Project: Securing a Microsoft Windows Environment

Purpose

This course-wide project introduces you to a variety of tasks and skills that are required for an entry-level security administrator who is tasked with securing systems in a Microsoft Windows environment.

Required Source Information and Tools

Web References: Links to Web references in the Instructor Guide and related materials are subject to change without prior notice. These links were last verified on September 25, 2019.

The following tools and resources will be needed to complete this project:

- Course textbook
- Access to the Internet

Learning Objectives and Outcomes

You will be able to:

- Describe the impact of adding Active Directory to an existing Windows network.
- Develop procedures for changing access controls.
- Develop procedures for ensuring a malware-free environment.
- Recommend Group Policy Objects for a Windows environment.
- Develop procedures for auditing security in a Windows system.
- Develop procedures for restoring a failed Windows system.
- Recommend Windows hardening techniques.
- Describe security goals and write policies for securing Windows applications.
- Ensure the integrity of all evidence collected in a Windows environment.

Overall Project Scenario

Always Fresh Foods Inc. is a food distributor with a central headquarters and main warehouse in Colorado, as well as two regional warehouses in Nevada and Virginia.

The company runs Microsoft Windows 2019 on its servers and Microsoft Windows 10 on its workstations. There are 2 database servers, 4 application servers, 2 web servers, and 25 workstation computers in the headquarters offices and main warehouse. The network uses workgroups, and users are created locally on each computer. Employees from the regional warehouses connect to the Colorado network via a virtual private network (VPN) connection.

Due to a recent security breach, Always Fresh wants to increase the overall security of its network and systems. They have chosen to use a solid multilayered defense to reduce the likelihood that an attacker will successfully compromise the company's information security. Multiple layers of defense throughout the IT infrastructure makes the process of compromising any protected resource or data more difficult than any single security control. In this way, Always Fresh protects its business by protecting its information.

Deliverables

This project is divided into several parts, as follows:

- Project Part 1: Active Directory Recommendations
- Project Part 2: Access Controls Procedure Guide

- Project Part 3: Malware Protection Procedure Guide
- Project Part 4: Group Policy Objects Recommendations
- Project Part 5: Security Audit Procedure Guide
- Project Part 6: System Restoration Procedure Guide
- Project Part 7: Network Security Controls Recommendations
- Project Part 8: Windows Hardening Recommendations
- Project Part 9: Secure Windows Applications Policy
- Project Part 10: Evidence Collection Policy

Project Part 1: Active Directory Recommendations

Scenario

Assume you are an entry-level security administrator working for Always Fresh. You have been asked to evaluate the option of adding Active Directory to the company's network.

Tasks

Create a summary report to management that answers the following questions to satisfy the key points of interest regarding the addition of Active Directory to the network:

1. System administrators currently create users on each computer where users need access. In Active Directory, where will system administrators create users?
2. How will the procedures for making changes to the user accounts, such as password changes, be different in Active Directory?
3. What action should administrators take for the existing workgroup user accounts after converting to Active Directory?
4. How will the administrators resolve differences between user accounts defined on different computers? In other words, if user accounts have different settings on different computers, how will Active Directory address that issue? (Hint: Consider security identifiers [SIDs].)

Required Resources

- Internet access
- Course textbook

Submission Requirements

- Format: Microsoft Word (or compatible)
- Font: Arial, size 12, double-space
- Citation Style: Follow your school's preferred style guide
- Length: 2 to 4 pages

Self-Assessment Checklist

- I addressed all questions required for the summary report.
- I created a well-developed and formatted report with proper grammar, spelling, and punctuation.
- I followed the submission guidelines.

Project Part 2: Access Controls Procedure Guide

Scenario

Changing access controls can have some undesirable effects. Therefore, it is important to carefully consider changes before making them and provide mechanisms to reverse changes if they have unexpected consequences.

Always Fresh management has asked you to develop procedures for changing any access controls.

The purpose of these procedures is to ensure that staff:

- Understand and document the purpose of each access control change request
- Know what access controls were in place before any changes
- Get an approval of change by management
- Understand the scope of the change, both with respect to users, computers, and objects
- Have evaluated the expected impact of the change
- Know how to evaluate whether the change meets the goals
- Understand how to undo any change if necessary

Tasks

Create a guide that security personnel will use that includes procedures for implementing an access control change.

