Microsoft
Technology
Associate

MICROSOFT TECHNOLOGY ASSOCIATE

Student Study Guide

EXAM 98-367
Security Fundamentals

Microsoft

Preparing for MTA Certification

MICROSOFT TECHNOLOGY ASSOCIATE (MTA)
STUDENT STUDY GUIDE FOR IT PROS

98-367 Security Fundamentals

Authors

Michael Teske (Windows Server Administration and Security). Michael has been teaching in the Network Specialist Program for 10 years at Northeast Wisconsin Technical College and has been involved as an engineer for 15 years. He has a passion for both teaching and technology and loves helping people find happiness in a career. Mike believes that learning technology should be fun but recognizes that the networking field is continually changing and can challenge even the brightest students. Mike also works as an independent consultant for several small businesses in northeast Wisconsin and enjoys bringing that real-world experience to the classroom on a daily basis. Michael has become known as "the Microsoft Guy" on campus. Michael's goal is to continue to teach network technology with the same enthusiasm and passion for many years to come and to help his students find the same joy and passion he has found in an amazing industry and career. Mike is the author of the Windows Server Exam Review Kit in the MTA Exam Review Kit series.

Patricia Phillips (Lead Author and Project Manager). Patricia taught computer science for 20 years in Janesville, Wisconsin. She served on Microsoft's National K-12 Faculty Advisory Board and edited the Microsoft MainFunction website for technology teachers for two years. For the past five years she has worked with Microsoft in a variety of roles related to K-12 curriculum development and pilot programs including Expression Studio web design and XNA game development. In her role as an author and editor, Patricia wrote several articles and a student workbook on topics including computer science, web design, and computational thinking. She is currently the editor of the Computer Science Teachers Association newsletter, the Voice.

Contents

Introduction

MTA validates building-block technology concepts and helps students explore, discover and pursue successful careers in Information Technology (IT) in an exciting and rewarding way! As the first step in the Microsoft Technology Certification Series, this new, entry-level certification provides students with confidence, credibility, and differentiation.

Explore IT career options without committing a lot of time and resources MTA exams validate the core technology knowledge that is in demand today by businesses around the world. Whether you want to explore becoming a network administrator, software engineer, web developer, or database analyst, MTA gets you started on the right path.

Prepare to compete A little investment in IT can go a long way in today's job market. Becoming MTA certified helps you build a solid foundation to prepare for intermediate technology studies and for Microsoft Certified Technology Specialist (MCTS) certifications. It can also help you compete on college admissions and jumpstart your IT career planning!

Empower yourself As the first step toward becoming an MCTS, MTA shows your commitment to technology while connecting you with a community of more than five million Microsoft Certified Professionals. Learn from them and show them what you know by becoming MTA certified!

This MTA Student Study Guide serves as a study tool to help students prepare for their MTA certification exam. Students are challenged with real-life situations for each of the major topics covered in the exam. Although successful completion of the study guide exercises does not guarantee that you will pass your MTA exam, it is an excellent way to gauge your readiness to take the exam and build confidence that you know your stuff on exam day.

I wish you all the best as you prepare for a successful career in technology!

Victoria Pohto

Victoria Pohto
MTA Product Marketing Manager

Career Planning

Most IT solutions or infrastructure built on Microsoft technologies require proficiency with one or all of the following products, often referred to as "The Microsoft Stack."

- Microsoft Windows® Server® as the data center or development platform
- Microsoft SQL Server® as the data and business intelligence (BI) platform
- Microsoft Visual Studio® as the suite of application life-cycle management tools

MTA is the starting point of Microsoft technology certifications, providing aspiring technologists with the fundamental knowledge essential to succeed with continued studies and a successful career with technology.

Preparing for and becoming MTA certified helps you explore a variety of career paths in technology without investing a lot of time and money in a specialized career path. When you find a path that is right for you, Microsoft learning products and certification can help you prepare and guide your longer-term career planning.

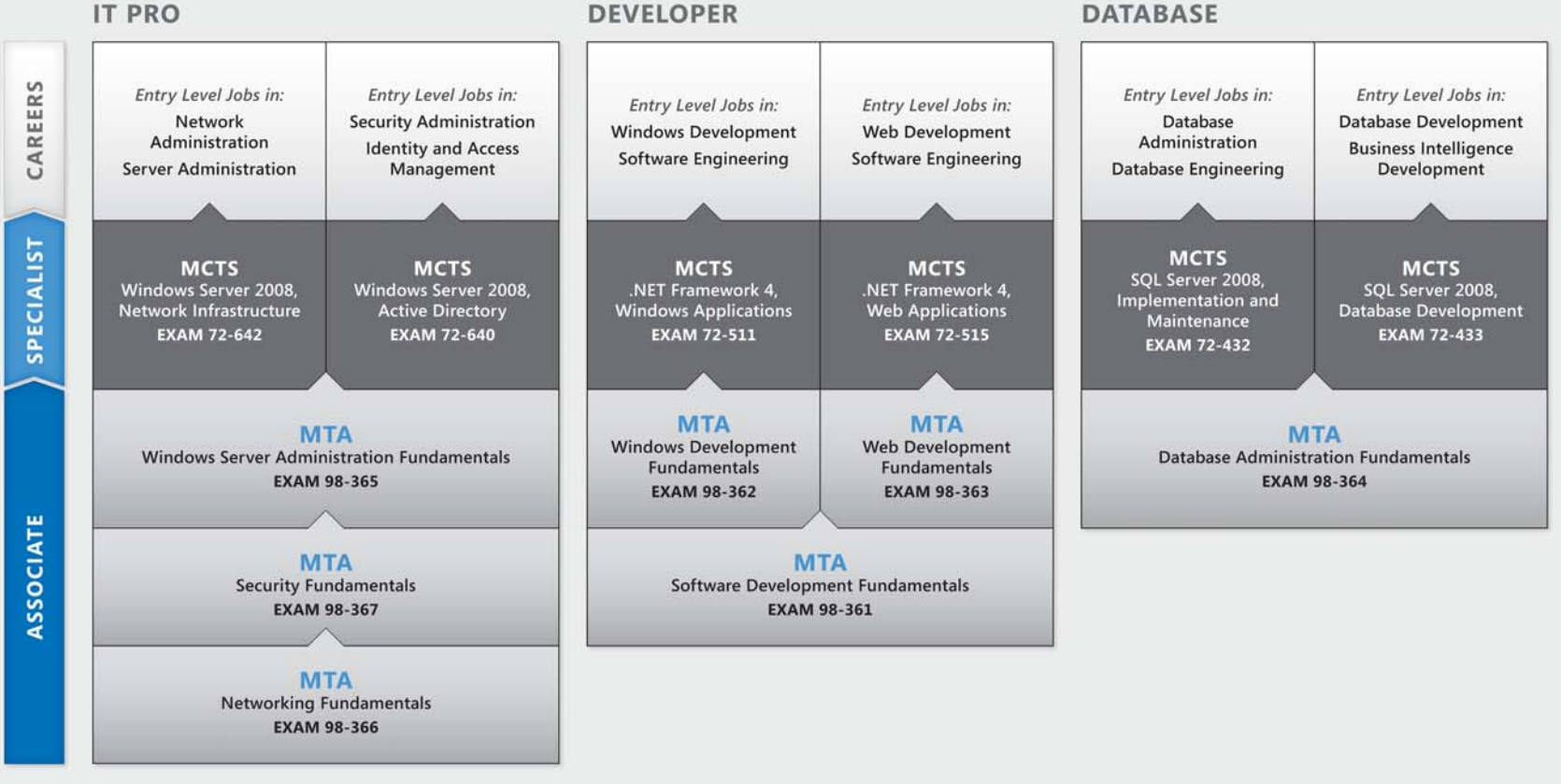
If you already know that you want to start building a career in technology, MTA preparation and certification is the recommended entry point. Becoming MTA certified shows that you have a firm working knowledge of the fundamental IT concepts critical for success with intermediate learning and certifications such as Microsoft Certified Technology Specialist (MCTS). Moreover, Microsoft certifications demonstrate an individual's commitment of self-investment and confidence to take his or her knowledge and skills to the next level with an industry-recognized credential.

MTA is not a "career certification," meaning that employers recognize you as "job ready," but it is the first step toward that career goal and can help differentiate you for an internship or to college admissions committees. As you prepare for your first job focusing on technology, be sure that you are equipped with an MCTS credential—the intermediate level certification that validates Microsoft product and technology skills.

