Vulnerability Assessment (VA) Knowledge Syllabus

Core learning objectives and assessment methodology

CONTENTS

DOCUMENT CONTROL STATEMENTS

Amendment History

Date	Author	Issue	Status
02/06/2020	Paul Richards	0.1	Initial draft
25/06/2020	Tech Panel	1.0	First issue
28/07/2020	Andrew Jones	1.1	Minor amendments
06/08/2020	Andrew Jones	1.2	Minor amendments
12/08/2020	Emma Philpott	1.3	Minor amendments
4/3/2021	Paul Richards	1.4	Minor amendments

1 INTRODUCTION

1.1 Knowledge areas to support self-study or course identification

This technical syllabus comprises of the technical skills and knowledge that Cyber Scheme expects candidates to possess for the Vulnerability Assessor (VA) exam.

Please note: where this material has been sourced from the Internet an appropriate citation and or acknowledgement of use has been included.

The syllabus contains a series of modules that should help you focus on preparation for the exam assessment. It is highly recommended that your learning journey include both theory and practical study.

1.2 Exam

The exam is split into 4 sections, all of which must be passed by obtaining 60% or more in each (a 50% pass in the multiple choice paper will lead to a pass but without a path way to CTM) :

1. Practical Phase- Vulnerability assessment, tool setup and project comprehension
    a. 30 mins
    b. Open book (Monitored, restricted internet access / candidates own notes and reference material may be used / copy and pasting from the question and resources is allowed)
    c. Provide examples of how a system (based on a scenario) is to be assessed
2. Longform Written Essay - Analysis and understanding of results
    a. 2 hours
    b. Closed book (No internet access / no reference materials / no copy and pasting from the question papers or resources provided)
    c. Produce a document to show the attack surface of a second scenario (may or may not be linked to practical phase - depending on the assessment paper on the day)
3. Multiple Choice Paper
    a. 100 questions
    b. 1 hour
    c. Closed book (No internet access / no reference materials / no copy and pasting from the question papers or resources provided)
4. Viva – Interview
    a. 15-30 minutes
    b. Closed book (No internet access / no reference materials / no copy and pasting from the question papers or resources provided)
    c. Interview style question and answer session to assess your understanding

1.3 Aims of the learning outcomes

- Provide an overview of the vulnerability assessment process.
- Learn about tools used during the vulnerability assessment process.
- Understand the underlying concepts of TCP/IP, Ports and Protocols.
- Apply critical thinking to solve problems encountered during an assessment
- Apply tools and techniques to assess:
    - external facing interfaces.

- internal interfaces
- the threat of malware (Antimalware solutions, Application allow listing)

- Assess the threat of common external attacks (Email, SMS etc)
- Assess the threat of common internal attacks (Web Applications, Downloads)
- Report/Explain Vulnerabilities found

1.4 Learning Objectives

- Understand Information security in the corporate world.
- Understand the laws and regulations involved with vulnerability assessing
- Understand quantifying and measuring risks associated with vulnerabilities
- Understand how to find internal and external vulnerabilities
- Understand how to test hardening measures for malware
- Report and explain vulnerabilities found throughout a project.

2 LEARNING OUTLINE

2.1 Section 1 –Information security in the corporate world.

- LO1.1 – Exploiting a vulnerability
- LO1.2 – Understanding the 'Scope'
- LO1.3 - Planning and Management
- LO1.4 – CIA Model
- LO1.5 – DDPRR Model

2.2 Section 2 – Laws and regulations involved with vulnerability assessing

- LO2.1 – Understand the basic hacking offence
- LO2.2 - Understand the Computer Misuse Act (1990)
- LO2.3 – Understand the Police and Justice Act (2006)
- LO2.4 – Understand the Data Protection Act (2018)

2.3 Section 3 – Quantifying and measuring risks associated with vulnerabilities

- LO3.1 – CVSS 3

2.4 Section 4 – Internal and external vulnerabilities

- LO4.1 - Use tools to scan and enumerate an external target network.
- LO4.2 - Use tools to scan and enumerate an internal target network.

