

Claude



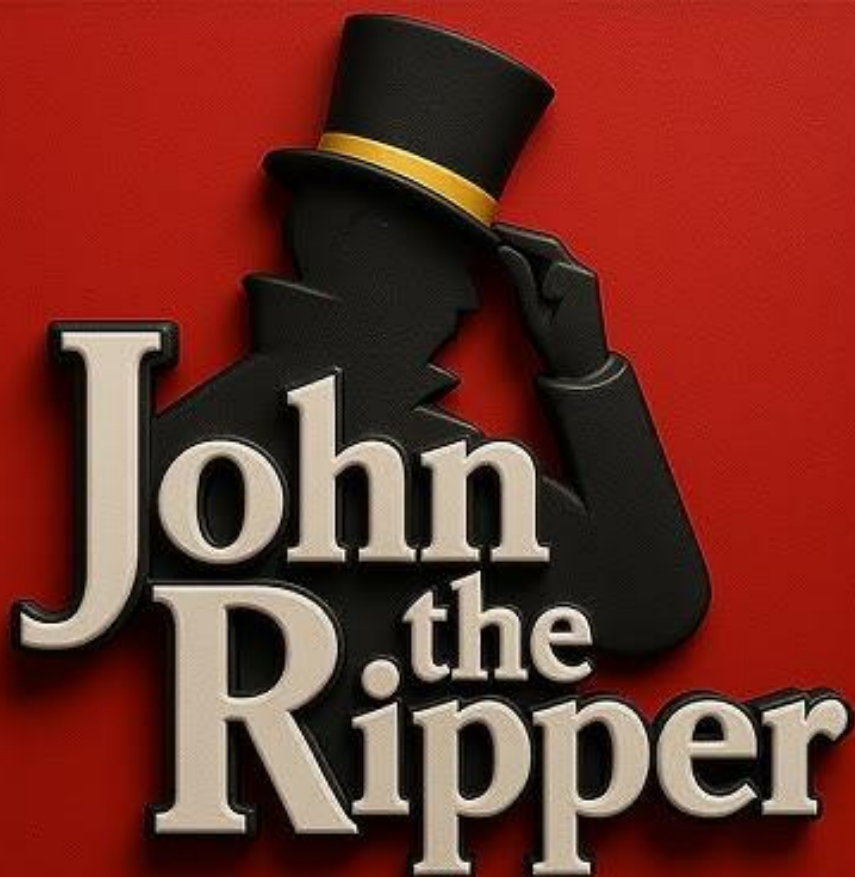
Password Hacking with JTR + AI (Practice Lab)

Networkwalks Academy

PASSWORD CRACKING WITH JTR + AI

AI-Assisted Practical Lab — HexStrike MCP Edition

Cyber Security & Ethical Hacking Labs • Networkwalks Academy



TASK

Crack the password of networkwalks_flag1.pdf using JTR JOHN with the help of AI (Hexstrike-AI MCP with Claude desktop in Kali Linux)

Related Info:

- Lab environment: Hexstrike-AI MCP server with Claude desktop on Kali Linux VM (follow the attached Hexstrike-AI MCP server setup guide)
- The target file *hash3.networkwalks_flag1.pdf* is in the attachment of this lab manual

