Seguretat Wi-Fi i Teletreball: Detecció d'Atacs i Mitigació de Riscos en Entorns Inalàmbrics Remots

Joan García Capell

30 de juny de 2025

Resum– Aquest projecte se centra en el desenvolupament d'un agent de seguretat per a entorns de teletreball, amb l'objectiu de detectar i mitigar atacs en xarxes Wi-Fi domèstiques o públiques. L'agent, executat en dispositius, monitorarà el tràfic de xarxa en temps real mitjançant diferents eines, identifica patrons d'atacs (com Evil Twin o deautenticació massiva) i generarà alertes mitjançant un dashboard interactiu. Implementa regles heurístiques bàsiques per a la detecció d'anomalies. El sistema inclou funcionalitats de registre de logs i accions automàtiques per la mitigació. Les proves es realitzaran en un entorn de laboratori simulat i els resultats confirmen l'alta eficàcia de l'agent en la detecció i mitigació d'atacs Wi-Fi, però també posen de manifest la complexitat d'implementar-lo en un entorn productiu.

Paraules clau– Ciberseguretat, Teletreball, Wi-Fi, Monitoratge, Detecció d'atacs, Agent

Abstract– This project focuses on the development of a security agent for remote-work environments, with the goal of detecting and mitigating attacks on home or public Wi-Fi networks. The agent, deployed on client devices, monitors network traffic in real time using various tools, identifies attack patterns (such as Evil Twin or mass deauthentication), and generates alerts via an interactive dashboard. It implements basic heuristic rules for anomaly detection. The system includes logging functionality and automated mitigation actions. Tests are carried out in a simulated laboratory environment, and the results confirm the agent's high effectiveness in detecting and mitigating Wi-Fi attacks, while also highlighting the complexity of deploying it in a production setting.

Keywords– Cybersecurity, Remote Work, Wi-Fi, Monitoring, Attack Detection, Agent.

1 Introducció

En l'era del teletreball, la seguretat de les connexions Wi-Fi esdevé un element crític, ja que moltes xarxes domèstiques i públiques no compten amb les mateixes mesures de protecció que les xarxes corporatives. Aquesta situació les fa especialment vulnerables a atacs com els Evil Twin [1], la deauthentication [2], el jamming [3] i el spoofing [4], que poden comprometre tant la privacitat com la integritat de les dades.

La motivació d'aquest projecte neix de la necessitat creixent de garantir una major seguretat en els entorns remots. Amb l'augment del teletreball, és essencial oferir solucions pràctiques que permetin als usuaris protegir-se davant d'aquests atacs, minimitzant riscos i evitant pèrdues d'informació o altres danys derivats de vulnerabilitats en la xarxa.

Aquest document exposa els principals aspectes del projecte, començant per una definició clara dels objectius: entendre el funcionament de les xarxes Wi-Fi i les amenaces associades, dissenyar l'arquitectura del sistema, desenvolupar el prototip de l'agent de monitoratge i realitzar proves en entorn controlat. A més, es descriurà la metodologia àgil adoptada i es detallarà la planificació del desenvolupament en diversos sprints amb dates clau i lliuraments específics. Finalment, es presentaran els resultats obtinguts i es discutirà com aquests poden contribuir a una millor protecció de les xarxes en entorns de teletreball.

• E-mail de contacte: Joan.GarciaC@autonoma.cat
• Menció realitzada: Tecnologies de la Informació
• Treball tutoritzat per: Miguel Carpio Miranda (DEiC)
• Curs 2024/25

2 OBJECTIUS

L'objectiu principal d'aquest projecte és desenvolupar un agent que monitoritzi i detecti atacs en xarxes Wi-Fi en entorns de teletreball, de manera que es puguin identificar riscos i millorar la seguretat en connexions domèstiques i públiques.

Per aconseguir-ho s'han marcat els següents subobjectius

2.1 Entendre el funcionament de les xarxes Wi-Fi i les possibles amenaces.

Es vol aprendre com funcionen les xarxes sense fils i quines amenaces poden afectar-les, com per exemple atacs tipus Evil Twin, deauthentication o altres vulnerabilitats habituals. Aquesta comprensió servirà de base per al disseny i desenvolupament del projecte.

2.2 Dissenyar l'Arquitectura del Sistema.

Cal definir com serà l'estructura del sistema, quins components tindrà i com interactuaran entre ells. Això inclou establir els requisits bàsics en termes de funcionalitat, rendiment i seguretat, per assegurar que l'agent compleixi les seves tasques de monitoratge i detecció.

2.3 Desenvolupar un Protòtip.

Aquesta fase consisteix en programar el prototip de l'agent, que haurà de capturar el tràfic Wi-Fi, analitzar els paquets que circulen i registrar els esdeveniments rellevants. El prototip ha de ser funcional per servir de prova de concepte.

2.4 Provar en Entorn Controlat.

Finalment, es realitzaran proves en un entorn emulat que recreï situacions reals, amb diferents access points i dispositius. L'objectiu és comprovar que l'agent detecta correctament els atacs i respon de manera efectiva a les amenaces.

3 ESTAT DE L'ART

Amb l'augment del teletreball, la seguretat en les xarxes Wi-Fi s'ha convertit en una preocupació important, ja que moltes xarxes, sobretot les domèstiques o públiques, no disposen de les mesures de protecció necessàries i són objecte d'atacs diversos.

Un dels atacs més coneguts és l'*Evil Twin Attack*, on un atacant crea un punt d'accés Wi-Fi fals per enganyar els usuaris perquè es connectin a ell, facilitant així l'accés a informació sensible.

D'altra banda, els atacs de *Deauthentication* desconnecten forçadament els dispositius de la xarxa, cosa que pot provocar interrupcions importants i obrir la porta a altres intrusions.

Els *Jamming Attacks* interfereixen amb la transmissió dels senyals Wi-Fi, bloquejant la comunicació entre dispositius i afectant el rendiment global de la xarxa.

En un *Spoofing Attack* es falsifiquen les identitats per accedir indegudament a la xarxa, cosa que pot comprometre la integritat de la informació.

Per a la detecció d'aquests atacs, s'utilitzen eines de monitoratge com **Kismet** [5] i la suite **Aircrack-ng** [6], que permeten recollir i analitzar el tràfic Wi-Fi en temps real, identificar xarxes sospitoses i auditar la seguretat dels sistemes.

Pel que fa als estàndards de seguretat, l'estàndard IEEE 802.11i (implementat com WPA2) estableix mecanismes d'encriptació i autenticació que han ajudat a protegir les xarxes Wi-Fi [7]. Més recentment, WPA3 ha estat introduït per millorar encara més aquesta protecció, tot i que encara es detecten vulnerabilitats [8].

Finalment, els sistemes de detecció d'intrusions Wi-Fi (WIDS) són clau per identificar activitats anòmales i intents d'intrusió en temps real [9].

