IoT Report for CyberHealth Ltd.

Details

Name

Institutional Affiliation

Date

Contents

Task 1

Comparison of three and five-layered architecture of IoT-based remote patient monitoring systems

i. Three-layered architecture in terms of security

In an IoT-based remote patient monitoring, a three-layered architecture has three main aspects and elements that are good in making solutions work (Kumar & Mallick, 2018). The three-layered architecture has the following components: application layer, network layer, and perception layer (Al Hinai & Singh, 2017). In the perception layer, some mobile devices and sensors perceive the data on medical issues and conditions, hence focusing on the data collection, which is a good solution to the recommended aspects.

In the network layer, there is the dissemination of data from the sensors to the central hub of data processing to help in making things better (Kumar & Mallick, 2018). Ideally, working with the data entails addressing the key network and connectivity issues to help in the transfer of data. The network layer is comprehensive and helps in making things better while transporting the right content as needed. Finally, the application layer has active customer-oriented software cases, which are good and effective in solving key medical issues.

Concerning security, there are risks such as distributed denial of services (DDoS), eavesdropping, Node jamming, heterogeneity, attack due to network congestion, and man in the middle problem (Kumar & Mallick, 2018). Since the IoT architecture is limited to three layers, the attacks are common and the penetration is possible, making it pose a greater security risk to an organization, a challenge that deserves a better mitigation strategy. Working with the right layer should always enhance a better and significant solution to the challenges (Al Hinai &

Singh, 2017). The following diagram is an illustration of the three-layered architecture IoT, which can be used to explain the security threats that deserve a better control and strategic approach to the situations and issues in place:

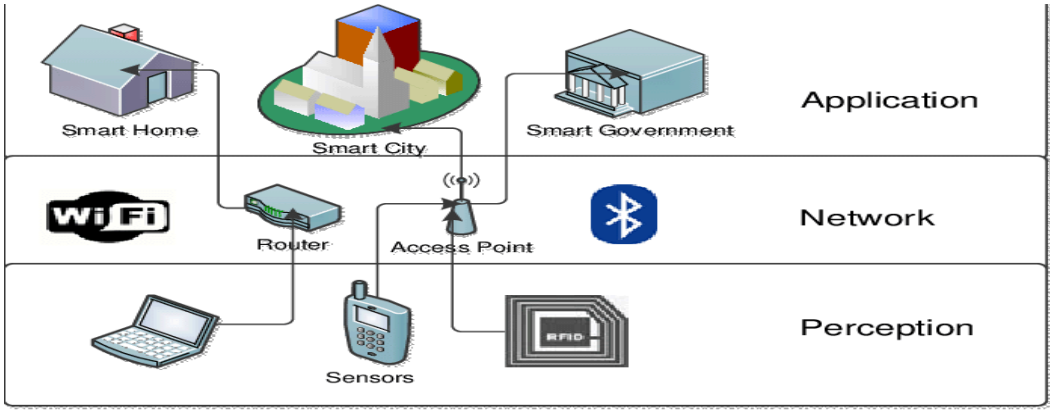

Figure 1: A three-layered IoT architecture

ii. Five-layered architecture in terms of security

In a five-layered architecture for the internet of things, various aspects make it unique and quality interns of the recommended standards of security as compared to the three-layered architecture (Al Hinai & Singh, 2017). The main focus is on the major applications, recommended standards, and key solutions in making the right decisions as needed. The following are some of the main layers of the five-layered IoT architecture:

The first layer is the perception layer whereby the sensors are established, and they collect the data to be used in the entire system (Al Hinai & Singh, 2017). Since the medical equipment has various functional aspects, the monitoring of medical conditions deserves a better approach, a complete look into the aspects of the collection of relevant health information such as blood pressure. The second layer is the network layer, whereby the transmission of information occurs, and the various network aspects make sense. The main

focus of the layer is the transmission of the data to the middle layer, and the network forms can be 3G, 4G, UTMS or Wi-Fi.

The third layer is the middle layer whereby the information collected from the network layer is computed, sorted, and made in a transmissible format (Al Hinai & Singh, 2017). Device addresses are located and precision applied in the getting of the right content of information while working to establish key and functional aspects in helping make things better and effective. The sensors have the right information and key content in making the best decisions count, which is ideal in enhancing the right approach and strategic metric in the channeling of the data (HaddadPajouh et al., 2020). The fourth layer is application whereby the sending of emails, activation of the alarms, and direction of the various health sensor devices are made. The information processed is assigned commands and activation of such systems makes things better in helping accomplish a reliable solution, which helps in addressing the right solution and focus on the major aspects of channeling the right information and content. Finally, the fifth layer is the business layer whereby the device analyses the method in which the information and the related services are delivered to the individuals.

