Resoldre un CTF (Capture The Flag)

Una gamificació per aprendre pentesting i hacking ètic

David Lozano Salart

Grau d'Enginyeria Informàtica
Seguretat Informàtica

Tutor/a de TF
Gerard Farràs Ballabriga
Professor/a responsable de l'assignatura
Andreu Pere Isern Deyà

9 de gener del 2024

Universitat Oberta de Catalunya

A la meva dona Elena, a qui he robat massa temps mentre perseguia el somni de continuar formant-me i aprenent en l'infinit univers de la informàtica i la ciberseguretat.

Al meu fill Biel, que cada dia em demostra que amb treball, esforç i constància no hi ha límits insuperables i que sempre m'ha animat a no defallir ni abandonar.

Al meu amic i enginyer informàtic Cesc Gómez i López, que com sempre passa amb les grans persones, ens va deixar massa aviat.

FITXA DEL TREBALL FINAL

Títol del treball:	*Resoldre un CTF (Capture The Flag): una gamificació per aprendre pentesting i hacking ètic*
Nom de l'autor:	*David Lozano Salart*
Nom del consultor/a:	*Gerard Farràs Ballabriga*
Nom del PRA:	*Andreu Pere Isern Deyà*
Data de lliurament (mm/aaaa):	*01/2024*
Titulació o programa:	*Grau d'enginyeria informàtica*
Àrea del Treball Final:	*Seguretat informàtica*
Idioma del treball:	*Català*
Paraules clau	*CTF, gamificació, hacking ètic*

Resum del Treball

La gamificació és l'ús d'elements de joc en contextos que no estan relacionats amb el joc (Deterding et al., 2011). En aquest projecte s'ha creat un CTF (*Capture The Flag*) complet amb una història i un conjunt de reptes. El relat dona pistes i crea un fil conductor. El conjunt s'ha dissenyat perquè tot encaixi i la sensació dels jugadors esdevingui tan immersiva com sigui possible: s'han de posar a la pell de qui protagonitza la història i omplir els buits per anar fent-la avançar. Les seves accions la completen. L'objectiu final és aprendre de forma divertida.

El disseny dels reptes s'ha dut a terme amb la intenció d'oferir el nombre més gran possible de tipologies de ciberseguretat actuals (*stego, binary exploitation, pwn, reversing, forensics, crypto, web)* per tal d'aportar escenaris diferents i desenvolupar noves capacitats en la mentalitat hacker dels jugadors. Les pistes, els jocs de paraules i els enigmes s'han dosificat de forma suficient per no ser ni massa reveladors ni excessivament críptics.

L'abast d'aquest projecte és obtenir un producte formatiu de qualitat. Per cada repte s'ha afegit un *writeup (*una proposta de resolució pas a pas), que proposa tècniques i eines per resoldre'l. Addicionalment, en els annexos, s'explica amb detall com crear des de zero el laboratori de proves amb les màquines virtuals (objectiu i atacant). Així, tothom que ho desitgi en pot fer ús reduint aquestes possibles barreres d'entrada.

Això és CTF4Edu. Us atreviu a resoldre tots els seus reptes?

Abstract

Gamification is the use of game elements (e.g. points) in non-gaming contexts

(Deterding et al., 2011). In this project, a complete CTF (Capture The Flag) has been created with a story and a set of challenges. The story gives clues and creates a conductive thread. The set has been designed so that everything fits together and the feeling of the players becomes as immersive as possible: they have to put themselves in the shoes of the protagonist of the story and fill in the gaps to move it forward. Their actions complete it. The ultimate goal is to learn in a fun way.

The design of the challenges has been carried out with the intention of offering the largest possible number of current cyber security typologies (stego, binary exploitation, pwn, reversing, forensics, crypto, web) in order to provide different scenarios and develop new capabilities in the hacker mentality of players. The clues, puns and riddles have been dosed enough to be neither too revealing nor overly cryptic.

The scope of this project is to obtain a quality training product. For each challenge, a writeup (a step-by-step resolution proposal) has been added, which proposes techniques and tools to solve it. Additionally, in the appendices, it is explained in detail how to create from scratch the test lab with the virtual machines (target and attacker). Thus, everyone who wants to can use it, reducing these possible entry barriers.

This is CTF4Edu. Do you dare to solve all its challenges?

Índex

1. Introducció 1
1.1. Context i justificació del Treball 1
1.2. Objectius del Treball 2
1.3. Impacte en sostenibilitat, ètic-social i de diversitat 4
1.4. Enfocament i mètode seguit 6
1.5. Planificació del Treball 6
1.6. Breu sumari de productes obtinguts 8
1.7. Breu descripció dels altres capítols de la memòria 8
2. Estat Actual 9
2.1 Estat de l'art 9
2.2 Formació segura (i més en Ciberseguretat) 12
3. Configuració del laboratori 12
3.1 Sistema de virtualització escollit 12
3.2 Configuració de l'entorn del laboratori - 13
3.3 Màquina Objectiu: Ubuntu Server 22.04.3 LTS 13
3.4 Màquina Atacant: Kali Linux 2023.3 13
4. CTF4Edu – Una gamificació en forma de reptes 14
4.1 Això del hacking ètic i els CTF és per tothom? 14
4.2 Proposta de Reptes pel CTF4Edu 14
4.3 – Repte 1: FTP vulnerable 15
4.4 – Repte 2: Anàlisi Forense i Directoris ocults en un *site* Wordpress 21
4.5 – Repte 3: *Site* PHP i MySQL vulnerable a Injecció SQL 38
4.6 – Repte 4: Esteganografia i ocultació d'informació 44
4.7 – Repte 5: Enginyeria Inversa 50
4.8 – Repte 6: Tipus de Fitxers Obscurs, xifratge i ocultació en text massiu 55
4.9 – Repte 7: Atacs de força bruta i obtenció de credencials 59
4.10 – Repte 8: Escalada de privilegis explotant CronJobs 64
5. Conclusions i treballs futurs 69
6. Glossari 70
7. Bibliografia 71
8. Annexos 74
8.1 Instal·lació del sistema de virtualització VirtualBox 7.0.12 74
8.2 Instal·lació d'Ubuntu Server 75
8.3 Importació de Kali Linux al nostre laboratori 84
8.4 CTF4Edu – Les vulnerabilitats (la història) 87
8.5 Repte 2: URL Dinàmica pel site Wordpress 93
8.6 Repte 3: Codi Font del Site Vulnerable a Injecció SQL 94
8.7 Repte 4: Codi font de la maqueta del *site* de l'usuari david 96
8.8 Repte 5: Codi font del programa elxefendevi.cpp 97
8.9 Descàrrega de la imatge .OVA del CTF4Edu 97
8.10 Llistat de flags del CTF4Edu 97
8.11 Llistat de puntuació del CTF4Edu 97

Llista de figures

Figura 1 Les tasques a realitzar al projecte 7
Figura 2 - Diagrama de Gantt del TFG 7
Figura 3 - Tauler Kanban del projecte 8
Figura 4 - Definició hacker 9
Figura 5 Number of Common CVE 2009 – 2023 ©Statista 10
Figura 6 Instal·lació vsftd 15
Figura 7 - Configuració vsftpd.conf 15
Figura 8 - Comprovació accés FTP anònim 16
Figura 9 - Reiniciar servei FTP 16
Figura 10 - Creació carpeta .banderanegra 16
Figura 11 - Error llegint fitxer -bandera 17
Figura 12 - Codificació flag base64 17
Figura 13 - Contingut fitxer -bandera 17
Figura 14 - IP màquina atacant 18
Figura 15 - Repte 1 - Escaneig de ports amb NMAP 18
Figura 16 - Repte 1 - Ports oberts 18
Figura 17 - Connectar-se a l'FTP 19
Figura 18 - ls a FTP 19
Figura 19 - Obtenció de la pista 19
Figura 20 - Text enigmàtic 19
Figura 21 - Contingut ocult FTP 20
Figura 22 - Contingut ocult FTP (2) 20
Figura 23 - Fitxers bandera 20
Figura 24 - Contingut -bandera encriptat 20
Figura 25 - Descodificant base64 -bandera 21
Figura 26 - Procés creació PCAPNG 21
Figura 27 - Captura de paquets tshark 21
Figura 28 - Generació de la pista al PCAPNG 21
Figura 29 - Codi QR al fitxer PCAPNG 22
Figura 30 - Actualització Ubuntu Server 22
Figura 31 - Instal·lació Apache i PHP 22
Figura 32 - Creació Carpeta Seveis Web 22
Figura 33 - Permisos per www-data a /serv/www 22
Figura 34 - Descàrrega i descompressió del Wordpress 22
Figura 35 - Fitxer configuració Apache 22
Figura 36 - Contingut configuracio Site Worpress 23
Figura 37 - Habilitació Site Wordpress 23
Figura 38 - Habilitació URL Site WP 23
Figura 39 - Deshabilita el site per defecte 23
Figura 40 - Es reinicia el servei d'Apache 23
Figura 41 - Connexió a MySQL 23
Figura 42 - Creació base de dades WP 23
Figura 43 - Creació Usuari wordpress a la BdD 24
Figura 44 - Configuració permisos usuari wordpress 24
Figura 45 - Reiniciar servei MySql 24
Figura 46 - Configuració de wp-config.php 24

Figura 47 - Configuració de credencials per accés BdD 24
Figura 48 - Consulta IP màquina-objectiu 24
Figura 49 - Inici instal·lació WP - Idioma 25
Figura 50 - Dades Usuari WP Instal·lació 25
Figura 51 - WP login 26
Figura 52 - Tauler de WP 26
Figura 53 - Permisos directori /adminsecret 26
Figura 54 - Creació robots.txt 27
Figura 55 - Contingut robots.txt 27
Figura 56 - Apache permet indexació contingut directoris 27
Figura 57 - Reiniciar servei Apache 27
Figura 58 - Creacio fitxer contenidor pista per flag 27
Figura 59 - Credencials WP 27
Figura 60 - Xifratge de contenidor credencials 28
Figura 61 - Ocultació flag al tauler WP 28
Figura 62 - Descàrrega de PCAPNG 28
Figura 63 - Estructura de carpetes pel repte 29
Figura 64 - Fitxer descarregat 29
Figura 65 - Tipus de fitxer PCAPNG 29
Figura 66 - Obertura fitxer amb Wireshark 29
Figura 67 - Fitxer PCAPNG obert amb Wireshark 30
Figura 68 - Barra de filtre de Wireshark 30
Figura 69 - Filtre aplicat a Wireshark 30
Figura 70 - Wireshark amb paquets filtrats 31
Figura 71 - Missatge ocult en paquet 31
Figura 72 - Desar la pista en un fitxer de text 31
Figura 73 - Nmap escaneig verificar màquina-objectiu 32
Figura 74 - Resultats Nmap 32
Figura 75 - Nmap profund contra màquina-objectiu 32
Figura 76 - Resultats Nmap màquina-objectiu 33
Figura 77 - Pàgina WP en construcció 33
Figura 78 - Post usuari Biel al WP 34
Figura 79 - Nikto contra site WP 34
Figura 80 - Gobuster contra site WP 35
Figura 81 - Nikto troba robots.txt 35
Figura 82 - Contingut robots.txt 35
Figura 83 - Contingut /adminsecret 36
Figura 84 - Copia fitxer trobat /adminsecret 36
Figura 85 - Tipus de fitxer 36
Figura 86 - Desencriptar amb OpenSSl el fitxer 37
Figura 87 - Obtenció credencials WP 37
Figura 88 - Login WP amb credencials 37
Figura 89 - Accés al WP 37
Figura 90 - Flag Repte 2 38
Figura 91 - Configuració ports.conf Apache 38
Figura 92 - Contingut ports.conf Apache 38
Figura 93 - Creació directori Site PhP 38
Figura 94 - Canvi permisos carpeta Site 38
Figura 95 - Configuració del Site per Apache 39
Figura 96 - Contingut c3ntr3d3v4c1n4c10.conf 39

Figura 97 - Habilitació nou site PHP 39
Figura 98 - Reiniciar servei Apache 39
Figura 99 - Copia del contingut a la carpeta del Site PHP 39
Figura 100 - Connexió a MySQL 39
Figura 101 - Creació BdD site PHP 39
Figura 102 - Creació usuariweb BdD 40
Figura 103 - Permisos usuariweb BdD 40
Figura 104 - Reconnexió a MySQL com usuariweb 40
Figura 105 - Creació taula usuaris a MySQL 40
Figura 106 - Afegir usuari vàlid taula usuaris 40
Figura 107 - Comprovació funcionament Login Site PHP 40
Figura 108 - Escaneig Nmap Repte3 41
Figura 109 - Resultat Nmap Repte3 41
Figura 110 - Login Page PHP Repte3 41
Figura 111 - Pàgina error - Autenticació Fallida Repte3 42
Figura 112 - Login Site amb Payload al camp nomusuari 43
Figura 113 - Login correcte amb SQLi 43
Figura 114 - Menú contextual Veure codi font 44
Figura 115 - Codi Font Pàgina amb flag i credencials 44
Figura 116 - Preparació Flag Repte 4 44
Figura 117 - Ocultació flag dins imatge 45
Figura 118 - Ocultació pistes metadades imatge 45
Figura 119 - Pista extra Repte4 45
Figura 120 - Metadades imatge amb pistes 45
Figura 121 - Pista doble concatenada a la imatge 46
Figura 122 - Connexió a CTF4Edu per SSH 46
Figura 123 - Sessió iniciada com a david a CTF4Edu 46
Figura 124 - Contingut /home/david a CTF4Edu 46
Figura 125 - Contingut directori WWW 47
Figura 126 - Copia del directori www a màquina atacant 47
Figura 127 - Inici de Simple Servidor HTTP 47
Figura 128 - Site www en local per investigar 48
Figura 129 - Imatge de Girona descarregada 48
Figura 130 - Metadades de foto de Girona 48
Figura 131 - Cerca de qui es Steg Hide 49
Figura 132 - Steghide a la foto de Girona 49
Figura 133 - Extracció de fitxer ocult a la imatge 49
Figura 134 - Obtenció Flag Repte4 49
Figura 135 - Missatge concatenat al final imatge 50
Figura 136 - Pista pel seguent repte 50
Figura 137 - Compilació elxefendevi 50
Figura 138 - Creació estructura de carpetes a CTF4Edu 50
Figura 139 - Creació carpeta elxefendevi 50
Figura 140 - Copia del programa compilar a CTF4Edu 50
Figura 141 - Detall del directori 51
Figura 142 - Troballa de benvist.txt 51
Figura 143 - Contingut de benvist.txt 51
Figura 144 - Execució del binari elxefendevi 51
Figura 145 - Copia del binari a la màquina atacant 52
Figura 146 - Execució de Ghidra 52

Figura 147 - Execució de Ghidra - Projecte 52
Figura 148 - Com importar binari a Ghidra 52
Figura 149 - Escollir binari del directori per importar 53
Figura 150 - Configuracions de Ghidra 53
Figura 151 - Icona de l'accés a CodeBrowser Ghidra 53
Figura 152 - Diàleg analisi per primer cop binari 54
Figura 153 - Opcions d'analisi de Ghidra 54
Figura 154 - Ghidra en execució 54
Figura 155 - Detall de la cadena trobada al binari 55
Figura 156 - Execució del xefendevi amb resposta correcta 55
Figura 157 - Codificació en md5 55
Figura 158 - CyberChef en execució 56
Figura 159 - S'encapsula en un ZIP el fitxer 56
Figura 160 - Copia de fitxers al directori elfrarellati 56
Figura 161 - Vista del contingut directori elfrarellati 57
Figura 162 - Contingut fitxer recepta.txt 57
Figura 163 - Analisi del fitxer cartell.pdf 57
Figura 164 - Copia de tot el contingut a la màquina atacant 57
Figura 165 - Intent de descomprimir cartell.pdf 58
Figura 166 - Descompressio del contingut de cartell.zip 58
Figura 167 - Contingut de sistemadecodificació.txt 58
Figura 168 - La pàgina CrackStation trencant el hash md5 58
Figura 169 - Resultat de cercar "Cerebrum" a biblia.txt 59
Figura 170 - Us de CyberChef per invertir missatge ROT47 59
Figura 171 - Creació carpeta .cripta 59
Figura 172 - Fitxer credencials 60
Figura 173 - Fitxer idusuari 60
Figura 174 - Compressió amb password dels fitxers de credencials 60
Figura 175 - Compressió del fitxer comprimit amb un altre password 60
Figura 176 - Es copia a la carpeta .cripta el fitxer comprimit 60
Figura 177 - Accés al directori on hi ha .cripta 61
Figura 178 - Contingut directori .cripta 61
Figura 179 - Copia del fitxer comprimit a la màquina atacant 61
Figura 180 - Intent de descomprimir el Zip 61
Figura 181 - Descompressió del fitxer amb pista 61
Figura 182 - Descompressió fallida 62
Figura 183 - Zip2john extraien el hash del zip 62
Figura 184 - John The Ripper amb RockYou per trencar el hash 62
Figura 185 - Extracció del contingut del Zip 63
Figura 186 - Fitxer credencials 63
Figura 187 - Fitxer idusuari 63
Figura 188 - Atac de força bruta per SSH amb Hydra 64
Figura 189 - Accés a CTF4Edu com a f0sk4 64
Figura 190 - Obtenció flag repte 7 64
Figura 191 - Document simulant practica copiada 64
Figura 192 - Script per esborrar carpeta pràctiques 65
Figura 193 - Script per sistema entrega practiques 65
Figura 194 - Pista Repte 8 65
Figura 195 - Contingut directori /home/f0sk4 65
Figura 196 - Missatge perlaf0sc4.txt 66

Figura 197 - Vista de Crontab a CTF4Edu 66
Figura 198 - Script modificat per preparar escalada de privilegis 67
Figura 199 - Watch ls per observar quan apareix h4ckbash 67
Figura 200 - h4ckbash amb bit SUID activat 67
Figura 201 - Execució de h4ckbash privilegiat 68
Figura 202 - Missatge amb la flag i comiat 68
Figura 137 Pàgina principal d'Oracle VirtualBox 74
Figura 138 - Paquets d'instal·lació de VirtualBox per plataforma 74
Figura 139 Instal·lació Oracle VirtualBox 7.0.12 - Windows 74
Figura 140 Avís VirtualBox - Network Interfaces 75
Figura 141 Oracle VirtualBox Instal·lat al sistema 75
Figura 142 Descàrrega Ubuntu Server 22.04.3 LTS 76
Figura 143 Crear nova màquina virtual a VirtualBox 77
Figura 144 Assistent nova màquina virtual a VirtualBox 77
Figura 145 Verifica que el teu password sigui segur 78
Figura 146 Configuració instal·lació desatesa SO a VirtualBox 78
Figura 147 Característiques hardware de màquina virtual a VirtualBox 79
Figura 148 - Creació de disc dur virtual a VirtualBox 79
Figura 149 Pantalla resum instal·lació màquina objectiu a VirtualBox 80
Figura 150 Instal·lació iniciada del sistema operatiu màquina objectiu 80
Figura 151 Ubuntu Server - Distribució teclat 81
Figura 152 Ubuntu Server - Idioma 81
Figura 153 Ubuntu Server - Tria del Sistema base 81
Figura 154 Ubuntu Server - En funcionament 82
Figura 155 - VirtualBox - Maquina Objectiu aturada 82
Figura 156 VirtualBox - Paràmetres 82
Figura 157 VirtualBox - Configuració de xarxa 83
Figura 158 Kali Linux - Màquines Virtuals 84
Figura 159 - Kali Linux per a VirtualBox 84
Figura 160 Menú Afegeix a VirtualBox 85
Figura 161 Fitxer d'importació de Kali Linux a VirtualBox 85
Figura 162 Màquina Virtual Kali Linux importada a VirtualBox 85
Figura 163 Kali Linux funcionant 86

1. Introducció

1.1. Context i justificació del Treball

La nostra és una societat digital, on cada dia hi ha més persones, dispositius i coses connectades a internet. Segons l'últim informe d'ACCIÓ (2023) i l'Agència de Ciberseguertat de Catalunya[1], els ciberatacs el 2022 van incrementar-se de mitjana un 50% respecte al 2021 i es calcula que han derivat en un cost anual d'uns 7000 milions d'euros a tot el món. A l'informe del Check Point Institute for Information Security concreten que l'any 2022 el nombre de ciberatacs en l'àmbit global va augmentar un 38% respecte a l'any 2021, però no a tots els països ha estat per igual (un 57% als Estats Units, un 77% al Regne Unit i un 26% a Singapur). Així mateix, ens informa que s'ha percebut que els grups de ciberdelinqüents que els duen a terme són més petits, més àgils i sobretot intenten explotar el fet que després de la pandèmia de la COVID-19, les institucions educatives com escoles, instituts i sobretot universitats van fer una aposta clara per les eines d'e-learning. (CPIIS 2023)

Aquests ciberdelinqüents o hackers pretenen vulnerar les mesures de seguretat i accedir als sistemes i a les dades per obtenir un benefici econòmic. Ara bé, no tots els hackers persegueixen els mateixos objectius. És oportú esmentar que existeixen els hackers ètics, *pentesters* o *white hat hackers*. Un hacker ètic és una persona que disposa de moltes habilitats i experteses en l'àmbit de la informàtica i de les comunicacions i que les usa per mirar de detectar i solucionar els problemes de seguretat que es troben en sistemes, serveis, programes, plataformes o eines digitals. (Wylie i Crawley, 2021)

Quan un hacker ètic pretén estudiar els sistemes d'una empresa o institució recercant-ne vulnerabilitats i errors per a protegir-la fent atacs controlats i diverses proves de penetració, diem que està fent *pentesting* i, per tant, exerceix de *pentester.* El *pentesting* són, doncs, les diferents proves de penetració als sistemes que acostumen a seguir unes fases ben determinades: enumeració i recol·lecció de dades, escaneig i anàlisis de vulnerabilitats, accés i explotació de les vulnerabilitats detectades, informar dels resultats de les proves (indicant si són més o menys crítiques) i de com solucionar les vulnerabilitats. (Wylie i Crawley, 2021)

Resumint, els hackers que fan *pentesting* per ajudar a protegir a les empreses diem que fan *hacking ètic.* Ara bé, es pot observar que hi ha dues realitats relacionades per a intentar protegir un sistema informàtic mitjançant el hacking ètic: la primera és actuar com ho faria un ciberdelinqüent que vol intentar penetrar-hi intentant trobar qualsevol vulnerabilitat; la segona és aprofitar el coneixement obtingut d'un *pentesting* per a pal·liar, mitigar o corregir els errors i vulnerabilitats per a protegir els nostres sistemes.

[1] Agència de Ciberseguretat de Catalunya: https://ciberseguretat.gencat.cat/ca/inici/index.html

Els hackers que volen detectar si és possible penetrar en un sistema i troben com fer-ho són els que s'anomenen el *Red Team*. Els que monitoren els sistemes, corregeixen els errors, mitiguen les vulnerabilitats i dissenyen la defensa dels sistemes davant dels possibles atacs són el *Blue Team*. Si barregem el vermell i el blau, tenim el *Purple Team*: grup de persones que faciliten la comunicació i el traspàs d'informació entre els membres del Red Team i del Blue Team. (Wylie i Crawley, 2021)

Avui dia als equips dels serveis informàtics de la majoria d'universitats catalanes i espanyoles (també de les empreses en general) no hi ha encara massa perfils professionals d'experts en hacking ètic, pentesting i ciberseguretat (INCIBE 2023). Així doncs, qui ha de dur a terme l'anàlisi de possibles vulnerabilitats dels sistemes informàtics i de les comunicacions acostumen a ser persones amb escassa formació en aquestes habilitats. I aquestes persones necessiten formar-se i practicar.

Addicionalment, hi ha assignatures del pla d'estudis del grau d'Enginyeria informàtica com Seguretat en Xarxes de Computadors (per esmentar-ne una) que potser podrien incorporar pràctiques similars a les proposades en aquest projecte. I potser algun dia poden aparèixer assignatures optatives específiques en ciberseguretat i hacking ètic que també n'utilitzin de similars.

El clàssic joc infantil atrapa la bandera en anglès s'anomena *capture the flag.* Al joc, dos equips, cadascú amb la seva bandera (*flag)*, han de protegir-la per evitar que els de l'equip rival els la prenguin; alhora, han d'intentar prendre la del rival sense ser atrapats. Un CTF (*Capture The Flag*) en l'àmbit de la ciberseguretat és un repte, un exercici, una gamificació on aquestes *flags* es troben amagades en entorns vulnerables creats expressament per activitats competitives o formatives. Les *flags* acostumen a ser textos, cadenes de caràcters, o nombres i serveixen per acreditar que els participants han adquirit l'habilitat necessària per a superar la vulnerabilitat plantejada als reptes.

Pel que fa a la motivació personal, sempre m'ha interessat la ciberseguretat, el pentesting i el hacking ètic, i per això vaig sol·licitar poder desenvolupar aquest TFG en l'àmbit de la seguretat informàtica. Vull aprendre pentesting, i augmentar els meus coneixements de seguretat informàtica per poder créixer professionalment en aquest àmbit. En un futur m'agradaria poder cursar un màster en ciberseguretat. Em sembla oportú afegir que sempre m'ha interessat molt la formació i compartir el coneixement. La idea de crear un CTF per ajudar altres persones a introduir-se en aquest camp i que puguin aprendre conceptes i tècniques de seguretat informàtica em semblava una cosa necessària: necessitem el màxim de gent per a fer front a les amenaces del món digital on vivim i viurem.

1.2. Objectius del Treball

L'objectiu general d'aquest treball és crear una gamificació formativa per aprendre pentesting i hacking ètic des de la visió del Red Team.

El CTF plantejat s'ha de poder resoldre de forma individual, progressiva, amb caràcter formatiu i enfocat a diferents col·lectius encara que no disposin de moltes habilitats en

el món de la ciberseguretat. Per això, s'escull crear un repte tipus Jeopardy[2] amb diferent nivell de dificultat.

La màquina-objectiu ha de ser una màquina virtual Linux amb un sistema operatiu actualitzat al màxim en el moment des de l'inici d'aquest projecte.

L'explotació de les vulnerabilitats trobades al CTF ha de permetre accedir als sistemes o a certes parts dels mateixos per obtenir unes dades amagades o protegides (les *flags* o banderes).

L'obtenció de les banderes ha de tenir diferent nivell de dificultat.

El conjunt de reptes ha d'incloure el màxim nombre de tipologies de ciberseguretat actuals, com les següents:

- ***Stego*** *(*Esteganografia): revelar informació oculta en altres fitxers, com ara imatges, vídeos, àudios, etc.
- ***Binary Exploitation***: Explotació de binaris per aconseguir altres finalitats, com una *shell*.
    - **Pwn**: Trobar vulnerabilitats en un binari o programa en un equip informàtic (normalment remot) per aconseguir controlar-lo mitjançant una escalada de privilegis.
- ***Reversing***: Enginyeria inversa per obtenir el codi font d'un programa compilat per analitzar-lo.
- ***Forensics*** *(Anàlisi forense)*: examinar i trobar petites parts d'informació ocultes en altres fitxers, bolcats de memòria, imatges de disc durs o paquets capturats en comunicacions.
- ***Crypto*** (Criptografia): explotar alguna feblesa en els algoritmes criptogràfics o en la seva implementació.
- ***Web***: explotar alguna vulnerabilitat de la tecnologia web emprada o en la seva seguretat per assolir altres propòsits.

La part pràctica del treball es resoldrà usant tècniques de pentesting contra la màquina-objectiu per aconseguir revelar les flags i així anar assolint el reptes.

El sistema atacant es proposa que sigui un sistema operatiu dedicat i especialitzat en tasques de pentesting i actualitzat a la seva darrera versió en el moment de dur a terme aquest projecte.

La resolució dels reptes de la part pràctica, es basarà en les 7 fases estàndard[3] d'un *pentesting* (Wylie i Crawley, 2021):

---

[2] El terme manlleva el nom del popular concurs televisiu nord-americà anomenat "Jeopardy!" on els participants competeixen en diverses categories i resolen problemes per guanyar punts. Fonts: Capture the Flag | Wikipedia (s.d.) consultat per darrera vegada el 15 d'octubre de 2023 a https://en.wikipedia.org/wiki/Capture_the_flag_(cybersecurity)
Jeopardy! | Wikipedia (s.d.) consultat per darrera vegada el 15 d'octubre de 2023 a https://en.wikipedia.org/wiki/Jeopardy!

1. Interacció prèvia
2. Recopilació d'informació
3. Modelatge d'amenaces
4. Anàlisi de vulnerabilitats
5. Explotació
6. Post-explotació
7. Informe (*writeup)*

Durant la resolució dels reptes, però, no tothom els sabrà resoldre. Per això els writeups tenen una clara voluntat formativa: es pretén que qui llegeixi i segueixi els passos de resolució de cada repte vagi formant aquesta mentalitat de *pentester* i vagi adquirint un ordre i unes habilitats per a resoldre els problemes.

Com que es proposa una gamificació, es planteja els reptes dins d'un context literari que els uneixi, una història que els doni sentit i faci més atractiva, lúdica i immersiva la participació dels usuaris o l'alumnat que la utilitzin.

Tot i que hi ha diferents plataformes per aprendre ciberseguretat i hacking ètic és evident que podem trobar-ne que explotin les mateixes vulnerabilitats o que tractin reptes semblants. Ara bé, la majoria estan segmentades, és a dir, tracten les vulnerabilitats per separat: hi ha reptes d'una temàtica i d'una altra, i d'una tercera, però molt poques que tots els reptes estiguin a la mateixa màquina, amb un mateix fil conductor, d'inici a fi. Per tant, es vol aportar una combinació de reptes que sumats a un relat original, permeti convertir el resultat final en genuí.

Es vol crear una gamificació amb una voluntat formativa i alhora divertida per a fer atractiu tot el procés d'adquisició de noves habilitats en pentesting i hacking ètic, i en definitiva, en ciberseguretat.

Com a darrer objectiu, es vol destacar que tant la història, com els jocs de paraules, les pistes, els enigmes i les ocurrències per acompanyar els reptes s'han pensat en català, i s'han ofert en aquesta llengua. Lamentablement, avui dia encara no és habitual trobar contingut formatiu d'aquesta temàtica en català, punt que també li ofereix aquest caire genuí.

1.3. Impacte en sostenibilitat, ètic-social i de diversitat

Sostenibilitat

Aquest projecte té la voluntat de desenvolupar unes habilitats formatives i educatives de qualitat mitjançant la gamificació d'un CTF. Com a producte final, s'obtindrà una màquina-objectiu, que es podrà usar per a intentar accedir-hi resolent els reptes del CTF i en aquest camí, permetre l'aprenentatge de tècniques, eines i metodologies aplicades de hacking ètic i *pentesting*. En conseqüència, requerirà com a mínim un

[3] The Penetration Testing Execution Standard v2.0 – (29/08/2023) consultat per darrera vegada el 15 d'octubre de 2023 a https://pentest-standard.com/

dispositiu electrònic que funciona amb energia elèctrica. Això no obstant, s'escollirà una configuració dels sistemes operatius de l'entorn virtual que comportin que els requisits de l'equip host on virtualment tindrem la nostra màquina atacant i la màquina-objectiu siguin els mínims, permetent l'esmentada formació amb un consum el més contingut possible d'energia i, alhora, permeten que dispositius amb menys recursos també puguin utilitzar aquest laboratori virtual, no afavorint sense necessitat el consumisme de dispositius d'última generació o la generació de residus provinents de l'eliminació dels equips obsolets.

Des del punt de vista dels ODS[4] (Objectius de Desenvolupament Sostenible) podem dir que es tindrà en compte:

- ***Goal 12: Responsible Consumption and Production***: No fomentar el malbaratament de dispositius, creant més residus i fomentant el consum no necessari d'aquests.

Comportament ètic i responsabilitat social

Des del punt de vista ètic, aquest projecte pretén crear un entorn formatiu per al desenvolupament de competències en el marc de la ciberseguretat per a qualsevol persona que hi estigui interessada. Així mateix, pretén fer pedagogia de la importància de l'enfocament ètic de les tècniques apreses i com utilitzar-les només en sistemes on s'ha obtingut el permís per a fer-ho i amb l'única finalitat de permetre disposar de més seguretat per als propietaris i els usuaris dels serveis que s'hi processen (sigui d'institucions públiques o empreses privades). Ara bé, com qualsevol altre coneixement, hi ha qui el pot usar per a fins espuris o en benefici propi, i no tenint en compte ni els drets ni els béns dels altres. Això no obstant, aquest aspecte és inherent a qualsevol font d'informació i en tot cas és responsabilitat de qui, tot i conèixer els marcs ètics i legals, en fa cas omís.

Per tot el que anteriorment s'ha exposat els objectius als quals aquest projecte es pot adherir són:

- **Goal 4: Quality Education**
- **Goal 9: Industry, Innovation, and Infrastructure**

Diversitat i drets humans

Aquest projecte no comporta de forma inherent cap desigualtat de gènere ni discrimina de cap forma per qüestió d'edat, ideologia, raça, religió ni per cap altra raó: és un objectiu d'aquest projecte que qualsevol persona interessada a formar-se en hacking ètic i pentesting pugui trobar útil el resultat final del d'aquest.

[4] Sustainable Development Goals | United Nations (s.d.) consultat per darrera vegade el 16 de noviembre del 2023 a https://www.un.org/sustainabledevelopment/sustainable-development-goals/

Addicionalment, en el redactat d'aquest TFG, s'ha utilitzat un llenguatge inclusiu i que no faci sentir exclosa a cap persona (per exemple en lloc de parlar dels alumnes i les alumnes es parla de l'alumnat). En cas d'aparèixer alguna excepció, com ara a la història que dona un sentit i cohesió als reptes, és per qüestions de guió i un pur recurs literari.