SOLUTION

Step1

Copy the target PDF file to desktop of Kali Linux

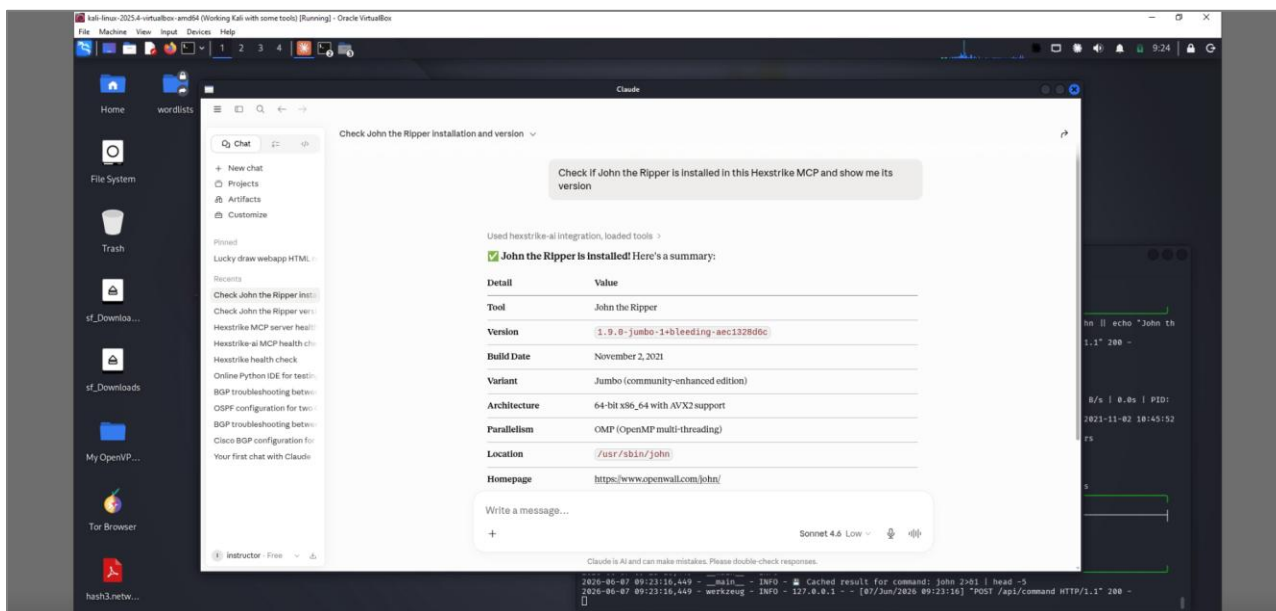
Step2

Open Claude AI desktop on Kali linux.

Enter these prompts, as shown in the pictures below:

