|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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:** | | | **25.10.2025** | | |
| **Sprawozdanie sprawdził:** | | | **dr. inż. Michał Kowal** | | |

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

Obraz zawierający czarne, ciemność

Zawartość wygenerowana przez AI może być niepoprawna.

Obraz zawierający czarne, ciemność

Zawartość wygenerowana przez AI może być niepoprawna.

…………………. …………………. …………………. ………………….

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

Obraz zawierający czarne, ciemność

Zawartość wygenerowana przez AI może być niepoprawna.

Obraz zawierający czarne, ciemność

Zawartość wygenerowana przez AI może być niepoprawna.

…………………. …………………. …………………. ………………….

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.

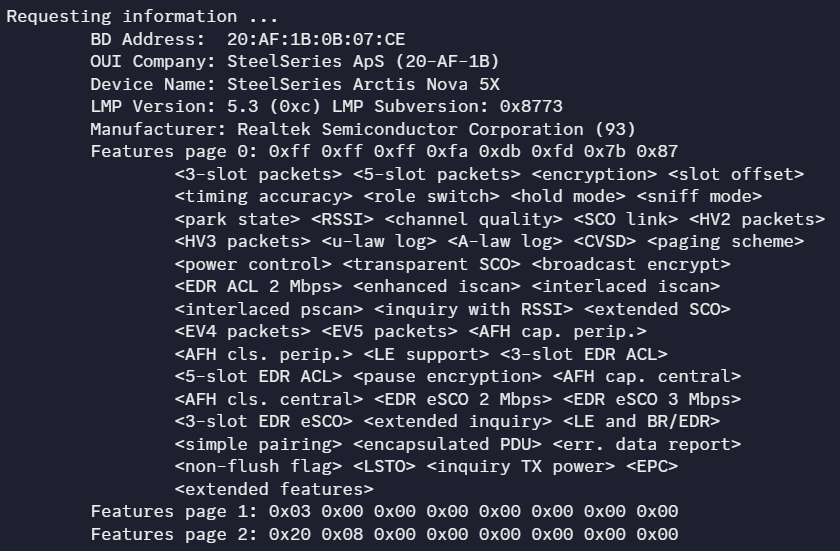
sudo hcitool scan

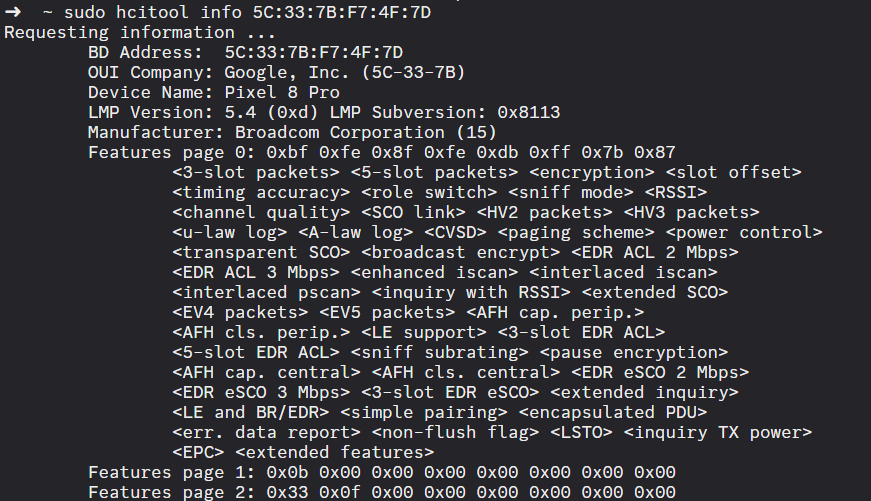
Scanning… Pierwszy skan nie zwrócić niczego, ale później udało się znaleźć urządzenia:

* **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>





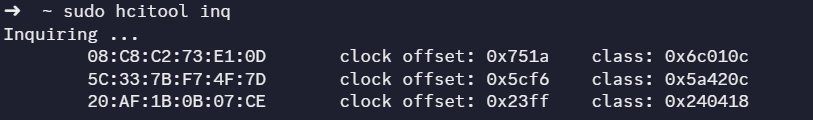
Obraz zawierający tekst, zrzut ekranu, Czcionka, dokument

Zawartość wygenerowana przez AI może być niepoprawna.