En conseqüència, i segons els ODS, els objectius on aquest TFG tindrà un impacte positiu són:

- **Goal 5: Gender Equality**
- **Goal 10: Reduced Inequalities**

1.4. Enfocament i mètode seguit

Principalment, el projecte té un enfocament pràctic: adquirir i posteriorment aplicar coneixements de pentesting per dissenyar un conjunt de vulnerabilitats en una màquina-objectiu per tot seguit, aplicant les tècniques adequades, explotar les vulnerabilitats, aconseguir la informació i acabar escalant privilegis.

En el cas dels reptes d'aquest projecte, però, a l'hora de resoldre'ls, els 7 punts estàndard es reduiran als 4 següents:

1. **Enumeration** (Enumeració) de serveis, ports, i recollida de dades de cada situació o equip.
2. **Analitzar les possibles vulnerabilitats** per aprofitar-les
3. **Explotar les vulnerabilitats** detectades (una o més d'una) fins a aconseguir l'objectiu (flag)
4. **Post-explotació**: recollir informació i avançar cap al següent repte.

Després de cada repte assolit caldrà recapitular les accions que s'han dut a terme, com s'han executat, per quin ordre i amb quina finalitat de tal manera que quedi documentada una possible solució al repte plantejat (*writeup*).

1.5. Planificació del Treball

La planificació del projecte s'ha basat en 2 aspectes principals: Les entrega de les PAC, seqüencials i progressives marquen una planificació tipus *waterfall* (en cascada), amb data d'inici i fi marcada per la mateixa temporalitat de l'assignatura; per a la part pràctica dels reptes, usaré un enfocament *agile* (àgil), amb *sprints*, pel fet que necessitaré aprendre com resoldre cadascun dels mateixos reptes dissenyats, intentar resoldre'l amb l'objectiu d'acabar obtenint la bandera per descriure-ho en el *writeup*, però sempre amb coherència amb la seqüència i el relat de la història. Per aquest punt, s'ha utilitzat la versió gratuïta de Trello per a fer un tauler Kanban.

Les tasques a realitzar, vista detallada:

Name	Duration	Start	Finish
TFG - Resoldre un CTF (Capture The Flag): una gamificació per aprendre pentesting i hacking ètic	88 days?	**27/09/23 08:00**	**26/01/24 17:00**
Gamificació: Redacció del relat que donarà sentit genuí als reptes del CTF	75 days?	27/09/23 08:00	09/01/24 17:00
PAC1 - Proposta i Pla de Treball	9 days?	**27/09/23 08:00**	**09/10/23 17:00**
Proposta, Estat de l'Art, documentació, motivacions...	7 days?	27/09/23 08:00	05/10/23 17:00
Pla de Treball i Planificació	1 day?	06/10/23 08:00	06/10/23 17:00
Entrega PAC1	1 day?	09/10/23 08:00	09/10/23 17:00
PAC 2 - Seguiment del Treball	21 days?	**10/10/23 08:00**	**07/11/23 17:00**
Instal·lació VirtualBox	1 day?	10/10/23 08:00	10/10/23 17:00
Instal·lació VM Kali Linux v.2023.3	1 day?	11/10/23 08:00	11/10/23 17:00
Instal·lació VM Ubuntu	1 day?	12/10/23 08:00	12/10/23 17:00
Definició dels 5 reptes del CTF	21 days?	10/10/23 08:00	07/11/23 17:00
Revisió Proposta i Pla de Treball (PAC1)	21 days?	10/10/23 08:00	07/11/23 17:00
REPTE 1	6 days?	17/10/23 08:00	24/10/23 17:00
REPTE 2	10 days?	25/10/23 08:00	07/11/23 17:00
Entrega PAC 2	0 days?	07/11/23 08:00	07/11/23 08:00
PAC 3 - Seguiment del Treball	18 days?	**08/11/23 08:00**	**01/12/23 17:00**
Revisió Reptes 1, 2 i ampliació borrador memòria final	3 days?	08/11/23 08:00	10/11/23 17:00
REPTE 3	6 days?	13/11/23 08:00	20/11/23 17:00
REPTE 4	9 days?	21/11/23 08:00	01/12/23 17:00
Entrega PAC 3	1 day?	01/12/23 08:00	01/12/23 17:00
PAC 4 - Memòria Final	27 days?	**04/12/23 08:00**	**09/01/24 17:00**
Revisió Reptes 3, 4 i ampliació memòria final	4 days?	04/12/23 08:00	07/12/23 17:00
REPTE 5	7 days?	08/12/23 08:00	18/12/23 17:00
Revisió Memòria Final d'acord als criteris de rigor, presentació i defensa de TFG	16 days?	19/12/23 08:00	09/01/24 17:00
Entrega PAC 4	1 day?	09/01/24 08:00	09/01/24 17:00
PAC 5 - Presentació del TFG en vídeo	4 days?	**10/01/24 08:00**	**15/01/24 17:00**
Preparació presentació	1 day?	10/01/24 08:00	10/01/24 17:00
Enregistrament de video	3 days?	11/01/24 08:00	15/01/24 17:00
Entrega PAC 5	1 day?	15/01/24 08:00	15/01/24 17:00
PAC 6 - Defensa asíncrona del TFG	5 days?	22/01/24 08:00	26/01/24 17:00

Figura 1 Les tasques a realitzar al projecte

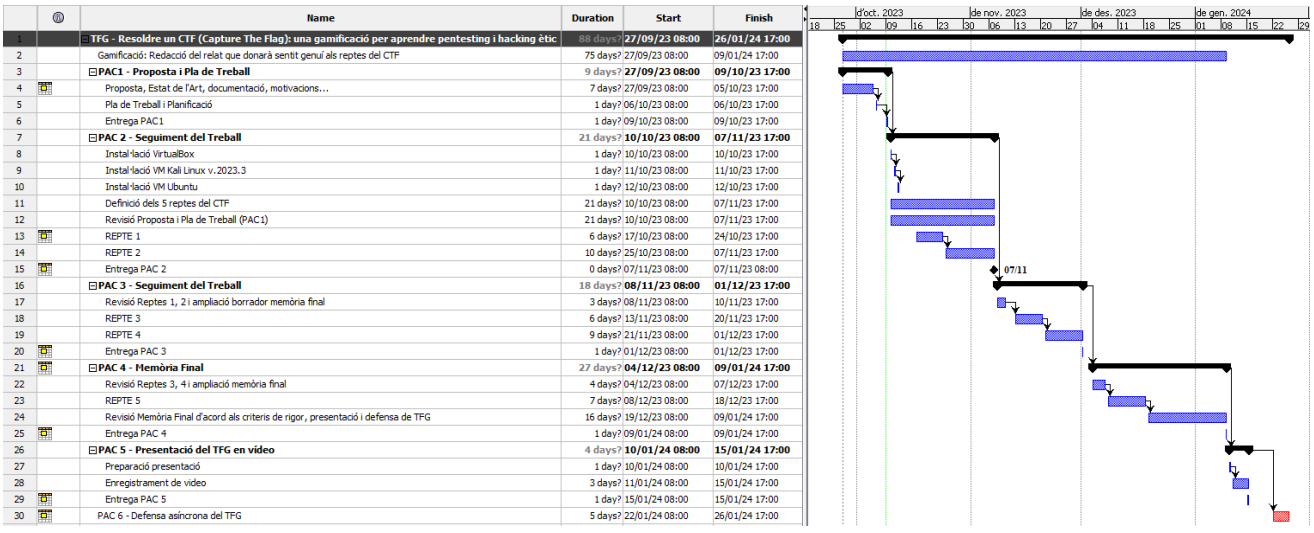


Figura 2 - Diagrama de Gantt del TFG

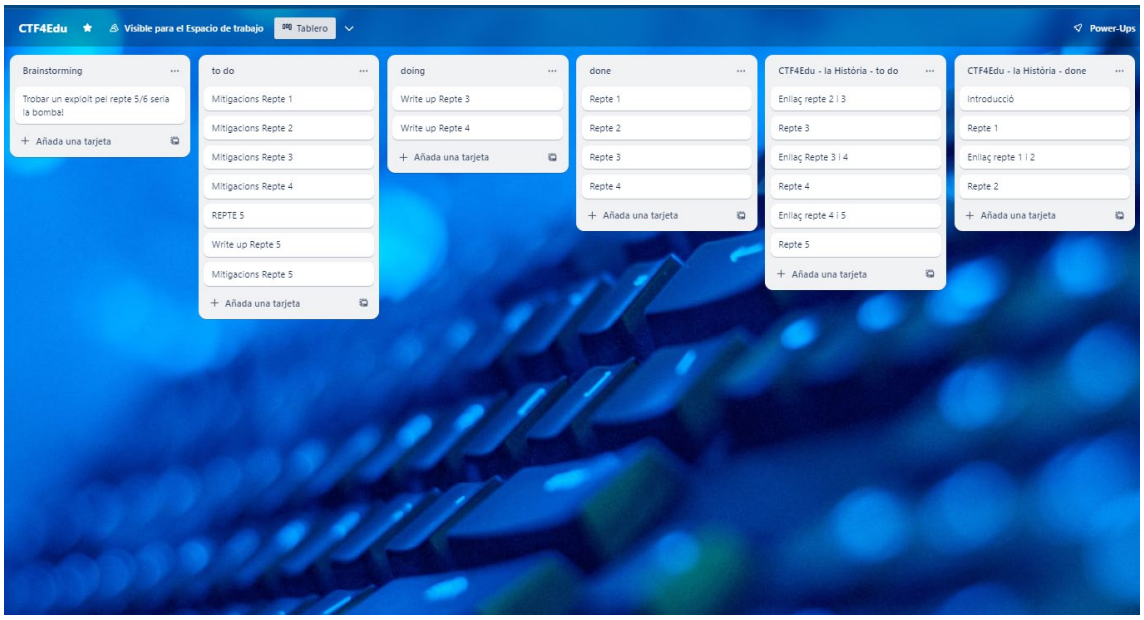


Figura 3 - Tauler Kanban del projecte

Durant els prop de noranta dies que dura tot aquest projecte, hi ha unes etapes molt clarament diferenciades:

1. Preparació del laboratori
2. Definició dels reptes del projecte i crear la història
3. Dur a terme els *pentesting* dels reptes, els writeups i obtenir les banderes
4. Completar la memòria final
5. Enregistrar la presentació del projecte
6. Defensar el projecte

1.6. Breu sumari de productes obtinguts

1. Màquina-objectiu en format .OVA [CTF4Edu]
2. Història “Les Vulnerabilitats” (Context, pistes i narrativa dels reptes)
3. *WriteUp* dels 8 reptes
4. Llistat de les flags de cada repte (per correcció / validació)
5. Llistat de puntuació de cada repte

1.7. Breu descripció dels altres capítols de la memòria

- **Capítol 2: Estat Actual**, on s’exposa el context de què són els hackers actualment, les creixents amenaces en forma de vulnerabilitats i els tipus de reptes CTF que existeixen, tant públics com privats, gratuïts i de pagament, també fent esment a diferents plataformes per aprendre i practicar habilitats en pentesting i hacking ètic.
- **Capítol 3: Configuració del laboratori**, on es detalla el sistema de virtualització i les decisions preses pel que fa als sistemes operatius de la màquina-objectiu i l’atacant.

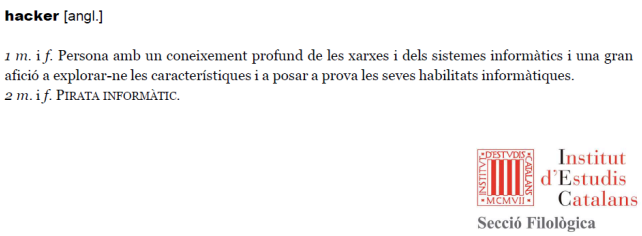
- **Capítol 4: CTF4Edu – Una gamificació en forma de repte**, on es detallen les configuracions necessàries a la màquina-objectiu per a preparar cadascun dels reptes i de forma adjunta a cadascun, el *writeup* d'aquests.
- **Capítol 5: Conclusions i treballs futurs**, on es revisa el projecte i l'acompliment dels objectius un cop finalitzat i s'infereixen possibles tasques futures com a millores per implementar en futurs projectes.
- **Capítol 6: Glossari**, on apareixen definits els termes específics del llenguatge tècnic utilitzat en el marc d'aquest projecte.
- **Capítol 7: Bibliografia**, on es detallen les fonts d'informació consultades per la realització d'aquest projecte.
- **Capítol 8: Annexos**, on es recull tota la documentació addicional que no sigui necessari incloure-la directament projecte o bé sigui massa extensa per incloure-la directament dins de un altre apartat del mateix (com la història).

2. Estat Actual

2.1 Estat de l'art

Fins no fa gaire temps, un hacker o el *hacking* només eren sinònims de ciberdelinqüent, pirata informàtic que comet actes il·legals. Malauradament, avui dia encara cal fer molta pedagogia al respecte i molta part de la nostra societat encara usa els termes de forma indistinta. No és gens estrany escoltar, llegir o visualitzar notícies on els professionals del periodisme només fan servir el terme hacker indistintament de pirata informàtic o ciberdelinqüent. En conseqüència, per la població general, els hackers només són *black hat hackers*, els *Anonymous*[5], els que roben les dades sanitàries dels hospitals (Arqué 2023) o segresten les dades de les universitats exigint-ne un rescat (Abelló 2023).

Afortunadament, hi ha avenços i un dels més recents l'ha proporcionat l'Institut d'Estudis Catalans[6] al seu DIEC[7] (*Diccionari de la llengua catalana*). El 27 de novembre de 2023, durant la realització d'aquest projecte, la Secció Filològica de l'Institut va fer la presentació de les novetats que s'incorporen al diccionari i una de les entrades noves és, precisament, el mot *hacker*. Concretament, el defineixen així:


hacker [angl.]

1 m. i *f.* Persona amb un coneixement profund de les xarxes i dels sistemes informàtics i una gran afició a explorar-ne les característiques i a posar a prova les seves habilitats informàtiques.
2 m. i *f.* PIRATA INFORMÀTIC.

Institut d'Estudis Catalans
Secció Filològica

Figura 4 - Definició hacker

[5] Grup activista que duu a terme ciberatacs i altres accions contra governs i institucions governamentals, entre d'altres. https://en.wikipedia.org/wiki/Anonymous_(hacker_group)
[6] Institut d'Estudis Catalans https://www.iec.cat/
[7] Diccionari de la llengua catalana https://dlc.iec.cat/

Tot i que per poder entendre els usos passats es continua definint també com a pirata informàtic, la primera entrada ja no és aquesta sinó la que es correspon a l'enfoc del terme que s'intenta divulgar en aquest projecte: el hacking ètic.

Les vulnerabilitats són febleses d'un sistema que permeten a un hacker atacar-lo i, per tant, que en comprometen la seguretat i la de les dades que pugui contenir.

El nombre de CVE[8]'s de Mitre[9] no para de créixer en els darrers anys, sobretot des de 2017 fins a dia d'avui. Per exemplificar-ho, es pot observar una imatge del nombre de vulnerabilitats i exposicions de seguretat informàtica comunes a escala mundial des del 2009 fins a l'abril de 2023[10]

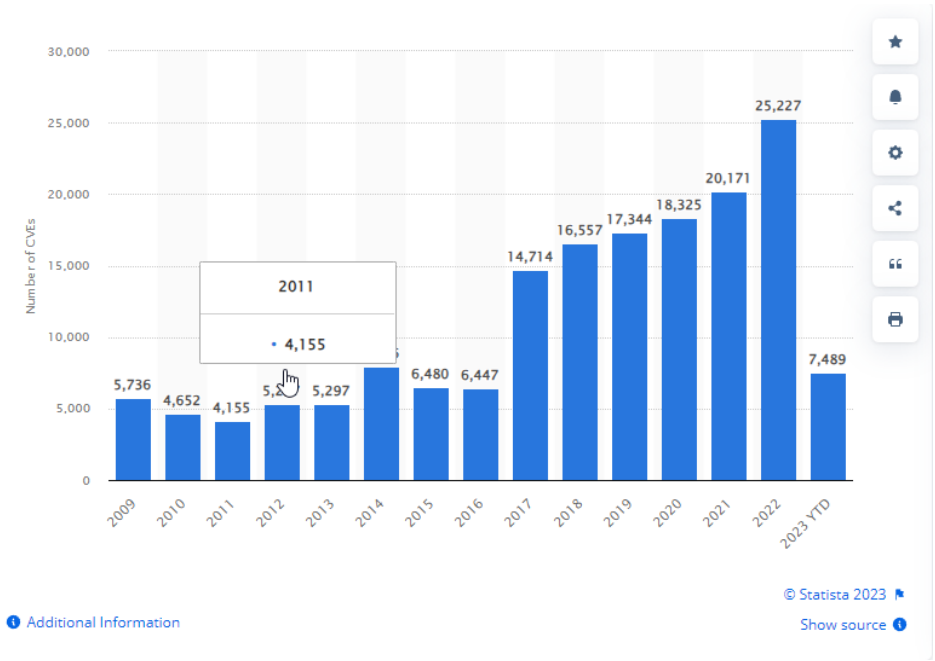


Figura 5 Number of Common CVE 2009 – 2023 ©Statista

Això significa que calen tots els esforços per a formar professionals experts en hacking ètic per contrarestar aquestes amenaces creixents. Ara bé, formar aquest tipus de professionals no és una tasca ni senzilla ni curta en el temps. De tota manera, cal dotar-nos de mecanismes per a fer-ho possible i la divulgació del coneixement i la formació són aspectes clau per l'èxit d'aquesta empresa.

Dins de la disciplina complexa d'adquisició de coneixements sobre temes de ciberseguretat i amb la finalitat també de poder protegir millor els sistemes van aparèixer les competicions CTF[11]: qui vagi guanyant més banderes va obtenint més punts per a guanyar la competició.

[8] CVE: Common Vulnerabilities and Exposures https://cve.mitre.org/
[9] Mitre: Mitre Corporation. Organització sense ànim de lucre dels Estats Units.
[10] Revista Statista: https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/
[11] CTF Wiki EN: https://ctf-wiki.mahaloz.re/introduction/history/

Actualment, hi ha moltes competicions de CTF (el concepte CTF va sorgir l'any 1996 en la DEFCON 4), sigui individual o per equips, on a la vegada es competeix per anar resolent reptes i guanyar punts. Una de les més conegudes en l'àmbit internacional és la DEFCON[12], que és un esdeveniment o una convenció de la comunitat hacker que es duu a terme anualment a Las Vegas (Estats Units d'Amèrica).

A 2023, hi ha 3 tipus de competicions CTF en l'àmbit mundial, tot i que com tot en el sector de les TIC i la ciberseguretat, és altament possible que en un futur això ja no sigui així i n'apareguin més.

El primer tipus és el *Jeopardy CTF* i es caracteritza per respondre preguntes i resoldre reptes en un temps determinat i això és el que va fent sumar punts. Acostumen a ser esdeveniments oberts al públic en general.

El segon tipus és l'anomenat *Attack & Defense CTF* i aquí uns participants fan el rol de Red Team i uns altres de Blue Team, a la vegada i en el mateix entorn. És una batalla de forces, on òbviament només pot guanyar un dels equips, i és qui pot prendre el control de l'equip o bé qui el pot protegir perquè això no succeeixi.

Hi ha un tercer tipus, un híbrid entre els dos tipus anteriors, que s'anomena *Mixed CTF* i que inclou una barreja de reptes, preguntes i confrontació per intentar prendre el control o defensar de l'equip rival.

Cal esmentar que, òbviament, hi ha molts esdeveniments privats, ja sigui d'organitzacions, universitats, instituts de recerca, etc. Tot ells promouen i preparen esdeveniments amb les seves pròpies regles i normes.

Avui dia, afortunadament hi ha moltes plataformes en línia que permeten usar aquest tipus de gamificació per millorar les habilitats i coneixements en ciberseguretat.

Si es vol participar en esdeveniments tipus Jeopardy, es pot accedir a:

- Over The Wire
- PicoCTF
- TryHackMe
- Hack the Box
- Hack a Sat
- CTF 101
- SANS Holiday Hack
- SANS Bootup CTF
- Microcorruption
- DEFCON Quals
- VulnHub

Si es vol participar en esdeveniments tipus "Attack and Defense", es pot accedir a:

- DEFCON Finals

[12] DEFCON CTF: https://defcon.org/html/links/dc-ctf.html

- SANS Cyber Ranges

Si es vol participar en esdeveniments “Mixed”, es pot accedir a:

- UCSB iCTF

Existeixen també alguns esdeveniments coneguts, però malauradament restringits al públic general (calen certes condicions per poder-hi accedir, depèn de cada cas):

- CTFd
- Hack the Box
- SANS
- CyberTalents
- Lockheed Martin CyberQuest
- Cyberskyline

2.2 Formació segura (i més en Ciberseguretat)

Quan es vol formar resolent reptes tipus CTF moltes vegades es requereix la descàrrega de màquines-objectiu o fitxers, documents, binaris, imatges, etc. L’objectiu és examinar-los i poder investigar, trobar pistes, *flags*, aplicar-los enginyeria inversa, o moltes altres accions. De la mateixa manera, alguns exploits poden fer inestables els sistemes on s’executen, i testejar-los en un entorn de laboratori, és una bona manera de verificar-ne la seguretat. (Wylie i Crawley, 2021).

Com a mesura de seguretat és altament recomanable separar i aïllar les activitats formatives CTF del nostre equip habitual (on hi ha les nostres dades personals).

Per aquest motiu, el millor per endinsar-se en el món dels CTF i de la ciberseguretat en general és utilitzar un laboratori (en la majoria dels casos, un entorn virtual). Així, la màquina virtual s’executa de tal manera que et permet aïllar-te del teu equip i entorn i, per tant, poder aprendre d’una manera més segura, i sense por a perdre el control del teu sistema ni patir efectes no desitjats. En cas de necessitat, el que li pugui passar al teu entorn de laboratori, es pot restaurar amb força facilitat i hauries de minimitzar la possible afectació cap al teu equip de treball personal.

3. Configuració del laboratori

3.1 Sistema de virtualització escollit

Per a instal·lar i configurar la màquina-objectiu es pot escollir entre diverses opcions de productes de virtualització, com ara VMWare[13], Oracle VirtualBox[14], etc.

Com que l’objectiu d’aquest projecte és obtenir un entorn d’aprenentatge el màxim accessible per tothom i amb el mínim cost, s’ha optat per escollir Oracle VirtualBox, ja que ofereix entorns de virtualització multiplataforma i amb totes les característiques

[13] VMWare https://www.vmware.com/
[14] VirtualBox https://www.virtualbox.org/wiki/VirtualBox

completes (VMWare té limitacions en certes versions per a macOS o bé cal pagar per la versió completa).

Addicionalment, una finalitat d'aquest projecte és poder distribuir en un sol fitxer la màquina-objectiu, per a facilitar-ne la descàrrega i la posterior utilització per part de qui vulgui fer servir aquest entorn d'aprenentatge. Oracle VirtualBox ofereix aquesta opció, exportant la màquina en format .OVA.

3.2 Configuració de l'entorn del laboratori -

L'entorn que es farà servir per a realitzar aquest projecte es basarà en la virtualització de dos sistemes: la màquina-objectiu i la màquina atacant.

Per a virtualitzar aquests dos sistemes, s'utilitzarà Oracle VirtualBox instal·lat en un equip amb Windows 10 i en un altre equip amb Windows 11, indistintament. Les màquines virtuals (objectiu i atacant) es desaran, a més a més, en un disc dur Samsung T7 de 4 TB per poder-les traslladar d'un equip a un altre i per a fer-ne còpies de seguretat. També es faran còpies de seguretat al núvol (Google Drive i Microsoft OneDrive).

Com que aquest projecte té una voluntat formativa s'afegeixen als annexos unes guies de com instal·lar la màquina-objectiu i la màquina atacant al nostre laboratori per tal que no calguin coneixements previs en aquest aspecte.

3.3 Màquina Objectiu: Ubuntu Server 22.04.3 LTS

Per a la màquina-objectiu s'ha escollit la darrera versió LTS de la distribució d'Ubuntu Server, doncs, és una reconeguda distribució del sistema operatiu Linux i segons i és la millor sobretot parlant d'escalabilitat (Techradar 2023). Mantinguda per Canonical[15], la versió que he utilitzat és la LTS (*Long Term Support*)

3.4 Màquina Atacant: Kali Linux 2023.3

Una de les millors distribucions del sistema operatiu Linux orientada a la ciberseguretat, és el KALI Linux[16], i està basada en una altra famosa distribució Linux: Debian[17]. Inclou múltiples i variades eines enfocades a la seguretat informàtica i a dur a terme tasques de *pentesting,* auditories de xarxes sense fils i de sistemes, anàlisis forenses, etc.

L'empresa *Offensive Security*[18] també coneguda com a *Offsec* és una empresa americana molt coneguda i reconeguda en el context de la seguretat informàtica i el *pentesting*. Forma a persones i professionals i et permet obtenir certificats d'expertesa

[15] Canonical: https://canonical.com/
[16] Kali Linux https://www.kali.org/
[17] Debian OS: https://www.debian.org/index.ca.html
[18] OffSec: https://www.offsec.com/

i de molt prestigi en el sector de la ciberseguretat com l'OSCP[19]. I és l'empresa responsable de la distribució i manteniment de la distribució de KALI Linux.

Per a realitzar aquest projecte s'utilitzarà la versió de Kali Linux 2023.3 que és la més recent disponible i amb el format de màquina virtual, que directament es pot descarregar des de la seva pàgina web[20].

4. CTF4Edu – Una gamificació en forma de reptes

4.1 Això del hacking ètic i els CTF és per tothom?

La resposta és sí de forma contundent; tingui o no coneixements informàtics o de pentesting, qualsevol persona amb interès en la matèria pot desenvolupar la mentalitat de hacker (hacker mindset). Per a fer pentesting no tan sols fan falta habilitats en informàtica sinó pensament pràctic (Wylie i Crawley, 2021). Així doncs, la clau és intentar anar desenvolupant aquesta mentalitat de hacker, i davant dels reptes, pensar com detectar i aprofitar les vulnerabilitats de la màquina-objectiu.

En cas de no saber com continuar en un repte concret del CTF4Edu sempre podem revisar la proposta del *writeup* del repte per a disposar d'una possible manera de resoldre'l, estudiar-la, entendre-la, intentar aplicar-la, i anar alimentant la nostra motxilla d'habilitats i la nostra mentalitat de hacker.

4.2 Proposta de Reptes pel CTF4Edu

El CTF4Edu té clarament finalitats formatives i educatives per un públic objectiu universitari, de secundària o bé personal tècnic amb interessos pel *pentesting*. En conseqüència es proposen una bateria de reptes el més variada possible per tal de poder introduir diverses de les tipologies específiques de la ciberseguretat i els CTF.

Els reptes s'han dissenyat per tal que segueixin el fil conductor de la història principal per aconseguir una experiència immersiva.

1. FTP vulnerable amb *login* anònim i codificació d'informació en base64
2. Anàlisi forense de paquets de xarxa i directoris ocults en servei Wordpress
3. *Site* PHP i MySQL vulnerable a SQL Injection
4. Esteganografia i ocultació d'informació
5. Enginyeria inversa
6. Tipus de fitxers Obscurs, xifratge i ocultació d'informació
7. Atacs de força bruta i obtenció de credencials
8. Escalada de privilegis explotant CronJobs

[19] OffSec Pen-200 OSCP Penetration Testing: https://www.offsec.com/courses/pen-200/
[20] Kali Format Virtual Box: https://cdimage.kali.org/kali-2023.3/kali-linux-2023.3-virtualbox-amd64.7z

4.3 – Repte 1: FTP vulnerable

Per a poder configurar aquest primer repte a la màquina objectiu, cal instal·lar-hi un servidor FTP[21].

Per a fer-ho, cal executar la comanda: sudo apt install vsftpd

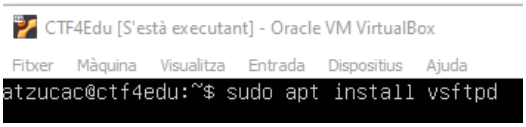


Figura 6 Instal·lació vsftd

Cal crear una carpeta que serà la que tindrà accés l'usuari anònim del servidor FTP i on hi desarem la flag. Per això executo:

sudo mkdir /home/compartir

Com que es vol permetre l'accés anònim i aquesta configuració està deshabilitada per defecte, cal editar el fitxer de configuració del servidor FTP vsftp[22] que es troba a /etc/vsftpd.conf. Per a fer-ho s'executa la comanda:

sudo nano /etc/vsftpd.conf

Al fitxer de configuració cal modificar el paràmetre anonymous_enable i establir-lo al valor YES.

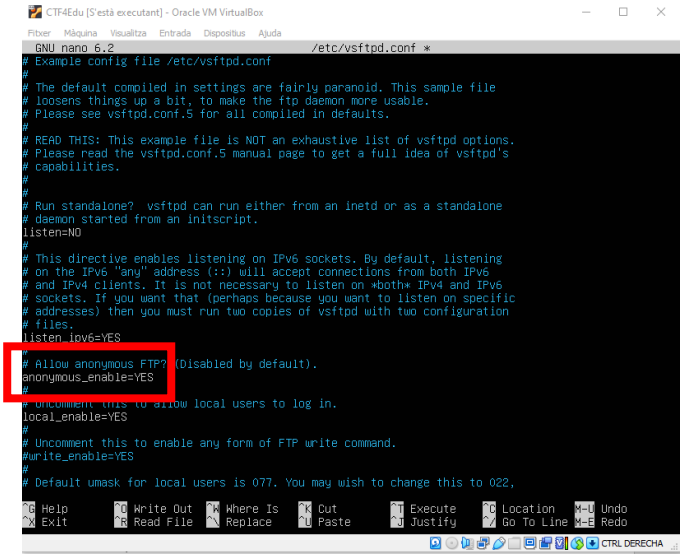


Figura 7 - Configuració vsftpd.conf

També cal modificar la ruta per defecte on l'usuari anònim accedirà quan es connecti al servidor FTP, i per tant afegim la entrada següent al fitxer: anon_root=/home/compartir

[21] FTP Server URL: https://ubuntu.com/server/docs/service-ftp
[22] Vsftpd "Very Secure FTP Daemon" https://help.ubuntu.com/community/vsftpd

Finalment, es desa el fitxer.

Per assegurar que es permetrà l'accés anònim es comprova llegint el contingut del fitxer de configuració i filtrant totes les entrades que coincideixen amb "anonymous". S'executa: cat /etc/vsftpd.conf | grep "anonymous"

Figura 8 - Comprovació accés FTP anònim

Tal i com indica el manual d'ús del servidor FTP, cal reiniciar el servei executant: sudo systemctl restart vsftp.service

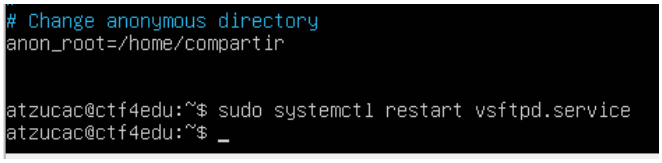


Figura 9 - Reiniciar servei FTP

Amb això ja es té configurat el servidor FTP vulnerable a la màquina objectiu, doncs exposa el port 21 i permet un accés anònim al mateix.

Per afegir una mica de dificultat al primer repte, el contingut de la primera *flag* es trobarà encriptat usant Base64[23].

S'accedeix a la carpeta arrel de l'usuari anònim FTP (/home/compartir).

Es crea una carpeta anomenada .banderanegra. Tots els fitxers i carpetes que comencen per '.', es mostren ocults[24] i per tant, és menys evidentment on hi ha la bandera amagada. S'executa la comanda: sudo mkdir .banderanegra

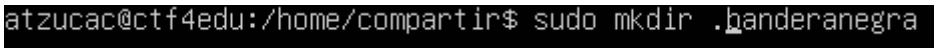


Figura 10 - Creació carpeta .banderanegra

S'afegeix un fitxer amb el nom -bandera dins de la carpeta .banderanegra. Tots els fitxers que comencen amb un guió ('-') tenen la característica que no és tan trivial de llegir el seu contingut. Per exemple, quan executo la comanda
cat -bandera s'obté un error.

[23] Base64 URL: https://en.wikipedia.org/wiki/Base64
[24] Hide Artifacts URL: https://attack.mitre.org/techniques/T1564/001/

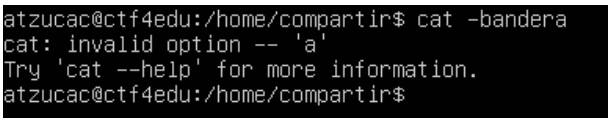


Figura 11 - Error llegint fitxer -bandera

Per a crear una mica d'entropia, s'afegeixen alguns fitxers més amb informació no rellevant.

Per a codificar la *flag* del repte1: ctf4edu_flag{J4t3nsl4P3rl4n3gr4} amb base64 i desar el resultat al fitxer -bandera, s'executa la comanda:

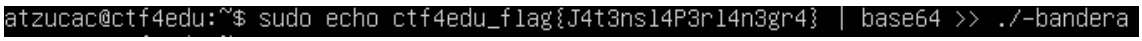


Figura 12 - Codificació flag base64

Si es comprova el contingut del fitxer, està codificat i per tant, ja tenim tot el repte1 configurat.

Figura 13 - Contingut fitxer -bandera

4.3.1 – *Writeup* Repte 1: visió del Red Team

Per a resoldre el repte, s'utilitzarà un sistema atacant KALI Linux, concretament la versió 2023.3.

Per a dur a terme l'atac a la màquina per a resoldre aquest repte caldrà seguir els següents punts:

1. Enumeració de serveis, ports, i recollida de dades de cada situació i/o equip.
2. Analitzar les possibles vulnerabilitats per aprofitar-les
3. Explotar les vulnerabilitats detectades (una o més d'una) fins aconseguir l'objectiu (flag)
4. Post-explotació: Avançar cap al següent repte

Tal i com apunta l'enunciat, es creu que es tenen indicis suficients per a saber que una màquina de la mateixa subxarxa on hi ha ara la nostra màquina atacant pot tenir alguna pista interessant.

