|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Kierunek:**  **CBE** | **Nazwa zajęć:**  **LABORATORIUM SIECI BEZPRZEWODOWYCH** | | | | **Ocena:** |
| **Nr. ćwiczenia:**  **1** | **Tytuł ćwiczenia:** | | | | |
| Bezpieczeństwo systemów Bluetooth Classic oraz Bluetooth Low Energy | | | | |
| **Termin:**  **Piątek 11:15 gr. P** | | **Data wykonania ćwiczenia:**  **17.10.2025** | | **Nr. grupy:**  **1** | |
| **Osoby wykonujące ćwiczenie:** | | | | **Podpisy:** | |
|  | | | |  | |
| Adam Wiktor | | | | Obraz zawierający czarne, ciemność  Zawartość wygenerowana przez AI może być niepoprawna. | |
| Kacper Powolny | | | |  | |
| Mateusz Jakoniuk | | | |  | |
|  | | | |  | |
| **Sprawozdanie wykonał:** | | | **Adam Wiktor** | | |
| **Data wykonania sprawozdania:** | | | **19.10.2025** | | |
| **Sprawozdanie sprawdził:** | | | **dr. inż. Michał Kowal** | | |

Oświadczam, że zapoznałem/łam się ze niniejszym sprawozdaniem i uważam je za poprawnie wykonane:

…………………. …………………. …………………. ………………….

Oświadczam/y iż poniższe sprawozdanie zostało wykonane przeze mnie/nas samodzielnie:

Obraz zawierający czarne, ciemność

Zawartość wygenerowana przez AI może być niepoprawna. Jakoniuk Powolny

…………………. …………………. …………………. ………………….

Cel ćwiczenia

1. Zgłębienie aspektów bezpieczeństwa systemów Bluetooth Classic oraz Bluetooth Low Energy.
2. Zapoznanie się z metodami ataku na system Bluetooth.
3. Zrozumienie podatności systemu Bluetooth.
4. Zapoznanie się z narzędziami do testowania bezpieczeństwa sieci Bluetooth zawartych w systemie Kali Linux.

Wykorzystany sprzęt i oprogramowanie

1. Dwa komputery z systemem operacyjnym Kali Linux.
2. Laptop z systemem operacyjnym Arch Linux.
3. Dwa adaptery Bluetooth.
4. Słuchawki SteelSeries Arctis Nova 5X.
5. Telefon Pixel 8 Pro.
6. Telefon iPhone.
7. Oprogramowanie zawarte w systemie operacyjnym Kali Linux.

Przebieg ćwiczenia

Rekonesans

sudo hciconfig

hci0: DOWN, adapter należy włączyć.

sudo hciconfig hci0 up

Ze względu na błąd (RF-KILL 132) musieliśmy dodatkowo wykonać komendę - rfkill unblock bluetooth, po wykonaniu tych dwóch: hci0: UP RUNNING.