En comparació amb les solucions comercials de WIPS, que sovint requereixen dispositius dedicats i una infraestructura de maquinari addicional, l'agent desenvolupat en aquest projecte ofereix un enfocament més lleuger i flexible. S'executaría directament en l'ordinador del treballador, sense necessitat d'instal·lar accessoris o punts d'accés específics, i aprofita les interfícies natives de Linux per capturar i analitzar trànsit. Això redueix tant els costos d'implantació com les dependències de manteniment de maquinari extern, alhora que garanteix una rapidesa de desplegament i una portabilitat òptima per a entorns de teletreball.

4 METODOLOGIA I PLANIFICACIÓ

Per al desenvolupament d'aquest projecte s'ha escollit la metodologia **Scrum** [10], ja que és una metodologia Agile que permet treballar de forma iterativa i flexible. Aquesta metodologia facilita la incorporació de feedback constant i l'ajust dels requisits a mesura que avança el projecte. Es planificarà el desenvolupament dividint-lo en diversos *sprints* breus, com es veu en la Fig. 10 de l'apèndix A.1, on es revisaran i validaran les funcionalitats de manera regular.

Sprint 1: Investigació i Anàlisi de Requisits. En aquest primer sprint es durà a terme una recerca per comprendre el funcionament de les xarxes Wi-Fi i identificar les amenaces més comunes, així com definir els requisits bàsics del sistema.

Sprint 2: Disseny de l'Arquitectura del Sistema. Es definirà l'estructura global de l'agent, especificant els components necessaris i establint la interacció entre ells, així com la selecció de tecnologies adequades.

Sprint 3: Desenvolupament del Protòtip. En aquest sprint es programarà el prototip, implementant els mòduls de captació de tràfic i d'anàlisi de paquets per detectar atacs en temps real.

Sprint 4: Integració i Proves en Entorn Controlat. Es duran a terme proves en un entorn simulat per verificar que l'agent detecta correctament els atacs (com Evil Twin, deauthentication, jamming i spoofing) i es faran els ajustos necessaris.

Sprint 5: Documentació i Preparació de la Presentació. Finalment, es recopilaran els resultats, s'elaborarà l'informe final i es prepararà la presentació oral del projecte.

5 INFRAESTRUCTURES DE XARXA PER AL TELETREBALL

Amb l'augment del teletreball, les organitzacions han adoptat diverses infraestructures per garantir un accés segur als recursos corporatius. Cada model ofereix avantatges i inconvenients, i el seu nivell de seguretat pot variar segons la configuració i la mida de l'empresa. A continuació es descriuen les solucions més habituals i les amenaces associades a cadascuna.

5.1 Xarxa Privada Virtual (VPN)

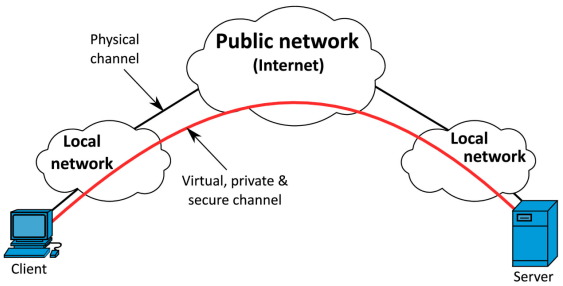

Fig. 1: Esquema d'una connexió VPN

La VPN (*Virtual Private Network*) és una de les opcions més comunes per a les petites i mitjanes empreses. Permet establir un túnel xifrat entre l'usuari i la xarxa corporativa, facilitant l'accés remot a fitxers i aplicacions (vegeu Fig. 1).

Tot i la seva simplicitat, la VPN pot ser vulnerable si el dispositiu client està compromès o si la connexió s'estableix des d'una xarxa Wi-Fi insegura. A més, una configuració inadequada o la manca d'autenticació multifactor pot exposar la infraestructura a atacs remots [11].

5.2 Accés remot a escriptori (RDP)

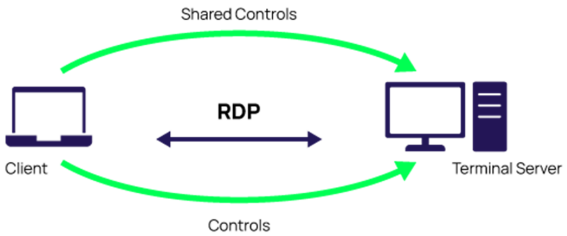

Fig. 2: Flux de controls amb RDP

L'accés mitjançant RDP (*Remote Desktop Protocol*) permet connectar-se de forma remota a un ordinador dins la xarxa corporativa, sovint des d'una connexió protegida per VPN. Aquesta opció és habitual en entorns on cal preservar l'entorn de treball local de l'empresa (vegeu Fig. 2).

Els riscos més habituals inclouen atacs de força bruta, vulnerabilitats no actualitzades en el servei RDP i connexions directes des d'internet sense una capa addicional de protecció. També cal assegurar una gestió correcta dels permisos i una supervisió constant de l'activitat.

5.3 Infraestructura d'Escriptori Virtual (VDI)

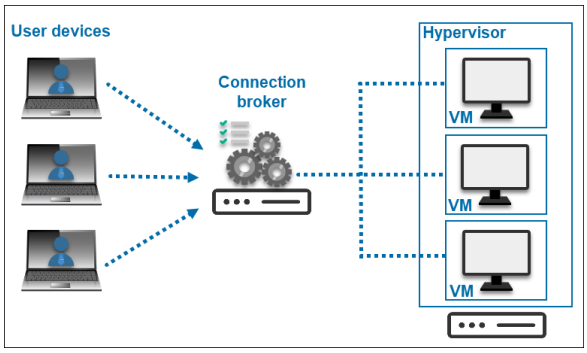

Fig. 3: Arquitectura d'una solució VDI

La VDI (*Virtual Desktop Infrastructure*) permet accedir a escriptoris virtuals allotjats en servidors interns de l'empresa. Tota la gestió de dades i aplicacions es fa des d'aquests servidors, reduint el risc de filtració d'informació sensible (vegeu Fig. 3).

Aquest model ofereix un alt nivell de control i seguretat, però pot ser costós d'implementar. Si no s'apliquen polítiques adequades de segmentació i autenticació, pot resultar vulnerable a atacs interns o elevacions de privilegi dins l'entorn virtual.

5.4 Escriptori com a Servei (DaaS)

Fig. 4: Model DaaS al núvol

El model DaaS (*Desktop as a Service*) és similar a la VDI, però les màquines virtuals s'allotgen al núvol i són gestionades per un proveïdor extern. Aquesta solució ofereix escalabilitat i facilita l'accés des de qualsevol lloc, sense necessitat d'infraestructura pròpia (vegeu Fig. 4).

Tanmateix, la seguretat depèn de la configuració del proveïdor i de les polítiques d'accés implementades. Un accés no controlat des de xarxes públiques o dispositius no gestionats pot exposar dades sensibles [12].

6 ANÀLISI D'AMENACES I VULNERABILITATS EN ENTORNS WI-FI DE TELETREBALL

Les xarxes Wi-Fi domèstiques i públiques utilitzades per treballadors en remot poden ser objectiu fàcil d'atacs si no es gestionen correctament. L'ús de dispositius personals, la manca de segmentació i la connexió a punts d'accés no fiables multipliquen els riscos per a les dades i sistemes corporatius. A continuació es detallen les principals vulnerabilitats i amenaces identificades en aquest context.

