

REVIEW LESSON

MTA Course: 98-367 Security Fundamentals
Lesson name: Understanding Network Security 3.4
Topic: Understand protocol security
(One 50-minute class period)
File name: SecurityFund_RL_3.4

Lesson Objective

3.4: Understand protocol security. *This objective may include, but is not limited to:* protocol sniffing, tunneling, DNSSEC, network sniffing, common attack methods.

Instructor preparation activities

- Make copies of Student Activity SecurityFund_SA_3.4

Resources, software, and additional files needed for this lesson

- SecurityFund_PPT_3.4
- SecurityFund_SA_3.4
- SecurityFund_SA_3.4_Key

Teaching Guide**Essential Vocabulary**

sniffing—also called eavesdropping, is the act of monitoring network traffic for data, such as cleartext passwords or configuration information. With a simple packet sniffer, all plaintext traffic can be read easily. Also, lightweight hashing algorithms can be cracked and the payload that was thought to be safe can be deciphered.

identity spoofing (IP address spoofing)—spoofing occurs when the attacker determines and uses an IP address of a network, computer, or network component without being authorized to do so. A successful attack allows the attacker to operate as if the attacker is the entity normally identified by the IP address.

Internet protocol security (IPsec)—a framework of open standards for helping to ensure private, secure communications over Internet protocol (IP) networks through the use of cryptographic security services. IPsec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection. Because IPsec is integrated at the Internet layer (layer 3), it provides security for almost all protocols in the TCP/IP suite. Because IPsec is applied transparently to applications; there is also no need to configure separate security for each application that uses TCP/IP.

Domain name system (DNS)—a hierarchical, distributed database that contains mappings between names and other information, such as IP addresses. DNS allows users to locate resources on the network by converting friendly, human-readable names like `www.microsoft.com` to IP addresses that computers can connect to.

Domain name system security extensions (DNSSEC)— a suite of extensions that add security to the DNS protocol.

Lesson Sequence

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

1. Student prompt: On a sheet of paper, list common network attack methods that they are familiar with.
2. Give students a few minutes to 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 (40 minutes)

1. Teacher Instruction (20 minutes)
 - Use the included PowerPoint® slides (4 and 5) to review Configuring IIS IP Address and DNS Restrictions.
 - Show the procedures and give the students 5-10 minutes to “walk through” the steps on their own PC’s.
 - Finally, have each student share their findings with the whole group.
2. Guided Practice (20 minutes)
 - After viewing the PowerPoint presentation, students will complete the student activity worksheet.
 - If time allows, you may review all or part of the student activity `SecurityFund_3.4_SA` , discussing student responses to the questions.

Assessment/lesson reflection (10 minutes, slide 3)

1. On the same paper they used for the Anticipatory Set, tell students to summarize the IPsec goals and how they are met.
 - Be sure to give ample time for students to write their answers.
 - If time allows, pick a few students to read their answers.
2. At the bottom of the page, tell students to write 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 TechNet: Common Types of Network Attacks**
<http://technet.microsoft.com/en-us/library/cc959354.aspx>
- **Microsoft TechNet: Introduction to DNSSEC**
[http://technet.microsoft.com/en-us/library/ee649205\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee649205(WS.10).aspx)
- **Microsoft TechNet: Introducing IPsec**
<http://technet.microsoft.com/en-us/library/cc961424.aspx>