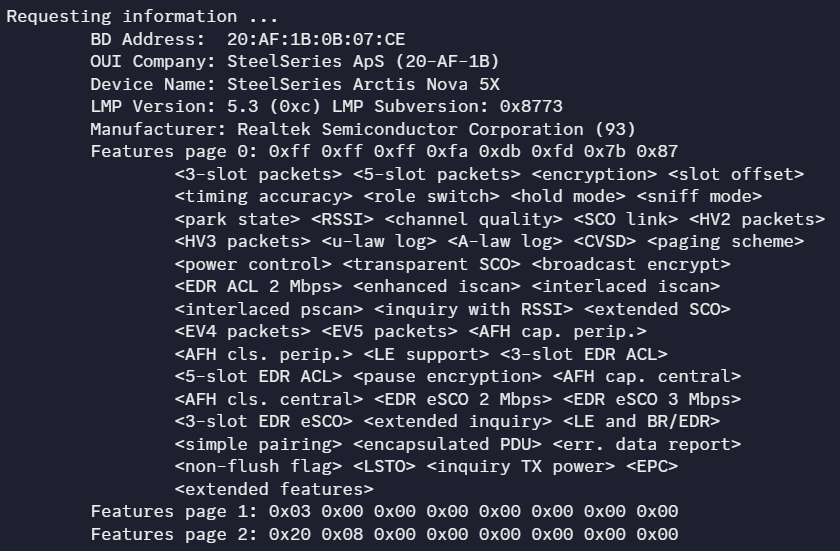
sudo hcitool scan

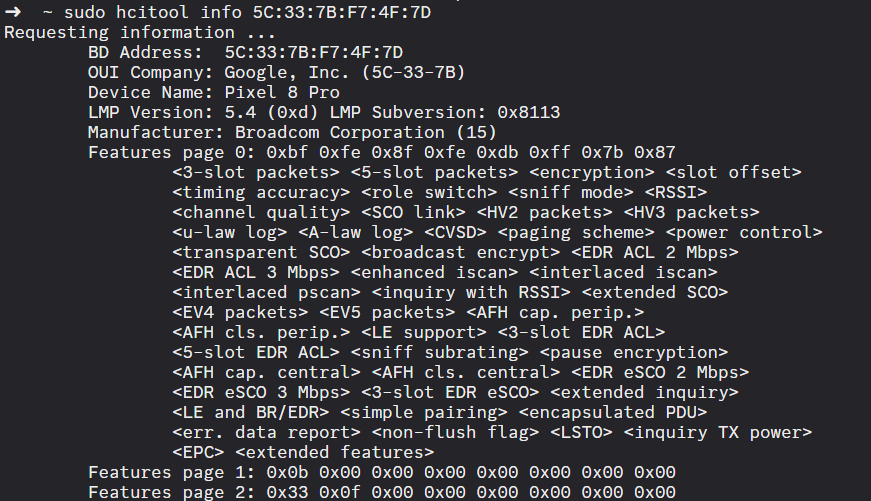
Scanning… Pierwszy skan nie zwrócić niczego, ale później udało się znaleźć urządzenia:

* **20:AF:1B:0B:07:CE SteelSeries Arctis Nova 5X**
* **5C:33:7B:F7:4F:7D Pixel 8 Pro**
* **08:C8:C2:73:E1:0D Adapter Bluetooth – Kali Linux**
* 28:C1:A0:3D:06:72 iPhone (Kacper)

W kolejnych zadaniach skupimy się na pierwszych trzech urządzeniach.

sudo hcitool info <adres MAC>





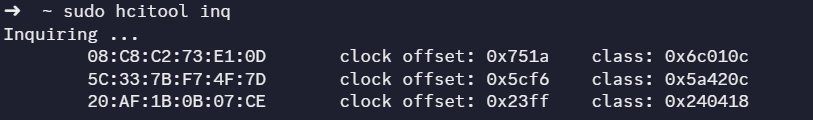
Obraz zawierający tekst, zrzut ekranu, Czcionka, dokument

Zawartość wygenerowana przez AI może być niepoprawna.

Wynik 1-3: hcitool dla słuchawek, telefonu i laptopa

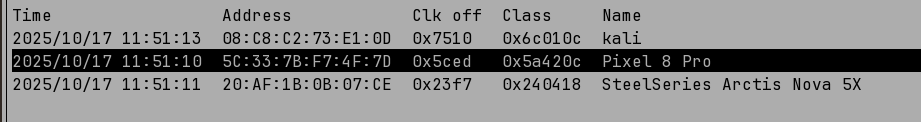
Poza adresem MAC widać dodatkowo informacje o producencie, nazwę urządzenia, wersję protokołu LMP (służącego do zarządzania połączeniami Bluetooth), a także „Features page”, o których można więcej poczytać w specyfikacji standardu Bluetooth.