KRACK (Key Reinstallation Attack): aquesta vulnerabilitat afecta el protocol WPA2 i permet a un atacant reinjectar claus criptogràfiques, interceptar dades i, fins i tot, manipular-les sense necessitat de desxifrat complet [13].

FragAttacks: un conjunt de vulnerabilitats descobertes recentment que exploten errors en la gestió de la fragmentació de trames en WPA2 i WPA3. Poden ser utilitzades per injectar paquets maliciosos o filtrar dades sensibles [19].

Deauthentication attacks: els atacs de desautenticació forcen la desconnexió d'un dispositiu de la xarxa Wi-Fi enviant paquets falsos de control. Són habituals en atacs de denegació de servei o com a pas previ per a suplantacions [15].

WPS actiu: la presència d'aquesta funcionalitat suposa un risc, ja que pot ser atacada mitjançant força bruta. Permet obtenir la contrasenya de la xarxa en minuts si no es desactiva [16].

Evil Twin i suplantació de SSID: mitjançant la creació d'un punt d'accés fals amb el mateix nom que una xarxa de confiança, els atacants poden capturar credencials o injectar codi maliciós en el tràfic de l'usuari [17].

Jamming i sniffing: el jamming consisteix en saturar el canal Wi-Fi amb interferències per tallar la comunicació. El sniffing, en canvi, permet interceptar tràfic de la xarxa sense fils si aquest no està degudament xifrat [18].

Altres amenaces a tenir en compte inclouen les **contrasenyes febles**, que poden ser trencades mitjançant atacs de diccionari si s'intercepta el procés d'autenticació, i la **manca de segmentació de xarxa**, típica en entorns domèstics, que permet que dispositius no autoritzats dins la mateixa LAN realitzin escanejos de ports o moviment lateral entre sistemes.

A més, la **presència de dispositius desconeguts a la xarxa** representa un risc constant, ja que poden actuar com a vectors d'atac si estan compromesos. Aquest fet és especialment rellevant en llars on es comparteix la xarxa amb altres persones o dispositius IoT sense control de seguretat.

Aquestes vulnerabilitats evidencien la necessitat d'una solució de monitoratge capaç de detectar comportaments anòmals i alertar sobre configuracions insegures. Un agent que monitoritzi l'estat de la xarxa i del dispositiu pot ajudar a mitigar part d'aquestes amenaces.

7 IDENTIFICACIÓ I SELECCIÓ DE FUNCIONALITATS CLAU

Com a resultat de l'anàlisi prèvia d'amenaces, s'han definit un conjunt de funcionalitats essencials per a l'agent de monitoratge, orientades a detectar vulnerabilitats i comportaments sospitosos en xarxes Wi-Fi en entorns de teletreball. A més de la seva rellevància en ciberseguretat, s'ha tingut en compte la viabilitat tècnica per implementar-les mitjançant Python a Linux.

La **detecció de vulnerabilitats KRACK i FragAttacks** es pot implementar capturant paquets EAPOL i identificant patrons sospitosos com missatges repetits (KRACK) o trames fragmentades amb comportament anòmal (FragAttacks). Per a això, es poden utilitzar biblioteques com `Scapy` o `Pyshark` i scripts com els desenvolupats per Vanhoef [19].

Per al **monitoratge de paquets de deautenticació**, es pot activar la interfície en mode monitor i filtrar per paquets de tipus `deauth`. Una freqüència elevada d'aquests paquets pot indicar un atac actiu [20].

La **verificació de l'estat del WPS** es pot fer escanejant les beacons amb `iw` o `nmcli` i identificant si el paràmetre WPS està present, alertant l'usuari en cas afirmatiu [21].

La **verificació del tipus de xifrat (WPA2/WPA3)** s'obté del mateix escaneig de beacons o des de les connexions establertes. Si es detecta el mode transicional WPA3 (accepta també WPA2), es genera una advertència.

L'**anàlisi de la fortalesa de la contrasenya** es pot fer localment (si el sistema ho permet) comprovant la longitud, entropia tipus de caràcters i coincidència amb llistes de contrasenyes febles conegudes. També es pot deduir la feblesa si l'SSID és un nom per defecte del fabricant.

La **detecció de suplantació de SSID** (Evil Twin) es realitza escanejant els SSIDs visibles i identificant si hi ha múltiples BSSIDs amb el mateix nom. Es poden fer comprovacions de canals, potència del senyal, xifrat o aplicació d'una whitelist de BSSIDs per decidir si un punt d'accés és legítim o sospitós [22].

Per a la **detecció de VPN**, el sistema pot utilitzar mòduls com `psutil` o `netifaces` per veure si hi ha una interfície activa com `tun0` o `tap0`, si l'encaminament per defecte va per aquestes interfícies o analitzant la IP pública. Si no hi és, es pot alertar l'usuari o bloquejar el tràfic amb regles de `iptables` (Kill-switch VPN).

La **detecció de jamming, sniffing i escanejos de ports** es pot abordar monitoritzant trames ARP per detectar ARP spoofing o anomalies en la latència i pèrdua de paquets. Per escanejos de ports es poden detectar connexions breus a molts ports en poc temps [23, 24, 25].

La **comprovació de segmentació de la xarxa** i de **dispositius connectats** pot ser més costosa, no obstant això, pot fer-se escanejant la LAN amb `arp-scan` o `nmap`. Això permet detectar dispositius desconeguts en una mateixa xarxa no segmentada. Si la xarxa està ben segmentada, serà molt complicat, ja que els BSSIDs dels APs que emeten per diferents ESSIDs, generen APs virtuals alternant el BSSID a partir de la MAC típica de l'AP. Per tant, l'única manera d'identificar que dos o més ESSIDs provenen del mateix AP, seria analitzant altres paràmetres com el canal, potencia, fabricant o interval de beacon. Tot i això, no és una forma determinista.

També s'ha de verificar si hi ha **ports oberts**, **antivirus actiu** i controlar el **rendiment de la xarxa**. Es poden usar comandes de sistema, biblioteques com `psutil` i comandes com `netstat` o `ss`. Respecte a l'anàlisi de ports, es podria utilitzar l'eina `nmap` o tractar de fer un script manual amb sockets i provant els diferents ports.

Finalment, es proposa una interfície gràfica senzilla amb

`tkinter` on es mostrin alertes i es pugui configurar la resposta automàtica del sistema (desconnexió, bloqueig, notificació), per tal d'actuar de manera preventiva davant les amenaces detectades.

8 ARQUITECTURA DE L'AGENT DE MONITORATGE

L'agent de monitoratge dissenyat per aquest projecte està estructurat de manera modular amb l'objectiu de garantir la seva escalabilitat, mantenibilitat i facilitat d'ús. Aquesta arquitectura permet executar el sistema com un servei de fons en equips Linux, amb capacitat per recollir dades de la xarxa, analitzar-les i aplicar mesures de protecció, tot mantenint la interacció amb l'usuari mitjançant una interfície gràfica senzilla però funcional.

