Room 3: Search skills

Summary:

- This room demonstrates how one can leverage the internet to obtain relevant information using special search engines and a variety of search operators.

Objective:

- To effectively explore the internet using specialized search engines, technical documentation, and search operators

Tools Used:

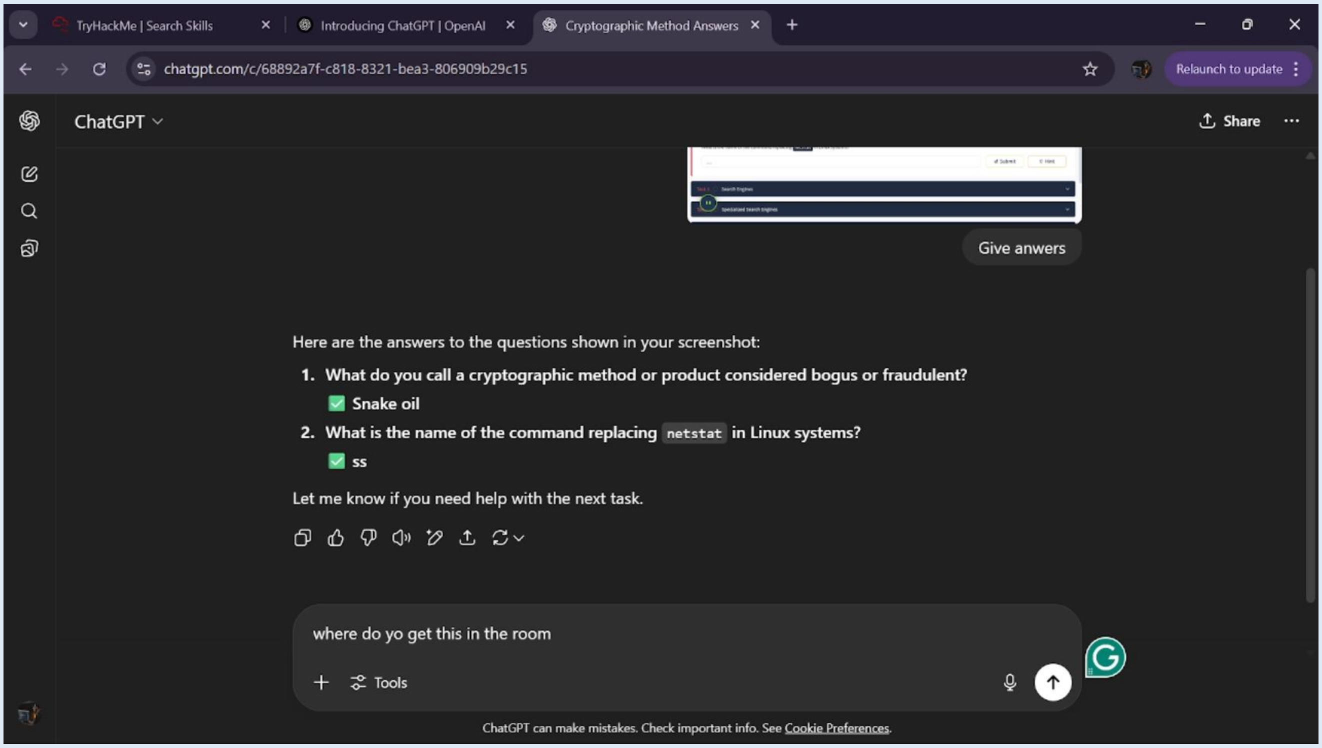
- Google Chrome
- Search Operators:
    - “exact phrase”
    - site:
    - “phrase” -“exact phrase”
    - Filetype:

- Specialized search engines:
    - Shodan
    - Censys
    - Virus.Total
    - Have I Been Pwned

- Critical Vulnerability Exposure & Exploit:
    - CVE Program
    - Exploit Database
    - GitHub
- Microsoft Windows

Steps Taken:

- Evaluated information sources


TryHackMe | Search Skills
Introducing ChatGPT | OpenAI
Cryptographic Method Answers
chatgpt.com/c/68892a7f-c818-8321-bea3-806909b29c15
Relaunch to update
ChatGPT
Share
Tools