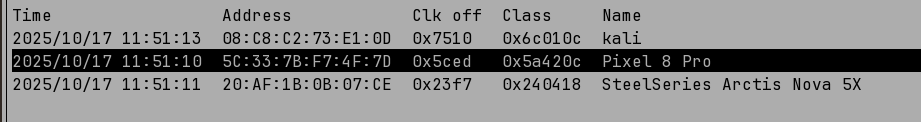
sudo hcitool inq



sudo btscanner

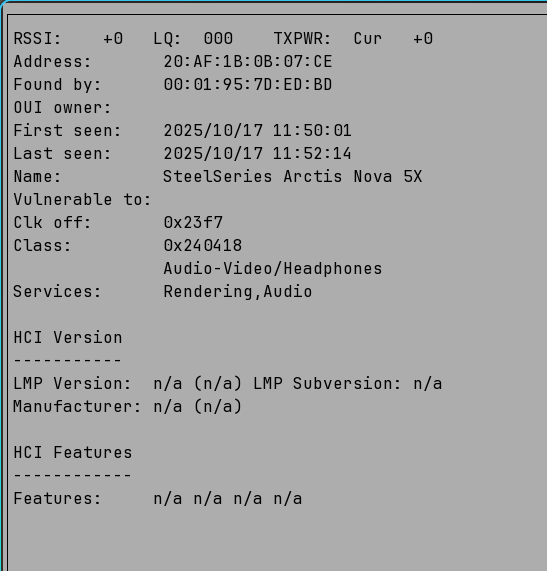
btscanner pokazuje bardzo podobne informacje o tych samych urządzeniach, ale jest interaktywny. Dodatkowo, ten program „tłumaczy” nazwy klas na rzeczywiste typy urządzeń – laptop, słuchawki, telefon.





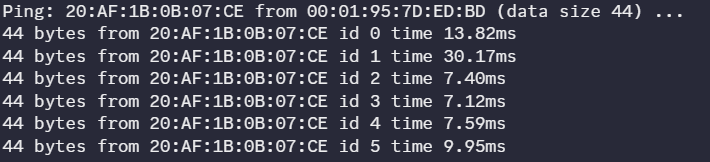
Obraz zawierający tekst, zrzut ekranu, dokument, Czcionka

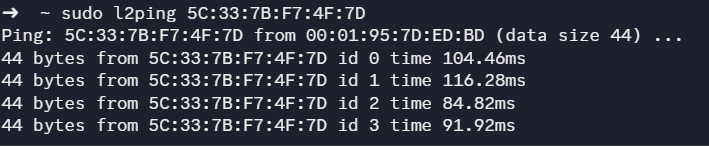
Zawartość wygenerowana przez AI może być niepoprawna.



sudo l2ping <adres MAC>

Ping wykonany na wszystkie urządzenia zakończył się sukcesem – odpowiadają ode na pakiety.

