

CONDUCT SECURITY ASSESSMENT AND TESTING

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

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.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT	PERFORMANCE CRITERIA
These describe the key outcomes which make up workplace function.	These are assessable statements which specify the required level of performance for each of the elements. <i>(Bold and italicised terms are elaborated in the Range)</i>
1. Gather information about organization and its systems	1.1 Organizational policies, procedures, and compliance requirements are reviewed to understand the security context. 1.2 Business processes, critical assets, and data flows are identified to determine assessment scope. 1.3 Hardware, software, and network infrastructure components are documented for security evaluation. 1.4 User roles, access privileges, and authentication mechanisms are reviewed to assess potential risks. 1.5 Existing security controls and previous assessment reports are collected for reference. 1.6 Threat landscape relevant to the organization's industry and environment is analyzed. 1.7 Information gathering methods (interviews, questionnaires, document reviews, system scans) are applied to ensure comprehensive data collection.
2. Scan and map the network	2.1 Network scanning objectives and scope are defined in line with organizational policies and assessment requirements. 2.2 Approved scanning tools (e.g., Nmap, Nessus,

	OpenVAS, Wireshark) are selected based on assessment needs. 2.3 Network discovery scans are conducted to identify active hosts, IP addresses, and connected devices. 2.4 Port scanning is performed to detect open, closed, and filtered ports on network devices. 2.5 Services and applications running on detected hosts are enumerated and documented. 2.6 Network topology is mapped to illustrate connections, pathways, and data flows. 2.7 Scanning results are validated to minimize false positives and ensure accuracy. 2.8 Findings are documented securely and shared with authorized stakeholders.
3. Enumerate target resources	3.1 Enumeration scope is defined to identify systems, services, and resources within the target environment. 3.2 Enumeration tools (e.g. Netcat, Nmap scripts, SMB enumeration, SNMPwalk, LDAP queries) are selected based on target systems. 3.3 User accounts, groups, and roles are enumerated to assess access privileges. 3.4 Network shares, directories, and services are identified and documented. 3.5 System banners, software versions, and configurations are collected for vulnerability analysis. 3.6 Third-party services, APIs, and applications connected to the target system are identified. 3.7 Enumeration findings are analyzed to reveal potential attack vectors. 3.8 Results are validated, documented, and shared with authorized stakeholders for further testing.

4. Exploit known vulnerabilities	4.1 Identified vulnerabilities are reviewed and prioritized based on severity, exploitability, and potential business impact. 4.2 Exploitation activities are planned in line with organizational policies, rules of engagement, and legal requirements. 4.3 Approved penetration testing tools and frameworks (e.g., Metasploit, Burp Suite, SQLmap) are selected for exploitation. 4.4 Exploits are executed in a controlled manner to validate the existence of vulnerabilities without disrupting business operations. 4.5 Exploitation attempts are monitored and documented, including successful access, privilege escalation, or data exposure. 4.6 Evidence of exploitation (screenshots, logs, payload outcomes) is collected securely for reporting. 4.7 Exploitation results are analyzed to determine potential risks and system weaknesses. 4.8 Findings are reported to stakeholders with recommendations for remediation.
5. Perform social engineering	5.1 Social engineering scope and objectives are defined in line with organizational policies, legal, and ethical guidelines. 5.2 Human-based attack vectors (e.g., phishing, pretexting, baiting, impersonation) are identified for testing. 5.3 Social engineering tools and techniques (e.g., phishing simulators, phone-based pretexting, onsite physical tests) are selected and approved. 5.4 Controlled social engineering exercises are carried out to assess employee awareness and adherence to security policies.

	5.5 User responses to social engineering attempts are monitored, recorded, and analyzed. 5.6 Findings are documented, including vulnerabilities in human behaviour, processes, or training gaps. 5.7 5.7. Recommendations for security awareness training and procedural improvements are provided to mitigate identified risks. 5.8 5.8. Results are communicated to stakeholders in a confidential and constructive manner.
6. Conduct System hacking	6.1 System hacking activities are planned and approved in line with organizational policies, scope, and legal requirements. 6.2 Attack vectors (password cracking, privilege escalation, session hijacking, malware injection) are identified based on assessment objectives. 6.3 Approved ethical hacking tools and techniques (e.g., Metasploit, Hydra, John the Ripper, keyloggers in controlled environments) are utilized. 6.4 System vulnerabilities are exploited in a controlled manner to gain unauthorized access and escalate privileges. 6.5 System defenses (antivirus, intrusion detection, access controls) are tested to evaluate their effectiveness. 6.6 Evidence of successful exploitation, privilege escalation, or data compromise is documented securely. 6.7 Risks and impacts of system hacking activities are analyzed and reported to stakeholders. 6.8 Recommendations for hardening systems against hacking attempts are provided.
7. Prepare security assessment and testing report	7.1 Social engineering scope and objectives are defined in line with organizational policies, legal, and ethical

