E-Portfolio: https://sam-tselapedi.github.io/CyberSecurity/nism.html

Network and Information Security Management: Reflective Essay

Global Citizenship and Leadership

The enthusiasm I had to study this module got challenged by the study group framework. I was aware that I would need to improve on skills required to function as a group member to promote cohesion and thrive. My team members and I struggled at first to establish ourselves as a functioning team. I needed to understand the intention and purpose of the university to arrange us in groups. I read an article titled "Group work as a form of assessment: Common problems and recommended solutions" (Davies, 2009).

I learned that the purpose was to develop transferable skills for life-long learning(teamwork, leadership, project management skills and communication skills).

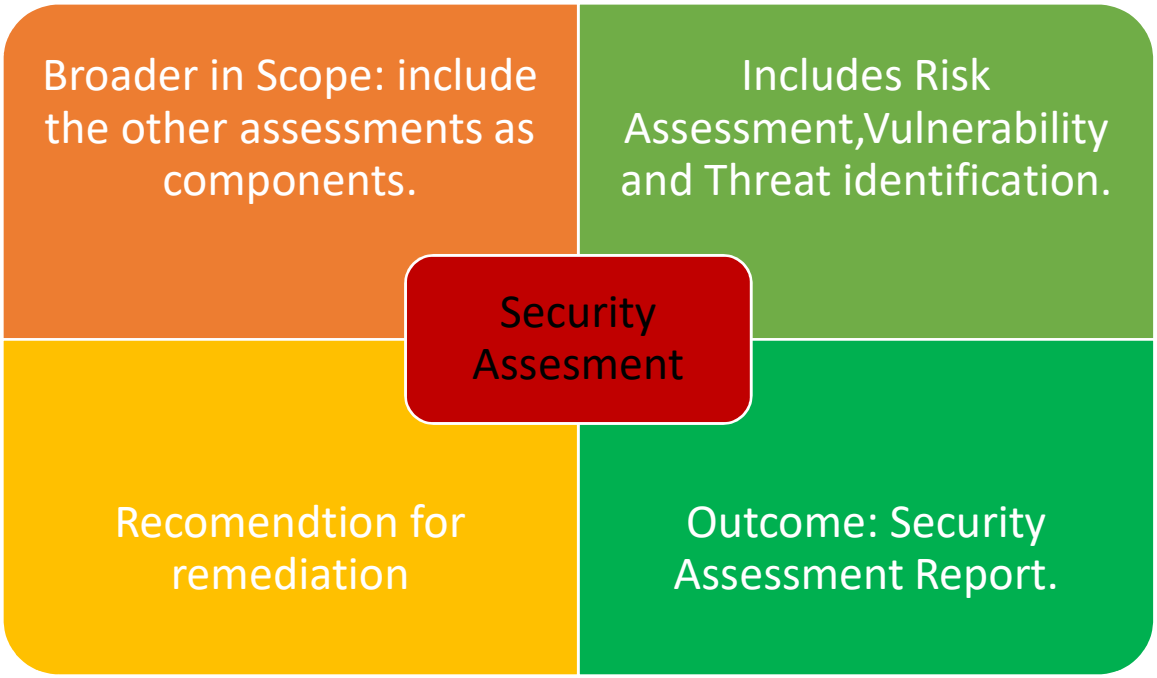
Unit 1-3: Reflection

Coming into this module, I had never used the Amazon AWS platform, although I am familiar with other virtualisation technologies such as Microsoft's Hype-V and VMWare. We experienced challenges with the web application. In troubleshooting the errors, I went through knowledge articles on how to resolve the permission error that prevented the system from coming up. Although we could not resolve the issue, I managed to learn more about the AWS platform. Most of the learning outcomes of the topics covered a revision for me because I have completed several network and information security before. However, while going through the 'Compromising a Medical Mannequin' research article, I reflected on the security flaws we have at my workplace. We are the largest pathology laboratory in South Africa. We do not see the security flaws in the medical testing instruments supplied by companies like Roche and Abbott. In most cases, we allow the device on the network without assessing threats that the medical testing instruments can introduce in our environment.

I have adopted a system thinking approach to assessing vulnerabilities and threats performing my duties. I was running my computer with the same credentials I use to manage the active directory domain, and I have since resorted to using a standard account for my computer.