Give anwers

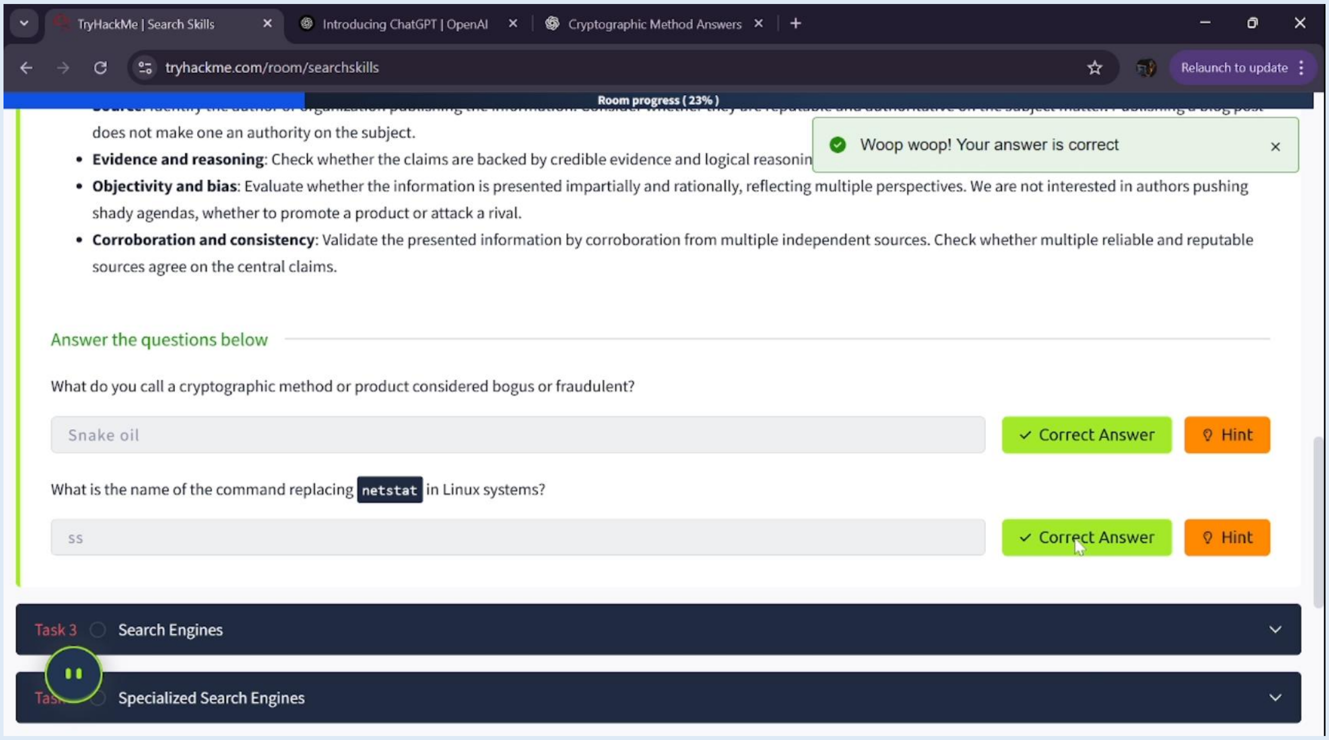
Here are the answers to the questions shown in your screenshot:

1. **What do you call a cryptographic method or product considered bogus or fraudulent?**
   ✅ **Snake oil**
2. **What is the name of the command replacing `netstat` in Linux systems?**
   ✅ **ss**

Let me know if you need help with the next task.

where do yo get this in the room

ChatGPT can make mistakes. Check important info. See Cookie Preferences.


TryHackMe | Search Skills
Introducing ChatGPT | OpenAI
Cryptographic Method Answers
tryhackme.com/room/searchskills
Relaunch to update
Room progress (23%)

does not make one an authority on the subject.

- **Evidence and reasoning**: Check whether the claims are backed by credible evidence and logical reasonin
- **Objectivity and bias**: Evaluate whether the information is presented impartially and rationally, reflecting multiple perspectives. We are not interested in authors pushing shady agendas, whether to promote a product or attack a rival.
- **Corroboration and consistency**: Validate the presented information by corroboration from multiple independent sources. Check whether multiple reliable and reputable sources agree on the central claims.