8.1 Arquitectura de l'agent de monitoratge

La Figura 5 mostra el diagrama d'alt nivell definit. Es tracta d'una arquitectura modular en la qual cada component té un paper clar: captura del tràfic, anàlisi i correlació, i gestió de respostes juntament amb la interfície d'usuari.

Els mòduls no s'executen en processos independents sinó com a fils (`threads`) dins del mateix procés Python. La comunicació entre ells es realitza mitjançant cues de missatges internes i crides a funcions, i els resultats d'anàlisi s'envien a la GUI a través de callbacks de Tkinter (`self.master.after`), cosa que garanteix que la interfície d'usuari no es bloquegi encara que el nombre d'esdeveniments sigui elevat.

D'aquesta manera, la captura de paquets amb Scapy en mode monitor i l'execució de cada prova (deautenticació, WPS, SSID spoofing, etc.) es fan en fils separats, mentre que l'actualització de l'estat i dels missatges es realitza de forma thread-safe, aprofitant el bucle d'esdeveniments de Tkinter per a la sincronització amb la GUI.

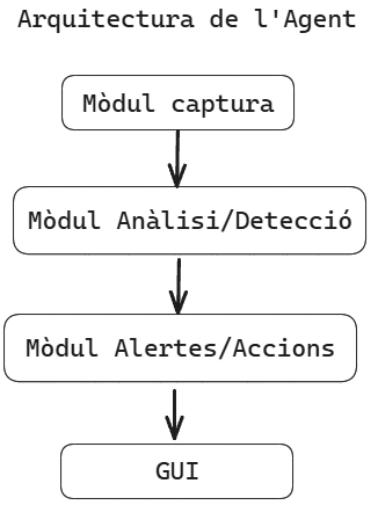

Fig. 5: Visió general de l'arquitectura implementada

8.2 Mòdul de captura de tràfic

Aquest mòdul s'encarrega d'obtenir dades de la xarxa de forma contínua. Per capturar paquets en temps real i analitzar-ne el contingut, es fa ús de biblioteques com `Scapy` i `Pyshark`. `Scapy`, que és la que més s'ha utilitzat, permet la manipulació i inspecció detallada de paquets a baix nivell, sent útil per identificar trames EAPOL, Beacon o Deauthentication [26]. `Pyshark`, basat en TShark, permet extreure informació estructurada dels paquets de forma eficient i ràpida, facilitant la detecció d'anomalies de forma automatitzada [27].

A més, aquest mòdul utilitza comandes del sistema per complementar les dades de la capa de xarxa. L'eina `iw` proporciona informació sobre l'estat de la interfície Wi-Fi, canals actius i configuració actual [28]. Amb `nmcli`, s'obtenen paràmetres com el SSID, el tipus d'autenticació i l'adreça IP associada [29]. Per detectar dispositius presents a la xarxa local, s'utilitza `arp-scan`, que envia peticions ARP a tots els dispositius d'un rang determinat [30]. Finalment, amb `nmap`, es poden identificar serveis actius i ports oberts, així com fer escanejos de vulnerabilitats superficials [31]. Aquest conjunt d'eines proporciona una base de dades fiable per a l'anàlisi de seguretat.

8.3 Mòdul d'anàlisi

Aquest mòdul processa les dades recollides pel mòdul anterior aplicant regles de detecció definides per identificar comportaments maliciosos o vulnerabilitats conegudes. Les regles poden detectar, per exemple, l'aparició de trames EAPOL repetides (indicadors d'un atac KRACK), trames fragmentades malformades (FragAttacks), trames Deauth recurrents o múltiples punts d'accés amb el mateix SSID (Evil Twin).

També es verifica la configuració actual del punt d'accés: si s'utilitza WPA2 o WPA3, si s'accepten connexions mixtes (mode transicional), si el WPS està actiu o si s'utilitza una VPN. L'anàlisi pot incloure també comprovacions de la força de la contrasenya, comparant-la amb patrons febles coneguts o noms de xarxa predeterminats.

Aquest mòdul es dissenya per funcionar de manera contínua, amb l'opció d'afegir noves regles en forma de fitxers YAML o JSON, fet que permet la seva ampliació sense alterar el codi principal.

8.4 Mòdul de notificació i resposta

Quan es detecta una anomalia o amenaça, aquest mòdul és responsable de gestionar la resposta del sistema. Pot registrar l'esdeveniment en un fitxer de log, generar notificacions visibles a l'usuari i executar accions automàtiques preconfigurades.

Les respostes automatitzades poden incloure l'ús de `iptables` per bloquejar connexions sospitoses, desactivar la interfície de xarxa amb `nmcli`, o eliminar xarxes conegudes no segures del sistema [32]. Aquest mòdul també pot restringir el tràfic de sortida si no es detecta cap interfície VPN activa. Totes aquestes accions es poden configurar segons el nivell de criticitat i el context de connexió (xarxa pública o privada, per exemple).

8.5 Interfície gràfica d'usuari (GUI)

La GUI servirà com a punt central de visualització i control per a l'usuari final. Es desenvoluparia amb `Tkinter`, permetent mostrar en temps real l'estat de la seguretat, les alertes actives, els dispositius detectats i la configuració actual [33].

Des de la GUI es podria activar o desactivar mòduls específics, establir respostes automàtiques, consultar informes d'activitat i configurar xarxes de confiança. El disseny buscarà l'equilibri entre accessibilitat i control, de manera que pugui ser utilitzada per usuaris no tècnics però també personalitzable per administradors de sistemes.

Aquest enfocament modular permet que el sistema sigui escalable i flexible. Les funcionalitats es poden actualitzar o substituir fàcilment i el sistema es pot integrar en entorns corporatius complexos o dispositius individuals amb pocs recursos.

9 Desenvolupament de l'agent de monitorització Wi-Fi

Aquest apartat descriu, des d'un punt de vista eminentment pràctic, com s'ha construït l'agent encarregat de vigilar la seguretat de la xarxa sense fils en entorns de teletreball. El desenvolupament s'ha dut a terme íntegrament sobre un entorn **Kali Linux Live USB**[34], de manera que no cal instal·lar cap sistema permanent ni modificar la configuració del portàtil corporatiu: simplement s'inicia el live-USB, es carrega l'script principal i l'agent comença a treballar. La Figura 6 mostra l'arquitectura que finalment s'ha aconseguit, i l'estructura de directoris i fitxers del projecte es detalla a l'Apèndix (Fig. 11). L'elecció de Kali respon a la seva disponibilitat de drivers Wi-Fi en mode *monitor* i a la presència prèvia de la major part de llibreries de seguretat.