Primer de tot, s'hauria de saber a quina subxarxa ens trobem i quina adreça IP té el nostre equip atacant. Per tant, podem usar la comanda IP.

S'obre una *Shell* i s'executo: ip a

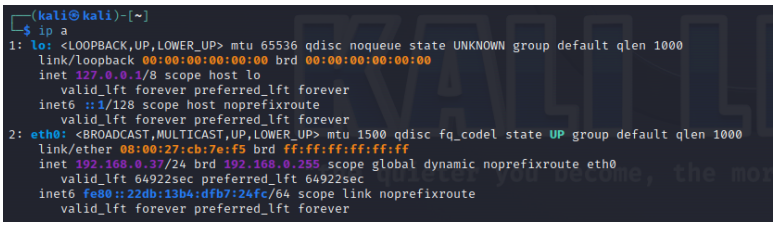


Figura 14 - IP màquina atacant

Amb el retorn de la comanda, s'observa que es troba a la subxarxa 192.168.0.x/24 (l'adaptador és eth0) i per tant, ja es tenen més dades per iniciar la fase d'enumeració.

Així doncs, per a poder veure quines màquines hi ha actives i poder continuar, es pot fer servir l'eina Nmap[25] que permet escanejar tota la xarxa

S'executa la comanda: nmap -sV 192.168.0.0/24

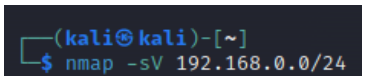


Figura 15 - Repte 1 - Escaneig de ports amb NMAP

La opció -sV és per intentar descriure la versió o obtenir la màxima informació del servei que es pugui estar executant a cada port obert.

Quan l'escaneig finalitza, l'interès comença a recaure a una màquina en concret:

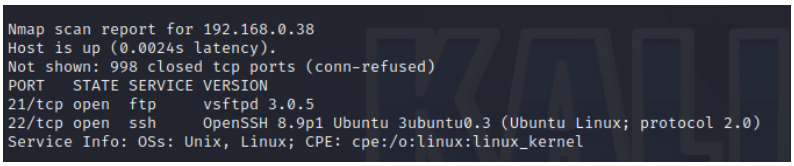


Figura 16 - Repte 1 - Ports oberts

Una de les paraules que s'ha interceptat era Ubuntu i a més a més, tots els equips de l'aula informàtica són Windows així que probablement s'està seguint la bona pista. Per tant, la IP de la màquina objectiu és **192.168.0.38**

Així doncs, ja es veu que hi ha una màquina Ubuntu que té el port 21 FTP obert i el port 22 SSH també. Amb aquest punt, es dona per finalitzada la fase d'enumeració i es comença a pensar una estratègia d'atac.

Com que una altra paraula captura parlava de **fitxer**, es comença per veure si puc iniciar sessió anònima al servidor FTP.

S'executa: ftp 192.168.0.38

[25] Nmap | Nmap.org accessible a: https://nmap.org/ data darrera consulta 3/12/2023

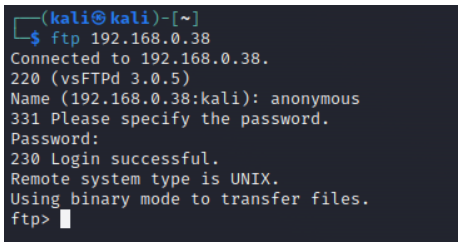


Figura 17 - Connectar-se a l'FTP

Quina sort! S'ha pogut connectar anònimament. Ara es comença a investigar a veure que es descobreix des de la carpeta on es troba. S'executa: ls

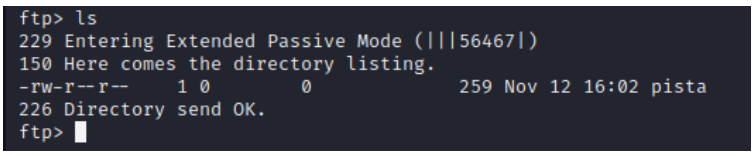


Figura 18 - ls a FTP

Perfecte. Hi ha un fitxer anomenat pista. Tal i com s'havia escoltat també a la conversa. Es descarrega el fitxer per a poder seguir investigant. S'executa:
get pista

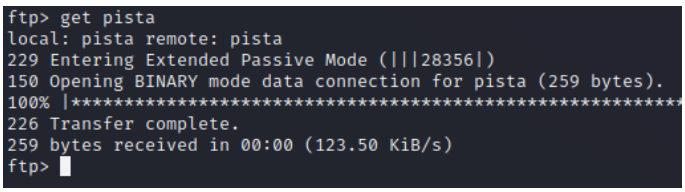


Figura 19 - Obtenció de la pista

De moment es deconnecta i s'investiga la pista. S'executa: exit

Tot seguit, s'intenta llegir el contingut del fitxer descarregat.
S'executa: cat pista

I dins del fitxer, hi ha un text una mica estrany i enigmàtic:

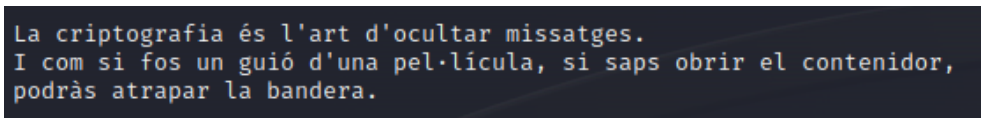


Figura 20 - Text enigmàtic

Sembla que això d'atrapar la bandera sigui com l'objectiu final. I també sembla que hi ha un missatge ocult, dins d'una mena de contenidor. Però, on deu ser tot això?

Com que no es tenen més pistes, se li acut que potser hi ha alguna cosa "oculta" a la carpeta del servidor FTP que no s'ha vist i per tant, s'hi reconecta per a seguir investigant.

Un cop fet, s'executa: ls -alis

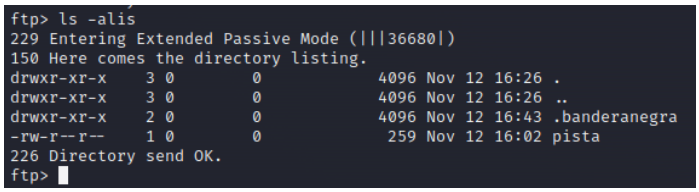


Figura 21 - Contingut ocult FTP

Perfecte. Hi havia una carpeta oculta que ara si que es veu. S'hi accedeix per a seguir investigant. S'executa: cd .banderanegra

I un cop dins, es torna a demanar un llistat del contingut ocult:

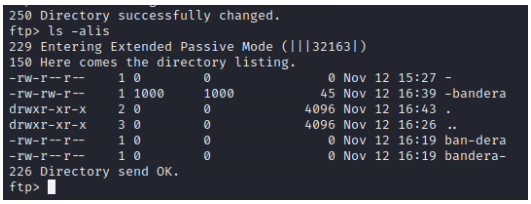


Figura 22 - Contingut ocult FTP (2)

Hi ha diversos fitxers amb el noms similars a bandera. Sembla que es va pel bon camí. Se'ls descarrega.

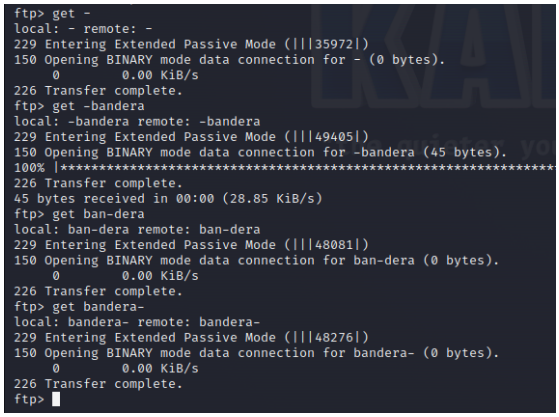


Figura 23 - Fitxers bandera

Es desconnecta i els vol analitzar localment.

L'únic que té alguna dada interessant és -bandera

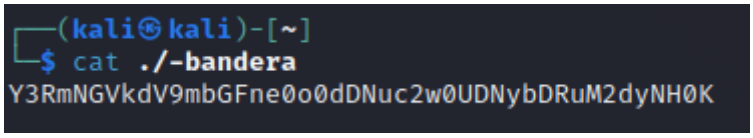


Figura 24 - Contingut -bandera encriptat

De tota manera, hi ha una cosa que fa ballar al cap. Hi havia una cosa que s'h escoltat a la conversa, alguna cosa relacionada amb el número 64. I llavors, s'ha recordat allò del text de la pista, del missatge ocult, el contenidor...I la criptografia. I si el missatge està codificat en Base64? S'intentar descodificar-lo a veure què s'obté. El paràmetre -d és per a descodificar.

Executo: base64 -d ./-bandera

```
┌──(kali㉿kali)-[~]
└─$ base64 -d ./-bandera
ctf4edu_flag{J4t3nsl4P3rl4n3gr4}
```

Figura 25 - Descodificant base64 -bandera

Ja es té la primera bandera. A veure on portarà o perquè serveix aquesta pista.

4.4 – Repte 2: Anàlisi Forense i Directoris ocults en un *site* Wordpress

Per a codificar aquest segon repte, es comença per a crear el fitxer PCAPNG des d'un terminal de Kali:

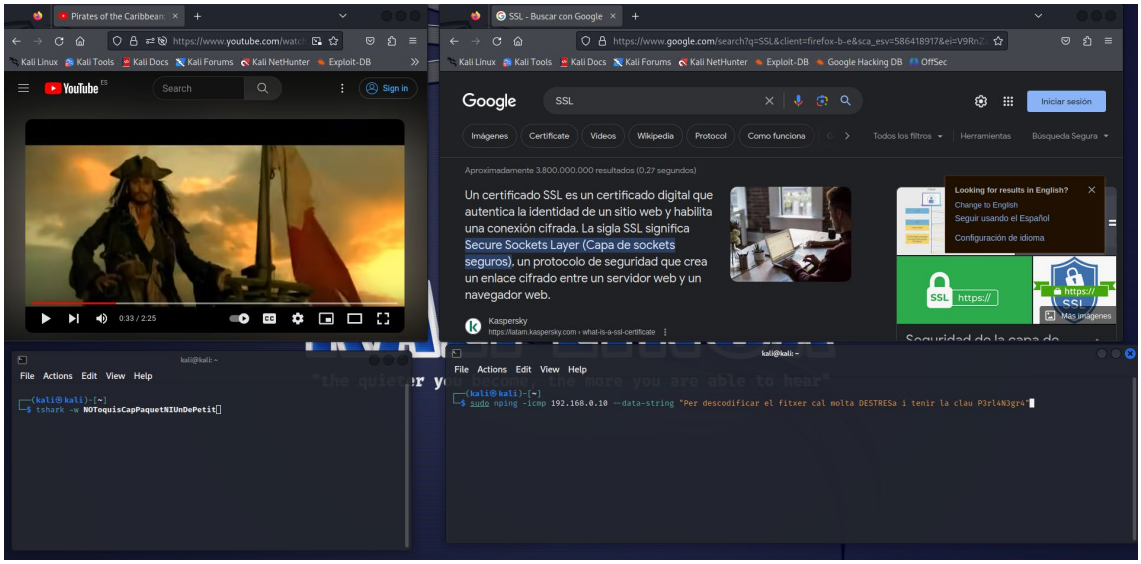


Figura 26 - Procés creació PCAPNG

S'obre un terminal i s'executa:

```
┌──(kali㉿kali)-[~]
└─$ tshark -w NOToquisCapPaquetNIUnDePetit
```

Figura 27 - Captura de paquets tshark

Aquesta comanda permet escriure al fitxer passat per paràmetre tots els paquets de la xarxa on es troba connectat el Kali i per defecte el desa en format PCAPNG. Per generar una mica de paquets de soroll, es visualitza el tràiler oficial de la pel·lícula "Pirates del Carib: La Maledicció de la Perla Negra" i es consulta la pàgina del protocol SSL.

Des d'un altre terminal, s'executa la comanda:

```
┌──(kali㉿kali)-[~]
└─$ sudo nping -icmp 192.168.0.10 --data-string "Per descodificar el fitxer cal molta DESTRESa i tenir la clau P3rl4N3gr4"
```

Figura 28 - Generació de la pista al PCAPNG

La comanda nping permet fer un ping generant un paquet ICMP i alhora annexar una cadena de text pla al darrera d'aquest. Amb aquest recurs, s'oculta el missatge que servirà de pista ja que conté una contrasenya que caldrà fer servir posteriorment.

Es crea una adreça de Gmail (ctf4edu@gmail.com) i es desa a l'espai al núvol d'aquest compte el fitxer PCAPNG i es comparteix amb permisos de lectura amb qualsevol que tingui l'enllaç:

https://drive.google.com/file/d/1UjVzipZFDhErtiwV4-GI0u4qwh1gnG0c/view?usp=sharing

També es genera un codi QR, que apunta al mateix enllaç:

Figura 29 - Codi QR al fitxer PCAPNG

Tot seguit, s'instal·la el WordPress a l'Ubuntu Server.

Primer de tot cal actualitzar el sistema:

```
atzucac@ctf4edu:~$ sudo apt update_
```

Figura 30 - Actualització Ubuntu Server

Tot seguit, i per les dependències s'instal·la l'Apache i el PHP:

```
atzucac@ctf4edu:~$ sudo apt install apache2 ghostscript libapache2-mod-php mysql-server php php-bcma
th php-curl php-imagick php-json php-mbstring php-mysql php-xml php-zip_
```

Figura 31 - Instal·lació Apache i PHP

Procedim a instal·lar-hi el WordPress:

```
atzucac@ctf4edu:~$ sudo mkdir -p /srv/www
```

Figura 32 - Creació Carpeta Seveis Web

```
atzucac@ctf4edu:~$ sudo chown www-data: /srv/www
```

Figura 33 - Permisos per www-data a /serv/www

```
atzucac@ctf4edu:~$ curl https://wordpress.org/latest.tar.gz | sudo -u www-data tar zx -C /srv/www_
```

Figura 34 - Descàrrega i descompressió del Wordpress

I a configurar l'Apache per al WordPress:

Es crea el fitxer de configuració:

```
atzucac@ctf4edu:~$ nano /etc/apache2/sites-available/worpress.conf_
```

Figura 35 - Fitxer configuració Apache

Amb la següent configuració:

```
atzucac@ctf4edu:~$ cat wordpress.conf
<VirtualHost *:80>
    DocumentRoot /srv/www/worpress
    <Directory /srv/www/wordpress>
        Options FollowsSymLinks
        AllowOverride Limit Options FileInfo
        DirectoryIndex index.php
        Require all granted
    </Directory>
    <Directory /srv/www/wordpress/wp-content>
        Options FollowSymLinks
        Require all granted
    </Directory>
</VirtualHost>
```

Figura 36 - Contingut configuracio Site Worpress

Habilita el site:

```
atzucac@ctf4edu:~$ sudo a2ensite wordpress_
```

Figura 37 - Habilitació Site Wordpress

Habilita la URL reescrivint-la:

```
atzucac@ctf4edu:~$ sudo a2enmod rewrite
```

Figura 38 - Habilitació URL Site WP

Deshabilita el site per defecte de “It Works”:

```
atzucac@ctf4edu:~$ sudo a2dissite 000-default
```

Figura 39 - Deshabilita el site per defecte

Reinicia el servei de l’Apache per aplicar canvis:

```
atzucac@ctf4edu:~$ sudo service apache2 reload
```

Figura 40 - Es reinicia el servei d'Apache

Per a configurar el WordPress es necessita crear una base de dades MySQL, un usuari i donar-li els permisos adequats per a poder operar amb la base de dades:

```
atzucac@ctf4edu:~$ sudo mysql -u root_
```

Figura 41 - Connexió a MySQL

```
mysql> CREATE DATABASE wordpress;
Query OK, 1 row affected (0.01 sec)
```

Figura 42 - Creació base de dades WP

```
mysql> CREATE USER wordpress@localhost IDENTIFIED BY '4tz1c4c$1p3rS3cr3t';
Query OK, 0 rows affected (0.02 sec)
```

Figura 43 - Creació Usuari wordpress a la BdD

```
mysql> GRANT SELECT,INSERT,DELETE,CREATE,DROP,ALTER
    -> ON wordpress.*
    -> TO wordpress@localhost;
Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
```

Figura 44 - Configuració permisos usuari wordpress

Un cop configurada la base de dades, s'habilita MySQL executant:

```
atzucac@ctf4edu:~$ sudo service mysql start
```

Figura 45 - Reiniciar servei MySql

Es configura el WordPress per tal de connectar amb la base de dades.

Primer es copia la configuració d'exemple a un fitxer anomenat wp-config.php:

```
atzucac@ctf4edu:/srv/www/wordpress$ sudo -u www-data cp wp-config-sample.php wp-config.php
```

Figura 46 - Configuració de wp-config.php

El següent pas, és configurar les credencials de la base de dades al fitxer de configuració:

```
atzucac@ctf4edu:~$ sudo -u www-data sed -i 's/database_name_here/wordpress/' /srv/www/wordpress/wp-c
onfig.php
atzucac@ctf4edu:~$ sudo -u www-data sed -i 's/username_here/wordpress/' /srv/www/wordpress/wp-config
.php
atzucac@ctf4edu:~$ sudo -u www-data sed -i 's/password_here/4tz1c4c$1p3rS3cr3t/' /srv/www/wordpress/
wp-config.php
atzucac@ctf4edu:~$
```

Figura 47 - Configuració de credencials per accés BdD

Per a configurar el site de WordPress, primer cal determinar la IP tenim de la màquina objectiu:

```
atzucac@ctf4edu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:ba:8d:07 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.41/24 metric 100 brd 192.168.0.255 scope global dynamic enp0s3
       valid_lft 81320sec preferred_lft 81320sec
    inet6 fe80::a00:27ff:feba:8d07/64 scope link
       valid_lft forever preferred_lft forever
atzucac@ctf4edu:~$ _
```

Figura 48 - Consulta IP màquina-objectiu

Des del navegador d'un altre equip de la xarxa, s'accedeix a la ip obtinguda 192.168.0.41 i es veu ja la pàgina d'inici de la instal·lació de WordPress i s'escull l'idioma:

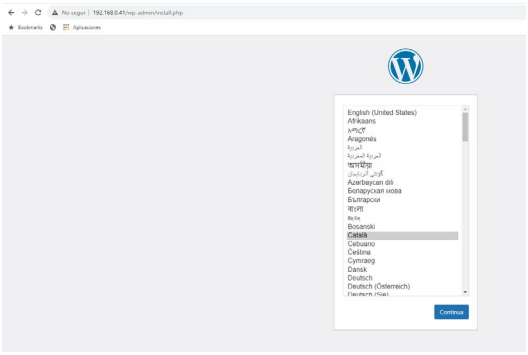


Figura 49 - Inici instal·lació WP - Idioma

Es configuren les dades del site i es dona d'alta un usuari, un password i una adreça de correu associada al compte.

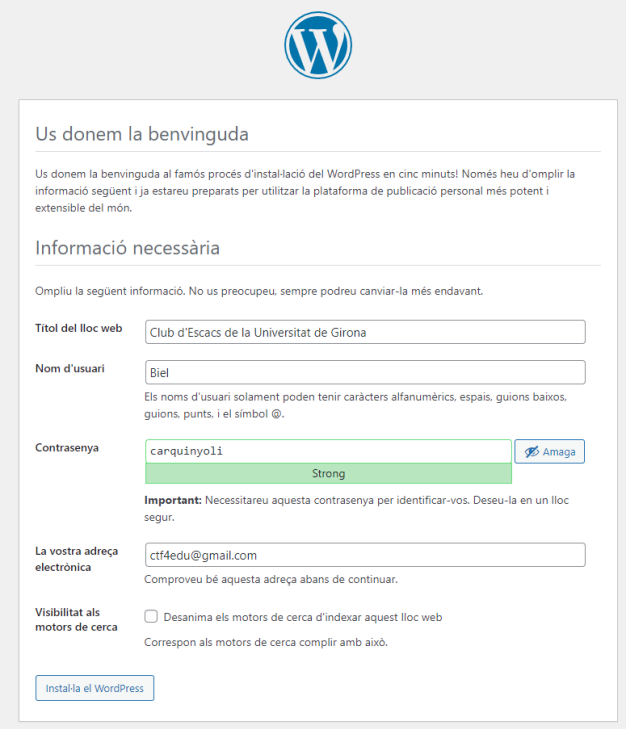


Figura 50 - Dades Usuari WP Instal·lació

S'instal·la el Wordpress i ja es té el site actiu pel repte.

Si es vol accedir a la pàgina del Tauler de WordPress (/wp-admin.php), demana identificació:

Figura 51 - WP login

I un cop s'identifica ja es pot accedir al Tauler de WordPress:

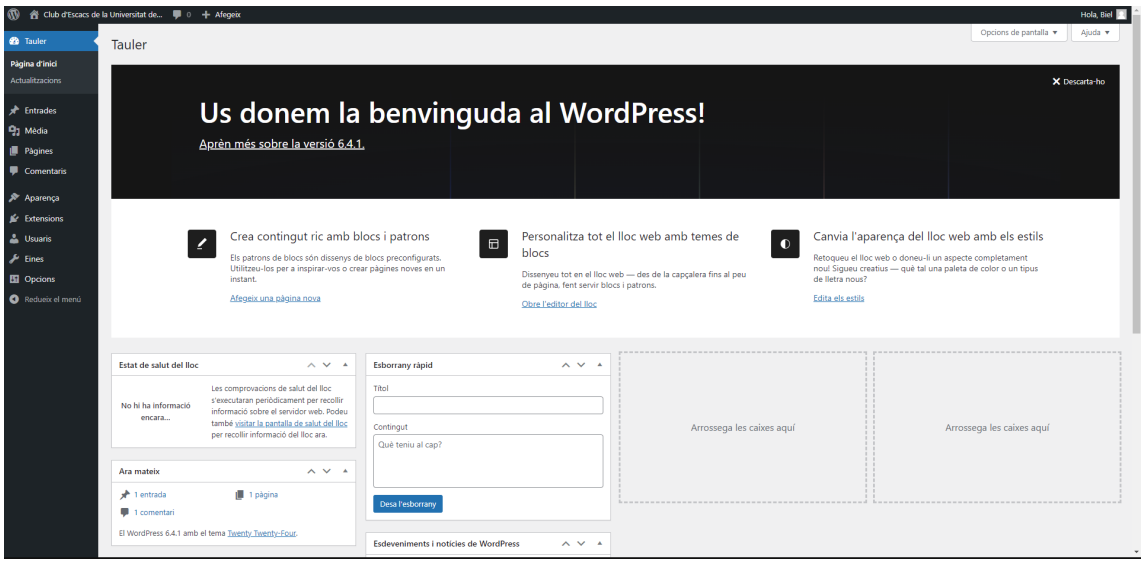


Figura 52 - Tauler de WP

Finalment es disposa d'un Wordpress totalment operatiu a la nostra màquina-objectiu, ara caldrà que s'utilitzi pel repte, on s'amagarà la flag a l'interior d'aquest Tauler.

A l'arrel del site es crea el directori /adminsecret

Es canvia el propietari i el grup del directori:

```
atzucac@ctf4edu:/srv/www/wordpress$ sudo chown www-data:www-data adminsecret_
```

Figura 53 - Permisos directori /adminsecret

Es continua creant el fitxer robots.txt i es desa l'arrel del site:

```
atzucac@ctf4edu:/srv/www/wordpress$ nano robots.txt_
```

Figura 54 - Creació robots.txt

I aqui s'hi posa la pista de que una carpeta anomenada /adminsecret dins del site no es vol que sigui indexada.

```
atzucac@ctf4edu:/srv/www/wordpress$ sudo cat robots.txt
User-Agent: *

Disallow: /adminsecret

Darrera modificació: 28/12/2022 by B.
```

Figura 55 - Contingut robots.txt

Per tant, aquesta carpeta s'haurà de fer accessible des de la configuracio de l'Apache. S'edita el fitxer /etc/apache2/sites-available/wordpress.conf i s'afegeix la opció +Indexes per tal que es permeti el llistat de directori quan s'hi vulgui accedir:

```
atzucac@ctf4edu:/srv/www/wordpress$ cat /etc/apache2/sites-available/wordpress.conf
<VirtualHost *:80>
    DocumentRoot /srv/www/wordpress
    <Directory /srv/www/wordpress>
        Options FollowSymLinks
        AllowOverride Limit Options FileInfo
        DirectoryIndex index.php
        Require all granted
    </Directory>
    <Directory /srv/www/wordpress/wp-content>
        Options FollowSymLinks
        Require all granted
    </Directory>
    <Directory /srv/www/wordpress/adminsecret>
       Options +Indexes
       Require all granted
    </Directory>
</VirtualHost>
```

Figura 56 - Apache permet indexació contingut directoris

I es reinicia el servei de l'Apache:

```
atzucac@ctf4edu:/srv/www/wordpress$ sudo service apache2 reload
```

Figura 57 - Reiniciar servei Apache

Es crea ara un fitxer on hi ha escrites les credencials de l'usuari de WP on hi ha la flag.

```
atzucac@ctf4edu:/srv/www/wordpress/adminsecret$ sudo nano tr3s0rP1r4t4.txt
```

Figura 58 - Creacio fitxer contenidor pista per flag

```
atzucac@ctf4edu:/srv/www/wordpress/adminsecret$ cat tr3s0rP1r4t4.txt
Ho deixo aqui protegit per no oblidar-ho:

credencials WP => biel / carquinyoli
```

Figura 59 - Credencials WP

Es xifra el fitxer amb openssl i des3 i es protegeix amb la clau (pista paquet PCAPNG):

```
atzucac@ctf4edu:/srv/www/wordpress/adminsecret$ sudo openssl des3 -salt -in tr3s0rP1r4t4.txt -out fi
txer.txt -k P3rl4N3gr4_
```

Figura 60 - Xifratge de contenidor credencials

Amb tot preparat, s'entra amb les credencials al site de WordPress i s'oculta la flag a la informació biogràfica del perfil de l'usuari:

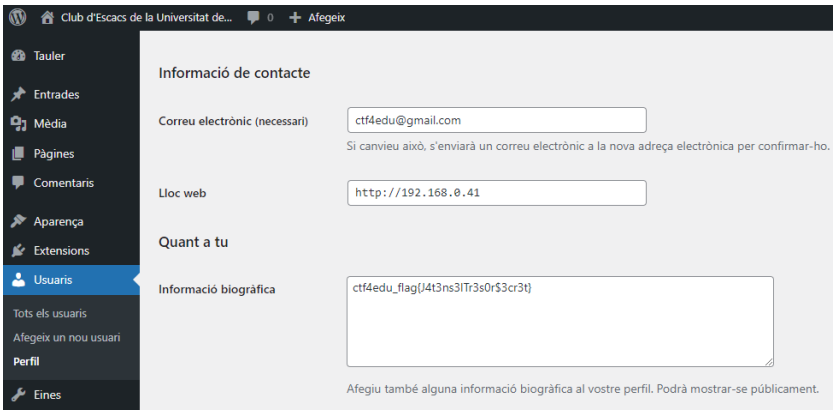


Figura 61 - Ocultació flag al tauler WP

4.4.1 – *Writeup* Repte 2: visió del Red Team

El codi QR apunta a l'enllaç:

https://drive.google.com/file/d/1UjVzipZFDhErtiwV4-GI0u4qwh1gnG0c/view?usp=sharing

Si s'hi accedeix, directament es veu la proposa de descarregar un fitxer:

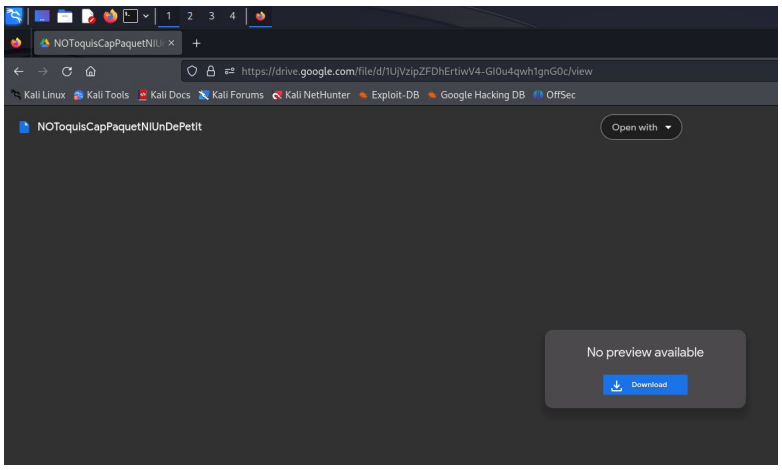


Figura 62 - Descàrrega de PCAPNG

Abans de descarregar-lo, es una bona idea crear una estructura de carpetes on anar desant la informació, ja que no se sap tot el que es necessitarà o es pot trobar:

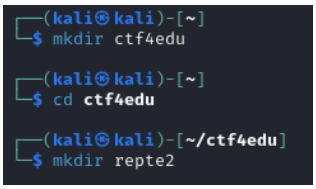


Figura 63 - Estructura de carpetes pel repte

I es descarrega el fitxer misteriós a la carpeta repte2

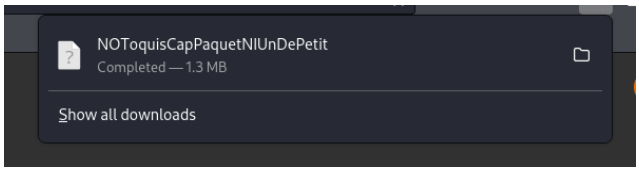


Figura 64 - Fitxer descarregat

Es copia a la carpeta repte2.

Es procedeix a analitzar-lo.

Per a començar es veu que té un nom tot curiós però es comença amb la comanda **file**[26], per a saber quin tipus de fitxer és:

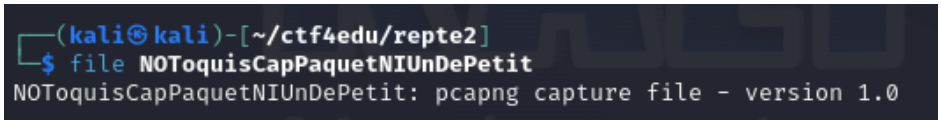


Figura 65 - Tipus de fitxer PCAPNG

Es veu que és un fitxer tipus pcapng[27], o sigui una traça de paquets de xarxa capturats. Per tant, l'obrim amb el Wireshark[28] a veure què trobem:

Figura 66 - Obertura fitxer amb Wireshark

[26] File command in Linux with examples (19/02/2021) | GeeksForGeeks: https://www.geeksforgeeks.org/file-command-in-linux-with-examples/
[27] PcapNG File Format (s.d) Erik Hjelmvik consultat per darrera vegada el 18/11/2023 a: https://pcapng.com/
[28] Wireshark - https://www.wireshark.org/

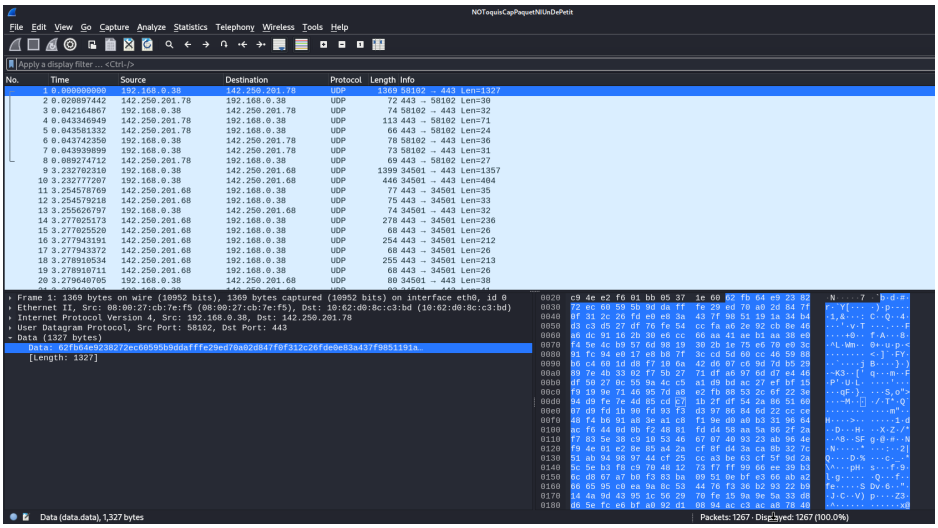


Figura 67 - Fitxer PCAPNG obert amb Wireshark

Es recorre una mica el fitxer però hi ha molts paquets i tampoc se sap el que s'està cercant. De cop i volta, cal adonar-se del nom del fitxer:

NoToquisCapPaquetNIUndePetit.

