International Journal of Synergy in Engineering and Technology
IJSET

Red Team Tool USB-Based Attack Using Raspberry Pi P4wnP1 A.L.O.A

Wan Ainul Alyani Wan Mohamed*, Alif Imran Abdul Manaf, Siti Norwahidayah Wahab

Faculty Computer Media and Technology Management, UC TATI, Kemaman, Terengganu.

*Corresponding author: ainulalyani@uctati.edu.my

KEYWORDS

Red Team
Raspberry Pi Zero
Human Interface Device (HID)
Cyber Security

ABSTRACT

This article presents the development of the A.L.O.A P4wnP1 USB-based Red Team tool using a Raspberry Pi Zero. The tool uses Human Interface Device (HID) attack techniques to simulate real-world cybersecurity threats. By integrating the P4wnP1 A.L.O.A framework and creating attack scripts with Ducky Script, it provides a simple and effective way to test vulnerabilities. Using social engineering, the tool is deftly disguised as a working PC speaker in order to remain undetected while carrying out attacks. Tests demonstrated that the tool successfully performed tasks such as disabling Microsoft Defender, downloading malware, and initiating ransomware attacks, all while remaining undetected. This project offers valuable insights into USB-based attacks. Future enhancements can focus on improving its stealth capabilities and adding more functions. By bridging the gap between cybersecurity research and useful technologies, the A.L.O.A P4wnP1 assists companies in fortifying their defenses against contemporary cyberthreats.

Received 08 July 2025; Revised 26 August 2025; Accepted 30 September 2025; Published 31 October 2025

1.0 INTRODUCTION

As technology advances, it has made managing and storing data easier, but it has also opened the door to new cybersecurity risks. One growing threat is USB-based attacks, which take advantage of trusted devices like keyboards and mice to compromise systems. These attacks can let cybercriminals inject malware or steal sensitive information, and they are becoming a bigger concern for businesses everywhere. P4wnP1 is an open-source framework designed to run on Raspberry Pi devices, enabling them to perform a variety of offensive security tasks such as HID-based attacks, network spoofing, and credential harvesting. A.L.O.A. in the context of P4wnP1 stands for "A Little Offensive Appliance". It refers to the framework's capability to turn a Raspberry Pi into a versatile and compact tool for offensive security purposes, including HID-based attacks, network spoofing, and credential harvesting. The name reflects the framework's focus on providing a lightweight, yet powerful, platform for penetration testing and Red Team operations [1].

The primary challenge lies in the limited awareness among employees regarding the risks associated with these attacks. Moreover, existing training programs frequently fail to adequately address methods for identifying or preventing such threats. Consequently, organizations remain susceptible to attacks that exploit human errors and vulnerabilities in system security. Improper use of USB devices can circumvent security protocols and cause significant harm, including enabling attackers to escalate privileges within a compromised system [2][3].

This project seeks to tackle these issues by developing a tool that simulates HID-based USB attacks, helping organizations better educate their employees and identify potential weaknesses in their systems. The goal is to study existing USB attack methods, create a hands-on tool for testing and training, and assess its effectiveness in raising awareness about these threats.

The focus of this study is to create a practical tool using a Raspberry Pi Zero to simulate USB-based attacks. The research will also explore how to design realistic training scenarios for employees and acknowledge the challenges, such as needing physical access to devices to run tests. Ultimately, this project aims to bridge the gap between theory and practice, offering organizations a valuable resource to strengthen their cybersecurity defenses.

2.0 LITERATURE REVIEW

2.1 HID Attack

HID attacks have become a significant threat in cybersecurity due to their ability to exploit the trust operating systems place in USB devices. These devices, such as keyboards, mice, and USB peripherals, are commonly used in both professional and personal settings. However, when compromised, they can provide attackers with unauthorized access to systems and sensitive data. HID attacks take advantage of this trust to execute malicious actions, such as stealing data, installing malware, or compromising a system. Given the rise in cyberattacks using HID techniques, understanding these methods and the tools employed in real-world attacks is essential. HIDs are designed to seamlessly communicate with systems, making them attractive targets for cybercriminals who exploit this trust [4] [5].

2.2 Example of HID-Based Tools in Red Team Operations

In Red Team operations, HID-based tools are used to simulate real-world attack scenarios to evaluate how well an organization's security measures hold up against HID threats. These tools are employed to test systems and identify vulnerabilities that attackers could exploit. Below is a comparison of various HID-based tools commonly used in Red Team operations.

