

CONDUCT SECURITY ASSESSMENT AND TESTING

ISCED UNIT CODE: 0612554 08A

TVET CDACC UNIT CODE: SEC/CU/CS/CR/08/5/MA

Relationship to Occupational Standards

This unit addresses the unit of competency: Conduct Security Assessment and Testing.

Duration of Unit: 150 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

Learning Outcomes	Durations (Hours)
1. Gather Information About Organization and its Systems	20
2. Scan and Map the Network	20
3. Enumerate Target Resources	20
4. Exploit Known Vulnerabilities	30
5. Perform Social Engineering	10
6. Conduct System hacking	40
7. Prepare Security Assessment and Testing Report	10
Total Hours	150

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Gather information about organization and its systems	1.1 Explain the importance of reconnaissance on a target system, network, or organization 1.2 Identify different types of reconnaissance: 1.2.1 Active 1.2.2 Passive. 1.3 Use OSINT (Open-Source Intelligence) tools to collect publicly available data. 1.4 Demonstrate the use of WHOIS lookup, DNS enumeration, and Google Dorking. 1.5 Utilise tools like Maltego, theHarvester, and Shodan for information gathering 1.6 Analyse email header and metadata for intelligence gathering	• Observation • Written tests • Oral questioning • Practical tests
2. Scan and map the network	2.1 Understand the purpose of network scanning for security, troubleshooting, and optimization. 2.2 Differentiate between various types of scans 2.2.1 ping scan 2.2.2 SYN scan 2.2.3 TCP scan 2.2.4 UDP scan 2.3 Use Nmap to discover live hosts, open ports, and services.	• Observation • Written tests • Oral questioning • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	2.4 Perform vulnerability scans 2.4.1 Nessus 2.4.2 OpenVAS 2.5 Interpret scan results to identify potential security gaps.	
3. Enumerate target resources	3.1 Enumerate Target Resources 3.2 Define enumeration and its role in cybersecurity and networking. 3.3 Conduct enumeration 3.3.1 File transfer enumeration 3.3.2 DNS enumeration 3.3.3 SMTP enumeration 3.3.4 Website enumeration 3.3.5 Remote connection enumeration 3.4 Perform LDAP and NetBIOS enumeration for directory services 3.5 Identify misconfigurations that could lead to privilege escalation	• Observation • Oral questioning • Practical tests • Written tests
4. Exploit known vulnerabilities	4.1 Use Metasploit Framework to exploit system vulnerabilities. 4.2 Demonstrate privilege escalation techniques on Windows and Linux based systems 4.3 Perform buffer overflow attacks and analyse the results. 4.4 Execute web-based attacks 4.4.1 SQL Injections 4.4.2 XSS 4.4.3 CSRF	• Observation • Written tests • Oral questioning • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
5. Perform social engineering	5.1 Define social engineering. 5.2 Identify different types of social engineering attacks 5.3 Analyse case studies of real-world social engineering attacks. 5.4 Conduct SET (Social-Engineer Toolkit) 5.4.1 Craft phishing emails. 5.5 Develop security awareness strategies to counter social engineering threats. 5.6 Understand ethical configurations and legal aspects of social engineering test	• Observation • Written tests • Oral questioning • Practical tests
6. Conduct System hacking	6.1 Explain the concept and objectives of system hacking in cybersecurity and IT system management 6.2 Demonstrate operating system exploitation techniques 6.2.1 privilege escalation 6.2.2 buffer overflow 6.2.3 kernel vulnerabilities. 6.3 Utilise password cracking tools 6.3.1 brute force 6.3.2 dictionary 6.3.3 rainbow table attacks. 6.4 Analyse hacking tools and frameworks to assess system vulnerabilities. 6.4.1 Metasploit	•

Learning Outcome	Content	Suggested Assessment Methods
	6.5 Deploy keylogging and spyware techniques to capture user credentials and monitor system activity. 6.6 Execute pivoting techniques to move laterally within a compromised network and escalate access privileges. 6.7 Apply methods for covering tracks 6.7.1 log manipulation 6.7.2 anti-forensics techniques 6.7.3 rootkits. 6.8 Implement system hacking countermeasures to mitigate threats. 6.8.1 intrusion detection 6.8.2 endpoint protection 6.9 patch management	
7. Prepare security assessment and testing report	7.1 Explain the significance of assessment and testing reports. 7.2 Document vulnerabilities and their impact based on CVSS scores. 7.3 Structure a professional security assessment report with findings and recommendations. 7.4 Utilise automated reporting tools in assessment and testing. 7.5 Develop remediation strategies based on industry best practice 7.5.1 OWASP 7.5.2 NIST	• Observation • Written tests • Oral questioning • Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	7.5.3 ISO 27001 7.6 Present security findings to technical and non-technical stakeholders.	

Suggested Methods of Instruction

- Instructor led facilitation of theory
- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Group discussions

Recommended Resources

S/No.	Category/Item	Description/ Specifications	Quantity	Recommended Ratio (Trainee: Item)
A	Learning Materials			
1.	Textbooks		13 pcs	13:1
2.	Installation manuals		5pcs	5:1
3.	Charts			
4.	PowerPoint presentations	For trainer's use		
B	Learning Facilities & infrastructure			
5.	Lecture/theory room		1	25:1
6.	Computer Laboratory		1	25:1
7.	Internet Connection			
C	Consumable materials			
8.	Printing papers		1 ream	1:20
9.	Toners		2 pcs	13:1
10.	Assorted colour of whiteboard			

	markers			
D	Tools and Equipment			
11.	Computers/Smartphones		25 pcs	1:1
12.	Projector		1 pc	25:1
13.	VMware/Oracle virtual box		25 pc	1:1
14.	Kali Linux or Parrot OS		25 pc	1:1
15.	Windows 11		25 pc	1:1