Lock pads information obtained from the internet

To conduct a thorough investigation of the vulnerabilities in Master Lock's 4400 Bluetooth lock and the 4901 biometric lock, it was essential to follow the Cyber Kill Chain framework and commence with the reconnaissance phase. In order to achieve this, I performed a series of activities, beginning with extensive research to gather as much information as possible about the target device from the internet. This involved locating official documentation for the locks, examining their specifications, understanding their operational mechanisms, and so on.

Master Lock Bluetooth Padlock (4400)

- Bluetooth Low Energy (BLE) keyless device that operates using Bluetooth Smart Protocol
- Can be unlocked via a mobile device or by entering a directional code on the lock keypad
- Sharing access is possible via the Master Lock Vault Home app with temporary and permanent sharing options
- Battery life lasts approximately two years under normal usage and up to four months under continuous phone mode
- The app offers tamper and low-battery alerts, access management, and audit trails for enhanced control, security, and convenience
- Not weatherproof, cannot be used outdoors.

Master Lock 4901DLH Biometric Padlock

- Biometric access control through fingerprints for up to 10 users.
- It has a backup access method via a directional code on the lock keypad.
- The lock has light indicators for notifications and an easy-to-replace CR2 battery.
- It does not require a smartphone app or data permissions for use.
- All functions are onboard and do not require any form of wireless connection.

Used tools

After gathering some initial information, I conducted research to determine the tools that would be most effective for snooping and conducting further investigation. I wanted to ensure that I had the right resources at my disposal in order to obtain the necessary information and make informed decisions. By carefully considering my options and selecting the best tools for the job, I was able to proceed with my investigation. Tools used for the investigation were the following:

- Kali Linux - a Debian-based open-source operating system designed for digital forensics and penetration testing, providing a platform for ethical hacking and security assessments. It was leveraged to use the tools further down the list.
- VMWare - software for creation and management of virtual machines (VMs). This was used to run Kali Linux.
- Bluetooth dongle TP-Link - a small device that allows a machine to communicate with other Bluetooth-enabled devices. In this case providing the kali machine with Bluetooth properties.
- hciconfig - a Linux command-line tool that is used to configure Bluetooth devices. It is used to enable and disable Bluetooth adapters, set their name, Bluetooth address, power settings, and more.

- hcitool - a command-line utility in Linux used to configure and interact with Bluetooth devices. It can be used to scan for nearby Bluetooth devices, display information about connected devices, connect to or disconnect from devices, and manipulate various Bluetooth settings.
- bettercap – is a tool used for network monitoring, network attacks, and security testing. It provides a wide range of features such as ARP spoofing, DNS spoofing, SSL stripping, and session hijacking, among others. Can be used for network reconnaissance, vulnerability scanning, and penetration testing.
- gatttool - a command-line tool used to connect and interact with devices that support the Bluetooth Low Energy (BLE) protocol. It allows users to establish a connection with a BLE device and explore its services, characteristics, and descriptors, as well as read and write its values.
- Wireshark – a network protocol analyzer that allows users to capture and analyze network traffic in real-time. It can be used to troubleshoot network issues, analyze security vulnerabilities, and perform various network-related tasks. For this specific case it was used to capture Bluetooth network packets and intercept communication between the Bluetooth lock and another device.

Bluetooth device recon

After conducting research on the device, I proceeded with the third step, which involved utilizing the tools and knowledge acquired to gather more detailed information about the device. I used various techniques and tools to obtain a comprehensive understanding of the device, which enabled me to gather more information about its functionalities, features, vulnerabilities, and weaknesses. By using the available tools, I was able to dig deeper into the device's structure and design, as well as its communication protocols, to identify any potential security gaps or flaws. This process of obtaining additional information through practical application and analysis allowed me to form a completer and more accurate picture of the device, which was crucial for further analysis and decision-making.

hciconfig

To begin the reconnaissance process using Kali Linux, the first step was to connect and utilize a Bluetooth dongle. This dongle was connected to the computer's USB port to enable Bluetooth communication on the virtual machine. After that, the Bluetooth adapter was activated using the hciconfig command. This command is used to configure Bluetooth devices on Linux systems. Video 1.1[1] provides a visual demonstration of these steps.