Wynik : 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

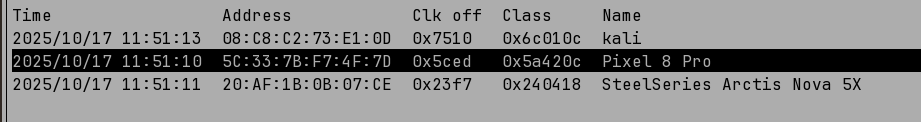


Wynik : hcitool inq wykonany w pobliskiej sieci – widoczny kolejno laptop, telefon i słuchawki

Komenda zwraca listę urządzeń Bluetooth w zasięgu wraz z ich adresem MAC – dokładnie te same, co opisaliśmy wcześniej. Obok tych fizycznych adresów widać clock offset (potrzebny do synchronizacji) oraz klasę – opisuje ona typ urządzenia, lecz zwracana jest ona jako liczba szesnastkowa.

sudo btscanner

btscanner pokazuje bardzo podobne informacje o tych samych trzech urządzeniach, ale jest interaktywny. Dodatkowo, ten program „tłumaczy” nazwy klas na rzeczywiste typy urządzeń – laptop, słuchawki, telefon. Po wybraniu urządzenia, można dokonać jego dokładniejszej analizy, podobnej do tej przedstawionej w hcitool info. Widoczne są jednak jeszcze inne informacje, takie jak „First seen”, „Last seen”, „Vulnerable to”, „Services”. Z niewyjaśnionego jednak powodu to narzędzie nie było w stanie dokonać poprawnej analizy słuchawek SteelSeries – zwrócone zostało n/a zamiast rzeczywistych informacji, które zostały znalezione przez poprzedni program.



Poniżej można zobaczyć dokładne opisy trzech urządzeń, na których się skupiliśmy

Obraz zawierający tekst, zrzut ekranu, dokument, Czcionka

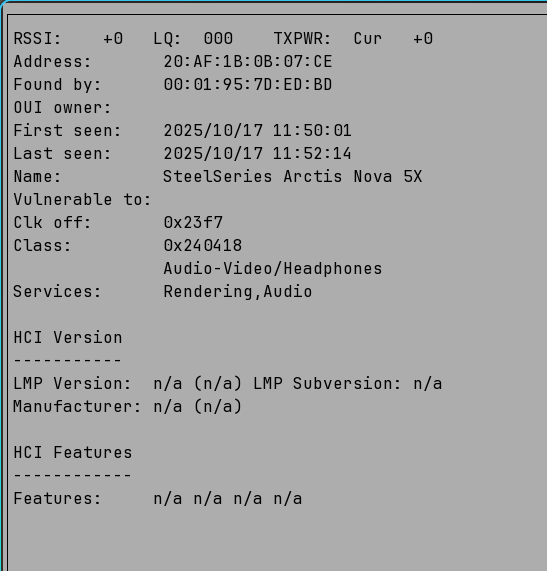
Zawartość wygenerowana przez AI może być niepoprawna.

Wynik : Opis laptopa Kali Linux wykonany btscanner

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Zawartość wygenerowana przez AI może być niepoprawna.

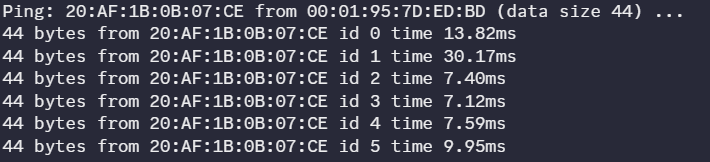
Wynik : Opis telefonu Pixel wykonany btscanner

