Unit 3 Study Guide: Cyber Security Testing and Controls

1.1 Different Types of Cyber Security Testing

Cyber security testing helps find weaknesses in systems, applications, and networks before attackers can exploit them.
Here are the main types:

1. **Vulnerability Scanning** – Automated tools scan systems for known weaknesses or outdated software.
2. **Penetration Testing (Pen Test)** – Ethical hackers simulate real attacks to test how well defences work.
3. **Network Testing** – Checks routers, firewalls, and connections for weak spots or misconfigurations.
4. **Application Testing** – Focuses on web and mobile apps to detect coding flaws like SQL injection or cross-site scripting.
5. **Social Engineering Testing** – Tests how users respond to phishing emails or fake calls.
6. **Wireless Security Testing** – Examines Wi-Fi networks for poor encryption or weak passwords.
7. **Configuration Reviews** – Ensures systems follow security best practices.
8. **Physical Security Testing** – Checks physical access controls such as locks, badges, and CCTV systems.

1.2 Why Cyber Security Testing is Important

- Helps discover weaknesses before attackers do.
- Protects sensitive data and reduces the chance of breaches.
- Ensures compliance with laws and industry standards (like GDPR or ISO 27001).
- Builds trust with customers and partners.
- Saves money by preventing costly cyber incidents.
- Strengthens overall security awareness in the organisation.

1.3 Comparing Types of Cyber Security Testing

Testing Type	Purpose	Method	Example
Vulnerability Scan	Find known issues	Automated tools	Nessus scan of company
Penetration Test	Simulate real	Manual & automated	Ethical hacker testing web
Social Engineering Test	Assess human behaviour	Phishing or phone scam tests	Fake email to test staff response
Network Test	Check network	Port scanning, firewall	Testing open ports on
Application Test	Find software bugs	Code review & attack simulation	Testing login forms for weaknesses

Summary:
Automated scans are quick and broad, while penetration tests are deeper and more realistic. Human testing adds insight that automation can miss.

1.4 Mitigations After Cyber Security Testing

After testing, organisations must act to fix what was found.
Common mitigation steps include:

- **Patch vulnerabilities** by updating software and operating systems.
- **Change configurations** to close open ports or disable weak settings.
- **Strengthen passwords** and enable multi-factor authentication.
- **Improve training** to reduce human error.
- **Review policies** to ensure future compliance.
- **Update firewalls** and intrusion detection systems.

1.5 Why Retesting is Important

- To confirm that all fixes actually work.
- New issues can appear after changes are made.
- Ensures long-term security, not just short-term fixes.
- Builds confidence that the system is safe to use again.

Example:
After applying patches to remove vulnerabilities, a follow-up scan ensures those weaknesses are truly gone.

1.6 How Cyber Security Testing Outcomes Can Be Reported

Reports should be clear and professional.
They often include:

- **Summary of findings** (what was tested and why).
- **List of vulnerabilities** ranked by severity.
- **Evidence** (screenshots, log entries, or test results).
- **Recommended actions** to fix issues.
- **Timeline** for improvements.

1.7 Why Testing Outcomes Must Be Reported

- Ensures accountability and transparency.
- Helps management understand business risks.
- Supports compliance with data protection laws.
- Guides future investments in cyber security.
- Provides evidence for audits or certifications.

2.1 Identifying Cyber Security Vulnerabilities

A **vulnerability** is any weakness that could be exploited by an attacker.
Ways to identify vulnerabilities:

- Run vulnerability scans and audits.
- Review access controls and configurations.
- Analyse system logs for unusual activity.
- Collect threat intelligence from trusted sources.
- Listen to user feedback and bug reports.

2.2 Steps When a Vulnerability is Found

1. **Record** the issue clearly with evidence.
2. **Assess** its risk level (low, medium, high, critical).
3. **Notify** responsible teams or management.
4. **Develop** a plan to patch or mitigate it.

5. **Apply** the fix safely and test again.

6. **Document** all actions taken.

2.3 Apply the Correct Response

Response depends on risk:

- **High-risk vulnerabilities** – fix immediately.
- **Medium risk** – plan and patch soon.
- **Low risk** – monitor or fix during routine maintenance.
  Always prioritise based on potential impact to data and systems.

2.4 Develop Communication to Mitigate Future Vulnerabilities

- Share lessons learned with all staff.
- Provide regular security awareness training.
- Issue internal security bulletins.
- Encourage employees to report suspicious activity.
- Work with suppliers to improve shared security practices.

3.1 Identify Cyber Security Controls

Controls are safeguards used to protect systems.
They can be grouped as:

- **Technical controls:** Firewalls, antivirus, encryption, access control.
- **Administrative controls:** Policies, training, background checks.
- **Physical controls:** Locks, cameras, entry systems.

3.2 Explain a Basic Cyber Security Framework

A **cyber security framework** is a structured way to manage risk.
Common frameworks include:

- **NIST Cybersecurity Framework** (Identify, Protect, Detect, Respond, Recover)
- **ISO/IEC 27001** (International standard for information security)
- **CIS Controls** (List of best practices for organisations)

Frameworks help organisations plan, implement, and measure cyber security performance.

3.3 Evaluate a Cyber Security Framework

When evaluating a framework:

- Check how well it fits your organisation’s size and risk level.
- Look at cost, complexity, and compliance needs.
- Review how clearly it defines roles, actions, and reporting.
- Ensure it helps improve resilience and incident response.

Example:
A small business might prefer CIS Controls for simplicity, while a large company could adopt ISO 27001 for certification.

4.1 How to Apply Controls

- Identify risks and choose suitable controls.
- Configure systems to enforce policies.
- Educate users about new procedures.
- Monitor systems to ensure controls remain active.

4.2 Implement a Basic Cyber Security Control

Example:
Control: Enabling multi-factor authentication (MFA).
Implementation Steps:

1. Choose an MFA method (e.g., app, SMS, hardware key).
2. Enable MFA on key systems (email, admin accounts).
3. Train users on setup and recovery.
4. Test regularly to confirm it works.

4.3 Justify the Implementation

Explain why the control was chosen:

- Reduces risk of stolen passwords.
- Easy to use and cost-effective.
- Meets compliance or audit requirements.
- Strengthens account protection.

4.4 Why a Control Might Not Be Applied

Sometimes controls can’t be applied because:

- Legacy systems don’t support modern security features.
- Cost or resource limits.
- Business disruption concerns.
- Need for compatibility with third-party software.

When this happens, organisations should use **compensating controls**, like stronger monitoring or restricted access.

Summary

Unit 3 focuses on testing, finding, and fixing weaknesses before attackers do.
It also teaches how to apply the right controls, report results, and continuously improve security.
Cyber security is not a one-time task it is a cycle of **testing, patching, retesting, and reporting** to keep systems safe and compliant.