The procedure guide must contain the steps Always Fresh security personnel should take to evaluate and implement an access control change. You can assume any change requests you receive are approved. Ensure that your procedures include the following:

- Status or setting prior to any change
- Reason for the change
- Change to implement
- Scope of the change
- Impact of the change
- Status or setting after the change
- Process to evaluate the change

Required Resources

- Internet access
- Course textbook

Submission Requirements

- Format: Microsoft Word (or compatible)
- Font: Arial, size 12, double-space
- Citation Style: Follow your school’s preferred style guide
- Length: 2 to 4 pages

Self-Assessment Checklist

- I created a procedure guide that provides clear instructions that anyone with a basic technical knowledge base can follow.
- I created a well-developed and formatted procedure guide with proper grammar, spelling, and punctuation.
- I followed the submission guidelines.

Project Part 3: Malware Protection Procedure Guide

Scenario

Always Fresh allows external users, such as vendors and business partners, to access the Always Fresh Windows environment. You have noticed a marked increase in malware activity in the test environment that seems to originate from external users. After researching the likely source of new malware, you conclude that allowing external users to connect to your environment using compromised computers exposes Always Fresh to malware vulnerabilities.

After consulting with your manager, you are asked to create a policy that will ensure all external computers that connect to Always Fresh environment are malware free. You create the following policy:

> "To protect the Always Fresh computing environment from the introduction of malware of any type from external sources, all external computers and devices must demonstrate that they are malware free prior to establishing a connection to any Always Fresh resource."

Consider the following questions:

1. What does "malware free" mean?
2. How can a user demonstrate that their computer or device is malware free?
3. What are the steps necessary to establish a malware-free computer or device?
4. How should Always Fresh verify that a client computer or device is compliant?

Tasks

Create a malware protection procedure guide that includes steps for installing and running anti-malware software. Fill in the following details to develop your procedure guide:

1. Provide a list of approved anti-malware software solutions—include at least three leading antivirus and two anti-spyware products. You may include Microsoft products and third-party products. Instruct users to select one antivirus and one anti-spyware product and install them on their computer.
2. Describe the process of:
    a. Ensuring anti-malware software and data is up to date. Mandate daily updates.
    b. Running regular malware scans. Mandate that automatic scans occur whenever the computer is idle. If that setting is unavailable, mandate daily fast scans and biweekly complete scans.
3. Provide steps to follow any time malware is detected.
    a. Immediate reaction—what to do with current work, leave the computer on or turn it off
    b. Who to contact
    c. What information to collect

The procedure guide may be used by company security professionals in the future. Hence, all steps listed should be clear and self-explanatory.

Required Resources

- Internet access
- Course textbook

Submission Requirements

- Format: Microsoft Word (or compatible)
- Font: Arial, size 12, double-space
- Citation Style: Follow your school's preferred style guide
- Length: 2 to 4 pages

Self-Assessment Checklist

- I created a procedure guide that provides clear instructions that anyone with a basic technical knowledge base can follow.
- I created a well-developed and formatted procedure guide with proper grammar, spelling, and punctuation.
- I followed the submission guidelines.

Project Part 4: Group Policy Objects Recommendations

Scenario

Always Fresh is expanding. The company is adding another application server and several workstations. As the IT infrastructure grows, it becomes more difficult to manage the added computers and devices.

Consider the Windows servers and workstations in each of the domains of a typical IT infrastructure. Based on your understanding of Group Policy, determine possible Group Policy Objects that will make it easier to manage groups of computers. Focus on common aspects of groups of computers, such as permissions for workstations or printers defined for use by groups of users.

Tasks

Recommend Group Policy Objects for the Always Fresh environment in a summary report to management. You must defend your choices with valid rationale.

Required Resources

- Internet access
- Course textbook

Submission Requirements

- Format: Microsoft Word (or compatible)
- Font: Arial, size 12, double-space
- Citation Style: Follow your school's preferred style guide
- Length: 2 to 4 pages

Self-Assessment Checklist

- I provided adequate recommendations for Group Policy Objects.
- I created a well-developed and formatted report with proper grammar, spelling, and punctuation.
- I followed the submission guidelines.