hcitool

After turning on my Bluetooth adapter, the next step was to scan for the device. Based on my research, I knew that the Bluetooth lock I was trying to find was a BLE (Bluetooth Low Energy) device. This meant that a normal scan using hcitool would not be able to detect it. Therefore, I used the lescan command, which scans specifically for BLE devices. Video 1.2[1] shows the scan in action, which provided me with the bdaddr (similar to a MAC address) and the name of the device. This information was crucial for further investigation and possible exploitation of the device.

gatttool

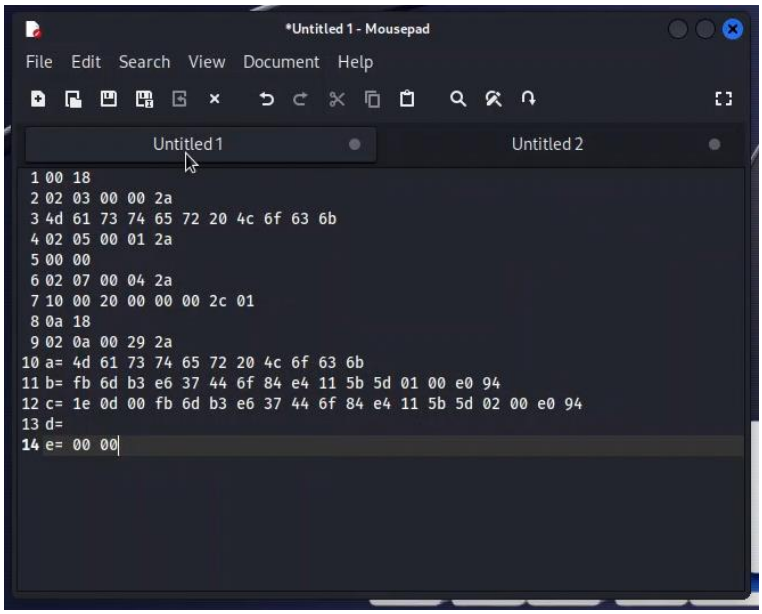
As the next step of my reconnaissance process, I employed gatttool in interactive mode to establish a connection with the Bluetooth lock and extract additional information from the device. After successfully connecting to the device, I executed the "primary" command to retrieve a list of services

that the device provides. In video 1.3[1], it can be seen that a service's UUID defines the properties and metadata of the accessed attribute, while the handle gives the address of a specific attribute. This information is useful in identifying the functions and characteristics of the lock and determining which attributes to explore further. By accessing the lock's services and attributes, I could gather valuable data that could help me identify vulnerabilities or potential attack vectors.

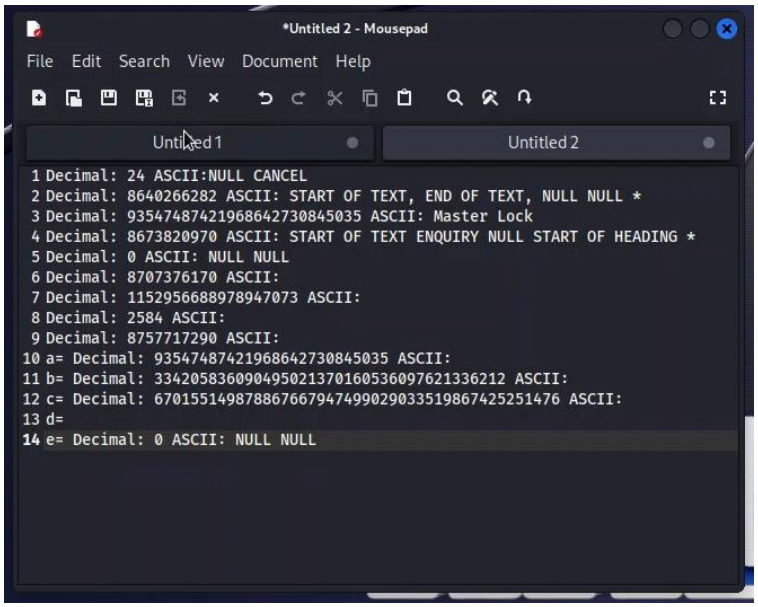
After successfully retrieving a list of services on the Bluetooth lock, I proceeded to extract more information by executing the "char-desc" command in gatttool interactive mode. This command provided me with a comprehensive list of handles and their corresponding UUIDs for the characteristics of the services obtained in the previous step. The step-by-step process of executing the "char-desc" command is demonstrated in video 1.4[1].