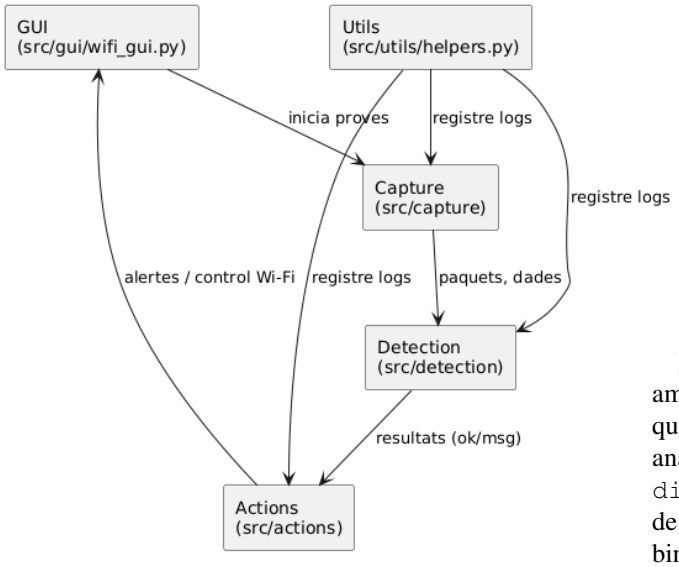

Fig. 6: Diagrama de l'arquitectura del prototi

9.1 Mòdul de captura de trànsit

El nucli d'aquest mòdul gestiona el canvi de la interfície Wi-Fi a *monitor mode* mitjançant la crida a la funció `enable_monitor_mode(iface)` de `utils.py`, que invoca `airmon-ng` per aturar processos conflictius i habilitar el mode monitor sobre la interfície detectada. Un cop en mode monitor, cada prova de detecció captura paquets mitjançant Scapy de forma puntual i acotada:

- **Detecció de desautenticació**: la funció `analyze_deauth(iface, timeout)` utilitza `sniff(iface=iface, timeout=timeout, store=True)` per recollir els paquets durant el període definit i filtra els frames IEEE 802.11 amb `subtype == 12`, comptant parells `(src, dst)` que apareixen $\geq$ 2 vegades i retornant un resultat boolean i un missatge descriptiu.

- **Anàlisi de jamming, Rickroll i marauding**: `analyze_marauding(iface, interval, duration)` arrenca en un fil separat un `sniff(iface=iface, prn=packet_handler, store=True)`, on es comptabilitzen beacons, errors CRC i altres tipus de trames (p. ex., ARP, Probe Request). Cada interval es compara amb un *baseline* inicial:

  - Si el nombre d'errors CRC excedeix el llindar superior, s'identifica un atac de *Jamming*.
  - Si el total de trames s beacon puja de sobte per sobre del llindar, es classifica com a *Rickroll*.
  - Si s'observen variacions irregulars en el nombre i tipus de trames (per exemple, pics de trames ARP o Probe Request procedents de múltiples adreces), es marca com a *Marauding*.

  Es genera una alerta amb el tipus d'atac detectat i s'escriu un registre detallat al fitxer de logs.

- **Verificació de WPS**: la funció `analyze_wps(iface, ssid, timeout)` captura trames `Dot11Beacon` i `Dot11ProbeResp` durant un temps limitat, parseja les TLVs vendor per detectar finestres WPS i determina el mètode en ús: *Push Button Configuration* (PBC) o *PIN*. Retorna un tupla `(activitat_wps, tipus_wps)`, on `activitat_wps` és *True* si s'ha detectat activitat i `tipus_wps` pren els valors `"PBC"` o `"PIN"`, o bé `Çap"` si no s'ha detectat cap activitat.

Durant cada prova, s'enregistra un fitxer de logs amb informació detallada d'esdeveniments i estadístiques, que es desa al directori de treball per a possibles anàlisis fora de línia. En finalitzar, l'agent crida `disable_monitor_mode(iface)` per restablir el mode gestionat. Aquest disseny puntual de captures, combinat amb la generació de logs, facilita el seguiment i la traçabilitat de les deteccions sense sobrecarregar indegudament els recursos del sistema.

9.2 Mòdul d'anàlisi i correlació

Totes les proves s'executen en temps real mitjançant l'API Python pròpia, que retorna un valor booleà i un missatge descriptiu per a cada test:

- **Anàlisi de contrasenya robusta:** la funció `analyze_password()` extreu la clau precompartida dels fitxers locals de configuració (p. ex. `/etc/wpa_supplicant.conf`) i realitza quatre comprovacions seqüencials: longitud mínima (8 caràcters), varietat de caràcters (majúscules, minúscules, dígits i símbols), càlcul d'entropia amb `estimar_entropia()` i anàlisi de patrons febles amb l'algoritme `zxcvbn`. Si alguna comprovació falla, retorna `False` i un motiu detallat; altrament, retorna `True`.
- **Anàlisi de protocol de seguretat:** la funció `analyze_protocol()` invoca `nmcli` per obtenir la sortida d'estat de la connexió (p. ex. `nmcli -f SSID,SECURITY dev wifi`) i extreu el xifrat utilitzat (WEP, WPA2, WPA3, etc.). Si hi ha retrocompatibilitat amb protocols menys segurs, la seguretat resultant s'equipara al protocol menys segur compatible; en cas que el protocol detectat sigui considerat insegur, retorna `False` amb un comentari explicatiu.
- **Detecció de suplantació d'SSID:** la funció `analyze_ssid_spoof()` comprova si existeixen més d'un BSSID emetent el mateix ESSID i compara cada adreça MAC detectada amb una llista blanca de SSID de confiança. Qualsevol emissor addicional que no figure a la whitelist dispara un avís de possible *Evil Twin*.
- **Comprovació de l'estat de la VPN:** la funció `analyze_vpn()` inspecciona les interfícies de túnel (p. ex. `tun0`, `tap0`) i les rutes per defecte del sistema per verificar que tot el trànsit passi pel túnel segur. En absència d'una connexió VPN activa, retorna `False` i un missatge indicant la necessitat d'habilitar-la.
- **Escaneig de ports:** la funció `analyze_ports()` utilitza `nmap.PortScanner()` per realitzar un escaneig SYN (rangs 1–65535) tant sobre l'host remot indicat com sobre la pròpia màquina local (`127.0.0.1`). D'aquesta manera es detecten ports oberts que podrien exposar serveis vulnerables, tant a l'exterior com dins de la mateixa xarxa local.

Un cop finalitzada cada prova, la informació obtinguda (resultat i missatge) es transmet directament al mòdul de resposta i notificació per tal de generar les alertes i accions de mitigació corresponents.

9.3 Mòdul de notificació i resposta

Cada prova individual invoca el mòdul de notificació perquè mostri immediatament, al costat de cada ítem de la GUI, un indicador i un missatge descriptiu si s'ha detectat algun problema.

Un cop finalitzat l'escaneig complet, el sistema calcula un percentatge global de seguretat. Si aquest valor queda per sota d'un llindar crític (p. ex. ¡ 30%), l'agent executa automàticament la desconnexió de l'usuari mitjançant:

```
nmcli device disconnect <interfície>
```

i immediatament mostra a l'usuari una alerta emergent amb informació sobre l'estat crític i dues opcions: "Acceptar i continuar desconnectat" o "Ignorar i reconnectar".(vegeu la Figura 7).

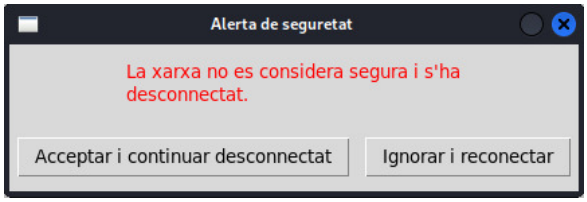

Fig. 7: Finestra d'alerta d'autodesconnexió per nivell de seguretat molt degradat

Aquesta estratègia permet avisar l'usuari tan aviat com es detecta qualsevol anomalia en els tests individuals, i en cas de risc sever, protegir-lo tallant el canal de comunicació i oferint-li la possibilitat de reconnectar-se sota la seva pròpia responsabilitat.