Hi ha lletres en majúscula, que si s'agafen totes soles, s'obté: NOTCPNIUDP

I si és una pista? El missatge està dient que no s'ha de cercar ni en paquets TCP ni tampoc en UDP? S'estableix el filtre i es restringeix que aquests paquets no apareguin. EL WireShark entre moltes altres funcions, permet aplicar filtres:

Figura 68 - Barra de filtre de Wireshark

S'aplica el filtre amb la sintaxi correcta:

Figura 69 - Filtre aplicat a Wireshark

I es veu això:

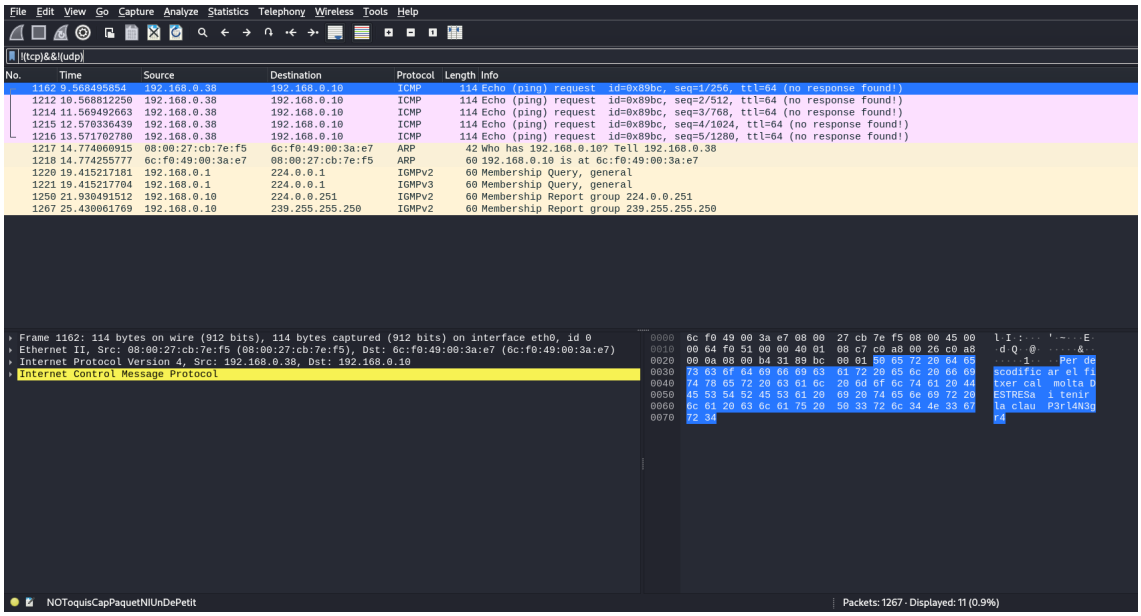


Figura 70 - Wireshark amb paquets filtrats

Cal fixar-se en els paquets ICMP, a la part inferior dreta de la pantalla:

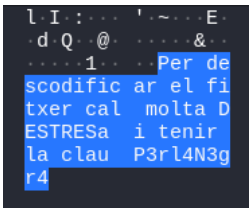


Figura 71 - Missatge ocult en paquet

“Per descofiicar el fitxer cal molta DESTRESa i tenir la clau P3rl4N3gr4”

No se sap encara què significa però millor que es desi en un fitxer a la carpeta del repte:

Figura 72 - Desar la pista en un fitxer de text

Arribats a aquest punt, potser seria una bona idea tornar a la fase d’enumeració, i analitzar més profundament tot aquest sistema objectiu per veure què més es pot descobrir.

S’inicia un escaneig més profund amb Nmap i per si ens cal fer posteriors consultes, es desa a la nostra carpeta de treball. Així doncs, crearem una carpeta anomenada nmap.

I s’executa Nmap amb els següents tags[29] a tota la VLAN que ja teníem del repte anterior:

[29] Nmap Cheat Sheet 2023: All the Commands, Flags & Switches | Nathan House (26/10/2023) accessible a: https://www.stationx.net/nmap-cheat-sheet/

```
┌──(kali㉿kali)-[~/ctf4edu/repte2]
└─$ nmap -sV -oN nmap/objectiu 192.168.0.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-03 15:48 EST
```

Figura 73 - Nmap escaneig verificar màquina-objectiu

-sV: Intenta determinar la versió dels serveis que es troben executant-se a cada port
-oN: Desa el resultat a un fitxer

I s' obté que la nostra màquina-objectiu té la IP 192.168.0.41.

```
Nmap scan report for 192.168.0.41
Host is up (0.0014s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.5
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.52 ((Ubuntu))
8080/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Figura 74 - Resultats Nmap

Ara que ja està clar, es llança un altre Nmap però contra la màquina-objectiu amb els següents tags:

```
┌──(kali㉿kali)-[~/ctf4edu/repte2]
└─$ nmap -sC -sV -oN nmap/inicial 192.168.0.41
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-03 16:00 EST
```

Figura 75 - Nmap profund contra màquina-objectiu

-sC: Executa l'escaneig amb els scripts NSE[30] per defecte.

Els scripts que es troben recollits a la NSE els poden fer i compartir els usuaris i permeten fer una millor descoberta dels ports, de les versions, detecció de vulnerabilitats, etc.

Quan acaba l'Nmap es consulta el resultat:

[30] Nmap Scripting Engine (NSE) | (s.d) Nmap.org accessible a: https://nmap.org/book/man-nse.html

```
┌──(kali㉿kali)-[~/ctf4edu/repte2]
└─$ cat nmap/inicial
# Nmap 7.94SVN scan initiated Sun Dec  3 16:00:00 2023 as: nmap -sC -sV -oN nmap/inicial 192.168.0.41
Nmap scan report for 192.168.0.41
Host is up (0.0011s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.5
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.0.38
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             259 Nov 12 16:02 pista
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 f6:bb:f7:09:0e:97:c3:fe:15:6a:28:1e:0b:cb:f7:90 (ECDSA)
|_  256 76:f2:10:40:94:f3:4a:35:b2:4a:d0:f3:d7:4e:fd:10 (ED25519)
80/tcp   open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Club d&#039;Escacs de la Universitat de Girona
| http-robots.txt: 1 disallowed entry
|_/adminsecret
|_http-generator: WordPress 6.4.1
|_http-server-header: Apache/2.4.52 (Ubuntu)
8080/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Dec  3 16:00:24 2023 -- 1 IP address (1 host up) scanned in 23.57 seconds

┌──(kali㉿kali)-[~/ctf4edu/repte2]
└─$
```

Figura 76 - Resultats Nmap màquina-objectiu

Es proposa crear un document per anar prenent notes del que s'ha fet, del que es va descobrint o de possibles hipòtesis o accions a executar.

Per tant, es creea el document pentesting.txt i s'hi afegeix la @IP de la màquina-objectiu i els ports oberts que ha trobat Nmap: 21, 22, 80, 8080.

Si s'obre un navegador i anem a la pàgina 192.168.0.41 (per defecte el port 80):

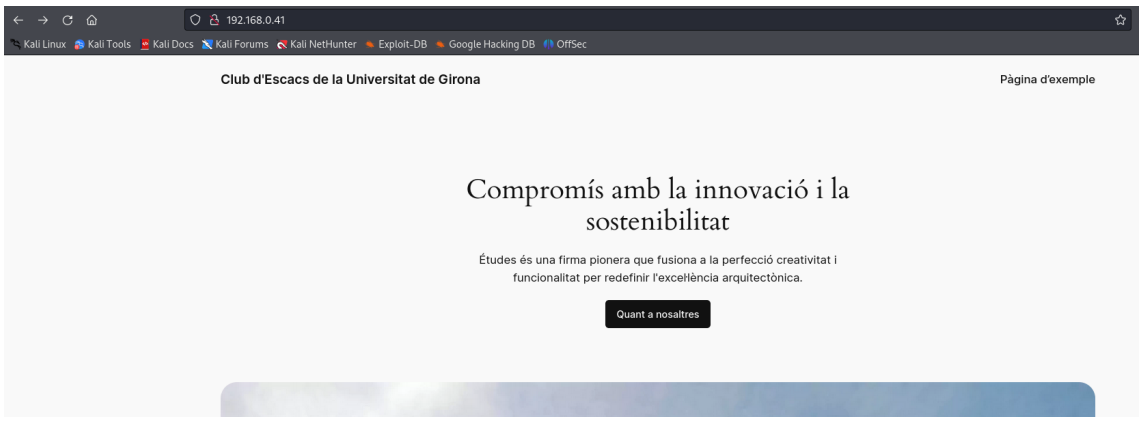


Figura 77 - Pàgina WP en construcció

Sembla una pàgina totalment de prova, com en construcció. De tota manera, si s'és observador i es va baixant per la pàgina, s'arriba un moment que es troba:

Figura 78 - Post usuari Biel al WP

Hi ha un misssatge de prova fet per un usuari anomenat Biel. Aquesta dada s'anota al nostre fitxer de pentesting.

Per a obtenir més informació d'un site, podem usar l'eina Nikto[31]:

-h: especifica un determinat host

Usem la comanda tee[32] per a desar el resultat de Nikto en un fitxer.

Figura 79 - Nikto contra site WP

També es pot obtenir molta informació de l'estructura de directoris d'un site mitjançant força bruta. A tal efecte es pot fer servir una de les potents eines que hi ha per a fer anàlisi de llocs web, com ara Gobuster[33], Dirbuster[34], Dirb[35], etc.

S' utilitza Gobuster perquè tot i no disposar d' interfície gràfica, és una eina més ràpida[36] que Dirbuster o Dirb.

Es pot llençar les dues eines en paral·lel per obtenir més informació, si es vol.

[31] Nikto 2.5 | Cirt.net accessible a: https://cirt.net/Nikto2 Consultat per darrera vega el 3/12/2023
[32] Tee https://www.geeksforgeeks.org/tee-command-linux-example/
[33] Gobuster (s.d.) accessible a: https://www.kali.org/tools/gobuster/ Consultat per darrera vega el 3/12/2023
[34] Dirbuster (s.d.) accessible a: https://www.kali.org/tools/dirbuster/ Consultat per darrera vega el 3/12/2023
[35] Dirb (s.d.) accessible a: https://www.kali.org/tools/dirb/ Consultat per darrera vega el 3/12/2023
[36]Gobuster full tutorial from noob to pro Updated 2023 | TechYRich (s.d.) accessible a: https://techyrick.com/gobuster-full-tutorial/

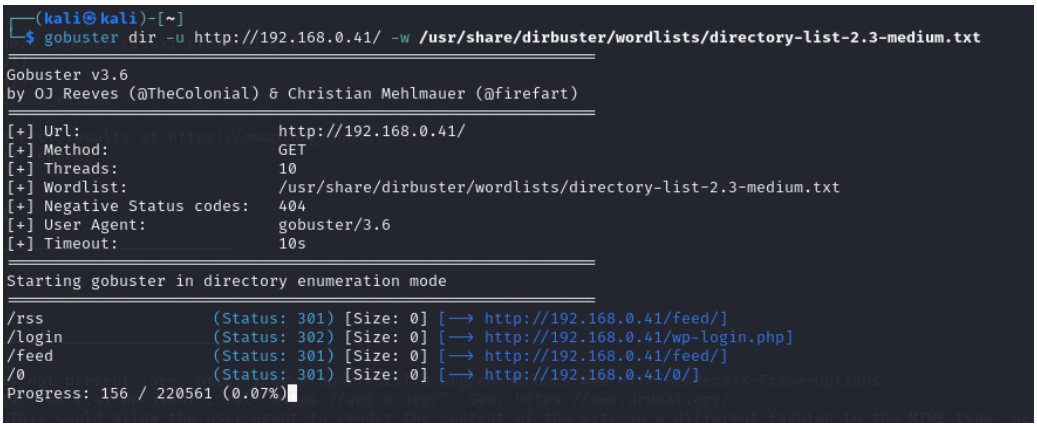


Figura 80 - Gobuster contra site WP

Els tags[37] que s'han fet servir a Gobuster:

Dir: Modalitat d'atac de força bruta a Directoris

-w: *Wordlist* o diccionari de potencials noms de directoris i fitxers per l'atac

-u: URL objectiu

Aquest processos són lents però mentre no finalitzen ja mostren resultats parcials que permeten seguir amb la investigació.

Cal fixar-se en el resultat de Nikto i ens indica que hi ha entrades que poden ser consultades manualment al fitxer robots.txt. Aquest fitxer (robots.txt) s'ha usat tradicionalment per excloure directoris del site que no es vol que els bots del motors de cerca els indexin.

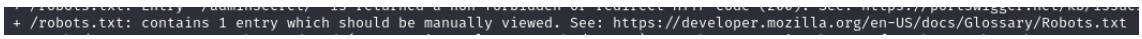


Figura 81 - Nikto troba robots.txt

Així doncs, es fa una ullada a aquest fitxer.

S'obre el navegador:

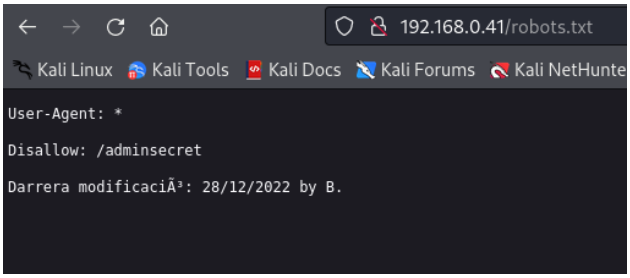


Figura 82 - Contingut robots.txt

[37] Gobuster Cheat Sheet | Matthew Hard (25/10/2023) accessible a: https://matthewhard.com/gobuster-cheat-sheet

El propi Nikto ja havia informat també de la existencia d'un directori anomenat /adminsecret però ara es troba una evidencia d'intent d'exclusió al fitxer robots.txt. A més, una possible hipòtesi és que aquest "B." que indica que va fer una modificació pot ser el Biel que s'ha trobat anteriorment. Una hipotesi més i tota la informació trobada que es pot posar al fitxer de pentesting.

Es procedeix a investigar aquest directori que s'ha detectat:

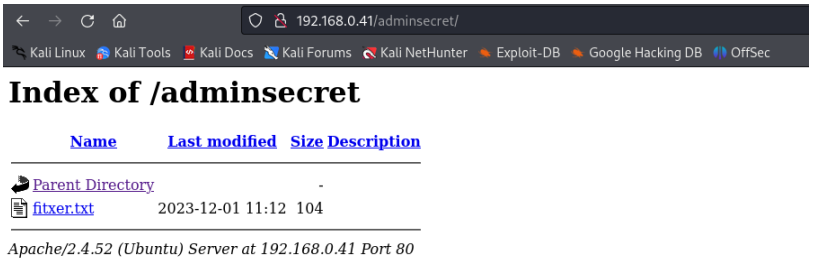


Figura 83 - Contingut /adminsecret

Aquest directori permet llistar el contingut i es troba un altre fitxer que es pot copiar a l'equip atacant per analitzar-lo:

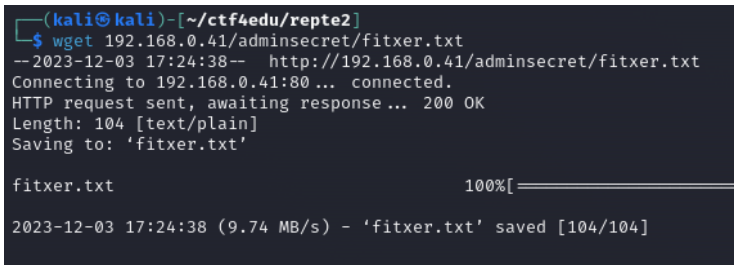


Figura 84 - Copia fitxer trobat /adminsecret

I ara, es va a investigar aquest fitxer.txt. Es comença per comprovar quin tipus de fitxer es (no es bona idea refiar-se de les extensions):

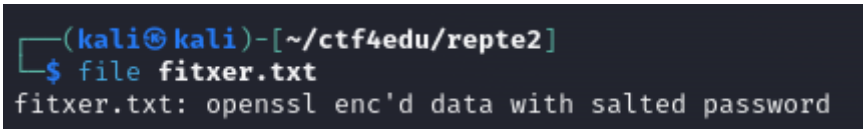


Figura 85 - Tipus de fitxer

Efectivament, el que es deia. No és un fitxer de text pla sinó un fitxer encriptat amb openssl i password.

Recordant els detalls, analitzant el paquet PCAPNG s'havia trobat una mena de pista i un password...potser es podria intentar fer-ho servir per accedir a desencriptar aquest fitxer.

Es recupera la pista, que deia:

“Per descofiicar el fitxer cal molta DESTRESa i tenir la clau P3rl4N3gr4”

Abans ha funcionat la tècnica de tenir els ulls molt oberts i no deixar escapar cap detall. Aquestes paraules majúscules de la pista DESTRES criden l’atenció. I si es tracta del sistema d’encriptació DES3[38]?

Es pot comprovar desencriptant amb openssl[39], des3 com a mètode de xifratge i el password o clau obtinguts a l’anàlisi del PCAPNG:

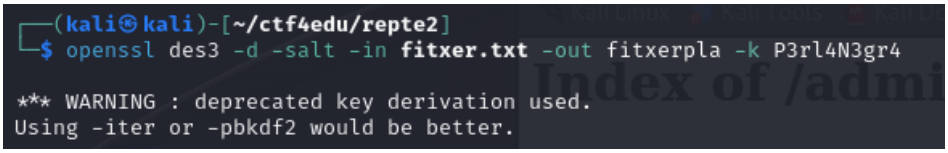


Figura 86 - Desencriptar amb OpenSSl el fitxer

Tot seguit, es veu que ha funcionat i es llegeix el contingut de fitxerpla:

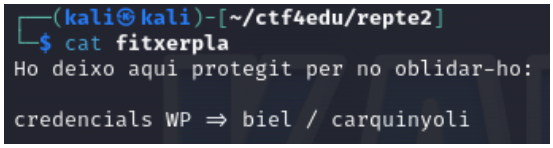


Figura 87 - Obtenció credencials WP

Un cop trobades les credencials del WordPress, es poden usar per entrar al site:

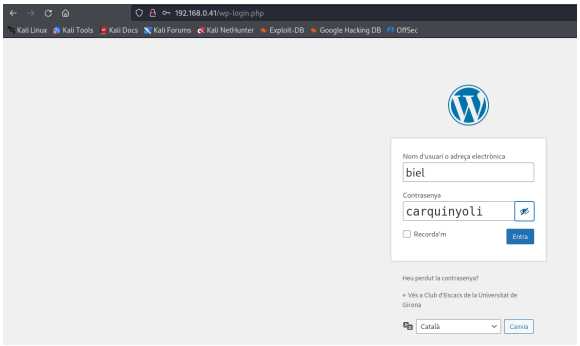


Figura 88 - Login WP amb credencials

Efectivament, les credencials son correctes.

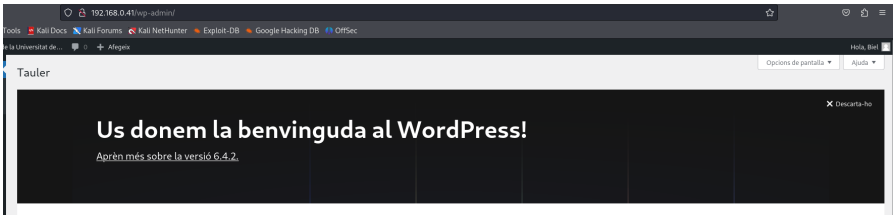


Figura 89 - Accés al WP

[38] Triple DES | Wikipedia (17/10/2023) accessible a: https://en.wikipedia.org/wiki/Triple_DES
[39]OpenSSL Cheat Sheet | Albertx accessible a: https://cheatography.com/albertx/cheat-sheets/openssl/

Anant a l'apartat d'usuaris, i accedint al perfil de l'usuari Biel, es pot trobar la *flag:*

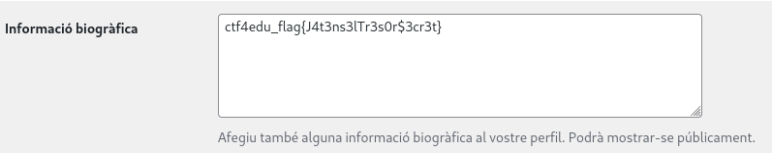


Figura 90 - Flag Repte 2

4.5 – Repte 3: *Site* PHP i MySQL vulnerable a Injecció SQL

Com que ja es té el WordPress del repte2 configurat al port 80 (per defecte), s'ha d'afegir un altre port on el servei d'Apache pugui escoltar per al nou site que es desenvoluparà per aquest repte d'injecció SQL.

Es comença editant el fitxer de configuració de l'Apache que es troba a /etc/apache2/ports.conf:

```
atzucac@ctf4edu:~$ sudo nano /etc/apache2/ports.conf
```

Figura 91 - Configuració ports.conf Apache

I s'hi afegeix que també escolti pel port 8080 (*Listen 8080*) :

```
  GNU nano 6.2                          /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80
Listen 8080

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Figura 92 - Contingut ports.conf Apache

Cal crear el directori on hi haurà tota la estructura del *site*:

```
atzucac@ctf4edu:/$ sudo mkdir /var/www/c3ntr3d3v4c1n4c10
```

Figura 93 - Creació directori Site PhP

Cal modificar els permisos d'aquesta nova carpeta:

```
atzucac@ctf4edu:/$ sudo chown -R atzucac:atzucac /var/www/c3ntr3d3v4c1n4c10/
```

Figura 94 - Canvi permisos carpeta Site

Cal crear el fitxer de configuració dels sites disponibles a l'Apache:

```
atzucac@ctf4edu:/var/www$ sudo nano /etc/apache2/sites-available/c3ntr3d3v4c1n4c10.conf_
```

Figura 95 - Configuració del Site per Apache

I es configura el *site* amb els paràmetres:

```
<VirtualHost *:8080>
        ServerName   c3ntr3d3v4c1n4c10
        ServerAlias  www.c3ntr3d3v4c1n4c10
        ServerAdmin  webmaster@localhost
        DocumentRoot /var/www/c3ntr3d3v4c1n4c10
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Figura 96 - Contingut c3ntr3d3v4c1n4c10.conf

Ara cal habilitar el host:

```
atzucac@ctf4edu:/var/www$ sudo a2ensite c3ntr3d3v4c1n4c10
Enabling site c3ntr3d3v4c1n4c10.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

Figura 97 - Habilitació nou site PHP

Tot seguit, cal activar la nova configuració:

```
atzucac@ctf4edu:/var/www$ sudo systemctl reload apache2
```

Figura 98 - Reiniciar servei Apache

Cal copiar tota la estructura del site a la carpeta corresponent:

```
┌──(kali㉿kali)-[~/ctf4edu/repte3/site]
└─$ scp *.* atzucac@192.168.0.41:/var/www/c3ntr3d3v4c1n4c10
atzucac@192.168.0.41's password:
autenticador.php
connexio.php
estils.css
index.php
tauler.php
```

Figura 99 - Copia del contingut a la carpeta del Site PHP

A continuació cal crear la base de dades i la taula usuaris:

```
atzucac@ctf4edu:~$ sudo mysql
```

Figura 100 - Connexió a MySQL

```
mysql> CREATE DATABASE ctf4edu;
Query OK, 1 row affected (0.02 sec)
```

Figura 101 - Creació BdD site PHP

Es crea un usuari **usuariweb** i se li assignen permisos complets sobre la base de dades ctf4edu

```
mysql> CREATE USER 'usuariweb'@'%' IDENTIFIED BY '4tz1c4c$1p3rS3cr3t';
Query OK, 0 rows affected (0.03 sec)
```

Figura 102 - Creació usuariweb BdD

```
mysql> GRANT ALL ON ctf4edu.* TO 'usuariweb'@'%';
Query OK, 0 rows affected (0.01 sec)
```

Figura 103 - Permisos usuariweb BdD

Tot seguit, cal sortir de mysql per tornar-hi a entrar amb les credencials d'usuariweb:

```
mysql> exit
Bye
atzucac@ctf4edu:~$ mysql -u usuariweb -p
```

Figura 104 - Reconnexió a MySQL com usuariweb

Cal crear la taula d'usuaris que es farà servir:

```
mysql> CREATE TABLE ctf4edu.usuaris ( id INT AUTO_INCREMENT, nomusuari varchar(50) NOT NULL, contras
enya varchar(50) NOT NULL, PRIMARY KEY(id));
Query OK, 0 rows affected (0.05 sec)
```

Figura 105 - Creació taula usuaris a MySQL

Cal afegir algun valor a la taula d'usuaris

```
mysql> INSERT INTO ctf4edu.usuaris (nomusuari,contrasenya) VALUES ("Elena","4k3st4s1k3sB0n4");
Query OK, 1 row affected (0.01 sec)
```

Figura 106 - Afegir usuari vàlid taula usuaris

Finalment, cal comprovar el funcionament de la pàgina del site i es donarà el repte per configurat:

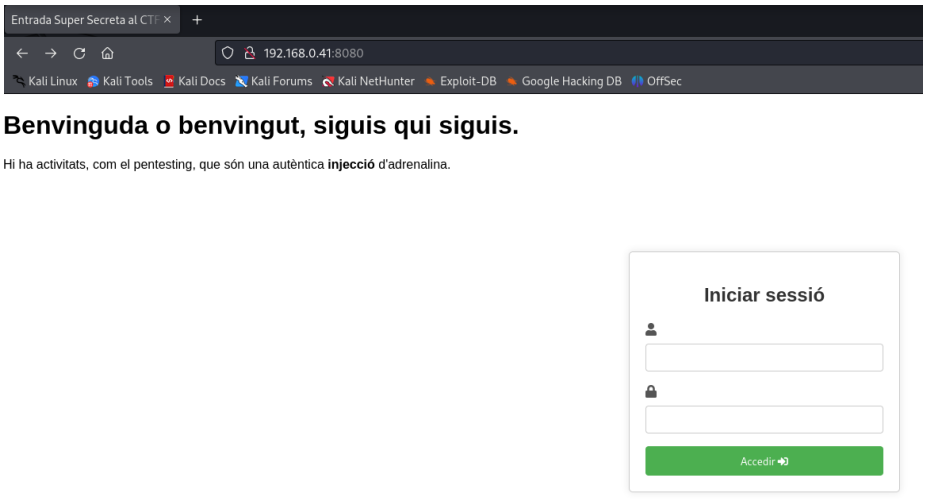


Figura 107 - Comprovació funcionament Login Site PHP

4.5.1 – *Writeup* Repte 3: visió del Red Team

Es recomanable començar creant una estructura de carpetes que permeti anar emmagatzemant la informació obtinguda o possibles fitxers i carpetes a estudiar. En aquest cas, es crea la carpeta repte3 dins de la carpeta ctf4edu.

Cal començar per descobrir la IP de la màquina-objectiu, ja que pot anar canviant. Així doncs, com que es coneix la xarxa on es troba, es crea la carpeta nmap i es llança un escaneig Nmap per a descobrir la seva IP desant el resultat al fitxer nmap/objectiu.

Figura 108 - Escaneig Nmap Repte3

Un cop finalitza, es pot observar que en aquest cas la màquina-objectiu té la IP 192.168.0.32 (cal recordar pel context de la història que és un equip Ubuntu)

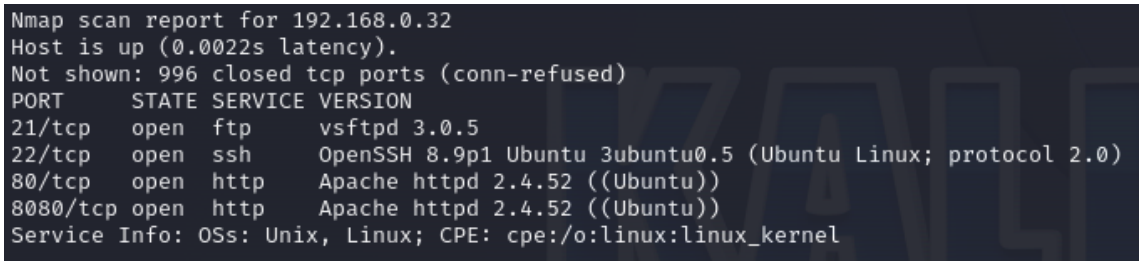


Figura 109 - Resultat Nmap Repte3

Cal notar que hi ha un servei web al port 8080 i que es pot procedir a investigar.

Per tant, es pot obrir un navegador web i accedir-hi a veure de què es tracta.

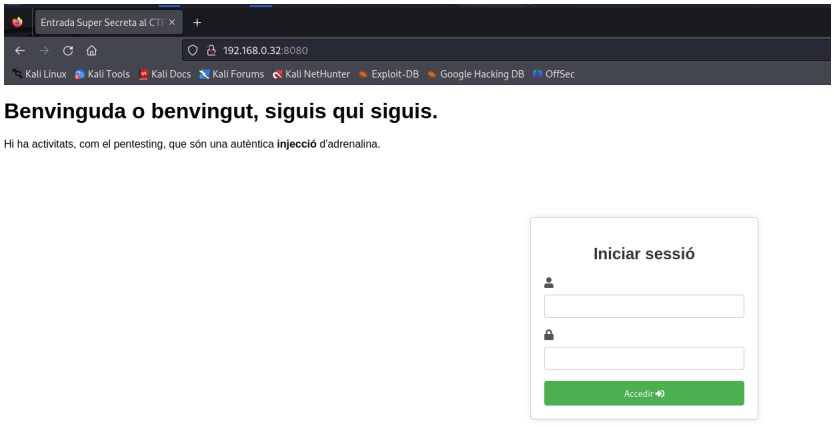


Figura 110 - Login Page PHP Repte3

A la pàgina d'identificació, es demana usuari i contrasenya. Es pot comprovar que cap de les més habituals (tipus admin – admin, admin – 1234, o bé altres combinacions no funcionen).

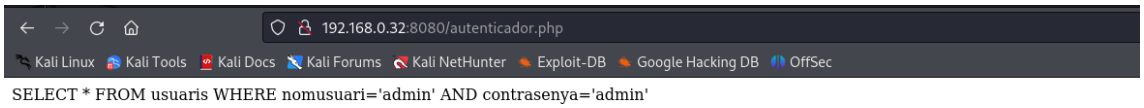


Figura 111 - Pàgina error - Autenticació Fallida Repte3

Aqui cal notar que de forma descuidada es mostra com es formula la consula a la base de dades.

Tornant a la pàgina d'identificació, és fàcil observar la pista "**injecció**" que evoca a utilitzar un atac d'injecció SQL (SQL Injection) per mirar d'accedir sense conèixer les credencials.

Un bon recurs pot ser conèixer o consultar diferents tipus de *payloads*[40] a utilitzar en injecció d'SQL, per utilitzar en diferents casos i per a diferents bases de dades.

En aquest cas concret, que es coneix com es llança la consulta per a validar les credencials, es pot usar un atac del tipus *Boolean-based (content-based) Blind SQLi*[41] és a dir, un atac d'injecció SQL cec basat en booleans.

Analitzant la consulta, es veu que es valida per separat el nom d'usuari i la contrasenya, i que òbviament coincideixin amb els que s'han introduit als camps corresponents.

Per coneixement de les taules de veritat de l'àlgebra de Boole, una igualtat del tipus "1 = 1" sempre retornarà CERT.

Aprofitant tot això, es pot intentar fer una càrrega (*payload*) d'injecció SQL que forci a la consulta a retornar CERT, fet que seria el mateix resultat de validar que usuari i contrasenya coincideixen amb els valors del registre de la base de dades.

Per a poder-ho aconseguir, cal analitzar adequadament la sintaxi de la consulta i veure que els valors dels paràmetres nomusuari i contrasenya es troben tancats entre cometes simples (').

També cal saber com "anul·lar" la validació de la contrasenya i aprofitant que es valida cada paràmetre per separat, podem afegir el simbol de comentari de la base dades (que no es coneix quina és ara per ara però fent una consulta al repositori de payloads, es factible fer-ho per assaig – error).

Així doncs, si es modifica adequadament el valor introduït en el camp nomusuari per afegir una cometa simple de tancament, una expressió lògica que retorni sempre cert i

[40] https://github.com/payloadbox/sql-injection-payload-list
[41] https://owasp.org/www-community/attacks/Blind_SQL_Injection

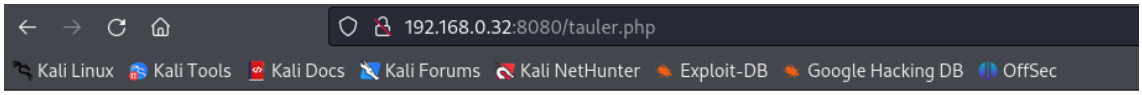
el símbol de comentari per tal que anul·li la validació del camp contrasenya, es podrà accedir sense conèixer les credencials.

Ràpidament es pot arribar a:

Figura 112 - Login Site amb Payload al camp nomusuari

On s'ha afegit ' OR 1 = 1 # just al darrera del nom d'usuari. Es pot utilitzar òbviament qualsevol altre nom d'usuari ja que qualsevol cosa o CERT sempre retornarà CERT. També cal obligatòriament escriure alguns caracters al camp de contrasenya però són indiferents ja que quedaran comentats i no es validarà la igualtat amb el valor del registre de la base de dades.

Al clicar al botó Accedir, es comprova efectivament que la injecció SQL ha estat un èxit.



Benvingut/da!

Figura 113 - Login correcte amb SQLi

De tota manera, només hi ha un missatge de benvinguda i res més.

Si s'inspecciona el codi font de la pàgina (clic amb el botó dret a un punt qualsevol de la pàgina) escollint la opció del menú contextual del navegador:

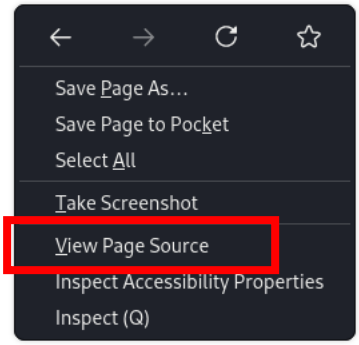


Figura 114 - Menú contextual Veure codi font

S'accedeix al codi font, on hi ha un missatge, la flag i unes credencials.

```
<!DOCTYPE html>
<html lang="ca">
<head>
    <meta charset="UTF-8">
    <title>Benvinguda</title>
</head>
<body>
    <div>
        <h1>Benvingut/da!</h1>
        <!--
          Ei,

          Ja t'he deixat llesta la maqueta del site. Ara caldria completar el codi i això ho has de fer tu.

          Hauríem de tenir llesta la part del tauler de la web com a molt tard el 01/01/2024!

          Et deixo les meves credencials perquè allà hi tinc material que potser et fa falta.

          Sobretot, no les passis a ningú, ok? Que ja prou forats de seguretat té el servidor aquest...

          Salut!

          usuari: david / p@wd: Tr1c3r4t0p$

          ctf4edu_flag{J4t3nsl4Ll1m0n4P3rL3sc0rb1t}
        -->
    </div>
</body>
</html>

```

Figura 115 - Codi Font Pàgina amb flag i credencials

4.6 – Repte 4: Esteganografia i ocultació d'informació

Aquest repte s'inicia descarregant una imatge[42] de Girona d'internet que servirà de base per anar ocultant informació.

