP, requirements for NAP.

Background

Components of the NAP infrastructure known as enforcement clients (ECs) and enforcement servers (ESs) require health state validation and enforce limited network access for noncompliant computers for specific types of network access or communication. Windows® 7, Windows XP Service Pack 3, and Windows Server® 2008 R2 include NAP support.

How does NAP enforce each of the following?

1. Internet Protocol security (IPsec)-protected traffic

   Answer: With IPsec enforcement, a computer must be compliant to initiate communications with other compliant computers. Because IPsec enforcement is leveraging IPsec, you can define requirements for protected communications with compliant computers on a per-IP address or per-TCP/UDP port number basis. IPsec enforcement confines communication to compliant computers after they have successfully connected and obtained a valid IP address configuration. IPsec enforcement is the strongest form of limited network access or communication in NAP.
   The components of IPsec enforcement consist of a Health Registration Authority (HRA) running Windows Server 2008 and an IPsec Relying Party EC in Windows 7, Windows XP Service Pack 3, and Windows Server 2008 R2. The HRA obtains X.509 certificates for NAP clients when they prove that they are compliant. These health certificates are then used to authenticate NAP clients when they initiate IPsec-protected communications with other NAP clients on an intranet.

2. IEEE 802.1X-authenticated network connections

   Answer: With 802.1X enforcement, a computer must be compliant to obtain unlimited network access through an 802.1X-authenticated network connection, such as to an authenticating Ethernet switch or an IEEE 802.11 wireless access point (AP). For noncompliant computers, network access is limited through a restricted access profile placed on the connection by the Ethernet switch or wireless AP. The restricted access profile can specify IP packet filters or a virtual LAN (VLAN) identifier (ID) that corresponds to the restricted network. 802.1X enforcement enforces health policy requirements every time a computer attempts an 802.1X-authenticated network connection. 802.1X enforcement also actively monitors the health status of the connected NAP client and applies the restricted access profile to the connection if the client becomes noncompliant.
   The components of 802.1X enforcement consist of NPS in Windows Server 2008 R2 and an EAP Quarantine EC in Windows 7 and Windows Server 2008 R2. For Windows XP with Service Pack 3, there are separate ECs for wired and wireless connections. 802.1X enforcement provides strong limited network access for all computers accessing the network through an 802.1X-authenticated connection.

3. Remote access VPN connections

   Answer: With VPN enforcement, a computer must be compliant to obtain unlimited network access through a remote access VPN connection. For noncompliant computers, network access is limited through a set of IP packet filters that are applied to the VPN connection by the VPN server. VPN enforcement enforces health policy requirements every time a computer attempts to obtain a remote access VPN connection to the network. VPN enforcement also actively monitors the health status of the NAP client and applies the IP packet filters for the restricted network to the VPN connection if the client becomes noncompliant.
   The components of VPN enforcement consist of NPS in Windows Server 2008 and a Remote Access Quarantine EC in Windows 7, Windows XP Service Pack 3, and Windows Server 2008 R2. VPN enforcement provides strong limited network access for all computers accessing the network through a remote access VPN connection.

   Note: VPN enforcement with NAP is different than Network Access Quarantine Control, a feature in Windows Server 2003. Network Access Quarantine Control relies on the creation of customized scripts and manual configuration of two tools (RQS.exe and RQC.exe) from the Windows Server 2003 Resource Kit Tools or included with Windows Server 2003 Service Pack 1 and later. Using Network Access Quarantine Control, administrators can create customized VPN connections for their users. These connections can check for required programs, and administrators can isolate a VPN connection until these checks have been performed. Network Access Quarantine Control is not part of NAP. It is compatible with VPN servers using NAP, although administrators might need to adjust some scripts. Administrators can use Network Access Quarantine Control and NAP simultaneously.

4. Dynamic Host Configuration Protocol (DHCP) address configurations

Answer: With DHCP enforcement, a computer must be compliant to obtain an unlimited access IPv4 address configuration from a DHCP server. For noncompliant computers, network access is limited by an IPv4 address configuration that allows access only to the restricted network. DHCP enforcement enforces health policy requirements every time a DHCP client attempts to lease or renew an IP address configuration. DHCP enforcement also actively monitors the health status of the NAP client and renews the IPv4 address configuration for access only to the restricted network if the client becomes noncompliant.
The components of DHCP enforcement consist of a DHCP ES that is part of the DHCP Server service in Windows Server 2008 R2 and a DHCP Quarantine EC in Windows 7, Windows Server 2008 R2, and Windows XP Service Pack 3.
Because DHCP enforcement relies on a limited IPv4 address configuration that can be overridden by a user with administrator-level access, it is the weakest form of limited network access in NAP.