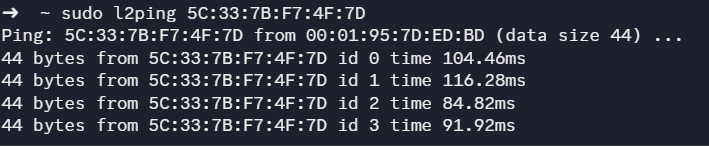


Wynik : niekompletny opis słuchawek SteelSeries wykonany btscanner

sudo l2ping <adres MAC>

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





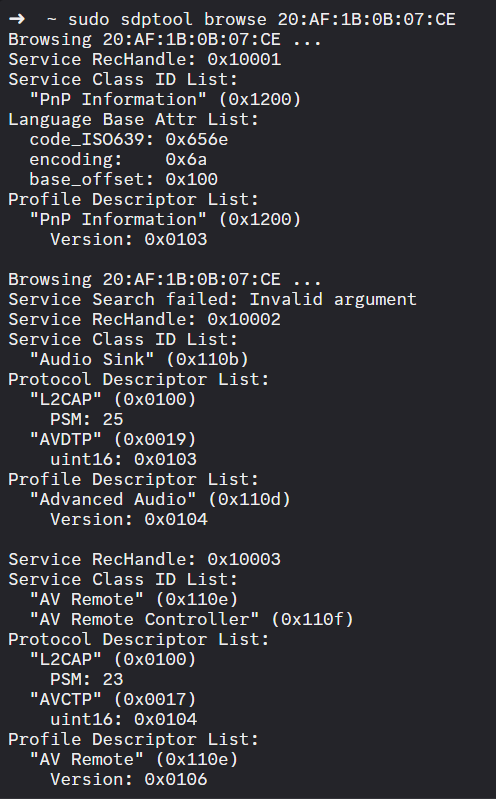
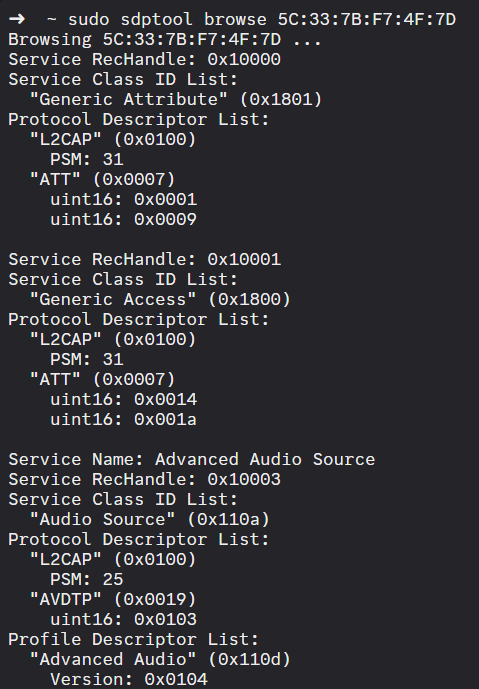
Obraz zawierający tekst, Czcionka, zrzut ekranu

Zawartość wygenerowana przez AI może być niepoprawna.

Wynik : l2ping wykonany dla słuchawek, telefonu i laptopa

sudo sdptool browse <adres MAC>

sdptool, jak nazwa wskazuje, służy do aktywowania protokołu SDP (Service Discovery Protocol) do analizowania dostępnych urządzeń Bluetooth i odpalonych na nich serwisach. Na każdym z urządzeń można zauważyć serwisy (znalezione lub nieznalezione – PnP, RecHandle) oraz powiązane z nimi protokoły (L2CAP, AVCTP, ATT).