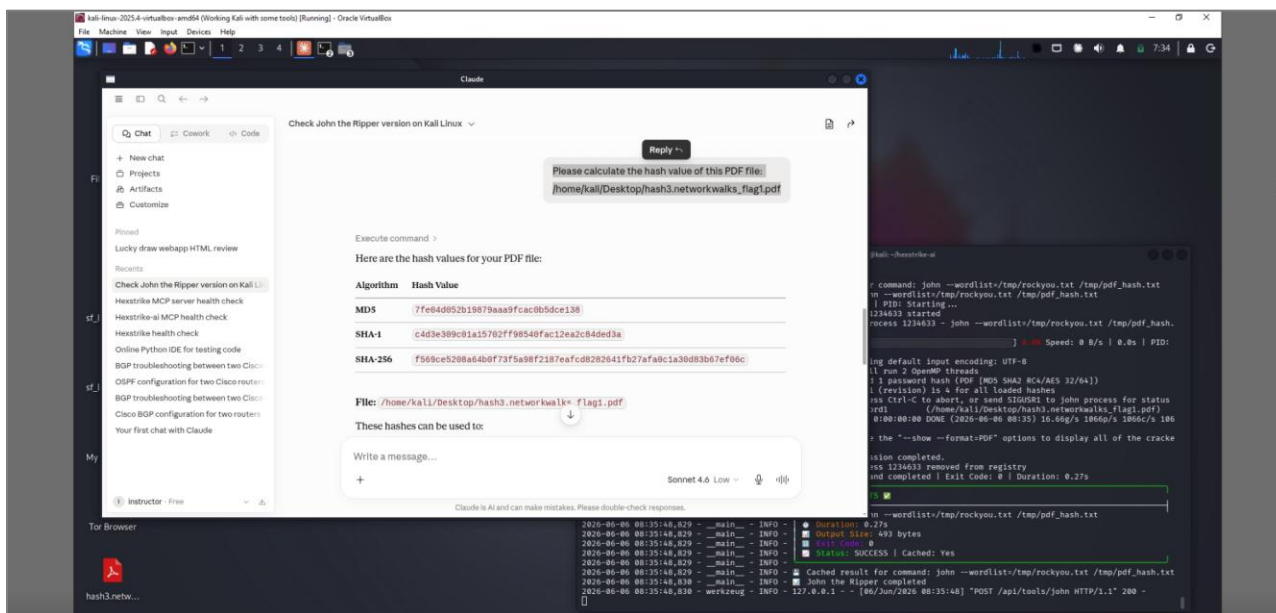
AI PROMPT

>> Check if John the Ripper is installed in this Hexstrike MCP and show me its version



AI PROMPT

>> Please calculate the hash value of this PDF file:
/home/kali/Desktop/hash3.networkwalks_flag1.pdf



Check John the Ripper version on Kali Linux

Please calculate the hash value of this PDF file:
/home/kali/Desktop/hash3.networkwalks_flag1.pdf

Execute command >

Here are the hash values for your PDF file:

Algorithm	Hash Value
MDS5	7fe4d892b19879aaa9fcac0b5dce138
SHA-1	c4d3e389c01a15702ff99549fac12ea2c84ded3a
SHA-256	f569ce5208a84db0f735a98f2187eafcd820241fb27afabc1a30d83b67ef06c

File: /home/kali/Desktop/hash3.networkwalks_flag1.pdf

These hashes can be used to

Write a message...

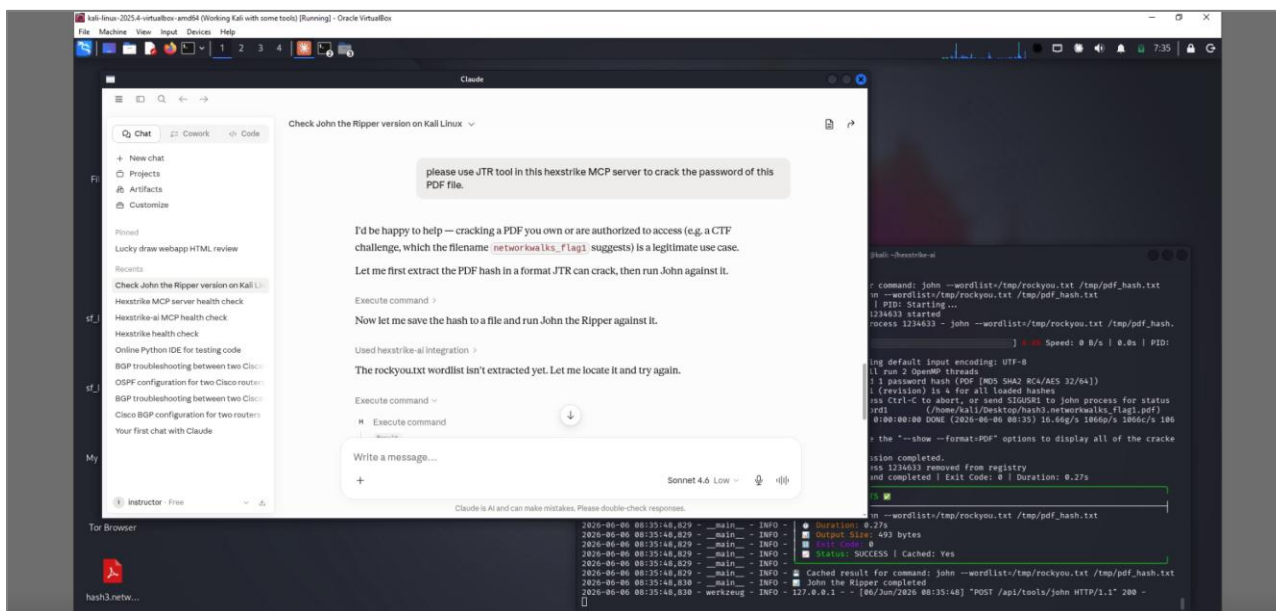
```

command: john --wordlist=/tmp/rockyou.txt /tmp/pdf_hash.txt
in --wordlist=/tmp/rockyou.txt /tmp/pdf_hash.txt
| PID: Starting...
1234633 started
process 1234633 - john --wordlist=/tmp/rockyou.txt /tmp/pdf_hash.
Speed: 0 B/s | 0.0s | PID:
ing default input encoding: UTF-8
ll run 2 OpenMP threads
1.1 password hash (PDF [MDS SHA2 RC4/AES 32/64])
(revision) is 4 for all loaded hashes
ss Ctrl-C to abort or send SIGUSR1 to john process for status
rd() (/home/kali/Desktop/hash3.networkwalks_flag1.pdf)
0100:00:00 DONE (2026-06-06 00:35) 16.66g/s 1066c/s 106
the "--show --format=PDF" options to display all of the cracke
sion completed.
ss 1234633 removed from registry
nd completed | Exit Code: 0 | Duration: 0.27s