Es genera la flag i es desa a un fitxer de text.

```
┌──(kali㉿kali)-[~]
└─$ echo ctf4edu_flag{J4t3nsL4rtD0c1lt4rM1ss4tg3s} > bandera.txt
```

Figura 116 - Preparació Flag Repte 4

[42] https://stock.adobe.com/es/images/colorful-yellow-and-orange-houses-and-famous-house-casa-maso-reflected-in-water-river-onyar-in-girona-catalonia-spain-church-of-sant-feliu-and-saint-mary-cathedral-at-background/103316544?prev_url=detail - Autor: Kavalenkava - Llicència estàndard no comercial

S'oculta a l'interior de la imatge la flag usant Steghide[43] que és un programa que permet fer aquesta ocultació de la informació en formats d'imatge i audio. I es protegeix amb una clau (*passphrase*).

```
┌──(kali㉿kali)-[~]
└─$ steghide embed -cf girona.jpg -ef bandera.txt -p "Tell me and I forget. Teach me and I remember. Involve me and I learn"
embedding "bandera.txt" in "girona.jpg"... done
```

Figura 117 - Ocultació flag dins imatge

S'utilitza l'eina Exiftool[44] que permet escriure a les metadades dels fitxers indicant el *tag* que es vol editar. Per exemple es mostra com s'afegeix el tag del comentari que fa de pista.

```
┌──(kali㉿kali)-[~]
└─$ exiftool -comment="passphrase⇒Tell me and I forget. Teach me and I remember. Involve me and I learn" girona.jpg
    1 image files updated
```

Figura 118 - Ocultació pistes metadades imatge

Es vol donar una pista extra per qui tingui bon ull. S'afegeix el tag autor de la imatge indicant el nom del programa utilitzat però en el format nom i cognom, com si fos una persona: "Steg Hide".

```
┌──(kali㉿kali)-[~]
└─$ exiftool -author="Steg Hide" girona.jpg
```

Figura 119 - Pista extra Repte4

Finalment s'executa altre cop ExifTool i es comprova que les dues pistes han quedat incorporades a les metadades:

```
┌──(kali㉿kali)-[~]
└─$ exiftool girona.jpg
ExifTool Version Number         : 12.67
File Name                       : girona.jpg
Directory                       : .
File Size                       : 1918 kB
File Modification Date/Time     : 2023:12:02 16:44:37-05:00
File Access Date/Time           : 2023:12:02 16:44:43-05:00
File Inode Change Date/Time     : 2023:12:02 16:44:37-05:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
XMP Toolkit                     : Image::ExifTool 12.67
Author                          : Steg Hide
Comment                         : passphrase⇒Tell me and I forget. Teach me and I remember. Involve me and I learn
Image Width                     : 4500
Image Height                    : 3000
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 4500×3000
Megapixels                      : 13.5
```

Figura 120 - Metadades imatge amb pistes

[43] Steghide: https://steghide.sourceforge.net/
[44] ExifTool: https://exiftool.org/

També es concatena al final del fitxer de la imatge un text pla, donant una pista doble: que la informació del propi repte és a prop (s'està seguint la guia correcta) i alhora, que pel proper repte cap continuar-lo per la carpeta anomenada **...**

Figura 121 - Pista doble concatenada a la imatge

4.6.1 – *Writeup* Repte 4: visió del Red Team

Cal començar el repte sabent la IP de la màquina-objectiu, que en el moment de fer aquest writeup és 192.168.0.32. En cas necessari, reviseu el detall de com fer-ho als reptes anteriors.

Com que del repte 3 es tenen les credencials d'un usuari del servidor ctf4edu, des del terminal del Kali es poden usar per a establir una connexió:

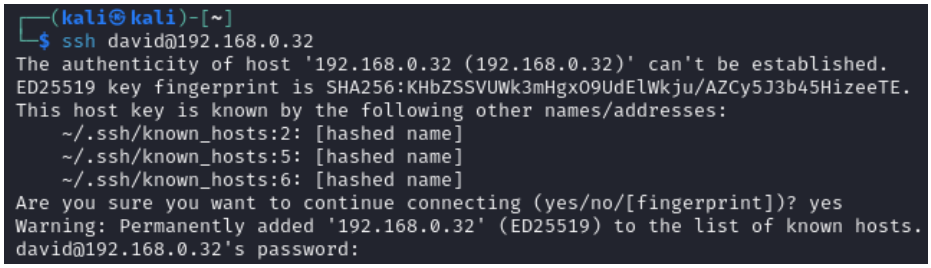


Figura 122 - Connexió a CTF4Edu per SSH

Pocs segons després ja hi estarem connectats:

Figura 123 - Sessió iniciada com a david a CTF4Edu

Es pot executar una comanda ls:

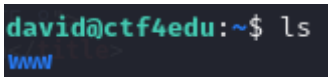


Figura 124 - Contingut /home/david a CTF4Edu

I això permet descobrir una carpeta anomenada "www". Seguint el repte 3, podria ser l'estructura o la web de la que parlava el missatge. Caldrà investigar.

S'accedeix a la carpeta i es verifica el contingut:

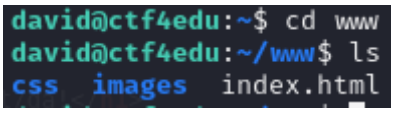


Figura 125 - Contingut directori WWW

Tot apunta que és una web.

Per a poder investigar més tranquilament, es copia tot el contingut de la carpeta www a la nostra màquina Kali. S'obre un altre terminal i s'executa:

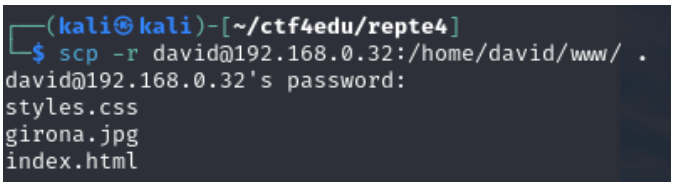
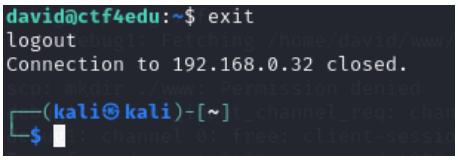


Figura 126 - Copia del directori www a màquina atacant

Un cop copiat, es tanca la connexió amb ctf4edu, per seguretat.



Es comprova la còpia i s'activa un senzill servidor http per a poder veure la pàgina que ens hem copiat localment a la nostra màquina atacant i pel port 80, aprofitant un dels mòduls que ja incorpora Python 3[45]:

Figura 127 - Inici de Simple Servidor HTTP

Obrint un navegador es pot visualitzar el contingut de la pàgina:

[45] https://docs.python.org/3/library/http.server.html

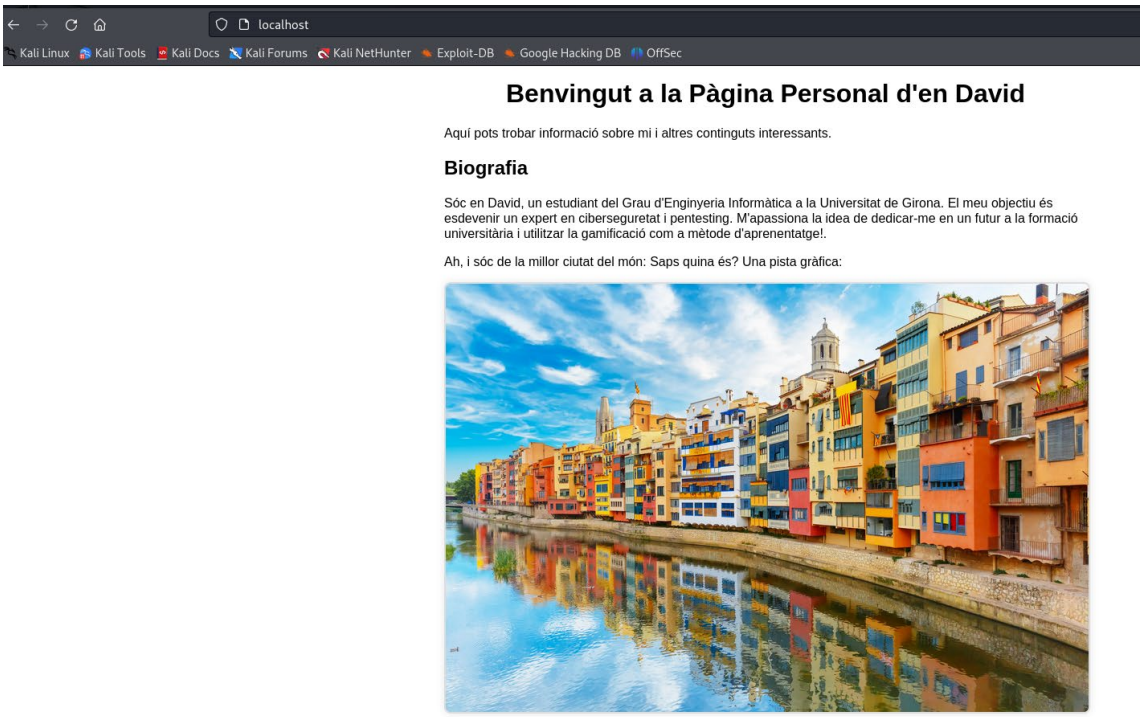


Figura 128 - Site www en local per investigar

Es descarrega la imatge per posterior estudi.

Figura 129 - Imatge de Girona descarregada

Aparentment, tal i com es veu a la web la imatge sembla normal però si es cerca a les metadades, amb una eina com ExifTool:

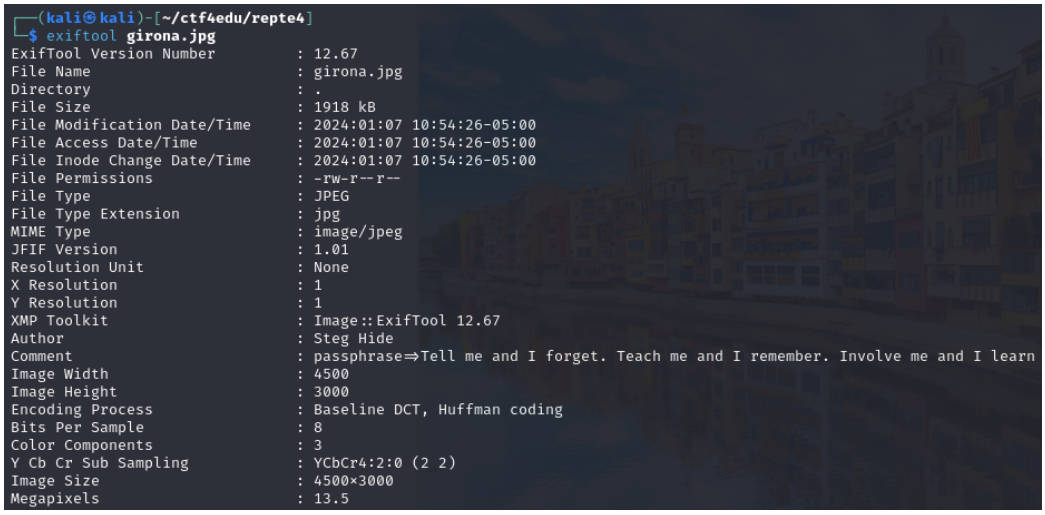


Figura 130 - Metadades de foto de Girona

Es poden trobar unes metadades que criden l'atenció com una *passphrase* a comentaris i que la imatge és d'un autor anomenat Steg Hide.

Fent una cerca de Steg Hide a un cercador web com Google suggereix que potser es volia dir Steghide escrit tot junt:

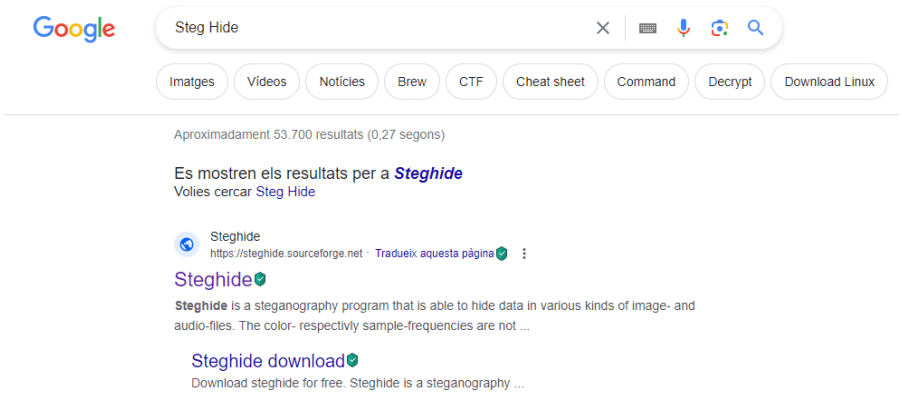


Figura 131 - Cerca de qui es Steg Hide

Analitzant el programa parla de que s'usa per esteganografia, per ocultar fitxers dins d'imatges. Potser això és la clau.

Aplicant Steghide a la imatge de girona.jpg, demana una passphrase:

```
┌──(kali㉿kali)-[~/ctf4edu/repte4]
└─$ steghide extract -sf girona.jpg
Enter passphrase:
```

Figura 132 - Steghide a la foto de Girona

Introduint la que s'ha obtingut de les metadades:
Tell me and I forget. Teach me and I remember. Involve me and I learn

S'informa que acaba d'extreure el fitxer bandera.txt

```
┌──(kali㉿kali)-[~/ctf4edu/repte4]
└─$ steghide extract -sf girona.jpg
Enter passphrase:
wrote extracted data to "bandera.txt".
```

Figura 133 - Extracció de fitxer ocult a la imatge

Observant el contingut de bandera.txt:

```
┌──(kali㉿kali)-[~/ctf4edu/repte4]
└─$ cat bandera.txt
ctf4edu_flag{J4t3nsL4rtD0c1lt4rM1ss4tg3s}
```

Figura 134 - Obtenció Flag Repte4

Si es continua examinant la imatge, a la recerca de cadenes de text afegides o embegudes:

Figura 135 - Missatge concatenat al final imatge

Es pot trobar al final de tot, una pista pel següent repte

Figura 136 - Pista pel seguent repte ...

4.7 – Repte 5: Enginyeria Inversa

Cal començar creant un codi font amb llenguatge C++ que simplement demana una resposta en forma d'entrada de teclat per part de l'usuari, fa una comparació de cadenes de text i si coincideixen, mostra la bandera. (Codi font a l'annex 8.8)

Un cop desenvolupat el codi font, cal compilar el programa:

Figura 137 - Compilació elxefendevi

Cal crear l'estructura de carpetes a /home/david del servidor ctf4edu.

Figura 138 - Creació estructura de carpetes a CTF4Edu

Cal crear la carpeta elxefendevi i copiar-hi al seu interior el fitxer compilat.

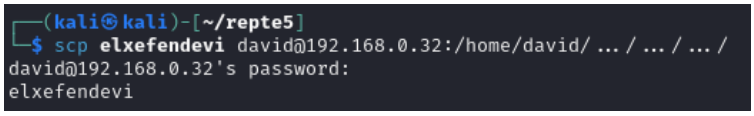


Figura 139 - Creació carpeta elxefendevi

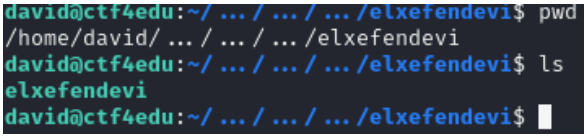


Figura 140 - Copia del programa compilar a CTF4Edu

Tot seguit es crea un fitxer de text (benvist.txt) per donar una pista de que una solució és aplicar enginyeria inversa.

4.7.1 – *Writeup* Repte 5: visió del Red Team

Cal connectar a ctf4edu amb les credencials de l'usuari david.

Cal executar un ls -alis per a poder veure tots els documents i directoris:

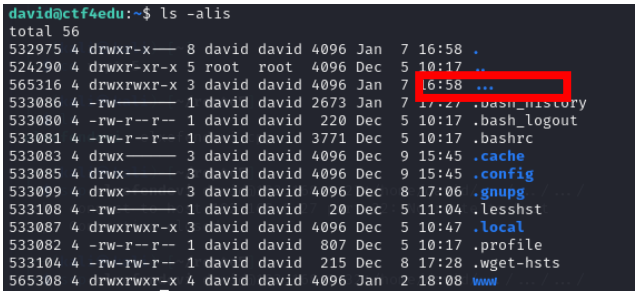


Figura 141 - Detall del directori ...

Cal fixar-se en l'existència del directori ... Llavors cal accedir-hi.

Successivament es va trobant, fins a tres vegades, directoris anomenats ...

Llavors, s'arriba a un directori on es troba un fitxer anomenat benvist.txt:

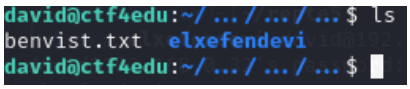


Figura 142 - Troballa de benvist.txt

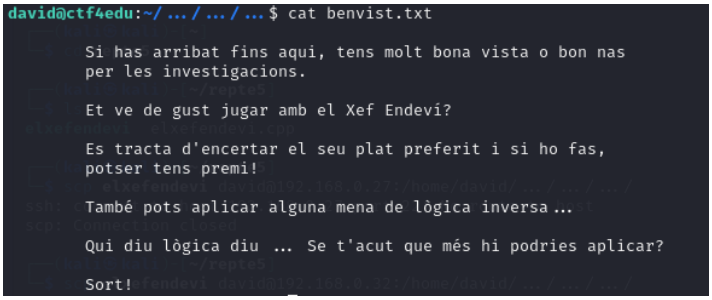


Figura 143 - Contingut de benvist.txt

Cal accedir al directori "elxefendevi" i al seu interior s'hi troba un fitxer executable:

Cal executar el fitxer:

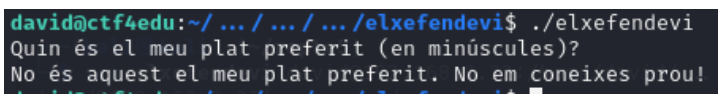


Figura 144 - Execució del binari elxefendevi

Es pot observar que si no es coneix el nom del plat, la solució d'escriure qualsevol cosa serà poc eficient.

Cal copiar l'executable per analitzar-lo des de la nostra màquina atacant.

Figura 145 - Copia del binari a la màquina atacant

Ara cal analitzar el binari. Es pot usar un programa com ghidra[46]. Ghidra està desenvolupat per la NSA[47] i és un conjunt d'eines que permeten, donat un codi compilat, desensamblar-lo, analitzar-lo, trobar-hi informació, etc.

Cal executar ghidra amb el programa elxefendevi

Figura 146 - Execució de Ghidra

Cal crear un nou projecte, donar-li un nom i una carpeta per començar a analitzar el binari. Cal clicar finalment a finish

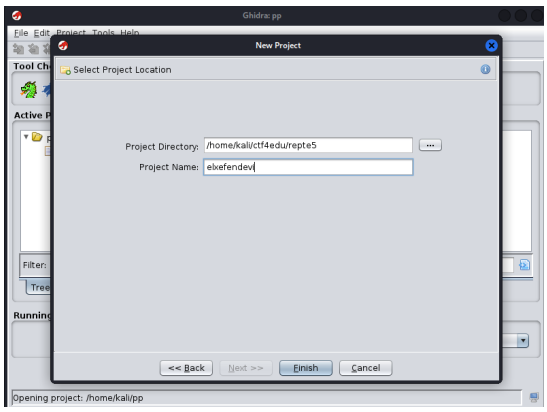


Figura 147 - Execució de Ghidra - Projecte

Quan apareix la finestra del projecte cal importar el binari al projecte. Cal fer clic a File > Import File... i escollir el binari.

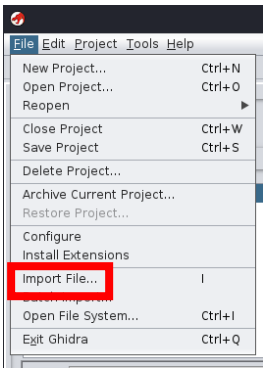


Figura 148 - Com importar binari a Ghidra

[46] https://ghidra-sre.org/
[47] https://www.nsa.gov/

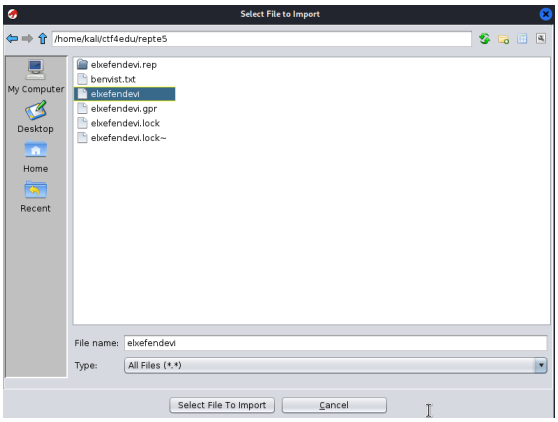


Figura 149 - Escollir binari del directori per importar

El propi programa ja infereix les dades per defecte, però com es veu si es volgués es podria canviar algun paràmetre i/o opció. Per aquest repte, cal deixar-ho per defecte.

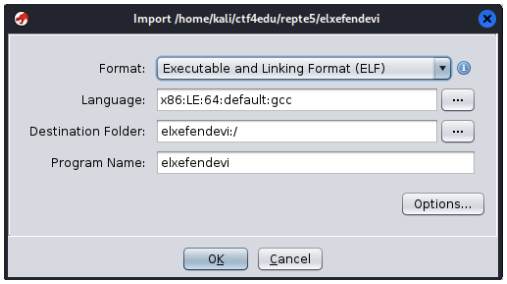


Figura 150 - Configuracions de Ghidra

Un cop importat el binari, cal iniciar el *CodeBrowser* fent clic a la icona de l' Hidra.

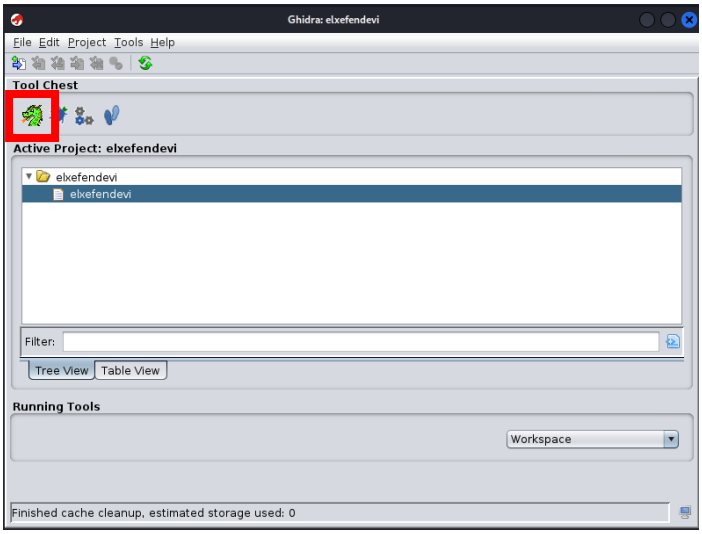


Figura 151 - Icona de l'accés a CodeBrowser Ghidra

El primer cop que s'obre un binari a un projecte ens pregunta si es desitja que l'analitzi. Cal contestar afirmativament.

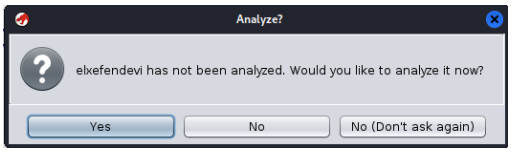


Figura 152 - Diàleg analisi per primer cop binari

A les opcions d'anàlisi, es recomana per aquest repte deixar-los per defecte:

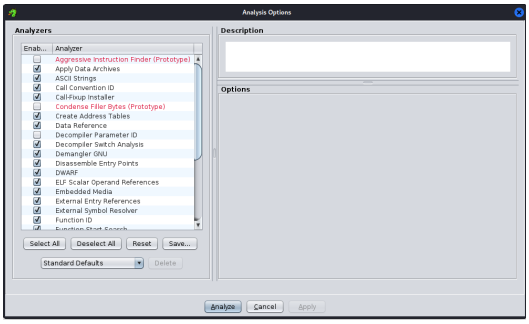


Figura 153 - Opcions d'analisi de Ghidra

Un cop l'anàlisi finalitza, apareix l'aplicació i les diferents finestres on hi ha el codi assemblador, etc.

Cal anar al menú Window > Defined Strings.

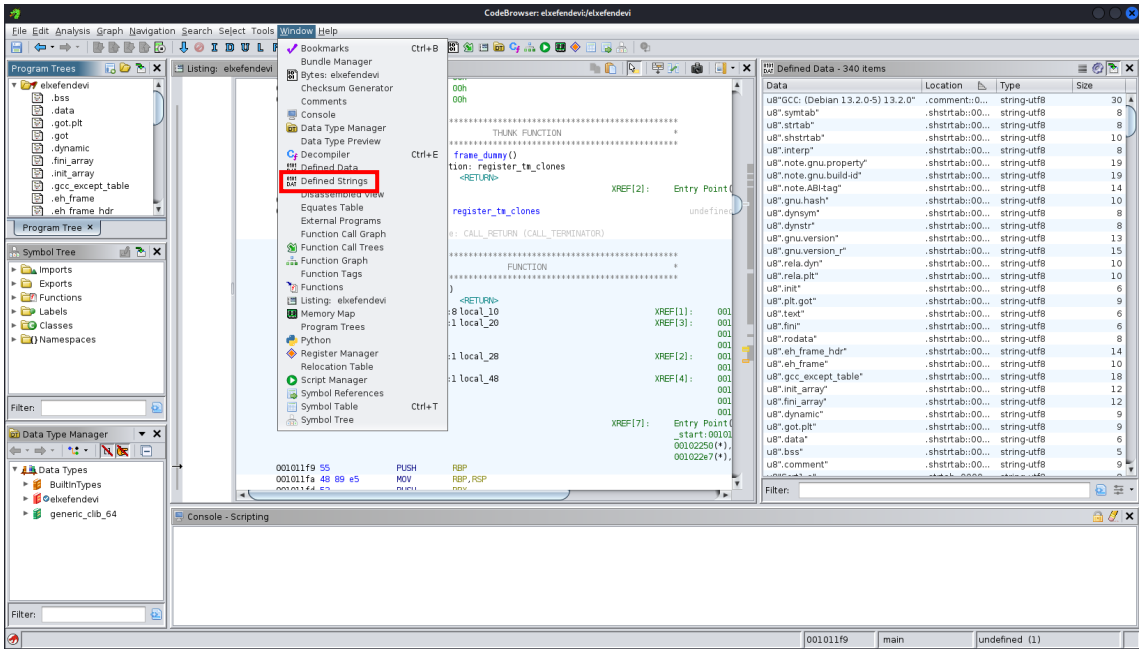


Figura 154 - Ghidra en execució

Això obre una subfinestra on apareixeran possibles cadenes de text que ghidra ha trobat en el procés d'analis.

Si es revisa la subfinestra de Defined Strings es pot trobar el nom del plat preferit de elxefendevi: "**escudella**".

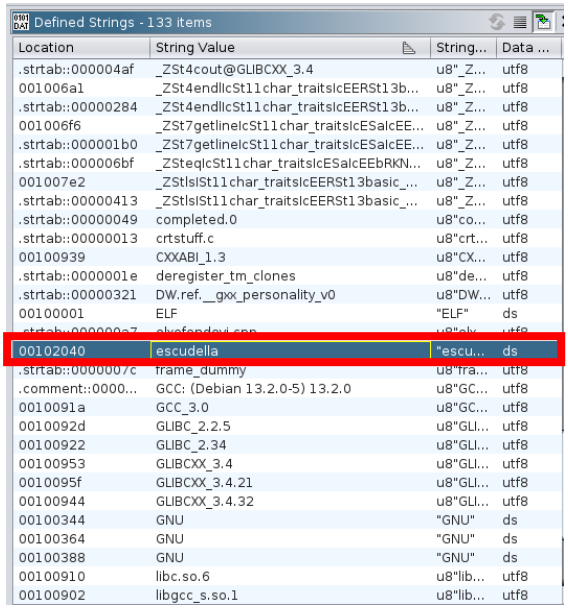


Figura 155 - Detall de la cadena trobada al binari

Amb aquesta informació, es pot tornar a executar el binari i obtenir el premi: la flag del repte.

```
david@ctf4edu:~/ ... / ... / ... /elxefendevi$ ./elxefendevi
Quin és el meu plat preferit (en minúscules)?escudella
Molt bé! ⇒ ctf4edu_flag{JaT3nsG4n4S1p0s0}
david@ctf4edu:~/ ... / ... / ... /elxefendevi$
```

Figura 156 - Execució del xefendevi amb resposta correcta

4.8 – Repte 6: Tipus de Fitxers Obscurs, xifratge i ocultació en text massiu

En aquest repte s'utilitzarà en algun moment el sistema de substitució ROT47, que es basa en ROT13[48].

Es codifica el nom del sistema "ROT47" aplicant la funció de hash md5[49]:

```
┌──(kali㉿kali)-[~/repte6]
└─$ echo -n 'ROT47' | md5sum
fc99bde0ad8831760632e4c4593250c5
```

Figura 157 - Codificació en md5

Es codifica amb ROT47 la flag del repte usant el servei web CyberChef[50] que serveix sobretot per a poder aplicar diferents patrons, funsions de hash, sistemes de codifinació, etc. encadenats un darrera l'altre i en un determinat ordre, com els passos d'una recepta de cuina (d'aqui el nom de CyberChef).

[48] https://en.wikipedia.org/wiki/ROT13
[49] https://en.wikipedia.org/wiki/MD5
[50] https://gchq.github.io/CyberChef/

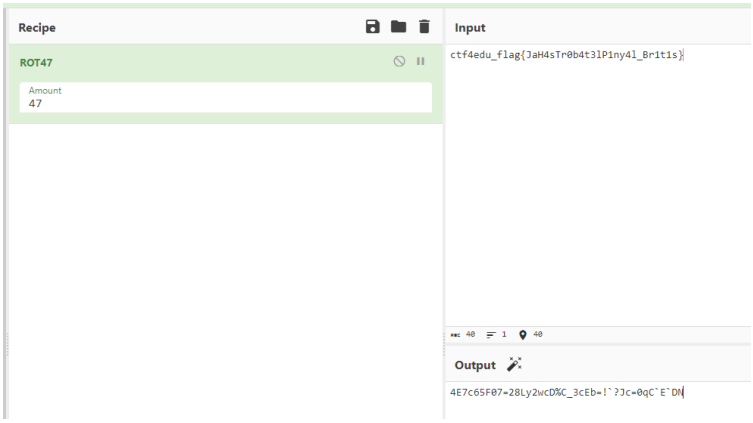


Figura 158 - CyberChef en execució

Cal descarregar d'internet un fitxer de text gran, massiu amb moltes linies i molt de contingut. S'escull una barreja de text tipus "Lorem Ipsum" que està escrit en llatí. Se l'anomena "biblia.txt".

Cal editar el fitxer "bíblia.txt". A la línia 1980, s'hi escriu una frase en llatí que significa "L'agulla no té cervell", la codificació de la flag ROT47 i una pista pel proper repte (La clau per obrir la cripta és B00k0fK3lls)

Acus non habet cerebrum => 4E7c65F07=28Ly2wcD%C_3cEb=!`?Jc=0qC`E`DN /// {24=2F A6C @3C:C =2 4C:AE2 éD q__<_7zb==D

Cal desar en un fitxer comprimit ZIP el contingut del fitxer sistemadecodificacio.txt que conté el mot ROT47 codificat amb md5. Cal protegir el ZIP amb una contrasenya, que és "escudella" (enllaçant amb l'anterior repte).

Figura 159 - S'encapsula en un ZIP el fitxer

Cal protegir el ZIP amb una contrasenya, que és "escudella" (enllaçant amb l'anterior repte).

Cal crear el directori "elfrarellatí" a ctf4edu des de l'usuari david a:

/home/david/.../.../.../elfrarellati

Cal copiar dins el directori del ctd4edu els fitxers generats per aquest repte:

Figura 160 - Copia de fitxers al directori elfrarellati

Es crea en aquest directori un fitxer de text pla (recepta.txt) amb una pista.

4.8.1 – *Writeup* Repte 6: visió del Red Team

Es connecta a ctf4edu amb les credencials de david.

S'observa que hi ha el directori "elfrarellati" al mateix nivell de directori que el repte anterior: /home/david/.../.../...

S'accedeix al directori i s'executa un "ls -alis"

Figura 161 - Vista del contingut directori elfrarellati

Es comença a mirar el contingut del fitxers de text. L'anomenat biblia.txt és un fitxer de text llarguíssim, aparentment tot en llatí.

El fitxer recepta.tx s'hi observa:

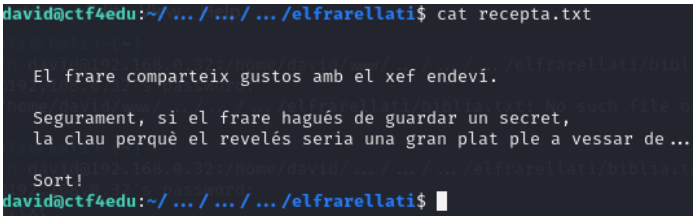


Figura 162 - Contingut fitxer recepta.txt

Amb la resolució de l'anterior repte s'obtenia que el plat preferit era "escudella".