Table 1: Comparison of HID-Based Tools in Red Team Operations

Tool Name	Attack Technique	Microcontroller	Key Features	Typical Use Case
Teensy	Keyboard emulation, mouse emulation, HID payload execution	ARM Cortex-M4	Compact, easy to program, supports advanced HID emulation	Used for executing complex HID attacks like keystroke injection and mouse emulation [6]
Rubber Ducky	Keyboard injection	Custom hardware	Pre-programmed keystrokes, emulates a USB keyboard	Commonly used for simple and rapid attacks that involve automated keystroke injection [7]
P4wnP1	Keyboard and mouse emulation, HID over Wi-Fi, network attacks	Raspberry Pi Zero	USB device emulation, Wi-Fi capabilities, stealth features	Used for more advanced Red Team exercises that require remote control or multi-stage attacks [8]
BadUSB	Malicious payload injection	Custom firmware on USB devices	Can be reprogrammed to perform various malicious actions	Ideal for exploiting system vulnerabilities via USB [9]
Bash Bunny	Keystroke injection, network-based attacks	ARM Cortex A7	Supports multiple attack types, includes payloads for diverse attacks	Used for in-depth penetration testing and advanced attack simulations [10]
Digispark	Keyboard emulation, data exfiltration	ATtiny85 microcontroller	Small form factor, programmable via Arduino IDE	Used for small-scale, stealthy attacks, often in social engineering contexts [6]

2.3 Real-World Examples of HID Attacks by Advanced Persistence Threat

A well-documented case of HID misuse involves the Advanced Persistence Threat (APT) group FIN7 [11]. This group used USB drives disguised as harmless gifts to breach systems in enterprises. The USBs, once plugged into computers, would execute commands to install backdoors and collect sensitive data—all while avoiding detection. This sophisticated approach underscores how easily trust in everyday devices can be exploited [12].

2.4 Comparison Of Similar Studies

A comparison of studies focusing on HID-based attacks and tools. It outlines each study's objectives, methods, and key findings, showcasing how researchers have explored USB vulnerabilities, malicious tools, and defensive strategies. The studies range from analyzing specific attack techniques and tools, like Rubber Ducky and Bash Bunny, to proposing comprehensive threat models such as the HID framework. The table also highlights the

development of innovative tool of HID-Based Attacks for Red Team operations, emphasizing advancements in both offensive and defensive cybersecurity practices.

Table 2: Comparison of Similar Studies on HID-Based Attacks and Tools

Author(s)	Title	Objective	Methodology	Key Findings
Nissim et al. (2017) [13]	USB-Based Attacks	To explore data exfiltration through USB devices.	Analyzed USB devices as potential vectors for unauthorized data transfer and network traffic interception.	Highlighted vulnerabilities in USB devices for data theft and proposed mitigation techniques
Singh et al. (2019) [12]	A Comprehensive Study on APT Attacks and Countermeasures for Future Networks and Communications	To examine APT attacks, focusing on HID techniques.	Investigated the tactics and techniques of FIN7, a known APT group, in leveraging HID for sophisticated breaches.	Demonstrated how HID vulnerabilities can enable persistent system compromise and data exfiltration
Zhao & Wang (2019) [6]	A Survey of Malicious HID Devices	To explore HID devices used for malicious purposes.	Studied microcontroller-based devices like Teensy, Digispark, and Bash Bunny for HID exploitation.	Identified how these tools can be adapted for cyberattacks, from simple keystroke injections to complex payloads
Sabry (2022) [4]	Threat and Vulnerability Modeling of Malicious Human Interface Devices	To propose a comprehensive model for HID threats.	Developed the HID Threat and Vulnerability (HIDTV) model to map vulnerabilities and their exploitation paths.	Provided a detailed framework for predicting and mitigating HID-based attacks
Nicho & Sabry (2023) [9]	Bypassing Multiple Security Layers Using Malicious USB Human Interface Device	To analyze the exploitation of HID vulnerabilities.	Investigated vulnerability exploitation techniques using HID tools for bypassing security measures.	Emphasized the risk posed by keyboard emulation and malicious USB payloads in bypassing layered security systems

3.0 METHODOLOGY

The methodology for developing the USB-based Red Team tool followed the ADDIE model, which included analysis, design, development, implementation, and evaluation phases. The analysis phase focused on defining the tool's objectives and identifying the necessary features based on existing tools. In the design phase, the system architecture was planned, and diagrams were created to guide the integration of the Raspberry Pi Zero with the P4wnP1 A.L.O.A

framework. The development phase involved setting up the Raspberry Pi with the framework, writing custom attack scripts, and integrating the hardware into a PC speaker for stealth. During the implementation phase, the tool was tested in controlled environments to assess its performance in executing attacks. Finally, the evaluation phase involved assessing the tool's ability to perform attacks and refining it based on feedback to ensure it met the intended objectives and could be used effectively in penetration testing. This structured approach helped ensure the tool was developed efficiently, tested thoroughly, and refined based on real-world feedback, resulting in a robust and stealthy tool for simulating HID-based cyberattacks.

