**! textele intre parantezele unghiulare sunt note pentru sine sau ce urmeaza sa mai adaug**

**<nu sunt in sigur de titlu, avand in vedere tema va fi o nuanta a Instrument de atacuri Wi-Fi>**

1. **Introducere**

In contextul unei societati tot mai dependente de mobilitate și conectivitate wireless, rețelele Wi-Fi au devenit nelipsite în viata noastra. Totuși, multe dintre aceste rețele rămân vulnerabile în fața unor atacuri simple, dar eficiente, din cauza unor brese de securitate în standardele de securitate sau a lipsei de configurare cu securitatea in minte.

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 care au ca tinta rețelele Wi-Fi au cunoscut o creștere semnificativă, atât ca număr, cât și ca diversitate. De la simple atacuri care obliga deviceul sa se deautentifice de la reteaua la care este conectat, până la atacuri mai sofisticate, cum ar fi Evil Twin (crearea unui punct de acces fals care imită unul legitim)[9] 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 lumii brese de securitate critice în protocolul WPA2 și a afectat milioane de dispozitive[1]. Aceste atacuri demonstrează cât de fragilă poate fi o infrastructură Wi-Fi aparent sigură și cât de ușor poate fi exploatată în lipsa unei securizări pe masura.

Lucrarea de fata demonstrează, printr-o abordare practică, vulnerabilități comune ale rețelelor Wi-Fi utilizând un microcontroller ESP32[10]. Acesta funcționează ca un punct de acces local, oferind o interfață de control pentru diverse acțiuni demonstrative, printr-un server web. Utilizatorul se conectează la rețeaua creată de microcontroller, 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 atac 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 wireless.

1. **Documentarea problemei**

Rețelele wireless au cunoscut o evoluție accelerată în ultimele două decenii, devenind un instrument 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 aveau si ele o multime 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 Aplicatii 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 larga 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 ofere 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 eficient și accesibil.

1. **Abordare teoretica**
   1. **Cazuri de utilizare**

Aplicațiile pentru testarea și efectuarea atacurilor asupra rețelelor Wi-Fi joacă un rol esențial în identificarea și înțelegerea vulnerabilităților rețelelor wireless. Acestea ofera numeroase oportunități practice și educaționale în diverse domenii, mai jos fiind 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 care deautentifica deviceurile de la retea 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 pot realiza demonstrații practice care arată cât de ușor pot fi exploatate anumite vulnerabilități, scotand in evidenta 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.  
 **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 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.

<introdu o diagrama completa de actori>

### **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.

<screenshot cu interfata grafica principala a aplicatiei web>

### **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.  
<screenshot in care este edidentiata comanda>

### **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.

<screenshot in care este edidentiata comanda>

### **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.

<screenshoturi in care este evidentiata comanda, pagina rezultata si afisarea datelor primite>

1. **Metode folosite**

**4.1 Atacul de Flood (Beacon Flood)**

**<pune referintele bibliografice salvate pentru subcapitole>**

#### **Cum funcționează AP-urile și cum trimit ele mesaje către dispozitive**

Un punct de acces Wi-Fi (AP) reprezintă o interfață wireless între dispozitive și rețeaua fixă, permițând dispozitivelor să comunice și să acceseze resurse externe prin intermediul undelor radio. Pentru a facilita conexiunea dispozitivelor, AP-ul transmite periodic mesaje specifice numite cadre de tip beacon. Aceste cadre au rolul principal de a anunța existența rețelei Wi-Fi, împreună cu informații esențiale, cum ar fi numele rețelei (SSID), parametrii de criptare, canalul folosit și alte setări ale rețelei. Cadrele beacon sunt trimise la intervale de aproximativ 100 de milisecunde, pe canalul radio ales pentru comunicare. Atunci când dispozitivele utilizatorilor caută activ o rețea wireless, ele ascultă aceste cadre beacon. Ulterior, dispozitivul decide dacă dorește să se conecteze la rețeaua respectivă, folosind informațiile obținute din beacon-uri. Astfel aceste mesaje sunt esențiale pentru gestiunea eficientă a conectivității și pentru menținerea interoperabilității între diferite dispozitive și a punctelor de acces. Transmiterea constantă și regulată a beacon-urilor permite dispozitivelor să identifice și să selecteze rapid rețeaua dorită fără a realiza operațiuni suplimentare de interogare și răspuns.