S'observa el fitxer "cartell.pdf":

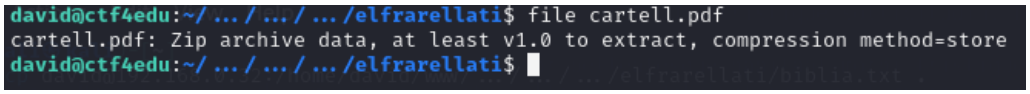


Figura 163 - Analisi del fitxer cartell.pdf

Es veu que no és realment un PDF sinó un fitxer Zip. Es una bona idea copiar tot el contingut a l' equip atacant i continuar investigant.

Figura 164 - Copia de tot el contingut a la màquina atacant

Un cop copiat. Es continua treballant amb cartell.pdf. Es canvia la extensió a .zip ja que li correspon i s'intenta descomprimir.

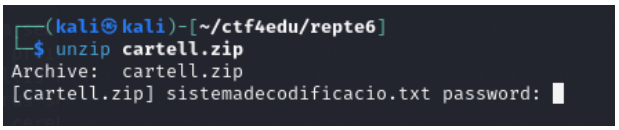


Figura 165 - Intent de descomprimir cartell.pdf

El missatge diu que el frare i el xef comparteixen gustos, així que s'intenta usar "escudella" com a password.

Figura 166 - Descompressio del contingut de cartell.zip

Funciona. Ara hi ha un nou fitxer anomenat sistemadecodificacio.txt. Es mira el contingut:

Figura 167 - Contingut de sistemadecodificació.txt

Sembla algun tipus de hash o de codi. Es recorda la pista de la història del repte que parla de "Crack Station". CrackStation[51] és una pàgina web que permet trencar diversos tipus de hash.

Efectivament, posant el hash a CrackStation es veu que era de tipus md5 i que el valor original era "ROT47".

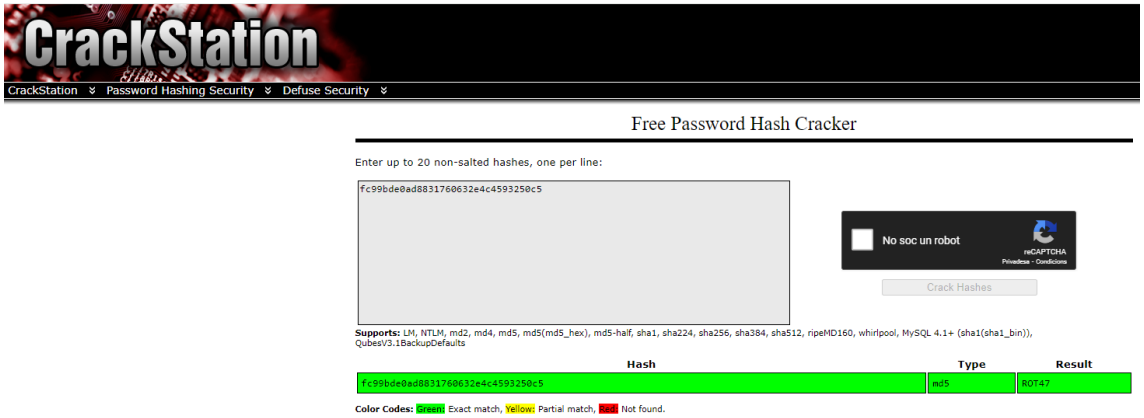


Figura 168 - La pàgina CrackStation trencant el hash md5

Segurament, alguna cosa cal fer amb el fitxer de bíblia.txt. També es recorda que hi havia una pista a la història, una frase en llatí "Cerebrum non habit".

S'usa la comanda grep per a cercar i extreure només les línies que tinguin coincidència amb la paraula "Cerebrum".

[51] https://crackstation.net/

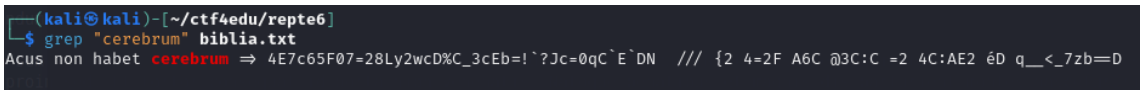


Figura 169 - Resultat de cercar "Cerebrum" a biblia.txt

Realment apareix. Hi ha coincidencia i a continuació, una cadena de caracters que no semblen llatí.

Abans s'ha trobat ROT47 com a pista. ROT47 és un tipus de xifrage de transposició basat en ROT13[52], que al final és un xifratge de Cesar on cada lletra original és substituida per la lletra o el caracter 47 posicions més endavant de l'alfabet de símbols del sistema. Podria ser, doncs que el missatge estés xifrat amb ROT47 i per tant, aplicant-lo inversament, s'obtindrà el text original.
S'usa l'eina CyberChef per a fer-ho:

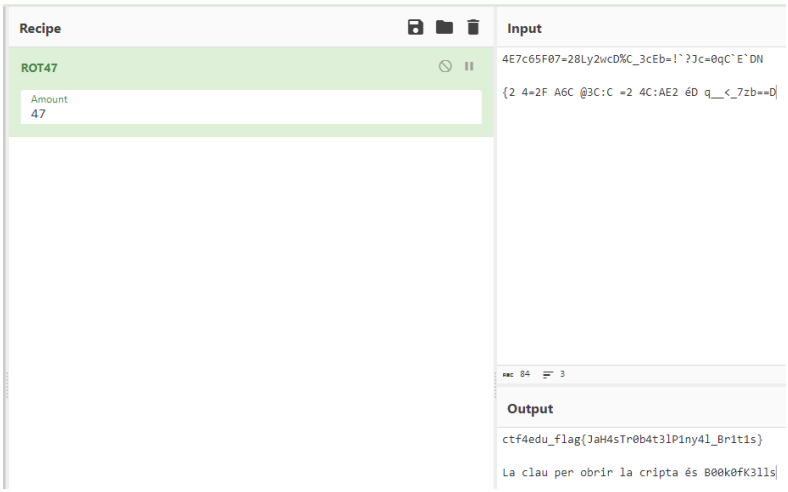


Figura 170 - Us de CyberChef per invertir missatge ROT47

S'obté la flag i una pista.

4.9 – Repte 7: Atacs de força bruta i obtenció de credencials

Es crea el directori ".cripta" a /home/david/.../.../...

Figura 171 - Creació carpeta .cripta

Es generen dos fitxers de text "credencials" i "idusuari". Al fitxer credencials s'hi posen una sèrie de passwords i al d'idusuari, una llista de possibles noms d'usuari.

[52] https://en.wikipedia.org/wiki/ROT13

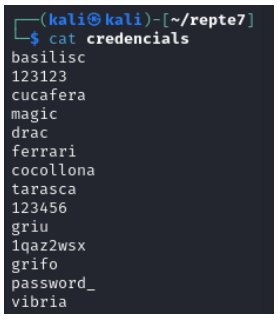


Figura 172 - Fitxer credencials

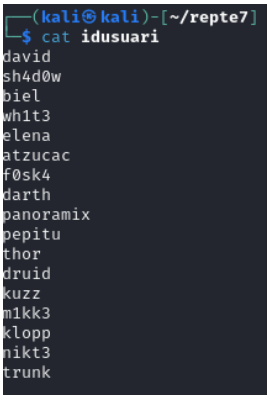


Figura 173 - Fitxer idusuari

Es comprimeixen els dos fitxers a un fitxer ZIP anomenat S1p3rS3cr3t.zip i protegit pel password: “@thebesthacker_intheworld”.

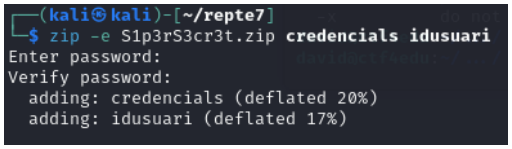


Figura 174 - Compressió amb password dels fitxers de credencials

S’afegeix el fitxer S1p3rSecret dins d’un fitxer ZIP anomenat S3cr3t.zip i protegit pel password “B00kOfK3lls” (del repte anterior)

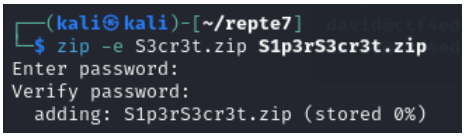


Figura 175 - Compressió del fitxer comprimit amb un altre password

Es copia el fitxer S3cr3t.zip a la carpeta .cripta de ctf4edu.

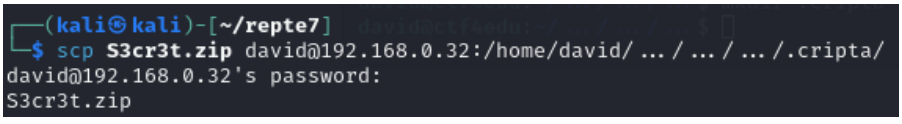


Figura 176 - Es copia a la carpeta .cripta el fitxer comprimit

Es crea un document de text a /home/f0sk4/bandera.txt amb la flag:

ctf4edu_flag{J4H4sTr0b4tlaP0rt4F0sk4}

4.9.1 – *Writeup* Repte 7: visió del Red Team

Es connecta a ctf4edu amb l'usuari david. Cal situar-se al directori: /home/david/.../.../...

Figura 177 - Accés al directori on hi ha .cripta

S'executa un "ls -alis" i s'observa un directori ocult anomenat .cripta. S'hi accedeix. S'executa tot seguit un "ls".

Figura 178 - Contingut directori .cripta

Es troba un fitxer ZIP, que es copia a la maquina atacant per a posterior analisi.

Figura 179 - Copia del fitxer comprimit a la màquina atacant

S'intenta descomprimir

Figura 180 - Intent de descomprimir el Zip

Demana un password. Cal recordar que el repte anterior s'ha obtingut una pista, quan s'ha descobert la flag: "La clau per obrir la cripta és B00k0fK3lls". S'utilitza aquest password.

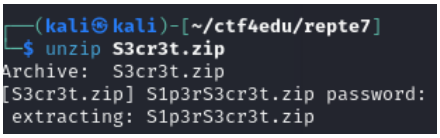


Figura 181 - Descompressió del fitxer amb pista

Funciona i s'observa que acaba d'extreure un altre fitxer ZIP anomenat "S1p3rs3cr3t.zip". S'intenta extreure:

Demana password. S'intenta "B00k0fK3lls" però no funciona:

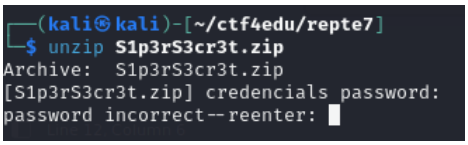


Figura 182 - Descompressió fallida

En aquest punt, es proposa dur a terme un atac de força bruta amb John The Ripper[53], que és una eina de codi obert i que serveix per a fer auditories de seguretat i per a recuperar contrasenyes, entre d'altres.

Cal extreure el hash del zip per intentar posteriorment trencar-lo i descobrir el password.

John the ripper té diverses utilitats per a diferents programes o tipus d'arxiu. Com que es disposa d'un Zip, caldrà usar la utilitat zip2john per extreure el hash i desar-lo en un fitxer de text anomenat hashzip.txt

Figura 183 - Zip2john extraien el hash del zip

Ara ja es pot intentar de trencar el password mitjançant un atac de força bruta. John the Ripper disposa d'un llistat de possibles passwords i que s'obté de llistes conegudes: els passwords més utilitzats, els que s'han filtrat alguna vegada de dades exposades, etc. Tanmateix, hi ha una llista de credencials especial i coneguda anomenada rockyou.txt[54] que conté una extensa col·lecció de possibles passwords.

Per tant, s'utilitza aquesta:

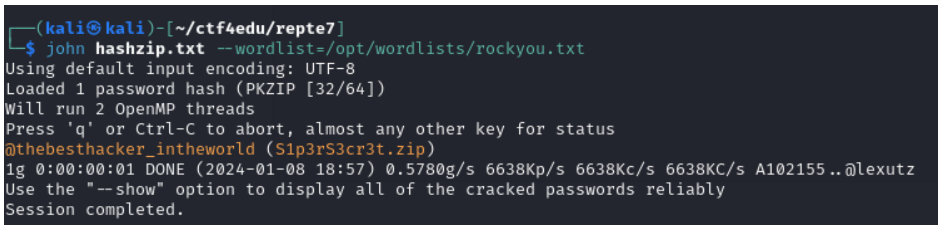


Figura 184 - John The Ripper amb RockYou per trencar el hash

S'ha tingut sort, i aquest ZIP utilitzava una contrasenya que pertanyia a la wordlist i John the ripper l'ha trobat i ens l'ofereix. En cas que no hagués funcionat, es podria intenta amb altres wordlists baixades d'internet, per exemple.

S'extreu el fitxer usant el password trobat per John The Ripper:

[53] https://www.openwall.com/john/
[54] https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

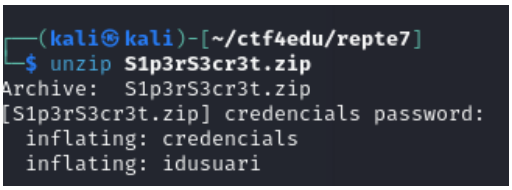


Figura 185 - Extracció del contingut del Zip

S'obtenen dos fitxers. Es mira què contenen.

Figura 186 - Fitxer credencials

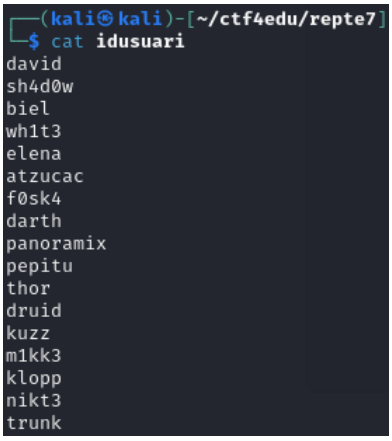


Figura 187 - Fitxer idusuari

Tot apunta a que s'ha trobat una possible llista de usuaris (idusuaris) i una possible llista de credencials. Estaven tan amagades i aparentment protegides que es pot pensar que totes o com a mínim alguna pot ser una credencial d'un usuari actiu. Per tant, s'intentarà dur a terme un atac de força bruta per accés SSH al servidor ctf4du amb les les dues llistes d'usuaris i credencials obtingudes. Per a dur a terme aquesta tasca, ara s'usarà una altra eina, hydra[55]

Hydra permet usar diferents *threads* en paral·lel (és a dir que és capaç d'atacar en diversos processos de forma concurrent).

Recapitulant, es disposa del coneixement de quin protocol atacar (SSH), la IP de la màquina-objectiu, les possibles llistes d'usuaris i passwords així que s'intenta esbrinar si algun d'aquests usuaris és actiu.

[55] https://www.kali.org/tools/hydra/

S'executa la comanda hydra amb els paràmetres anteriors:

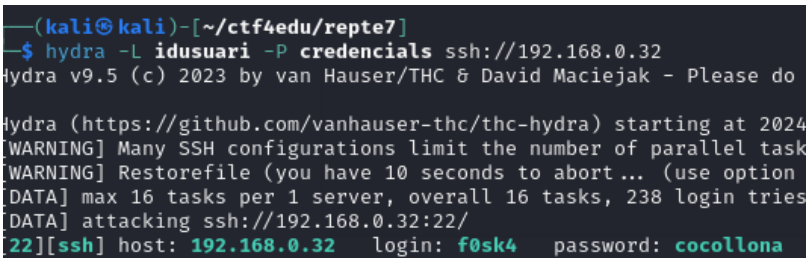


Figura 188 - Atac de força bruta per SSH amb Hydra

Es troba una parella d'usuari i password: **f0sk4** / **cocollona**

S'intena usar les noves credencials per accedir a ctd4edu via SSH:

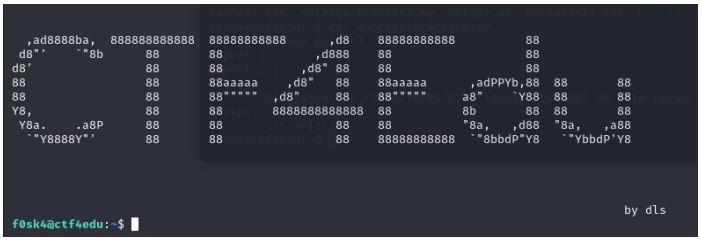


Figura 189 - Accés a CTF4Edu com a f0sk4

Es comprova que efectivament s'hi té accés.

Fent un ls, trobem el fitxer bandera.txt:

Figura 190 - Obtenció flag repte 7

4.10 – Repte 8: Escalada de privilegis explotant CronJobs

Es crea el directori pràctiques a /home/f0sk4

Es crea la ruta de directoris:
/UdG/EnginyeriaInformatica/Practiques/SeguretatXarxesComputadors

Es crea un document fals simulant una practica per un alumne:

Figura 191 - Document simulant practica copiada

Es crea l'script en python per esborrar directori /practiques:

```
f0sk4@ctf4edu:~$ cat neteja.py
#!/usr/bin/env python3
import os
import sys
try:
        os.system('rm -r /home/f0sk4/practiques/* ')
except:
        sys.exit()
```

Figura 192 - Script per esborrar carpeta pràctiques

Es crea l'script en python per entregarPractiques:

```
f0sk4@ctf4edu:~$ cat entregarPractica.py
#!/usr/bin/env python3
import os
import sys
try:
        os.system('cd /home/f0sk4/practiques/; python3 -m http.server 9090')
except:
        sys.exit()
```

Figura 193 - Script per sistema entrega practiques

Es crea un fitxer de text amb una pista:

```
f0sk4@ctf4edu:~$ cat perlaf0sk4.txt

   f0sk4, recorda com funciona la nostra "pizzeria" de Pràctiques

   1) Verifica que ens han fet el Bizum amb el concepte "Sopar Ahir xxx"

   2) Avisa a xxx que estigui davant un terminal per descarregar la practica (ip_ctf4edu:9090)

   3) Copia la practica d'altres anys dirigida a xxx a la carpeta /practiques

   4) executa ./entregarPractica.py (Això obre un servidor http al port 9090)

   5) avisa a xxx que a partir d'aquest missatge té 5 minuts! per a descarregar la practica.

   6) Al cap de 5 minuts la pràctica s'esborra automàticament
      (he programat que el teu script per esborrar el directori s'executi cada 5 minuts ;-))


                        Root.
```

Figura 194 - Pista Repte 8

Es crea la bandera de root

ctf4edu_flg{4r4J43tsR00td3l_CTF4edu_F3l1c1t4ts!}

4.10.1 – *Writeup* Repte 8: visió del Red Team

Es connecta a ctf4edu amb les credencials de f0sk4 obtingudes al repte anterior. S'executa "ls -alis"

```
f0sk4@ctf4edu:~$ ls
bandera.txt  entregarPractica.py  neteja.py  perlaf0sk4.txt  practiques  UdG
f0sk4@ctf4edu:~$
```

Figura 195 - Contingut directori /home/f0sk4

S'observa el contingut de perlaf0sk4.txt:

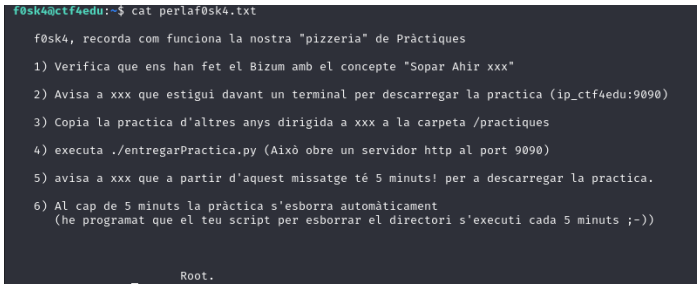


Figura 196 - Missatge perlaf0sc4.txt

S' explica com es té muntat tot el tema del servidor de pràctiques plagiades
També s'indica que Root, que es qui escriu el missatge ha programat l'execució d'un script de pyton de la f0ska per tal que s'executi cada 5 minuts.

Això evoca a una tasca de Cron[56] que és una utilitat del sistema operatiu per a programar tasques de forma automatitzada. Per a poder-ho fer, cal introduir cada tasca a la taula crontab que hi ha al directori /etc. El fitxer està tabulat indicant a la primera columna els minuts, la segona les hores, la tercera el dia del mes, etc. I així, introduint els valors que es necessitin amb el format adequat es pot anar fent la programació dels binaris / programes / scripts a executar.

Es visualitza doncs si, efectivament, això que diu el missatge és cert:

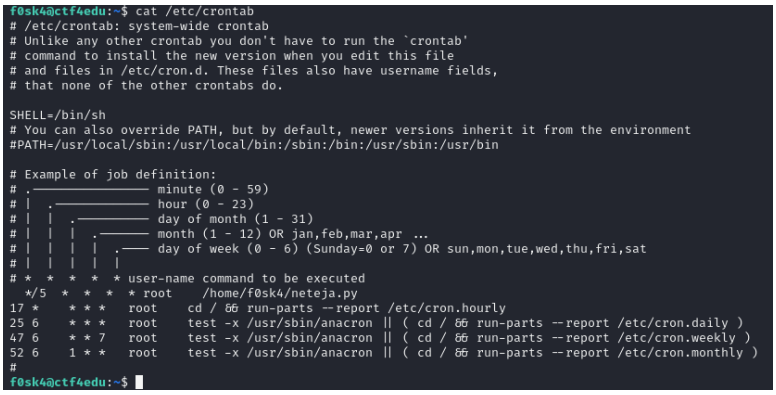


Figura 197 - Vista de Crontab a CTF4Edu

S'observa que hi ha una entrada, efectivament, de l'execució de l'script amb un */5 a la primera columna. Com que es la columna de minuts, això significa cada 5 minuts. De moment, tot concorda.

Cal tenir en compte quin usuari executa l'script a crontab i és root. Bones noticies. Si s'aconsegueix canviar l'script, quan s'executi a crontab és com si ho estés executant root.

S'intenta modificae l'script i poder realitzar una escalada de privilegis.

Per a dur-la a terme, es proposa modificar l'script que s'executa a crontab.

[56] https://en.wikipedia.org/wiki/Cron

La idea és copiar el /bin/bash i donar-li permisos al bit SUID[57] de tal manera que quan s'executi es pugui ser root. Això es fa amb la comanda chmod +s i el binari que li volem donar permisos al bit SUID.

Es fa una copia i posteriorment es modifica l'script de python.

```
#!/usr/bin/env python3
import os
import sys
try:
        os.system('cp /bin/bash /home/f0sk4/h4ckbash;chmod +s /home/f0sk4/h4chbash')
except:
        sys.exit()
```

Figura 198 - Script modificat per preparar escalada de privilegis

Es pot executar un "watch ls" per veure quan apareix el binari h4ckbash

```
Every 2.0s: ls

bandera.txt
entregarPractica.py
h4ckbash
neteja.bak
neteja.py
perlaf0sk4.txt
practiques
UdG
```

Figura 199 - Watch ls per observar quan apareix h4ckbash

Al cap de de 5 minuts, apareix.

Si s'executa un "ls -alis" es veu que té el bit SUID activat

```
f0sk4@ctf4edu:~$ ls -alis
total 1432
565321    4 drwxr-x--- 6 f0sk4 f0sk4    4096 Jan  9 02:11 .
524290    4 drwxr-xr-x 6 root  root     4096 Jan  7 20:35 ..
565344    4 -rw-rw-r-- 1 f0sk4 f0sk4      38 Jan  9 00:29 bandera.txt
565333    4 -rw------- 1 f0sk4 f0sk4     778 Jan  9 00:28 .bash_history
565323    4 -rw-r--r-- 1 f0sk4 f0sk4     220 Jan  7 20:35 .bash_logout
565324    4 -rw-r--r-- 1 f0sk4 f0sk4    3771 Jan  7 20:35 .bashrc
565326    4 drwx------ 2 f0sk4 f0sk4    4096 Jan  7 20:43 .cache
565343    4 -rwxrwxr-x 1 f0sk4 f0sk4     139 Jan  9 00:48 entregarPractica.py
565351 1364 -rwsr-sr-x 1 root  root  1396520 Jan  9 02:15 h4ckbash
565340    4 -rw------- 1 f0sk4 f0sk4      40 Jan  8 22:17 .lesshst
565328    4 drwxrwxr-x 3 f0sk4 f0sk4    4096 Jan  7 21:02 .local
565349    4 -rwxrwxr-x 1 f0sk4 f0sk4     115 Jan  9 02:05 neteja.bak
565332    4 -rwxrwxr-x 1 f0sk4 f0sk4     147 Jan  9 02:11 neteja.py
565346    4 -rw-rw-r-- 1 root  root      669 Jan  9 01:01 perlaf0sk4.txt
565331    4 drwxrwxr-x 2 f0sk4 f0sk4    4096 Jan  9 00:52 practiques
565325    4 -rw-r--r-- 1 f0sk4 f0sk4     807 Jan  7 20:35 .profile
565342    4 -rw------- 1 f0sk4 f0sk4      26 Jan  9 00:39 .python_history
565339    4 drwxrwxr-x 3 f0sk4 f0sk4    4096 Jan  9 00:53 UdG
```

Figura 200 - h4ckbash amb bit SUID activat

Es pot intentar executar h4ckbash i escalar privilegis. Es fa::

S'executa amb el paràmetre -p (privilegiat) i s'escalen privilegis. Amb whoaml es veu que s'és root.

[57] https://www.fosslinux.com/121765/linux-permissions-demystified-suid-sgid-sticky-bit.htm

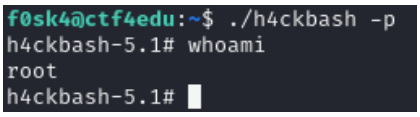


Figura 201 - Execució de h4ckbash privilegiat

Ara ja es pot accedir a la flag de root, havent completat el CTF4Edu i tots els seus reptes.

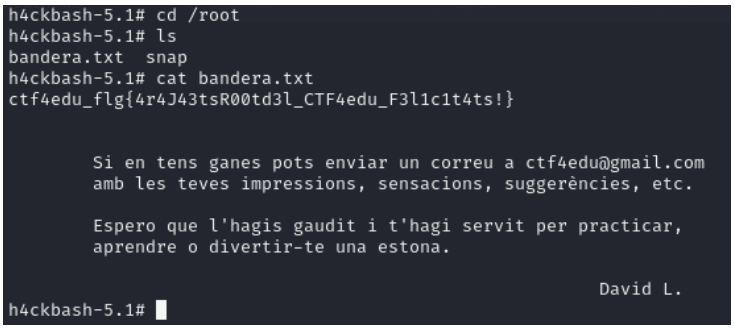


Figura 202 - Missatge amb la flag i comiat

5. Conclusions i treballs futurs

Pel que fa als aspectes formatius, he après moltíssim dels tipus de reptes CTF, he desenvolupat noves habilitats i n'he perfeccionat de les que ja tenia i sobretot, he començat a desenvolupar la meva pròpia mentalitat de hacker. Coneixia els CTF i havia intentat de resoldre algun repte, però no amb la intensitat, coneixement i profunditat que disposo després d'acabar el projecte. I el millor de tot és que això només és el principi, perquè vull continuar en aquest camí formatiu.

Sempre m'ha agradat escriure ficció, però mai havia hagut de lligar tota una història amb pistes i reptes o adaptar els reptes a la història perquè tot tingui sentit. En aquest aspecte, tot i que m'ha suposat un gran repte, estic content del resultat final per l'extensió de la història que transcorre al llarg dels 8 reptes i per la variabilitat d'aquests, permetent veure'n la majoria de les tipologies de ciberseguretat que existeixen.

La proposta mínima era fer 5 reptes i al final n'he pogut entregar 8, per tant, molt content i satisfet. Ara bé, tot i que he investigat moltíssim, no m'ha estat possible descobrir o explotar una vulnerabilitat tipus "zero day" pel fet que jo mateix m'havia imposat treballar amb les darreres versions del sistema operatiu de la màquina-objectiu (i òbviament, és més difícil de trobar vulnerabilitats noves i explotar-les).

Pels punts anteriors, puc constatar que s'han complert els objectius del projecte.

Pel que fa als objectius personals, també puc constatar que els he complert després de l'aprenentatge, millora i coneixement de tècniques i habilitats de hacking ètic i pentesting.

Referent a les línies de treball futur, penso que es podria afegir a aquest projecte una "visió del Blue Team", amb un estudi de mitigacions de la vulnerabilitat o problema exposat a cada repte.

Amb una mica de capacitat creativa es podria adaptar el reptes, les pistes, els enigmes i la història a altres idiomes com el castellà o l'anglès, per exemple. A més a més, es podria afegir nous reptes o modificar-ne algun dels existents i fer créixer la història (o adaptar-la a canvis de reptes i/o de pistes).

Addicionalment, es podria crear un site on els jugadors i les jugadores s'hi poguessin registrar per anar introduint al seu perfil les flags trobades i que automàticament se li vagi incrementant el seu comptador personal de punts. També s'hi podrien afegir noves OVA, writeups , píndoles formatives, etc.

6. Glossari

- black hat hacker: ciberdelinqüent
- CTF: en l'àmbit de la ciberseguretat, competició individual o en grup que consta en la resolució d'un nombre concret de reptes d'àmbit divers. Per cada repte, s'obté normalment una flag i al validar-la, s'obtenen uns punts d'acord a la dificultat, el temps de resolució, etc.
- CVE (Common Vulnerabilities and Exposures): conjunt de vulnerabilitats indexades en una base de dades a nivell mundia i gestionades per Mitre Corporation. Per cada CVE existeix un sol codi que la identifica, anomenat CVE ID.
- e-learning: aprenentatge virtual
- Exploit: és un programari o script que aprofita un error o vulnerabilitat en un sistema informàtic per provocar un comportament no intencionat en aquest.
- Flag: bandera. En l'àmbit dels CTF, són els objectius a aconseguir per acreditar la superació dels reptes. Normalment tenen una codificació comuna: un hash o una expressió regular.
- FTP: File Transfer Protocol, protocol utilitzat comúment al port 21, s'utilitza per a la transferència de fitxers.
- hacker ètic: professional de la ciberseguretat que utilitza el seu coneixement tècnic per analitzar, avaluar i detectar les vulnerabilitats dels sistemes informàtics o les xarxes de comunicacions sense amb permís i de forma legal.
- Màquina Virtual: màquina completa amb un sistema operatiu funcional que funciona com un sistema operatiu aïllat, i dins d'un entorn de virtualització
- Payload: part d'un atac maliciós que pretén dura terme una acció concreta en e sistema objectiu, incloent la instal·lació de programari maliciós, execució de comandes, etc.
- Pentester: hacker ètic
- Pentesting: diferents proves de penetració als sistemes que acostumen a seguir unes fases ben determinades: enumeració i recol·lecció de dades, escaneig i anàlisis de vulnerabilitats, accés i explotació de les vulnerabilitats detectades, informar dels resultats de les proves (indicant si són més o menys crítiques) i de com solucionar les vulnerabilitats.
- Root: Usuari del sistema amb privilegis màxims.
- Script: Tros de codi amb finalitats dirigides, crides del sistema i que podem executar des de l'intèrpret de comandes sense necessitat de compilar.
- Site: lloc web o pàgina web.
- SQL Injection: vulnerabilitat que permet l'accés no controlat a un sistema de bases de dades mitjançant una entrada de dades que no està correctament validada.
- SSH: Secure Shell Protocol, protocol per operar en dispositius que poden ser accessibles a través de la xarxa de forma remota.
- White hat hacker: hacker ètic
- Writeup: Guia pas a pas per explotar totes les vulnerabilitats i/o resoldre una màquina o un repte d'aquesta.

