Robots Security Assessment and Analysis Using Open-Source Tools

Benjamin Yankson, Tyler Loucks, Andrea Sampson and Chelsea Lojano
HackIoT Lab - College of Emergency Preparedness, Homeland Security and Cybersecurity
University at Albany, Albany, USA

Byankson@albany.edu

Abstract: The Internet of things (IoT) has revolutionized many aspects of the world, including industrial systems, automobiles, home automation, and surveillance, to name a few. IoT has offered a multitude of conveniences for our daily lives, such as being able to control our thermostats remotely, view our home surveillance cameras while away, or have a smart television that can surf the web. However, the widespread adoption of IoT devices combined with their vast device vulnerabilities results in significant security risks reinforcing the need for more robust default security controls and public awareness. As such, this paper aims to discover and document security vulnerabilities in the Asus Zenbo Junior IoT robot, along with providing a few best practices when securing smart home devices. This work presents an experiment using several security vulnerability assessment tools such as Nmap and OpenVAS scans to assess cybersecurity vulnerability currently present on Zenbo based on the 4P forensic investigative framework. The result of the experiment shows multiple open ports were discovered, along with miscellaneous information that an attacker could use to their advantage to attack the Zenbo robot. Based on the result, this work presents various security precautions that can help users protect against cyber-attack.

Keywords: Security, Robot, Assessment, attacks

1. Introduction

With the number of IoT devices forecasted to nearly triple from 9.7 billion in 2020 to more than 29 billion in 2030, security in these types of devices needs to be a more prominent topic of discussion because of the enormous consequences that a compromised device can lead to (Vailshery, 2022). For example, compromised IoT devices such as a smart robot like Zenbo, smart television, or smart fridge could open a pathway in a network for an attacker to infiltrate through. Vulnerable IoT devices are a problem that can affect both everyday people and businesses of all sizes. The scale of IoT attacks can range drastically from someone spying through a webcam to turning a device into a zombie as a part of their botnet to take down corporate websites. IoT security is an issue that affects millions of people around the world, and some people or businesses may even be completely unaware that their device is compromised. In today's age, downtime or data breaches of any amount can amass severe monetary losses for organizations. A 2021 IBM report (IBM, 2021) demonstrated that the United States continues to record the costliest data breach incidents worldwide. The report depicted that the average global cost of a data breach has reached over $4 million, far greater than the Ponemon Institute's Cost of a Data Breach Report for 2020(Barati & Yankson, 2022); which put the average cost of worldwide data breaches in 2020 amounted to $3.86 million. To put this into context, between 2005 and 2019, a report from the Privacy Rights Clearinghouse (PRC) shows about 9,015 data breaches, accounting for 11,690,762,146 breached records (Demeyer, 2011). Remediation and repair efforts also have to be compensated for; that does not account for any losses from factors such as missed sales, which vary greatly depending on the type of organization (e-commerce, video streaming service, and others).

To begin addressing IoT security, we believe two specific aspects will assist in lowering the number of successful attacks. First, more extensive vulnerability testing from the manufacturer is required before the product ships. Two, increasing user awareness about IoT device security and best practices to implement into their home networks. Improving these two aspects will strengthen IoT security and, in turn, lower the rate of successful attacks across all sectors, including home, medical, and industrial systems. The result of our work will contribute to current academic and industry discussions by showcasing the various vulnerabilities and security issues present in our smart home devices, such as the Asus Zenbo robot. Secondly, this work intends to contribute to the discussion surrounding more robust security controls in home-based IoT devices to minimize the potentially devastating consequences that can follow a successful attack.