The MTA Certification path on the next page shows you the MTA exams that are recommended prior to taking on some of Microsoft's intermediate technology certification, MCTS.

Microsoft Technology Associate Certification Paths

MTA is the recommended first step in the Microsoft IT Certification Program, and does not require pre-requisite exams. MTA certifications are not a pre-requisite for MCTS exams. *One MTA exam = One certification.*



For full Microsoft Certification roadmaps, visit **http://www.microsoft.com/learning/certification**

Exploring Job Roles

Choosing a career path is a big decision and it's not always easy, but you're not alone! Microsoft created a career site to help students understand the options and possibilities of pursuing a career in IT. The site also connects you with learning resources, student techie communities, and much more to help you prepare for a career in technology.

To chart your career with Microsoft technology, visit *www.microsoft.com/learning/career/en/us/career-org-charts.aspx*.

Database Administrator

As a database administrator, you are in charge of important databases that span multiple platforms and environments. You are a strong team player who thrives in a fast-paced environment. You build complex, highly scalable databases that meet business needs and security requirements. You are an expert in optimizing, maintaining, and troubleshooting databases, but also in designing archival, data distribution, and high-availability solutions.

Server Administrator

As a server administrator, you are in charge of implementing and managing some of the most important technology in your organization—the servers. You use extensive monitoring and profiling tools to manage the network and tune systems so they perform at optimal levels. You are an expert in Active Directory®, and you have an in-depth understanding of network protocols, and file and directory security.

Computer Support Technician

Consider starting your IT career by becoming a consumer support technician. You don't need any formal work experience, but a company might require that you know how to install, administer, and troubleshoot operating systems in a home network environment that has desktop computers, laptops, and printers. As a consumer support technician, you'll also handle network, virus, malicious software, and hardware support issues. You'll typically find this position in small to medium-sized organizations.

Exploring Job Roles

Web Developer

As a web developer, you are an expert in using the dynamic programming tools and languages that fuel the web. You might work independently or be part of a team that builds and integrates interactive web sites, applications, and services for both internal and public sites. Your role is to make it work, which means developing web applications and testing them on various browsers, enhancing and modifying them as necessary to ensure the best experience for the user. As a web developer, you might also architect websites, design data-driven applications, and find efficient client-server solutions. You must have an in-depth understanding of the software development life cycle and be able to communicate project status, issues, and resolutions.

Windows Developer

As a Windows client developer, knowing how to optimize Windows code and track bugs is a given. But you also know how to use Microsoft Visual Studio® and the Microsoft .NET framework to design, develop, test, and deploy Windows-based applications that run on both corporate servers and desktop computers. Your key talents include understanding multiple Windows application models and n-tier applications, and knowing how to work with object-oriented programming, algorithms, data structures, and multithreading. Windows Developers have an in-depth understanding of software engineering principles, software life cycles, and security principles.

Additional Online Resources for New Developers:

http://msdn.microsoft.com/beginner

http://msdn.microsoft.com/rampup

Imagine Cup

imagine cup™ by Microsoft®

The Imagine Cup is the world's premier student technology competition where students from around the world can learn new skills, make new friends, and change the world. Competitions include Software Design, Embedded Development, Game Design, Digital Media and Windows Phone 7. The brightest young minds harness the power of technology to take on the world's toughest problems.

www.imaginecup.com

Value of Certification

Technology plays a role in virtually everything we do. In the 20-plus years since Microsoft has been certifying people on its products and technologies, millions of people have gained the knowledge, expertise, and credentials to enhance their careers, optimize business solutions, and create innovation within just about every business and social sector imaginable. Today's Information Technology (IT) hiring managers are more often using professional credentials, such as Microsoft certification, to identify properly skilled IT candidates. Certification becomes a way to easily differentiate qualified candidates in a sea of resumes.

The job outlook for IT professionals, as reported in a study prepared by the U.S. Department of Labor's Bureau of Labor Statistics (BLS), is positive! The BLS indicates an increase that will be "faster than the average for all occupations through 2014" for Computer Support Specialists, Systems Engineers, Database Administrators, and Computer Software Engineers. One significant message resulting from this study is that information and communications technology (ICT) skills are the entry ticket to the job market, regardless of the country, industry, or job function. Information Technology is clearly an area worth investing time, resources, and education in – and technology certification is a key part of the education process, validating product and technology expertise as a result of their learning experiences.

Microsoft IT Certifications provide objective validation of the ability to perform critical IT functions successfully for worldwide IT professionals, developers, and information workers. Microsoft certifications represent a rich and varied spectrum of knowledge, job roles, and responsibilities. Further, earning a specific certification provides objective validation of the candidate's ability to perform critical IT functions successfully. Embraced by industry professionals worldwide, Microsoft certification remains one of the most effective ways to help reach long-term career goals.

MTA 98-367

SECURITY FUNDAMENTALS

1

Understanding Security Layers

IN THIS CHAPTER

- 1.1 Understand core security principles
- 1.2 Understand physical security
- 1.3 Understand Internet security
- 1.4 Understand wireless security

Understand core security principles

SCENARIO: Blue Yonder Airlines has expanded over the past 18 months and has recently gone through a security audit to ensure that the technical system is secure. Several areas needing improvement were identified. The CIO has asked Toni Poe, Blue Yonder Airlines' security consultant, to provide some essential security training for the front-line staff. The goal is to minimize the risk for potential security threats by educating staff members in the area of social engineering, as well as some basic security principles.

Toni has assessed the security rights of each staff member related to computer access and perimeter access. Toni notes that some staff members have elevated privileges to access Blue Yonder Airlines intranet site. He also knows that it is important to stress the Confidentiality, Integrity, and Availability triangle in his training.

1. **Toni plans to implement the principle of least privilege. How will this affect the staff members?**
   - **a.** staff members will maintain their current access to all resources
   - **b.** staff members will be granted the smallest set of privileges to the resources
   - **c.** staff members will have to log on as administrator to have access to their resources
2. **What would be an example of providing availability as it relates to security training?**
   - **a.** making sure all the workstations are turned on
   - **b.** ensuring that all staff members have perfect attendance for work
   - **c.** protecting against a Distributed Denial of Services attack
3. **What is an example of social engineering?**
   - **a.** calling a staff member while pretending to be someone else to gain information that can provide access to sensitive information
   - **b.** developing social awareness of security threats within an organization
   - **c.** building a social networking website

hint

Social engineering is not related to social networking. The ultimate goal of a hacker is to obtain as much information by exploiting the human side of security.

Answers

1. Implementing the principle of least privilege means that:
   b. staff members will be granted the smallest set of privileges to the resources
2. Providing availability as it relates to security training means:
   c. protecting against a Distributed Denial of Services attack
3. An example of social engineering could include:
   a. calling a staff member while pretending to be someone else to gain information that can provide access to sensitive information

Essential details

- The **CIA (confidentiality, Integrity and Availability) Triangle** is the concept of ensuring the prevention of unauthorized disclosure of information, the erroneous modification of information, and the prevention of unauthorized withholding of information or resources.
- The **principle of least privilege** requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks.
- **Social engineering** is any type of behavior that can inadvertently or deliberately aid an attacker in gaining access to a user's password or other sensitive information.

FAST TRACK HELP

- **http://technet.microsoft.com/en-us/library/cc875841.aspx**

Understand physical security

SCENARIO: Erin Hagens has just been promoted to security officer for Woodgrove Bank. This position carries huge responsibility for the safety of the customer's money and information, not to mention the bank's reputation. This role necessitates that she keep current on a long list of requirements for securing Woodgrove Bank. A banking industry regulatory agency has informed Erin that the bank will undergo a security audit to ensure that they are in compliance with industry regulations and standards. Erin understands the request and must do her due diligence to provide whatever information the regulators need as they target potential security holes. Her biggest concern is the physical security of the bank's systems.

1. **What can Erin do to ensure physical security of the bank desktop computers?**
   - **a.** disable the use of floppy drives or USB drives by using group policies
   - **b.** have a guard posted in every cubical area
   - **c.** obtain locking mechanisms for each desktop so they cannot be carried away
2. **Erin has a concern that people can authenticate to the servers in the data center. What can she do to prevent normal users from logging onto those systems?**
   - **a.** make sure the server is locked up
   - **b.** remove the keyboards from all servers
   - **c.** create a group policy that applies to the servers to Deny Log on Locally for all non-administrative users
3. **What can Erin do to prevent the use of key loggers in the bank?**
   - **a.** ensure that the terminals are locked and do a periodic inspection of the ports on the systems
   - **b.** nothing—Erin cannot control what gets plugged into her computers
   - **c.** convert all computers to touch screen monitors

hint

It may not be financially feasible or physically possible for the bank to convert all systems to touch screens.