After successfully retrieving the list of handles and their corresponding UUIDs, I proceeded to the next step in my reconnaissance process. This involved using the "char-read-hnd [handle]" command to read the data from all the handles. The command returns the handle's data in hexadecimal format, which can then be decoded and translated to ASCII or decimal if not encrypted (the lock uses AES 256-bit encryption). Analyzing this data further and reading it can be crucial in discovering vulnerabilities and potential attack vectors in the Bluetooth lock. Video 1.5[1] provides a demonstration of this process.

The information I managed to extract from the handles, after decoding them, is presented in Pictures 1.1 and 1.2 below. These pictures display important data that could potentially reveal details about the device's functionalities, security measures, and other crucial information. The decoded data can aid in developing an understanding of the device's inner workings and help in formulating further steps for reconnaissance or attacking.



Picture 1.1 RAW data



Picture 1.2 Decimal and ASCII data

bettercap

As part of my reconnaissance process, I also utilized bettercap tool to gather information about the Bluetooth lock. I initiated the ble.recon command to scan and locate the Bluetooth lock, followed by the ble.enum command to obtain a list of services and characteristics available on the BLE device. Using the ble.write command, I attempted to write data into the handle which was found to be writable. However, it was discovered that only two values, 0 and 1, could be written. Video 1.6[1] showcases the aforementioned steps in detail.

Wireshark

To supplement my use of gatttool and bettercap, I also utilized Wireshark to inspect the packets being transmitted between the Bluetooth lock and its connected device. Wireshark allowed me to analyze the packets at a deeper level, which provided me with a more comprehensive understanding of the communication between the two devices. By analyzing the packet data, I was able to identify patterns and glean further information that was not readily apparent through other methods. Video 1.7[1] provides a detailed overview of the captured packets and their contents, as well as other relevant information obtained through the use of Wireshark.

Flipper zero

Upon conducting research and experimenting with the flipper zero, it was discovered that the device lacks the functionality to act as a master device in a Bluetooth Low Energy (BLE) connection. Specifically, the flipper zero can only serve as a client device and cannot act as a master device to connect to a BLE slave device such as the Bluetooth lock.

In the case of the Bluetooth lock, the authorized phone acts as a master device while the lock acts as a slave device. However, the flipper zero can only connect to a master device manually by the user.

It's important to note that the flipper zero is constantly evolving and its capabilities may change with future updates or revisions.

References

4400

Bluetooth lock 4400 information on the internet:
4400EC Bluetooth & Electronic Locks | Master Lock. (n.d.).
https://www.masterlock.com/products/product/4400EC

Battery safety datasheet
https://cdn.masterlock.com/masterlock/resources/documents/pdf/ML_SDS_CD-001396.pdf

Lock Instruction guide https://cdn.masterlock.com/electronic-products-support-documents/4400ENT-4401LHENT_Padlock-Instruction-Guide.pdf

Lock. (n.d.). Model No. 4400EURD | Master Lock. https://www.masterlock.eu/home-personal/product/4400EURD

Master Lock 4400D bluetooth hangslot - deurbeslag.nl. (n.d.). https://www.deurbeslag.nl/master-lock-4400d-hangslot.html#long-desc

Master Lock Padlock, Bluetooth Lock, 1-29/32 in. Wide, 4400 (Pack of 2) - - Amazon.com. (n.d.).
https://www.amazon.com/Master-Lock-Padlock-Bluetooth-1-29/dp/B071477RQ9

Master Lock. (n.d.). https://www.fbisecurity.com/master-lock-440-bluetooth-padlock.html