Project Part 5: Security Audit Procedure Guide

Scenario

Always Fresh wants to ensure its computers comply with a standard security baseline and are regularly scanned for vulnerabilities. You choose to use the Microsoft Security Compliance Toolkit to assess the basic security for all of your Windows computers, and use OpenVAS to perform vulnerability scans.

Tasks

Develop a procedure guide to ensure that a computer adheres to a standard security baseline and has no known vulnerabilities.

For each application, fill in details for the following general steps:

1. Acquire and install the application.
2. Scan computers.
3. Review scan results.
4. Identify issues you need to address.
5. Document the steps to address each issue.

Required Resources

- Internet access
- Course textbook

Submission Requirements

- Format: Microsoft Word (or compatible)
- Font: Arial, size 12, double-space
- Citation Style: Follow your school’s preferred style guide
- Length: 2 to 4 pages

Self-Assessment Checklist

- I created a procedure guide that provides clear instructions that anyone with a basic technical knowledge base can follow.
- I created a well-developed and formatted procedure guide with proper grammar, spelling, and punctuation.
- I followed the submission guidelines.

Project Part 6: System Restoration Procedure Guide

Scenario

One of the security improvements at Always Fresh is setting up a system recovery procedure for each type of computer. These procedures will guide administrators in recovering a failed computer to a condition as near to the point of failure as possible. The goal is to minimize both downtime and data loss.

You have already implemented the following backup strategies for workstation computers:

- All desktop workstations were originally installed from a single image for Always Fresh standard workstations. The base image is updated with all patches and new software installed on live workstations.
- Desktop workstation computers execute a cloud backup every night at 1:00 a.m.

Consider the following for a computer that encounters a disk drive failure or some other error that requires restoration:

1. How much data has been modified between the last backup and the time of failure?
2. What images are necessary to recover the workstation?
3. What are the steps necessary to fix the problem that cause the data loss?
4. What steps should Always Fresh take to avoid a reoccurrence of this issue in the future?

Tasks

Create a procedure guide that describes the necessary steps for recovering a desktop workstation computer. Fill in details for each of the following steps:

1. Describe the processes of:
   a. Fixing the problem that caused the failure in the first place. Keep the description of this process general. Just address the problem and ensure the recovery process starts with a functional computer.
   b. Restoring the newly repaired computer to a base workstation.
   c. Restoring local data for the specific workstation that failed.
2. Provide the steps to follow for each of the restore operations. Assume you will be using the Windows Backup and Restore utility.

Required Resources

- Internet access
- Course textbook

Submission Requirements

- Format: Microsoft Word (or compatible)
- Font: Arial, size 12, double-space
- Citation Style: Follow your school’s preferred style guide
- Length: 2 to 4 pages

Self-Assessment Checklist

- I created a procedure guide that provides clear instructions that anyone with a basic technical knowledge base can follow.
- I created a well-developed and formatted procedure guide with proper grammar, spelling, and punctuation.
- I followed the submission guidelines.

Project Part 7: Network Security Controls Recommendations

Scenario

Due to the Always Fresh expansion, management wants additional network controls to protect their growing network.

Tasks

Consider the Windows servers and workstations in the domains of a typical IT infrastructure. Based on your understanding of network security controls, recommend at least four possible controls that will enhance the network's security. Focus on ensuring that controls satisfy the defense in depth approach to security.

Summarize your network security controls in a summary report to management. You must provide rationale for your choices by explaining how each control makes the environment more secure.

Required Resources

- Internet access
- Course textbook

Submission Requirements

- Format: Microsoft Word (or compatible)
- Font: Arial, size 12, double-space
- Citation Style: Follow your school's preferred style guide
- Length: 2 to 4 pages

Self-Assessment Checklist

- I selected appropriate network security controls for the Always Fresh network environment.
- I provided rationale for my choices by explaining how each control makes the environment more secure.
- I created a well-developed and formatted summary report with proper grammar, spelling, and punctuation.
- I followed the submission guidelines.