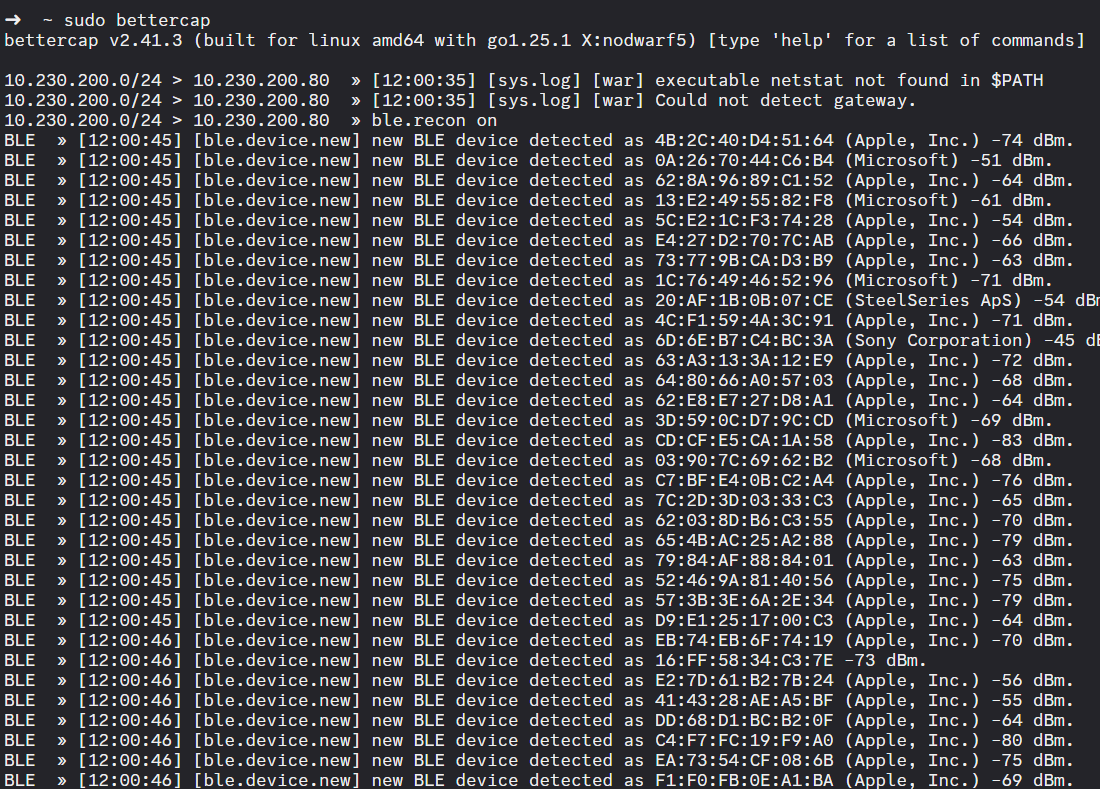
Obraz zawierający tekst, zrzut ekranu, Czcionka, menu

Zawartość wygenerowana przez AI może być niepoprawna.

Wynik : Analiza sdptool brose słuchawek, telefonu i laptopa

sudo bettercap

Pozwala on na analizę wielu typów ruchu bezprzewodowego, ale działa również dla Bluetooth. Po uruchomieniu szukane są urządzenia – jest ich więcej niż 3, które wcześniej analizowaliśmy



Wynik : bettercap uruchomiony w sali laboratoryjnej

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

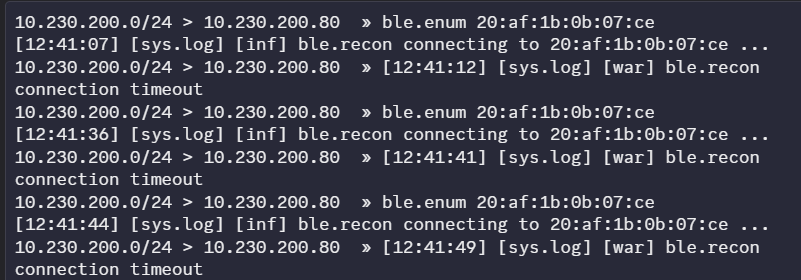
Po włączeniu skanowania ble.recon on i odczekaniu kilku minut, można zobaczyć wyniki skanu. Podstawowe informacje o urządzeniach są wyświetlone w wygodny sposób, posortowane według jakości sygnału wyrażonej w dBm



