**! 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.

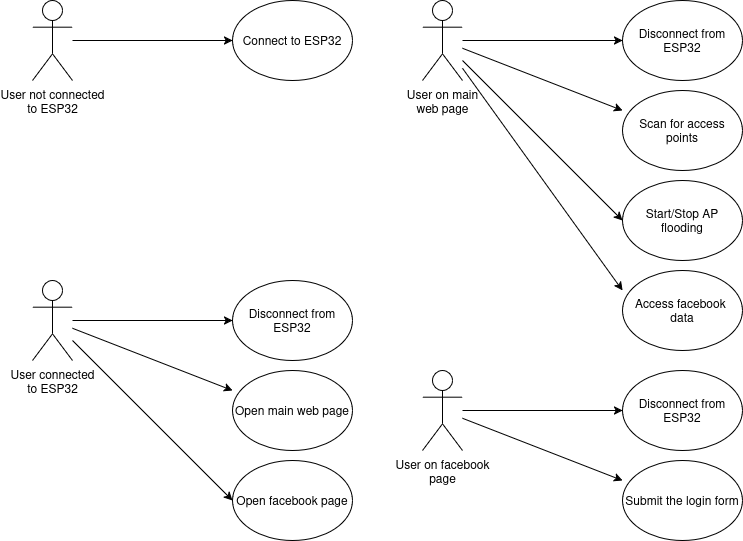
Spre deosebire de alte soluții, aplicația rulează complet local, fără acces la internet, ceea ce permite testarea într-un mediu izolat și controlat. Prin această abordare, proiectul combină elemente de rețelistică, securitate cibernetică și dezvoltare embedded într-un instrument educațional eficient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



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

### **Utilizator neconectat la ESP32**

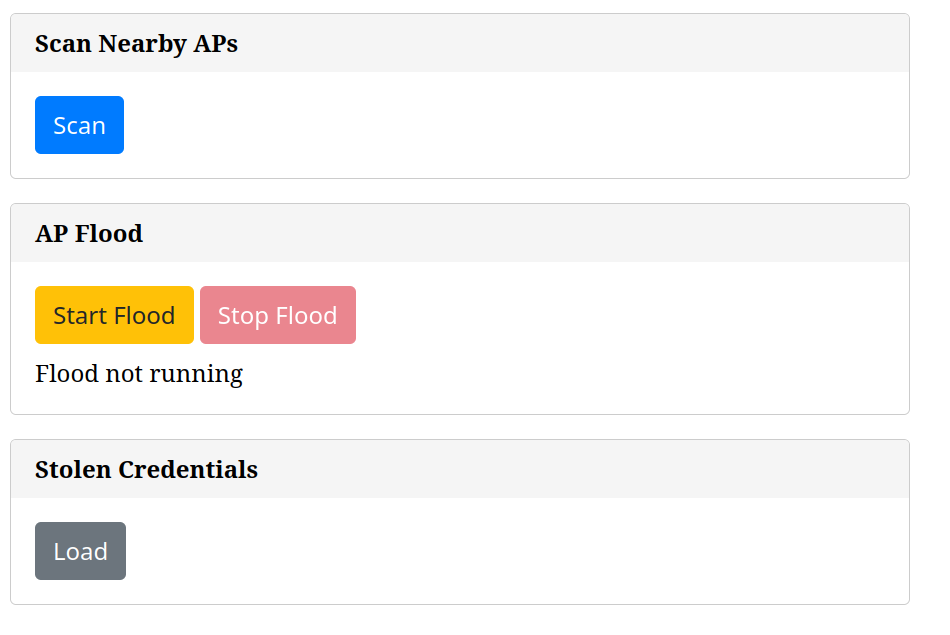
Actor: Utilizator  
*Descriere*: Utilizatorul nu este conectat la ESP32.  
Flux:  
 Utilizatorul caută rețele Wi-Fi.  
 Identifică rețeaua Wi-Fi generată de ESP32.  
 Se conectează la rețea.  
Rezultat: Utilizatorul este conectat la ESP32.

### **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**

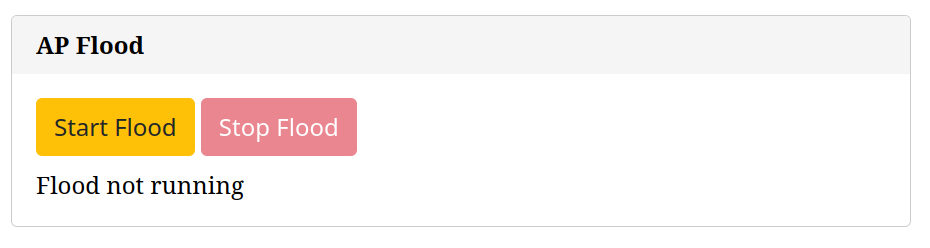
Actor: Utilizator  
Precondiție: Utilizator conectat și pagina web ESP32 accesată.  
Descriere: Utilizatorul accesează funcționalitățile oferite de pagina web.  
Flux principal:  
 Utilizatorul are opțiuni clare prezentate în interfață:  
 Poate să activeze atacul AP Flood.  
 Poate să scaneze AP-urile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