Master Lock 4400EC Bluetooth® Indoor Padlock for Business Applications | Taylor Security & Lock. (n.d.).
https://www.taylorsecurity.com/master-lock-4400ec-bluetooth-indoor-padlock-for-business-applications/

PCMag. (2017, January 20). Master Lock 4400D Indoor Bluetooth Padlock Review. PCMAG.
https://www.pcmag.com/reviews/master-lock-4400d-indoor-bluetooth-padlock

New Atlas. (2016b, March 26). Review: Master Lock Bluetooth smart padlock. New Atlas.
https://newatlas.com/master-lock-bluetooth-smart-padlock/40745/

DATA-SHEET-BLE-PADLOCK-INDOOR https://www.patchindustrial.co.za/wp-content/uploads/2016/06/DATA-SHEET-BLE-PADLOCK-INDOOR.pdf

BosnianBill. (2016, August 2). (897) Review: Master Lock Bluetooth Smart Padlock (JUNK!) [Video]. YouTube. https://www.youtube.com/watch?v=YsKMsvx8vvo

Masterlock 4400D Indoor Bluetooth Programmable Padlock. (n.d.). Your Site Name Goes Here.
https://sbsimpson.com/product/master-lock-4400d-indoor-bluetooth-padlock-safety-and-security-80-04448/

4901

4901DLH Bluetooth & Electronic Locks | Master Lock. (n.d.).
https://www.masterlock.com/products/product/4901DLH

4901DLH Biometric Lock Sheet
https://cdn.masterlock.com/masterlock/resources/documents/pdf/4901_Instruction_Sheet.pdf

Lock. (n.d.-b). Model No. 4901EURDLH | Master Lock. https://www.masterlock.eu/home-personal/product/4901EURDLH

https://www.amazon.com/Master-Lock-4901DLH-Fingerprint-Biometric/dp/B082TG3B32

Source, L. (n.d.). Master Lock 4901DLH Biometric Lock. The Lock Source. https://www.thelocksource.com/products/master-lock-4901dlh-lock-biometric-fingerprint-padlock-keyless-locks-support-up-to-10-finger-prints

Recon research using kali

Wolff, J. (2021). Get Started With Bluetooth Low Energy. www.jaredwolff.com. https://www.jaredwolff.com/get-started-with-bluetooth-low-energy/

UUID Decoder | UUIDTools.com. (n.d.). https://www.uuidtools.com/decode

Matt Brown. (2022, October 17). Bluetooth Low Energy Hacking Part 1 - Intro to Bluetooth Low Energy Security [Video]. YouTube. https://www.youtube.com/watch?v=lhLff9VACU4

Cannot connect to BLE device on Raspberry Pi. (n.d.). Stack Overflow. https://stackoverflow.com/questions/32947807/cannot-connect-to-ble-device-on-raspberry-pi

Matt Brown. (2022b, October 17). Bluetooth Low Energy Hacking Part 2 - Sniffing Bluetooth Low Energy [Video]. YouTube. https://www.youtube.com/watch?v=dsZN0dqh81k

Sławomir Jasek. Hacking Bluetooth Smart Locks-workshop https://smartlockpicking.com/slides/BruCON0x09_2017_Hacking_Bluetooth_Smart_locks.pdf

Null Byte. (2019, May 17). Identify & Target Bluetooth Devices with Bettercap [Tutorial] [Video]. YouTube. https://www.youtube.com/watch?v=YDpjGTojByw

Team, A., & Team, A. (2022). Tools for Recon Bluetooth Devices by using Kali Linux | All About Testing. All About Testing. https://allabouttesting.org/tools-for-recon-bluetooth-devices-by-using-kali-linux/

Meyers, J. (2020, January 20). *Snoop on Bluetooth Devices Using Kali*. WonderHowTo. https://null-byte.wonderhowto.com/how-to/bt-recon-snoop-bluetooth-devices-using-kali-linux-0165049/

Wolff, J. (2021b). Get Started With Bluetooth Low Energy. www.jaredwolff.com. https://www.jaredwolff.com/get-started-with-bluetooth-low-energy/

Document videos