Unit 4-6: Reflection

Security Assessment



Vulnerability Assessment and Testing

- Detect.
- Validate.
- Remediate.
- Document.

Network Discovery Scans — Scan a range of IP addresses for open ports.

- TCP SYN/ACK scanning
- Popular tool : Nmap

Network Vulnerability Scans — Uses a vulnerability database and signatures to check for known vulnerabilities on open ports.

- False Positive/Negative.
- Authenticated Scans
- Tools :Nessus,OpenVAS.

Web Vulnerability Scans — Scans web applications for web vulnerabilities,which are not typicall detected by network vulnerability scans.

- Scan all apps
- Scan applications before moving to production.
- Scan applications regularly.
- PCI-DSS/GPDR compliance require quartely audits or Web Application Firewall(WAF)
- Tools: Nikto,Acunetix,Burpsuite,Wapiti

Penetration Testing

<table>
<tr>
<td>Hazards of Pen Testing

• Application crashes.
• Data Corruption.
• Denial of Service.</td>
<td>Whitebox Test

• Complete knowledge of the system.
• Bypasses reconnaissance stage, reducing time.
• Increased likelihood of finding security flaws.</td>
<td>Blackbox Test

• No knowledge of the system.
• Simulate external attacker.
• Real-world results.</td>
<td></td>
<td>Testing Methodologies

• OWASP
• NIST
• OSSTMM
• FedRAMP
• PCI-DSS</td>
</tr>
<tr>
<td>Vulnerabilities are exploited in Pen-Test.

Exploitation is not a hazard.</td>
<td></td>
<td></td>
<td></td>
<td>If Pen-test detects an active compromise, report to the security contact.</td>
</tr>
<tr>
<td colspan="5">Tools : Metasploit,Core-Impact.Immunity Canvas | Plartforms : Kali Linux ,BactraTrackPentestTools</td>
</tr>
</table>

I had an awareness and knowledge about network security. However, after going through these study units, I have gained knowledge about the importance of securing coding in product development. It is encouraged that software developers adopt making security implicit when coding and not consider security controls when they have a finished product. While I have learned about software vulnerabilities such as SQL injection and cross-site scripting, I also realised the importance of securing the software installed on the appliances (virtual and physical) used to protect threatened assets such as firewalls and anti-malware applications.

Working as a team/group:

It was a good learning experience for me to work as a group with other individuals I have not worked with before. If was to work with the same group again, the one change that would make the group work together more effectively is communication skills. It was a challenge to get the group member to establish communication initially. I took the initiative to establish contacts amongst the group members and configured a Microsoft SharePoint portal for collaboration. The one skill I learned from working in a team is being initiative and taking leadership. We adopted conjunctive methodology to complete all assignments, and we divided and assigned tasks amongst each other. We demonstrated respect for the opinions of others in the group, and this assisted us in recovering and improving on the previous challenges we faced. Antonios is one member to give a specific compliment for coordinating and taking leadership when we had tasks to complete if I was to pick.

Final Project: Executive Summary

The final report produced contained a detailed outline of identified risks. To ensure that all key stakeholders understand the testing result, we highlighted key findings in non-technical terms. We included an analysis of the potential business impact to enable stakeholders to understand the priority levels of vulnerabilities identified. The report provided insight into exploitability difficulty. Exploitability difficulty is a closely related factor to implications for risk scoring. We then offered remediation advice, and remediations actions vary in complexity. Some can be fixed with patches or updates, while reconfiguration or coding change may be required; thus, we also provided details and references for the remediation actions.

Network and Information Security Management: Processes

Information systems architecture must meet business and security requirements. Security should be implicit into information systems by design. Security must be balanced with the business requirements; thus, a tradeoff will be required between security and business to achieve balance.

As a technical team member, I believe security can be achieved through the defence in depth by applying multiple controls at different levels around the protected asset. Change management is essential to evaluate the security impact of the proposed change. Security Incidents and Events Management should be included in the processes of managing and profiling security challenges.

Conclusion

This module was challenging and covered various topics, and I intend to use the knowledge I gained through studying this module. In particular, I would like to expand my knowledge and learn more about risk management, information security management, and information security governance in the future. Dr Nawaz Khan provided us with feedback on how he has observed student's writing. His observation was that we tend to do a descriptive essay with citations included when writing artefacts, and we do not express our views. I intend to work on improving my analytical and critical skills to improve on reflective academic writing.