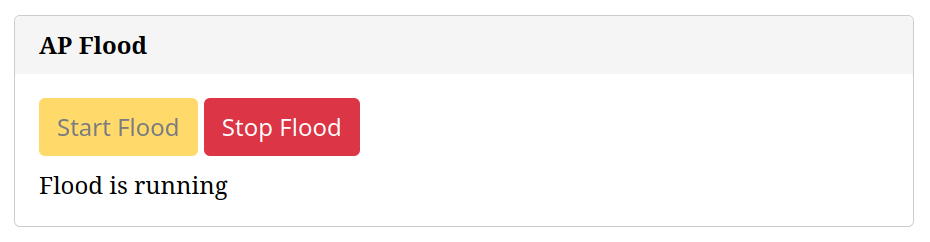


### **Activarea și oprirea atacului AP Flood**

### 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.

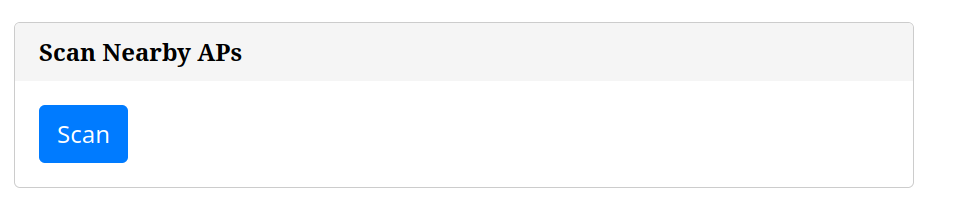


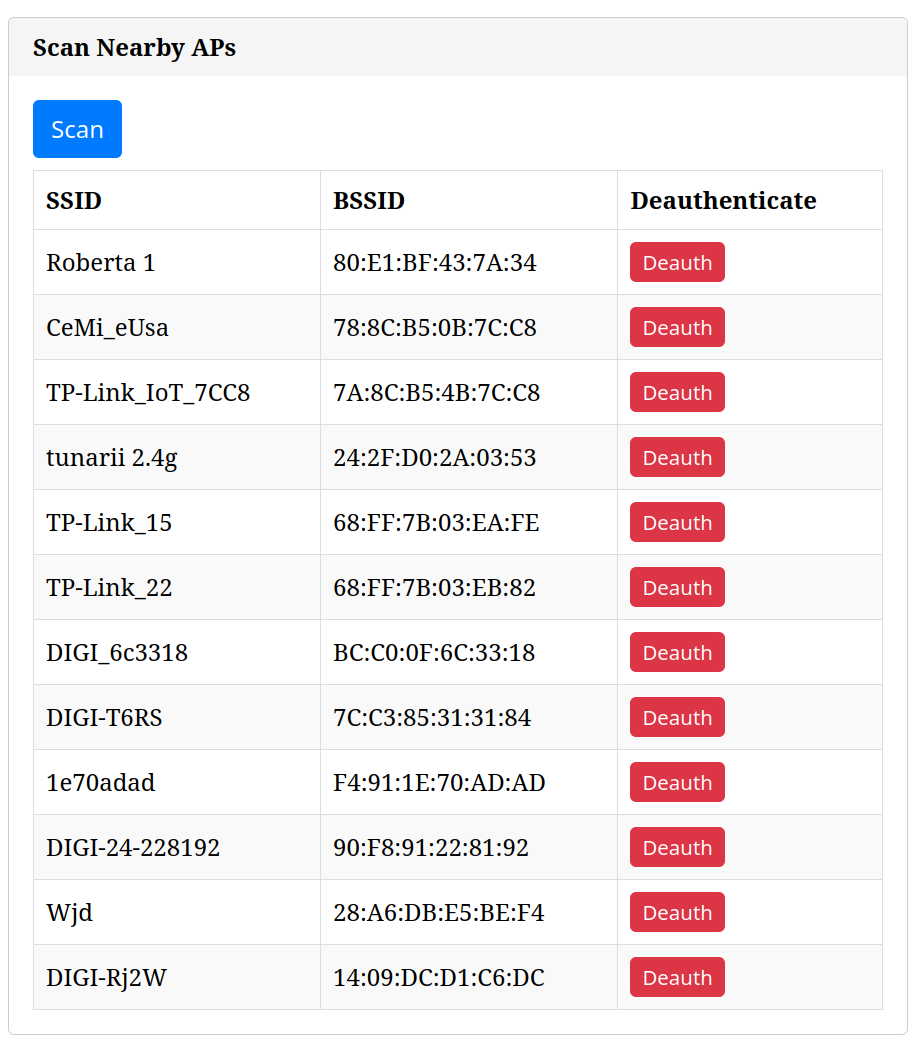
  
<screenshot cu rezultatul pe telefon/latop>

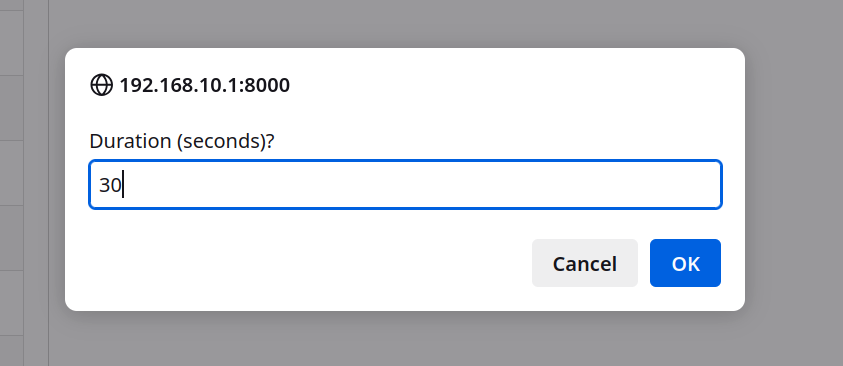
### **Scanarea AP-urilor și atacul de tip Deauthentication**

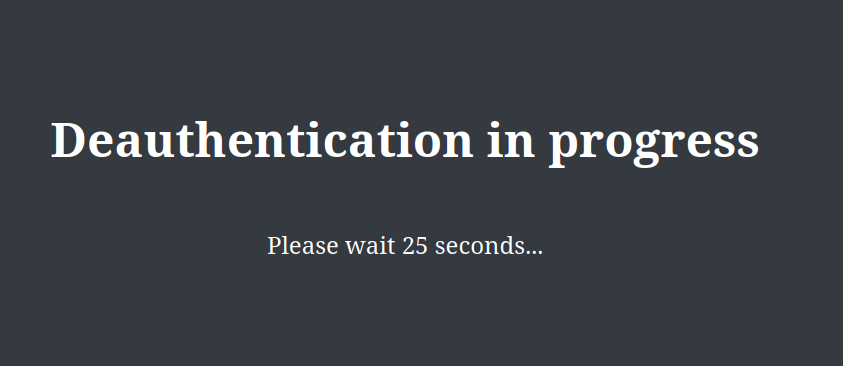
Actor: Utilizator  
Precondiție: Utilizator conectat și a accesat pagina ESP32.  
Descriere: Utilizatorul scanează AP-urile și lansează atacuri de tip Deauth.  
Flux:  
 Utilizatorul selectează opțiunea „Scan AP-uri”.  
 ESP32 afișează o listă cu AP-urile găsite în apropiere.  
 Utilizatorul selectează 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.  
 La final dupa tecerea perioadei de autentificare, utilizatorul este rugat sa se reconecteze la ESP32.