On security grounds, the five-layered IoT has issues such as phishing, data access authentication problems, and malicious active X scripts (Al Hinai & Singh, 2017). Working with the significant processes deserve a better approach in making the entire aspect better, or a solution-based to help in addressing the major challenges. As compared to the three-layered IoT, the five-layered IoT is good in solving several security issues and threats that may be in the network (HaddadPajouh et al., 2020). The vulnerabilities are not as severe as the

three-layered IoT architecture, whereby the focus should be on addressing and enhancing a significant solution to make the right content and a significant approach to focus on the reliable solutions and other issues that need to be implemented in the internet of things. The following is a network diagram of five-layered IoT architecture:

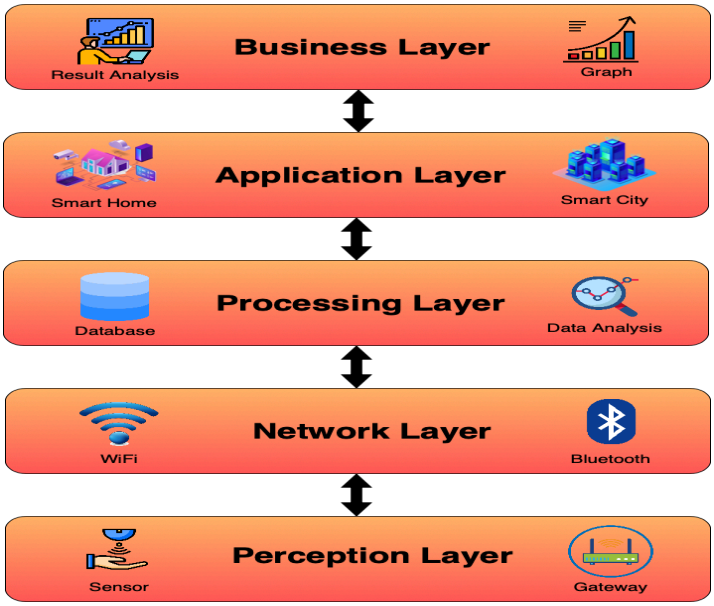

Figure 2: Five-layered IoT architecture

Task 2

Risk in cybersecurity

A risk in cybersecurity refers to a weakness that is likely to result in challenges of poor compliance with the security rules and obligations (Peterson et al., 2018). A risk is a challenge that may result in an attack of the information system, a reduction in the quality of information being implemented as well as other issues that deserve better attention as needed. The main focus should be on the major implementations, and key security needs. Cybersecurity risks are more of

loopholes that can be used by malicious parties to channel their attacks into the system and cause threats to the system (Peterson et al., 2018). Sabotage, penetration attacks as well as loss of integrity and information assurance are possible in the risks, hence making the issues adverse is a significant aspect that needs to be addressed, in accomplishing a key solution, and enhancing the better aspects that need a better and quality solution as planned.

Risk assessment of selected IoT application using a risk assessment framework

A selected application is “My Pulse.” In the Google Play store, My Pulse is a good application in the monitoring of heart rate in a remote setting. The application collects biometric information and behavior metrics in helping predict and monitor heart rates (Boeckl et al., 2019). Focusing on the significant aspects of monitoring the success of the heart rate requires a better approach in implementing key solutions, and working on the right approaches in helping identify the major heart rate-related issues (Boeckl et al., 2019). Pulse is monitored frequently and using IoT with a five-layer architecture, various security risks need to be analyzed in helping identify the right content and information to be used in making a significant solution and approach to the major processes implemented as needed.

The security risks associated with the "My Pulse" application include phishing attacks whereby emails are sent through the application in the form of adverts, and they can be used for extortion and getting information about content that deserves careful attention. Working with the right parties requires careful and good observation in making the right choices and implementation of key strategies in helping accomplish a major solution as required. Necessarily, the main focus is on the applicable approaches and enhancing a crucial strategy in making the right security mitigation measures.

Other risks associated with the application include authentication problems. Significantly, there is the need to focus on making the right authentication decisions, to help in becoming better and effective (Boeckl et al., 2019). Major solutions associated with the application such as getting the right details are seen as a challenge, and the focus should entail working with the needed approaches to help in solving the main aspects that need a better chance. Ideally, the main focus is on applying a good solution, working through risk mitigation measures. Since "My Pulse" is used by most people, reducing the levels of attack require a significant threat modeling approach in helping make the necessary choices and decisions that should be changed as needed. The risk analysis reveals challenges in information security and other aspects that should be mitigated following the right security audit.

