Vulnerability Assessment Policy

CSA217.com

Created by: Patrick Murphy, Vulnerability Assessor

Reviewed by: Arsalan Parsaei, Professor

Approved by: Arsalan Parsaei, Manager

Overview

Vulnerability management is a process in which security vulnerabilities are searched for and reported on in a given system or network of computers. A scope of systems to analyse is defined and tested in order to discover any risks in the systems, and these risks are documented. Vulnerability management is an essential process for organizations to follow to maintain secure operations of their technological infrastructure.

Purpose

This policy's purpose is to define the vulnerability assessment process and methods for CSA217.com. This document provides a standardized method to follow when conducting vulnerability assessments, including the scope of assessment and the analysis process to ensure the security risks are documented and dealt with. It also links to documents used to remediate the discovered vulnerabilities.

Scope

The main asset to be assessed is the MSL2.0 server. The Windows 10 machine is to be used as protection for the MSL server and should eventually be assessed for its own vulnerabilities to secure the entire network. This server is an extremely important asset to the company and should be assessed thoroughly.

Policy

The vulnerability assessment process for CSA217.com must adhere to the PCI DSS security standards. Wireless access points must be searched for each quarter, and any unauthorized points must be documented and dealt with. Internal and external network scans must be performed at least once a quarter and rescans must be completed if the scans do not pass. Rescans must be done until a passing scan is achieved. External scans will be completed by an Approved Scanning Vendor (ASV), whereas internal scans will be done by the CSA217.com security team.

Scans will be completed using tools approved by CSA217.com management. Currently approved tools include nmap and Nessus. These scans will be done in the off-hours from Friday evening at 19:00 to Saturday morning at 07:00, as to avoid disrupting systems. All employees are expected to comply with any requests from the security team to ensure they can complete scans successfully.

Any Security vulnerabilities that are discovered will be documented, and a plan to remediate the vulnerability to the safest state possible will be created. Employees are expected to cooperate with the security team in the process of remediating these vulnerabilities.

Type of Vulnerability Assessment

A white box vulnerability assessment will be conducted on the MSL2 server. This involves scanning the machine using its credentials to dig deeper into where potential vulnerabilities may reside. Nessus will be used to conduct a credentialed scan for vulnerabilities on the server and the most impactful and risky vulnerabilities will be documented, as well as the steps to remediate them.

Vulnerability Assessment Process

A fully credentialed Nessus scan will be run on the MSL2 server to discover any vulnerabilities it may have. The most dangerous results of this scan will be analysed, and remediation solutions will be recommended. The results of the scan will be documented and will be found in the related documents section along with the remediation recommendations document. The assessment team will test the Windows 10 protective machine to ensure it can protect the server from DDoS and other types of attacks using its anti-DDoS and honeypot software. A kali machine is used to scan and attack the network to guarantee the network is safe from such attacks.

Exceptions

The Windows machine that is being used to protect the MSL2 server from DDoS and other attacks has been excluded from this assessment. It is a fully updated, brand new machine that has been set up to be as safe as possible and therefore does not need another assessment.

Enforcement

CSA217.com employees who are found to have violated this policy will be disciplined. The security of CSA217.com is paramount to its business, employees who are not following this policy may be terminated, and legal action can be initiated if the violation is significant.

Related Documents

[1] Nessus scan of the MSL2 server - 8803_Project_2MSL2CScan.html

[2] Vulnerability remediation document - 8803_Project_2Remediation.docx

[3] Asset table - 8803_Project_AssetTable.xlsx

Revision History

[1] December 09, 2021 – Initial Vulnerability Assessment Policy document created.

[2] December 12, 2021 – Addition of Nessus scan results

[3] December 14, 2021 – Addition of remediation document

[4] December 15, 2021 – Process section addition

Glossary

Approved Scanning Vendor (ASV) – An organization approved by the PCI SCC to complete external scans.

Payment Card Industry Data Security Standard (PCI DSS) – A standard set by PCI that any organization that processes payment card information must adhere to in order to maintain security of the payment card data.

MSL2 – Metasploitable Linux 2.0, the operating system running on the new server.

Nessus – A state of the art software used to scan machines for software vulnerabilities.