9.4 Interfície gràfica

Per facilitar la supervisió en temps real, s'ha desenvolupat una GUI senzilla que presenta la informació i la gravetat de cada prova de forma clara i dinàmica. La interfície s'estructura com una llista de control (*checklist*) on apareixen tots els tests disponibles (anàlisi de contrasenya, protocol, SSID, VPN, ports, WPS, desautenticació, marauding, etc.), cadascun amb un indicador visual (punt negre, icona de confirmació o de fallada) i un botó "Run" per executar-lo de manera individual.

A la part superior de la finestra es mostren en tot moment:

- L'ESSID de la xarxa actual.
- La IP del *gateway*.
- L'estat del mode monitor, amb dos botons per "Activar Monitor" i "Desactivar Monitor".
- Un botó "Iniciar Escaneig Complet" per llançar tots els tests de cop.

A mesura que s'executen els tests, els indicadors s'actualitzen automàticament i, en cas de detectar-se cap problema, es desplega un missatge de text al costat de l'ítem corresponent que descriu breument la incidència. En la part inferior, es calcula i mostra un percentatge global de seguretat que resumeix l'estat de la xarxa analitzada Figura 8)

9.5 Validació en laboratori

L'agent s'ha provat en un entorn controlat però representatiu de casos reals, utilitzant diversos equips i topologies per validar-ne la robustesa i versatilitat. Concretament:

- S'han emprat routers domèstics convencionals i xarxes *mesh* per reproduir diferents escenaris d'abast i cobertura.
- S'han clonay xarxes mitjançant dispositius mòbils (smartphones) i punts d'accés falsos, per verificar la detecció d'*Evil Twin* i suplantacions d'SSID.

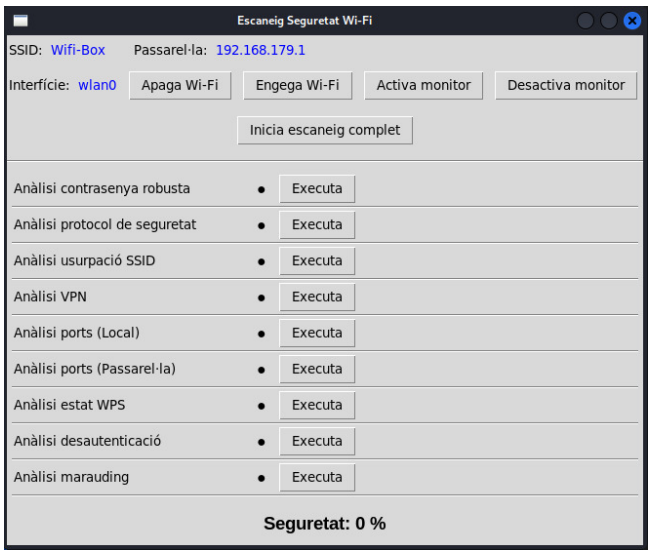

Fig. 8: Captura de la GUI amb checklist de tests, ESSID, IP del gateway i controls de mode monitor

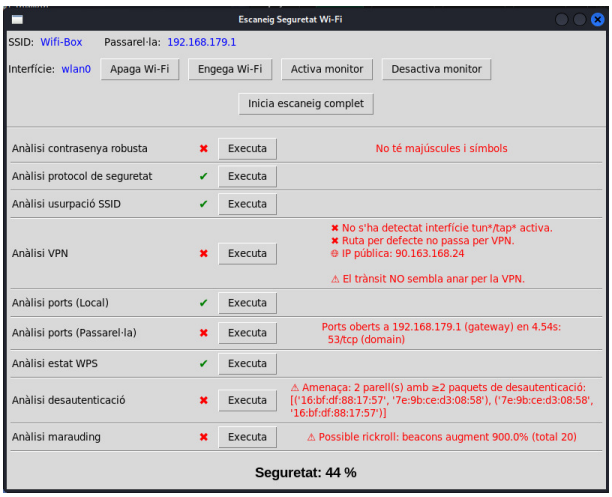

Fig. 9: Escenari de laboratori amb routers domèstics, xarxa mesh fent comprovacions en condicions normals

- S'ha accedit al panell d'administració dels routers per segmentar la LAN, provar contrasenyes diverses i modificar opcions de seguretat (WEP, WPA2, WPA3, WPS), mesurant la capacitat de l'agent per reconèixer canvis en la configuració.
- Per comprovar l'anàlisi de ports, s'han publicat serveis a la xarxa interna obrin ports sota diferents escuses (HTTP, SSH, DNS), i s'ha contrastat el comportament de l'escàner local i de gateway.
- S'han activat opcions de WPS i s'han realitzat atacs de desautenticació massiva, *marauding* i *Rickroll* emprant tant equips externs (altres ordinadors amb Scapy i aircrack-ng) com dispositius especialitzats (Flipper Zero i ESP32).

Amb aquestes proves s'ha confirmat la ràpida detecció i notificació de cada tipus d'atac, així com la correcta actuació automàtica de bloqueig de connexió quan la seguretat es degrada per sota del llindar definit. A la Figura 9 es mostra un exemple d'implantació i execució de proves en el banc de laboratori.

10 Conclusions

Aquest treball ha permès recórrer tot el cicle de desenvolupament d'una solució de seguretat enfocada a entorns de teletreball, assolint els objectius plantejats al pla inicial del TFG:

1. *Entendre el funcionament de les xarxes Wi-Fi i les possibles amenaces*. La revisió bibliogràfica i la reproducció pràctica d'atacs (KRACK, FragAttacks, suplantació d'SSID, jamming, explotació de WPS, etc.) han aportat una visió sòlida del model de vulnerabilitats de les xarxes 802.11. El coneixement adquirit ha estat clau per definir les proves i els llindars utilitzats a l'agent.
2. *Dissenyar l'arquitectura del sistema*. Tot i que no s'ha implementat íntegrament la capa de mitigació avançada (p. ex. regles `iptables`), s'ha documentat i planificat una arquitectura modular captura, anàlisi, notificació que facilita l'extensió futura i l'adaptació a altres plataformes o sensors.
3. *Desenvolupar un prototip*. El prototip resultant és plenament funcional per a la majoria de proves dissenyades, integra una GUI lleugera i opera en un entorn Kali Live USB. Hauria estat desitjable arribar a una versió més polida per exemple amb detecció contínua sense perdre la connexió però la implementació actual demostra la viabilitat de la proposta.
4. *Provar en entorn controlat*. S'han realitzat assajos exhaustius amb routers domèstics, xarxes *mesh*, dispositius mòbils i eines d'atac (ordinadors, Flipper Zero, ESP32). Aquesta fase ha resultat la més motivadora i ha confirmat la capacitat del prototip per detectar i informar ràpidament sobre incidents reals.