1.1 Problem Statement

Since the number of IoT devices in the world is in the tens of billions and cyberattack rates continue to increase year after year, IoT devices need to implement much stronger security controls (Vailshery, 2022). For example, according to Kaspersky, an anti-virus and computer security service provider, IoT cyberattacks doubled yearly during the first half of 2021. From January to June this year, some 1.51 billion breaches of Internet of Things (IoT) devices took place, which is an increase from 639 million in 2020. There are over 1.5 billion IoT breaches, most of which use the telnet remote access protocol (Cyrus, 2021). The failure to secure IoT devices has and will continue to have massive consequences for everyday users and businesses. Damages can come in the form of

data being stolen, privacy being violated, loss of current or potential customers, and so on. With cybercrime expected to grow 15% per year and possibly reach $10.5 trillion annually by 2025, there needs to be a larger focus on securing IoT devices around the world in hopes of helping prevent users and businesses from suffering a successful attack (Morgan, 2022). In other words, since the rate of cyberattacks and cybercrime will significantly increase over the next few years, this reinforces the need for IoT manufacturers and users to secure their products better.

While there is no surefire method to mitigate cyberattacks completely, manufacturers and users can take a couple of steps to secure themselves better. On the manufacturer's side, more comprehensive vulnerability assessments should be conducted to help discover any security issues that should be remediated before the product ships. Another step the manufacturer should take to strengthen security would be defaulting the device to automatically download and install software/security updates so that burden does not fall on the user. On the user's side, there are also a few steps to take to secure their IoT devices. One step is to place all IoT devices onto a network separate from the home network, such as a guest network. The other step is to ensure that the device is on the latest software/security patch version, even if automatic updates are enabled. Ultimately, this paper serves to showcase some of the vulnerabilities that can be found in smart home IoT devices like Zenbo. The rest of the paper is organized as follows: Section 2 presents an overview of the background and related work. Section 3 details the methodology, 4P forensic framework, and vulnerability assessment case study using Nmap and OpenVas. Section 4 presents a discussion of the experimental result, and Section 5 concludes the paper and highlights future works.

2. Background and Related Work

The Zenbo Junior robot is advertised as a home companion that packs "loads of IoT functions," which "helps you to be more efficient" by integrating more artificial intelligence into your life (Zenbo Junior—Expansive Applications, n.d.). Zenbo Junior is a smart robot that can follow commands from the user to perform many actions, such as following a user around, spinning in place, or controlling other home IoT devices through Amazon Alexa integration. ASUS also details how Zenbo can be an excellent tool for the medical field as Zenbo can act as an interface for medical patients to enter health care information. ASUS also offers "Zenbo Lab," which allows Zenbo to run the python code created. These use cases convey how helpful and convenient a smart robot can be for someone. However, while convenient, security is often an issue that is not touched on nearly as much as it should be. If access or control to Zenbo falls into the hands of an attacker, there is a possibility that the attacker could have access to many other devices. This can include other smart home devices ranging from security cameras to televisions or even baby monitors. At the same time, extremely convenient and helpful to many, security needs to be a top priority for owners of smart robots such as Zenbo because of the massive consequences that can result from a compromised robot.

In 2016 Mirai botnet used around 100,000 malicious endpoints, essentially made up of IoT devices (Woolf, 2016). In this case, the compromised IoT devices were part of the botnet controlled by two malicious actors who used these devices to conduct distributed denial-of-service (DDoS) attacks (What is the Mirai Botnet? n.d.). As a result, the attackers were able to take down many high-profile websites, including Twitter, Reddit, and Netflix, to name a few (Woolf, 2016). While the total monetary damage of a DDoS attack entirely depends on the organization's size and downtime, many sources estimate that the monetary damage can range anywhere from tens of thousands to hundreds of thousands of dollars (Newman, 2021). On top of that, experiencing a successful DDoS attack will also cause reputational damage, which could deter current and potential future clients from using an organization's service or product. Regardless of the number of damages, no organization wants to experience a successful DDoS attack, be spied on by strangers through a webcam, or have their home IoT devices controlled by a malicious attacker.

Another excellent example of a compromised smart home IoT device is the Enabot Ebo Air smart robot. Much like ASUS' Zenbo, this robot is equipped with a camera, speaker, microphone, and wheels, allowing it to move around the house freely (Enabot, n.d.). Essentially, Enabot developed this smart robot so that the home could be monitored while away and so that it could remotely "connect with your loved ones" (Enabot, n.d.). Unfortunately, while all of that sounded great, it was discovered that these robots had the same hard-coded admin credentials (Hashim, 2022). This means that if an attacker can access the network that the robot is on, they will also be able to connect to Ebo via SSH because of this vulnerability (Hashim, 2022). Once inside, the attacker would have access to all of Ebo's functionality (view a live feed of the camera, listen through the microphone, and others .) and all information stored on the robot. Although the vulnerability was caught before shipping, this example conveys the potential severity of a successful IoT hack.