Wynik : Analiza ruchu sieciowego narzędziem ble

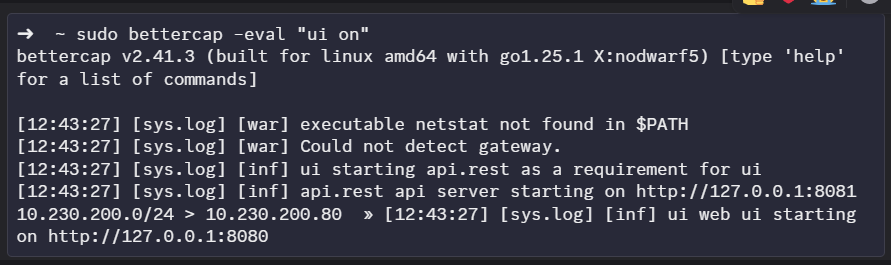
ble.enum <adres MAC>

Próbowano wykonać enumerację dla słuchawek SteelSeries, lecz z nie udało się naprawić problemu z timeout.



Wynik : Nieudana analaiza słuchawek przy pomocy narzędzia ble

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.

Wynik : Analiza przy pomocy bettercap z UI

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.

Obraz zawierający tekst, zrzut ekranu, Czcionka, Jaskrawoniebieski

Zawartość wygenerowana przez AI może być niepoprawna.

Obraz zawierający tekst, zrzut ekranu, komputer, oprogramowanie

Zawartość wygenerowana przez AI może być niepoprawna.

Laptop : Zmiana aliasu na laptopie i jego klasy



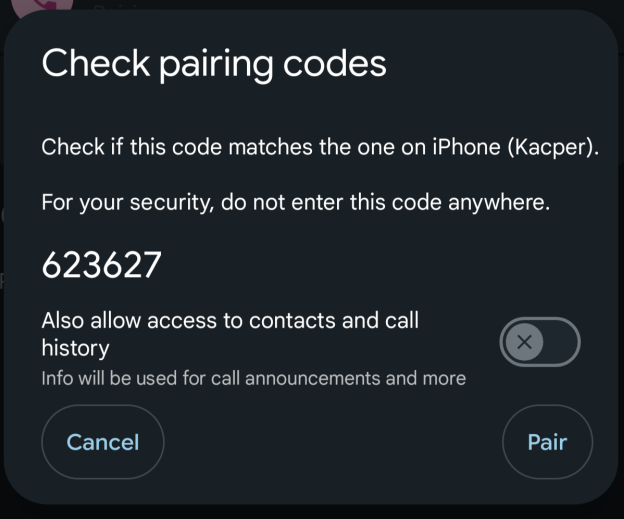
Telefon : Kali Linux podszywający się pod telefon

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.



Telefon : Połączenie z podstawionym urządzeniem

Obraz zawierający tekst, multimedia, zrzut ekranu, elektronika

Zawartość wygenerowana przez AI może być niepoprawna.

Laptop : Widok ze strony podstawionego urządzenia

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.

Obraz zawierający tekst, Czcionka, zrzut ekranu

Zawartość wygenerowana przez AI może być niepoprawna.

Error : Błąd btlejuice-proxy zgłaszany w trakcie zajęć

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.

Obraz zawierający tekst, zrzut ekranu, sztuka

Zawartość wygenerowana przez AI może być niepoprawna.

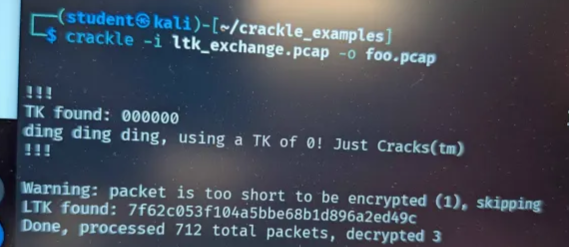
Error : Nienzalezione urządzenia spełniające warunek z zadania

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\_...

