Seminar Session 2: STRIDE and DREAD tools

Outline:

- ➔ Announcements
- ➔ STRIDE & DREAD
- ➔ Seminar 2 Questions
- ➔ Reminders – Assessments
- ➔ Q&A

Announcements:

- ➔ Group Website Allocation: are provided. Have the same IP.
- ➔ Reminder for the group assessment in unit 6.
- ➔ Each group work with their own website.
- ➔ Participate with the module wiki.
- ➔ Formative Assessments:
    - Guidance towards main assessment → Peer Evaluation
    - Evidence for E-portfolio

Discussion:

Group 1 presentation (my group, ppt could be found in the Artefacts section)

- ➔ Feedback: Good demonstration of understanding.

Group 3 presentation:

Top three vulnerabilities:

1. Brute force attacks - high risk
2. Denial of Service (DoS) attack - medium risk
3. Security control - medium risk

Potential mitigations:

- WPA and WPS, Key reinstallation attack – should be replaced by WPA3
- Implement Content Distribution Network (CDN) and Web Application Firewall (WAF) could report abnormal traffic and block it.
- Use of zero-trust architecture.

Group 2 presentation:

Top three vulnerabilities:

1. Network Security Solutions → high risk

2. Network Protocols → medium risk

3. Unsecure Software → medium risk

Threat mitigation possibilities:

- Account Lockout
- Zero trust architecture
- IPS/IDS
- Packet filtering
- two factor authentication
- Honeypot
- Cyber training

Note: How can this be implemented in a real case and where for what expected benefit?

➔ Implementation of cost and benefit analysis to get a better understanding for the importance and practicability for a real case.