Nevertheless, while smart home IoT devices make for an excellent target for attackers, the medical and industrial sectors of the world also face instances of IoT devices being compromised and used maliciously. Imagine the robot used to bring pills daily to the hospital, spying on a user without the user's knowledge. It is a scary and unsettling thought to think about it. In the case of the Aethon TUG smart robot, these fears came to fruition. These robots are used in hospitals to deliver medication and supplies and perform miscellaneous tasks. However, some of the vulnerabilities found in these robots could allow attackers to disrupt the functionality of the robots, surveil patients and even obtain confidential information through the camera (Lakshmanan, 2022). Also, attackers could even have launched ransomware through these robots' network connectivity which could have affected the entire hospital (Lakshmanan, 2022). Like Enabot's Ebo, these vulnerabilities were caught before any attacker could exploit them (Lakshmanan, 2022).

On the other hand, industrial robots assist many different manufacturing processes. They are primarily used in big factories to help increase efficiency in product production. This includes many tasks, such as moving large objects/materials, welding, and assembling parts. The critical difference between the previously mentioned robots and industrial robots is that if a vulnerability is successfully exploited, it can lead to serious physical injury on top of monetary and reputational damage. Like the other IoT robots, the vulnerabilities stem from the robots being connected to the Internet. This Internet connection is the pathway that malicious actors use to launch their attacks. As Gaudin states, "Malicious hackers could get into a robot's controller system and adjust its actions, which could create a dangerous situation in the factory or enable the robots to build unsafe products on the production line" (2017). Overall, no matter what type of IoT robot (smart home, medical, or industrial), there are multiple security concerns that each present a different challenge for manufacturers and users to manage.

Using a weak or out-of-date encryption standard will raise the chances of an IoT device being successfully breached, which could compromise important information stored on the device. These devices can also allow the patient to interact virtually with a medical professional, and if the information is being transmitted in plaintext, an attacker could conduct a man-in-the-middle attack to intercept the network traffic being transmitted (Langkemper, n.d.). Software such as Wireshark makes it incredibly easy to intercept and log any network traffic that is being transmitted. With medical patient information being protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the security and use of strong encryption of these robots are necessary to maintain the confidentiality and integrity of any medical information being transmitted. One of the best steps to take in protecting IoT devices is ensuring the use of advanced encryption standards (AES). AES is generally agreed upon as "one of the best encryption protocols available, as it flawlessly combines speed and security, letting us enjoy our daily online activities without any disruption." When used correctly, successful attacks can be prevented (Rimkienė, 2020). Ensuring that the data transmitted from IoT devices is encrypted is crucial to the overall security of IoT devices.

As it relates to IoT, access control is "a set of permissions for a connected camera or any IoT device that specify which users are granted access and the operations they are permitted to perform" (Access control list (ACL) for Internet of things (IoT), 2020). Only certain users are granted access to the system, which is something that many IoT devices should have when it comes to security and privacy. This concept benefits devices with cameras or microphones, such as baby monitors, smart robots, or home surveillance systems. Access controls can take many forms, including mandatory access control, role-based access control, and discretionary access control. While these forms of access control all operate and assign permissions differently, they all ensure that only the people who need access receive access. Implementing access controls on smart home IoT devices can ensure that users who have access can control and perform activities with the devices. This can mean anything from updating the device remotely to viewing the security cameras while away from home. Implementing access control is a common practice in the business world to maintain the principle of least privileges and ensure a more robust security posture. Those same principles can be applied to the home network with your own IoT devices, making your smart home IoT devices and network much more secure.