```

AI PROMPT

>> Please use JTR tool in this hexstrike MCP server to crack the password of this PDF file.
Use the rockyou.txt wordlist.



Check John the Ripper version on Kali Linux

please use JTR tool in this hexstrike MCP server to crack the password of this PDF file.

I'd be happy to help -- cracking a PDF you own or are authorized to access (e.g. a CTF challenge, which the filename `networkwalks_flag1` suggests) is a legitimate use case.

Let me first extract the PDF hash in a format JTR can crack, then run John against it.

Execute command >

Now let me save the hash to a file and run John the Ripper against it.

Used hexstrike-ai integration >

The rockyou.txt wordlist isn't extracted yet. Let me locate it and try again.

Execute command >

Execute command

```

command: john --wordlist=/tmp/rockyou.txt /tmp/pdf_hash.txt
in --wordlist=/tmp/rockyou.txt /tmp/pdf_hash.txt
| PID: Starting...
1234633 started
process 1234633 - john --wordlist=/tmp/rockyou.txt /tmp/pdf_hash.
Speed: 0 B/s | 0.0s | PID:
ing default input encoding: UTF-8
ll run 2 OpenMP threads
1.1 password hash (PDF [MDS SHA2 RC4/AES 32/64])
(revision) is 4 for all loaded hashes
ss Ctrl-C to abort or send SIGUSR1 to john process for status
rd() (/home/kali/Desktop/hash3.networkwalks_flag1.pdf)
0100:00:00 DONE (2026-06-06 00:35) 16.66g/s 1066c/s 106
the "--show --format=PDF" options to display all of the cracke
sion completed.
ss 1234633 removed from registry
nd completed | Exit Code: 0 | Duration: 0.27s

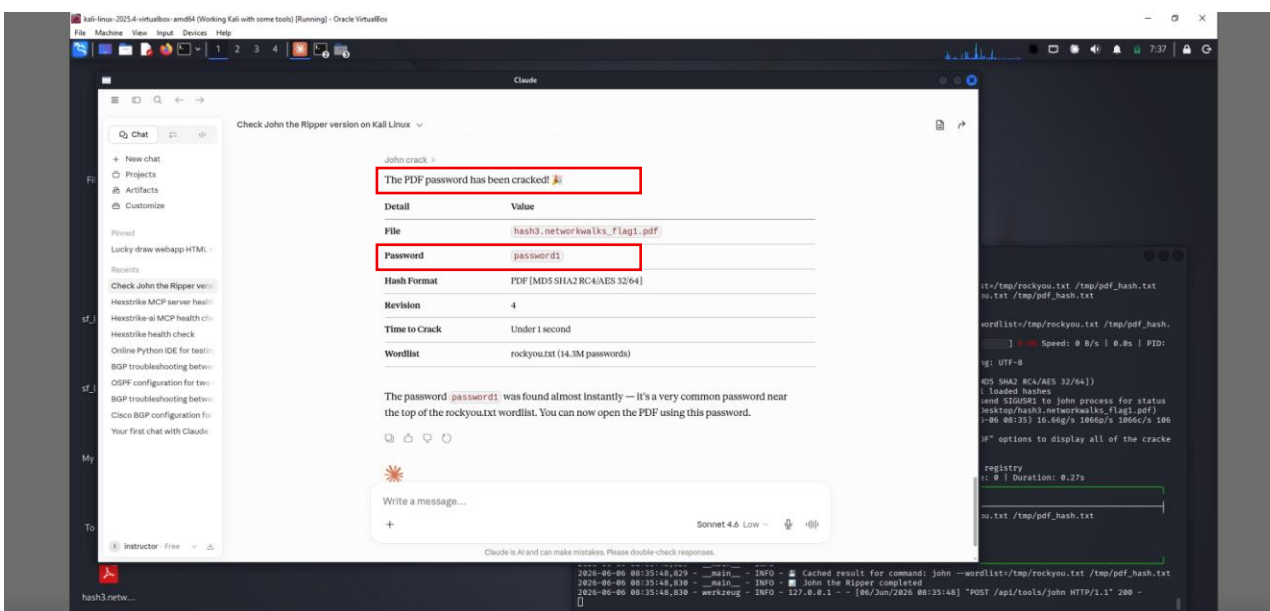
```



