Network and Information Security Management November 2021 B

« Collaborative Learning Discussion 1

Pavendran Wimalendran

Initial Post

95 days ago

3 replies

Last 79 days ago

This article examines how medical equipment is growing increasingly reliant on technology, increasing the likelihood of being a target of cyber-attacks. A breach in medical environments, especially in training environments, can have a long-term ripple effect on the medical profession and potentially impact thousands of lives due to incorrect analysis of life-threatening critical data by medical personnel. (Gilsson, et al, 2015)

The two vulnerabilities revealed in this exercise were denial of service attacks (DOS) and brute force attacks, both of which were easily exploited with basic skills and tools against training medical equipment.

DOS attacks are carried out by flooding a target or network with unwanted traffic in order to prevent it from operating normally or rendering it unreachable (Z Chao-Yang - 2011). This can be avoided by monitoring and analysing network data for unusual activity and alerting the appropriate personnel to take action.

Brute force attacks are also characterised as 'trial and error' attacks because attackers test every possible combination of access credentials until they succeed (Stiawan, et al,2019). This can be avoided by implementing strong password policies, such as employing complicated passwords and locking accounts after a specific number of failed attempts, as well as monitoring user behaviour and alerting.

References:

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. Sighealth.

Z Chao-Yang. (2011) 'DOS Attack Analysis and Study of New Measures to Prevent'. Available from: https://ieeexplore.ieee.org/abstract/document/5997473/citations?tabFilter=papers [Accessed 12/11/2021]

Deris Stiawan, Mohd. Yazid Idris, Reza Firsandaya Malik, Siti Nurmaini, Nizar Alsharif, Rahmat Budiarto, (2019) "Investigating Brute Force Attack Patterns in IoT Network", Journal of Electrical and Computer Engineering. Available from: **https://www.hindawi.com/journals/jece/2019/4568368/** [Accessed 13/11/2021]

Reply

Maximum rating: -

3 replies

1 

Post by **Grace Clarke**

87 days ago

Peer Response

Hi Pavendran,

Thank you for your informative post outlining the major threats and vulnerabilities within the paper, it is interesting that the students were able to successfully exploit the system with little to no training.

Your opening paragraph highlighted that a breach in medical environments can have long term far reaching impacts, having thought about this, attacks of this type could cause medical students to misdiagnose patients, which could potentially be life threatening. Therefore it is essential as Nawaz highlighted in my post that these attacks are proactively prevented and not investigated after a breach has taken place, therefore highlighting the use of logging and monitoring tools as a preventative to these attacks.

As you mentioned DOS attacks can be prevented by monitoring for unwanted traffic, such as by using firewalls. Alice pointed out that these firewalls can sometimes be ineffective as hackers are finding new ways to overcome them. Developing on Alice's point further a way to mitigate this is to use AI for firewalls, for example they can use intelligent detection technologies to improve the capability of detecting advanced threats and unknown threats.

The AI firewall uses the intelligent detection engine to train threat detection models based on massive samples and continuously optimize the models based on real-time traffic data, improving threat detection capabilities (Shui, 2021).

References

Shui, L., 2021. *What Is an AI Firewall? AI Firewalls vs. NGFWs - Huawei*. [online] Huawei. Available at: [Accessed 21 November 2021].

Reply

2  Reply to  Grace Clarke from Nawaz Khan ↑

84 days ago

Re: Peer Response

The AI firewall uses the intelligent detection engine to train threat detection models based on massive samples and continuously optimize the models based on real-time traffic data, improving threat detection capabilities (Shui, 2021).

Hi All,

This is a great point. This is good food for thought! My only concern is, modern-day infrastructure allows us to hide and change IPs instantly, do you think AI blended firewall can be a plausible idea in these circumstances?

Regards,

Nawaz

Reply

3  Reply to  Grace Clarke from Pavendran Wimalendran ↑

79 days ago

Re: Peer Response

Hi Grace. Thank you for your response, and you do bring up a good point, as Nawaz has pointed out in his post.

The majority of today's firewalls are rule-based. Their knowledge consists of a set of rules that they use to process packets they receive. They can't accomplish anything that hasn't been explicitly programmed into them. This makes the system easier to set up, but it also makes it less flexible and adaptable to changing conditions. A firewall service governed by AI, on the other hand, can defend a computer network from both known and unknown threats without any human intervention.

Reply

Maximum rating: -

Add your reply

Your subject

Type your post

Choose files No file chosen

Submit

Use advanced editor and additional options

OLDER DISCUSSION

Summary Post

NEWER DISCUSSION

Summary Post