3. Methodology

To begin the security vulnerability assessment of Zenbo, we adapt the 4P Investigation framework as proposed by Yankson et al. (2020). The framework consists of planning, preservation, processing, and presentation of results. The process begins "Planning" component. This involves establishing the scope and identifying the Asus Zenbo Junior as the medium involved. The processing component allows the assessor to prepare, set up, scan the medium and store the information. This component requires the Investigator to select the toolset necessary to collect and analyze available information. For this experiment, we will be selecting Nmap and OpenVas. The preservation component allows the assessor to document the type of information available and the state. At

this stage, the assessor can gather the necessary information to understand the inner working of the medium under investigation. Finally, the Presentation component involves collecting and analyzing the information found.

3.1 Tool Setup & Scenarios

The investigation has been performed on the Asus Zenbo Junior smart home IoT(Figure 1) to acquire data such as media recorded by the Zenbo, OS information, OS patch level information, and User ownership information using Nmap and OpenVAS free vulnerability software. The vulnerability testing Zenbo Junior involved three pieces of equipment: Zenbo Junior, a WAVLINK router, a Macbook Air 2016 for Nmap, and a Dell XPS 15 7590 for OpenVAS. In addition, we chose to use free vulnerability scanners to search for vulnerabilities and system information (patch level, operating system version, and others.) to allow the replicability of our work.

We powered on the router but did not connect the ethernet cable to the wall jack to avoid connecting to the main campus network. Next, we connected Zenbo Junior and the laptop to the WavLink WiFi router depicted in Figure 2. The IP address of Zenbo can be obtained by either opening the" Zenbo Lab" or through the device's settings. The WiFi network of this Zenbo uses a class C IP address, in this case, 192.168.10.128. Considering that the laptop Zenbo connected to the router locally, we began scanning Zenbo for vulnerability and open ports. Figures 3-5 show that Nmap was used multiple times with various scans that searched for the device's operating system, open TCP/UDP ports, and MAC address.

The results show that Zenbo is vulnerable to attacks and can link the Zenbo App to show ownership information. Based on preliminary data and current research, we made the following hypotheses:

- H1: Internal storage content of Zenbo can be accessed or manipulated, putting into question the confidentiality and integrity of information.
- H2: Zenbo can easily be subject to attack due to multiple open ports

To experiment to prove our set hypothesis based on preliminary findings, we set up a DELL laptop running Macbook Air 2016 for Nmap and a Dell XPS 15 7590 for OpenVAS (Figures 1-2).

Figure 1: Asus Zenbo Junior Robot

Figure 2: WavLink WiFi Adapter

3.2 Nmap Scanning TCP Port on Asus Zenbo Junior

To conduct the initial Scanning to determine an open port that can subject the device to an attack, the attacker's machine-running interfaces must be active to access the interfaces of Zenbo and acquire port information. As per Figure 3 below, we scan using the command *nmap -p 1-65535 -T4 -A -v*. This command allows us to scan all TCP ports on Zenbo Junior. We repeated the same command for UDP. The TCP and UPD port scan is depicted in Figure 3, Figure 4, and Figure 5. The results show that the Zenbo Junior model ran on the Android operating system version 6.0.1 with the security patch level from August 1, 2018. Checking for updates on the device does not allow us to update the operating system version or the security patch level.

The scan, as depicted in Figure 3, found multiple open TCP ports open, including ports # 8422, #19321, and #19323. The scan result also identified the current Mac Address of the Zenbo. The UPD scan result shows approximately 13 more open ports in filtered states. The open UDP ports include #1060, #1485, and others. (refer to Figure 4 for a list of the result of open ports). There were also a handful of open TCP/UDP ports on

Zenbo. Specifically, UDP port 4444 was left open on Zenbo, and both TCP/UDP port 4444 have vulnerabilities associated with them. First, port 4444 is the default listener port for Metasploit (SpeedGuide). Also, “some rootkit, backdoor, and Trojan horse software open and uses port 4444” (McKay, 2021). McKay describes how malware can use this port to eavesdrop on traffic and communications, exfiltrate data, and even download new malicious payloads (McKay, 2021). Ultimately, information about Zenbo, such as its MAC address and any open TCP/UDP ports, was obtained by using various Nmap scans. Subsequent to this, we run OpenVAS against Zenbo junior to identify any known vulnerabilities. The operating system and patch level are outdated, which inherently introduces security concerns.