#### **Tipurile de pachete Wi-Fi cu accent pe beacon frame**

Protocolul Wi-Fi utilizează mai multe tipuri de pachete pentru gestionarea comunicării wireless, fiecare având roluri bine definite. Există trei categorii majore de pachete: pachete de management, pachete de control și pachete de date. Cadrele de management se ocupă de administrarea rețelei Wi-Fi și includ tipuri esențiale precum beacon-uri, probe request, probe response, autentificare și asociere. Pachetele de control asigură fluxul de comunicare și controlează transmisiile, în timp ce cele de date conțin efectiv informația utilă transmisă între dispozitive.  
 Cadrele beacon fac parte din categoria pachetelor de management și sunt de importanta maxima pentru funcționarea normală a rețelei wireless. Acestea sunt trimise periodic de către AP-uri pentru a-și anunța prezența și configurația. Un cadru beacon conține, în mod obligatoriu, informații despre SSID (numele rețelei), parametrii de suport (rate de transfer, canale folosite, metode de criptare) și alte date relevante pentru conexiune. Importanța acestui tip de cadru constă în faptul că permite dispozitivelor să detecteze rețelele disponibile rapid și să decidă dacă rețeaua corespunde cerințelor lor înainte să se conecteze efectiv.

<aici vor fi puse digrama unui pachet general, si cum difera cele 3 intre ele>

#### **Cum funcționează și de ce este eficient atacul de tip Beacon Flood**

Atacul de tip Beacon Flood exploatează modul în care dispozitivele caută și detectează rețele Wi-Fi folosind pachete beacon. În cadrul acestui atac, dispozitivul ESP32 generează și transmite o cantitate foarte mare de cadre beacon false într-un interval scurt de timp, fiecare având SSID-uri diferite. Dispozitivele din raza de acțiune a ESP32, în special telefoanele mobile și laptopurile care caută activ rețele wireless, vor primi și afișa aceste rețele false ca fiind valide. În unele cazuri, acest atac poate cauza suprasolicitarea interfeței grafice a dispozitivelor, care încearcă să afișeze și să gestioneze un număr extrem de mare de rețele.  
Eficiența atacului vine tocmai din faptul că dispozitivele sunt proiectate să detecteze și să listeze rapid orice rețea disponibilă, ceea ce face ca numărul mare de beacon-uri false să devină rapid problematic. Acest tip de atac nu necesită autentificare sau conectare la rețelele victimă, făcându-l foarte simplu și eficient. În plus, dificultatea de a distinge între rețele reale și false face ca acest atac să fie extrem de disruptiv, putând provoca confuzie și chiar incapacitatea dispozitivelor de a se conecta normal la rețelele legitime.