Figure 1 illustrates the key components and their interactions within the system. It shows how the Raspberry Pi Zero is connected to various devices and how it emulates USB peripherals, such as keyboards and storage devices, to execute HID-based attacks. The diagram highlights the flow of data between the Raspberry Pi and the target machine, detailing how the Raspberry Pi can trigger a sequence of attacks, including payload execution and data retrieval. It serves as a visual guide for understanding the tool's setup, function, and attack execution process.

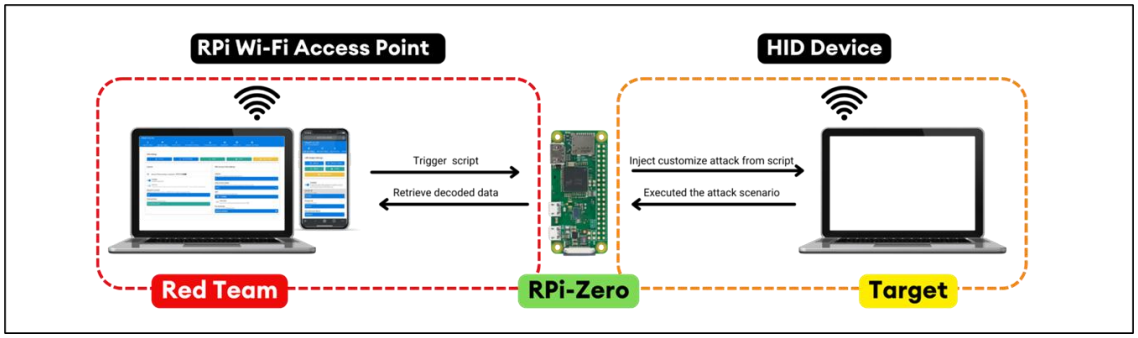

Figure: 1: Block diagram of P4wnP1 A.L.O.A using Raspberry-Pi Zero

Figure 2 illustrates the flowchart of P4wnP1 A.L.O.A outlines the sequential steps the system follows to execute HID-based attacks. It begins with powering up the Raspberry Pi and connecting it to a network. Once the connection is established, the system configuration is verified. The attacker then customizes the attack script, which is executed on the target machine. The tool monitors the progress of the attack and evaluates the results. If the attack is successful, feedback is provided; if not, the system prompts the attacker to adjust the script and retry. This flow ensures that the attack process is structured and adaptable for different scenarios.

