API INFORMER UMCS 2020 - testy penetracyjne

Prawdopodobne zagrożenia:

Jedyne scenariusze pozwalające na wykorzystanie naszego oprogramowania zakładają przypadki w których:
- osoby nieuprawnione mogą wysyłać i odbierać dane z API
- potencjalny atakujący ma fizyczny dostęp do urządzenia na którym działa aplikacja (raspberry pi) - rozwiązanie: zamontowanie obudowy uniemożliwiającej dostęp do portów urządzenia.
- potencjalny atakujący odnajduje lukę bezpieczeństwa w oprogramowaniu urządzenia, poprzez skanowanie dostępnych/otwartych portów i identyfikację usług.

W celu minimalizacji potencjalnego zagrożenia zostaną przeprowadzone następujące testy:

1. Weryfikacja autoryzacji i uwierzytelniania podczas wysyłania zapytań do API
    - API powinno odpowiadać tylko i wyłącznie na zapytania pochodzące z urządzenia(raspberry pi). Próba wysłania zapytań do end-pointa z innego urządzenia niż raspberry pi w celu sprawdzenia czy API weryfikuje użytkowników.
    - Sprawdzenie czy uwierzytelnienie urządzenia zachodzi tylko i wyłącznie za pomocą adresu mac/ip. Jeżeli tak potencjalnym zagrożeniem jest spoofing. W tym scenariuszu atakujący wysyła pakiety mające na celu rozłączenie nas od sieci WiFi gdy już jesteśmy rozłączeni loguje się do sieci WiFi korzystając z adresu MAC, który był przypisany do naszego urządzenia raspberry pi. Prawdopodobne jest, że będzie mu przypisany ten sam adres ip co pozwoli mu na wysyłanie zapytań do API o ile inne zabezpieczenia nie zostaną wprowadzone.

2. W celu sprawdzenia urządzenia pod kątem dostępnych zagrożeń, porty urządzenia powinny zostać przeskanowanie przykładowo za pomocą narzędzia nmap, następnie powinna zostać przeprowadzona próba identyfikacji usług na portach poprzez komunikację z tymi usługami. Wszelkie zidentyfikowane usługi powinny zostać sprawdzone w bazach danych exploitów, znanych podatności. Przykładowa baza danych expoloitów: expoit-db.com