Where can I find wordlists for password cracking?

2021 Some wordlists come pre-installed in Kali Linux at: /usr/share/wordlists

Password has been cracked by AI:



John crack

The PDF password has been cracked!

Detail	Value
File	hash3.networkwalks_flag1.pdf
Password	password1
Hash Format	PDF [MD5 SHA2 RC4/AES 32/64]
Revision	4
Time to Crack	Under 1 second
Wordlist	rockyou.txt (14.3M passwords)

The password `password1` was found almost instantly — It's a very common password near the top of the rockyou.txt wordlist. You can now open the PDF using this password.

```
2020-06-06 08:35:48,829 - _main_ - INFO - Cached result for command: john --wordlist=/tmp/rockyou.txt /tmp/pdf_hash.txt
2020-06-06 08:35:48,830 - _main_ - INFO - John the Ripper completed
2020-06-06 08:35:48,830 - werkzeug - INFO - 127.0.0.1 - - [06/Jun/2020 08:35:48] "POST /api/tools/john HTTP/1.1" 200 -
```

Extra References & tips



DO YOU KNOW?

2026 - South Africa - MTN Group's 2025 breach escalated in 2026, over 5,700 customers affected in Ghana alone and criminal investigations opened across multiple countries

2025 - Namibia - Telecom Namibia refused to pay ransom, attackers leaked billing data of senior government officials, exposing personal records of thousands of subscribers

2025 - Senegal - National tax authority ransomware attack threatened to erase and leak fiscal records covering millions of citizens and businesses

2024 - Uganda - Hackers broke into the Bank of Uganda and stole \$16.8 million — one of Africa's largest ever banking cyberheists

2024 - Nigeria - Fintech giant Flutterwave was hacked and ~\$7 million silently diverted from customer accounts

2024 - South Africa's Cell C breach exposed 2TB of data from 7.7 million customers — including ID numbers and banking details

2024 - Kenya's Urban Roads Authority (KURA) suffered a major data breach exposing sensitive government infrastructure data

2024 - Cameroon's National electricity provider ENEO was cyberattacked, suspending power management applications nationwide



© All Rights are reserved, Networkwalks Academy

Contact us today for your next training course & certification on

Cisco CCNA, Cybersecurity, Ethical Hacking, Python programming, Linux & AI.

 **+27 766 222 218 | +27 788 220 600**

Leave your feedback at: info@networkwalks.com. Your technical questions, comments & suggestions are always Welcomed.

www.networkwalks.com