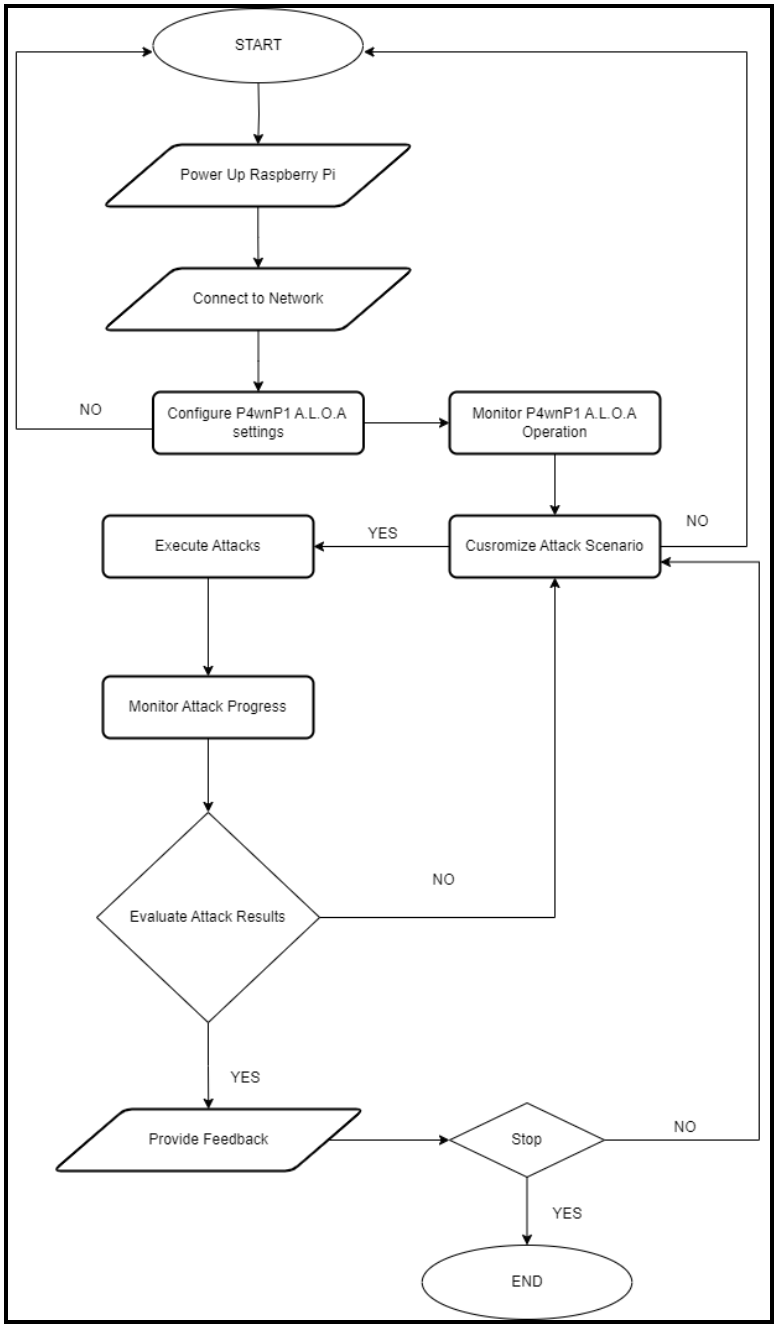

Figure 2: Flowchart of P4wnP1 A.L.O.A

Figure 3 refers to the design and integration of the Raspberry Pi Zero within a regular PC speaker, which was a crucial aspect of the hardware development for the USB-based Red Team tool. This integration allowed the Raspberry Pi to carry out HID-based attacks while maintaining the appearance and functionality of an ordinary speaker.

Figure 4 shows that the Raspberry Pi Zero was discreetly placed inside the speaker's casing, with the necessary modifications made to the speaker's internal circuitry. The Raspberry Pi was powered using a DC-DC step-up converter, ensuring that both the speaker and the Raspberry Pi

received the correct power supply. This configuration allowed the speaker to continue performing its regular function of emitting sound while the Raspberry Pi executed various cyberattacks such as keystroke injections, disabling security features, or launching malware.

By using this social engineering technique, where the device looks like a standard office item, the tool was able to avoid detection during its operations. The speaker effectively acted as a cover for the Raspberry Pi, enabling it to perform stealthy attacks without raising suspicion, making it ideal for Red Team and penetration testing activities.

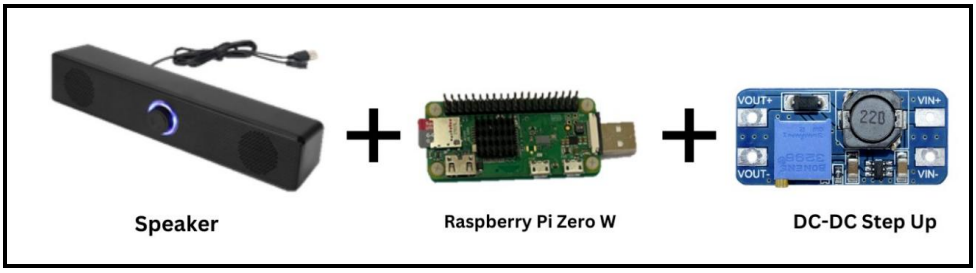

Figure 3: Integration of the Raspberry Pi Zero W and DC-DC Step-Up Converter inside a PC Speaker. This configuration allows the speaker to function normally while concealing the Raspberry Pi for executing HID-based attacks.