Answers

1. To ensure physical security of desktop computers, Erin can:
   a. **disable the use of floppy drives or USB drives by using group policies.** Most computers do have a mechanism to attach a locking device to the desktops, however, disabling USB and floppy drives disables a larger threat.
2. To prevent normal users from logging onto the systems, Erin can:
   c. **create a group policy that applies to the servers to Deny Log on Locally for all non-administrative users.** A bigger issue is people are in the data center with physical access. However, normal users should not have the ability to log on locally.
3. To prevent the use of key loggers in the bank, Erin will have to:
   a. **ensure that the terminals are locked and do a periodic inspection of the ports on the systems**

Essential details

- **Keystroke logging** (often called **key logging**) is the process of recording the keys typed on a keyboard, typically without the users' knowledge.
- **Access controls** are the mechanisms for limiting access to certain items of information or to certain controls based on users' identities and their membership in various predefined security groups..

FAST TRACK HELP

- **http://technet.microsoft.com/en-us/library/bb457125.aspx**
- **http://www.microsoft.com/smallbusiness/security.aspx**

Understand Internet security

SCENARIO: Terry Adams is the desktop administrator for Tailspin Toys. To stay current with the latest Internet technologies, Tailspin Toys has decided to upgrade their browsers to Internet Explorer (IE) 8. Terry wants to make sure that they utilize many of the security features built into the browser while still maintaining functionality within the company's intranet. Terry also would like to educate his users to be good "Internet citizens" and practice safe web surfing. He knows that the first line of defense in Internet security is an informed and skilled user.

1. **Terry wants to configure the Internet zone feature in IE 8 in such a way that users can easily access content on the local intranet while still maintaining a high level of security. What should he do?**
   - **a.** create a perimeter network and make sure the intranet site is located there and have a single PC in each department designated the Intranet Browsing PC (IBPC)
   - **b.** go into the Internet Options, choose Security and add their intranet site to the list of Local Intranet Sites
   - **c.** print the content of the intranet site weekly and distribute it through interoffice mail
2. **What can Terry tell his staff to look for to be assured that they are on a secured website?**
   - **a.** a padlock in the lower right corner of the browser and **https://** in the address bar
   - **b.** the contact information on the site
   - **c.** they should not be browsing secure sites because you can't trust any site
3. **What is the security level set to in the Restricted Sites zone?**
   - **a.** low; the sites are restricted and therefore not a concern
   - **b.** high; disables most features, has the maximum safeguards, and protects against harmful content
   - **c.** medium; a nice balance between too restrictive and too open

hint

The default level in the restricted sites zone is set to High.

Answers

1. To configure the Internet zone feature in IE 8 and enable users to easily browse the local intranet, Terry should:
   b. go into the Internet Options, choose Security and add their intranet site to the list of Local Intranet Sites
2. To be sure that they are on a secure site, staff members can look for a:
   a. a padlock in the lower right corner of the browser and https:// in the address bar. This does not guarantee that the site is secure. However, it is a start.
3. The security level in the Restricted Sites zone is:
   b. high; disables most features, has the maximum safeguards, and protects against harmful content

Essential details

- An **Internet zone** contains websites that are not on your computer or on your local intranet, or that are not already assigned to another zone. The default security level is Medium.
- A **secure site** is a website with the capability of providing secure transactions, ensuring that credit card numbers and other personal information will not be accessible to unauthorized parties..

FAST TRACK HELP

- **http://support.microsoft.com/kb/174360**

Understand wireless security

SCENARIO: Pilar Ackerman is the systems administrator for Fourth Coffee—a national chain of very popular and profitable coffee cafés. Competition in the coffee café business is fierce! To maintain a competitive edge, Fourth Coffee plans to add open, high-speed, wireless access for their customers and secured wireless for employees at all 200 Fourth Coffee locations. Pilar is faced with several security concerns and must ensure that their business traffic is secured. In addition to that, he is under pressure to make this new feature a winning strategy.

1. **What is the most secure protocol that Pilar can implement to ensure that the business-related traffic is encrypted?**
   - **a.** Wired Equivalent Privacy (WEP)
   - **b.** WiFi Protected Access (WPA) 2
   - **c.** Extensible Authentication Protocol (EAP)
2. **Aside from encrypting the business wireless traffic, what else can Pilar do to add another level of security?**
   - **a.** implement access point isolation and hide the Service Set Identifier (SSID)
   - **b.** turn off the business access points when customers come in
   - **c.** enable MAC filtering
3. **Pilar would like his employees to be independent in troubleshooting their own wireless connections before contacting him. What basic troubleshooting step that he can instruct them to do?**
   - **a.** reboot their computers
   - **b.** power cycle the wireless access points
   - **c.** right-click the network icon in the system tray and select Troubleshoot Problems

hint

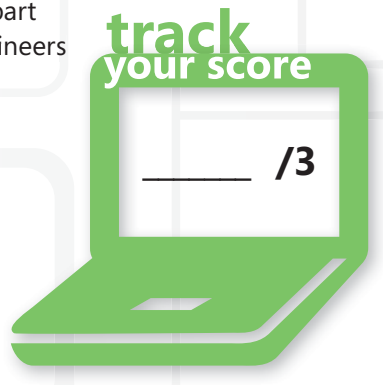
Power cycling the access point would disconnect other users from the network.

Answers

1. The most secure protocol that Pilar can implement to ensure that the business-related traffic is encrypted is:
   b. **WiFi Protected Access (WPA) 2.** EAP is a feature of security that handles authentication and WPA is more secure than WEP.
2. Pilar can add another level of security by:
   a. **implementing access point isolation and hiding the Service Set Identifier (SSID).** MAC filtering is an option; however, MAC addresses can be "faked" or "spoofed." Hiding the SSID is a simple security measure that can be implemented.
3. Pilar can instruct the staff to troubleshoot by:
   c. **right-click the network icon in the system tray and selecting Troubleshoot Problems**

Essential details

- A **Service set identifier (SSID)** is a 32-character, unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the communicating stations on a wireless LAN.
- **Wi-Fi protected access (WPA)** is a Wi-Fi standard that was designed to improve upon the security features of WEP.
- **Wired equivalent privacy (WEP)** is an encryption algorithm system included as part of the 802.11 standard, developed by the Institute of Electrical and Electronics Engineers as a security measure to protect wireless LANs from casual eavesdropping.



FAST TRACK HELP

- **http://technet.microsoft.com/en-us/magazine/2005.11.securitywatch.aspx**
- **http://windows.microsoft.com/en-US/windows-vista/What-are-the-different-wireless-network-security-methods**
- **http://www.windowsnetworking.com/articles_tutorials/Securing-Wireless-Network-Traffic-Part1.html**

2

Understanding Operating System Security

IN THIS CHAPTER

- 2.1A Understand user authentication
- 2.1B Understand user authentication
- 2.2 Understand permissions
- 2.3 Understand password policies
- 2.4 Understand audit policies
- 2.5A Understand encryption
- 2.5B Understand encryption
- 2.6 Understand malware

Understand user authentication

SCENARIO: Jim Hance is a security administrator for Coho Winery. A variety of security threats have occurred over the past few months and management is more than a little concerned. They cannot afford to have the system jeopardized; their customers expect a reliable and secure site. Jim is reviewing the security policies for Coho Winery to determine where the company may need stronger policies or at least to update the existing policies and security measures. His first task is determining the company's strengths as it relates to user authentication.

1. **Jim knows that stronger passwords are a critical element in the security plan. What characteristics make up a strong password?**
   - **a.** contains 7+ characters; does not contain the user name, real name, or company name
   - **b.** contains sequential numbers embedded within the company name
   - **c.** contains the user's last name and email address
2. **What protocol can be used to secure workstation and computer authentication across the network?**
   - **a.** TCP/IP
   - **b.** Kerberos
   - **c.** Lightweight Directory Access Protocol
3. **What strategy can Jim implement to reduce the number of times a user would have to authenticate to access a particular resource?**
   - **a.** two-factor authentication
   - **b.** digital certificates
   - **c.** Single Sign-on (SSO)

hint

Reducing the number of times a user has to authenticate can reduce the possibilities of his or her credentials being captured.

