Background

Collaborative Learning Discussion 1 is based on the paper "Compromising a Medical Mannequin", that analysis the cybersecurity gaps identified in the field of medical devices. As part of the core research, a team of undergraduate computing student team was given access to a medical training mannequin and challenged to compromise within a semester (four months). Students carried out brute force attacks and a denial of service

(DoS) attack. Brute force attacks were executed using BackTrack 5 from a live CD and using a virtual machine configuration. The denial of service attack was performed through a network protocol.

In addition to the discussion, based on the paper, a group activity also completed. The result from the group activity was presented in the seminar: STRIDE and DREAD tools. The activity was primarily focused on the DREAD assessment tool.

Learning Outcomes

✓Project management
✓Critical thinking and analysis
✓Problem-solving
✓Communication and Literacy skills
✓Various security solutions
✓Critical Reflection

Reflections

The reflection activity is completed using "ROLFE, FRESHWATER, & JASPER 'WHAT' MODEL".

Phase	Description
What	Based on the paper "Compromising a Medical Mannequin", students were asked to identify the significant threats and vulnerabilities discussed in the paper and necessary mitigation strategies. Also, students were tasked with a group activity to prepare and present a summary using the DREAD tool.
So What?	The students' assessments primarily focused on critical vulnerabilities discussed in the paper - brute force attack and denial of service attack. Even though some common themes related to remediation solutions were noted, like complex password policy for brute force attack, a range of solutions

	were discussed. Some of them were technical, and some of them were non-technical, like security awareness training. The remediation activities ranged from using a firewall for Denial Of Service (DoS) attack to security awareness training for social engineering attacks. See Summary Post related to Collaborative Learning Discussion 1 below in Artefacts section. The group activity helped to understand the real-world requirement to use the assessment tool – DREAD. In addition, the project management skills also utilised to complete the task for the seminar.
Now What?	Various remediation solutions and tools discussed during this collaborative learning can be learned profoundly and applied to numerous situations.

	Tools like DREAD and STRIDE can be applied in the future to perform an assessment. Last but not least, the project management technics can be applied going forward for future assessment.

Meeting Notes

During this engagement (Collaborative Learning Discussion 1), Group 1 had one critical meeting and numerous chats using Discord, a chat platform. During our meeting, we used the DREAD tool to identify the score for each security threat. The result was used to discuss during the seminar. The contract was developed using Discord chat, and Google Drive was used to share the ideas.

Professional Skills Matrix

During this module, I learned and developed my skills related to network assessment and security solutions and project management skills.

Summary

Even though this was an initial team activity, I inspired by the active engagement and participation from the students, specifically from Group1. In addition to various security solutions, project management skills such as time management, resources management, I learned from the assignment during the Team Contract development and development of the deliverable for the seminar: STRIDE and DREAD tools. This assignment also helped me to enhance my communication and literacy skills.

The only challenge associated with the assignment was to manage the scope of the discussion. This can be looked at as a total solution or looked at as a subset from a campus of a healthcare network. Based on the assumption, security threats and solutions can be different. We overcome the challenge by applying professional judgment, critical thinking and analysis to identify the "sweet spot" for our discussion.

The discussions demonstrated that the students were empowered to use their leadership skills to define the scope and solutions. A list of security solutions, discussed, shared and analysed. Specifically, I inspired by two of them for creative application, which I provided my review: 1) Firewall for DoS Attacks 2) Security Awareness Training for Social Engineering Attacks. Two peer reviews and a summary post for the assignment helped me improve my critical reflection skills.

Artefacts

Feedback perspective, related to Initial Post, Tutor highlighted to include the reference related to the original paper Compromising a Medical Mannequin, which I have addressed in the Summary Post.

Summary Post

Introduction

There is no better time to talk about protecting the medical industry from cyber thread than now. In December 2020, IBM warned the governments and organisations about the attacks targeted towards the corporations critical to the circulation of COVID-19 vaccines (CBC, 2020).