En síntesi, el projecte ha passat d'un coneixement inicial limitat a un sistema operatiu que evidencia la fragilitat de moltes configuracions domèstiques i la necessitat d'eines accessibles per a l'usuari final. Les limitacions detectades, principalment l'obligació de commutar la interfície entre *monitor* i *managed*, el consum energètic i alguns falsos positius en entorns densos, obren línies de treball futures, com la incorporació de xips de doble ràdio o la federació d'agents col·laboratius.

Malgrat aquests reptes, es pot afirmar que els quatre objectius fonamentals del TFG s'han complert, aportant una base sòlida per evolucionar cap a un producte més madur que reforci la ciberseguretat en escenaris de teletreball.

Agraïments

Per cloure aquest projecte, vull expressar el meu més sincer agraïment a totes les persones que m'han acompanyat i donat suport al llarg d'aquest treball de fi de grau.

En primer lloc, voldria donar les gràcies a Miguel Carpio, pel seu seguiment constant durant aquests mesos i per les seves orientacions precises que m'han ajudat a millorar cada detall de la memòria i del prototip.

En segon terme, agraeixo profundament a Minsait l'oportunitat que em va brindar d'incorporar-me al seu equip, permetent-me créixer professionalment i descobrir de primera mà les tecnologies que finalment he aplicat en aquest treball. El suport dels meus companys i responsables ha estat clau per assolir els objectius plantejats.

Finalment, vull agrair a la meva parella el seu suport incondicional, paciència i ànims constants durant tot el procés. Sense el seu recolzament, aquest projecte hauria estat molt més difícil d'engegar i culminar.

A tots, moltes gràcies.

REFERÈNCIES

[1] Spiceworks, "What is Evil Twin Attack?," [Online]. Available: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-evil-twin-attack/. [Last Access: 05-Mar-2025].

[2] Wikipedia, "Wi-Fi deauthentication attack," [Online]. Available: https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack. [Last Access: 05-Mar-2025].

[3] Knowridge, "New Wi-Fi Attack Uses Smart Surfaces to Jam Specific Devices," [Online]. Available: https://knowridge.com/2025/03/new-wi-fi-attack-uses-smart-surfaces-to-jam-specific-devices/. [Last Access: 05-Mar-2025].

[4] CloudRadius, "Wi-Fi Spoofing: A Major Threat to Network Security," [Online]. Available: https://www.cloudradius.com/wi-fi-spoofing-a-major-threat-to-network-security/. [Last Access: 05-Mar-2025].

[5] Kismet Wireless, "Kismet," [Online]. Available: https://www.kismetwireless.net/. [Last Access: 05-Mar-2025].

[6] Redeszone, "Aircrack-ng Tutorial: Hackear redes Wi-Fi," [Online]. Available: https://www.redeszone.net/tutoriales/seguridad/aircrack-ng-hackear-redes-wifi/. [Last Access: 05-Mar-2025].

[7] Brainkart, "IEEE 802.11i Wireless LAN Security," [Online]. Available: https://www.brainkart.com/article/IEEE-802-11i-Wireless-LAN-Security_8486/. [Last Access: 05-Mar-2025].

[8] Netspotapp, "What is WPA3?," [Online]. Available: https://www.netspotapp.com/es/blog/wifi-security/what-is-wpa3.html. [Last Access: 05-Mar-2025].

[9] Wikipedia, "Wireless Intrusion Prevention System," [Online]. Available: https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system. [Last Access: 05-Mar-2025].

[10] Wikipedia, "Scrum (software development)," [Online]. Available: https://en.wikipedia.org/wiki/Scrum_(software_development). [Last Access: 05-Mar-2025].

[11] eSecurityPlanet, "Secure Access for Remote Workers: VPN, RDP, and VDI Compared," [Online]. Available: https://www.esecurityplanet.com/endpoint/secure-access-for-remote-workers-rdp-vpn-vdi/. [Last Access: 10-Apr-2025].

[12] IBM, "Desktop as a Service (DaaS)," [Online]. Available: https://www.ibm.com/think/topics/desktop-as-a-service/. [Last Access: 10-Apr-2025].

[13] Mathy Vanhoef, "KRACK Attacks: Breaking WPA2," [Online]. Available: https://www.krackattacks.com/. [Last Access: 10-Apr-2025].

[14] Mathy Vanhoef, "FragAttacks: Fragmentation and aggregation attacks against Wi-Fi," [Online]. Available: https://www.fragattacks.com/. [Last Access: 10-Apr-2025].

[15] Baeldung, "Wireless Disassociation Attacks," [Online]. Available: https://www.baeldung.com/cs/wireless-disassociation-attacks. [Last Access: 10-Apr-2025].

[16] PCWorld, "The 5 most dangerous WLAN attacks," [Online]. Available: https://www.pcworld.com/article/2072976/attention-the-5-most-dangerous-wlan-attacks.html. [Last Access: 10-Apr-2025].

[17] Kaspersky, "Evil Twin Attacks," [Online]. Available: https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks. [Last Access: 10-Apr-2025].

[18] Max Planck Institute, "Wi-Fi Jamming Research," [Online]. Available: https://www.mpg.de/24247447/wifi-jamming. [Last Access: 10-Apr-2025].

[19] M. Vanhoef, "FragAttacks," [Online]. Available: https://github.com/vanhoefm/fragattacks. [Last Access: 10-Apr-2025].

[20] R. Poudel, "Detecting WiFi Deauthentication Attack using Python and Scapy," [Online]. Available: https://www.researchgate.net/publication/343472668. [Last Access: 10-Apr-2025].

[21] CISA, "WPS Vulnerable to Brute Force," [Online]. Available: https://www.cisa.gov/news-events/alerts/2012/01/06/wi-fi-protected-setup-wps-vulnerable-brute-force-attack. [Last Access: 10-Apr-2025].

[22] Samiux, "WAIDPS: Wireless Auditing IDS in Python," [Online]. Available: https://github.com/samiux/waidps. [Last Access: 10-Apr-2025].

[23] Edureka Community, "How to detect ARP spoofing using a Python script," [Online]. Available: https://www.edureka.co/community/300545/how-to-detect-arp-spoofing-using-a-python-script. [Last Access: 10-Apr-2025].

[24] J. Lin, "pyscanlogger," GitHub repository, [Online]. Available: https://github.com/John-Lin/pyscanlogger. [Last Access: 10-Apr-2025].

[25] Wyze Forums, "Waze Sense Wi-Fi / RF Jamming," [Online]. Available: https://forums.wyze.com/t/waze-sense-wi-fi-rf-jamming/282224. [Last Access: 10-Apr-2025].

[26] P. Biondi, "Scapy," [Online]. Available: https://scapy.net. [Last Access: 10-Apr-2025].

[27] K. Mladenov, "PyShark," [Online]. Available: https://github.com/KimiNewt/pyshark. [Last Access: 10-Apr-2025].

[28] Linux Wireless, "iw – nl80211 based CLI configuration utility for wireless devices," [Online]. Available: https://wireless.wiki.kernel.org/en/users/documentation/iw. [Last Access: 10-Apr-2025].