Answers

1. A strong password:
   a. **contains 7+ characters; does not contain the user name, real name, or company name**
2. To secure workstation and computer authentication across the network, Jim can use:
   b. **Kerberos**
3. To reduce the number of times a user would have to authenticate to access a particular resource, Jim can implement:
   c. **Single Sign-on (SSO)**

Essential details

- **Authentication** is the process of obtaining identification credentials such as name and password from a user and validating those credentials against some authority.
- **Kerberos** authenticates the identity of users attempting to log on to a network and encrypts their communications through secret-key cryptography.
- **Lightweight directory access protocol (LDAP)** is a network protocol designed to work on TCP/IP stacks to extract information from a hierarchical directory such as X.500.
- **Remote authentication dial-in user service (RADIUS)** is an Internet protocol in which an authentication server provides authorization and authentication information to a network server to which a user is attempting to link.

FAST TRACK HELP

- **http://www.microsoft.com/windowsserver2008/en/us/ad-main.asp**
- **http://web.mit.edu/Kerberos/#what_is**
- **http://technet.microsoft.com/en-us/library/bb463152.aspx**

Understand user authentication

SCENARIO: The Graphic Design Institute (GDI) has more than 30,000 students. The security of the students' personal information, including financial data, address, family contacts, special health needs, and grades, is the top priority of the network administrative team. However, over the past few months student data has been compromised on several occasions. Personal data has shown up on a social networking site, much to the embarrassment of the network team. GDI officers have asked the network administrator, Todd Rowe, to implement stronger authentication measures for the students, as well as eliminate IT staff from logging on with elevated privileges. Todd has several options, but is aware of the need to keep the processes fairly easy for the helpdesk staff.

1. **Todd wants to implement two-factor authentications. What can he use?**
   - **a.** smart card and user password
   - **b.** two passwords
   - **c.** two user IDs with two passwords
2. **What service can the GDI staff use instead of signing in with elevate privileges?**
   - **a.** Remote Desktop
   - **b.** Secondary Logon-Run As
   - **c.** User Manager for Domains
3. **What is a disadvantage of using biometric identification?**
   - **a.** the user must have hands
   - **b.** cost is prohibitive for many organizations
   - **c.** a retina scan can be faked

hint

Biometric identification is extremely secure; however, the devices to support biometrics are cost-prohibitive.

Answers

1. To implement two-factor authentications, Todd can use:
   a. **smart card and user password**
2. Instead of signing in with elevated privileges, the staff can use:
   b. **Secondary Logon-Run As**
3. A disadvantage of biometric identification is:
   b. **cost is prohibitive for many organizations**

Essential details

- A **certificate** is an electronic credential that authenticates a user on the Internet and intranets.
- **Public key infrastructure (PKI)** is an asymmetric scheme that uses a pair of keys for encryption: the public key encrypts data, and a corresponding secret key decrypts it.
- The **Run As** command allows a user to run specific tools and programs with different permissions than the user's current logon provides.
- Steps to change your password:
  - Press <control><alt><delete> and select Change Password
- Steps to use Secondary Logon or Run As. . .
  - Right-click the application icon and select Run As Administrator

FAST TRACK HELP

- **http://technet.microsoft.com/en-us/library/cc782756(WS.10).aspx**
- **http://technet.microsoft.com/en-us/library/cc756862(WS.10).aspx**
- **http://technet.microsoft.com/en-us/library/cc261673(office.12).aspx**

Understand permissions

SCENARIO: Fabrikam, Inc. has recently under gone a basic reorganization and a variety of corporate changes. Shawn Richardson is the network administrator at Fabrikam and has been assigned the task of aligning the company servers with the new organizational reality. As a first step, Shawn has completed a security audit of the company's Microsoft® Windows Server® 2008 R2 file servers and has determined that folder and share security needs to be revised based on corporate reorganization. Shawn must present his plan to management and give directions to his team members to complete the project.

1. **Shawn has noticed that some shares on the file system are not secured. What is the default permission setting when a share is created?**
   - **a.** everyone with Read permission
   - **b.** administrators with the Full Control permission
   - **c.** everybody with the Full Control permission
2. **Why should Shawn enforce User Account Control (UAC) across the domain?**
   - **a.** so that he can control the user accounts
   - **b.** to help prevent unauthorized changes to computers on the domain
   - **c.** to allow the users to authenticate with the administrator password to perform an administrative task
3. **What feature (also available with Active Directory objects) will make Shawn's job easier when reassigning permissions by not having to assign permissions to every parent and child folder?**
   - **a.** batch files
   - **b.** inheritance
   - **c.** staff people

hint

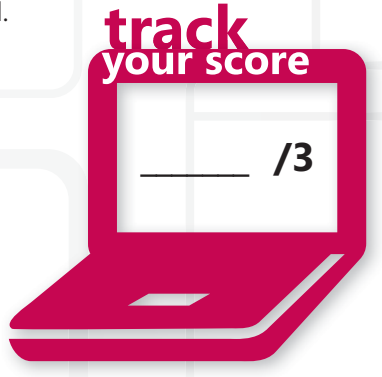
Inheritance allows the propagation for rights or permissions from a parent object to a child object. This feature can be blocked or removed.

Answers

1. When a share is created, the default permission is:
   a. **everyone with Read permission**
2. Shawn should enforce User Account Control (UAC) across the domain because:
   b. **it will help prevent unauthorized changes to computers on the domain**
3. Shawn's job can be made easier when reassigning permissions by using:
   b. **inheritance**

Essential details

- **Permissions** include Full control, Modify, Read & Execute, List folder Contents, Read, and Write and can be applied to both folder and file objects. Permissions can also be applied to Active Directory objects.
- **Inheritance** is the concept of permissions that are propagated to an object from a parent object. Inheritance is found in both file system permissions and Active Directory permissions. It does not apply to share permissions.
- **New Technology File System (NTFS), FAT, and FAT32.** The primary difference between NTFS and FAT file systems is the ability apply security to the file system. You can grant or deny various permissions on NTFS. NTFS also supports the ability to encrypt data.
- **Share and NTFS permissions** are applied based on how the resource is accessed. Share permissions are effective when the resource is being accessed through the network whereas NTFS permissions are effective all the time. When share and NTFS permissions are applying to the same resource, the most restrictive permission wins.



FAST TRACK HELP

- **http://technet.microsoft.com/en-us/library/cc730772.aspx**
- **http://technet.microsoft.com/en-us/library/cc771375.aspx**
- **http://technet.microsoft.com/en-us/library/cc770906(WS.10).aspx**

Understand password policies

SCENARIO: Jay Hamlin has been given the unenviable task of enforcing stronger password policies for Wingtip Toys. He understands the need for complex passwords of a minimum length, but is having a difficult time making the staff understand how the security of the entire Wingtip Toys organization can depend upon these couple requirements along with a few more that he plans to put into place. He must also determine how many times a user can attempt to log in before his or her account is locked out, how often users must change passwords, and how often users can reuse a favorite password.

His plan for a Password Complexity Policy includes the following criteria for passwords:

- Cannot contain the user's login name
- Must be at least 6 characters or greater
- Must contain three of the following four characters: upper case, lower case, number, and special character

1. **What dilemma is Jay facing if he makes his password requirements too difficult?**
   - **a.** a complex password can be hard to guess and difficult to remember
   - **b.** Jay will no longer have friends at work
   - **c.** users will not use the passwords
2. **What does the policy of maximum password age mean?**
   - **a.** determines how old the user must be to create a password
   - **b.** refers to the duration before a password has to be changed
   - **c.** refers to how old the password must be before the user is allowed to change it
3. **What happens when you set the value of Enforce Password History to 10?**
   - **a.** the user has 10 attempts to validate his or her password
   - **b.** the password must be used for at least 10 days before it can be changed
   - **c.** the system remembers the last 10 passwords and will not allow the user to reuse any of the previous 10

hint

Password history prevents users from reusing their passwords.

Answers

1. The dilemma Jay faces with difficult password requirements is that:
   a. **a complex password can be hard to guess and difficult to remember**
2. Maximum password age:
   b. **refers to the duration before a password has to be changed**
3. When you set the value of Enforce Password History to 10:
   c. **the system remembers the last 10 passwords and will not allow the user to reuse any of the previous 10**

Essential details

- **Account lockout** is a security feature in Windows that locks a user account if a number of failed logon attempts occur within a specified amount of time, based on security policy lockout settings.
- A **password attack** is an attack on a computer or network in which a password is stolen and decrypted or is revealed by a password dictionary program.
- **Password sniffing** is a technique employed by hackers to capture passwords by intercepting data packets and searching them for passwords.
- Microsoft Windows Server 2008 allows for fine-grained password policies, which allows for more flexible password policy assignment throughout an organization within Active Directory®.