Woop woop! Your answer is correct

Answer the questions below

What do you call a cryptographic method or product considered bogus or fraudulent?

Snake oil

✓ Correct Answer | Hint

What is the name of the command replacing `netstat` in Linux systems?

ss

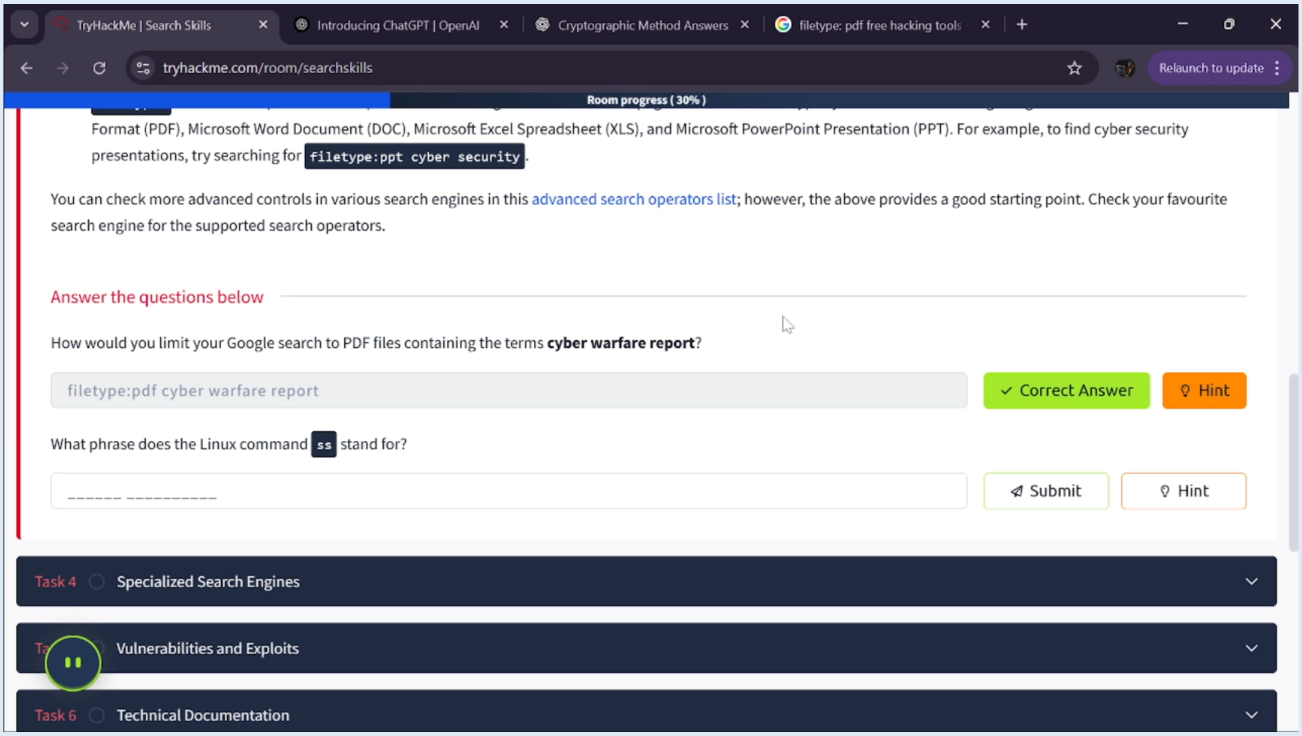
✓ Correct Answer | Hint

Task 3 Search Engines

Specialized Search Engines

- Explored search operators using Google:

Filetype:


TryHackMe | Search Skills
Introducing ChatGPT | OpenAI
Cryptographic Method Answers
filetype: pdf free hacking tools
tryhackme.com/room/searchskills
Relaunch to update
Room progress (30%)

Format (PDF), Microsoft Word Document (DOC), Microsoft Excel Spreadsheet (XLS), and Microsoft PowerPoint Presentation (PPT). For example, to find cyber security presentations, try searching for `filetype:ppt cyber security`.

You can check more advanced controls in various search engines in this advanced search operators list; however, the above provides a good starting point. Check your favourite search engine for the supported search operators.