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







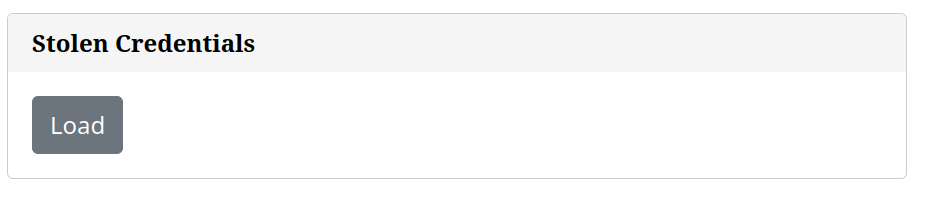


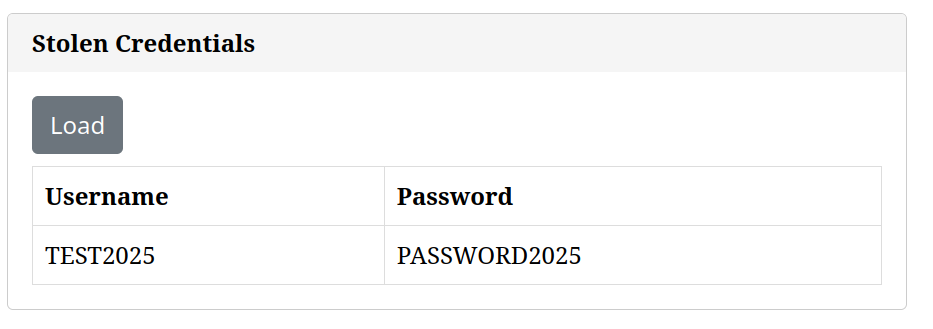


<screenshot in care este edidentiata comanda>

1. **Afisarea credentialelor**

Actor: Utilizator (intenționat, adică cel care controlează ESP32)  
Precondiție: ESP32 a capturat deja credențiale de la utilizatori neavizați prin pagina falsă de Facebook.  
Descriere: Utilizatorul accesează interfața web a ESP32 și apasă un buton care afișează într-un tabel toate perechile de username și parolă introduse de victime.  
Flux:  
 Utilizatorul accesează pagina principală a aplicației ESP32.  
 Navighează la secțiunea de vizualizare date capturate.  
 Apasă pe butonul „Afișează credențiale”.  
 ESP32 citește fișierul (sau zona de memorie) unde sunt salvate datele capturate.  
 Interfața web afișează un tabel cu toate username-urile și parolele interceptate.  
Rezultat: Utilizatorul poate vizualiza local datele capturate, fără conexiune la internet.

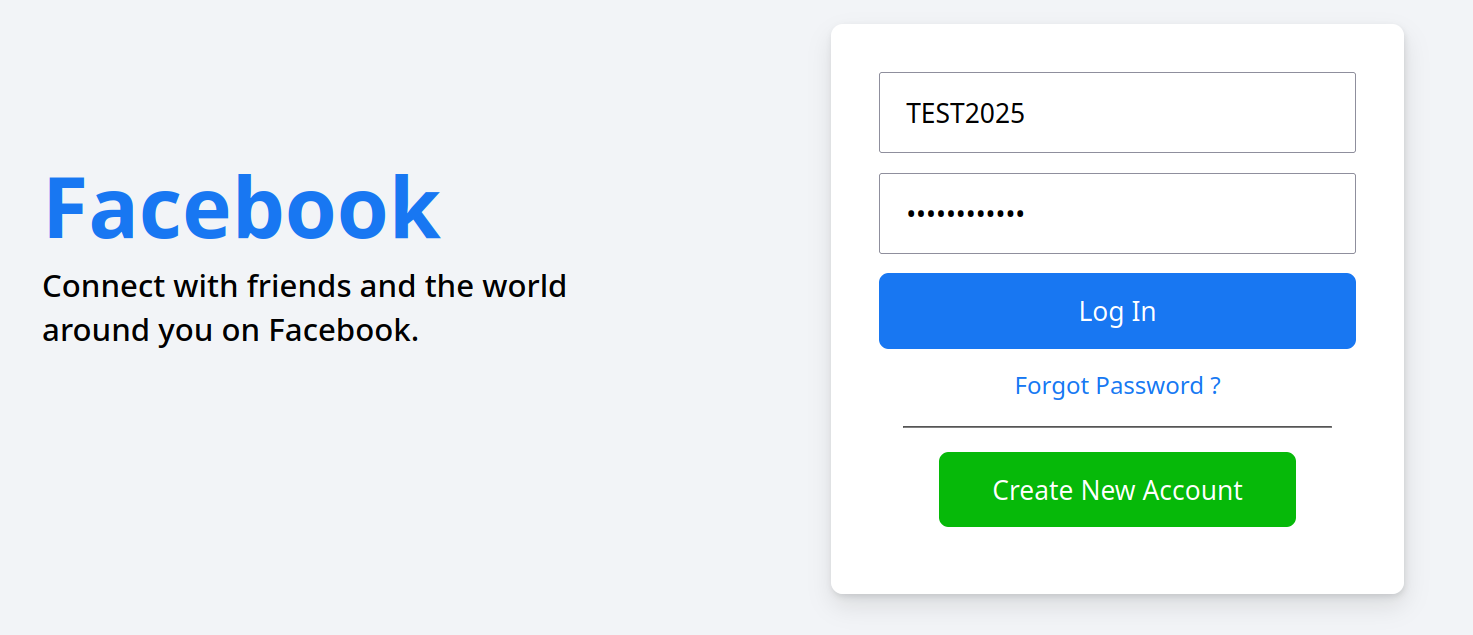




### **Victimă conectată la ESP32 și redirecționată prin DNS Hijacking**

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>



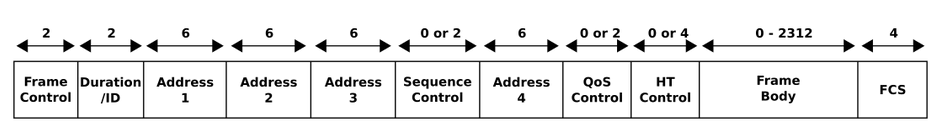
1. **Metode folosite**

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

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

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

Un punct de acces (Access Point – AP) este componenta care face legătura între rețeaua locală cablată și dispozitivele wireless, permițând comunicația acestora prin unde radio. AP-ul implementează standardul IEEE 802.11, care definește structura fizică și logică a comunicației Wi-Fi, incluzând formatele cadrelor, canalele radio, modurile de autentificare și negocierea criptării. Într-o rețea tipică, AP-ul poate fi un router, dar și un dispozitiv dedicat conectat la un controller de rețea. Comunicarea în rețelele Wi-Fi se face prin cadre (frames) care sunt transmise în eter la nivelul Layer 2 (legătură de date). Aceste cadre sunt împărțite în trei mari categorii: cadre de management, cadre de control și cadre de date. Cadrele de management controlează conexiunile: includ beacon-uri, autentificare, asociere, disasociere și deautentificare. Cadrele de control gestionează transmiterea datelor (ACK, RTS/CTS), iar cele de date conțin informația utilă pentru aplicații.  
 Toate cadrele urmează o structură generală cu antet, adrese MAC, control de durată, secvență, câmpuri opționale și eventual payload. AP-ul emite periodic cadre beacon, transmise broadcast pe canalul curent, prin care își anunță existența și oferă detalii despre rețea. Aceste beacon-uri conțin: SSID (numele rețelei), canalul folosit, metodele de criptare (ex. WPA2), viteze suportate, compatibilități (HT/VHT/HE), și sunt recepționate pasiv de toate dispozitivele aflate în zonă.  
Când un client dorește conectarea, trimite un probe request sau ascultă beacon-urile, apoi inițiază authentication și association. AP-ul răspunde cu cadre specifice pentru fiecare etapă. Doar după stabilirea asocierii și negocierii criptării poate începe schimbul de cadre de date.  
 Întreg procesul inițial (scanare, autentificare, asociere) are loc în clar, fără criptare, ceea ce îl face vulnerabil la analiză, falsificare sau interferență. De aceea, etapa de conectare este adesea vizată în testele de securitate și în atacurile Wi-Fi, deoarece permite emularea comportamentului unui AP fără parcurgerea autentificării reale. Prin înțelegerea acestor fluxuri de mesaje și rolul cadrelor implicate, pot fi dezvoltate atât aplicații funcționale (routere, sniffer-e), cât și instrumente de testare a securității wireless.