FAST TRACK HELP

- **http://technet.microsoft.com/en-us/library/cc784090(WS.10).aspx**
- **http://technet.microsoft.com/en-us/library/cc875814.asp**

Understand audit policies

SCENARIO: The network for Margie's Travel must be very secure. The files contain customer information including credit card numbers, birthdates, and addresses, as well as photocopies of passports. Identity theft would be a real possibility if the system was hacked into. Obviously, this is not an acceptable risk for Margie's Travel.

Arlene Huff is the systems administrator for Margie's Travel. The company has asked her to track who attempts to log into the system and at what times of the day the attempts occur. They also have asked her to create a system to track when confidential files are opened and by whom. Arlene gladly took on this task and did not raise a huff.

1. **Arlene wants to log when someone fails to log into the system as administrator, but why would she want to log when they are successful also?**
   - **a.** to determine if and when someone is authenticating successfully with elevated privileges
   - **b.** to make sure they are getting in without any problems
   - **c.** to monitor drive space on the computer
2. **Where are file audit events written when auditing is enabled?**
   - **a.** audit event log
   - **b.** pfirewall.log
   - **c.** security event log
3. **Why is it important to properly secure audit logs?**
   - **a.** so that potential hackers cannot delete the event logs to cover their tracks
   - **b.** it's not important, no one looks at audit logs
   - **c.** so only authorized personnel can view the log files

hint

Skilled computer hackers will modify the audit logs when they are finished obtaining information so that it will appear as though they were never there.

Answers

1. Arlene wants to log when someone successfully logs into the system as well as when they fail:
   a. **to determine if and when someone is authenticating successfully with elevated privileges.** If someone failed four times and was then successful the fifth time it could indicate hacker activity.
2. Enabled file auditing events are written in the:
   c. **security event log**
3. It important to properly secure audit logs
   a. **so that potential hackers cannot delete the event logs to cover their tracks**

Essential details

- **Auditing** is the process an operating system uses to detect and record security-related events, such as an attempt to create, access, or delete objects such as files and directories.
- An **audit policy** is a policy that determines the security events to be reported to the network administrator.
- The **security log**, which can be generated by a firewall or other security device, lists events that could affect security, such as access attempts or commands, and the names of the users involved.

FAST TRACK HELP

- **http://technet.microsoft.com/en-us/library/dd408940(WS.10).aspx**
- **http://technet.microsoft.com/en-us/library/dd349800(WS.10).aspx**

Understand encryption

SCENARIO: Adventure Works has recently expanded its mobile sales force. The management team has recently come to recognize the unique security considerations associated with hundreds of laptop computers simultaneously located in hundreds of unsecure locations.

David Johnson is the network administrator in charge of the Adventure Works mobile sales force. He has recently come under fire from the management team regarding the sensitive data that could potentially fall into the competition's hands if any of the laptop computers were to be stolen or misplaced. They must have a solution that can ensure the confidentiality of data on the mobile stations that are all running Windows® 7 Enterprise—and they need it soon!

1. **What can David enable to make sure their data is safe?**
   - **a.** Encrypting File System (EFS)
   - **b.** password protected screen saver
   - **c.** BitLocker
2. **What must be configured to ensure that the Bitlocker® storage can be reclaimed?**
   - **a.** the salesperson's personal identification and login credentials
   - **b.** BitLocker to use data recovery agents
   - **c.** the Secret Retrieval Agent
3. **What are some considerations David will have to ponder when deciding to use BitLocker?**
   - **a.** the conscientiousness and self-discipline of the sales staff
   - **b.** the deployment of hardware because BitLocker requires a system reserved partition
   - **c.** it's so easy that there aren't any serious considerations

hint

Bitlocker requires a system-reserved partition created during a standard installation.

Answers

1. To make sure the data is safe, David must enable:
   c. BitLocker
2. To ensure that the secured data can be reclaimed in the event that Bitlocker protected storage is moved to another computer, the administrator must create and properly store:
   b. BitLocker to use data recovery agents
3. When using BitLocker, the administrator must consider:
   b. the deployment of hardware because BitLocker requires a system reserved partition

Essential details

- **BitLocker (ToGo)** drive encryption is a data-protection feature available in Windows Server 2008 R2 and in some editions of Windows 7.
- **Encrypting file system (EFS)** is a feature of Windows that allows you to store information on your hard disk in an encrypted format.
- **Encryption** is the process of encoding data to prevent unauthorized access, especially during transmission.

FAST TRACK HELP

- **http://technet.microsoft.com/en-us/windows/dd408739.aspx**
- **http://technet.microsoft.com/en-us/library/cc732774.aspx**
- **http://technet.microsoft.com/en-us/library/ee706523(WS.10).aspx**
- **http://technet.microsoft.com/en-us/library/ee706518(WS.10).aspx**

Understand encryption

SCENARIO: The owner of Southridge Video takes great pride in the close relationship that she has with the managers in the various branch offices up and down the coast. Weekly communication is the key to maintaining the relationships and keeping on top of business progress and challenges.

The owner and managers would like to replace their Monday morning conference call with a secure Monday morning video conference between corporate headquarters and the various branch offices. They have asked the WAN administrator, Jeff Wang, to create a cost-effective solution. The solution must work between the remote branch offices, so having a dedicated connection between offices is too expensive. The best solution is to utilize each office's Internet connection.

1. **What will create a secured connection over an unsecured network?**
   - **a.** Virtual Private Network (VPN)
   - **b.** configuring the callback feature on their Routing and Remote Access Server
   - **c.** using a social networking site to have the conference meetings
2. **Jeff needs to decide between Point to Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP). Which protocol is more secure?**
   - **a.** PPTP
   - **b.** L2TP
   - **c.** neither, they both pass information in clear text
3. **What is a public certificate?**
   - **a.** an award given in recognition of superior business security policies
   - **b.** part of a two-part encryption that is not shared with other parties
   - **c.** a digitally signed statement that is commonly used for authentication and to information on open networks

hint

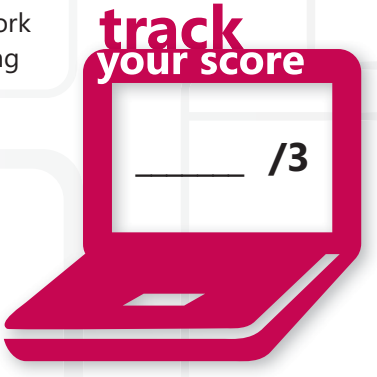
A private key certificate is a portion of two-part encryption that resides with the originating computer and is not shared.

Answers

1. A secured connection over an unsecured network can be created with a:
   a. **Virtual Private Network (VPN)**
2. The more secure protocol is:
   b. **L2TP.** PPTP uses MPPE for security, which is less secure than L2TP, which uses IPsec as its encryption method.
3. A public certificate is:
   c. **a digitally signed statement that is commonly used for authentication and to secure information on open networks**

Essential details

- **Layer 2 tunneling protocol with Internet protocol security (L2TP/IPSec)** is a combination of PPTP and Layer 2 Forwarding (L2F) that uses IPsec for encryption.
- The user keeps the **private key** secret and uses it to encrypt digital signatures and to decrypt received messages.
- The user releases the **public key** to the public, who can use it for encrypting messages to be sent to the user and for decrypting the user's digital signature.
- A **virtual private network (VPN)** is a secured tunnel running over a public network such as the Internet that uses encryption technology so that data is safe from being intercepted and understood by unauthorized users.



FAST TRACK HELP

- **http://technet.microsoft.com/en-us/library/cc700805.aspx**

Understand malware

SCENARIO: Consolidated Messenger handles customer feedback for many area businesses. Each day they receive thousands of email messages from happy and unhappy customers, which they funnel to the appropriate individuals at their client companies.

Mary Kay Anderson is the systems administrator for Consolidated Messenger. The company has had several outbreaks of viruses on the network that seem to have been propagated through email. They have asked Mary Kay to host a "lunch and learn" session to educate Consolidated Messenger staff about malicious software and email. Mary Kay has also been assigned the task to find a solution that will better protect the system.

