Within the article “Compromising a Medical Mannequin”, several critical ideas were brought up about the threats within the medical community. In particular, there has been a rise in cyber threats and the medical community is a major target. Unlike other fields that may be targeted, the medical community has significantly higher risks associated with possible attacks. An attack on a critical device, such as a pacemaker, could lead to someone’s death. As reported by the U.S. Food and Drug Administration (FDA), there have been known deaths or other complications due to attacks on medical devices yet (FDA, 2013, as cited in Glisson, 2015). Specifically as stated in the article, medical mannequin’s that are used for training students are shown to have significant vulnerabilities. The two main vulnerabilities are a weakness in the network security solution and the network protocol (Glisson, 2015). These two vulnerabilities were exploited through the use of brute force and denial of service attacks (Glisson, 2015).

Several ways can be used to help protect the mannequins and stop the threats to the system. One of the most common ways to stop brute force attacks is through account lockouts. This alone isn’t a foolproof solution though. It would be prudent to block the IP addresses of individuals who have failed several login attempts and can also only allow known IP addresses to sign in (Sheridan, 2021). Lastly, captcha would be effective in stopping automated attacks, as presented in the article (Sheridan, 2021).

For denial-of-service attacks, several methods can be used to prevent them. Packet filtering can be particularly effective in preventing the use of spoofed IP addresses (Mahjabin et al, 2017). Similar to brute force attack prevention, IP addresses identifications are still also effective. As well, IP hop filtering can be implemented to determine if the packets being sent are valid( Mahjabin et al, 2017). The implementation of a next-generation firewall could also be effective in securing the network that the mannequins are a part of. These firewalls include built-in intrusion protection systems(IPS) and Intrusion detections systems(IDS) (Thomason, 2012). With these devices, they will be able to actively monitor traffic and provide another layer of protection. Overall, despite the vulnerabilities within the mannequin’s, the medical community has several options available that they can use to secure them.

References:

Read Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) [Compromising a Medical Mannequin**.**](https://aisel.aisnet.org/amcis2015/HealthIS/GeneralPresentations/5/) Healthcare Information Systems and Technology (Sighealth).

Mahjabin, T., Xiao, Y., Sun, G., Jian, W. (2017) A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks.* 13(12): 1-33. Available from: <https://journals.sagepub.com/doi/pdf/10.1177/1550147717741463>

Sheridan, E.(2021) Blocking Brute Force Attacks.Available from: [https://owasp.org/www-community/controls/Blocking\_Brute\_Force\_Attacks#](https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks) [Accessed 12 November 2021].

Thomason, S. (2012) Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices. *Global Journal of Computer Science and Technology Network, Web & Security’.* 12(13): 1-5.Available from: <https://globaljournals.org/GJCST_Volume12/6-Improving-Network-Security-Next-Generation.pdf>