1. **Introducere**

Într-o societate tot mai dependentă de mobilitate și conectivitate wireless, rețelele Wi-Fi au devenit esențiale în aproape toate aspectele vieții moderne. Totuși, multe dintre aceste rețele rămân vulnerabile în fața unor atacuri simple, dar eficiente, din cauza unor deficiențe în standardele de securitate sau a lipsei de configurare adecvată. Utilizatorii obișnuiți, de cele mai multe ori, nu conștientizează pericolele la care se expun atunci când se conectează la o rețea publică, deschisă sau necunoscută.

În ultimii ani, atacurile cibernetice ce vizează rețelele Wi-Fi au cunoscut o creștere semnificativă, atât ca număr, cât și ca diversitate. De la simple atacuri de tip deauthentication – care forțează dispozitivele să se deconecteze de la rețea – până la atacuri mai sofisticate, cum ar fi Evil Twin (crearea unui punct de acces fals care imită unul legitim) sau DNS spoofing, vulnerabilitățile exploatate țintesc în special rețelele personale și cele publice neprotejate. Un exemplu celebru este atacul KRACK (Key Reinstallation Attack), care a expus slăbiciuni critice în protocolul WPA2 și a afectat milioane de dispozitive. Astfel de atacuri demonstrează cât de fragilă poate fi o infrastructură Wi-Fi aparent sigură și cât de ușor poate fi exploatată în lipsa unei securizări adecvate.

Proiectul prezent demonstrează, printr-o abordare practică și educațională, vulnerabilități comune ale rețelelor Wi-Fi utilizând un microcontroller ESP32. Acesta funcționează ca un punct de acces local, oferind printr-un server web o interfață de control pentru diverse acțiuni demonstrative. Utilizatorul se conectează la rețeaua creată de ESP32, iar prin intermediul paginii web poate interacționa cu funcționalitățile aplicației. Aceasta permite scanarea rețelelor din proximitate, deconectarea clienților conectați la un anumit punct de acces, redirecționarea cererilor DNS către o pagină de tip phishing și generarea masivă de rețele false.

Interacțiunea este intuitivă: imediat după conectare, utilizatorul accesează interfața web și selectează modul de testare dorit. Toate operațiile sunt executate local, fără conexiune la internet, ceea ce permite o demonstrație complet controlată și sigură. Scopul principal este evidențierea riscurilor reale la care se expun utilizatorii în lipsa unei infrastructuri wireless securizate, oferind totodată un cadru pentru învățare, testare și conștientizare în domeniul securității rețelelor fără fir.

1. **Documentarea problemei**

Rețelele wireless au cunoscut o evoluție accelerată în ultimele două decenii, devenind un pilon esențial al infrastructurii digitale moderne. Primele standarde Wi-Fi, precum IEEE 802.11b, lansat în 1999, ofereau viteze modeste și metode de criptare precum WEP (Wired Equivalent Privacy), care s-au dovedit rapid ineficiente. În timp, acestea au fost înlocuite cu standardele WPA și ulterior WPA2, care au adus îmbunătățiri semnificative, dar nu au fost lipsite de probleme. În anul 2017, atacul KRACK (Key Reinstallation Attack), detaliat de cercetătorii Vanhoef și Piessens, a demonstrat existența unei vulnerabilități critice în WPA2, afectând milioane de dispozitive la nivel global. (vezi [1], [2], [8])

În prezent, standardul WPA3 oferă un nivel superior de securitate, dar adoptarea lui este lentă. Multe dispozitive continuă să utilizeze protocoale mai vechi sau configurări nesigure, ceea ce lasă rețelele expuse. În paralel, utilizatorii se conectează frecvent la rețele publice sau deschise, fără a înțelege riscurile de securitate asociate – precum interceptarea traficului, capturarea de date sensibile sau redirecționarea către site-uri malițioase.Conform Wi-Fi Alliance, WPA3 este disponibil din 2018, dar multe dispozitive nu oferă suport complet pentru acesta [8].