**2. Management frames**

În arhitectura rețelelor Wi-Fi, cadrele de management joacă un rol esențial în stabilirea, întreținerea și întreruperea conexiunilor între dispozitivele client și punctele de acces. Aceste cadre sunt definite în standardul IEEE 802.11 și sunt prezente în toate fazele de funcționare ale unei rețele wireless, cu excepția transmiterii efective a datelor. Ele conțin informații despre parametrii rețelei, inițiază procesele de autentificare și asociere, permit roaming-ul între AP-uri și gestionează deconectările controlate sau forțate.  
 Structura generală a unui cadru de management include: un câmp Frame Control (care identifică tipul și subtipul), durata transmisiunii, adresele MAC implicate (stație, AP, destinatar), câmpuri de control al secvenței și un payload variabil, compus din Information Elements. Spre deosebire de cadrele de date, cele de management sunt întotdeauna transmise necriptat, fiind interpretate direct de orice dispozitiv care ascultă canalul activ.

Printre cele mai importante tipuri se numără:  
 Beacon – transmis de AP pentru a semnaliza existența rețelei;  
 Probe request/response – utilizate pentru căutarea și anunțarea activă a rețelelor;  
 Authentication/Deauthentication – inițiază sau încheie procesul de autentificare;  
 Association/Disassociation – realizează și încheie conexiunea logică MAC.

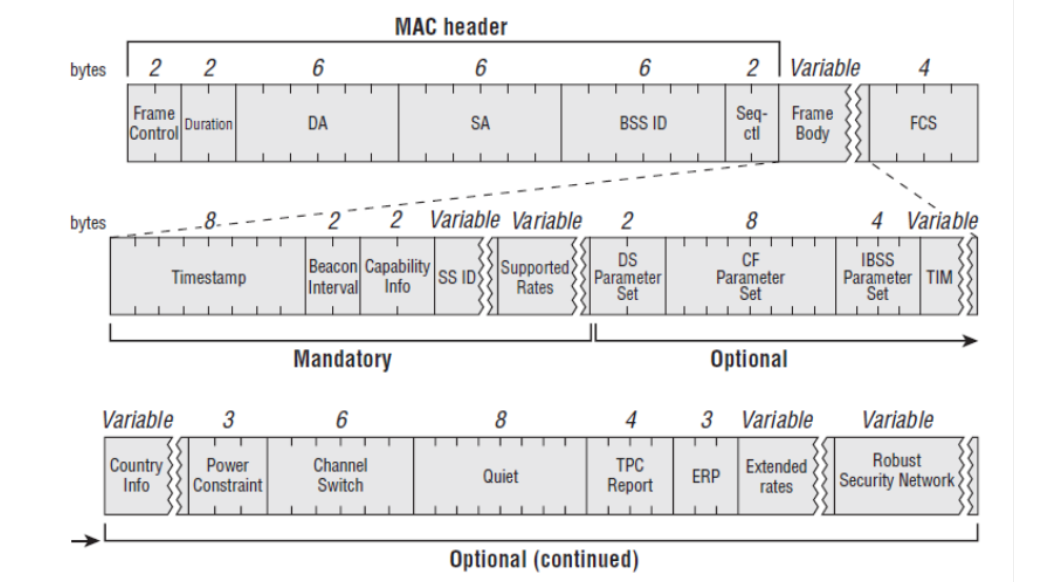
Un flux tipic implică: clientul trimite un probe request, AP-ul răspunde cu probe response; clientul trimite authentication request, AP-ul îl validează și trimite răspunsul; clientul trimite apoi association request, la care AP-ul răspunde pozitiv dacă acceptă conexiunea. Acești pași sunt obligatorii pentru ca o sesiune de date să poată începe.

Faptul că aceste cadre nu sunt protejate criptografic face posibilă interceptarea, falsificarea sau injectarea lor. Este suficient un atacator în raza rețelei cu un adaptor Wi-Fi capabil de „monitor mode” pentru a trimite cadre deauthentication false și a forța deconectarea dispozitivelor legitime. Din acest motiv, aceste cadre sunt vizate în numeroase atacuri wireless (ex: DoS, Evil Twin, Captive Portal). Deși există extensii moderne ale standardului (ex. 802.11w – Protected Management Frames), suportul nu este universal, ceea ce lasă multe rețele și dispozitive vulnerabile.

**3. Beacon frames**

Cadrele de tip beacon reprezintă coloana vertebrală a funcționării pasive a unei rețele wireless. Acestea sunt transmise periodic, fără cerere, de către orice punct de acces (AP), pentru a-și anunța prezența și a furniza informații descriptive despre rețea. Transmise la fiecare 100 de milisecunde (sau alt interval configurat), beacon-urile permit dispozitivelor client să afle automat că există o rețea în zonă și să obțină toate detaliile necesare conectării.  
 Structura unui beacon frame include: antetul cadrului (Frame Control, durată, adrese), un timestamp pentru sincronizarea dispozitivelor, intervalul beacon, BSSID-ul (MAC-ul AP-ului), și o colecție de Information Elements (IEs). Aceste IEs sunt blocuri TLV (type-length-value) care conțin:  
 SSID-ul rețelei (nume),  
 tipul și nivelul criptării (WEP/WPA2/WPA3),  
 vitezele suportate,  
 canalul radio activ,  
 extensii pentru roaming sau mesh,  
 capabilități de rețea (802.11n/ac/ax).

Beacon-urile sunt transmise broadcast pe canalul activ, ceea ce înseamnă că toate dispozitivele aflate în raza AP-ului pot recepționa aceste mesaje. Clienții le utilizează pentru a popula lista de rețele vizibile, pentru roaming automat între AP-uri, pentru sincronizarea ceasurilor interne și pentru alegerea celei mai bune rețele în funcție de semnal și suport.  
Deoarece beacon-urile sunt transmise în clar, fără criptare sau semnătură, acestea pot fi ușor imitate. Un atacator poate crea beacon-uri false cu SSID-uri identice sau aleatorii, păcălind dispozitivele să încerce conectarea la o rețea falsă sau saturând lista de rețele afișate. Această metodă este baza atacurilor de tip AP Flood și Evil Twin, în care se creează zeci sau sute de rețele false pentru a induce confuzie sau pentru a captura date de autentificare.



