**Week 4 Overview: Breach Analysis and Mitigation**

This week focuses on **understanding real-world security breaches**, learning how to **analyze attacks**, and exploring strategies to **mitigate future risks**. You will also be introduced to **Kali Linux**, a powerful suite of tools used for penetration testing and security assessments.

**Key Learning Areas**

**1. Understanding Security Breaches**

* Review **major data breaches** from recent years and analyze how they occurred (*Swinhoe, 2020*).
* Learn how to **identify weaknesses** that attackers exploit.
* Explore **real-world case studies**, considering:
  + What data was compromised.
  + Who was responsible and how the breach unfolded.
  + Whether escalation or spread was stopped in time.
  + Legal, ethical, and social consequences for organizations.

**2. Mitigating Security Threats**

* Discuss **strategies to prevent and respond** to common cyberattacks.
* Understand how **incident response plans** are developed and executed.
* Learn to **recommend appropriate defensive measures**, such as:
  + Firewalls and intrusion prevention systems.
  + Secure coding and patch management.
  + Staff awareness and training to reduce human error.

**3. Kali Linux and Penetration Testing Tools**

* Get hands-on experience with **Kali Linux**, a platform widely used for:
  + Scanning networks and websites.
  + Identifying vulnerabilities and open ports.
  + Detecting outdated or unpatched software.
  + Testing for known weaknesses in Content Management Systems (CMS).
* Evaluate which tools are most suitable for different types of security assessments (*Bhatt, 2018; Bhingardeve & Franklin, 2018*).

**Practical Activities**

**Collaborative Wiki Activity**

* Work with classmates to perform scans on your assigned website using Kali Linux.
* Answer key questions such as:
  + Which operating system and web server are in use?
  + Does the site use a CMS like WordPress or Drupal?
  + What protections are in place (firewall, proxy, CDN)?
  + Are there open ports, and are they expected?
  + Are there known vulnerabilities or outdated software versions?
* Share results and troubleshooting tips in a **group wiki** with:
  + **FAQ section:** Post and answer common questions.
  + **Results section:** Share scan findings for group review and feedback.

**Breach Analysis Case Study Seminar**

* Select a real-world breach and complete a **breach checklist**, including:
  + Type of data affected.
  + Timeline of events.
  + Escalation and containment actions.
  + Notification of authorities (e.g., ICO).
  + Social, legal, and ethical implications.
* Present how you would have responded as the Information Security Manager (ISM) to prevent future incidents.

**Collaborative Discussion 2**

* Debate the **pros and cons of logging** in security, with a focus on:
  + The benefits of logging for tracking security issues.
  + The risks of logging, such as vulnerabilities like **Log4j**.
* Support your arguments with academic references (*Berger, 2024; Nyangaresi et al., 2024*).

**Learning Outcomes by the End of Week 4**

By the end of this unit, you will be able to:

1. **Describe typical breach attacks** and understand how they occur.
2. **Propose mitigations** to prevent or reduce the impact of future attacks.
3. **Use Kali Linux tools** to identify security weaknesses and analyze systems.
4. **Evaluate and select appropriate tools** for different testing scenarios.
5. **Understand the legal, social, and ethical issues** surrounding cybersecurity breaches.
6. **Collaborate effectively** through wikis and discussions to share findings and insights.

**Why This Week Matters**

Week 4 bridges **theory and practice**:

* You’ll apply the skills learned in previous weeks to **real-world scenarios**.
* Gain **hands-on experience** using professional penetration testing tools.
* Build teamwork and communication skills by collaborating on shared projects.
* Develop a deeper understanding of both **technical defenses** and **organizational responsibilities** in cybersecurity.

In summary, Week 4 prepares you to **analyze security breaches**, **recommend effective mitigations**, and **use advanced security tools** to protect network systems against evolving cyber threats.