2.5 Section 5 – Hardening measures for malware

- LO5.1 – Use techniques to assess the hardening of a system to malware
- LO5.2 – Use techniques to assess the threat of attacks via email / SMS etc
- LO5.3 – Use techniques to assess the treat of users introducing malware

2.6 Section 6 – Reporting and explaining vulnerabilities

- LO6.1 - Audience
- LO6.2 - Technical Writing Skills
- LO6.3 - Executive Summary

3 MARKING

3.1 Section 1 - Information security in the corporate world.

Learning Outcome	Core Skill	Details	Examined
LO1.1	Exploiting a vulnerability	Windows Linux Other Web based	Multiple Choice
LO1.2	Understanding the 'Scope'	Understanding client requirements. Scoping to fulfil client requirements	Multiple Choice Practical
LO1.3	Planning and Management	Accurate timescale scoping Resource planning	Multiple Choice Practical
LO1.4	CIA Model	What is Confidentiality, Integrity and availability? Attacks against Confidentiality, Integrity and availability	Multiple Choice
LO1.5	DDPRR Model	Understanding the Deter, Detect, Protect, React and Recover model	Multiple Choice

3.2 Section 2 – Laws and regulations involved with vulnerability assessing

Learning Outcome	Core Skill	Details	Examined
LO2.1 LO2.2 LO2.3 LO2.4	Law and Compliance	Impact of the laws against VA assessors Knowledge of the UK legal issues involved in the Computer Misuse Act (1990) Knowledge of the UK legal issues involved in the Police and Justice Act (2006) Knowledge of the UK legal issues involved in the Data Protection Act (2018) Human rights Act (1998) Awareness of sector-specific regulatory issues.	Multiple Choice Practical Longform

3.3 Section 3 - Quantifying and measuring risks associated with vulnerabilities

Learning Outcome	Core Skill	Details	Examined
LO3.1	CVSS 3	CVSS v3 CVSS calculator Manual CVSS calculations	Multiple Choice Longform

3.4 Section 4 - Internal and external vulnerabilities

Learning Outcome	Core Skill	Details	Examined
LO4.1	Use tools to scan and enumerate an external target network	Networks / IP addresses / ports VA tools Requirements and configuration	Multiple Choice, Practical Longform VIVA
LO4.2	Use tools to scan and enumerate an internal target network.	Networks / IP addresses / ports VA tools Requirements and configuration False positives and reading results Exporting and reporting	Multiple Choice, Practical Longform VIVA

3.5 Section 5 – Hardening measures for malware

Learning Outcome	Core Skill	Details	Examined
LO5.1	Use techniques to assess the hardening of a system to malware	Malware Anti-Malware Allow listed applications Sandboxing	Multiple Choice, Practical Longform VIVA
LO5.2	Use techniques to assess the threat of attacks via email / SMS etc	Phishing Email hardening Assessing techniques	Multiple Choice, Practical Longform

LO5.3	Use techniques to assess the treat of users introducing malware	Internet Browsers Browser hardening Assessing techniques	Practical Longform VIVA

3.6 Section 6 - Reporting and explaining vulnerabilities

Learning Outcome	Core Skill	Details	Examined
LO6.1	Audience	Technical / non-technical Language Understanding the different types of people that will be reading a report, and how to cater the style of writing towards the different types.	Multiple Choice Longform
LO6.2	Technical Writing Skills	Understand the differences in writing in a technical format and style.	Multiple Choice Longform
LO6.3	Executive Summary	The importance of an Executive summary and what makes up a summary. Common pitfalls in writing a technical summary.	Multiple Choice Longform

4 REMOTE ASSESSMENTS AND DISABILITY

Cyber scheme will, where possible, make provision for any additional time or support that might be required if you have any medical or learning disability, but you need to make contact with Cyber Scheme at least 3 working days ahead of the exam to ensure appropriate adjustments are made and the assessor is properly briefed. You will need to provide adequate information about your condition in order for the appropriate adjustments to be made.

Cyber Scheme takes seriously the management of sensitive PII and as such will not make a formal record or retain any information provided other than to support any preparation an Assessor might need to undertake, and a record of any additional time allowed. All provided PII information will be deleted after the conclusion of the assessment

Use of this document

This document and its contents are published under a Crown Copyright and managed through the NCSC Cyber Essentials partner, IASME.

It is designed to support professionals prepare for an NCSC approved assessment.