Attacking Pathways of Health Information System (HIS)

Ying He¹, Kun Ni¹, Cunjin Luo²,³

¹University of Nottingham, Nottingham, UK
²University of Essex, Colchester, UK
³Southwest Medical University, Luzhou, China

Abstract

The health information system (HIS) has been targeted by the hackers especially during the pandemics of COVID 19. This paper is motivated by the recent cyber incidents happened to healthcare organisations. This study was conducted to demonstrate how the HIS can be hacked and provide some recommendations to protect the HIS. We created a simulated virtual environment by implementing an open-source medical system. We then followed the NIST pen-testing methodology to perform ethical hacking. The hacking was successful, and we have managed to exploit several vulnerabilities of the simulated HIS. We then proposed cyber security recommendations to protect the HIS. Future work will consider demonstrating attacks to a specialized cardiac diagnosis medical system, e.g. the arrhythmia detection and classification in ambulatory ECGs, and explore how the core of its algorithms can be hacked and protected.

1. Introduction

Health sector has been targeted by the cyber attackers who aims to bring down the health critical infrastructure. This research is motivated by the recent security incidents happened to the healthcare organisations, including the US Department of Health and Human Services [1], the World Health Organisation [2] and some pharmaceutical companies, etc [3]. The United States Public Health Service reported that about 100 million pieces of patient information were stolen every month in 2020 [4]. Cyber attackers can not only destroy HIS, but also gain access to or modify sensitive medical diagnosis records produced by diagnosis components such as the ECGs [5-10].

Ethical hacking can help identify vulnerabilities and is an active defense to protect systems through discovering attack paths in the targeted system [3]. It is demonstrated through launching security attacks towards the targeted system. However, this practice can potentially damage the system, and cannot be applied directly over a real-world setting. Therefore, a virtual environment is required to simulate a HIS that can be used for ethical hacking purpose. There are some research efforts demonstrating ethical hacking towards HIS as well as some diagnosis and proposing solution to counteract such attacks [11-15], however, their work considers only a limited number of vulnerabilities (e.g. the OWASP top 10 vulnerabilities).

In this paper, we created a simulation platform through implementing an open-source health information system, OpenEMR, on a virtual environment. In order to simulate a realistic environment, we also installed some software, which health organisations always use. We then launched ethical hacking towards the simulated HIS using various tools. We were able to exploit some vulnerabilities and penetrated the system.

This paper makes the following contribution,

- Builds a HIS simulation platform by implementing an open-source medical system.
- Demonstrates ethical hacking (pen-testing) to the HIS simulation environment using various ethical hacking tools following the NIST ethical hacking framework.
- Proposes security solutions to mitigate security risks and protect the HIS.

3. Methods

We adopted the NIST ethical hacking framework [16] to carry out the study following key stages of planning, discovery, attack, and reporting. Firstly, we set up a simulation platform by implementing an open-source HIS, the OpenEMR. We then launched ethical hacking to exploit vulnerabilities of the simulated HIS. Finally, we propose security solutions to counteract such attacks.

3.1 HIS Simulation

We created a simulation environment to simulate a medical worker’s machine with the OpenEMR installed. The targeted machine was set to have some open ports,
which is common for medical workers computer. We also installed some software that health organisations always use. The system, software, and service versions are old because the medical organisation’s machines always lack upgrade. Figure 1 depicts the structure of the simulated network. Two machines: the targeted host and the attack host, were set up. The targeted host machine got a cyberattack, and the attack host machine launched an attack.

3.2. Ethical Hacking & Result Analysis

We have launched a series of attacks using various ethical hacking tools. Those includes, Nmap scanning, Xray scanning, SQLMap and Metasploit. Table 1 shows the tools used in different stages following the NIST framework,
The results show that the ethical hacking was successful. There were 7 successful exploits out of 24 exploits. These exploits are related to improper input validation, cross-site request forgery, remote code execution, denial of service attack, improper authentication, remote access backdoor, deserialization of untrusted data. 3832 seconds expert time were taken for the exploits.

5. Security Recommendations

To prevent such attacks, improper input validation can be mitigated by using an input validation framework such as the OWASP ESAPI Validation API [17]. Cross-site request forgery and deserialization can be counteracted by using the OWASP XSS Prevention Cheat Sheet [18]. Remote code execution and remote access backdoor can be addressed using web application firewall (WAF) [19]. Denial of service (DoS) attack should be stopped at an earlier stage through enabling DoS protection, dropping packets from malicious sources [20]. Multi-factor authentication should be used to address improper authentication [21].

6. Discussion and Conclusion

This research created a simulated health information system (HIS) by implementing OpenEMR, that allows for carrying out ethical hacking. We have carried out the pentest using the NIST framework and identified a set of vulnerabilities related to improper input validation, cross-site request forgery, remote code execution, denial of service attack, improper authentication, remote access backdoor, deserialization of untrusted data. As OpenEMR is widely used by health organisations, this research has significance for health organisations to address similar security vulnerabilities and prevent similar attacks.

Future work will establish a cardiac intelligent medical diagnosis system with computational models [22-25] and explore how the core of its algorithms can be hacked and protected. Future work will also consider AI-based ethical hacking to automate the testing processes and applying a comprehensive set of security mechanisms to prevent against cyber-attacks in health information system [26-30].

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 61803318).

References

[2] Beware of criminals pretending to be WHO. https://www.who.int/about/communications/cyber-security

Table 1: Ethical Hacking Actions Following NIST Ethical Hacking Framework

<table>
<thead>
<tr>
<th>NIST Stages</th>
<th>Key Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanning</td>
<td>Use Nmap scanning tool to identify the number of ports, port status, protocol, and operating system.</td>
</tr>
<tr>
<td></td>
<td>Use Xray scanning tool to identify the vulnerabilities.</td>
</tr>
<tr>
<td>Discovery</td>
<td>Use information collected from the scanning stage to decide about the exploits.</td>
</tr>
<tr>
<td>Attack</td>
<td>Use SQLMap tool to exploit SQL injection related vulnerabilities.</td>
</tr>
<tr>
<td></td>
<td>Use Metasploit tool to probe networks and applications related flaws and vulnerabilities.</td>
</tr>
<tr>
<td>Reporting</td>
<td>Produce report using information collected from ethical hacking tools.</td>
</tr>
</tbody>
</table>


Address for correspondence:

My Name.
Cunjin Luo

My Full postal address.
Key Laboratory of Medical Electrophysiology, Ministry of Education, Institute of Cardiovascular Research, Southwest Medical University, Luzhou 646000, China

My E-mail address.
cunjin.luo@yahoo.co.uk