\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Orchard machine 192.168.xx.112

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

after nmap scan you should see port

3389 open

\*\*\*\*\*

Download this exploit https://www.exploit-db.com/exploits/47519

run it like this

python 192.168.xx.112 3389

it should give you thinVNC login creds

now go to https://192.168.xx.112:3389/ and login using the creds you found, you should access to the target macihne Desktop, now upload nc.exe and get reverse shell.

\*\*\*\*\*\*\*\*

Priv-esc

\*\*\*\*\*\*\*\*\*

you will see "Iperius Backup -Freeware" Software installed in the target machine (this why you have vnc access to the target machine)

proof of concept from exploit-db:

https://www.exploit-db.com/exploits/46863

and you got the root.