**4. AP Flood prin beacon-uri**

AP Flood-ul este o tehnică de perturbare a funcționării rețelelor wireless care folosește cadre beacon false pentru a simula existența mai multor rețele fictive într-o zonă. Acest atac este posibil din cauza comportamentului dispozitivelor client: în mod normal, acestea recepționează toate cadrele beacon primite pasiv și le interpretează ca rețele valide. Dacă un atacator generează sute sau mii de astfel de beacon-uri, fiecare cu un SSID diferit, dispozitivul va adăuga toate aceste rețele în listă, fără o modalitate de validare a autenticității.  
 Dispozitive precum ESP32 permit programarea în așa fel încât să trimită beacon-uri într-o buclă, fiecare având un BSSID (MAC) diferit și un SSID unic sau mimat după rețele reale. Aceste beacon-uri sunt transmise broadcast pe canalul dorit, afectând toate dispozitivele aflate în raza de acțiune. Un telefon sau laptop va afișa toate aceste rețele ca fiind disponibile, ceea ce încetinește lista de afișare, poate cauza blocaje în interfața grafică și face dificilă conectarea la rețele reale.  
Atacul este și mai eficient dacă sunt folosite SSID-uri frecvente sau memorate de dispozitivul victimă. În astfel de cazuri, clientul poate încerca automat conectarea (auto-connect), ceea ce duce la un consum suplimentar de resurse, eșecuri de conectare și întreruperi în rețelele reale. În unele cazuri, firmware-ul dispozitivului poate intra în bucle de scanare sau poate reseta interfața Wi-Fi.  
 Beacon-urile false pot fi transmise și pe mai multe canale, crescând raza de acțiune a atacului. Deoarece standardul 802.11 nu include semnături sau criptare pentru beacon-uri, dispozitivele client nu au un mecanism nativ pentru a respinge beacon-urile falsificate. Această lipsă de verificare le face vulnerabile chiar și în rețele moderne, în special dacă nu sunt folosite sisteme suplimentare de filtrare sau detecție a anomaliilor.

**5. Deauthentication frames**

Cadrele de tip Deauthentication sunt cadre de management definite în standardul IEEE 802.11 și au rolul de a încheia oficial procesul de autentificare dintre un client și un punct de acces (AP). Ele sunt parte din mecanismul de control al conexiunilor într-o rețea Wi-Fi și pot fi transmise de ambele părți: atât de client, cât și de AP. Când un astfel de cadru este recepționat, conexiunea este considerată încheiată și orice comunicare ulterioară necesită reluarea autentificării și asocierii.

Structura unui cadru de deauthentication este simplă. El include:  
 Antetul de control (Frame Control) care specifică tipul „Management” și subtipul „Deauthentication”,  
 Trei adrese MAC: sursa (expeditorul), destinația (receptorul) și BSSID (rețeaua),  
 Câmpul de „Reason Code”, care explică motivul deautentificării (ex: cod 3 – „deautentificat de AP”).

Deauthentication-ul este distinct de disassociation: primul încheie autentificarea, în timp ce al doilea încheie asocierea. Cele două pot apărea împreună, dar standardul le separă logic și funcțional. Spre exemplu, dacă un client se mișcă într-o zonă fără semnal, AP-ul poate trimite un cadru de deauthentication pentru a încheia corect sesiunea, prevenind posibile conflicte de stare.  
 Toate cadrele de tip deauthentication sunt transmise în clar, fără criptare sau protecție criptografică în standardul original. Din acest motiv, ele sunt extrem de vulnerabile la falsificare. Un atacator aflat în apropierea rețelei poate genera manual cadre de acest tip folosind un adaptor Wi-Fi compatibil și software specializat (ex: aireplay-ng). Dispozitivele client, dacă recepționează aceste cadre false, consideră în mod legitim că au fost deautentificate și încheie conexiunea.  
 Deauthentication-ul este utilizat și în mod legitim, spre exemplu când un AP dorește să elibereze un client inactiv sau când un client se reconectează manual. Totuși, lipsa oricărei forme de autentificare a sursei acestor cadre face ca ele să fie un vector de atac des întâlnit. Standardul IEEE 802.11w încearcă să adreseze această problemă prin introducerea „Protected Management Frames”, dar suportul este limitat.  
În mod obișnuit, cadrele deauthentication sunt trimise direct (unicast) către un client specific, dar pot fi trimise și broadcast pentru a afecta toți clienții simultan. Majoritatea dispozitivelor moderne ignoră deauthentication broadcast din cauza abuzurilor frecvente, însă rămân vulnerabile la atacurile direcționate.

**6. Atacurile de deautentificare**

Atacurile de tip Deauthentication se bazează pe trimiterea unor cadre false de deautentificare (deauthentication frames) către dispozitivele client dintr-o rețea Wi-Fi. Aceste cadre sunt o parte legitimă a protocolului IEEE 802.11 și sunt folosite în mod normal pentru a încheia conexiunile dintre client și punctul de acces (AP). Cu toate acestea, lipsa oricărei forme de autentificare a acestor cadre în standardul de bază le face extrem de vulnerabile la spoofing și abuz.  
 Într-un atac clasic, atacatorul transmite în mod repetat cadre de deauthentication către un client sau către toți clienții conectați la un AP. Dispozitivele recepționează aceste cadre și consideră că deconectarea este legitimă. Drept urmare, ele încheie conexiunea și, în funcție de sistemul de operare și configurare, pot încerca automat reconectarea. Dacă atacatorul repetă trimiterea acestor cadre la intervale scurte, clientul nu mai reușește să se reconecteze, fiind prins într-un ciclu de deconectare continuă.

Există două variante principale ale atacului:

Broadcast Deauthentication – cadrele sunt trimise către toți clienții conectați la un AP. Este ușor de executat, dar multe dispozitive moderne ignoră cadrele broadcast nesemnate.

Unicast Deauthentication – cadrele sunt trimise țintit către adresa MAC a unui client. Este mai eficient, deoarece dispozitivul client consideră sursa ca fiind autentică.

Un atacator are nevoie de:

un adaptor Wi-Fi compatibil cu modul „monitor” și capabil de injecție de pachete,  
 software specializat (ex. aireplay-ng, mdk3, Scapy),  
 identificarea adresei MAC a clientului și BSSID-ul AP-ului (prin scanare cu airodump-ng).

Un exemplu tipic: atacatorul identifică un client activ, trimite cadre de deauthentication, clientul se deconectează și în timpul reconectării, atacatorul poate captura „4-way handshake”-ul pentru a încerca spargerea parolei WPA.

Pentru a combate aceste atacuri, standardul 802.11w introduce Protected Management Frames (PMF), care criptează cadrele de management (inclusiv deauthentication). Totuși, multe dispozitive nu suportă complet acest standard, iar altele îl dezactivează din motive de compatibilitate. În absența PMF, rețelele rămân vulnerabile la atacuri de deautentificare, mai ales în medii publice sau nesecurizate.