Figure 3: Nmap scanning for all open TCP ports

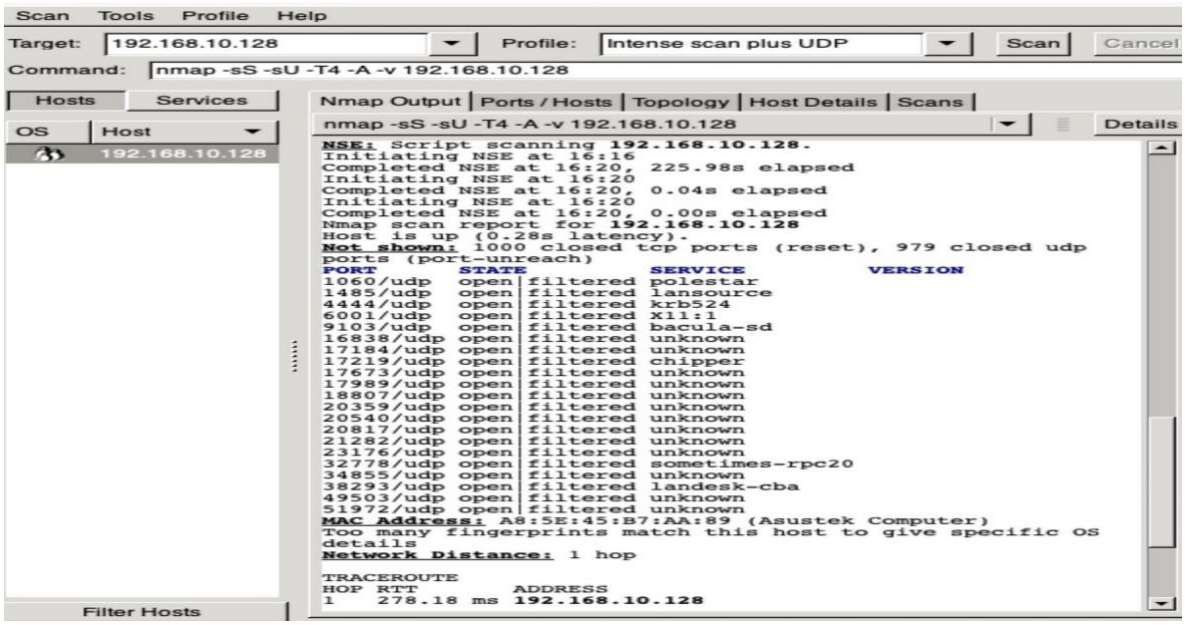

Figure @. Nmap scanning for all UDP ports

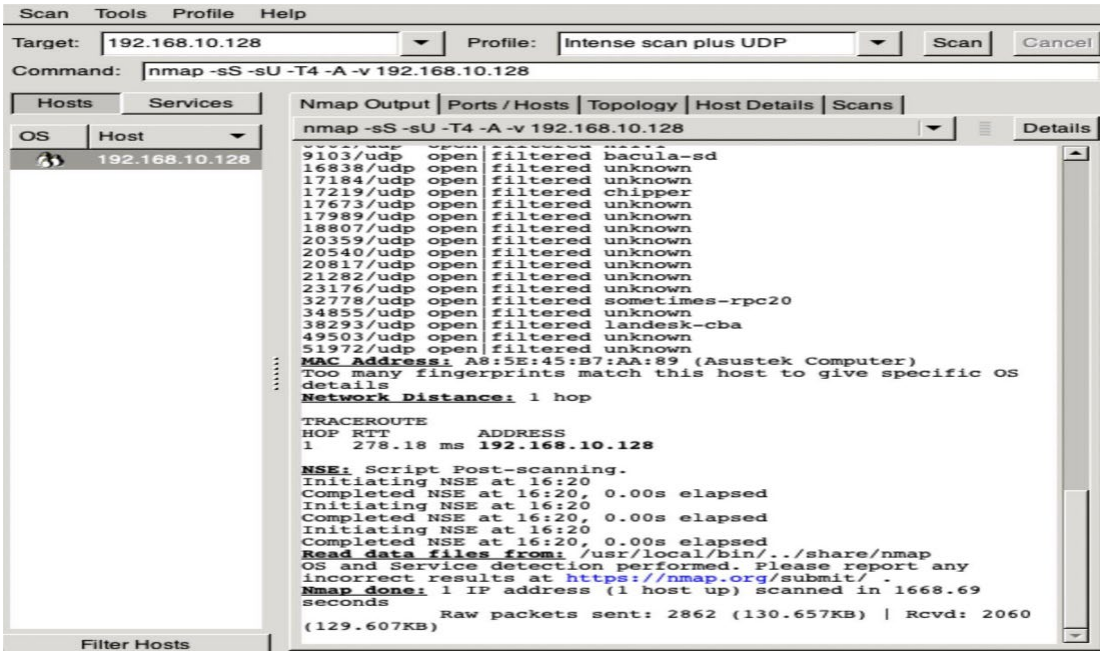

Figure 4: Nmap scanning for UDP ports as well as MAC Address

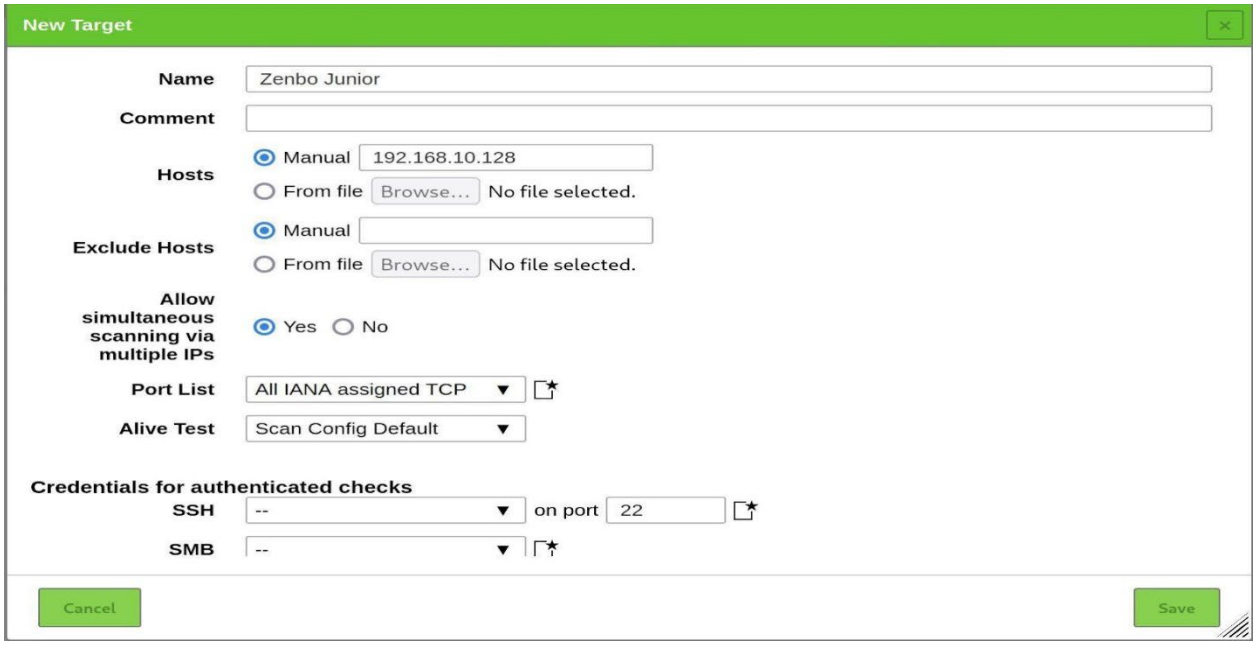

Figure 5: Task creation with OpenVAS

4. Discussions

The result of the experiment shows multiple open ports were discovered, along with miscellaneous information that an attacker could use to their advantage to attack the Zenbo robot. Since vulnerable home IoT devices can provide attackers a pathway into the home network, that also means that they could access any other network devices that are connected. This would include devices such as a Ring doorbell camera and Google Nest security cameras. This leaves the unsettling possibility of being spied on by a stranger. Such an act has been documented where an attacker could talk through one of the security cameras to a home user (Ring hacked, 2021). Unfortunately, many families worldwide have experienced this uncomfortable feeling of violating their privacy due to the weak security often present in their IoT devices. While the invasion of privacy is much harder to put a number on for damages compared to a successful cyber-attack, it can be argued that it is just as crucial for both organizations and users to consider the security and privacy implication when developing and purchasing smart home IoT devices, respectively.

