փաստաթղթավորում

### Նախագծին ուղեկցող փաստաթղթավորման օրինակ

### Նախագծի ամբողջական անվանումը

**ArmathRF**

### 

### Նախագծի համառոտ նկարագիրը

**ArmathRF-ը սարք է, որով հնարավոր է ստուգել, արդյոք այլ սարքերը (Wi-Fi, BLE) պաշտպանված են։**  
Սարքը փորձարկում է հարձակում իրականացնել սարքերի վրա, և եթե սարքը չի կարողանում պաշտպանվել հարձակումից, ապա այն համարվում է խոցելի։

Սարքը փորձում է անջատել wifi ցանցը, և եթե ցանցը չի անջատվում ապա պաշտպանված է։

### Տեխնիկական նկարագրություն

**Սարքավորում և բաղադրիչներ**

* Հիմնական վերահսկող սարք՝ Raspberry Pi Zero W
* Մոդուլներ՝
  + OLED display (SSD1306 128x32)
  + Կոճակներ (3 հատ)
  + Wi-Fi adapter

**Ծրագրային ապահովում**

* Python
* C++

### 

### Նախագծի հեղինակներ

* Նարեկ Գևորգյան
* Մարիա Վարդանյան

### Նպատակ և խնդիրներ

Նկարագրիր՝ ինչու է ստեղծվում սարքը․ օրինակ՝

* Wi-Fi և BLE սարքերի անվտանգության ստուգում
* Կիբերանվտանգության կրթական նպատակներ
* Սովորողների/մասնակիցների պրակտիկ փորձի զարգացում

### Աշխատանքի ընթացք (Workflow)

Քայլ առ քայլ նկարագիր, թե ինչպես է օգտագործվում սարքը․

1. Սարքը միացնել սնուցման աղբյուրին
2. OLED էկրանին երևում է գլխավոր մենյուն
3. Օգտատերը կոճակներով ընտրում է ցանկալի գործառույթը
4. Սարքը կատարում է սկանավորում կամ հարձակում
5. Արդյունքը ցուցադրվում է էկրանին

### Հաջորդ քայլեր (Future work)

* Սարքի վերջնական դիզայն (տուփ, սնուցման համակարգ)
* Նոր ֆունկցիոնալության ավելացում (օրինակ՝ Bluetooth spoofing, MITM attacks)
* Ավելի լավ UI էկրանին

### Գործառույթներ (Functionalities)

Թվարկիր կոնկրետ հնարավորությունները․

* Wi-Fi ցանցերի սկանավորում
* BLE սարքերի հայտնաբերում
* Կեղծ մուտքի կետ (Fake AP) ստեղծում
* Deauthentication հարձակում (DoS)
* Պաշտպանված/անպաշտպան սարքերի ցուցադրում էկրանին

### Տեսողական նյութեր

* Նախագծի աշխատանքային փուլերի լուսանկարներ (3–5 հատ)

### Հետադարձ կապ և կոնտակտային տվյալներ

* Անուն՝ Նարեկ | Հեռ.՝ +374 55 44 41 39
* Անուն՝ Մարիա | Հեռ.՝ +374 89 00 09 78