**7. Ce este DNS**

DNS (Domain Name System) este un sistem esențial pentru funcționarea internetului, responsabil pentru traducerea numelor de domenii ușor de înțeles de oameni (ex: [www.example.com](http://www.example.com" \t "/home/robert/Documents\\x/_new)) în adrese IP (ex: 93.184.216.34), pe care calculatoarele le pot utiliza pentru a comunica între ele. Sistemul DNS funcționează ca o agendă telefonică distribuită, oferind rapid adresa unui server atunci când un utilizator introduce un URL într-un browser.  
 DNS este organizat ierarhic. În vârf se află serverele root, care știu unde se află serverele pentru fiecare top-level domain (TLD), precum .com, .org, .ro. Sub acestea urmează serverele TLD care direcționează către serverele autoritare pentru fiecare domeniu (ex: example.com). Aceste servere autoritare cunosc adresele exacte ale subdomeniilor (ex: www, mail, ftp).  
Când un utilizator accesează un site, dispozitivul său trimite o interogare DNS către un server recursiv (de obicei, serverul DNS al providerului de internet sau unul public ca Google 8.8.8.8). Acesta caută în cache, iar dacă nu are răspunsul, inițiază o serie de interogări recursive pentru a obține IP-ul corect. Răspunsul este apoi returnat dispozitivului, care inițiază conexiunea către acel IP.  
 Sistemul DNS este rapid, flexibil și extensibil, dar prezintă și puncte slabe: interogările sunt de obicei transmise în text clar (UDP pe portul 53), fără criptare, ceea ce permite interceptarea, modificarea sau manipularea lor de către atacatori. Acest lucru a dus la dezvoltarea unor extensii precum DNSSEC, DoT (DNS over TLS) și DoH (DNS over HTTPS), care oferă integritate și confidențialitate. În lipsa acestor protecții, un atacator poziționat între client și serverul DNS poate modifica răspunsurile, direcționând utilizatorul către servere false.

**8. Mesajele DNS**

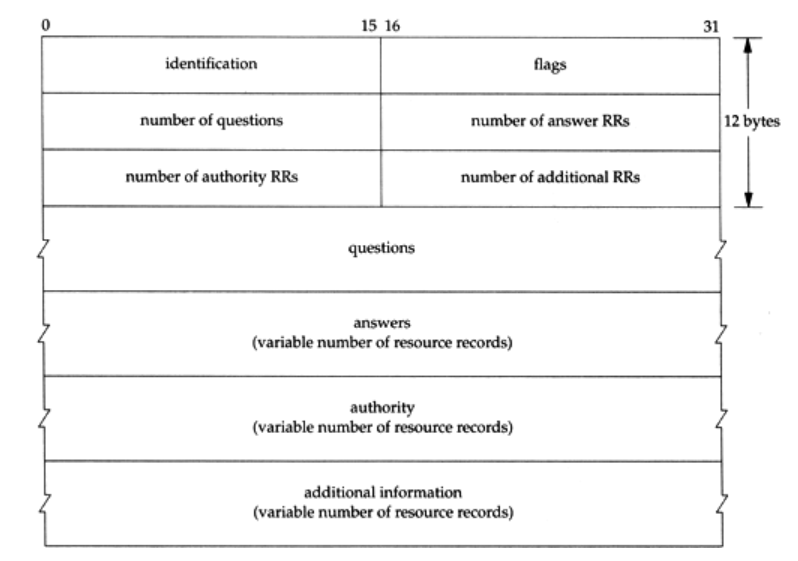
Protocolul DNS definește două tipuri principale de mesaje: request (interogare) și response (răspuns). Aceste mesaje sunt transmise de obicei prin protocolul UDP, pe portul 53, deși în unele cazuri (zone transfer, DNSSEC) se folosește TCP. Formatul mesajului DNS este standardizat și are o structură bine definită care permite funcționarea ierarhică și rapidă a sistemului.

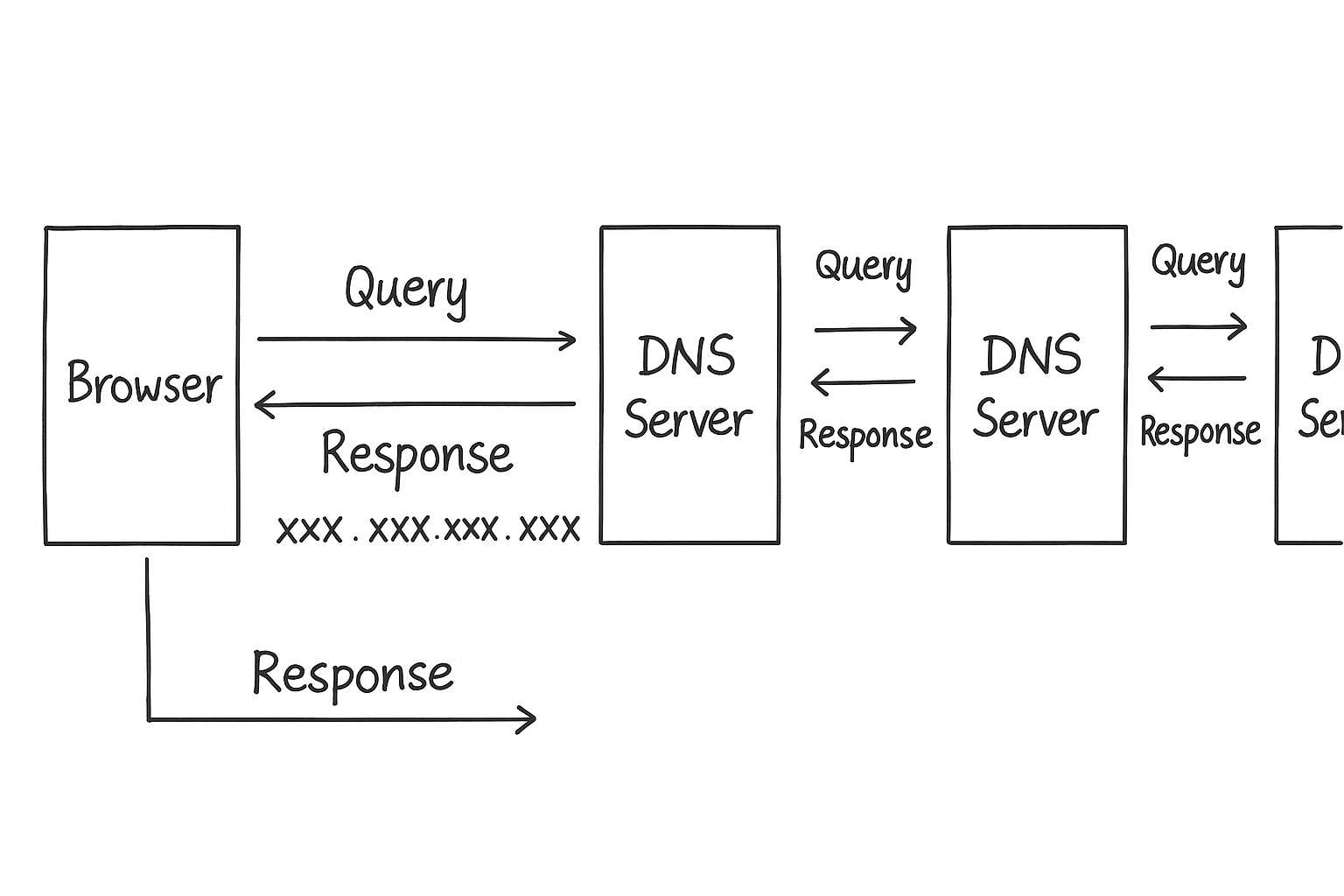
Un mesaj DNS conține următoarele secțiuni:

Header – 12 octeți care includ ID-ul unic al cererii, tipul mesajului (query/response), coduri de eroare, câmpuri de control (ex: dacă este răspuns autoritar, dacă se permite recursivitate).

Question – secțiunea care conține numele de domeniu solicitat și tipul de înregistrare (de regulă A pentru IPv4, AAAA pentru IPv6, dar și MX, CNAME, NS etc.).  
 Answer – secțiunea răspuns, care conține datele returnate (ex: IP-ul asociat cu domeniul).  
 Authority – indică serverul autoritar pentru domeniul interogat.  
 Additional – poate include informații adiționale utile (ex: alte IP-uri, TTL, recorduri de tip OPT pentru EDNS).

Într-o interogare simplă, un client cere „Care este IP-ul pentru www.example.com?”. Serverul DNS răspunde cu un mesaj de tip response în care secțiunea „Answer” conține înregistrarea de tip A: „93.184.216.34”. Dacă serverul nu cunoaște adresa, poate returna un răspuns „non-authoritative” sau poate redirecționa interogarea mai departe.  
 Lipsa de criptare a acestor mesaje le face vulnerabile la atacuri de tip spoofing și hijacking. Un atacator poate forja un răspuns fals către un client înainte ca serverul DNS legitim să răspundă, păcălindu-l astfel că IP-ul corect pentru un domeniu este cel al unui server malițios. Această tehnică stă la baza atacului de tip DNS Hijacking. Tehnologiile moderne încearcă să contracareze aceste riscuri prin validare criptografică (DNSSEC) sau criptare completă a transportului (DoT, DoH), dar implementarea nu este universală.





9. DNS Hijacking

DNS Hijacking este o tehnică prin care un atacator interceptează sau falsifică răspunsurile DNS ale unui utilizator, direcționându-l către adrese IP diferite de cele reale. Atacul exploatează în special lipsa criptării și verificării autenticității mesajelor DNS în scenariile clasice. Un dispozitiv compromis sau un atacator aflat în aceeași rețea poate intercepta cererea DNS și trimite un răspuns modificat mai rapid decât serverul legitim, convingând clientul că adresa IP a site-ului solicitat este alta.

Atacul poate avea loc în mai multe moduri:

Client-side hijacking – malware modifică configurația DNS a dispozitivului;

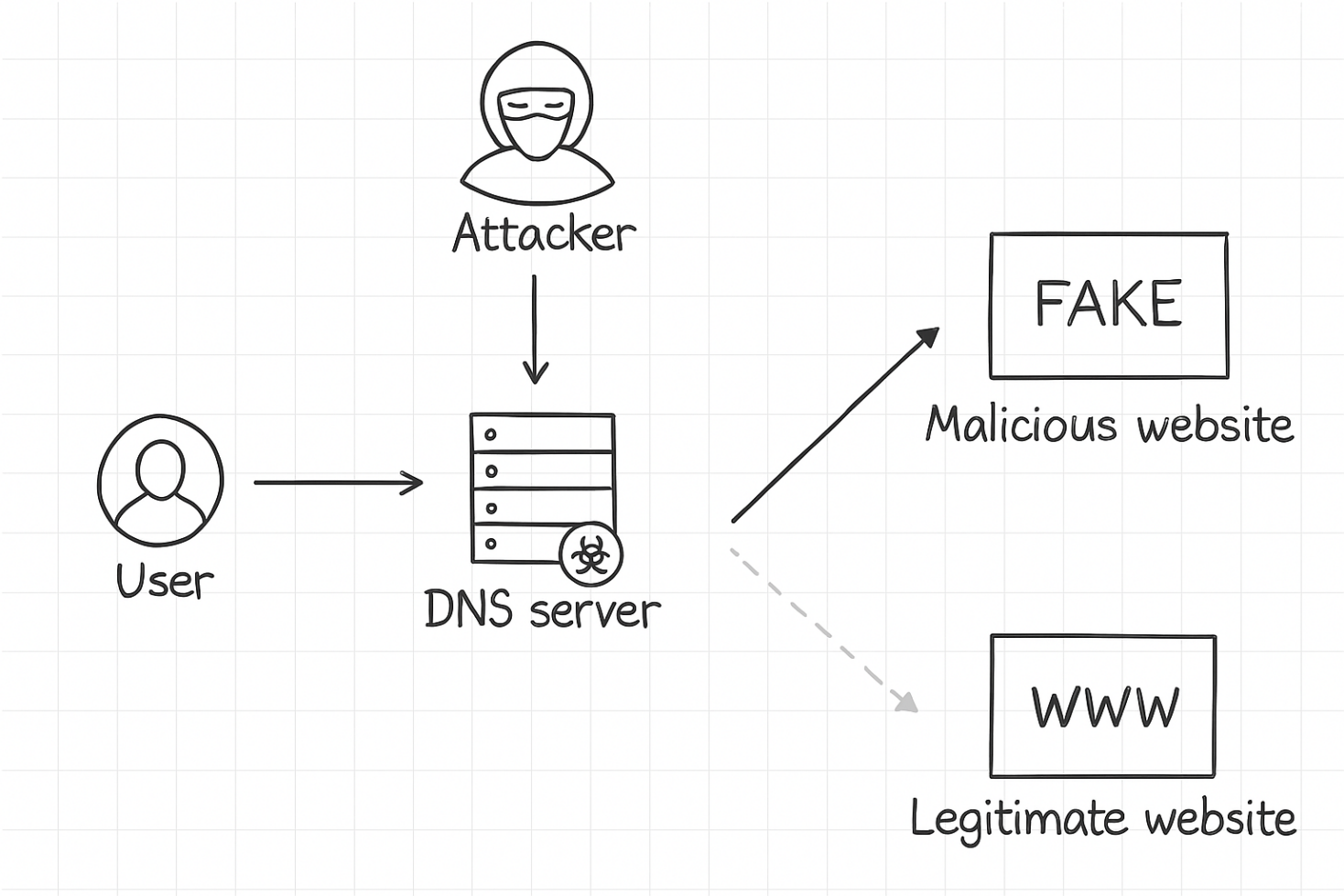
Router hijacking – atacatorul schimbă setările DNS pe routerul victimei;

Man-in-the-Middle – atacatorul aflat în aceeași rețea (ex: într-un Wi-Fi public) interceptează și răspunde la cereri DNS;

Evil AP DNS injection – un AP fals configurează prin DHCP un server DNS controlat de atacator.