Emerging IoT devices are inherently vulnerable to security and privacy issues which usually stem from exposed services/ports, weak encryption protocols, and lackluster access control. Regarding IoT security, the FBI states, "Your fridge and your laptop should not be on the same network. Keep your most private, sensitive data on a separate system from your other devices" (FBI, 2019). Separating the insecure IoT devices on your network ensures that even if an attacker compromises one of the IoT devices, they no longer have easy access to the rest of the network. Think of having a guest network for the home with IoT devices. In this case, the guest network would isolate these insecure devices from the rest of the network. Organizations implement different solutions, such as VLAN or DMZ, to achieve the same isolation concept with their public-facing web and email servers. While establishing and connecting the IoT devices to a separate network may seem arduous at first, it is well worth the time investment, as the alternative is accepting the possibility that the device becomes compromised by an attacker.

Another security precaution is changing the default credentials on the home devices. This step can help stop attackers from gaining access to the router, WiFi security cameras, and other wireless network devices. Attackers can easily exploit and gain access to a device left with default credentials, making this step an integral part of securing the IoT devices and overall network. Newly created passwords for the devices should contain more than eight uppercase and lowercase characters combined with symbols and numbers. Besides strong passwords, multi-factor authentication should also be considered, which provides much more security and something only the authorized user can access. Whether using SMS or an authenticator app to receive the one-time passcodes, this step greatly strengthens the security of devices. Lastly, since new security vulnerabilities are constantly being discovered, users must update their IoT devices regularly. Installing updates and patches can iron out any previously found security vulnerabilities that an attacker could have exploited. All in all, separating the IoT devices from the rest of the network, changing the default credentials on the devices, and maintaining the current patch level are some basic security steps that can help the user mitigate possible cyber-attacks.

5. Conclusions

There is no denying that smart home IoT devices device, such as Zenbo Junior robot, can offer users great convenience in their daily lives by assisting them with miscellaneous tasks such as remotely controlling their thermostats, wirelessly viewing their security cameras, or even being able to lock/unlock their front door while away from home. However, IoT devices such as these often suffer from inadequate security features, which can cause them to be a prime target for attackers attempting to infiltrate private networks. In this work, we have demonstrated that, based on the experimental results, the security vulnerabilities present in the Asus Zenbo Junior IoT robot. These vulnerabilities can make the Zenbo Junior robot an easy subject of attack due to multiple open ports. Also, the Internal storage content of Zenbo can be accessed or manipulated, putting into question the confidentiality and integrity of information. Based on the result, this work presents various security precautions that can help users protect against cyber-attack. Furthermore, the countermeasures provided can strengthen the security of their devices, such as changing the device's default credentials, keeping the devices up to date with the most recent patch level, and using a separate network, specifically the Asus Zenbo IoT device.

Based on the related work supports the finding that these vulnerabilities are not isolated to Asus Zenbo Junior. In addition, smart home IoT devices such as WiFi surveillance cameras or smart robots will usually suffer from similar security pitfalls, such as leaving unused ports open, shipping with an out-of-date security patch, or having lackluster authentication for remote access. These ever-present security issues can have massive consequences on the user and even cause damage to other organizations."

References

Access control list (ACL) for the Internet of things (IoT). AnyConnect. (n.d.). Retrieved November 4, 2022, from https://anyconnect.com/access-control/

Barati, M & Yankson, B (2022) "Predicting the Occurrence of a Data Breach." International Journal of Information Management Data Insights, Volume 2, Issue 2, ISSN 2667-0968, https://doi.org/10.1016/j.jjimei.2022.100128.