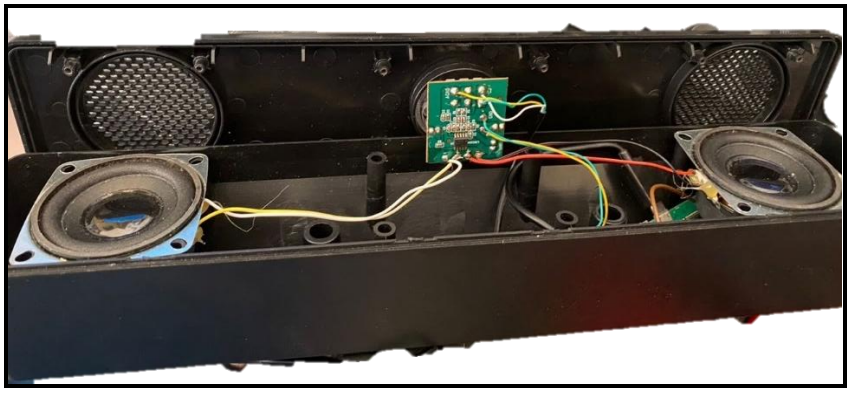

Figure 4: Fully Assembled PC Speaker with Embedded Raspberry Pi Zero W Running P4wnP1 A.L.O.A Framework.

4.0 CONCLUSION

The conclusion highlights the success of developing the USB-based Red Team tool using the P4wnP1 A.L.O.A framework on a Raspberry Pi Zero. The tool effectively simulated HID-based attacks, such as disabling security software, downloading malicious files, and executing ransomware, while maintaining stealth by being integrated into a regular PC speaker. This integration allowed the tool to remain undetected during operations, making it a valuable asset for Red Team and penetration testing. Despite its success, challenges with more advanced security measures were identified, suggesting that continuous updates and refinements are

needed. Overall, the tool proved to be a versatile and efficient solution for simulating real-world cyberattacks.

Author Contribution

Alif Imran bin Abdul Manaf: Methodology, investigation, visualisation, writing and editing. Wan Ainul Alyani Wan Mohamed: Investigation, supervision, writing, and editing. Siti Norwahidayah Wahab: Methodology, writing and editing.

Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

5.0 REFERENCES

[1] MaMe82. (2018). P4wnP1 A.L.O.A. 1–10. Retrieved from https://github.com/RoganDawes/P4wnP1_aloa

[2] EC-Council. (2021). Cybersecurity awareness in Malaysia: Aware: EC-Council. Retrieved from https://aware.eccouncil.org/cybersecurity-awareness-in-malaysia.html

[3] Pham, D. V., Syed, A., & Halgamuge, M. N. (2011). Universal serial bus-based software attacks and protection solutions. Digital Investigation, 7(3–4), 172–184. https://doi.org/10.1016/j.diin.2011.02.001

[4] Sabry, I. (2022). Threat and vulnerability modelling of malicious human interface devices. Technology, Engineering & Mathematics (EPSTEM), 21, 241–247. Retrieved from www.isres.org

[5] Brandao, P., & Scanavez, R. (2021). Bad USB: why must we discuss this threat in companies? Rrj, 2(3), 561–567. https://doi.org/10.52865/RR/2021-2-3-1

[6] Zhao, S., & Wang, X. A. (2019). A survey of malicious HID devices. In Lecture Notes in Networks and Systems (pp. 777–786). https://doi.org/10.1007/978-3-030-33506-9_71

[7] Potocký, S., & Štulrajter, J. (2022). The human interface device (HID) attack on Android lock screen non-biometric protections and its computational complexity. Science & Military, 17(1), 29–36. https://doi.org/10.52651/sam.a.2022.1.29-36

[8] Tolleson, B. (2023). Potential security vulnerabilities in Raspberry Pi devices with mitigation strategies. ODU Digital Commons.

[9] Nicho, M., & Sabry, I. (2023). Bypassing multiple security layers using malicious USB human interface device. 501–508. https://doi.org/10.5220/0011677100003405

[10] Patterson, C. (2017). IT security can create its own threats: Consider the "Bash Bunny" pen testing device. Exec Security TSCM. Retrieved from https://execsecurity.com/news/cybersecurity-threats-bash-bunny-pen-testing-device/

[11] Ahmed, D. (2023). FBI warns of hackers mailing malicious USB drives to spread ransomware. Hackread - Latest Cybersecurity News, Press Releases & Technology Today. Retrieved from https://www.hackread.com/fbi-hackers-mail-malicious-usb-drives-ransomware/

[12] Singh, S., Sharma, P. K., Moon, S. Y., Moon, D., & Park, J. H. (2019). A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. Journal of Supercomputing, 75(8), 4543–4574. https://doi.org/10.1007/s11227-016-1850-4

[13] Nissim, N., Yahalom, R., & Elovici, Y. (2017). USB-based attacks. Computers and Security, 70, 675–688. https://doi.org/10.1016/j.cose.2017.08.002