

Assessing the Security Posture and the Creation of Report and Remediation Plan for a Designated System

By Cory Tyzack

Introduction

The project was decided based on a job role change into Cyber Security. The project focuses on identifying vulnerabilities in a system and producing the relevant report with the findings followed by a remediation plan which will be presented to the system owner with possible actions to take to deal these vulnerabilities.

Aims & Objectives

The aim of the project is to ensure that an assessment has taken place on the system and a remediation plan is in place to help the system owner achieve a level of security for the system so that it can enter the service.

The objectives to ensure this aim is met are as follows:

- To complete a literature review on the subject area
- Conduct an IT Health Check on the System and populate findings into a report
- Plan and complete a remediation action plan on the risks

Research Findings

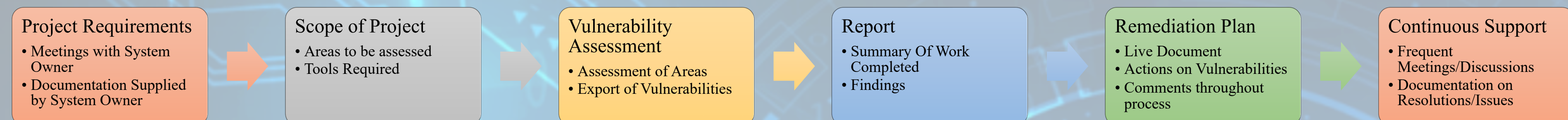
The Cyber Security Literature Review was aimed towards areas within the current job role. These Areas Included:

- Information Assurance (IA) – CIA Triad – Identifying, Understanding and Managing Risk
- Risk Management in IA – Processes and Procedures
- Security Frameworks – ISO 27005/NIST Framework steps to protect Information
- Technology Assurance – How continually secure a technology or system can be from threats
- Vulnerability Assessment – Identifying Vulnerabilities through different tools
- IT Health Check – External and Internal Testing on systems such as (Desktop/Server builds, Security patching of Operating Systems and Wireless Network Configuration)



Design and Implementation

The Design and Implementation follows the step-by-step process as pictured in the flowchart below.



Following this flow chart allows the tester to logically move through the vulnerability assessment to create the report of findings as well as the remediation plan. Tools used to complete the IT Health Check include Nessus to find vulnerabilities within Infrastructure and Operating System Builds etc. and HashCat within the Kali Linux Distributions used to try crack domain passwords . The vulnerabilities found can then be exported and displayed in the report with a description and risk rating as shown in the example below.



045	Windows Domain	Weak Passwords The passwords for the domain users were checked against the list of top 100K passwords taken from HavelBeenPwned.com and published by NCSC. Several accounts were found to have passwords which appeared on this list.	High 
-----	----------------	---	---

This Vulnerability was found using HashCat. There was passwords used within the domain that were in the password list provided by the National Cyber Security Centre (NCSC). This list is available to anyone, if used maliciously then the network is at risk of attack. These passwords will need to be changed immediately and the current password system will need to be assessed by the system owner to ensure a secure password policy.

002	Outdated or Unsupported Third-Party Software Hosts contained third-part software packages which were outdated, some of which were affected by publicly reported security vulnerabilities.	High 	• Third Party software to be managed centrally with required patches installed when available • Permissions set on Standard User accounts to stop users installing 3rd Party Software • Investigation removal of unsupported software and replace with supported software	TBC	R	System Owner to assign investigation to engineer within team
-----	---	---	--	-----	---	--

The image above is taken from the remediation plan. It provides details on possible fixes which the system owner could take. This would be dependent on the system and is not a case of one action fixes all. It is up to the system owner with guidance of the cyber expert which fix they use if any. In this example it could be a case of system owner changing permissions on standards accounts, removing any software that is not relevant for the system or implementing a managed software solution such as software centre to ensure to ensure all software is up to date.

Conclusion and Recommendations

The project was a success and the system owner happy with the outcome so the aim and objectives were achieved, The literature review provided good knowledge and understanding for the direction of the project.

The report and remediation plan provided good detail for the system owner to work towards a secure system but detailing each vulnerability and suggested actions to remediate.

Recommendations for future project included possibility of more in-depth analysis between the tester and the system owner. This would be achieved by planning frequent meetings to discuss the vulnerabilities and progression. This would ensuring that any disagreements between the attendees on solutions for the vulnerabilities could be resolved. The final recommendation would be to start a live document on the vulnerabilities with good fixes so there are standards in place to achieve a secure system in timely matters.