7. Bibliografia

Llibres:

Breaking into Information Security: Learning the Ropes 101 (2023) GILL, A Independently published (CANADA). ISBN: 9781549903588

Computer Networking: A Top-Down Approach (2022) 8th Edition KUROSE, J. & ROSS, K. Harlow (UK). Pearson Education Limited. ISBN:9781292405469

Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali (2018) OCUPPYTHEWEB. San Francisco (USA) . No Starch Press, Inc. ISBN: 9781593278557

The Linux Command Line. A complete introduction (2013) SHOTTS, W.E. San Francisco (USA) . No Starch Press, Inc. ISBN: 9781593273897

The Pentester BluePrint: Starting a career as an ethical hacker (2021) WYLIE, P. & CRAWLEY, K. Indianapolis (USA). John Wiley & sons, Inc. ISBN: 9781119684305

Informes, articles, notícies, blogs, webs, documentació en línia, etc:

‘A 38% Increase in 2022 Global Cyberattacks**’** (2023) *Check Point Research,* 5 de gener. Disponible a: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/ (data de consulta: 5 de gener de 2023)

‘Best Linux server distro of 2023’ (2023) *Mayanak Sharma*, (Techradar), 07 de desembre de 2023. Disponioble a: https://www.techradar.com/best/best-linux-server-distro (8 de desembre de 2023)

‘Ciberseguridad en el sector educativo’ (2023) (INCIBE), 10 d’octubre de 2023. Disponible a: https://www.incibe.es/empresas/blog/ciberseguridad-en-el-sector-educativo (data de consulta: 12 de desembre de 2023)

‘CTF: Entrenamiento en seguridad informática’ (2014) *Rafael Pablos (INCIBE)*, 26 de febrer de 2014. Disponible a: https://www.incibe-cert.es/blog/ctf-entrenamiento-seguridad-informatica (data de consulta: 15 d’octubre de 2023)

‘Capture-The-Flag Competitions: all you ever wanted to know!’ (2021) ENISA News, 10 de maig del 2021. Disponible a: https://www.enisa.europa.eu/news/enisa-news/capture-the-flag-competitions-all-you-ever-wanted-to-know (data de consulta: 12 d’octubre de 2023)

Agència pública per a la competitivitat de l’empresa catalana – ACCIÓ (2023). *La ciberseguretat a Catalunya.* Barcelona: Govern de Catalunya

Disponible a: https://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/eic-la-ciberseguretat-a-catalunya#blocMaterials_b62ef8b5-b28b-11e8-92dc-005056924a59
(data de consulta: 15 d'octubre de 2023)

Arqué Nueno, V. (2023) 'Els ciberatacants del Clínic reclamen 4,5 milions de dòlars i diuen que han robat 4 TB de dades', 324, 10 de març del 2023. Disponible a:https://www.ccma.cat/324/en-directe-lhospital-clinic-informa-sobre-la-situacio-actual-despres-del-ciberatac/noticia/3216960/ (data de consulta: 27 d'octubre de 2023)

Borràs Abelló, E. (2021). 'L'atac informàtic a la UAB ha afectat més de 650.000 arxius i els delinqüents demanen 3 M€', Ara, 15 d'octubre de 2021. Disponible a: https://www.ara.cat/societat/atac-informatic-uab-afectat-650000-documents-delinquents-reclamen-3-milions-euros_1_4149226.html

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). 'From Game Design Elements to Gamefulness: Defining "Gamification"', *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, p. 9-15. Disponible a: https://doi.org/10.1145/2181037.2181040
(data de consulta: 27 de desembre de 2023)

KALI (2023) Kali Docs: Official Documentation. Diponible a: https://www.kali.org/docs/
(darrera data de consulta: 5 de gener de 2024)

Hacktricks (2023) Linux Privilege Escalation Disponible a: https://book.hacktricks.xyz/linux-hardening/privilege-escalation
(darrera data de consulta: 5 de gener de 2024)

SimpliLearn (2023). What is Steganography? Types, Techniques, Examples & Applications .Disponible a: https://www.simplilearn.com/what-is-steganography-article

*Vry4n_* (2022) Exploiting the Cron Jobs Misconfigurations. Disponiable a: https://vk9-sec.com/exploiting-the-cron-jobs-misconfigurations-privilege-escalation (data de consulta: 27 de desembre de 2023)

Plataformes amb reptes CTF:

***TryHackMe* (2023).** Disponible a: https://tryhackme.com/ [en línia]
(darrer accés el 02/01/2024)

PicoCTF (2023) Disponible a: https://picoctf.org/ [en línia]
(darrer accés el 02/01/2024)

HackTheBox (2023) Disponible a: https://www.hackthebox.com/ [en línia]
(darrer accés el 02/01/2024)

Bandit - OvertheWire (2023) Disponible a: https://overthewire.org/wargames/bandit/
[en línia] (darrer accés el 02/01/2024)

8. Annexos

8.1 Instal·lació del sistema de virtualització VirtualBox 7.0.12

Des del sistema amfitrió obrim un navegador d'internet i accedim a la URL (https://www.virtualbox.org/wiki/Downloads)

Figura 203 Pàgina principal d'Oracle VirtualBox

Com que el sistema amfitrió és un Windows, cerquem la versió corresponent (*Windows hosts*):

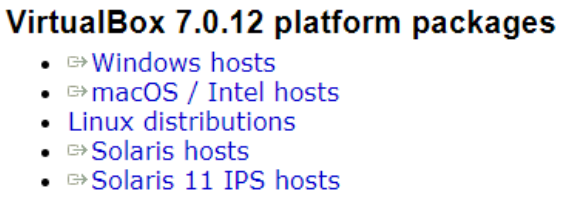


Figura 204 - Paquets d'instal·lació de VirtualBox per plataforma

Un cop fem clic al damunt de la plataforma corresponent, se'ns descarrega l'instal·lador i l'executem.

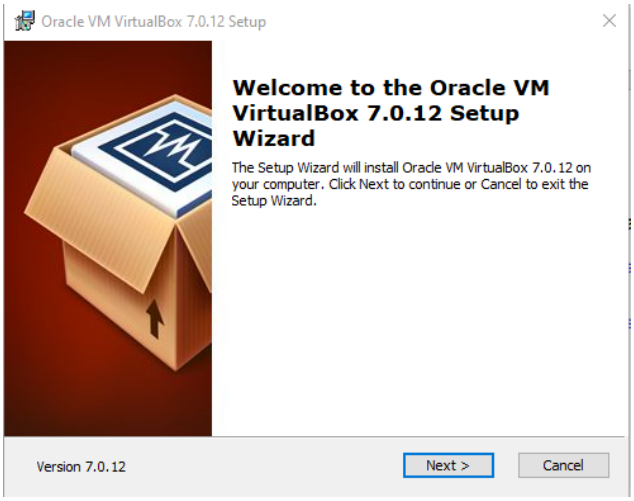


Figura 205 Instal·lació Oracle VirtualBox 7.0.12 - Windows

Si fos necessari es podria canviar els paràmetres d'instal·lació però per a dur a terme el nostre laboratori ja ens va bé deixar-los tots per defecte, per tant, anem fent clic a "Next" a cada pantalla d'opcions.

Quan arribem a l'apartat de la instal·lació de les interfícies de xarxa, ens apareix aquest avís, on cal fer clic a "Yes" per a dotar de connectivitat a les nostres màquines virtuals:

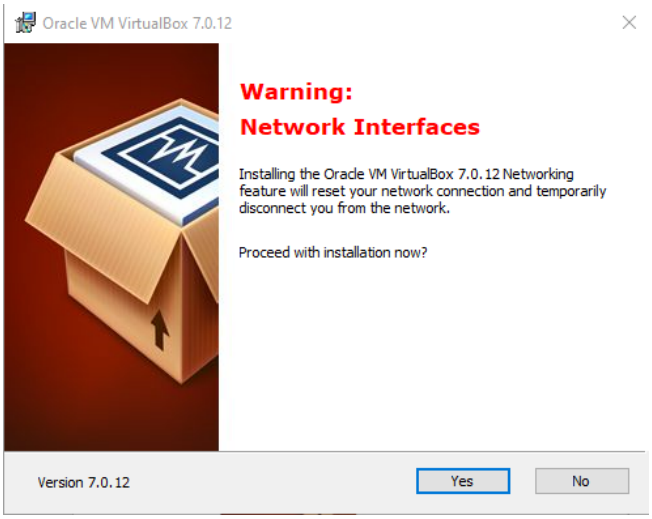


Figura 206 Avís VirtualBox - Network Interfaces

Fent tots aquests passos ens ha de permetre continuar amb la instal·lació de l'entorn de virtualització a la nostra màquina amfitrió per a continuar amb la construcció del laboratori.

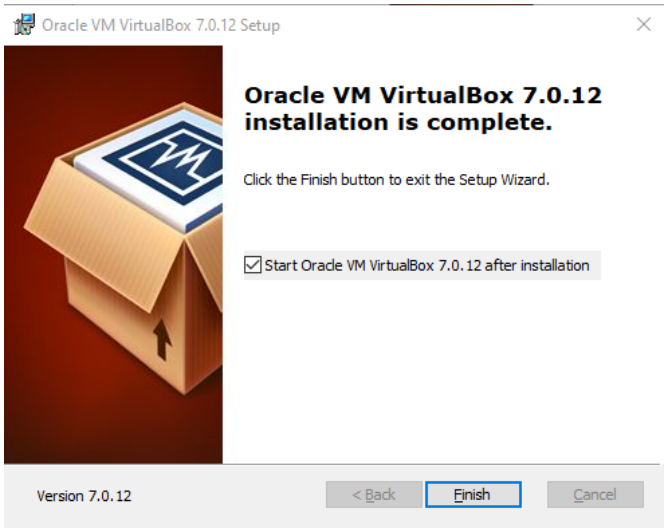


Figura 207 Oracle VirtualBox Instal·lat al sistema

8.2 Instal·lació d'Ubuntu Server

La versió d'Ubuntu Server utilitzada és la més recent i la podem descarregar des de la URL (https://ubuntu.com/download/server)

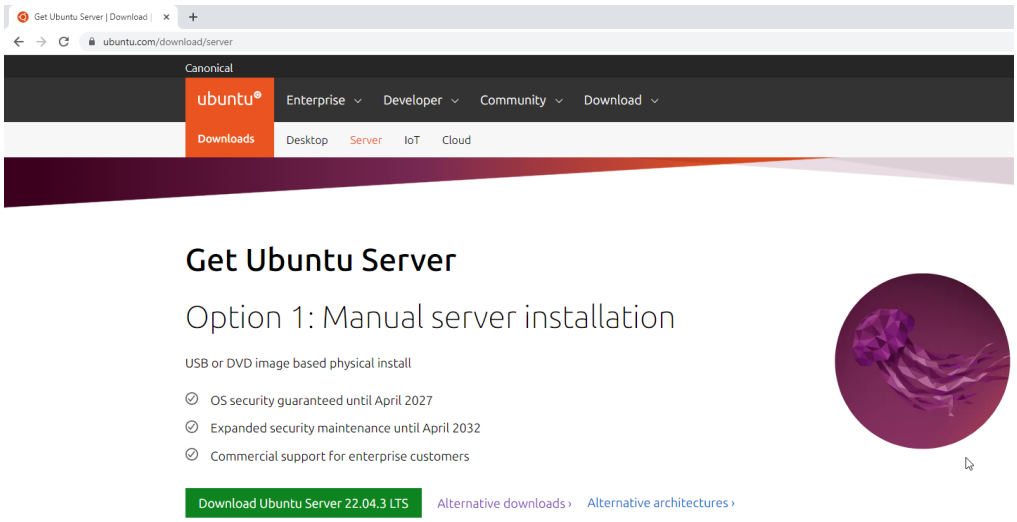


Figura 208 Descàrrega Ubuntu Server 22.04.3 LTS

Fem clic a "Download Ubuntu Server 22.04.3 LTS" i ens descarreguem la .ISO

Un cop descarregada la utilitzarem per a crear una nova màquina virtual des del nostre entorn de virtualització Oracle VirtualBox.

Obrim VirtualBox i fem clic al botó “Nova”

Figura 209 Crear nova màquina virtual a VirtualBox

A l’assistent de creació de nova màquina virtual, li donarem un nom CTF4Edu, escollirem una carpeta on desar la màquina i li indicarem quina ISO de sistema operatiu volem usar per a fer la instal·lació (i en el nostre cas escollirem la ISO de l’Ubuntu Server que ens hem descarregat prèviament). Això ja permet que el VirtualBox detecti que es tracta d’un sistema operatiu Linux 64-bit.

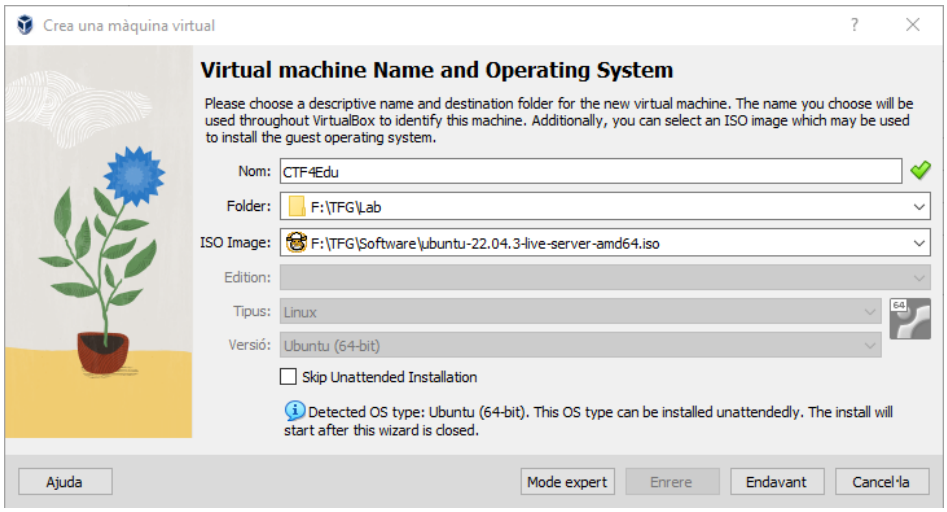


Figura 210 Assistent nova màquina virtual a VirtualBox

Tot seguit, fem clic a “Endavant”, per a configurar la instal·lació desatesa del sistema operatiu, ja que en el nostre cas es permet. Escollim un nom d’usuari i un password segur[58] (usuari: **atzucac** i password: **P3ss1g0ll3s2023**)

[58] Podem usar un servei com https://password.kaspersky.com/ per a comprovar-lo.

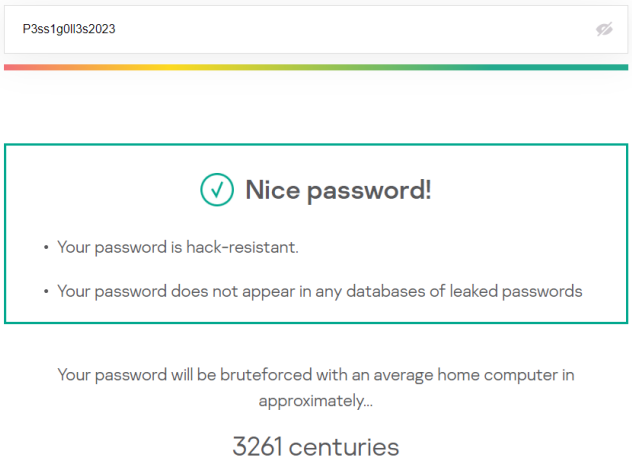


Figura 211 Verifica que el teu password sigui segur

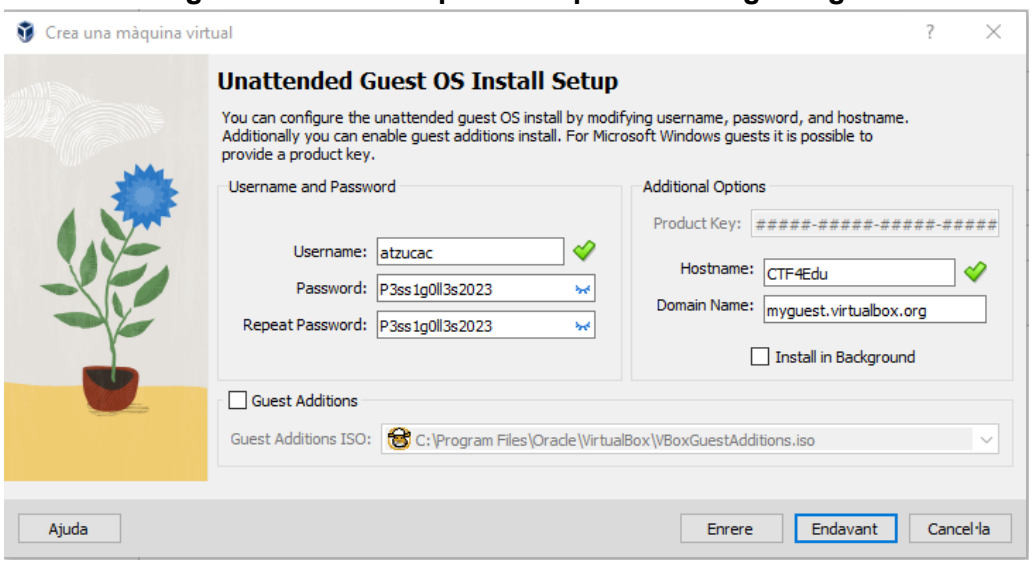


Figura 212 Configuració instal·lació desatesa SO a VirtualBox

Tot seguit deixem per defecte les característiques tècniques de la màquina virtual. VirtualBox ens proposa 2 GB de RAM i 1 CPU, i ho deixem així a garantir la màxima compatibilitat amb tots els dispositius que puguin utilitzar el nostre sistema sense problemes (tot i que cada dia els equips són més potents i disposen de més capacitat, és la voluntat d'aquest projecte no excloure ningú per raons de menys recursos de maquinari). Fem clic a "Endavant".

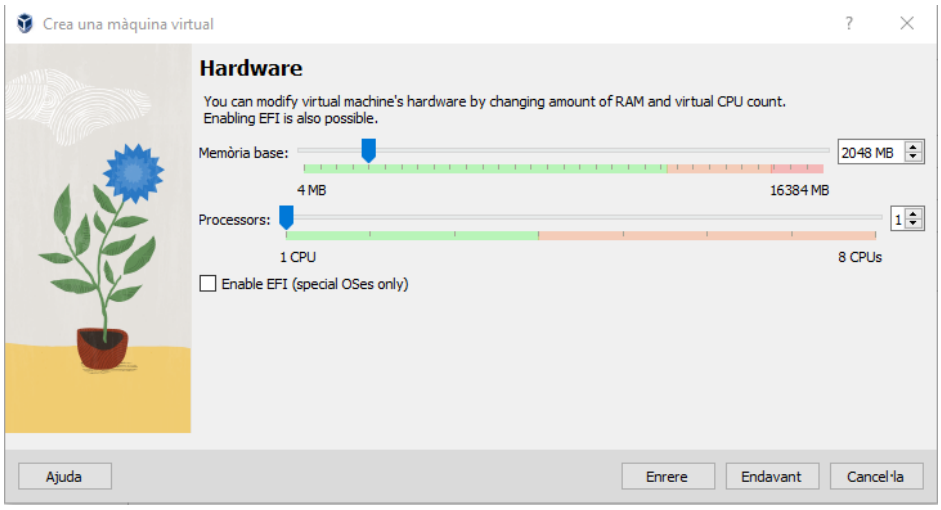


Figura 213 Característiques hardware de màquina virtual a VirtualBox

Per finalitzar indiquem com volem que sigui el disc dur de la nostra màquina objectiu. Escollim la opció per defecte, que és crear un nou disc dur vidual i deixem desmarcada la casella de “prereserva d’espai de disc” (). Això permet que mentre no faci falta, la màquina no consumirà més espai de disc en l’equip amfitrió i seguint amb la política d’economitzar recursos per a fer el màxim d’accessible el nostre CTF, és la millor opció. Fem clic a “Endavant”.

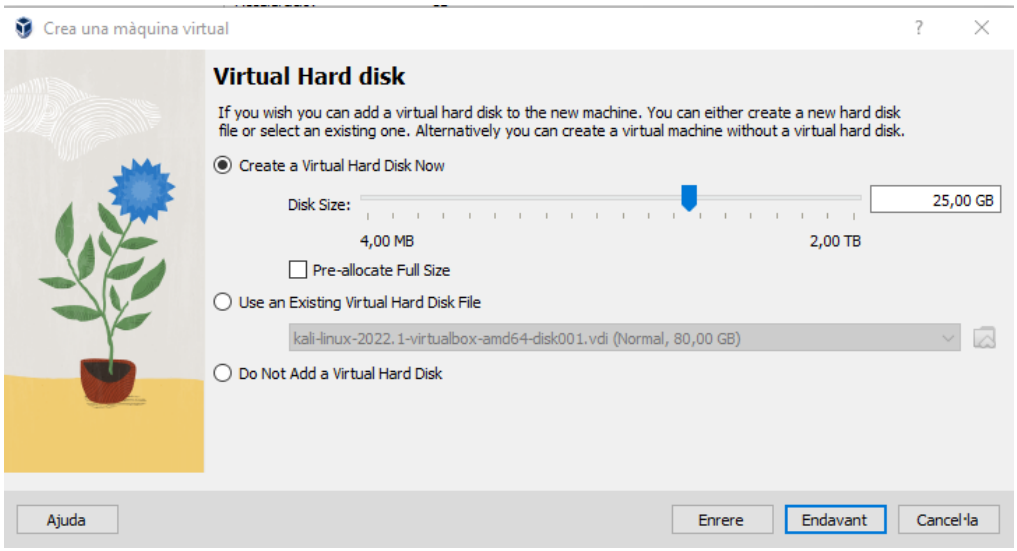


Figura 214 - Creació de disc dur virtual a VirtualBox

Finalment, VirtualBox en mostra una pantalla resum amb tot el que hem escollit fins ara. Com que hem anat verificant pas a pas cada opció, fem clic a “Finish” i la instal·lació desatesa de la nostra màquina objectiu, iniciarà.

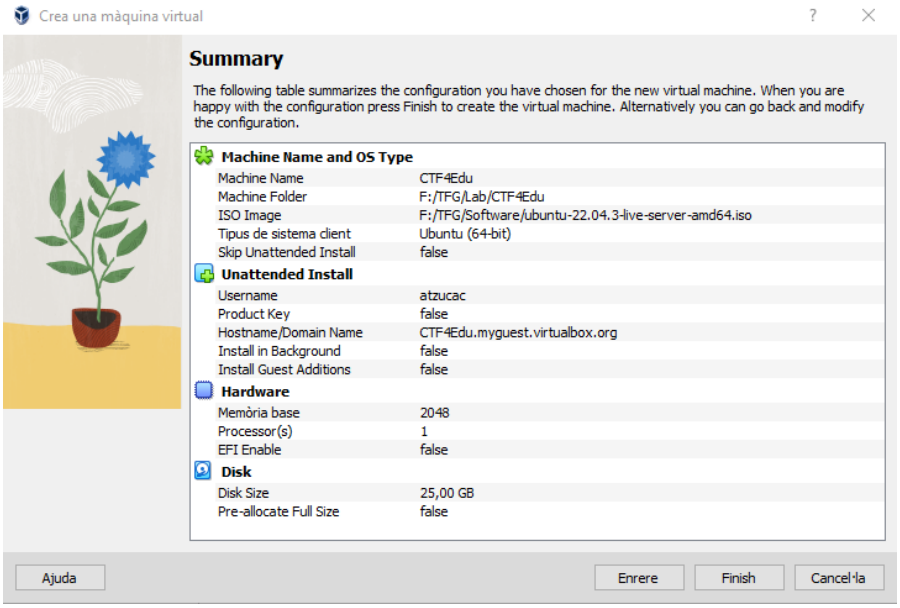


Figura 215 Pantalla resum instal·lació màquina objectiu a VirtualBox

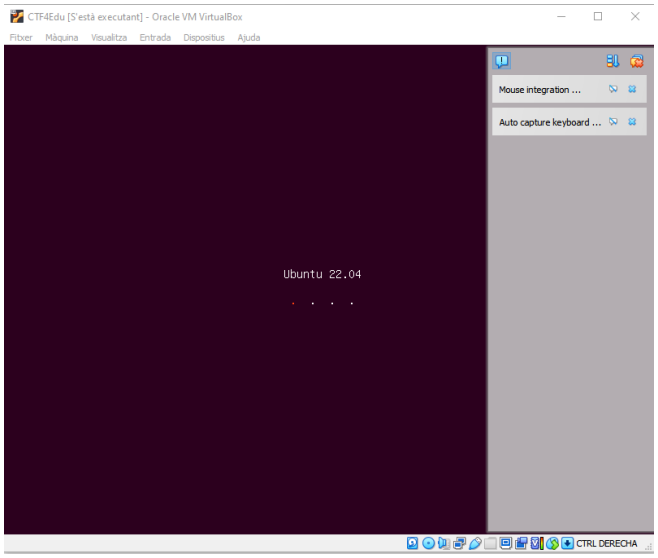


Figura 216 Instal·lació iniciada del sistema operatiu màquina objectiu

Durant el procés de instal·lació ens demanarà que escollim l'idioma del propi sistema (pel nostre projecte escollim l'anglès, per defecte) i la distribució del nostre teclat (on indiquem variant català del teclat espanyol).

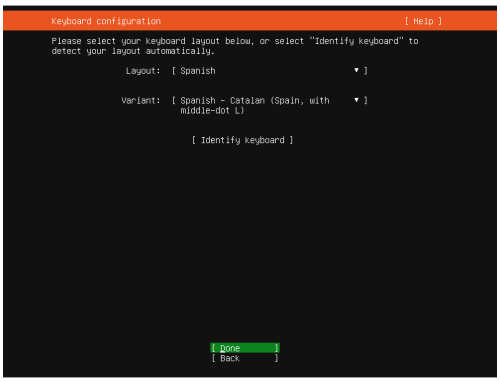


Figura 217 Ubuntu Server - Distribució teclat

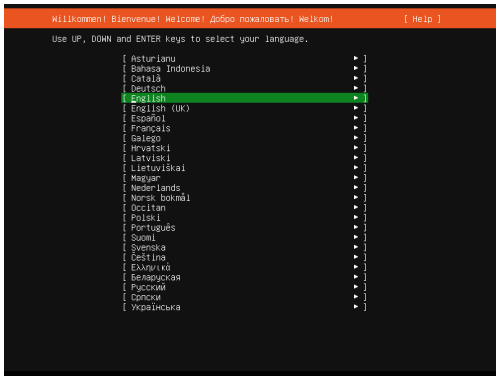


Figura 218 Ubuntu Server - Idioma

Indiquem que volem la instal·lació d'Ubuntu Server, com a instal·lació base:

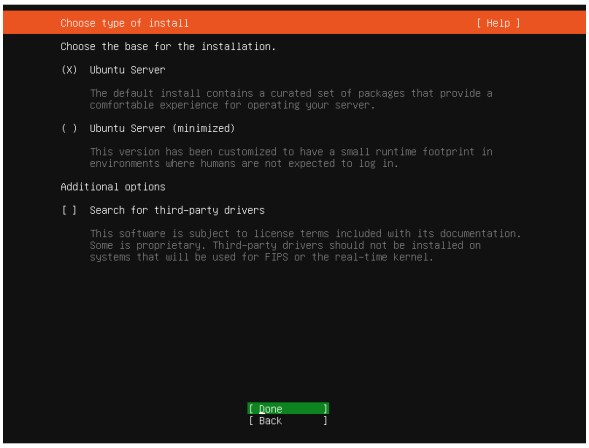


Figura 219 Ubuntu Server - Tria del Sistema base

Deixem la resta d'opcions per defecte i iniciem la instal·lació.

Un cop acaba el procés, obtenim la màquina objectiu preparada per a configurar el reptes del nostre CTF.

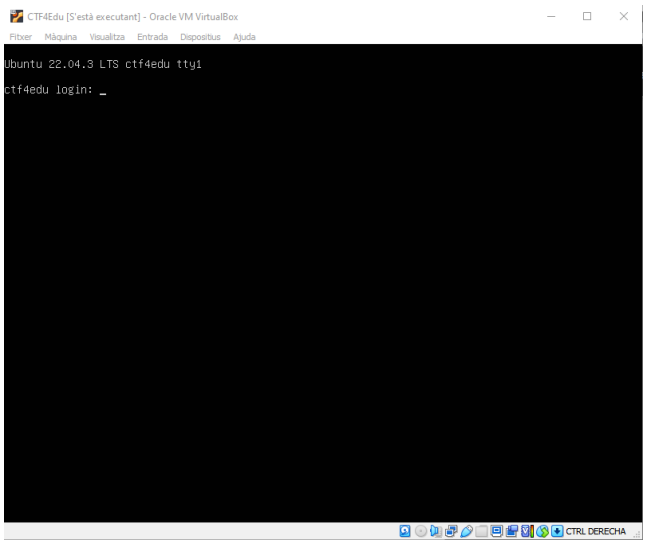


Figura 220 Ubuntu Server - En funcionament

8.2.1 Configuració de l'adaptador de xarxa de la màquina objectiu

Per a dotar de connectivitat a la màquina objectiu, es configurarà l'adaptador de xarxa en mode "bridge" (adaptador pont) de tal manera que la interfície física de xarxa es compartirà amb la màquina amfitriona i el router amb servidor DHCP on aquesta estigui connectada (actualment la LAN de casa de l'autor que és 192.168.0.1/24).

Amb la màquina objectiu aturada a VirtualBox:

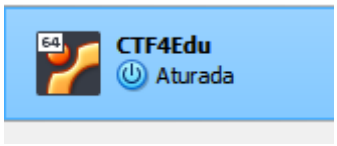


Figura 221 - VirtualBox - Maquina Objectiu aturada

Anem a la opció "Paràmetres"

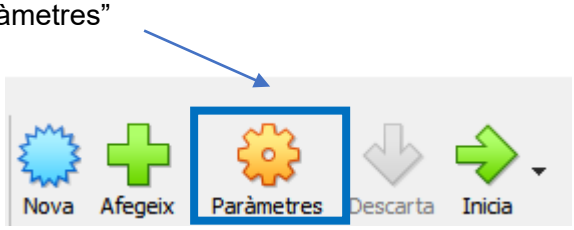


Figura 222 VirtualBox - Paràmetres

I configurem l'apartat de xarxa tal i com hem indicat, utilitzant l'adaptador de la màquina amfitriona com a adaptador pont (mode bridge)

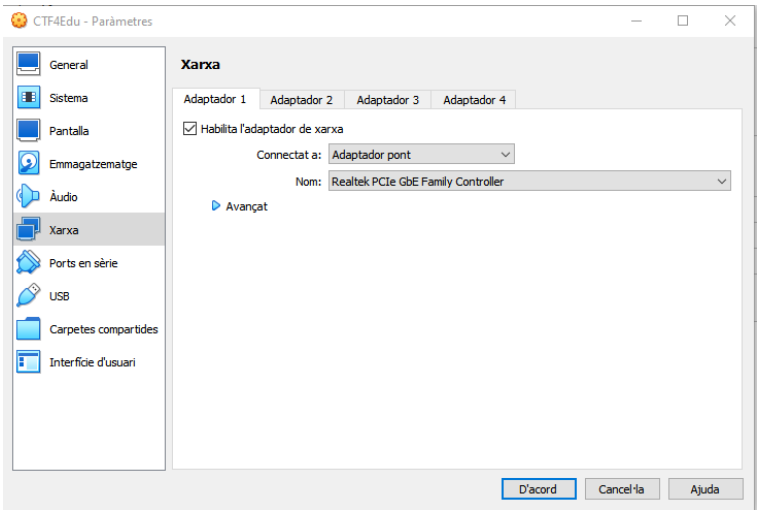


Figura 223 VirtualBox - Configuració de xarxa

8.3 Importació de Kali Linux al nostre laboratori

Anem a la pàgina https://www.kali.org/

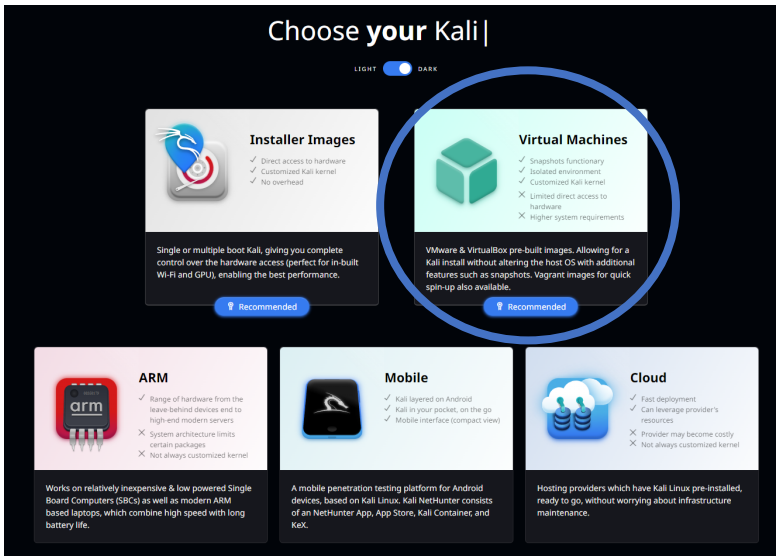


Figura 224 Kali Linux - Màquines Virtuals

A la secció de màquines virtuals, escollim la distribució de Kali per VirtualBox

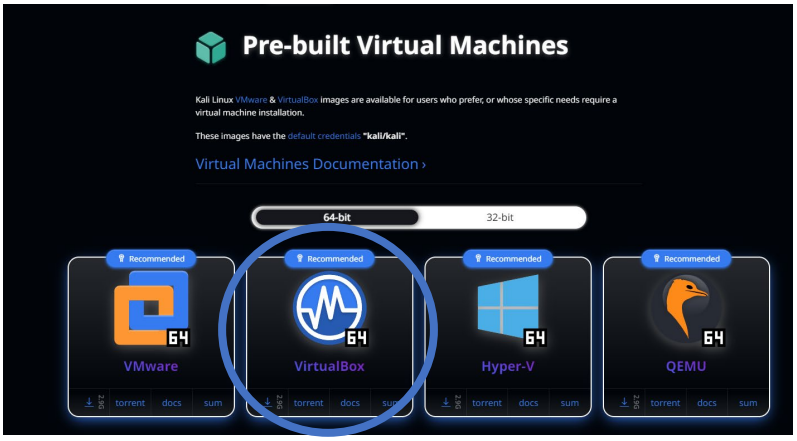


Figura 225 - Kali Linux per a VirtualBox

Un cop descarregat el fitxer comprimit que conté la màquina virtual (en format *7z*[59], cal fer els següents passos per a importar-la a VirtualBox:

Ara cal que descomprimim el fitxer (p. ex: kali-linux-2023.3-virtualbox-amd64.7z) a una carpeta temporal que escollim (o el deixem a la mateixa on l'hem descarregat)

Obrim VirtualBox i fem clic a "Afegeix":

[59] 7Zip URL: https://www.7-zip.org/

Figura 226 Menú Afegeix a VirtualBox

Naveguem fins a la carpeta on hem descomprimit la imatge de la màquina virtual i seleccionem el fitxer amb extensió .vbox

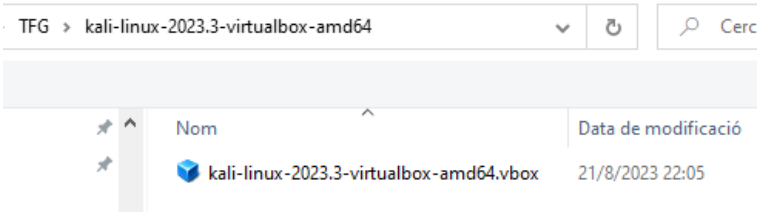


Figura 227 Fitxer d'importació de Kali Linux a VirtualBox

Un cop seleccionat, fem clic a “Obre” i ja la tindrem importada al nostre VirtualBox.

