JONES & BARTLETT LEARNING
An Ascend Learning Company

Project: Information Systems Security

Purpose

This project provides you an opportunity to analyze risks, threats, and vulnerabilities, apply countermeasures, and audit an information systems environment.

Required Source Information and Tools

Web References: Links to web references are subject to change without prior notice. If a web reference is no longer available, try searching for an updated version on Google or by using the Wayback Machine (https://archive.org/web/) to access it.

To complete the project, you need the following:

1. Course textbook
2. A Windows 7 or Windows 10 computer, preferably with the default installation
3. Access to the Internet
4. The following documentation provided as a handout by your instructor:
    - NIST SP 800-30 revision 1, Guide for Conducting Risk Assessments (also available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf)
    - Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (focus on the Allegro version) (also available at http://www.cert.org/resilience/products-services/octave/)

Learning Objectives and Outcomes

You will:

- Explain how to assess risks, threats, and vulnerabilities
- Evaluate potential outcomes of a malware attack and exposure of confidential information
- Evaluate information systems security countermeasures
- Create a gap analysis plan
- Evaluate and select a risk assessment methodology
- Analyze the purposes of system hardening
- Analyze Windows security events
- Evaluate information systems security activities in terms of business success

Introduction

Contemporary organizations collect, store, and transmit a tremendous amount of highly sensitive data. Despite the many benefits that information technology offers, these systems are not always completely secure. Proper controls must be put in place to mitigate security risks and protect vital business information.

Deliverables

The project is divided into three parts. Details for each deliverable can be found in this document. Your instructor will assign due dates for each part.

- Project Part 1: Risks, Threats, and Vulnerabilities
- Project Part 2: Gap Analysis Plan and Risk Assessment Methodology
- Project Part 3: System Hardening and Auditing

Project Part 1: Risks, Threats, and Vulnerabilities

Scenario

Fullsoft, Inc. is a software development company based in New York City. Fullsoft's software product development code is kept confidential in an effort to safeguard the company's competitive advantage in the marketplace. Fullsoft recently experienced a malware attack; as a result, proprietary information was leaked. The company is now in the process of recovering from this breach.

You are a security professional who reports into Fullsoft's infrastructure operations team. The chief technology officer (CTO) asks you and your colleagues to participate in a team meeting to discuss the incident and its potential impact on the company.

Tasks

1. Prepare for the meeting by deliberating on the following questions:
   - What circumstances may have allowed this incident to occur, or could allow a similar incident to occur in the future?
   - What insights about risks, threats, and/or vulnerabilities can you glean from reports of similar incidents that have occurred in other organizations?
   - What potential outcomes should the company anticipate as a result of the malware attack and possible exposure of intellectual property?
   - Which countermeasures would you recommend the company implement to detect current vulnerabilities, respond to the effects of this and other successful attacks, and prevent future incidents?
2. Write an outline of key points related to the questions above that the team should discuss at the meeting.

Required Resources

- Textbook for this course
- Internet access

Submission Requirements

- Format: Microsoft Word or compatible
- Font: Arial 12-point, double-spaced
- Citation Style: Follow your school's preferred style guide
- Length: 1–2 pages

You are encouraged to respond creatively, but you must cite credible sources to support your work.

Self-Assessment Checklist

- I created an outline that describes key points the team should discuss at the meeting. My outline describes:

  - Circumstances that may have allowed the malware infection to occur, or could allow a similar incident to occur in the future
  - Insights about risks, threats, and/or vulnerabilities from reports of similar incidents that have occurred in other organizations
  - Potential outcomes of a malware attack and exposure of confidential information
  - Countermeasures the company should implement
- I conducted adequate independent research for this part of the project.
- I followed the submission guidelines.

Project Part 2: Gap Analysis Plan and Risk Assessment Methodology

Scenario

After the productive team meeting, Fullsoft's chief technology officer (CTO) wants further analysis performed and a high-level plan created to mitigate future risks, threats, and vulnerabilities. As part of this request, you and your team members will create a plan for performing a gap analysis, and then research and select an appropriate risk assessment methodology to be used for future reviews of the Fullsoft IT environment.

An IT gap analysis may be a formal investigation or an informal survey of an organization's overall IT security. The first step of a gap analysis is to compose clear objectives and goals concerning an organization's IT security. For each objective or goal, the person performing the analysis must gather information about the environment, determine the present status, and identify what must be changed to achieve goals. The analysis most often reveals gaps in security between "where you are" and "where you want to be."

Two popular risk assessment methodologies are NIST SP 800-30 revision 1, Guide for Conducting Risk Assessments, and Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). Your focus will be on the OCTAVE Allegro version, which is a more concise version of OCTAVE. When reviewing the methodologies, consider the following:

- Which features or factors of each methodology are most important and relevant to Fullsoft?
- Which methodology is easier to follow?
- Which methodology appears to require fewer resources, such as time and staff, but still provides for a thorough assessment?