În cazul proiectului bazat pe ESP32, hijacking-ul este realizat local, fără a accesa o rețea externă. ESP32 acționează simultan ca AP și server DNS. Prin DHCP, dispozitivele care se conectează primesc ca DNS server chiar adresa ESP32-ului. Ulterior, când utilizatorul accesează un domeniu (ex: „facebook.com”), cererea este interceptată de ESP32, care returnează propriul IP în locul adresei reale. Browserul utilizatorului deschide automat o pagină web găzduită local pe ESP32 – o clonă a paginii Facebook. Utilizatorul introduce datele, care sunt stocate de atacator.

Această tehnică este extrem de eficientă în rețele neprotejate și este dificil de detectat de către utilizatori obișnuiți, întrucât domeniul din bara de adresă rămâne aparent corect, iar conexiunea nu este securizată (HTTP în loc de HTTPS). Protejarea împotriva acestui tip de atac necesită validarea criptografică a răspunsurilor DNS (DNSSEC), criptarea traficului DNS (DoH/DoT) și evitarea conectării la rețele necunoscute.

****

**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>

## Arhitectura aplicației server-side pe ESP32

Pentru a susține funcționalitățile de scanare, atac și captare de date demonstrativă, aplicația rulează trei servere independente în paralel pe dispozitivul ESP32. Aceste servere sunt:

Un server web principal care expune o interfață REST simplă prin HTTP pe portul 8000, permițând utilizatorului să scaneze rețele, să activeze atacuri de tip deauthentication și flood.

Un server dedicat pentru pagina falsă de Facebook, expus pe portul 80, folosit în contextul unui atac DNS hijacking pentru a capta credențialele introduse de utilizator.

Un server DNS pe portul standard 53, care răspunde la interogările DNS și direcționează utilizatorii către ESP32 atunci când aceștia solicită domenii vizate (ex: facebook.com).

Toate cele trei servere sunt active simultan și rulează concurent folosind mecanismele asincrone ale sistemului de operare încorporat pe ESP32 (ex: FreeRTOS, task-uri separate).

### 1. Serverul Web Principal – Port 8000

Acest server gestionează comenzile principale transmise de utilizator printr-o interfață REST simplificată. Este punctul central de interacțiune și oferă acces la toate funcțiile experimentale.

Rutele expuse sunt:

#### 

#### GET /

Returnează pagina principală HTML (interfața de control).

Afișează butoanele pentru scanare, flood, attack etc.

#### GET /scan

Inițiază un proces de scanare a rețelelor Wi-Fi din proximitate.

Răspunsuri posibile:

200 OK – returnează un JSON cu lista rețelelor descoperite:

<structura JSON>

500 Internal Server Error – eroare în procesul de scanare (ex: Wi-Fi deja ocupat).

#### GET /attack?bssid=...&timeout=...

Inițiază un atac de deautentificare împotriva rețelei specificate.

Parametrii:

bssid: adresa MAC a AP-ului țintă.

timeout: durata atacului în secunde.

Răspunsuri:

200 OK – atacul a fost pornit cu succes.

400 Bad Request – lipsesc parametrii obligatorii.

500 Internal Server Error – eroare internă la lansarea atacului (ex: modul Wi-Fi instabil).

Efect: ESP32 imită AP-ul țintă și transmite cadre de deauthentication; în timpul atacului, ESP32 devine indisponibil pentru conexiuni.

#### GET /flood

Pornește atacul de tip AP Flood (transmiterea de cadre beacon false).

Răspunsuri:

200 OK – flood-ul a fost pornit.

500 Internal Server Error – imposibil de inițiat flood-ul.

#### GET /flood/stop

Oprește atacul flood dacă este activ.

Răspunsuri:

200 OK – atacul a fost oprit cu succes.

409 Conflict – atacul nu era activ (nu există instanță de flood pornită).

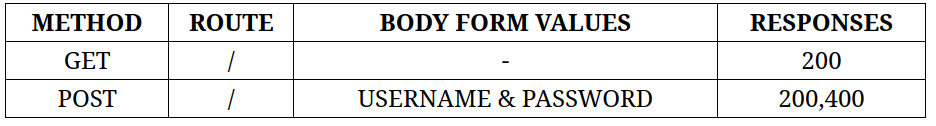
#### POST \*

Orice încercare de a face POST pe acest server este respinsă cu 404 Not Found.

Nu se acceptă trimiterea de date pe acest endpoint.

### 2. Serverul Facebook Fals – Port 80

Acest server este activat automat și rulează pe portul standard HTTP, simulând o pagină legitimă de autentificare Facebook. Este utilizat în contextul unui atac DNS hijacking, unde utilizatorul este direcționat către această pagină în loc de site-ul real.



#### GET /

Returnează pagina HTML statică ce imită interfața de autentificare Facebook.

Conține un formular cu câmpuri pentru username și parolă.

Această pagină este aproape identică vizual cu pagina reală, dar este servită de ESP32 fără TLS (HTTP simplu).

#### POST /

Este activat când utilizatorul introduce datele în formular și apasă „Log in”.

Serverul procesează formularul și salvează local datele introduse.

Nu există nicio validare reală – pagina de răspuns poate afișa un mesaj generic sau redirect în buclă.

Informațiile pot fi afișate ulterior în interfață de către utilizator (ex: printr-un buton în / din serverul principal care citește aceste date).

### 3. Serverul DNS – Port 53

Acest server DNS minimalist este activ doar pentru a intercepta cererile DNS ale dispozitivelor conectate la ESP32. După conectare prin DHCP, dispozitivul client primește adresa ESP32-ului ca DNS principal. Astfel, toate interogările DNS sunt direcționate către ESP32.

Comportamentul este următorul:

Dacă se solicită un domeniu care conține facebook (ex: www.facebook.com):

Serverul returnează IP-ul local al ESP32, obligând clientul să acceseze pagina falsă.

Pentru orice altă cerere:

Fie este blocată (returnând un răspuns vid sau 127.0.0.1),

Fie este ignorată, în funcție de implementare.

Această redirecționare permite simularea unui DNS hijacking complet local, fără acces la internet și fără intervenții externe. Victima crede că a fost conectată la internet și deschide site-ul Facebook, dar în realitate interacționează cu ESP32.

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/>