Laboratory #6

Lab #6: Define a Remote Access Policy to Support Remote Healthcare Clinics

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Define the scope of an remote access policy as it relates to the Remote Access Domain
- Identify the key elements of a remote access policy within an organization as part of an overall security management framework
- Align the remote access policy with the organization's goals for compliance
- Mitigate common risks and threats found within the Remote Access Domain with proper security controls and countermeasures as defined in the remote access policy definition
- Create a remote access policy definition incorporating a policy statement, standards, procedures, and guidelines

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to perform this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #6:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to perform this lab:
    a. Microsoft Office 2007 or higher
    b. Adobe PDF reader
    c. Internet access

Recommended Procedures

Lab #6 – Student Steps

1. Review with the instructor sample Remote Access Policy documents found on the Internet:
    SANS Institute: Remote Access Policy Template
    http://www.sans.org/security-resources/policies/Remote_Access_Policy.pdf

    Higher-Education: Clark University
    http://www.clarku.edu/offices/its/policies/remoteaccess.cfm

Higher-Education: Purdue University

http://www.purdue.edu/policies/pages/information_technology/v_1_6.shtml

Healthcare: UNC School of Medicine & Healthcare Clinic

http://www.med.unc.edu/security/hipaa/documents/SOM%20Remote%20Access%20Policy%202009%20Final.pdf

2. Discuss what the risks and threats are within the Remote Access Domain per the bulleted list provided:
   - Brute force user ID and password attacks
   - Users or employees unaware of the risks, threats, and dangers of the Internet and shared Wi-Fi or broadband Internet access
   - Multiple access attempts and login retries
   - Unauthorized access to IT systems, applications, and data
   - Privacy data or confidential data is compromised remotely
   - Data leakage occurs in violation of Data Classification Standard
   - Remote worker's laptop is stolen
   - Remote worker's token device is stolen
   - Remote worker requires access to patient medical records system through public Internet

3. Discuss what organizations can do to mitigate the risks and threats identified within the Remote Access Domain

4. Complete the Lab #6 – Assessment Worksheet deliverables: Identify Elements of a Remote Access Policy Definition, Create a Remote Access Policy Definition for Multiple Healthcare Clinics

5. Complete the Lab #6 – Assessment Questions & Answers and submit with this lab.

Deliverables

Upon completion of the Lab #6: Define a Remote Access Policy to Support Remote Healthcare Clinics, the students are required to provide the following deliverables:

1. Lab #6 – Assessment Worksheet: Identify Elements of a Remote Access Policy Definition

2. Lab #6 – Assessment Worksheet: Create a Remote Access Policy Definition for Multiple Remote Healthcare Clinics

3. Lab #6 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #6 that the students must demonstrate:

1. Was the student able to define the scope of a remote access policy as it relates to the Remote Access Domain? – [**20%**]

2. Was the student able to identify the key elements of remote access policy within an organization as part of an overall security management framework? – [**20%**]

3. Was the student able to align the remote access policy with the organization's goals for compliance? – [**20%**]

4. Was the student able to mitigate common risks and threats found within the Remote Access Domain with proper security controls and countermeasures as defined in the remote access policy definition? - [**20%**]

5. Was the student able to create a remote access policy definition incorporating a policy statement, standards, procedures, and guidelines? – [**20%**]

Current Version Date: 11/23/2011

Lab #6 – Assessment Worksheet

Elements of a Remote Access Domain Policy

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

For each of the identified risks and threats within the Remote Access Domain, identify a security control or security countermeasure that can help mitigate the risk or threat. These security controls or security countermeasures will become the basis of the scope of the Remote Access Domain Policy definition to help mitigate the risks and threats commonly found within the Remote Access Domain.

Remote Access Domain Risks & Threats	Risk Mitigation Tactic/Solution
Brute force user ID and password attacks	
Multiple login retries and access control attacks	
Unauthorized remote access to IT systems, applications, and data	
Privacy data or confidential data is compromised remotely	
Data leakage in violation of existing Data Classification Standards	

Current Version Date: 11/23/2011

Remote Access Domain Risks & Threats	Risk Mitigation Tactic/Solution
Mobile worker laptop is stolen	
Mobile worker token or other lost or stolen authentication device	
Remote worker requires remote access to medical patient online system through the public Internet	
Users and employees are unaware of the risks and threats caused by the public Internet	

Lab #6 – Assessment Worksheet

Define a Remote Access Policy to Support Remote Healthcare Clinics

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you are to create an organization-wide Remote Access Policy for a mock organization under a recent compliance law. Here is your scenario:

- Regional ABC Healthcare Provider with multiple remote, healthcare branches and locations throughout the region

- Online access to patients' medical records through the public Internet is required for remote nurses and hospices providing in-home medical services

- Online access to patients' medical records from remote clinics is done through SSL VPN secure web application front-end through the public Internet

- The organization wants to be in compliance with HIPAA and IT security best practices regarding remote access through the public Internet in the Remote Access Domain

- The organization wants to monitor and control the use of remote access by implementing system logging and VPN connections

- The organization wants to implement a security awareness & training policy mandating that all new hires and existing employees obtain remote access security training. Policy definition to include HIPAA and ePHI (electronic personal healthcare information) security requirements and a mandate for annual security awareness training for all remote or mobile employees

Instructions

Using Microsoft Word, create a Remote Access Policy Definition capturing the elements of the policy as defined in the Lab #6 – Assessment Worksheet. Use the following policy template for the creation of your Remote Access Policy definition for a regional healthcare provider with remote medical clinics.

ABC Healthcare Provider

Remote Access Policy for Remote Workers & Medical Clinics

Policy Statement

{Insert policy verbiage here}

Purpose/Objectives

{Insert purpose of the policy as well as the objectives – bulleted list of the policy definition}

Scope

{Define this policy's scope and whom it covers.

Which of the seven domains of a typical IT infrastructure are impacted?

What elements or IT assets or organization-owned assets are within the scope of this policy?}

Standards

{Does this policy point to any hardware, software, or configuration standards? If so, list them here, and explain the relationship of this policy to these standards. In this case, Remote Access Domain standards should be referenced such as encryption standards, SSL VPN standards, – make any necessary assumptions.}

Procedures

{Explain how you intend to implement this policy organization-wide and how you intend to deliver the annual or on-going security awareness training for remote workers and mobile employees.}

Guidelines

{Explain any road blocks or implementation issues that you must address in this section and how you will overcome them per defined policy guidelines.}

Note: Your policy document must be no more than 3 pages long.

Lab #6 – Assessment Worksheet

Define a Remote Access Policy to Support Remote Healthcare Clinics

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

This lab presents the risks and threats commonly found in the Remote Access Domain and how the use of the public Internet introduces new challenges regarding security and compliance for organizations. The students created a Remote Access Policy definition specific to a healthcare organization requiring remote access to patients' medical records systems from remote clinics and patient homes from mobile nurses and healthcare providers in the field.

Lab Assessment Questions & Answers

1. What are the biggest risks when using the public Internet as a WAN or transport for remote access to your organization's IT infrastructure?

2. Why does this mock healthcare organization need to define a Remote Access Policy to properly implement remote access through the public Internet?

3. What is the relationship between an Acceptable Use Policy (AUP) and a Security Awareness & Training Policy?

4. One of the major prerequisites for this scenario was the requirement to support nurses and healthcare professionals that are mobile and who visit patients in their homes. Another requirement was for remote clinics to access a shared patient medical records system via a web browser. Which type of secure remote VPN solution is recommended for these two types of remote access?

5. When trying to combat unauthorized access and login attempts to IT systems and applications, what is needed within the LAN-to-WAN Domain to monitor and alarm on unauthorized login attempts to the organization's IT infrastructure?

6. Why is it important to mobile workers and users about the risks, threats, and vulnerabilities when conducting remote access through the public Internet?

7. Why should social engineering be included in security awareness training?

8. Which domain (not the Remote Access Domain) throughout the seven domains of a typical IT infrastructure supports remote access connectivity for users and mobile workers needing to connect to the organization's IT infrastructure?

9. Where are the implementation instructions defined in a Remote Access Policy definition? Does this section describe how to support the two different remote access users and requirements as described in this scenario?

10. A remote clinic has a requirement to upload ePHI data from the clinic to the organization's IT infrastructure on a daily basis in a batch-processing format. How should this remote access requirement be handled within or outside of this Remote Access Policy definition?

11. Why is a remote access policy definition a best practice for handling remote employees and authorized users that require remote access from home or on business trips?

12. Why is it a best practice of a remote access policy definition to require employees and users to fill in a separate VPN remote access authorization form?

13. Why is it important to align standards, procedures, and guidelines for a remote access policy definition?

14. What security controls, monitoring, and logging should be enabled for remote VPN access and users?

15. Should an organization mention that they will be monitoring and logging remote access use in their Remote Access Policy Definition?