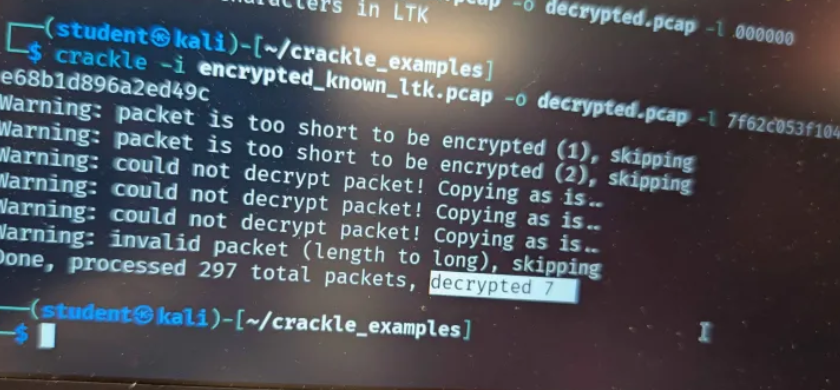


Wynik : odzysnanie klucza TK i LTK z transmisji sieciowej

TK found: 000000

LTK found: 7f62c…

crackle -i encrypted\_known\_ltk…



Wynik : Deszyfracja pakietów odnalezionym kluczem LTK

Decrypted: 7

Udało się odszyfrować ruch sieciowy zgodnie z instrukcją.

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.

Wynik : Udany brute force wykonany na przechwyconych danych

PIN: 654321

Link Key: d0:36:9b…

Wnioski, obserwacje i analiza

Narzędzia rekonensansowe, zarówno starsze, nowsze, mniej i bardziej interaktywne wszystkie działały dosyć podobnie i zwracały w większości te same informacje – głownie dlatego, że wszystkie korzystały z paczki BlueZ. Czasem jedynie można było napotkać dogodności, takie jak "tłumaczenie" nazw klas sprzętowych bądź graficzny interfejs. Z tego powodu zatem najlepiej jest używać po prostu narzędzia, które najlepiej pasuje do naszych potrzeb i jest dalej wspierane. Powinniśmy korzystać jednak z nowych rozwiązań – hcitool chociażby został zastąpiony przez bluetoothctl.

Pokazuje to jednak, że rekonesans Bluetooth jest prosty w wykonaniu i każdy z laptopem z systemem Linux może przeskanować swoje otoczenie w poszukiwaniu fizycznych adresów (BD\_ADDR) pobliskich urządzeń, jak i ich klas i nazw. Jest to wystarczające do próby ataku.

Jednym z takich ataków był spoofing, który również okazał się prosty w wykonaniu ze zgromadzonymi wcześniej informacjami. Pokazuje to, że podszycie się pod inne urządzenie jest realnym zagrożeniem, zatem parowanie Bluetooth powinno być wykonywane szybko i w uzgodniony sposób, żeby nikt nie zdążył się podszyć, a także należy zwrócić uwagę na wyświetlający się kod podczas parowania. Specyfikacja Bluetooth nie posiada lepszych sposobów obrony – nie zawiera ona wbudowanych mechanizmów walidacji ogłaszanych nazw, adresów i klas.

Ostatnie dwa zadania pokazują podatność parowania BLE na łamianie TK i LTK koniecznych do szyfrowania ruchu pomiędzy sparowanymi urządzeniami oraz klasyczny Brute Force. Problematyczną częścią pierwszego ataku jest przechwycenie całego procesu parowania, a problemem drugiego z nich jest przestrzeń kluczy. Ataki Brute Force są realnym problemem wszędzie, gdzie używany jest PIN – jest to mało skomplikowany sposób autentykacji. Starsze wersje Bluetooth używały połączenia PIN+MAC, żeby stworzyć Link Key, a jednocześnie nie był ustawiany limit nieudanych parowań. Z tego powodu należy przynajmniej nie ustawiać PINu typu 0000 bądź 1234.

**Podsumowując**, powszechnie stosowany i przez wszystkich lubiany protokół Bluetooth jest bardzo podatny na podszycie i inne ataki. Większość ataków jest jednak zależna od fizycznej odległości atakującego od ofiary. Oznacza to, że możemy zwiększyć swoje bezpieczeństwo, jeśli parujemy urządzenia w domu, a publicznie jesteśmy już do nich podłączeni.