**Week 3 Overview: Vulnerability Assessments and Scanning**

This week focuses on **vulnerability assessments**, from basic processes like **Cyber Essentials** to more advanced **penetration testing** approaches. You will learn how to use scanning tools to identify weaknesses in a network or website, analyze the results, and create a **professional vulnerability assessment report**.

**Key Learning Areas**

**1. Approaches to Vulnerability Assessments**

* Understand different **vulnerability assessment methods**, ranging from:
  + **Paper-based processes**, like Cyber Essentials.
  + **Automated vulnerability scans** using open-source tools.
  + **Crest-certified penetration tests** for deeper, professional-level testing.
* Learn when to **apply each approach** depending on the type and size of the organization being tested.

**2. Scanning and Testing Tools**

* Use open-source network scanning tools such as:
  + **Traceroute** – to track the path of data packets and identify network delays.
  + **Dig and nslookup** – to gather information about DNS records, mail servers (MX records), and hosting details.
* Identify key information like:
  + Number of hops between your computer and the target site.
  + Where the biggest network delays occur.
  + Main domain servers and registered contacts.
  + Hosting locations and infrastructure details.

**3. Analyzing Results and Reporting**

* **Interpret scan results** to find possible security vulnerabilities.
* **Create a baseline audit document** that will:
  + Serve as the foundation for deeper penetration tests later in the course.
  + Highlight potential risks and weaknesses.
  + Recommend strategies to mitigate vulnerabilities.

**Practical Activities**

* **Scanning Activity:**  
  Practice using traceroute, dig, and nslookup to collect network data about an assigned website.
* **Prepare for the Breach Analysis Seminar:**  
  Review materials in Unit 4 to discuss your findings.
* **Module Wiki Updates:**  
  Share important terms, tools, or insights with your peers.
* **Vulnerability Assessment Assignment:**
  + Produce a **600-word analysis report** accounting for **30% of your grade**.
  + Your report must include:
    - Identified vulnerabilities and relevant security standards (e.g., GDPR).
    - A list of tools to be used with clear justifications.
    - Potential business impacts of running scans (e.g., during or outside business hours).
    - Recommendations to address the most critical risks.
    - A timeline for assessment and testing.

*This report lays the groundwork for a more detailed****executive summary****in Unit 6.*

**Assignment Evaluation Criteria**

The report will be graded in four main areas (each weighted at 25%):

1. **Knowledge & Understanding:**  
   Research-based analysis of vulnerabilities and security challenges.
2. **Application of Knowledge:**  
   Choosing and justifying appropriate scanning tools.
3. **Criticality:**  
   Identifying tool limitations, assumptions, and outlining a timeline for assessments.
4. **Presentation & Structure:**  
   Professional formatting, accurate referencing, and clear communication.

*Use tables and bullet points to keep your report concise and within the word count.*

**Learning Outcomes by the End of Week 3**

You will be able to:

1. **Select the right assessment approach** for different types of organizations.
2. **Use open-source scanning tools** to perform vulnerability tests.
3. **Analyze scanning results** and recommend solutions to address vulnerabilities.
4. **Create professional reports** that summarize findings and provide actionable security improvements.

**In summary**, Week 3 equips you with the **practical skills and theoretical knowledge** to conduct vulnerability assessments, analyze network weaknesses, and effectively communicate your findings to stakeholders. This lays the foundation for more advanced penetration testing and risk management later in the module.