STUDENT ACTIVITY 2.1_A_KEY: INTERNET SECURITY

MTA Course: 98-367 Security Fundamentals
Lesson name: User Authentication 2.1_A
Topic: Understanding user authentication
File name: SecurityFund_SA_2.1_A_Key

Lesson Objective

2.1_A: Understand user authentication. *This objective may include but is not limited to*: multifactor; smart cards; RADIUS; public key infrastructure (PKI); understand the certificate chain; biometrics; Kerberos and time skew; using Run As to perform administrative tasks; password reset procedures.

Resources, software, and additional files needed for this lesson

Internet access is desired.

Directions to the student

Summarize the key points in a brief discussion of each of the following concepts:

1. Strong passwords *http://technet.microsoft.com/en-us/library/cc756109(WS.10).aspx*
   A weak password:

   - Is no password at all.
   - Contains your user name, real name, or company name.
   - Contains a complete dictionary word. For example, *Password* is a weak password.

   A strong password:

   - Is at least seven characters long.
   - Does not contain your user name, real name, or company name.
   - Does not contain a complete dictionary word.
   - Is significantly different from previous passwords. Passwords that increment (*Password1*, *Password2*, *Password3* ...) are not strong.

2. Single sign-on *http://technet.microsoft.com/en-us/library/cc262235(office.12).aspx*
   In Microsoft® Office SharePoint® Server 2007, single sign-on (SSO) authentication enables users to access multiple system resources without having to provide authentication credentials more than once. Office SharePoint Server 2007 implements SSO authentication by including a Windows® service and a secure credentials database.

3. Dumpster diving *http://technet.microsoft.com/en-us/library/cc875841.aspx*
   Illicit waste analysis—*dumpster diving*, as it is commonly termed—is a valuable activity for hackers. Business paper waste can contain information that is of immediate benefit to a hacker, such as discarded account numbers and user IDs, or can serve as background information, for example telephone lists and organization charts. This latter type of information is invaluable to a social engineering hacker, because it makes him or her appear credible when launching an attack.

4. Spoofing *http://technet.microsoft.com/en-us/library/aa997157(EXCHG.65).aspx*
   Common technique spammers use is to configure the **From** line in an e-mail message to hide the sender's identity. Although SMTP does not require verification of a sender's identity, Exchange 2003 provides the following functionality to help minimize address spoofing*: http://technet.microsoft.com/en-us/library/aa997157(EXCHG.65).aspx*

5. Social engineering *http://technet.microsoft.com/en-us/library/cc875841.aspx*
   To attack your organization, social engineering hackers exploit the credulity, laziness, good manners, or even enthusiasm of your staff. Therefore it is difficult to defend against a socially engineered attack, because the targets may not realize that they have been duped, or may prefer not to admit it to other people. The goals of a social engineering hacker—someone who tries to gain unauthorized access to your computer systems—are similar to those of any other hacker: they want your company's money, information, or IT resources.

6. Phishing *http://technet.microsoft.com/en-us/library/cc512622.aspx*
   Phishing is a way to trick computer users into revealing personal or financial information through a website. A common online phishing scam starts with an e-mail message that looks like an official notice from a trusted source such as a bank, credit card company, or reputable online merchant. Recipients of the message are directed to a fraudulent website where they are asked to provide personal information, such as an account number or password. This information is then usually used to commit identity theft.

7. Pharming *http://social.technet.microsoft.com/Forums/en-US/exchangesvrantivirusandantispam/thread/8ecccc46-a80c-44a2-b3cd-961cc30f0efb*
   Pharming (pronounced "farming") is another form of online fraud, very similar to its cousin phishing. Pharmers rely upon the same bogus websites and theft of confidential information to perpetrate online scams, but are more difficult to detect in many ways because they are not reliant upon the victim accepting a "bait" message. Instead of relying completely on users clicking on an enticing link in fake email messages, pharming instead redirects victims to the bogus website even if they type the right Web address of their bank or other online service into their Web browser.