Tasks

- Create a high-level plan to perform a gap analysis.
- Review the following two risk assessment methodologies:
  - NIST SP 800-30 rev. 1, Guide for Conducting Risk Assessments (formerly titled " Risk Management Guide for Information Technology Systems")
  - Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Allegro version
- Create a report that includes the gap analysis plan, a brief description of each risk assessment methodology, a recommendation for which methodology Fullsoft should follow, and justification for your choice.

Required Resources

- Textbook for this course
- Internet access

Submission Requirements

- Format: Microsoft Word or compatible
- Font: Arial 12-point, double-spaced
- Citation Style: Follow your school's preferred style guide
- Length: 3–4 pages

You are encouraged to respond creatively, but you must cite credible sources to support your work.

Self-Assessment Checklist

- I created a plan for performing a gap analysis of the IT environment.
- I evaluated and selected a risk assessment methodology.
- I summarized each methodology, recommended which methodology Fullsoft should follow, and provided justification for my choice.
- I conducted adequate independent research for this part of the project.
- I followed the submission guidelines.

Project Part 3: System Hardening and Auditing

Scenario

Fullsoft's chief technology officer (CTO) established a plan to mitigate risks, threats, and vulnerabilities. As part of the mitigation plan, you and your team members will configure baseline security controls on all workstations (harden the systems), which run either Windows 7 or Windows 10. For this effort, you will ensure that the antivirus software is running properly and implement a control related to password-hacking attempts.

In addition, Fullsoft's CTO has asked your team to pay special consideration to continuously monitoring, testing, and improving countermeasures. The CTO points out that within the first 24 hours of configuring baseline security, you may sometimes receive alerts that malware has been quarantined within an antivirus program or notice a failed logon attempt captured by the Windows audit log. In response, you make a note to check the security of the workstation for which you will configure baseline security.

The CTO also requests a report on the work you performed, part of which will be incorporated into the company's IT security policy procedures. The report should also include the purposes of system hardening and auditing, and an additional area of concern or emerging trend related to information systems security that's relevant to Fullsoft.

At the end of the report, include a brief statement that explains how your work on this project relates to the larger responsibility you have for supporting the company's success regarding IT security. Your statement will be considered a part of your upcoming performance review.

Tasks

If possible, complete the hardening and auditing tasks using a personal computer with the default installation of Windows 7 or Windows 10. If you do not own the necessary hardware and software, consult with your instructor about alternatives. After your work on this project is complete, you may need to return the settings to the previous configuration.

1. Ensure that you are logged in as an administrator. Using a computer that has Windows 7 or Windows 10 installed:
    a. Review the antivirus program. Ensure that it is up to date, is configured for automatic updates, and is scheduled to run quick scans regularly. Note when the last full system scan was run and any issues you observe with the software.
    b. Configure audit logging to identify all failed password attempts into the system.

2. After at least 24 hours, check the Windows workstation for security events. Be sure to review the audit log in Windows Event Viewer.

3. Write a report in which you:

    - Explain how you ensured the antivirus program is up to date, scheduled to run regular quick scans, and when the last full system scan was run. Describe anything significant you observed.

    - Explain how you configured audit logging to record all failed password attempts into the system.

    - Describe all the potentially problematic security events that occurred in the 24-hour period after checking the antivirus software and configuring audit logging.

- Explain what was done (or should be done) to correct any problems encountered.
- Explain the purposes of system hardening and auditing in terms of the company's goal of maintaining information systems security. Also describe an additional area of concern or an emerging trend related to information systems security that you think warrants the company's attention in the immediate future.
- Briefly explain how your work on this project relates to your responsibility to help the company achieve its IT security goals.

Required Resources

- Textbook for this course
- A Windows 7 or Windows 7 computer, preferably with a default installation
- Internet access

Additional Resources

- **Audit logon events:** https://technet.microsoft.com/en-us/itpro/windows/keep-secure/basic-audit-logon-events
- **How to See Who Logged Into a Computer and When:** http://www.howtogeek.com/124313/how-to-see-who-logged-into-a-computer-and-when/
- **Event Logs:** https://technet.microsoft.com/en-us/library/cc722404(v=ws.11).aspx
- **Using Event Viewer to Troubleshoot Problems:** http://www.howtogeek.com/school/using-windows-admin-tools-like-a-pro/lesson3/

Submission Requirements

- Format: Microsoft Word or compatible
- Font: Arial 12-point, double-spaced
- Citation Style: Follow your school's preferred style guide
- Length: 3–4 pages

You are encouraged to respond creatively, but you must cite credible sources to support your work.

Self-Assessment Checklist

- I summarized the system-hardening and auditing configuration steps I implemented on a computer using Windows 7 or Windows 10, including:
    - How I ensured the antivirus software is running properly
    - How I configured audit logging of all failed password attempts
- I described potentially problematic security events that occurred within a 24-hour period, and noted actions that were taken (or should be taken) to address them.
- I explained the purposes of system hardening and auditing in terms of the company's overarching goal of maintaining information systems security.
- I proposed at least one area of concern or emerging trend related to information systems security that warrants additional attention.
- I explained how my work on this project relates to my professional responsibility to help the company achieve its IT security goals.

- I conducted adequate independent research for this part of the project.
- I followed the submission guidelines.