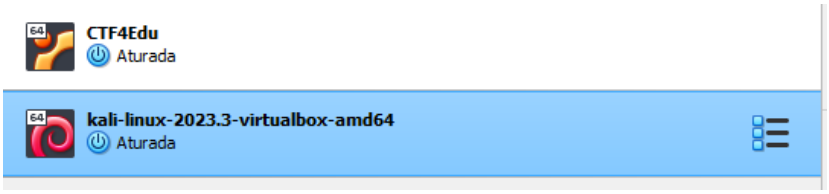


Figura 228 Màquina Virtual Kali Linux importada a VirtualBox

Configurem l’adaptador de xarxa virtual en mode *brigde* (es segueix exactament el mateix procediment explicat detalladament en l’apartat de la instal·lació de l’Ubuntu Server).

Nota: Si hi ha recursos suficients disponibles a la màquina host on executem el laboratori del CTF, una bona idea és dotar de més memòria RAM virtual respecte de la configuració de la màquina virtual per defecte (2048 MB).

Ja podem usar la màquina atacant, amb les credencials per defecte que ens ofereix el fabricant (usuari: **kali** / password: **kali**)

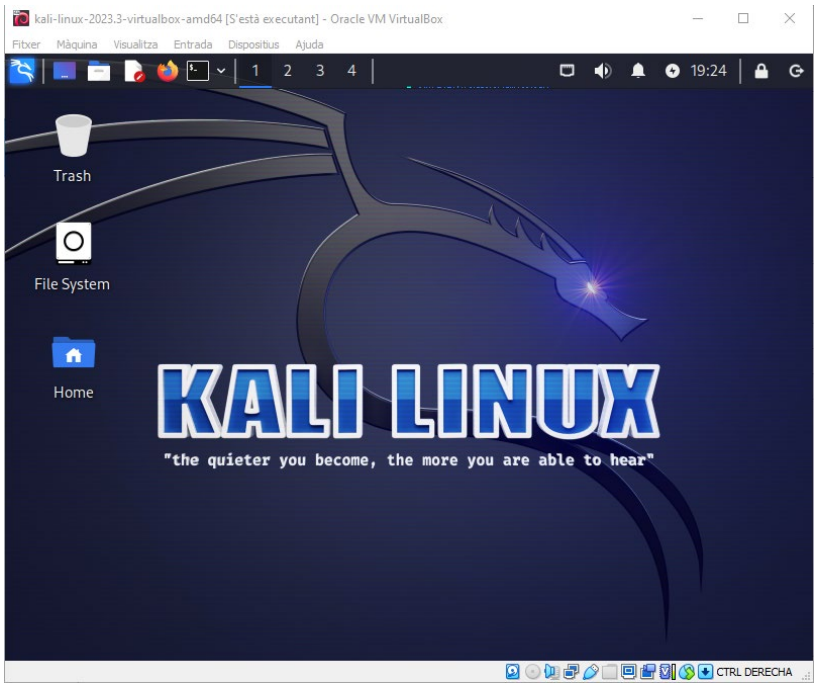


Figura 229 Kali Linux funcionant

8.3.1 – Configuració de la distribució del teclat

A la màquina virtual, per defecte hi ha configurada la distribució de teclat americana, i per tant, no és la que s'ajusta al teclat a Catalunya. Per aquest motiu, és important que configurem el teclat per tal que admeti i reconegui el caràcters en català o castellà.

Per a fer-ho obrim una *Shell*[60] *de Linux (Terminal Emulator)* i:

Si ens trobem en un equip Windows, la comanda a executar és: setxkbmap es winkeys

```
┌──(kali㉿kali)-[~]
└─$ setxkbmap es winkeys
```

En el cas d'un equip Mac, la comanda és:

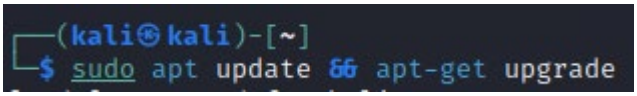
```
┌──(kali㉿kali)-[~]
└─$ setxkbmap es mac
```

Cal dur a terme aquesta acció cada vegada que iniciem el sistema.

8.3.2 – Actualitzar la màquina atacant a la darrera versió

[60] Unix Shell URL: https://en.wikipedia.org/wiki/Unix_shell

Com a norma general, és molt recomanable verificar que no hi ha disponibles noves versions del sistema o dels paquets inclosos en la distribució. Per tant, abans de començar qualsevol sessió de *pentesting* cal comprovar i instal·lar totes les actualitzacions pendents possibles, per a disposar de les versions més actualitzades de les eines disponibles. Per a actualitzar el Kali, obrim una *shell* i executem:



8.4 CTF4Edu – Les vulnerabilitats (la història)

Sona el molest despertador i no vols obrir els ulls mandrosos i adormits. La nit ha sigut curta després del llarg informe del *pentesting* d'ahir. Et comencen a venir records de la tasca feta, de l'enviament del PDF al client. Entre el cansament i el fred, trobes que precisament ara és quan estàs millor al llit. Tens molta son i el despertador, pesat, insisteix altre cop. D'esma, fas el gest d'aturar l'alarma, però, de cop, recordes que avui tens la reunió amb el gerent de la Universitat Oberta de Catalunya i com si la idea et comencés a estirar dels peus del llit, d'un bot saltes cap a la dutxa: no vols fer tard, avui no.

Enretires la cortina, obres l'aixeta i badalles. Entres a la dutxa amb l'aigua encara un xic freda perquè la teva consciència climàtica va per davant del teu confort: no podem malgastar aigua i tothom ho hauria de fer, et dius mentalment. Deu minuts de rellotge i cap a fora. Suficient. Una mica de vida pel planeta.

Mentre t'eixugues amb la tovallola penses amb tot el que li vols dir al gerent. No serà una reunió fàcil. Ni agradable.

Vestir, badall i cafè. Tanques la casa, agafes la motxilla i cap al tren. Un cop al vagó, treus el portàtil i repasses l'informe obtingut del *pentesting* que fas fer als servidors de la UOC. Al gerent no li agradarà el que has trobat, però és millor que ho hagis detectat tu que no pas els ciberdelinqüents. Com a membre de l'Agència de Ciberseguretat de Catalunya, fa anys que intentes fer tot el possible per evitar que els *black hat* hackers facin massa de les seves...

I just en aquest moment, no saps ben bé per què, recordes el teu primer cop. La primera vegada que vas resoldre una màquina. Era un joc, un CTF. Te'l van proposar en una pràctica d'una assignatura del grau d'enginyeria informàtica i encara te'n recordes com si fos avui. Hi havia uns quants reptes, i de cop recordes tot com va anar. Sí, i tant! El primer parlava de...

REPTE1

Estudies enginyeria informàtica a la Universitat de Girona, concretament a l'escola politècnica superior, molt a prop de l'estadi del Girona F.C. Ahir, dia de partit, el Girona va tornar a guanyar i tu i la teva colla vau acabar tardíssim després d'una llarga nit de festa per celebrar que continueu líders.

Has passat per bar del campus a buscar el teu cafè per mirar de suportar millor les llargues classes i estàs assegut en una de les cadires del passadís de les aules informàtiques, pensant com t'ho faràs per poder mantenir-te despert. Mentre fas glops al teu cafè, sents una conversa per casualitat: un alumne parla per telèfon amb algú i li reclama de males maneres que vol la seva pràctica final feta, que per això li ha pagat. De cop, silenci. Tu fas veure que estàs distret amb el teu mòbil, però interceptes algunes paraules que el noi diu en veu alta, com repetint el que li diu algú a l'altra banda: **Ubuntu, fitxer, pista, 64**. Ràpidament, aixeques la mirada del teu dispositiu mòbil i, no saps ben bé per què, intentes fixar-te en els detalls del noi del telèfon. És pèl-roig i duu una samarreta del Barça. De cop es gira cap a tu, i com si estiguessis fent alguna cosa que no toca, abaixes la mirada, com si alguna cosa t'hagués de fer vergonya. Et fa por que no t'hagués pescat observant-lo més del compte.

Tu continues dissimulant mentre el noi comença a caminar i tornes a fixar-te què està fent, aprofitant l'anonimat que ara et dona el fet que es trobi d'esquena. Es dirigeix cap a l'aula informàtica més propera. Arribats a aquest punt, decideixes investigar: no és just que ningú faci servir mètodes il·lícits per a superar una assignatura. El bon nom de l'enginyeria informàtica és a les teves mans. Somrius pel que acabes de pensar. Això del bon nom i tal. De vegades, ets d'una intensitat... De tota manera, sigui com sigui, el que estigui passant t'ha despertat la curiositat i pocs segons després que el pèl-roig entrés a l'aula, tu el segueixes i t'asseus a un dels ordinadors un parell de files per darrere seu, amb el teu llapis de memòria on hi ha un Kali Linux i inicies el sistema. Aquesta aula, com la majoria de les que hi ha a la Universitat de Girona és una aula Windows. Estàs convençut que si el noi ha entrat aquí després de la conversa telefònica és perquè algun dels ordinadors d'aquesta mateixa subxarxa, la VLAN d'aules, conté alguna pista per a destapar tota aquesta trama. No pots veure què fa exactament el noi, ara mateix, i decideixes recollir el màxim d'informació pel teu propi compte i amb els teus coneixements actuals. Esperes que tot el que has après fins ara et pugui servir per esbrinar què està passant. A continuació, connectes el teu llapis de memòria a l'ordinador i et disposes a iniciar el teu sistema operatiu per investigar.

REPTE2

De cop hi volta et fixes en una cosa ben curiosa: el noi pèl-roig amb la samarreta del Barça a qui seguies per descobrir l'entramat de les pràctiques té el mòbil a la mà i sembla que està fotografiant la CPU de l'ordinador que utilitza. Per a recordar quin ordinador és i continuar investigant et fixes en les coordenades cartesianes de l'ordinador (fila 6, pc 4). Caram: 6 i 4. 64. Potser és una casualitat? Sigui com sigui, els nombres que són potències de 2 als d'enginyeria informàtica li són familiars i, per tant, fàcils de recordar.

Mentre calculaves en quin ordinador es trobava el pèl-roig, no has vist què feia després. Ara mateix ja no té el mòbil a les mans i en aquest instant extreu alguna cosa de l'ordinador. Se'l posa a la butxaca, agafa la motxilla i sembla que marxa. Mentre passa a prop teu cap a la sortida, el mires discretament: fa més bona cara i, per tant, sospites que potser ja ha obtingut la pràctica. Dissimules una mica més mirant el *Moodle* de la universitat.

Quan calcules que ja ha sortit, al cap de pocs segons, t'aixeques i comences a comptar files, arribant a la 6. Un, dos, tres i quatre: és aquest PC, et dius mentalment. T'asseus a l'ordinador on era ell fa uns pocs minuts i intentes projectar mentalment com tenia el mòbil situat per a veure si trobes a què li estava fent una foto. Treus, el teu mòbil de la butxaca, et situes al moment quan l'has vist a ell, obres l'*app* de la càmera i enfoques l'ordinador. Amb els dits, fas zoom i et fixes en una mena d'imatge, petita al costat de l'etiqueta de l'ordinador, on hi ha el model, el número de sèrie, el fabricant, etc. Fas encara una mica més de zoom i veus això per pantalla:

És un codi QR, però està tan integrat a l' etiqueta que tot fa pensar que apunta a la web del fabricant de l'ordinador per a facilitar buscar-ne les dades. Ben bé no saps per què et fixes en els ordinadors propers, però a l'etiqueta no tenen res. Així doncs, decideixes capturar-lo i veure realment on apunta. Tanques l'*app* de càmera del mòbil, obres la d'escanejar QR i t'apareix el següent enllaç per pantalla:

https://drive.google.com/file/d/1UjVzipZFDhErtiwV4-GI0u4qwh1gnG0c/view?usp=sharing

Això fa pinta de ser un document o fitxer compartit. Ho vols investigar però no et pots quedar en aquest ordinador. Així que canvies de lloc, busques un ordinador tranquil de la zona més apartada de l'aula i t'envies l'enllaç per correu, des del mòbil. Et treus el teu llapis de memòria amb el Kali Linux de la butxaca i et disposes a investigar què deu ser aquest fitxer misteriós al qual accediràs tan bon punt aparegui la frase escrita al fons d'escriptori: "*The quieter you become, the more you are able to hear*". De moment, el drac ja ha començat a brillar. I tu tens més ganes que mai de fer el que estàs fent.

REPTE 3

Continues davant de l'ordinador, obrint terminals i anant executant comandes per veure què pots arribar a saber. Ningú sap què estàs fent, però no pots evitar de mirar la porta d'entrada de l'aula, encara que sigui de cua d'ull, per veure si el noi pèl-roig torna i et comença a increpar, com si d'alguna manera hagués deduït que estàs investigant-lo a ell o el que fa. Tota la informació que es pot obtenir en la fase de *Reconnaissance* necessita una mica de temps, no ens enganyem. Tens l'adrenalina a dalt de tot, perquè t'adones que estàs avançant tot i que no saps ben bé cap a on. De moment, estàs recollint una mena de *flags* que segueixen un mateix patró: *ctf4edu_flag{missatge}* que desconeixes si et seran d'utilitat en un futur. Això no obstant, creus que ets al lloc correcte i que aquesta màquina-objectiu que has trobat té la clau de volta de tot. Si poguessis aconseguir més informació, seria genial. I per això mateix, vols continuar.

Executes una comanda “clear” i tot seguit una comanda “ls”, tot i que ho fas pràcticament sense pensar. Mires la pantalla i t’adones que tens la poca informació que has recollit fins ara en un fitxer anomenat dades.txt i de cop penses que la teva mare té raó quan et diu que has d’ordenar millor les coses. Has començat tan de sobte que ni tan sols has creat una estructura de carpetes per anar desant tota la teva investigació. Així que comences per aquí: crees una carpeta amb el nom “ctf4edu “ i trasllades el fitxer dades.txt a dins. Entres dins la carpeta i continues a partir d’aquí. No caldria, però no pots evitar executar una comanda “ls” per a comprovar que el fitxer és on òbviament ha de ser.

En el terminal on s’estaven executant les comandes d’anàlisi, sembla que el procés ha acabat. Observes els resultats atentament, i somrius. Edites el fitxer de dades per incorporar-hi la nova informació. La descoberta portarà el vaixell de la teva investigació a un nou port per on continuar l’aventura.

REPTE 4

Amb les credencials obtingudes amb la investigació que has dut a terme fins ara, et sorgeix un dilema: les utilitzes per a comprovar si funcionen i a veure què més descobreixes o ho deixes aquí? La pregunta et va fent voltes al cap quan de sobte veus, en una de les teves revisions un xic paranoiques de l’entorn, a la teva companya Sira entrar per la porta de l’aula. La Sira et saluda i tu aixeques la mà, a tall de retorn. La Sira és una noia d’una bellesa captivadora, i tot li queda bé. T’has fixat que s’ha rapat els cabells al zero i et sorprèn que des d’ahir, hagi perdut els seus cabells rinxolats. Veus que se t’apropa així que t’aixeques de la cadira per saludar, i de passada allunyes la seva mirada del teu monitor. Decideixes tocar el tema, de forma ocurrent, sobre el seu nou pentinat i ella riu quan li fas referència a Histieu, quan al segle IV aC ocultava informació rapant els cabells dels esclaus, tatuant-los el missatge al damunt de la pell del cap i deixant que els hi tornés a créixer per enviar-los a Aristàgores informant dels plans invasors dels perses. El sistema potser era lent, però altament efectiu: si algú interceptava a l’esclau, no hi havia perill que ni sota tortura aquest pogués revelar el missatge doncs no el coneixia per molt que el duia tatuat sota el cabell. I si arribava sa i estalvi a destí, revelar-lo era molt fàcil: només li havien de rapar el cap i llegir la informació. Un dels primers casos d’esteganografia de la història.
De cop, mires el rellotge. Et disculpes per semblar una mica brusc, però li dius que encara has d’acabar una pràctica de seguretat en xarxes de computadors i vas una mica endarrerit i t’hi hauries de posar. Ella, riallera i simpàtica com sempre, s’acomiada i es dirigeix a una altra fila d’ordinadors de l’aula. I tu tornes a la teva pantalla, el teu terminal i et disposes a utilitzar les credencials per connectar-te al servidor ctf4edu. Ara ja no dubtes en absolut.

REPTE 5

Tens la comanda escrita al terminal del teu Kali i prems enter. Quan et pregunta la contrasenya, bufes i escrius ràpidament la credencial trobada. Un *banner* indicant que t’has connectat a CTF4Edu apareix i de cop ja has iniciat sessió. No pots evitar de llistar el contingut del directori, a veure què apareix al teu monitor. Un calfred et recorre l’espinada, entre nervis i emoció. WWW. Una carpeta aparentment d’un *site*. De fet, on

vas trobar les credencials ja parlava d'alguna mena de material així. Estàs a punt d'accedir al directori quan et sona el mòbil. Mires la pantalla i veus el nom: "Patuufa". És la teva germana petita. Primer de tot, ara no és bon moment. Estàs enmig d'una investigació perillosa i no vols despenjar el telèfon. També coneixes el procediment: si no ho fas, no pararà de trucar. Una vegada i una altra, és insistent com ella sola. Fins que li agafis. Així que, després de les reflexions, dius com amb pressa:
-Ei, *patufa*. És urgent? Estic a punt d'entrar a classe.
-És mentida. Em vas dir que avui a la tarda no tenies classe.
-Eh... (no t'havies fixat de l'hora que era i encara no has ni parat per dinar). Què vols?
-Necessito la teva ajuda amb un problema de mates: "Un xef es troba un endeví i aquest li planteja un enigma: Si un triple de bàsquet són 3 punts, què és més gran: el triple de punts o tres triples punts?"
-És broma, no? Has pensat el problema abans de trucar?
-No, per això et tinc a tu.
-Has de fixar-te en els detalls! Són la clau. El triple de 3 punts són 9. 1 triple punt, és 3 i tres triples punts, 3 x 3 o sigui nou. La solució és que cap és més gran. Són iguals.
-Ets un geni, germanet. Després ho passo a la llibreta. Muaa!

Quan penja et mires la pantalla. I somrius una miqueta. Et cau bé, la teva germana. És una mica esbojarrada, però és intel·ligent i molt llesta tot i que massa impacient.
De cop, tornes a mirar la pantalla. Potser, et dius mentalment, aquests consells que dones, com de guru del coneixement, et serviran fins i tot a tu: Amb el que tens entre mans, trepitges un terra fràgil i més val que tu també et fixis en tots els detalls.

REPTE 6

La Sira ha acabat de treballar amb els ordinadors de la facultat i se t'acosta per acomiadar-se. Tu estàs tan concentrat amb tot el que estàs descobrint que no la veus arribar fins que la seva mà ja reposa al damunt de la teva espatlla.
-Ei, marxo. Que vagi molt bé la pràctica.
-Eh...gràcies. Sí, sí... i tant! La pràctica, és clar! (no recordaves l'excusa que li havies donat.)
-Per cert, et volia dir una cosa. Tu vas anar de vacances a Irlanda, oi? És que recordo que en vam parlar.
-Sí, sí. A l'agost. Per?-preguntes encuriosit
-No perquè et volia dir si l'estació de Crack Station és a prop de la zona de Temple Bar. Resulta que he trobat un allotjament just al costat d'aquesta estació, però no la trobo al mapa.
-No recordo cap "Crack Station" de quan vaig estar a Dublin. Segur que era aquest nom?
-Sí, espera...ho busco. Ah, no! No sé on tinc el cap. -Somriu. -Crampton! Volia dir Crampton.
-Crampton sí, és a 200 metres. Súper a prop!
-Merci!-Somriu altre cop. Fa mitja volta i marxa.

Tu no pares de mirar-la mentre surt de l'aula. De cop, t'arriba un Whats. És ella que t'envia una frase en llatí: "Ja saps que la Sira és un cas. Cerebrum non habet 😉". Somrius. Ara parla d'ella en tercera persona. Aixeques les celles i deixes el mòbil.

De cop, recordes què estàs fent. Et tornes a concentrar. Seriós, tornes a analitzar més detalls d'aquella carpeta que, i encara no saps com ha pogut passar, fa tanta estona que et recorda a la teva germana i al seu problema de matemàtiques...

REPTE 7

Tot i els progressos, la cosa s'està posant complicada. Tot el teu cap està com comprimit, atrapat. Necessites fer un descans ,però saps que no et pots aturar aquí. Recordes que un dia a casa no hi havia manera que et passés el mal de cap i el pare, intentant fer-se el graciós, va dir allò de –"Com deia John The Ripper, anem per parts". I tu li vas dir Jack. I ell –"no, em dic Josep". I tu -No, pare. Et dic que l'assassí de l'època victoriana era Jack The Ripper. I tu has dit John! Però ell a la seva...
I després amb la mala cara que feies, encara et parlava que si fossis el monstre Hydra, tallant-te el cap que et feia mal en faries prou. I a tu no et feia gens ni mica de gràcia...
-A vegades, quan ens quedem encallats, cal aplicar força bruta! -deia el pare. –Ah, i posar rock! Això no falla mai. *Rock you, baby*!!!!

I tu, pensant: pare, no. Ja en tinc prou amb el mal de cap. Més ridícul no.

El cap no millora, però aquest record... sembla impossible. T'ha donat una idea, sí, i tant. Una idea meravellosa i creativa per intentar aprofitar la informació que acabes de trobar. I sembla que, posant-la en pràctica, avançaràs cap al tram final d'aquesta aventura.

REPTE 8

Efectivament. Portaves un ibuprofèn líquid al fons de la butxaqueta de la motxilla. I tot i que ja ho havies revisat, a la tercera l'has localitzat.

Et trobes millor, però falta menys d'una hora per a tancar l'edifici de la facultat i t'has d'espavilar: O ara o mai. Sense accés a la màquina no podràs trobar evidències de cap tipus.

Fins ara, amb l'anterior usuari, has creat una carpeta .temp i has anat transmetent uns binaris rere uns altres. Els donaves permisos per executar searchexploit, LinEnum, GTB, LinPeas, Enum4Linux... Res! L'ubuntu 22.04 que tenen no té ara per ara vulnerabilitats "zero day" o tu no les has sabut trobar, et dius...

Ara, unes noves credencials et permeten tornar a investigar. I quan observes el que tens al davant dels ulls, no t'ho pots creure. Has descobert com s'ho fan per traficar amb les pràctiques copiades. Et copies els fitxers de text, per a tenir evidències del que has anat trobat i analitzes els scripts. No en tens cap dubte: això ho resoldràs!
Et disposes a fer el que toca fer. Ja saps com fer-ho i no dubtaràs a fer-ho. Estàs plenament segur que, un cop escalis privilegis, la màquina serà teva. I obtindràs tota la informació necessària per a desmuntar aquesta trama.

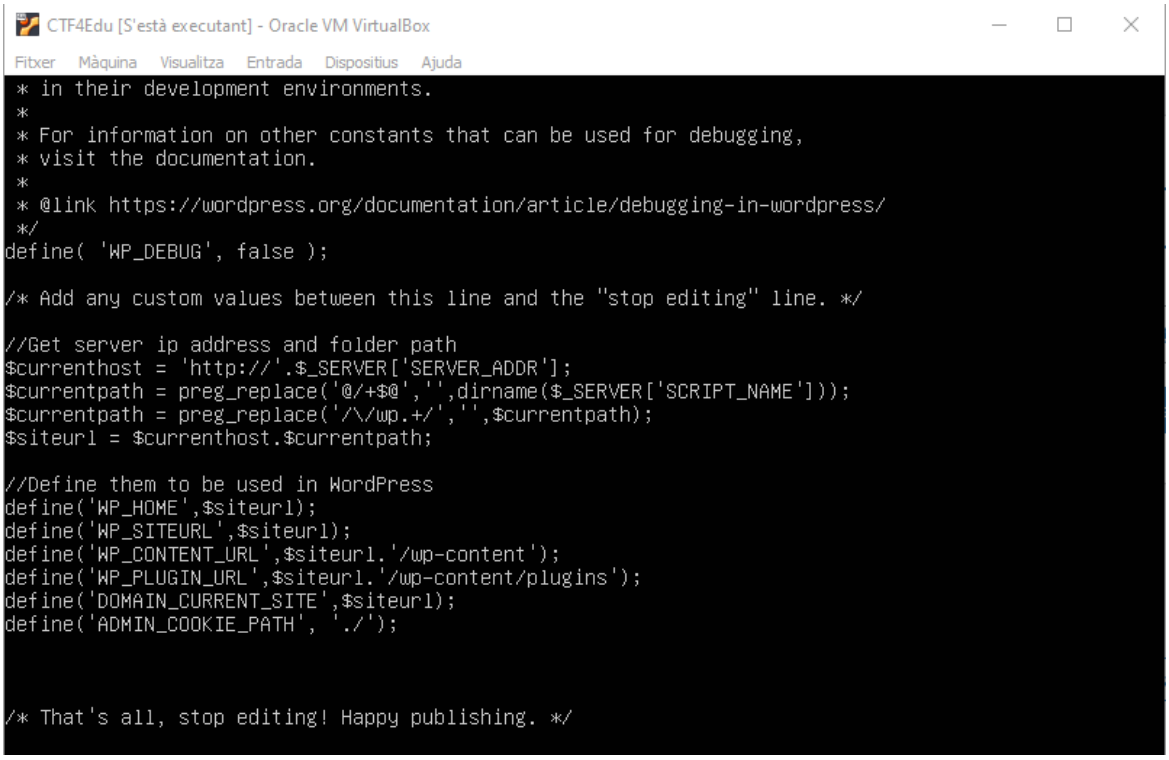
I no saps si d'això en faràs la teva professió d'aquí uns quants anys. Però has descobert una cosa que t'encanta: resoldre reptes.

I aquesta actitud, és una gran actitud per afrontar la vida!

8.5 Repte 2: URL Dinàmica pel site Wordpress

Com que el laboratori es fa sobre màquines virtuals i amb configuració de xarxa en mode pont (*bridge)*, l'adreça IP del servidor de la màquina-objectiu pot anar canviant al llarg de les diferents sessions de laboratori.

Per evitar els problemes d'IP estàtica al site de Wordpress configurat al repte 2 i per a fer que sempre funcioni independentment de que la adreça IP pugui canviar, es modifica el fitxer wp-config-php que hi ha a la carpeta /svr/www/wordpress del servidor per tal de corregir aquest problema[61].



La idea es utilitzar la funcionalitat del PHP per a poder obtenir informació del servidor i de l'entorn d'execució amb a partir de $_SERVER['SERVER_ADDR'], com per exemple la direcció IP del servidor. Després, amb $_SERVER['SCRIPT_NAME'], obtenim la ruta completa i el nom del fitxer de l'script actual.

Explicacions de les expressions regulars:

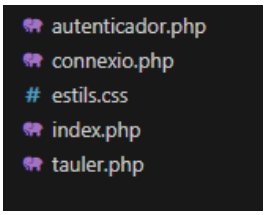
@/+$@ s'utilitza per eliminar el nom del fitxer de la ruta.

[61] LARQQA'S BLOGFOLIO. Consultat per darrera vegada el 26/12/2023 a la URL: https://larqqa.github.io/blog/ideas/wordpress-dynamic-ip/

//wp.+/ s'utilitza per eliminar els noms de les carpetes de Wordpress de la ruta, com per exemple wp-admin.

8.6 Repte 3: Codi Font del Site Vulnerable a Injecció SQL

El *site* consta d'uns pocs fitxers PHP + CSS, ja que es tractava de poder sobretot fer èmfasi en la vulnerabilitat de la injecció SQL i per tant s'ha fet una versió minimalista i vulnerable.



index.php

```php
<!DOCTYPE html>
<html lang="ca">
<head>
    <meta charset="UTF-8">
    <title>Entrada Super Secreta al CTF4Edu</title>
    <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.15.3/css/all.css">
    <link rel="stylesheet" href="estils.css">
</head>
<body>
    <h1>  Benvinguda o benvingut, siguis qui siguis.</h1>
    <p>  Hi ha activitats, com el pentesting, que són una autèntica <b>injecció</b> d'adrenalina.</p>
    <div class="login-container">
        <h2>Iniciar sessió</h2>
        <form action="autenticador.php" method="post">
            <label for="nomusuari"><i class="fas fa-user"></i></label>
            <input type="text" id="nomusuari" name="nomusuari" required>

            <label for="contrasenya"><i class="fas fa-lock"></i></label>
            <input type="password" id="contrasenya" name="contrasenya" required>

            <button type="submit">Accedir <i class="fas fa-sign-in-alt"></i></button>
        </form>
    </div>
</body>
</html>

```

connexio.php

```php
<?php

// Establir connexió amb la base de dades

$servidor= "localhost";

$usuari= "usuariweb";

$password = "4tz1c4c$1p3rS3cr3t";

$basedades = "ctf4edu";

// Comprovar la connexió
$conn = mysqli_connect($servidor, $usuari, $password, $basedades);

if (!$conn) {

    echo("Sembla que alguna cosa no ha anat massa bé. No puc accedir a la base de dades. Em sap greu :-(");

}

?>
```

repte3 > autenticador.php

```php
<?php

include_once 'connexio.php';

// Recollir dades del formulari
$nomusuari = $_POST['nomusuari'];
$contrasenya = $_POST['contrasenya'];

// Consulta SQL per autenticar l'usuari
$sql = "SELECT * FROM usuaris WHERE nomusuari='$nomusuari' AND contrasenya='$contrasenya'";
$resultat = $conn->query($sql);

// Comprovar si l'autenticació és vàlida
if ($resultat->num_rows > 0) {
    header("Location: tauler.php");
    exit();
} else {
    echo $sql;
    echo "<br>\n";
    echo "<h1><strong>Autenticació fallida. Comprova les credencials introduïdes.</strong></h1>";
}


?>
```

repte3 > tauler.php

```php
<!DOCTYPE html>
<html lang="ca">
<head>
    <meta charset="UTF-8">
    <title>Benvinguda</title>
</head>
<body>
    <div>
        <h1>Benvingut/da!</h1>
        <!--
          Ei,

          Ja t'he deixat llesta la maqueta del site. Ara caldria completar el codi i això ho has de fer tu.

          Hauríem de tenir llesta la part del tauler de la web com a molt tard el 01/01/2024!

          Et deixo les meves credencials perquè allà hi tinc material que potser et fa falta.

          Sobretot, no les passis a ningú, ok? Que ja prou forats de seguretat té el servidor aquest...

          Salut!

          usuari: david / p@wd: Tr1c3r4t0p$

          ctf4edu_flag{J4t3nsl4Ll1m0n4P3rL3sc0rb1t}
        -->
    </div>
</body>
</html>

```

8.7 Repte 4: Codi font de la maqueta del *site* de l'usuari david

index.html > ...

```html
<!-- index.html -->

<!DOCTYPE html>
<html lang="ca">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Pàgina Personal d'en David</title>
    <link rel="stylesheet" href="css/styles.css">
</head>
<body>

    <div class="container">
        <h1>Benvingut a la Pàgina Personal d'en David</h1>
        <p>Aquí pots trobar informació sobre mi i altres continguts interessants.</p>

    <!-- Secció Bio -->
        <section class="bio">
            <h2>Biografia</h2>
            <p>Sóc en David, un estudiant del Grau d'Enginyeria Informàtica a la Universitat de Girona.
               El meu objectiu és esdevenir un expert en ciberseguretat i pentesting.
               M'apassiona la idea de dedicar-me en un futur a la formació universitària i utilitzar la
               gamificació com a mètode d'aprenentatge!.</p>
        </section>
    <!-- Fi de la secció Bio -->


        <p>Ah, i sóc de la millor ciutat del món: Saps quina és? Una pista gràfica:</p>

        <img src="images/girona.jpg" alt="Girona">

    </div>

</body>
</html>

```

8.8 Repte 5: Codi font del programa elxefendevi.cpp

endevi.cpp

```cpp
#include <iostream>
#include <string>
#include <locale>

int main() {
    // Configura la localització per admetre caràcters especials
    std::locale::global(std::locale(""));

    // Pregunta a l'usuari pel seu plat preferit en català
    std::cout << "Quin és el meu plat preferit (en minúscules)?";

    // Llegeix la resposta de l'usuari
    std::string resposta_usuari;
    std::getline(std::cin, resposta_usuari);

    // Comprova si la resposta és correcta
    if (resposta_usuari == "escudella") {
        std::cout << "Molt bé! => ctf4edu_flag{JaT3nsG4n4S1p0s0}" << std::endl;
    } else {
        std::cout << "No és aquest el meu plat preferit. No em coneixes prou!" << std::endl;
    }

    return 0;
}
```

8.9 Descàrrega de la imatge .OVA del CTF4Edu

Per poder accedir a la màquina-objectiu d'aquest projecte, es comparteix l'enllaç per a facilitar-ne la descàrrega:

https://drive.google.com/file/d/14KvmxnHKauyag1DX61hX8Tjh0dxrpjex/view?usp=sharing

8.10 Llistat de flags del CTF4Edu

1. Repte 1 => ctf4edu_flag{J4t3nsl4P3rl4n3gr4}
2. Repte 2 => ctf4edu_flag{J4t3ns3lTr3s0r$3cr3t}
3. Repte 3 => ctf4edu_flag{J4t3nsl4Ll1m0n4P3rL3sc0rb1t}
4. Repte 4 => ctf4edu_flag{J4t3nsL4rtD0c1lt4rM1ss4tg3s}
5. Repte 5 => ctf4edu_flag{J4T3nsG4n4S1p0s0}
6. Repte 6 => ctf4edu_flag{JaH4sTr0b4t3lP1ny4l_Br1t1s}
7. Repte 7 => ctf4edu_flag{J4H4sTr0b4tlaP0rt4F0sk4}
8. Repte 8 => ctf4edu_flg{4r4J43tsR00td3l_CTF4edu_F3l1c1t4ts!}

8.11 Llistat de puntuació del CTF4Edu

1. Repte 1 => 100 punts
2. Repte 2 => 300 punts
3. Repte 3 => 300 punts
4. Repte 4 => 250 punts
5. Repte 5 => 300 punts
6. Repte 6 => 300 punts
7. Repte 7 => 300 punts

8. Repte 8 => 300 punts