The likelihood of occurrence of the security risks in using the application is 32% considering the frequency of use, and the integrated approaches applied and implemented (Boeckl et al., 2019). Ideally, the major focus should be on addressing the significant issues, working on a competitive solution, and working on the major deliverables as needed. Ideally, the focus should be on the mitigation plan, something that must be addressed adequately. Upon occurrence, the My Pulse android application can cause adverse costs associated with the loss of information and other challenges that can be attested to due to the significant issues to present. Ideally, the focus and key integration need a better protocol, and address of the major elements of change to make the right content, and key solutions in enhancing a quality application and focus on the integrated plans as needed (Boeckl et al., 2019). A risk assessment on the application reveals a significant security breach threat and compromise of the application aspect, something

that ought to be addressed in making the right solution, and content to be implemented in a manner that deserves a better protocol and approach in changing how things work in general.

Task 3

Analysis of End-to-End Security Vulnerabilities and concerns using 3-layer architecture

End-to-end security vulnerabilities with using 3-layered architecture entail significant aspects of security and one of the vulnerabilities is Distributed Denial of Services (DDoS), whereby the malicious parties get into the information system and cause a service block, whereby the major operational aspects are compromised. In DDoS, the major challenge comes from challenges of poor adherence to the policies of security, hence the crucial services are blocked, making the end-to-end security become better.

Eavesdropping is a security vulnerability in the 3-layered architecture. Listening to information by third parties silently is common in such an architecture, whereby the end-to-end security is compromised by the security issues that come in the path. The main challenge is having the worst of the worst in the form of security. Leakage of information through a malicious third-party listener is considered a major challenge in the security aspects. An implementation of the right content, key metrics, and other aspects deserve a better approach in making things work as needed.

In our virtual lab, Kali Linux software was used in the analysis of the end-to-end vulnerabilities. The following is a typical example of the functionality test associated with the Kali Linux analysis of the security architecture:

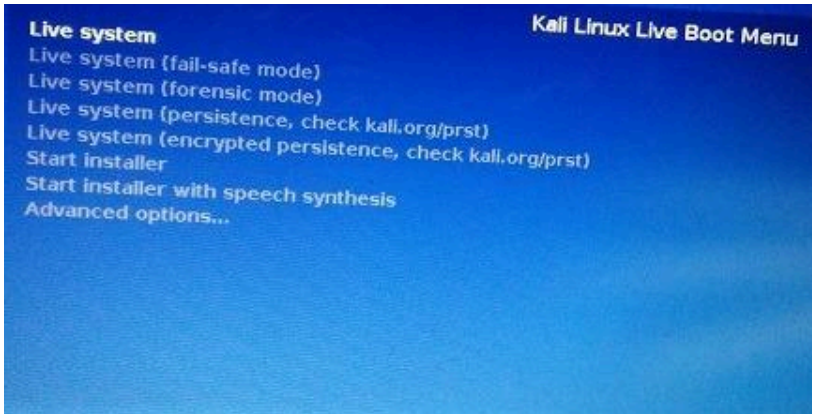

Figure 1: The boot up process of Kali Linux software.

Figure 2: A comprehensive analysis of hacking in the end-to-end connection.

Figure 2: Checking for password integrity of the system IoT.