#### **Cum te poți apăra de atacul de tip Beacon Flood**

Protecția împotriva atacurilor de tip Beacon Flood poate fi realizată prin mai multe abordări, atât la nivel tehnologic cât și prin metode de conștientizare a utilizatorului. O metodă tehnică eficientă este configurarea dispozitivelor pentru a ignora sau limita numărul de rețele noi afișate într-un interval scurt de timp, evitând astfel saturarea interfeței. În plus sistemele de operare moderne pot fi dotate cu filtre care detectează și blochează automat rețelele false pe baza anumitor caracteristici (cum ar fi generarea rapidă de SSID-uri aleatorii și similare).  
Din punctul de vedere al infrastructurii, administratorii de rețea pot implementa mecanisme de monitorizare și alertare atunci când sunt detectate comportamente anormale sau un număr neobișnuit de mare de beacon-uri. De asemenea, utilizatorii pot fi educați să nu se conecteze automat la rețele necunoscute și să verifice întotdeauna legitimitatea rețelelor Wi-Fi înainte de conectare, ceea ce reduce eficiența acestui tip de atac. Folosirea unor instrumente de detectare a atacurilor și implementarea protocoalelor de criptare avansată, cum ar fi WPA3, contribuie suplimentar la creșterea rezistenței împotriva unor astfel de atacuri disruptive și ușor de realizat.

**4.2 DNS Hijacking**

**Ce este DNS <schimba subtitlul>**

DNS (Domain Name System) reprezintă un sistem fundamental utilizat pe internet, având ca rol principal transformarea numelor de domenii (precum [www.google.com](http://www.google.com" \t "/home/robert/Documents\\x/_new)) în adrese IP numerice corespunzătoare (precum 172.217.16.4). În esență, DNS acționează ca un director telefonic al internetului, permițând utilizatorilor să acceseze site-uri web folosind nume ușor de memorat în locul unor adrese numerice complicate. Atunci când un utilizator introduce un URL în browser, acesta este tradus într-o adresă IP corespunzătoare prin intermediul DNS.  
Structura sistemului DNS este ierarhică, fiind organizată în diverse niveluri și tipuri de servere, de la serverele rădăcină și cele de nivel superior (Top-Level Domain – TLD) până la servere DNS locale și cache-uri DNS. Acest proces de rezolvare a numelor implică interogări recursive și iterative între servere, asigurând astfel o gestionare eficientă a adreselor și o rezolvare rapidă și fiabilă a domeniilor. DNS reprezintă o componentă esențială în navigarea pe internet, oferind o interfață simplă și eficientă între utilizatori și resursele online, iar integritatea și securitatea acestuia sunt critice pentru funcționarea corectă și sigură a internetului global.

**Ce face un server DNS <schimba sau integreaza cu subcapitolul anterior>**

Un server DNS este un dispozitiv sau serviciu care gestionează interogările DNS și realizează conversia numelor de domenii în adrese IP. Atunci când un utilizator solicită accesul la o anumită pagină web, cererea inițială trece printr-un server DNS care identifică adresa IP corespunzătoare domeniului solicitat. În mod uzual, serverele DNS sunt configurate să păstreze o bază de date actualizată, în care fiecare nume de domeniu cunoscut este asociat cu o adresă IP specifică. Există mai multe tipuri de servere DNS implicate în rezolvarea unei interogări DNS. Serverul DNS local sau recursiv primește cererea inițială și încearcă să ofere un răspuns rapid folosind informații stocate în cache-ul local. Dacă nu are informația solicitată, serverul recursiv va trimite interogarea către alte servere DNS superioare. Serverele autoritare, care au autoritate asupra anumitor domenii specifice, furnizează răspunsuri definitive pentru domeniile administrate. Astfel, serverul DNS acționează ca un mediator eficient între utilizator și resursele solicitate pe internet, asigurând rezolvarea rapidă și precisă a adreselor și menținând buna funcționare a comunicației între dispozitive și servere.

<diagrama in care se prezinta flowul unui schimb de mesaje intre server si client>