Project Part 8: Windows Hardening Recommendations

Scenario

As a security administrator for Always Fresh, you have been instructed to ensure that Windows authentication, networking, and data access are hardened. This will help to provide a high level of security.

The following are issues to be addressed through hardening techniques:

- Previous attempts to protect user accounts have resulted in users writing long passwords down and placing them near their workstations. Users should not write down passwords or create passwords that attackers could easily guess, such as words founds in the dictionary.
- Every user, regardless of role, must have at least one unique user account. A user who operates in multiple roles may have multiple unique user accounts. Users should use the account for its intended role only.
- Anonymous users of the web server applications should only be able to access servers located in the demilitarized zone (DMZ). No anonymous web application users should be able to access any protected resources in the Always Fresh IT infrastructure.
- To protect servers from attack, each server should authenticate connections based on the source computer and user.

Tasks

Create a summary report to management that describes a hardening technique that addresses each issue listed above. Provide rationale for each selection.

Required Resources

- Internet access
- Course textbook

Submission Requirements

- Format: Microsoft Word (or compatible)
- Font: Arial, size 12, double-space
- Citation Style: Follow your school’s preferred style guide
- Length: 2 to 4 pages

Self-Assessment Checklist

- I addressed all issues required for the summary report.
- I created a well-developed and formatted report with proper grammar, spelling, and punctuation.
- I followed the submission guidelines.

Project Part 9: Secure Windows Applications Policy

Scenario

One of the security improvements for the Always Fresh IT environment is to ensure all workstations and servers run secure applications. The company needs policies that set security requirements for the software. These policies will guide administrators in developing procedures to ensure all client and server software is as secure as possible.

Specifically, you will write two policies to ensure web server software and web browsers are secure. Your policy statements will describe the goals that define a secure application.

Consider the following questions for web server software and web browsers:

1. What functions should this software application provide?
2. What functions should this software application prohibit?
3. What controls are necessary to ensure this applications software operates as intended?
4. What steps are necessary to validate that the software operates as intended?

Tasks

Create two policies—one for web server software and one for web browser clients. Remember, you are writing policies, not procedures. Focus on the high-level tasks, not the individual steps.

Use the following as a guide for both policies:

- Type of application software
- Description of functions this software should allow
- Description of functions this software should prohibit
- Known vulnerabilities associated with software
- Controls necessary to ensure compliance with desired functionality
- Method to assess security control effectiveness

Required Resources

- Internet access
- Course textbook

Submission Requirements

- Format: Microsoft Word (or compatible)
- Font: Arial, size 12, double-space
- Citation Style: Follow your school's preferred style guide
- Length: 1 to 2 pages

Self-Assessment Checklist

- I created two policies that addressed all issues.
- I followed the submission guidelines.

Project Part 10: Evidence Collection Policy

Scenario

After the recent security breach, Always Fresh decided to form a computer security incident response team (CSIRT). As a security administrator, you have been assigned the responsibility of developing a CSIRT policy that addresses incident evidence collection and handling. The goal is to ensure all evidence collected during investigations is valid and admissible in court.

Consider the following questions for collecting and handling evidence:

1. What are the main concerns when collecting evidence?
2. What precautions are necessary to preserve evidence state?
3. How do you ensure evidence remains in its initial state?
4. What information and procedures are necessary to ensure evidence is admissible in court?

Tasks

Create a policy that ensures all evidence is collected and handled in a secure and efficient manner. Remember, you are writing a policy, not procedures. Focus on the high-level tasks, not the individual steps.

Address the following in your policy:

- Description of information required for items of evidence
- Documentation required in addition to item details (personnel, description of circumstances, and so on)
- Description of measures required to preserve initial evidence integrity
- Description of measures required to preserve ongoing evidence integrity
- Controls necessary to maintain evidence integrity in storage
- Documentation required to demonstrate evidence integrity

Required Resources

- Internet access
- Course textbook

Submission Requirements

- Format: Microsoft Word (or compatible)
- Font: Arial, size 12, double-space
- Citation Style: Follow your school’s preferred style guide
- Length: 1 to 2 pages

Self-Assessment Checklist

- I created a policy that addressed all issues.
- I followed the submission guidelines.