**Week 5 Overview: Logging, Forensics, and Future Trends**

This week focuses on **logging** and **forensics**, two key areas in **investigating and resolving security breaches**. You will learn how to configure logging on different operating systems, explore best practices for collecting and analyzing log data, and gain hands-on experience with **forensic tools** to investigate network and system breaches.

**Key Learning Areas**

**1. Logging for Security and Monitoring**

* Understand the **role of logging** in detecting and investigating cyber incidents.
* Explore **differences between logging on Windows and Linux systems**, including:
  + Key logging tools for each operating system.
  + Challenges in interpreting logs due to system security features.
* Learn **best practices** for setting up logging to ensure accurate and useful data collection.
* Study **Windows logging basics** and centralized logging methods like **Syslog** (*Eaton, 2003; SolarWinds, 2020*).

**2. Forensics and Breach Investigations**

* Explore how **forensic tools** are used to:
  + Collect and analyze digital evidence from systems and networks.
  + Reconstruct events leading to a breach.
  + Identify compromised systems, attackers’ methods, and timelines.
* Practice analyzing sample data using forensic techniques to gain insights into real-world breach scenarios.

**3. Vulnerability Assessment Reporting**

* Review and critique a **sample vulnerability assessment report template** (*Purplesec*).
* Understand how to structure reports to meet **NCSC (National Cyber Security Centre)** guidelines for penetration testing preparation.
* Identify:
  + What works well in reporting.
  + What should be improved or revised for clarity and effectiveness.

**Practical Activities**

* **Lecturecast:**  
  Learn why logging is critical, how to set it up effectively, and common issues encountered in log analysis.
* **Collaborative Discussion 2 (Week 2):**  
  Continue debating **the benefits and risks of logging**, including vulnerabilities like **Log4j**, and support arguments with academic references.
* **Case Study – Reporting Template Review:**  
  Answer questions such as:
  + Does the template meet baseline requirements for penetration testing?
  + What are its two strongest features or examples?
  + What are two areas that could be improved?
* **Prepare for Next Week’s Debate:**  
  Teams will prepare **PowerPoint presentations** for a seminar on **Generative AI and its impact on network security**.
* **Module Wiki Updates:**  
  Share key insights, terms, and findings to support collaborative learning.

**Reflection and E-Portfolio**

* Record challenges faced during the activities and how you overcame them.
* Reflect on how these experiences will improve your final report.
* Add insights and evidence to your **e-portfolio** for assessment.

**Learning Outcomes by the End of Week 5**

By completing this unit, you will be able to:

1. **Set up and configure logging** for Windows and Linux systems effectively.
2. **Select and use forensic tools** to gather and examine digital evidence.
3. **Analyze log files and forensic data** to investigate breaches and identify security issues.
4. **Evaluate reporting practices**, ensuring they align with cybersecurity standards like NCSC.
5. **Apply critical thinking** to improve reporting, auditing, and breach investigation methods.

**Why This Week Matters**

Logging and forensics are at the **core of breach detection and response**.

* Logging provides the **evidence trail** needed to understand what happened during an attack.
* Forensics helps **reconstruct incidents** and supports legal and ethical decision-making.
* Strong reporting and analysis ensure organizations can **prevent future breaches** and strengthen their cybersecurity posture.

In summary, Week 5 equips you with the **technical and analytical skills** to monitor systems, investigate breaches, and create professional reports that meet cybersecurity standards.