**Ce se întâmplă când te conectezi la o rețea (serverul DNS prin DHCP)**

Când un dispozitiv se conectează la o rețea Wi-Fi sau prin cablu, acesta folosește protocolul DHCP (Dynamic Host Configuration Protocol) pentru a obține automat configurația necesară funcționării în rețea. Printre aceste informații se află și adresa IP a dispozitivului, adresa gateway-ului implicit și serverele DNS care vor fi utilizate pentru rezolvarea adreselor. DHCP simplifică procesul de conectare, permițând dispozitivului să se conecteze automat, fără configurări manuale din partea utilizatorului.  
 Odată conectat, dispozitivul client primește automat una sau mai multe adrese ale serverelor DNS configurate în rețeaua respectivă. De exemplu, într-o rețea casnică obișnuită, routerul va furniza prin DHCP propriul său IP drept server DNS principal, iar routerul va redirecționa mai departe aceste interogări către serverele DNS externe configurate. Configurarea automată prin DHCP asigură utilizatorului o experiență transparentă și fără probleme, însă introduce și un potențial punct slab: dacă dispozitivul DHCP furnizează în mod intenționat adrese DNS malițioase sau false, dispozitivele conectate vor deveni vulnerabile la atacuri de tip DNS Hijacking.

**Cum poate fi folosit ESP32 pentru DNS Hijacking și redirecționarea utilizatorului către o pagină falsă**

ESP32 poate implementa eficient atacul DNS Hijacking datorită capacității sale de a acționa simultan ca server DNS și punct de acces Wi-Fi. În acest scenariu, ESP32 furnizează prin protocolul DHCP propriul său IP ca server DNS pentru dispozitivele conectate. Astfel, toate cererile DNS ale utilizatorului trec prin ESP32. Când utilizatorul încearcă să acceseze un site cunoscut, cum ar fi Facebook.com, ESP32 interceptează cererea DNS și, în loc să returneze adresa IP reală a site-ului, returnează propriul său IP.  
 Această manipulare determină dispozitivul utilizatorului să direcționeze traficul web către ESP32, considerând că aceasta este adresa corectă a serverului solicitat. La portul 80, ESP32 servește o pagină web falsă, o copie exactă a site-ului original (în exemplul dat, o copie a paginii de autentificare Facebook). Utilizatorul, fără a bănui că a fost redirecționat, introduce datele personale sau credențialele de autentificare. Aceste date sunt apoi capturate și stocate de ESP32, demonstrând clar cât de simplu poate fi compromisă securitatea utilizatorului într-o rețea nesigură sau compromisă. Acest tip de atac subliniază importanța configurărilor DNS sigure și a utilizării unor rețele Wi-Fi cunoscute și securizate.

<digrama in care se prezinta modificarea adusa de atac>

**4.3 Atac de deautentificare**

Atacurile de tip deautentificare reprezintă o metodă eficientă prin care atacatorul întrerupe conexiunea unui dispozitiv la o rețea Wi-Fi. Aceste atacuri exploatează natura protocolului IEEE 802.11, care permite dispozitivelor și punctelor de acces să trimită cadre speciale pentru a încheia conexiuni.

<Adauga descrierea plus schema unui mesaj de deautentificare>

### **Deautentificarea prin trimiterea de pachete broadcast**

Unul dintre atacurile clasice implică trimiterea de cadre de deautentificare către toate dispozitivele conectate la un anumit AP, folosind adresa de tip broadcast. Aceste cadre sunt parte a protocolului Wi-Fi (cadre de management), având ca rol legitim să anunțe dispozitivele că au fost deconectate de AP. Când dispozitivele primesc aceste cadre, reacționează imediat prin încetarea conexiunii și încercarea unei reconectări. Astfel, trimiterea repetată a unor astfel de cadre ar trebui, teoretic, să cauzeze o întrerupere continuă și persistentă a conexiunilor dispozitivelor conectate.

Totuși, în practică, acest atac nu mai este la fel de eficient cum era în trecut. Dispozitivele moderne au devenit mai rezistente la astfel de atacuri, prin actualizări ale firmware-ului și îmbunătățiri software. Mulți producători implementează filtre speciale care identifică și ignoră cadrele broadcast de deautentificare, mai ales când acestea apar în mod repetat sau suspect. Din cauza acestei rezistențe crescute, metoda prin broadcast nu a fost inclusă în proiectul actual, deoarece și-a pierdut eficiența în mediile reale, fiind acum considerată o tehnică depășită și ușor de contracarat.