	guidelines. 7.2 Human-based attack vectors (e.g., phishing, pretexting, baiting, impersonation) are identified for testing. 7.3 Social engineering tools and techniques (e.g., phishing simulators, phone-based pretexting, onsite physical tests) are selected and approved. 7.4 Controlled social engineering exercises are carried out to assess employee awareness and adherence to security policies. 7.5 User responses to social engineering attempts are monitored, recorded, and analyzed. 7.6 Findings are documented, including vulnerabilities in human behavior, processes, or training gaps. 7.7 Recommendations for security awareness training and procedural improvements are provided to mitigate identified risks. 7.8 Results are communicated to stakeholders in a confidential and constructive manner.
--	---

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
ICT infrastructure components may include but not limited to:	• Hardware • Software • Network infrastructure
Threat landscape may cover but not limited to:	• Industry-specific risks • Environmental risks • Emerging threats • Known vulnerabilities
Scanning tools may include but not limited to:	• Nmap • Nessus

Variable	Range
	• OpenVAS • Wireshark
Enumeration scope may include but not limited to:	• Systems • Services • Resources • Network shares and directories
Penetration testing tools may include but not limited to:	• Metasploit • Burp Suite • SQLmap
Exploitation activities may include but not limited to:	• Access attempts • Privilege escalation • Data exposure evidence
Social engineering tools and techniques may include but limited to:	• Phishing simulators • Phone pretexting tools • Onsite testing
Report compliance may include but not limited to:	• Organizational policies • Contractual requirements • Legal standards • Regulatory obligations

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Knowledge of hardware, software, and network infrastructure components and their role in organizational security.
- Understanding of industry-specific risks, environmental risks, emerging threats, and known vulnerabilities that may impact systems and data.
- Skills in using tools such as Nmap, Nessus, OpenVAS, and Wireshark to identify vulnerabilities and analyze network/system security.
- Ability to enumerate systems, services, resources, and network shares/directories to gather technical intelligence for security assessment.

- Practical competence in the use of tools such as Metasploit, Burp Suite, and SQLmap to simulate real-world attacks.
- Knowledge of exploitation techniques including system access attempts, privilege escalation, and identifying evidence of data exposure.
- Understanding of social engineering tools and techniques such as phishing simulators, phone pretexting, and onsite testing to assess human-related vulnerabilities.
- Knowledge of organizational policies, contractual requirements, legal standards, and regulatory obligations to prepare compliant security assessment reports.

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:

- Communications (verbal and written);
- Proficient in Digital literacy;
- 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 of Competency	Assessment requires evidence that the candidate: 1.1 Organizational policies, procedures, and compliance requirements were reviewed and documented to determine the security context. 1.2 Hardware, software, and network infrastructure components were documented for evaluation. 1.3 Threat landscape relevant to the organization's industry and environment was analyzed and documented. 1.4 Approved scanning tools (Nmap, Nessus, OpenVAS,
-----------------------------------	--

	Wireshark) were selected and documented. 1.5 Network discovery scans were conducted and documented to identify active hosts, IP addresses, and connected devices. 1.6 Port scanning results were documented to show open, closed, and filtered ports. 1.7 Network topology was mapped and documented to illustrate connections, pathways, and data flows. 1.8 Scope of enumeration was defined and documented to identify systems, services, and resources. 1.9 Network shares, directories, and services were identified and documented. 1.10 Results were validated, documented, and shared with authorized stakeholders. 1.11 Enumeration findings were analyzed, documented, and mapped to potential attack vectors. 1.12 Approved penetration testing tools and frameworks (Metasploit, Burp Suite, SQLmap) were selected and documented. 1.13 Exploitation attempts were monitored and documented, including evidence of access, privilege escalation, or data exposure. 1.14 Scope and objectives of social engineering activities were defined and documented in line with policies, legal, and ethical guidelines. 1.15 Human-based attack vectors (phishing, pretexting, baiting, impersonation) were identified and documented for testing. 1.16 Approved tools and techniques (phishing simulators, phone pretexting, onsite tests) were selected and documented. 1.17 Findings were documented, highlighting vulnerabilities in human behavior, processes, or training gaps. 1.18 Results from information gathering, scanning, enumeration, exploitation, and social engineering were compiled and documented into a structured report.
--	--

	1.19 Recommendations for remediation, mitigation, and security improvements were documented. 1.20 Report was reviewed and documented to ensure compliance with organizational policies, contracts, and legal requirements. 1.21 Final report was documented, stored securely, and archived in line with organizational and regulatory standards.
2. Resource Implications for competent 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.