[29] NetworkManager, "nmcli – Command-line tool for controlling NetworkManager," [Online]. Available: https://developer.gnome.org/NetworkManager/stable/nmcli.html. [Last Access: 10-Apr-2025].

[30] R. Hills, "arp-scan: The ARP Scanner," [Online]. Available: https://linux.die.net/man/1/arp-scan. [Last Access: 10-Apr-2025].

[31] G. Lyon, "Nmap Network Mapper," [Online]. Available: https://nmap.org. [Last Access: 10-Apr-2025].

[32] Netfilter, "iptables – Administration tool for IPv4 packet filtering and NAT," [Online]. Available: https://netfilter.org/projects/iptables/index.html. [Last Access: 10-Apr-2025].

[33] Python Software Foundation, "tkinter — Interfaces de usuario gráficas (GUI) con Tk," Documentación oficial de Python 3.13, [Online]. Available: https://docs.python.org/es/3.13/library/tkinter.html. [Last Access: 10-Apr-2025].

[34] g0tmi1k, *Making a Kali Bootable USB Drive on Windows*, [Online]. Disponible en: https://www.kali.org/docs/usb/live-usb-install-with-windows/. [Last Access: 15-Jun-2025].

APÈNDIX

A.1 Diagrama de Gantt

A.2 Estructura de carpetes

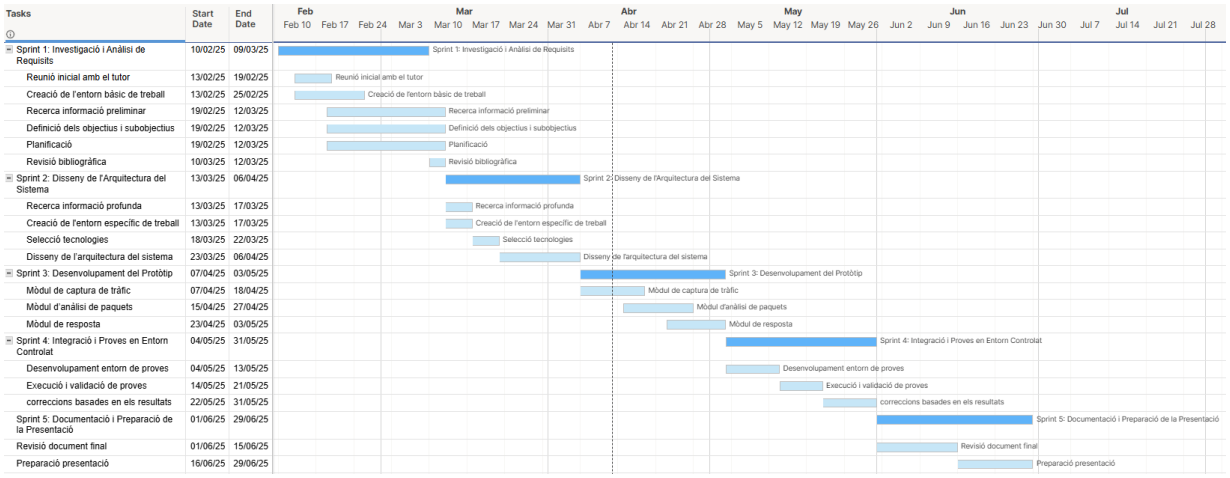

Fig. 10: Diagrama de Gantt Febre 2025 - juny 2025

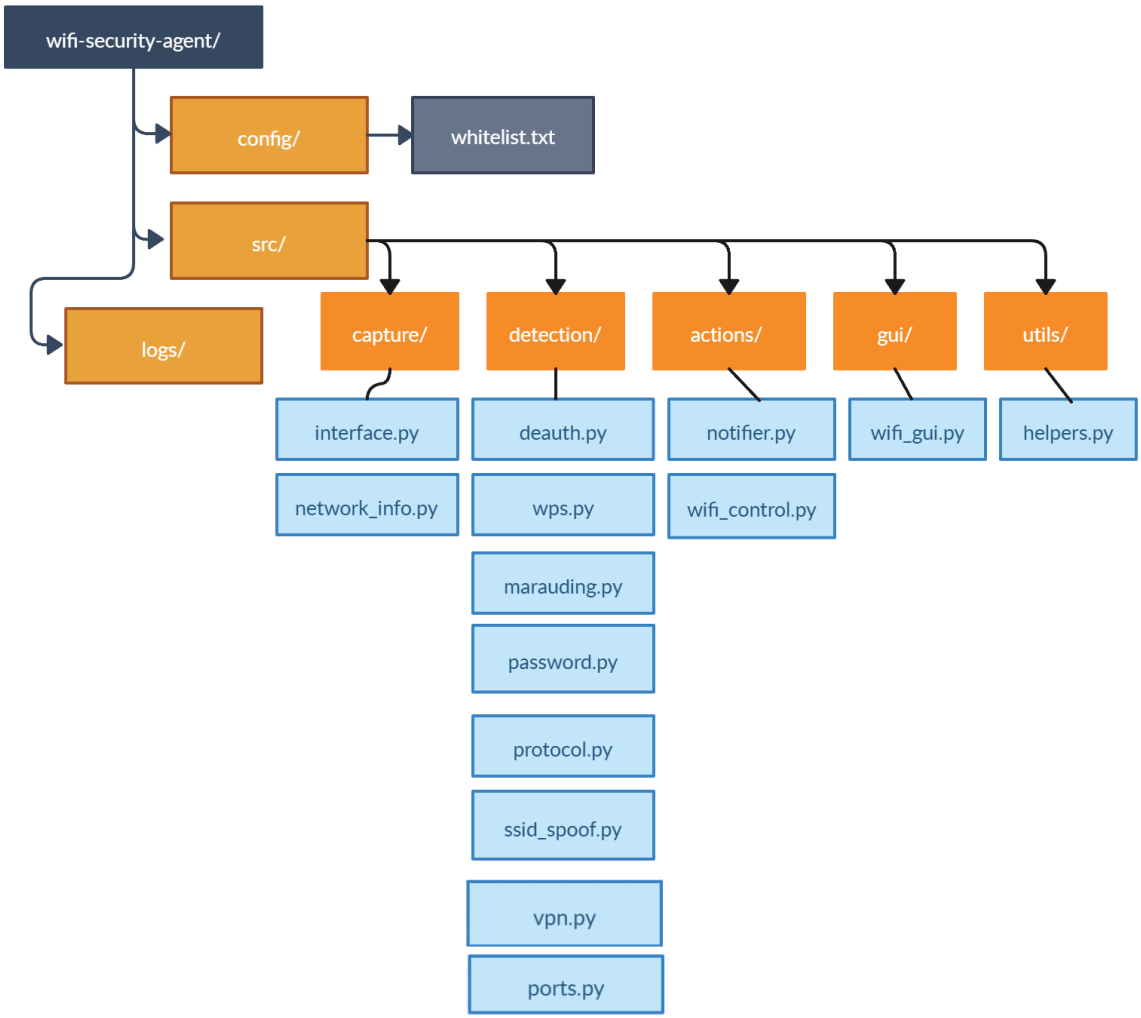

Fig. 11: Estructura de les carpetes i codi del prototip