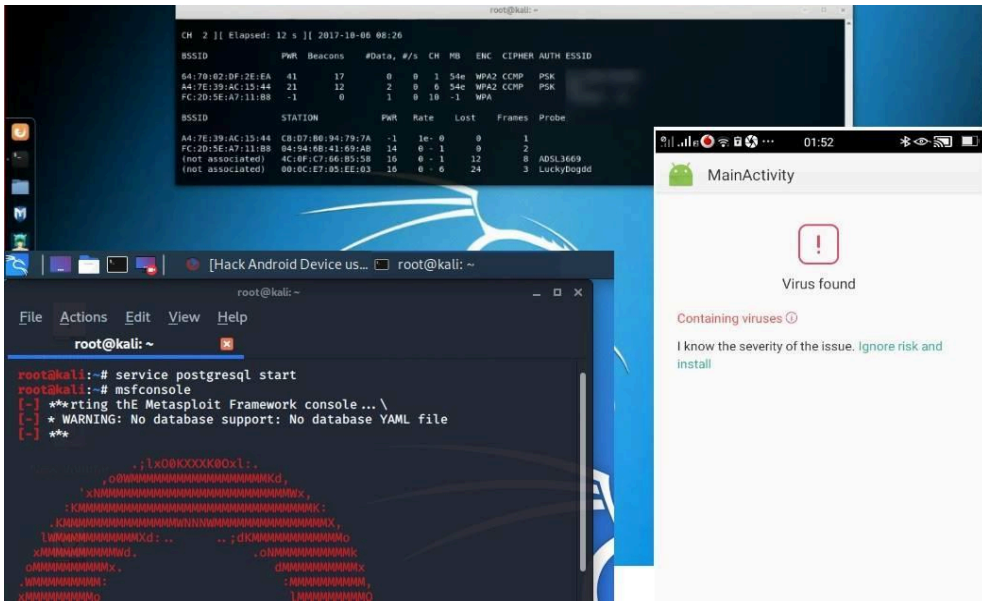

Figure 3: An output showing identification and detection of a virus threat.

Task 4

Security mitigation strategies for security vulnerability concerns

The security concerns can be mitigated through the hardening of network communication. Security strengthening techniques must be implemented in a manner that is good to help in preventing a future occurrence (Qui et al., 2019). Network hardening is a common term that includes various techniques such as firewalls, solutions such as establishing a demilitarized zone (DMZ), and scanning of the network to reduce the penetration levels (Qui et al., 2019). Additionally, increasing the number of nodes is a key solution in making the right decisions, and implementing the main aspects to change and enhance a key solution to address the threats, and working on competency-based protocols for the networks to be good and effective.

In the virtual lab, the following is a test of the integrity of the IoT:

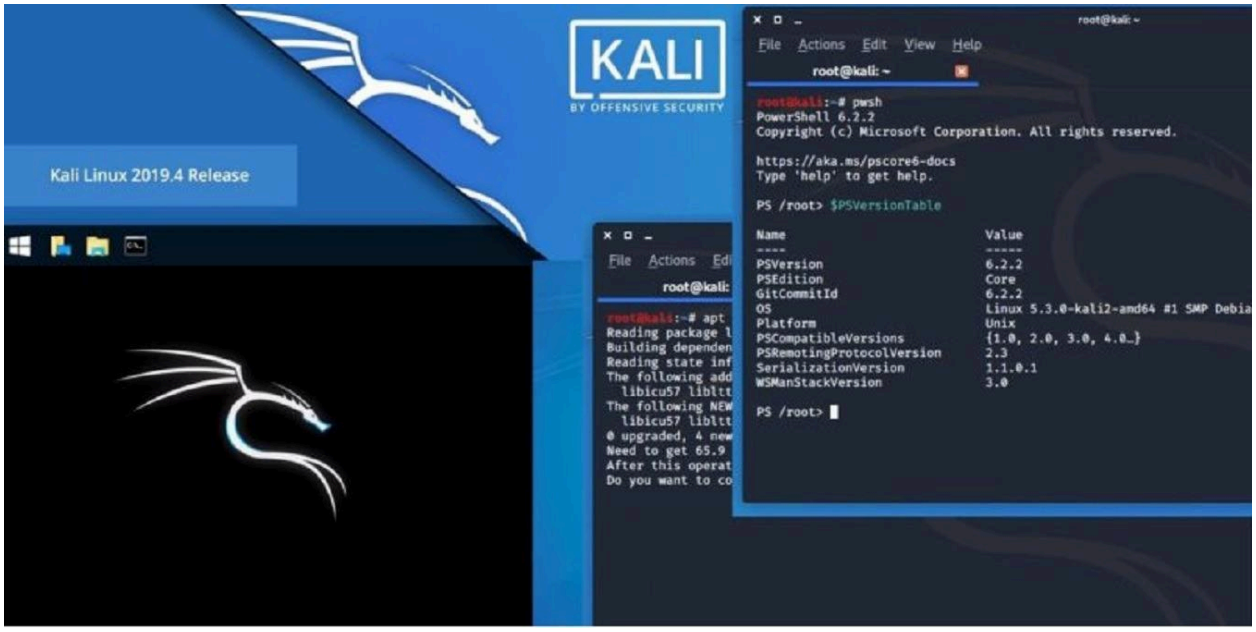

Figure 4: Testing of the security integrity in the system using Kali Linux

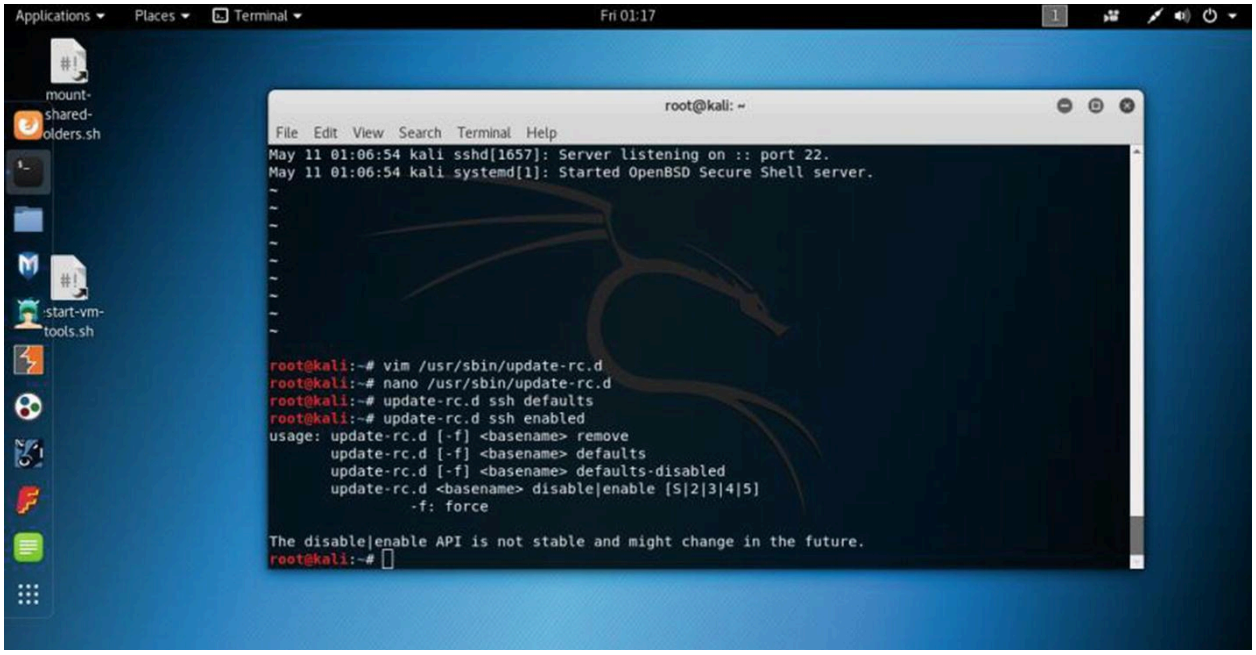

Figure 5: Confirmatory test for the IoT security integrity and resistance of the IP address.

Task 5

Potential adversarial attacks with examples possible in autonomous or driverless car domain of IoT

In the IoT domain, potential adversarial attacks include manipulation of ML methods, to results in challenges, and other adverse aspects (Qui et al., 2019). Enhancing a significant solution requires a better approach in making things better and key protocols in changing the monitoring system of the cars. Additionally, kidnapping is possible with autonomous cars, whereby a hacker gets access to the artificial intelligence codes and manipulates the movement of the car, which creates a different aspect, necessarily needed for security (Qui et al., 2019). The adversarial attacks may result in the damage of the car, and challenges in working with the right control strategies, hence reducing the key threats, and other aspects, hence making the process generally difficult.

References

Al Hinai, S., & Singh, A. V. (2017, December). Internet of things: Architecture, security challenges, and solutions. In 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS) (pp. 1-4). IEEE. https://ieeexplore.ieee.org/abstract/document/8286004/

Boeckl, K., Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., ... & Scarfone, K. (2019). Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks. US Department of Commerce, National Institute of Standards and Technology. https://a51.nl/sites/default/files/pdf/NIST.IR.8228.pdf

HaddadPajouh, H., Khayami, R., Dehghantanha, A., Choo, K. K. R., & Parizi, R. M. (2020). AI4SAFE-IoT: An AI-powered secure architecture for the edge layer of the Internet of things. Neural Computing and Applications, 32(20), 16119-16133. https://link.springer.com/article/10.1007/s00521-020-04772-3

Kumar, N. M., & Mallick, P. K. (2018). The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. Procedia computer science, 132, 109-117. https://www.sciencedirect.com/science/article/pii/S1877050918309049

Peterson, D. C., Adams, A., Sanders, S., & Sanford, B. (2018). Assessing and addressing threats and risks to cybersecurity. Frontiers of health services management, 35(1), 23-29. https://journals.lww.com/frontiersonline/FullText/2018/09000/Assessing_and_Addressing_Threats_and_Risks_to.4.aspx

Qiu, S., Liu, Q., Zhou, S., & Wu, C. (2019). Review of artificial intelligence adversarial attack and defense technologies. *Applied Sciences*, *9*(5), 909. https://www.mdpi.com/421422