

```

File Actions Edit View Help
root@kali: ~#
root@kali: ~# hydra -l /usr/share/wordlists/metasploit/user -p /usr/share/wordlists/metasploit/password ftp://192.168.11.1
hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-27 04:13:18
[0014] max 1 task per 1 server, overall 1 task, 1 login try (111/p/1), +1 try per task
[0074] attacking ftp://192.168.11.1/
[ATTN01] target 192.168.11 - login "/usr/share/wordlists/metasploit/user" - pass "/usr/share/wordlists/metasploit/password" - 1 of 1 [child 0] (0/0)
[0010-ATTN07] target 192.168.11 - login "/usr/share/wordlists/metasploit/user" - pass "/usr/share/wordlists/metasploit/password" - 2 of 1 [child 0] (1/1)
[0010-ATTN07] target 192.168.11 - login "/usr/share/wordlists/metasploit/user" - pass "/usr/share/wordlists/metasploit/password" - 3 of 1 [child 0] (2/2)
[STATUS] 2.00 tries/min, 1 tried in 00:00:01, 1 to do in 00:00:00, 1 active
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-27 04:14:04

root@kali: ~#
root@kali: ~# hydra -l /usr/share/wordlists/metasploit/user -p /usr/share/wordlists/metasploit/password ftp://192.168.11.1
hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-27 04:18:18
[0074] max 1 task per 1 server, overall 1 task, 1 login try (111/p/1), +1 try per task
[0014] attacking ftp://192.168.11.1/
[ATTN01] target 192.168.11 - login "/usr/share/wordlists/metasploit/user" - pass "/usr/share/wordlists/metasploit/password" - 1 of 1 [child 0] (0/0)
[0010-ATTN07] target 192.168.11 - login "/usr/share/wordlists/metasploit/user" - pass "/usr/share/wordlists/metasploit/password" - 2 of 2 [child 0] (1/1)
[STATUS] 2.00 tries/min, 1 tried in 00:00:01, 1 to do in 00:00:00, 1 active
[0010-ATTN07] target 192.168.11 - login "/usr/share/wordlists/metasploit/user" - pass "/usr/share/wordlists/metasploit/password" - 3 of 3 [child 0] (2/2)
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-27 04:19:04

root@kali: ~#

```

```

--(kali@kali)-[~]
--$ nmap -sS 192.3.4
You requested a scan type which requires root privileges.
QUITTING!

--(kali@kali)-[~]
--$ nmap -sS 192.168.2.2
You requested a scan type which requires root privileges.
QUITTING!

--(kali@kali)-[~]
--$ nmap -sT 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-27 03:56 EST
stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
connect Scan Timing: About 20.28% done; ETC: 03:56 (0:00:20 remaining)
stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
connect Scan Timing: About 20.38% done; ETC: 03:56 (0:00:20 remaining)
stats: 0:01:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
connect Scan Timing: About 84.85% done; ETC: 03:57 (0:00:11 remaining)
stats: 0:01:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
connect Scan Timing: About 92.75% done; ETC: 03:57 (0:00:05 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.04s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
1/tcp     open  ftp
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 69.40 seconds

--(kali@kali)-[~]
--$

--(kali@kali)-[~]
--$ nmap -sV 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-27 03:58 EST
stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
service scan Timing: About 0.00% done
stats: 0:01:17 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
service scan Timing: About 0.00% done
stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
service scan Timing: About 50.00% done; ETC: 04:02 (0:01:55 remaining)
stats: 0:02:58 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
service scan Timing: About 50.00% done; ETC: 04:03 (0:02:00 remaining)
stats: 0:03:00 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
service scan Timing: About 50.00% done; ETC: 04:03 (0:02:10 remaining)

```