Last few weeks, students were actively engaged in a collaborative discussion generating a vast amount of ideas, views and solutions. This summary post is developed based on the learning through the discussions and team activities conducted for preparing the seminar titled "STRIDE and DREAD tools".

Background

The research paper Compromising a Medical Mannequin discusses various cybersecurity gaps identified in the domain of medical devices. As part of the core research, a team of undergraduate computing student team was given access to a medical training mannequin and challenged to compromise within a semester (four months). Students carried out brute force attacks and a denial of service (DoS) attack. Brute force attacks were executed using BackTrack 5 from a live CD and using a virtual machine configuration. The denial of service attack was performed through a network protocol.

Threat Modeling (STRIDE and DREAD)

Security threat modelling tools such as STRIDE and DREAD can be used to assess the potential threats and possible impact so that the solution can be secured before implementation.

STRIDE is a thread modelling tool and acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Security specialists can use this framework and mnemonic to identify the potential security threats and address those gaps before implementation. The STRIDE provides a structured method to identify all possible threats. However, prioritising the issues for remediation is not supported by STRIDE.

DREAD is a different thread modelling tool, and this acronym stands for discoverability, reproducibility, exploitability, affected users, and damage. Unlike STRIDE, DREAD can be used to prioritise security threats. Each factor (e.g. discoverability) for a given security threat can be given a score (for example, 1 to 10). The overall level of risk for the security threat is calculated by dividing the total factors by the number of factors. A higher score represents a high level of threat. Usually, during prioritisation, security threat with higher score should be addressed first.

Using STRIDE, organisations can identify the inventory of threats and remediation activities can be prioritised using DREAD.

Vulnerability 1: Brute Force Attack

Risks related to Brute force attacks can be mitigated by implementing various technical controls. Enforcing strong passwords with password complexity, implementing an account lockout policy with a limited number of login attempts and configuring time delays between login attempts are simple but effective technical controls. In addition, implementing security verification questions and enabling multi-factor authentication are a few other technical controls that can minimise the risks related to brute force attacks (O'DRISCOLL, 2020).

In addition, robust security awareness training can be utilised to manage the risks associated with brute force. Till also highlighted that security awareness training can be leveraged to manage the risks related to social engineering attack (Langbein, 2021)

Vulnerability 2: Denial of Service Attack

Hardening wireless systems using industry security benchmarks such as the Center for Internet Security (CIS) security benchmark can help to address the threads related to denial of service attack. In addition, restrict access to the network by filtering the media access control (MAC) address will minimise the risks associated with denial of service attack (CISA, 2020).

As Anum highlighted, solutions like firewalls also can be utilised to manage the risks related to Denial of Service Attack (Rashid, 2021).

Conclusion

Organisations should use systematic approaches to identify security threats and prioritise remediation activities. As noted above, each security threat can be remediated using various security solutions. Organisations must perform a comprehensive assessment considering each solution, pros, cons and limitations before selecting appropriate security solutions.

References:

CBC. (2020) Cyberattacks target COVID-19 vaccine distribution effort. Available from: https://www.cbc.ca/news/world/coronavirus-vaccine-distribution-ibm-warns-hackers-1.5826602 [Accessed 30 May 2021].

CISA. (2020) Securing Wireless Networks. Available from: https://us-cert.cisa.gov/ncas/tips/ST05-003 [Accessed 30 May 2021].

Glisson, W. B., Andel, T., McDonald, T., Jacobs, M., Campbell, M. and Mayr, J. (2015) 'Compromising a Medical Mannequin'.

Langbein, T. (2021) Initial Post. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=256170 [Accessed 30 May 2021].

O'DRISCOLL, A. (2020) What is a Brute Force Attack? Examples & How to Avoid Attacks. Available from:

https://www.comparitech.com/blog/information-security/brute-force-attack/ [Accessed 30 May 2021].

Rashid, A. (2021) Initial Post. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=256232 [Accessed 30 May 2021].