REVIEW LESSON

MTA Course: 98-367 Security Fundamentals
Lesson name: Network Isolation 3.3
Topic: Understand network isolation (One 50-minute class period)
File name: SecurityFund_RL_3.3_B

Lesson Objective

3.3: Understand network isolation. *This objective may include, but is not limited to:* VLAN's, routing, honeypot, perimeter network, NAT, VPN, IPsec, Server and Domain Isolation.

Preparation Details

Instructor preparation activities

- Make copies of Student Activity SecurtyFund_SA_3.3_B

Resources, software, and additional files needed for this lesson

- SecurityFund_PPT_3.3_B
- SecurityFund_SA_3.3_B
- Hardware requirements:
  2 GB RAM
  3.0 GB available hard disk space
  2.0 Ghz+ CPU
- Software requirements on the host computer:
  Windows® XP / Windows Server® 2008 R2 / Windows 7
  Virtual PC 2007 / Virtual Server 2005 R2

Teaching Guide

Essential Vocabulary

Perimeter Network—a perimeter network (also known as DMZ, demilitarized zone, and screened subnet) is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet. perimeter network is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has access to equipment in the perimeter network, rather than any other part of the network.

honeypot—a security program designed to lure and distract a network attacker with decoy data. The honeypot appears to be a system that the intruder would like to crack but is in reality safely separated from the actual network. This allows network administrators to observe attackers and study their activities without the intruders knowing they are being monitored. Honeypot programs get their name from the "like a bear to honey" metaphor.

Internet Protocol Security (IPsec)—IPsec is an Internet protocol security standard that provides a general policy–based IP layer security mechanism that is ideal for providing host-by-host authentication. IPsec policies are defined as having security rules and settings that control the flow of inbound and outbound traffic on a host system. These policies are managed centrally in Active Directory using group policy objects (GPOs) for policy assignments to domain members. They provide the ability to help establish secure communications between domain members, which is the basis for this solution.

Network Address Translation (NAT)— The process of translating between private IP addresses used within an intranet or other private network and global Internet IP addresses. This approach makes it possible to use a large number of private IP addresses within the private network without depleting the limited number of available numeric global Internet IP addresses. Variations of NAT displaying similar functions include IP aliasing, IP masquerading, and Port Address Translation.

routing—the process of forwarding packets between networks from source to destination.

virtual LAN (VLAN)—a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

virtual private network (VPN)—virtual private network nodes on a public network such as the Internet communicate among themselves using encryption technology so that their messages are as safe from being intercepted and understood by unauthorized users as if the nodes were connected by private lines.

Lesson Sequence

Activating prior knowledge/lesson staging (Anticipatory Set: 10 minutes)

1. Student prompt (see PowerPoint® slide 3) Many risks are associated with VPNs because workstations connect to the network and measures need to be addressed to ensure that the risk is eliminated.
    1. What are these risks?
    2. How can you control access?
       On a sheet of paper, record your ideas.
2. Give students a few minutes to research and respond, allowing them to work until they have finished.
3. As time permits, call on a few students to report to the group with their responses.

Lesson activity (30 minutes)

1. Teacher Instruction
    - Use the included PowerPoint presentation to review VPNs.
2. Guided Practice
    - Using the Student Activity handout SecurityFund_SA_3.3_B complete the following:
      Download, install and view the "Server and Domain Isolation Demo" consisting of two demonstration scenarios:
      - Server and Domain Isolation Demo (Basic)
      - Server and Domain Isolation Demo (Advanced)

      The Basic demo shows just Domain Isolation and Server Isolation.
      The Advanced demo includes No Fallback Group Isolation, Boundary Group Isolation, and Encryption Group Isolation.

      The demonstrations make use of 5 non-persistent virtual machines running Windows Server 2008 R2 (evaluation copy), but two virtual machines (Cairo and Rome) are configured to use the "Luna" Windows XP Style user interface.

      Refer to the included SecurityFund_SA_3.3_B and SDI Script Steps for more details on each scenario, and step-by-step instructions.

Assessment/lesson reflection (10 minutes)

1. Students examine various analysis tools used for Intrusion Detection and Integrity Analysis listed on slide 12. On the same paper they used for the Anticipatory Set, they should list additional tools they locate on these or other sites.
   - Be sure to give ample time for students to record their findings.
   - If time allows, pick a few students to read their findings.
2. At the bottom of the page, tell students to write down any questions they have or any topics about which they would like more assistance.
3. After class, look through the student responses and follow up with any student requiring additional help.

Microsoft® resources and Web links

- **Microsoft Downloads: Server and Domain Isolation Demo**
  http://www.microsoft.com/downloads/details.aspx?FamilyID=13a0ab69-2113-482e-a6d1-911aff9e9e2d&displaylang=en
- **Port 25: Communication from the Open Source Community at Microsoft: Honeypots and User Mode Linux Part 2: Forensic Analysis**
  http://port25.technet.com/archive/2006/08/04/Honeypots-and-User-Mode-Linux-Part-2_3A00_--Forensic-Analysis.aspx
- **TechNet: Virtual Private Networking with Windows Server 2003 and Windows Server 2008: Overviews**
  http://technet.microsoft.com/en-us/network/bb545442.aspx