CYBER SECURITY ASSESSMENT AND TESTING

UNIT CODE: SEC/CU/CS/CR/7/5/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Conduct cyber security assessment and testing

Duration of Unit: 110 hours

Unit Description
This unit covers the competencies required to conduct cyber 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.

Summary of Learning Outcomes

1. Gather information about organization and its systems
2. Scan and map the network
3. Enumerate target resources
4. Exploit known vulnerabilities
5. Perform social engineering
6. Prepare security assessment and testing report

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods

1. Gather information about organization and its systems	• Meaning of terms
	• Information gathering and reconnaissance
	• Methods of information gathering
	  • Social engineering
	  • Search engines
	• Target mapping
	• Organization operation structures
		• Observation
		• Written tests
		• Oral questioning
		• Practical tests

2. Scan and map the network	• Meaning of terms • Probing and scanning • Drawing network topology • Services enumeration • Vulnerability assessment	• Observation • Written tests • Oral questioning • Practical tests
3. Enumerate target resources	• Meaning of terms • User identification and log in credentials • Service, protocol ,workgroup and database enumeration	• Observation • Oral questioning • Practical tests • Written tests

Learning Outcome	Content	Suggested Assessment Methods
	• Password cracking	
4. Exploit known vulnerabilities	• Meaning of terms • Payload preparation and deployment • Deploying methods • Deployment of exploits • Access to remote hosts maintenance • Proof of concepts	• Observation • Written tests • Oral questioning • Practical tests
5. Perform social engineering	• Meaning of terms • Information gathering • Social engineering technics • User and system manipulation	• Observation • Written tests • Oral questioning • Practical tests
6. Prepare security assessment and testing report	• Meaning of terms • Report preparation • Report dissemination • Report filing	• Observation • Written tests • Oral questioning • Practical tests

Suggested Methods of Instruction

- Demonstration by trainer
- Practice by the trainee
- Field trips
- Discussions

Recommended Resources

Equipment	Materials and supplies
• Computers • Printers • Cameras • Phones • Photocopiers	• Stationery •
Reference materials • Manufacturers' manuals • Relevant catalogues • Tables • National and international standards	