Conform documentației oficiale Aircrack-ng [1], deautentificarea de tip broadcast nu mai funcționează eficient deoarece majoritatea clienților wireless nu mai răspund la astfel de cadre, mai ales în lipsa unei autentificări reale sau a unui handshake WPA/2 activ. Mai mult decât atât, dacă ESP32 (sau orice alt dispozitiv) nu este asociat oficial cu rețeaua și nu este recunoscut ca AP legitim, multe dispozitive vor considera pachetele primite ca fiind neautentice și le vor ignora complet.  
 Din cauza acestei rezistențe crescute și a modificărilor aduse în comportamentul clientului, metoda prin broadcast nu a fost inclusă în proiectul actual, deoarece și-a pierdut eficiența în mediile reale, fiind acum considerată o tehnică depășită și ușor de contracarat.

### **Deautentificarea selectivă prin utilizarea SSID și BSSID**

Ca alternativă mult mai eficientă, proiectul actual implementează un atac sofisticat și specific, care folosește SSID-ul și BSSID-ul (adresa MAC a routerului) punctului de acces țintă pentru a realiza o deautentificare selectivă. În această abordare, dispozitivul ESP32 este configurat să utilizeze exact același SSID și BSSID ca routerul țintă. Astfel, atunci când un dispozitiv trimite cadre de date routerului real, aceste cadre sunt captate și de ESP32, deoarece acesta pretinde că este același AP legitim.  
În realitate, dispozitivul utilizatorului nu este autentificat la ESP32, ceea ce determină ESP32 să răspundă cu un cadru de deautentificare direct adresat dispozitivului respectiv. Deoarece cadrul de deautentificare este trimis direct dispozitivului țintă (și nu prin broadcast), acesta are șanse mult mai mari să fie acceptat și procesat. Dispozitivele moderne consideră aceste cadre legitime, fiind trimise direct de la punctul de acces cu care ele cred că sunt asociate. Acest tip de atac evită complet filtrele obișnuite de protecție, deoarece nu implică mesaje de broadcast și este specific unui singur dispozitiv vizat, ceea ce îl face foarte eficient în medii reale și practice.

**4.4 Prezentarea structurii codului <schimba mai tarziu>**

<explica fisierele header si ce fac functiile din el in linii mari>

<o sa fie structurat exact ca notiunile de mai sus, pe atacuri>

1. **Bibligrafie**

[1] 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. URL: <https://doi.org/10.1145/3133956.3134027>

[2] IEEE Standards Association, “IEEE Std 802.11™-2016,” IEEE, 2016. URL: <https://standards.ieee.org/ieee/802.11/1733/>

[3] Aircrack-ng Project. “Aircrack-ng suite,” 2023. URL: <https://www.aircrack-ng.org/>

[4] Wireshark Foundation. “Wireshark - Go Deep,” 2023. URL: <https://www.wireshark.org/>

[5] D. Ryan. “WiFi Pineapple - Wireless auditing,” Hak5, 2023. URL: <https://www.hak5.org/>

[6] Spacehuhn Technologies. “ESP8266 Deauther,” GitHub repository, 2023. URL: <https://github.com/SpacehuhnTech/esp8266_deauther>

[7] Reaver Project. “Wifite 2,” GitHub repository, 2023. URL: <https://github.com/derv82/wifite2>

[8] IEEE, “WPA3 specification,” Wi-Fi Alliance, 2018. URL: <https://www.wi-fi.org/discover-wi-fi/security>

[9] Grayson, M., McNab, J., & Turner, S. (2013). Wi-Fi Security: WPA and 802.11i. Cisco Press.

[10] Espressif Systems. (2023). ESP32 Technical Reference Manual. <https://docs.espressif.com/projects/esp-idf/en/latest/esp32/>