### **2.1 Unelte software și hardware pentru testarea securității Wi-Fi**

Pentru analiza și testarea vulnerabilităților rețelelor wireless, comunitatea de securitate a dezvoltat numeroase unelte open-source și comerciale. Mai jos sunt prezentate cele mai relevante, împreună cu avantajele și limitările acestora.

#### **Aircrack-ng**

Aircrack-ng este o suită de unelte pentru auditarea rețelelor wireless. Permite capturarea de pachete, efectuarea de atacuri de tip deauthentication și spargerea cheilor WEP/WPA prin metode de brute-force sau dictionary attack.[3]

Avantaje:

Suport extins pentru diverse tipuri de plăci de rețea.

Poate recupera parole Wi-Fi reale în mod controlat.

Este integrat în distribuții specializate precum Kali Linux.

Dezavantaje:

Necesită cunoștințe avansate de rețelistică și Linux.

Nu are interfață grafică, lucrând exclusiv în linie de comandă.

Nu este portabil pe platforme embedded precum ESP32.

**Wireshark**

Wireshark este cel mai utilizat analizator de trafic de rețea, permițând inspecția detaliată a pachetelor capturate, inclusiv cele Wi-Fi (802.11). [4]

Avantaje:

Analiză protocolară foarte detaliată.

Interfață grafică intuitivă.

Utilizare profesională în audituri și depanări de rețea.

Dezavantaje:

Nu include funcții de atac, doar analiză pasivă.

Nu este adaptat pentru rularea pe dispozitive embedded.

Poate fi dificil de utilizat pentru începători.

**Wifite**

Wifite este o unealtă automatizată care combină mai multe instrumente (Aircrack-ng, Reaver, Bully) și permite lansarea rapidă de atacuri asupra rețelelor Wi-Fi din apropiere.[7]

Avantaje:

Automatizează întregul proces de testare.

Ideal pentru demonstrații și testări rapide.

Suportă multiple metode de atac asupra WPA și WEP.

Dezavantaje:

Este limitat ca opțiuni avansate de configurare.

Necesită drivere speciale și compatibilitate hardware.

Nu suportă protocoale moderne precum WPA3.

**ESP8266 Deauther**

ESP8266 Deauther este un proiect open-source dezvoltat pentru microcontrollerul ESP8266, care permite lansarea de atacuri Wi-Fi (deauthentication, beacon flood, probe request flood) printr-o interfață web ușor de folosit.[6]

Avantaje:

Extrem de portabil și ieftin (ESP8266 costă 3-5 euro).

Ușor de folosit pentru demonstrații didactice.

Interfață web integrată și prietenoasă.

Dezavantaje:

Limitat la câteva tipuri de atacuri simple.

Nu permite captură de trafic sau analiză complexă.

Nu suportă funcționalități precum DNS hijacking.

ESP8266 are resurse hardware limitate față de ESP32.

**Alte soluții**

Există și soluții comerciale precum Hak5 WiFi Pineapple, care oferă o gamă extinsă de funcționalități într-un pachet profesionist. Acestea sunt însă costisitoare, greu de personalizat și nu sunt potrivite pentru utilizare academică sau educațională open-source. [5]

**2.2 Poziționarea proiectului actual**

Proiectul dezvoltat în cadrul acestei lucrări își propune să depășească limitările proiectelor existente, oferind o soluție portabilă, ușor de utilizat și versatilă pentru testarea și înțelegerea vulnerabilităților rețelelor wireless. Platforma hardware aleasă, ESP32, oferă resurse superioare față de ESP8266 și suport pentru mai multe interfețe de rețea și operațiuni concurente.

Prin intermediul unui server web integrat, utilizatorul poate:

* vizualiza rețelele Wi-Fi din proximitate;
* selecta o rețea și executa un atac de tip deauthentication;
* activa redirecționarea DNS către o pagină de phishing (ex: Facebook);
* genera automat rețele Wi-Fi false (AP flood) pentru simularea unui atac de confuzie.

Spre deosebire de alte soluții, aplicația rulează complet local, fără acces la internet, ceea ce permite testarea într-un mediu izolat și controlat. Prin această abordare, proiectul combină elemente de rețelistică, securitate cibernetică și dezvoltare embedded într-un instrument educațional complet, eficient și accesibil.