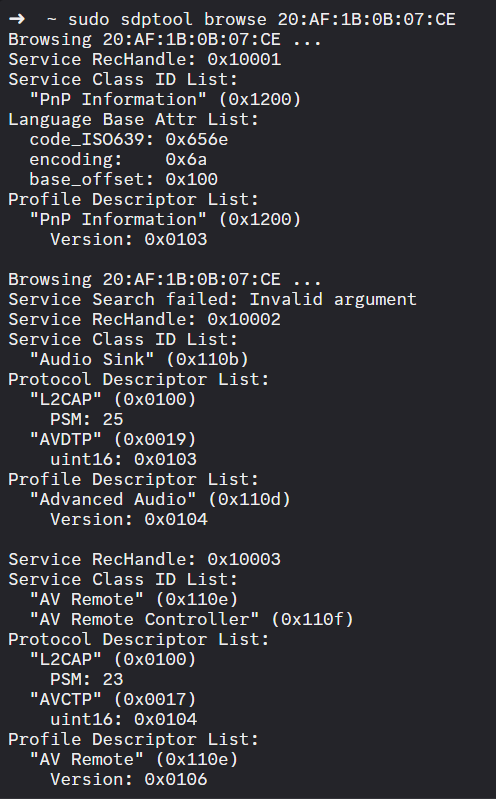


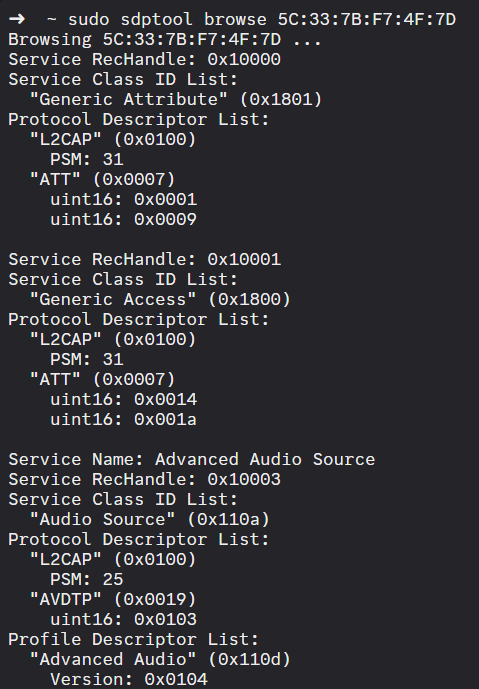


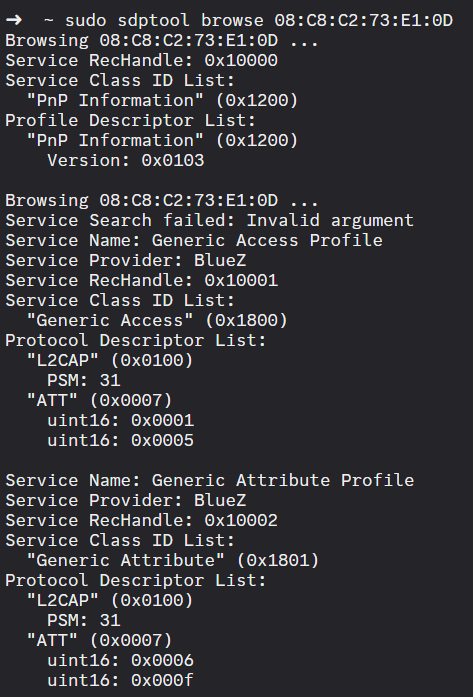
Obraz zawierający tekst, Czcionka, zrzut ekranu

Zawartość wygenerowana przez AI może być niepoprawna.