1. **What should the staff members do when they receive a suspicious email from a customer or coworker that contains an embedded hyperlink?**
   - **a.** delete the email and then contact Mary Kay and the customer or coworker
   - **b.** quickly click the hyperlink to see what might happen to assess the threat themselves
   - **c.** forward the email to other coworkers warning them that the email is not legitimate
2. **What can Mary Kay do to prevent suspicious emails from entering their network?**
   - **a.** install Microsoft® Forefront® and Threat Management Gateway and configure it to block malicious emails
   - **b.** disable internet email
   - **c.** threaten coworkers that they will be dismissed if they forward any email
3. **What tool can Mary Kay download to remove malicious software (malware)?**
   - **a.** Remote Server Administration Tools (RSAT)
   - **b.** Microsoft Windows Malicious Software Removal Tool
   - **c.** any web-advertised security software tools—they are all the same

hint

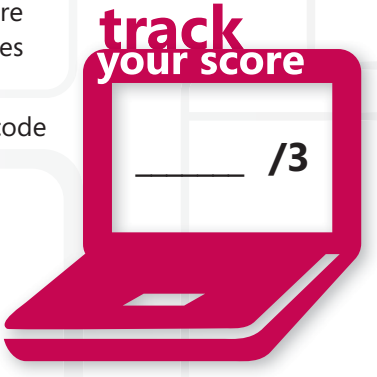
A malicious software removal tool is included in Windows updates.

Answers

1. When staff members receive a suspicious email that contains an embedded hyperlink they should:
   a. **delete the email and then contact Mary Kay and the customer or coworker.** Never forward an email with suspicious content. If an email has an attachment or link in it, contact the sender and verify that he or she sent the message.
2. To prevent suspicious emails from entering the network, Mary Kay can:
   a. **install Microsoft Forefront and Threat Management Gateway and configure it to block any malicious emails.** Exchange server has several spam filtering tools. Forefront and TMG are additional security measures to better protect the system.
3. To remove malicious software (malware), Mary Kay can download:
   b. **Microsoft Windows Malicious Software Removal Tool**

Essential details

- A **bot** is a program that performs some task on a network, especially a task that is repetitive or time-consuming.
- A **rootkit** is collection of software programs that a hacker can use to gain unauthorized remote access to a computer and launch additional attacks.
- **Spyware** is software sometimes referred to as spybot or tracking software. Spyware uses other forms of deceptive software and programs that conduct certain activities on a computer without obtaining appropriate consent from the user.
- A **trojan** is a program that appears to be useful or harmless but contains hidden code designed to exploit or damage the system on which it is run.
- A **worm** uses self-propagating malicious code that can automatically distribute itself from one computer to another through network connections.



FAST TRACK HELP

- **http://www.microsoft.com/downloads/details.aspx?FamilyId=F24A8CE3-63A4-45A1-97B6-3FEF52F63ABB&displaylang=en**
- **http://support.microsoft.com/kb/889741**

3

Understanding Network Security

IN THIS CHAPTER

- 3.1 Understand dedicated firewalls
- 3.2 Understand Network Access Protection (NAP)
- 3.3A Understand Network Isolation
- 3.3B Understand Network Isolation
- 3.4 Understand protocol security

Understand dedicated firewalls

SCENARIO: Matt Berg has earned several Microsoft certifications and is now his own boss as an independent security consultant. Trey Research has retained his services to perform a security assessment of their network. Trey Research has several servers that are exposed to the Internet and they fear that their internal network may be vulnerable to an attack. They have a single perimeter firewall, but they don't know if that is enough. Matt's job is to assess the situation and make recommendations as to how Trey Research can protect their data.

1. **What should Matt recommend that Trey Research to do with their Internet exposed servers?**
   - **a.** create a perimeter network to isolate those servers from the internal network
   - **b.** outsource the associated services
   - **c.** no action is needed—the servers are fine where they are on the internal network
2. **Is a single perimeter firewall sufficient for Trey Research?**
   - **a.** yes—a single firewall provides more than enough protection in any environment
   - **b.** no—Trey Research's concerns are justified. They should have several security appliances that provide "defense in depth" for their organization as well as enabling workstation software firewalls and antivirus
   - **c.** no—they should also create a DMZ
3. **Does stateful packet inspection or stateless packet inspection provide better security?**
   - **a.** a stateless packet inspection because it is more efficient and can stop more packets
   - **b.** neither—they do not provide any type of security
   - **c.** stateful because it inspects the packets as they pass through the connection

hint

Stateless packet inspection is a faster type of security and requires less memory but is not completely reliable.

Answers

1. Matt should recommend that Trey Research:
   a. **create a perimeter network to isolate those servers from the internal network.** Internet-exposed servers and devices should not reside on an internal network. They should be segmented or isolated into a secured part of the network.
2. Is a single perimeter firewall sufficient for Trey Research?
   b. **no—Trey Research's concerns are justified. They should have several security appliances that provide "defense in depth" for their organization as well as enabling workstation software firewalls and antivirus.** No single solution can secure a network; however, providing several layers of security reduces a company's exposure.
3. The better packet inspection choice is:
   c. **stateful, because it inspects the packets as they pass through the connection**

Essential details

- A **firewall** is a security system intended to protect an organization's network against external threats—such as hackers—coming from another network, such as the Internet.
- **Packet filtering** is the process of controlling network access based on IP addresses. Firewalls will often incorporate filters that allow or deny users the ability to enter or leave a local area network (LAN).
- A **proxy server** is a security appliance that manages Internet traffic to and from a local area network and can provide other features, such as document caching and access control.

FAST TRACK HELP

- **http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx**
- **http://technet.microsoft.com/en-us/library/cc700828.aspx**
- **http://technet.microsoft.com/en-us/library/cc700820.aspx**

Understand Network Access Protection (NAP)

SCENARIO: Adventure Works is one of the nation's largest suppliers of high-end sporting equipment. Twenty-five Adventure Works sales associates travel throughout the country selling sporting equipment to retailers. They return to corporate headquarters every Friday with their laptops for meetings and training.

Allie Bellew is the network administrator for Adventure Works and would like to implement a method for ensuring that the mobile devices are in a good state of security "health" when they access the corporate network during these Friday meetings.

1. **What control or strategy can Allie implement to assure security health?**
   - **a.** Network Access Protection, which will verify the integrity of each mobile device
   - **b.** virus scans each time sales associates log in
   - **c.** re-imaging each laptop prior to connecting to the network
2. **Aside from protecting against a virus infected laptop, what else can NAP do?**
   - **a.** protect against lost data
   - **b.** nothing else—it is simply a glorified virus scan
   - **c.** verify the complete integrity of the device by checking that it has the most recent software updates or configuration changes
3. **What can Allie do about computers that are not compatible with NAP?**
   - **a.** upgrade the computers that are not compatible
   - **b.** define exceptions in NAP for those devices that are not compatible
   - **c.** prevent those devices from using the network

hint

Exceptions can be defined for "mission-necessary" systems until they can be upgraded.

Answers

1. Allie can implement:
   a. **Network Access Protection, which will verify the integrity of each mobile device**
2. Aside from protecting against a virus infected laptop, NAP can:
   c. **verify the complete integrity of the device by checking that it has the most recent software updates or configuration changes.** Systems that have not received updates can be as problematic as systems infected by malware.
3. For computers that are not compatible with NAP, Allie should:
   b. **define exceptions in NAP for those devices that are not compatible**

Essential details

- **Network Access Protection (NAP)** is a new platform and solution that controls access to network resources based on a client computer's identity and compliance with corporate governance policy.
- **NAP enforcement points** are computers or network access devices that use NAP or can be used with NAP to require the evaluation of a NAP client's health state and provide restricted network access or communication.

FAST TRACK HELP

- **http://technet.microsoft.com/en-us/network/cc984252.aspx**
- **http://technet.microsoft.com/en-us/network/bb545879.aspx**
- **http://www.microsoft.com/windowsserver2008/en/us/nap-faq.aspx**

Understand Network Isolation

SCENARIO: Coho Winery has been in the winery business for three generations. They still produce quality wine from the same vineyards and in the same ancient cellars. Even most of their business organization has remained the same for decades. It's now time to update the corporate side of Coho with new technologies related to their data-keeping infrastructure.

