CONDUCT CYBER SECURITY ASSESSMENT AND TESTING

UNIT CODE: SEC/OS/CS/CR/10/6/A

UNIT DESCRIPTION

This unit covers the competencies required to conduct security assessment and testing. It involves gathering information about organization and its systems, scan and mapping of network, enumerating network resources, exploiting known vulnerabilities, performing social engineering and preparing security assessment and testing report.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
1. Gather information about organization and its systems	1.1 Types of information required is established according line with the industry best practice 1.2 The nature of the target is determined in line with the information required 1.3 Search engines are considered in information gathering 1.4 Information gathering is conducted in adherence to the target social engineering 1.5 Information gathering is conducted in line with manufacturers guide of the source of the information 1.6 Organization operation platform is established in line industry best practice
2. Scan and map the network	2.1 Live hosts are identified as per the standard operation procedure 2.2 Network topology is drawn based on industry best practice 2.3 Services running on the live hosts are identified in line industry best practices 2.4 Vulnerable points are identified as per the services on the host
3. Enumerate target resources	3.1 Users are identified as per the standard operating procedure 3.2 Authorization credentials are established as per the organization ICT policy 3.3 Enumeration in services are established based on the organization policy

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
	3.4 Protocols enumeration is performed as per the standard operating procedure 3.5 Work groups are established in line with the network and active directory 3.6 Database is enumerated in line with industry best practice 3.7 Rainbow tables are designed based on industry best practice
4. Exploit known vulnerabilities	4.1 Exploits are deployed in line with industry best practice 4.2 Payloads are prepared and deployed in line with the environment and industry best practice and ethics 4.3 Deploying methods are established in line with the expected target 4.4 Access to remote host is maintained per standard operating procedure 4.5 Exploitation proof of concept is generated in line with the standard operating procedure
5. Perform social engineering	5.1 Methods of manipulating human emotion are exercised as per workplace procedures 5.2 System users are manipulated using the system as per the industry best practice 5.3 System is manipulated using third party vendors in line with industry best practice
6. Prepare security assessment and testing report	6.1 Security assessment and testing reports are prepared in line with the organizations approved format 6.2 Security assessment and testing reports are shared with relevant parties as per the organization policy 6.3 Security assessment and testing reports are documented and filled according organization filing system 6.4 Security assessment and testing risk mitigation recommendations are prepared and shared with the relevant parties

RANGE

This section provides work environments and conditions to which the performance criteria apply. It allows for different work environments and situations that will affect performance.

Variable	Range
	•

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Troubleshooting techniques
- ICT Infrastructure auditing procedures
- ICT safety and precautious measures
- ICT Prevention measures
- Performance monitoring techniques
- ICT policy
- Causes of hardware and software failure
- Components of ICT Infrastructure
- User training procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:	
• Communications (verbal and written); • Proficient in ICT; • Time management; • Analytical • Faults troubleshooting • Problem solving; • Planning;	• Decision making; • Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects	Assessment requires evidence that the candidate:

of Competency	1.1 Targets nature was determined in line with the information required 1.2 Types of information required was established according line with the industry best practice 1.3 Organization operation platform was established in line industry best practice 1.4 Network topology was drawn based on industry best practice 1.5 Vulnerable points were identified as per the services on the host 1.6 Protocol's enumeration was performed as per the standard operating procedure 1.7 Authorization credentials were established as per the organization ICT policy 1.8 Payloads were prepared and deployed in line with industry best practice and ethics 1.9 Exploitation proof of concept was generated in line with the standard operating procedure 1.10 System users were manipulated using the system as per the industry best practice
2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Practical demonstration 3.3 Observation
4. Context of Assessment	Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.