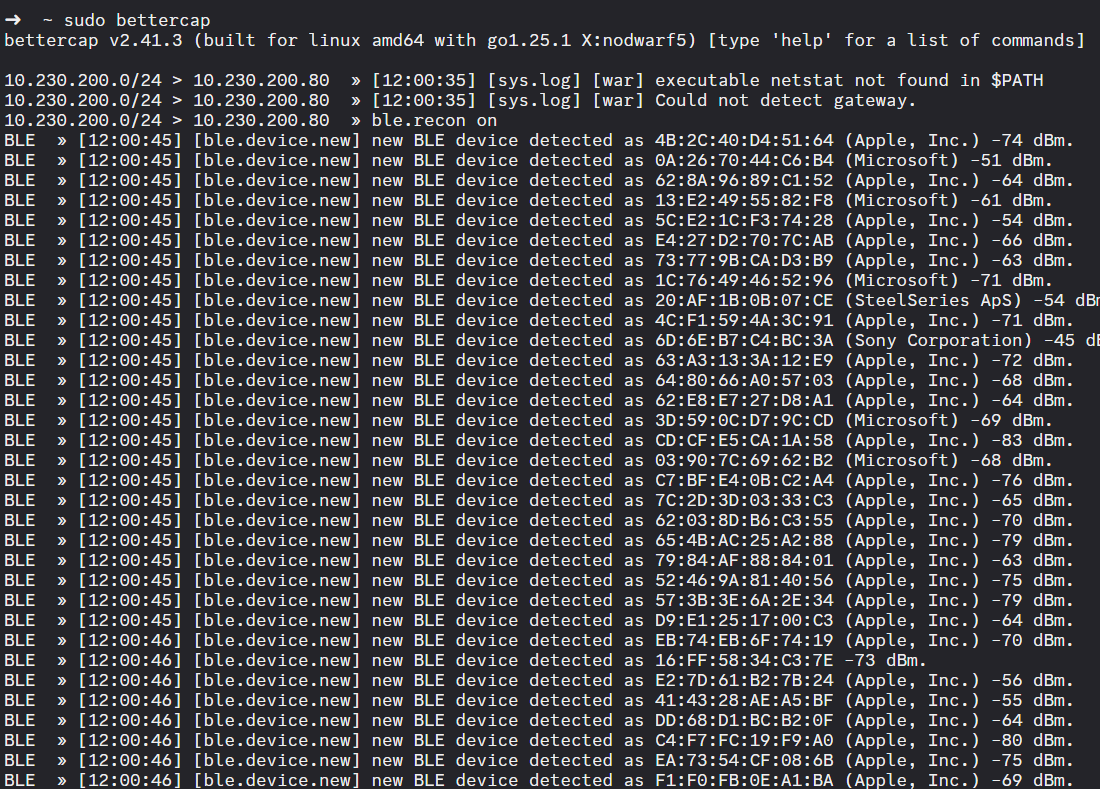
sudo sdptool browse <adres MAC>



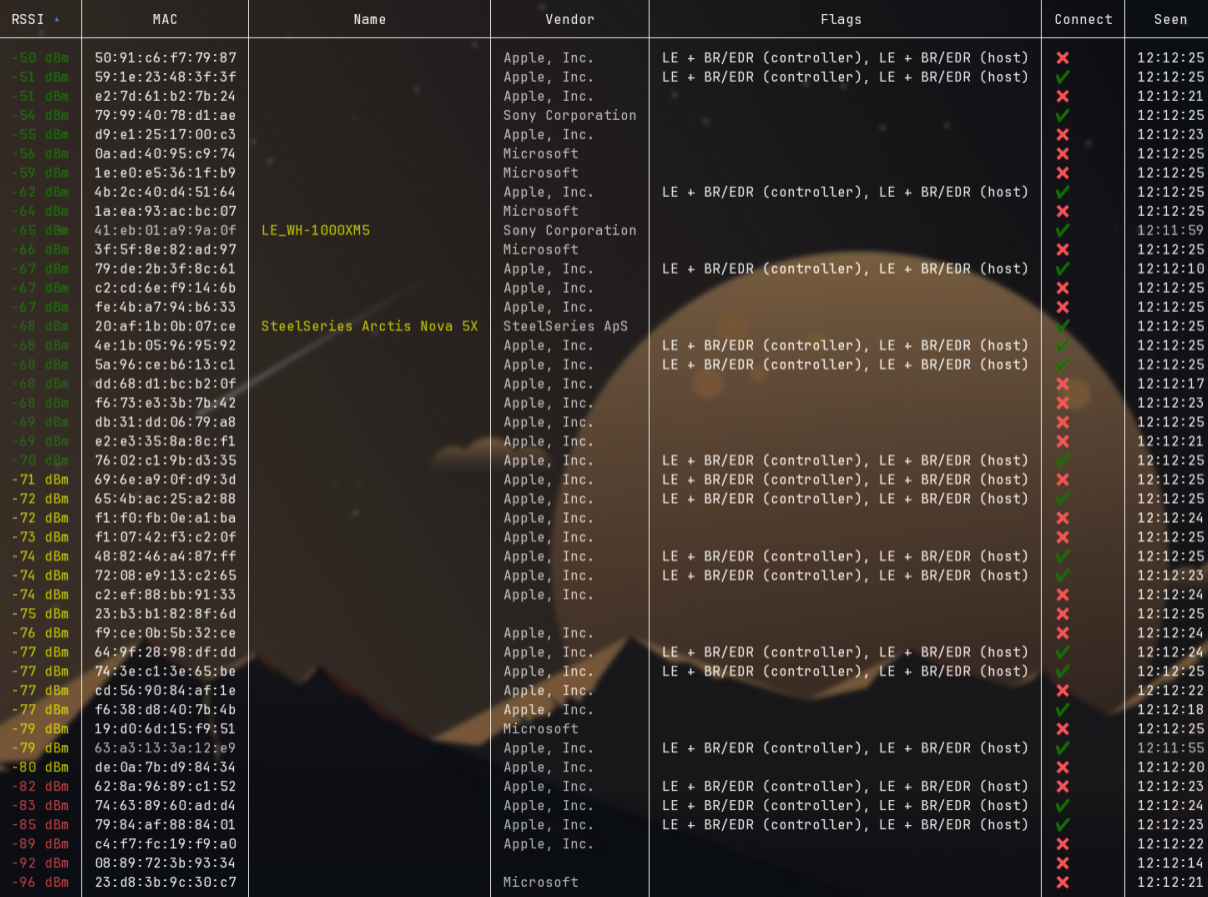




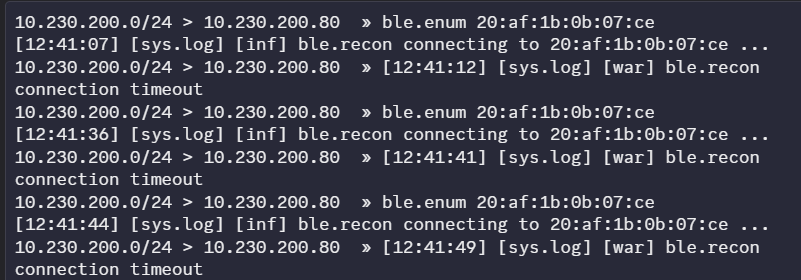
sudo bettercap



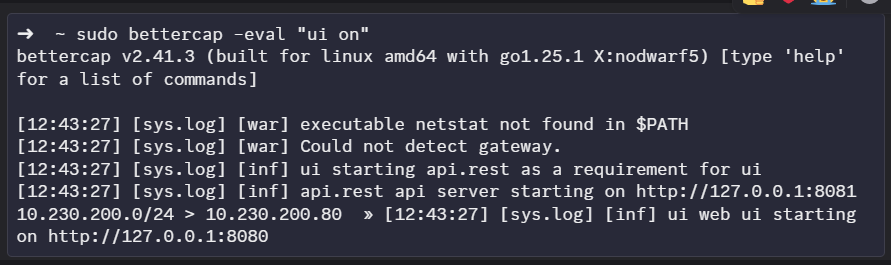
ble.recon on -> ble.recon off -> ble.show



ble.enum <adres MAC>



sudo bettercap -eval “ui on” – skan urządzeń BLE, porównanie z ble.enum

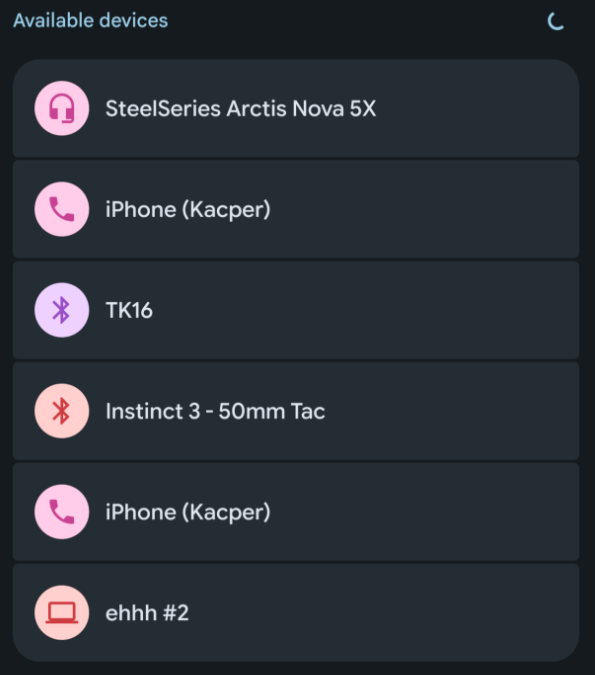


Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Zawartość wygenerowana przez AI może być niepoprawna.