Karen Berg has been assigned the task of assessing Coho Winery's network infrastructure and to provide recommendations based on their specific needs:

- Most of the employees need Internet access.
- The computers in the winery plant are isolated and don't need Internet access.
- "Work at home" employees should have Virtual Private Network access using IP Security.

1. **What can Karen do to prevent the plant computers from gaining Internet access?**
   - **a.** create a VLAN that does not allow Internet access but is trunked to the main network
   - **b.** manually configure each computer so it doesn't have a gateway
   - **c.** remove Internet Explorer from the computers
2. **What technology will Karen have to implement to allow Internet access for office employees without exposing them to the Internet?**
   - **a.** set up one walk-up computer that has a public IP address so it can access the Internet
   - **b.** give each office user a dialup modem to establish an Internet connection
   - **c.** implement a router to perform Network Address Translation that will allow several private addresses to participate on a public network
3. **What Microsoft Windows Server 2008 R2 role can accomplish both the Internet access and VPN solution?**
   - **a.** DHCP
   - **b.** Remote Desktop Service
   - **c.** Routing and Remote Access Service

hint

Most server operating systems have some form of routing technology. Minimum requirements include having multiple network interface cards (NICs).

Answers

1. To prevent the plant computers from gaining internet access, Karen can:
   a. **create a VLAN that does not allow Internet access but is trunked to the main network**
2. To allow Internet access for office employees without exposing them to the Internet, Karen can:
   c. **implement a router to perform Network Address Translation that will allow several private addresses participate on a public network.** Most retail wireless routers perform Network Address Translation or Port Address translation, which will allow home network devices (Xbox, laptops, and so on) to have Internet access.
3. Microsoft Windows Server 2008 R2 can accomplish both the Internet access and VPN solution with:
   c. **Routing and Remote Access Service (RRAS).** RRAS can serve as both a VPN and Internet gateway. VPN access can be secured using several security protocols including IP Security (IPsec).

Essential details

- **Network Address Translation (NAT)** is the process of converting between IP addresses used within an intranet or other private network and Internet IP addresses.
- **Routing** is the process of forwarding packets between networks from source to destination.
- A **Virtual LAN (VLAN)** is 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.

FAST TRACK HELP

- **http://technet.microsoft.com/en-us/network/bb531150.aspx**
- **http://technet.microsoft.com/en-us/network/bb545655.aspx**
- **http://www.microsoft.com/downloads/en/details.aspx?FamilyID=7E973087-3D2D-4CAC-ABDF-CC7BDE298847&displaylang=en**
- **http://en.wikipedia.org/wiki/Virtual_LAN**

Understand Network Isolation

SCENARIO: Arlene Huff is the systems administrator for Margie's Travel and has been very busy in recent weeks securing company and customer data. There had been suspicious activity on the network, but thankfully Arlene's actions to track network users have secured the system. But the challenge of securing confidential data is an ongoing task.

The owner of the company, Margie, would like her remote travel agents to have access to the corporate network so that they can check email and post appointments booked for that day. Margie has decided to allow the travel agents to use their home computers but must be assured that the information is secured. The security of client information is her top priority.

1. **What would be the best general solution for Margie's Travel?**
   - **a.** implement a VPN server to allow the travel agents remote access
   - **b.** set up a modem bank and have the travel agents purchase modems for their home computers so they can dial the office
   - **c.** there isn't a solution for what Margie wants
2. **What is a potential risk in having the travel agents use their home computers for VPN access?**
   - **a.** nothing—the VPN handles everything and encrypts the data
   - **b.** the travel agents may forget to disconnect which will keep the VPN connection open preventing others from connecting
   - **c.** simply having a VPN does not prevent potential viruses and malware on the home computer from infecting the network
3. **Arlene is worried about would-be attackers penetrating the VPN. What can she set up to "lure" attackers to better understand their methods?**
   - **a.** a honeypot outside the perimeter network, which is a falsified program that can emulate a VPN or service
   - **b.** a fancy website that says "Nothing to see here"
   - **c.** a fake VPN that never answers

hint

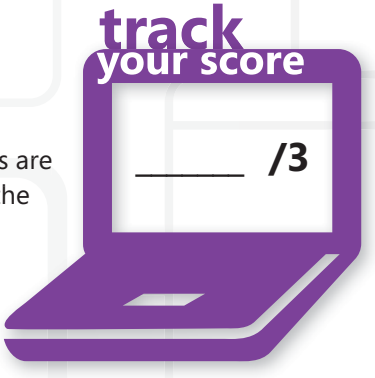
Honeypots are located all across the Internet and are used to discover methods that attackers might use to compromise a system.

Answers

1. The best general solution for Margie's Travel is to:
   a. **implement a VPN server to allow the travel agents remote access.** She can configure the VPN to use several methods of encryption.
2. The risk in having the travel agents use home computers for VPN access is that::
   c. **simply having a VPN does not prevent potential viruses and malware on the home computer from infecting the network.** Arlene can use Direct Access, which is new with Windows 7 and Windows Server 2008 R2, to help mitigate potential risks.
3. To "lure" attackers to better understand their methods Arlene can create:
   a. **a honeypot outside the perimeter network, which is a falsified program that can emulate a VPN or service**

Essential details

- A **perimeter network** (also known as DMZ, demilitarized zone, and screened subnet) is a physical or logical network that contains and exposes an organization's external services to a larger, untrusted network, usually the Internet.
- **Internet Protocol Security (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 data.
- **Virtual private network (VPN)** nodes on a public network such as the Internet communicate among themselves using encryption technology so that the messages are as safe from being intercepted and understood by unauthorized users, as though the nodes were connected by private lines.



FAST TRACK HELP

- **http://technet.microsoft.com/en-us/network/dd420463.aspx**

Understand protocol security

SCENARIO: Since Todd Rowe, the network administrator at the Graphic Design Institute, implemented stronger security measures to protect student data, the number of reported leaks has fallen to zero! The administration is pleased but Todd knows it is a constant battle to keep data secure from attacks.

Todd's friend Neil Black is an expert on the methods used to attack private data stores. Todd has asked Neil to give a presentation to the administration and office employees on network security, protocol security measures, attack methods, and prevention. Todd knows that an informed staff is part of the complete strategy in preventing and intercepting attacks.

1. **What type of attack configures a computer to appear as another computer on a trusted network by using the IP address or the physical address?**
   - **a.** identity spoofing
   - **b.** computer faking
   - **c.** application-layer attack
2. **What security protocol can help protect data from being modified, corrupted, or accessed without authorization?**
   - **a.** DNSSEC
   - **b.** IP Security (IPsec)
   - **c.** NetBIOS
3. **What type of an attack poisons a network or computer to the point where the system is rendered unusable?**
   - **a.** man-in-the-middle attack
   - **b.** password attack
   - **c.** denial of service (DOS) attack

hint

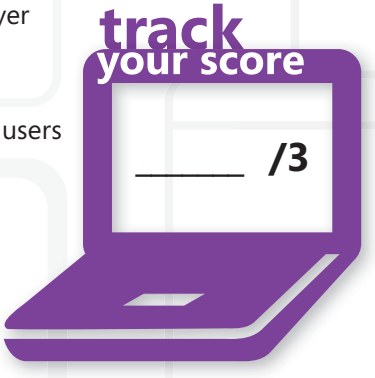
There are several forms of distributed denial of services (DOS) attacks that can either hinder a computer, server, or application from functioning.

Answers

1. An attack that configures a computer to appear as another computer on a trusted network is:
   a. **identity spoofing**
2. The security protocol that can help protect data from being modified, corrupted, or accessed without authorization is:
   b. **IP Security (IPsec).** Ipsec can be used not only for VPN security but also with local area network traffic. 80 percent of most security attacks come from within the organization. Assuming that the data inside the perimeter firewall is safe is a dangerous assumption.
3. An attack that poisons a network or computer to the point where the system is rendered unusable is a:
   c. **denial of service (DOS) attack**

Essential details

- **Sniffing** is the act of monitoring network traffic for data, such as cleartext passwords or configuration information.
- **Identity spoofing (IP address spoofing)** occurs when the attacker uses an IP address of a network, computer, or network component without being authorized to do so.
- **Internet protocol security (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.
- **Domain name system (DNS)** is 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 such as *www.microsoft.com* to IP addresses that computers can connect to.