1. **Abordare teoretica**
   1. **Cazuri**

Aplicațiile pentru testarea și efectuarea atacurilor asupra rețelelor Wi-Fi joacă un rol esențial în identificarea și înțelegerea vulnerabilităților rețelelor wireless, oferind numeroase oportunități practice și educaționale în diverse domenii. Mai jos sunt prezentate câteva exemple relevante de utilizare a unor astfel de aplicații:

**Auditarea securității rețelelor wireless** – Aplicațiile care efectuează atacuri Wi-Fi pot fi utilizate pentru auditarea securității unei rețele și identificarea punctelor slabe. Administratorii de rețea pot astfel simula atacuri reale, cum ar fi cele de tip deauthentication sau DNS spoofing, pentru a verifica dacă infrastructura de rețea este configurată corect și securizată corespunzător. De exemplu, o companie poate folosi astfel de instrumente pentru a testa periodic rețelele interne și pentru a remedia rapid eventualele vulnerabilități identificate.

**Educație și conștientizare** – Aceste aplicații sunt extrem de utile în mediile educaționale și academice pentru a demonstra vulnerabilitățile reale ale rețelelor wireless. Profesorii și formatorii pot realiza demonstrații practice care arată cât de ușor pot fi exploatate anumite vulnerabilități, subliniind necesitatea unor măsuri de securitate mai bune. De exemplu, studenții pot învăța cum funcționează atacurile Wi-Fi, observând efectul unui atac DNS hijacking sau al unui atac de tip Evil Twin într-un laborator controlat.

**Cercetare și dezvoltare în securitate informatică** – Cercetătorii din domeniul securității cibernetice utilizează aceste instrumente pentru a realiza experimente și pentru a descoperi noi vulnerabilități sau metode de apărare. De exemplu, cercetătorii pot analiza și documenta comportamentul unor dispozitive sau rețele Wi-Fi atunci când sunt expuse la atacuri simulate, contribuind astfel la dezvoltarea unor standarde și protocoale mai sigure.

**Testarea dispozitivelor noi** – Dezvoltatorii și producătorii pot utiliza astfel de aplicații pentru a testa securitatea dispozitivelor noi înainte ca acestea să ajungă pe piață. De exemplu, înainte de lansarea unui nou router Wi-Fi sau a unui dispozitiv IoT, producătorul poate testa dispozitivul folosind aceste instrumente pentru a se asigura că acesta rezistă atacurilor comune precum AP flood sau deauthentication.

* 1. **Cazuri de Utilizare**

**Actori implicați:**  
 Utilizator – Persoană care interacționează intenționat cu ESP32.  
 Victimă (Utilizator neavizat) – Persoană care se conectează la ESP32 crezând că este o rețea legitimă.  
 ESP32 – dispozitivul ce oferă funcționalitățile descrise.

### **Cazuri de utilizare și fluxuri detaliate:**

### **Utilizator neconectat la ESP32**

Actor: Utilizator  
*Descriere*: Utilizatorul nu este conectat la ESP32.  
Flux:  
 Utilizatorul caută rețele Wi-Fi.  
 Identifică rețeaua Wi-Fi generată de ESP32.  
 Se conectează la rețea.  
Rezultat: Utilizatorul este conectat la ESP32.

### **Utilizator conectat la ESP32 fără a accesa pagina web**

Actor: Utilizator  
Precondiție: Utilizator conectat deja la rețeaua ESP32.  
Descriere: Utilizatorul nu a accesat pagina web a ESP32.  
Flux:  
 Utilizatorul deschide un browser web.  
 Introduce manual adresa IP a ESP32 (ex: 192.168.4.1).  
Rezultat: Utilizatorul accesează pagina web servită de ESP32.

### **Utilizator accesează pagina web ESP32**

Actor: Utilizator  
Precondiție: Utilizator conectat și pagina web ESP32 accesată.  
Descriere: Utilizatorul accesează funcționalitățile oferite de pagina web.  
Flux principal:  
 Utilizatorul are opțiuni clare prezentate în interfață:  
 Poate să activeze atacul AP Flood.  
 Poate să scaneze AP-urile din apropiere.