Cyrus C. (2021), IoT Cyberattacks Escalate in 2021, IoT World Today. Retrieved December 20, 2022. https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/

Enabot. (n.d.). Retrieved November 4, 2022, from https://na.enabot.com/

Demeyer, S. (2011) "Research methods in computer science." 2011 27th IEEE International Conference on Software Maintenance (ICSM), Williamsburg, VI, 2011, pp. 600-600. doi: 10.1109/ICSM.2011.6080841.

Gaudin, S. (2017, May 9). Industrial robots are a weak security link. CSO Online. https://www.csoonline.com/article/3195332/industrial-robots-are-security-weak-link.html

Hashim, A. (2022, July 28). Numerous Security Vulnerabilities Found In Enabot Ebo Air Smart Robot. Latest Hacking News | Cyber Security News, Hacking Tools, and Penetration Testing Courses.

https://latesthackingnews.com/2022/07/28/numerous-security- vulnerabilities-found-in-enabot-ebo-air-smart-robot/

Install Nessus Offline (Nessus). (n.d.). Retrieved November 14, 2022, from https://docs.tenable.com/nessus/Content/InstallNessusOffline.htm

IBM, *"IBM Report: Cost of a Data Breach Hits Record High During Pandemic."* (2022). Available: newsroom Online https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic [Accessed: August 15, 2022] [Accessed: August 23, 2022]

Lakshmanan, R. (2022, April 15). JekyllBot:5 Flaws Let Attackers Take Control of Aethon TUG Hospital Robots. The Hacker News. Retrieved November 4, 2022, from https://thehackernews.com/2022/04/new-jekyllbot5-flaws-let-attackers-take.html

Langkemper, S. (n.d.). The most important security problems with IoT devices. Eurofins Cyber Security. Retrieved November 4, 2022, from https://www.eurofins- cybersecurity.com/news/security-problems-IoT-devices/

McKay, D. (2021, January 8). Why Are Some Network Ports Risky, And How Do You Secure Them? How-To Geek. Retrieved November 8, 2022, from https://www.howtogeek.com/devops/why-are-some-ports-risky-and-how-do-you-secure-them/

Morgan, S. (2020, November 13). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damages-6- trillion-by-2021/

Newman, S. (2021, October 17). The True Cost of DDoS Attacks. Infosecurity Magazine. https://www.infosecurity-magazine.com/opinions/the-true-cost-of-ddos-attacks/

SpeedGuide. (n.d.). Port 4444 (tcp/udp). SpeedGuide. Retrieved November 8, 2022, from https://www.speedguide.net/port.php?port=4444

Tech Tuesday: Internet of Things (IoT) — FBI. (2019, December 3). [Press Release]. Retrieved October 31, 2022, from https://www.fbi.gov/contact-us/field-offices/portland/news/press- releases/tech-tuesday-internet-of-things-iot

Rimkienė, R. (2020, December 11). What is AES Encryption, and How Does It Work?Cybernews. https://cybernews.com/resources/what-is-aes-encryption/

Ring hacked: How to protect your Ring smart device | NordVPN. (2021, December 23). https://nordvpn.com/blog/ring-doorbell-hack/

Vailshery, L. S. (2022, August 22). IoT-connected devices worldwide 2019-2030. Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

What is the Mirai Botnet? (n.d.). Cloudflare. Retrieved November 3, 2022, from https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

Woolf, N. (2016, October 26). DDoS attack that disrupted the Internet was the largest of its kind in history, experts say. The Guardian. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Yankson, B. Iqbal, F. and P.C. K. Hung. (2020) "4P-based forensics investigation framework for smart connected toys". In Proceedings of the 15th International Conference on Availability, Reliability, and Security (ARES '20). Association for Computing Machinery, New York, NY, USA, Article 44, 1–9. https://doi.org/10.1145/3407023.3409213

Zenbo Junior—Expansive Applications, Flipped Learning. (n.d.). Zenbo Global. Retrieved October 27, 2022, from https://zenbo.asus.com/product/zenbojuniorii/overview/