Spoofing Bluetooth Devices

Jako cel obraliśmy słuchawki telefon iPhone (Kacper). Ponownie zostało użyte narzędzie btscanner żeby zdobyć informacje. Po wykonaniu poleceń, Kali Linux podszywający się pod telefon Kacpra pojawił się w możliwych połączeniach Bluetooth.

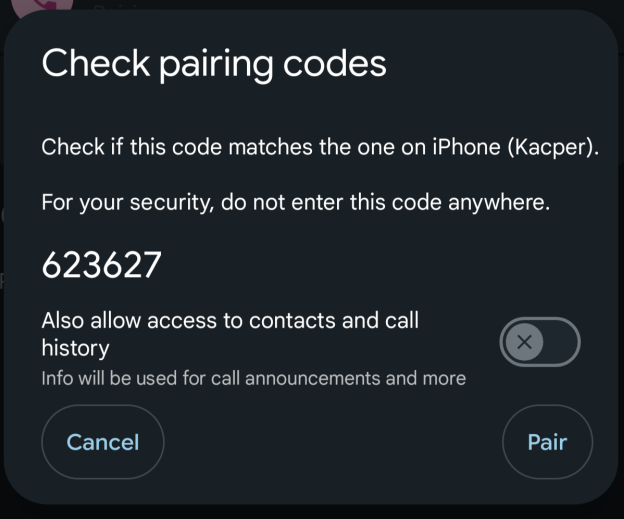


Skan pokazuje, że rzeczywiście są dwa teoretycznie takie same urządzenia, ale o innym adresie MAC.