### **Activarea și oprirea atacului AP Flood**

### Actor: Utilizator Precondiție: Utilizator în pagina web ESP32. Descriere: Utilizatorul pornește sau oprește atacul AP Flood. Flux: Utilizatorul selectează „Start AP Flood”. ESP32 începe să genereze rețele false în mod continuu. Utilizatorul poate apăsa ulterior „Stop AP Flood”. ESP32 oprește generarea rețelelor false.

Rezultat: Atacul AP Flood este controlat complet de utilizator.

### **Scanarea AP-urilor și atacul de tip Deauthentication**

Actor: Utilizator  
Precondiție: Utilizator conectat și a accesat pagina ESP32.  
Descriere: Utilizatorul scanează AP-urile și lansează atacuri de tip Deauth.  
Flux:  
 Utilizatorul selectează opțiunea „Scan AP-uri”.  
 ESP32 afișează o listă cu AP-urile găsite în apropiere.  
 Utilizatorul selectează un AP țintă din listă.  
 Introduce durata dorită pentru atac.  
 Activează atacul.  
 ESP32 lansează atacul de tip Deauth împotriva AP-ului țintă pentru perioada selectată.

Rezultat: Dispozitivele conectate la AP-ul țintă sunt deautentificate temporar.

### **Victimă conectată la ESP32 și redirecționată prin DNS Hijacking**

Actor: Victimă (Utilizator neavizat)  
Descriere: O victimă se conectează la ESP32 crezând că este o rețea legitimă și accesează un site.  
Flux:  
 Victima caută și identifică rețeaua Wi-Fi falsă creată de ESP32.  
 Victima se conectează la această rețea fără să suspecteze ceva.  
 Victima deschide browserul și încearcă să acceseze un site popular (de exemplu: facebook.com).  
 Prin DNS hijacking, ESP32 redirecționează traficul victimă către o pagină falsă (imitând pagina de autentificare Facebook).  
 Victima introduce datele de autentificare.  
 ESP32 captează și salvează credențialele introduse de victimă.  
Rezultat: Credințele victimei sunt interceptate și salvate local pe ESP32.

1. **Bibligrafie**
2. M. Vanhoef and F. Piessens, “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2,” Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017. [Online]. Available: https://doi.org/10.1145/3133956.3134027
3. IEEE Standards Association, “IEEE Std 802.11™-2016,” IEEE, 2016. [Online]. Available: [https://standards.ieee.org/ieee/802.11/1733/](https://standards.ieee.org/ieee/802.11/1733/" \t "/tmp/wps-robert/x/_new)
4. Aircrack-ng Project. “Aircrack-ng suite,” 2023. [Online]. Available: [https://www.aircrack-ng.org/](https://www.aircrack-ng.org/" \t "/tmp/wps-robert/x/_new)
5. Wireshark Foundation. “Wireshark - Go Deep,” 2023. [Online]. Available: [https://www.wireshark.org/](https://www.wireshark.org/" \t "/tmp/wps-robert/x/_new)
6. D. Ryan. “WiFi Pineapple - Wireless auditing,” Hak5, 2023. [Online]. Available: [https://www.hak5.org/](https://www.hak5.org/" \t "/tmp/wps-robert/x/_new)
7. Spacehuhn Technologies. “ESP8266 Deauther,” GitHub repository, 2023. [Online]. Available: [https://github.com/SpacehuhnTech/esp8266\_deauther](https://github.com/SpacehuhnTech/esp8266_deauther" \t "/tmp/wps-robert/x/_new)
8. Reaver Project. “Wifite 2,” GitHub repository, 2023. [Online]. Available: [https://github.com/derv82/wifite2](https://github.com/derv82/wifite2" \t "/tmp/wps-robert/x/_new)
9. IEEE, “WPA3 specification,” Wi-Fi Alliance, 2018. [Online]. Available: https://www.wi-fi.org/discover-wi-fi/security

·