EISA COMPUTER-BASED ASSESSMENT: CYBERSECURITY (3 HOURS)

This External Integrated Summative Assessment (EISA) evaluates competencies across ELOs 1-5 from the Cybersecurity qualification. Candidates demonstrate COMPUTER-BASED skills in risk analysis, threat protection, monitoring, response, and recovery in simulated scenarios.1

Assessment Instructions

· Duration: 3 hours (180 minutes).

· Resources: Computer with internet access (simulated environment), provided tools (e.g., Wireshark, firewall software, backup utilities).

· Tasks: 4 integrated COMPUTER-BASED tasks building on a central scenario of a mid-sized South African company (TechSecure Ltd) facing escalating cyber threats.

· Submission: Screenshots, reports, and configurations saved in a zipped folder labeled with candidate ID.

· Marking: Total 100 marks; pass mark 60%.2

MARKING GUIDELINE – EISA COMPUTER-BASED ASSESSMENT: CYBERSECURITY

Task 1: Risk Analysis and Vulnerability Scan (45 minutes, 25 marks)

Requirements:

• Scan the simulated network using Nmap or OpenVAS; identify top 5 risks.
Top 5 risks identified:

1. Open port 22 (SSH) exposed to external network allowing brute force attacks
2. Open port 3389 (RDP) exposed increasing risk of remote compromise
3. Phishing attack leading to credential harvesting
4. Unpatched MySQL vulnerability (CVE-2023-1234) enabling database exploitation
5. Reconnaissance scanning activity from IP 192.168.1.100 indicating pre-attack mapping

• Document vulnerabilities with CVSS scores and potential impacts (e.g., data breach leading to R5 million fine).

Example vulnerabilities with CVSS and impact:

- CVE-2023-1234 (MySQL) – CVSS 9.8 (Critical): Full database compromise, data breach, POPIA fines up to R10 million

- Open RDP Port – CVSS 8.1 (High): Unauthorized remote access, ransomware deployment
- Weak credentials from phishing – CVSS 8.5 (High): Account takeover and lateral movement
- SSH brute force exposure – CVSS 7.5 (High): Server compromise
- DoS vulnerability – CVSS 6.5 (Medium): Service disruption and downtime losses

• Recommend patches and configurations (e.g., disable RDP if unused).

Recommended controls:

- Apply MySQL security patch for CVE-2023-1234
- Disable RDP (port 3389) or restrict via VPN
- Implement firewall rules to block suspicious IP 192.168.1.100
- Enforce strong password policies and MFA
- Conduct phishing awareness training

Task 2: Threat Protection and Mitigation (45 minutes, 25 marks)

Requirements:

• Configure a virtual firewall (e.g., pfSense) to block malicious IPs and enable IDS rules.

Firewall configuration:

- Block IP 192.168.1.100
- Enable IDS/IPS (Snort/Suricata) rules for SYN flood detection
- Configure rate limiting and port filtering for SSH and RDP
- Enable logging and alerts for suspicious traffic

• Implement endpoint protection: Encrypt sample data files with AES-256 and set up multi-factor authentication simulation.

Endpoint protection implemented:

- Files encrypted using AES-256 encryption standard
- MFA enabled using password + OTP (simulated authenticator)

- Endpoint antivirus/anti-malware enabled and updated

• Test and verify mitigation effectiveness.

Verification results:

- Malicious IP successfully blocked
- SYN flood attempts dropped by firewall
- Unauthorized login attempts denied due to MFA
- Malware signatures detected and quarantined

Task 3: Monitoring and Incident Response (45 minutes, 25 marks)

Requirements:

• Set up monitoring with Wireshark or Snort; capture and analyze traffic for anomalies.

Monitoring results:

- Captured abnormal traffic patterns indicating lateral movement
- Identified repeated login attempts and unusual SMB traffic
- Detected ransomware communication signatures

• Execute incident response: Isolate affected systems, notify stakeholders per policy.

Incident response actions:

- Isolated infected machines from network
- Disabled compromised user accounts
- Notified IT management and compliance team
- Initiated containment procedures to stop spread

• Log actions aligning with cybersecurity ethics and governance (e.g., no data tampering).

Ethical and governance actions:

- Maintained integrity of evidence (no alteration of logs)
- Documented all actions taken during response
- Ensured confidentiality of sensitive client data
- Followed incident response policy and POPIA compliance requirements

Task 4: Recovery Protocols (45 minutes, 25 marks)

Requirements:

• Restore from offsite backup using tools like Veeam or rsync; compare pre/post hashes.

Recovery actions:

- Restored data from offsite backup
- Verified integrity using hash comparison (SHA-256)
- Confirmed restored data matches original baseline

• Differentiate backup (proactive copies) vs. recovery (restoration process); document steps.

Backup vs Recovery:

- Backup: Regular copying of data to secure storage to prevent loss

- Recovery: Process of restoring data after failure or attack
  Steps followed:

1. Identify clean backup
2. Restore systems
3. Verify integrity
4. Resume operations

• Validate system functionality and update recovery plan for future (e.g., 3-2-1 rule).

Validation and improvements:

- Systems tested and confirmed operational
- Applications and databases functioning correctly
- Updated recovery plan to include 3-2-1 backup rule (3 copies, 2 media types, 1 offsite)
- Implemented frequent backup intervals to meet RPO of 4 hours