Obraz zawierający tekst, paragon, Czcionka, zrzut ekranu

Zawartość wygenerowana przez AI może być niepoprawna.

Po zmianie adresu MAC na Kali Linuxie, widać było tylko jedno urządzenie – iPhone (Kacper), do którego podłączono się telefonem Pixel.



Atak Man-in-the-Middle

Server proxy został uruchomiony na pierwszym Kali Linuxie po próbach naprawy – niestety program ostatni raz był aktualizowany około 7 lat temu.

Drugi Kali Linux połączył się z proxy, o czym został powiadomiony serwer. Na localhost:8080 próbowano wybrać cel, ale wtedy otrzymaliśmy nieznany błąd na proxy.

Bluetooth Off-by-One

Po zatrzymaniu procesów wpływających na interfejs bezprzewodowy (905 wpa\_supplicant), włączono tryb monitorowania na karcie bezprzewodowej wlan0. Po użyciu narzędzia tshark nie udało się jednak znaleźć adresów MAC spełniających warunek off-by-one. Następnie wyłączony został tryb monitorowania.

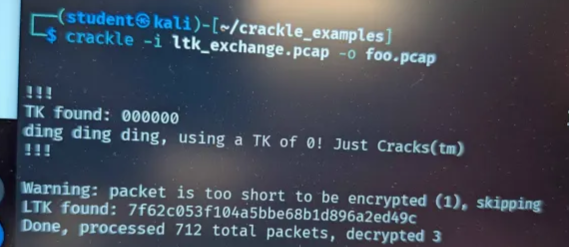
[zdjecie kacpra]

bluetooth\_tools nie zostało wgrane na nasze maszyny z Kali Linux, zatem nie byliśmy w stanie dokończyć zadania.

Bluetooth Low Energy TK Cracking

Po pobraniu plików z eportalu zostały wykonane komendy:

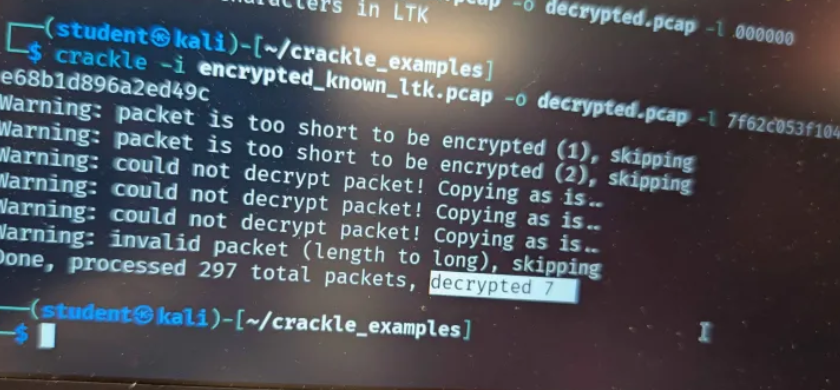
crackle -i ltk\_...



TK found: 000000

LTK found:

crackle -i encrypted\_known\_ltk…



Decrypted: 7

Classic PIN Attack

Narzędziem btcrack zostały zcrackowane przechwycone dane do złamania klucza LK i kodu PIN, w wyniku tego zostały wyeksportowane informacje:

Obraz zawierający tekst, zrzut ekranu, miejsce parkingowe/przestrzeń, Czcionka

Zawartość wygenerowana przez AI może być niepoprawna.

PIN:

Link Key:

Wnioski, obserwacje i analiza

Lorem ipsum dolor sit amet, consectetur adipiscing elit. In placerat neque sit amet felis tincidunt bibendum eget id odio. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Ut ac purus dictum, convallis magna vitae, malesuada risus. Pellentesque gravida dolor a porta ultrices. Quisque sit amet vulputate dolor. Curabitur eleifend vel augue in aliquam. Cras vitae fermentum tortor. Morbi sed lectus dapibus ex vestibulum tempus. Suspendisse eu urna enim. Donec eget erat lorem.