FAST TRACK HELP

- **http://technet.microsoft.com/en-us/library/cc959354.aspx**
- **http://technet.microsoft.com/en-us/library/ee649205(WS.10).aspx**

4

Understanding Security Software

IN THIS CHAPTER

Understand client protection

SCENARIO: Jeff Hay is the network administrator for Tailspin Toys. During the off-season for toy sales, the Tailspin technology staff is kept busy maintaining and upgrading various systems in preparation for the busy holiday sales spike.

Jeff is eager to have this time to service all of the computers and update the software. He is concerned about company employees installing software from the Internet. Jeff realizes that using reputable antivirus software can only do so much. The network consists of a mix of Windows XP, Windows 7, and Windows Server 2008 R2.

1. **What can Jeff do to ensure that the computers have the latest security updates?**
   - **a.** implement Windows Software Update Services to control all Microsoft updates for both the operating systems and any Microsoft product in use
   - **b.** come in early every Monday and run Windows Updates on each computer
   - **c.** email company employees and instruct them to perform Windows Updates during their lunch breaks
2. **What can Jeff do to prevent company employees from downloading and installing software from the Internet?**
   - **a.** enable User Account Control on all Windows 7 computers as well as configure software restriction policies
   - **b.** send a strongly worded email with the Internet Usage Policy attached to all users
   - **c.** disable Internet access for all users
3. **What method should Jeff use to identify Internet software in Software Restriction Policies?**
   - **a.** hash rule
   - **b.** path rule
   - **c.** zone rule

hint

The hash rule creates a hash checksum based on the executable. The path rule restricts software located within a certain path.

Answers

1. To ensure that the computers have the latest security updates, Jeff can:
   a. **implement Windows Software Update Services to control all Microsoft updates for both the operating systems and any Microsoft product in use**
2. To prevent employees from downloading and installing software from the Internet, Jeff can:
   a. **enable User Account Control on all Windows 7 computers as well as configure software restriction policies**
3. To identify Internet software in Software Restriction Policies, Jeff can use:
   c. **zone rule**

Essential details

- **Antivirus** is a computer program that scans a computer's memory and mass storage to identify, isolate, and eliminate viruses, and also examines incoming files for viruses as the computer receives them.
- **User account control (UAC)** helps prevent malicious programs (malware) from damaging a computer and helps organizations deploy a better-managed desktop. With UAC, applications and tasks always run in the security context of a non-administrator account, unless an administrator specifically authorizes administrator-level access to the system.

FAST TRACK HELP

- **http://www.microsoft.com/security_essentials/market.aspx**
- **http://technet.microsoft.com/en-us/library/bb457141.aspx**
- **http://technet.microsoft.com/en-us/library/bb456987.aspx**
- **http://windows.microsoft.com/en-ZA/windows7/what-is-user-account-control**

Understand email protection

SCENARIO: Recently the Coho Winery has experienced a series of problems with email spam; some employees have even fallen prey to identity theft through phishing scams. John Kane is the systems administrator for Coho Winery and the task of resolving the problems has landed directly on his desk. After some research he has come up with some solutions. John intends to address these issues by implementing various security measures and most important, providing some much-needed company education as it relates to best practices while using email.

1. **What can John do to help reduce the amount of spam that hits their Microsoft Exchange server?**
   - **a.** at a minimum, enable reverse DNS lookup on the SMTP virtual server
   - **b.** disable Internet email
   - **c.** change their domain name
2. **What should Coho users do when they receive an email from a company they know with a request to click the link to "verify their account information?"**
   - **a.** delete the email
   - **b.** forward to the rest of the company with a warning not to click on the link
   - **c.** click the link because they "know" that it is a legitimate message based on the company name
3. **Aside from enabling reverse DNS lookups, what else can John do to secure his Exchange server?**
   - **a.** enable Autodiscover
   - **b.** add Sender Policy Framework (SPF)
   - **c.** update the antivirus software

hint

Antivirus software on an email server does not provide protection against spam.

Answers

1. To help reduce the amount of spam that hits their Microsoft Exchange server, John can:
   a. **at a minimum, enable reverse DNS lookup on the SMTP virtual server.** Configuring the system to do a reverse DNS lookup crosschecks the domain name with a PTR record that is the IP address associated with that domain name. If the IP address does not match the record associated with that domain name, it is not delivered.
2. When users receive an email from a company they know with a request to "verify their account information," they should:
   a. **delete the email.** Companies will not ask for account information through email in today's climate. Users should be diligent when receiving an email like this. They can also call the company to alert them of the message.
3. Aside from enabling reverse DNS lookups, John can:
   b. **add Sender Policy Framework (SPF).** SPF allows the administrator to configure the server to establish who is allowed to send email from their domain.

Essential details

- **Spam** is unsolicited, unwanted email sent by someone with whom the recipient has no personal or business relationship.
- **Phishing and pharming** are techniques used to trick computer users into revealing personal or financial information.
- An **SPF record** is an extension of the SMTP protocol that prevents spammers from forging the From fields in email messages by verifying that the IP address in the SMTP Received header is authorized to send email for the sender's domain.
- **Spoofing** is the impersonation of an email sender, IP connection, or a domain that causes an email message to appear as though it originates from a sender other than the actual sender of the message.

FAST TRACK HELP

- **http://technet.microsoft.com/en-us/exchange/dd251269.aspx**
- **http://www.microsoft.com/athome/security/email/phishing/video1.mspx**
- **http://www.microsoft.com/presspass/features/2003/nov03/11-17spamfilter.mspx**

Understand server protection

SCENARIO: A few years ago Humongous Insurance (HI) reorganized their business and technology infrastructure. Alfons Parovsky has recently been hired as the server administrator for HI. The records regarding the security updates are rather sketchy and he does not want any major security lapses to occur during his time as the administrator. To be sure everything is up to standards, Alfons has decided to immediately perform a security assessment on the datacenter. He would like to ensure that the servers meet all the necessary security requirements and are being updated regularly. Alfons also wants to ensure that HI does not have any exposures to the networks in their remote locations.

1. **What tool can Alfons use to assess HI servers have any vulnerabilities related to the operating system and installed software?**
   - **a.** Microsoft Baseline Security Analyzer
   - **b.** Event Viewer
   - **c.** Resource Monitor
2. **What service can Alfons enable to ensure that the servers are receiving all necessary software updates?**
   - **a.** Windows Backup Service
   - **b.** Routing and Remote Access Service
   - **c.** Windows Software Update Service
3. **What can Alfons do to ensure that the domain is secure in the remote locations?**
   - **a.** install a Read-Only domain controller in the remote sites
   - **b.** remove any servers in the remote sites and have employees transfer files using email
   - **c.** enforce stronger password policies in the remote sites using fine-grained passwords

hint

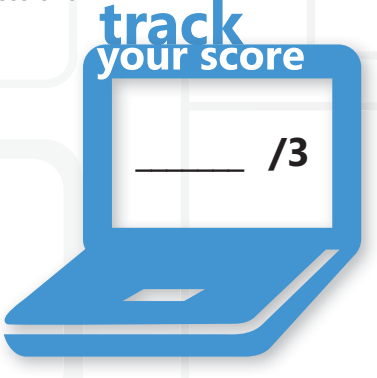
Stronger passwords do not reduce the exposure of a domain controller.

Answers

1. To assess vulnerabilities related to the operating system and installed software, Alfons can use:
   a. **Microsoft Baseline Security Analyzer.** MBSA is an easy-to-use tool that can provide instant feedback and resources to identify potential vulnerabilities on servers and workstations. It analyzes the operating system and any installed Microsoft software.
2. To ensure that the servers are receiving all necessary software updates, Alfons can enable:
   c. **Windows Software Update Service.** Alfons can create a separate group for his servers so that he can selectively manage what updates are installed and when.
3. To ensure that the domain is secure in the remote locations, he can:
   a. **install a Read-Only domain controller (RODC) in his remote sites.** Read-only domain controller (RODC) is a new type of domain controller in the Windows Server 2008 operating system. With an RODC, organizations can easily deploy a domain controller in locations where physical security cannot be guaranteed.

Essential details

- **DNS dynamic update** enables DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
- **Microsoft Baseline Security Analyzer (MBSA)** is a tool designed for the IT professional that helps small and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance.
- **Windows Server Update Services (WSUS)** enables information technology administrators to deploy the latest Microsoft product updates to computers that are running the Windows operating system.



FAST TRACK HELP

- **http://technet.microsoft.com/en-us/security/cc184923.aspx**
- **http://technet.microsoft.com/en-us/security/cc185712.aspx**
- **http://technet.microsoft.com/en-us/library/cc755058(WS.10).aspx**