Answer the questions below

How would you limit your Google search to PDF files containing the terms **cyber warfare report**?

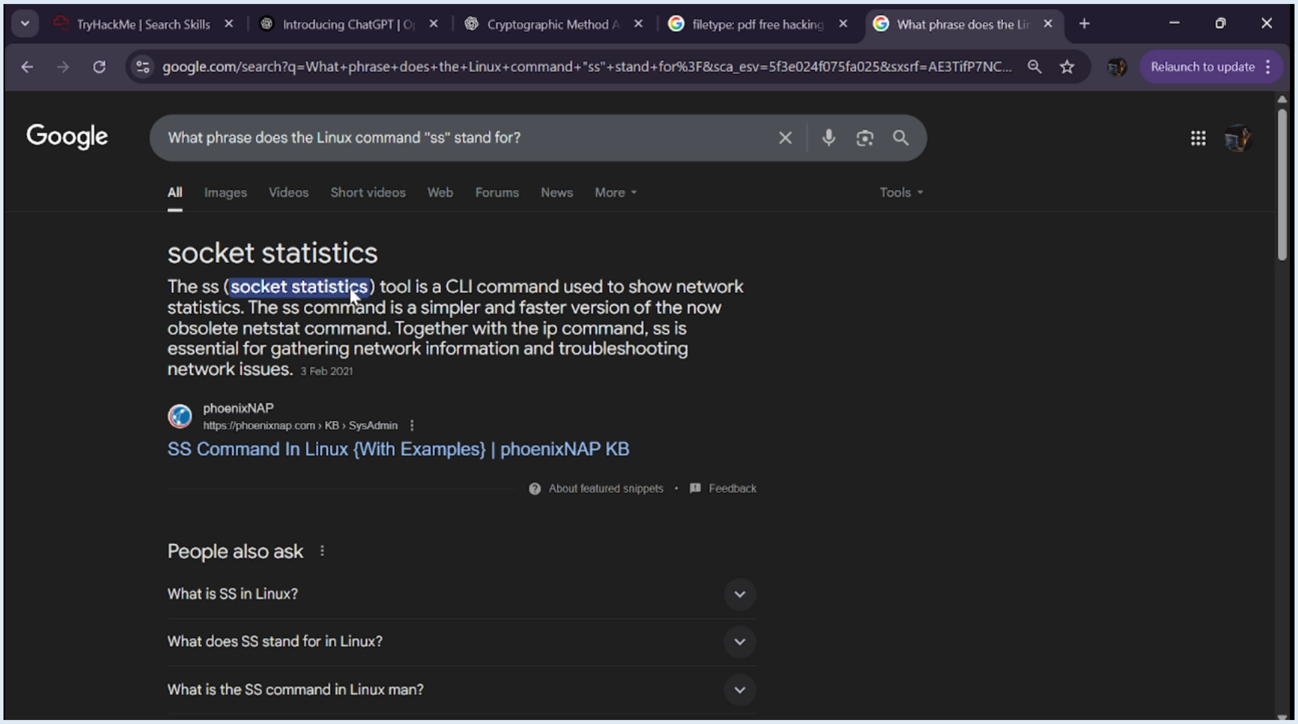
```
filetype:pdf cyber warfare report
```

What phrase does the Linux command `ss` stand for?

______ __________

Submit
Hint
Task 4 Specialized Search Engines
Vulnerabilities and Exploits
Task 6 Technical Documentation

“exact phrase”


TryHackMe | Search Skills
Introducing ChatGPT | O
Cryptographic Method A
filetype: pdf free hacking
What phrase does the Li
google.com/search?q=What+phrase+does+the+Linux+command+"ss"+stand+for%3F&sca_esv=5f3e024f075fa025&sxsrf=AE3TifP7NC...
Relaunch to update
Google
All
Images
Videos
Short videos
Web
Forums
News
More
Tools

What phrase does the Linux command "ss" stand for?

socket statistics

The ss (socket statistics) tool is a CLI command used to show network statistics. The ss command is a simpler and faster version of the now obsolete netstat command. Together with the ip command, ss is essential for gathering network information and troubleshooting network issues. 3 Feb 2021

phoenixNAP
https://phoenixnap.com › KB › SysAdmin
SS Command In Linux {With Examples} | phoenixNAP KB

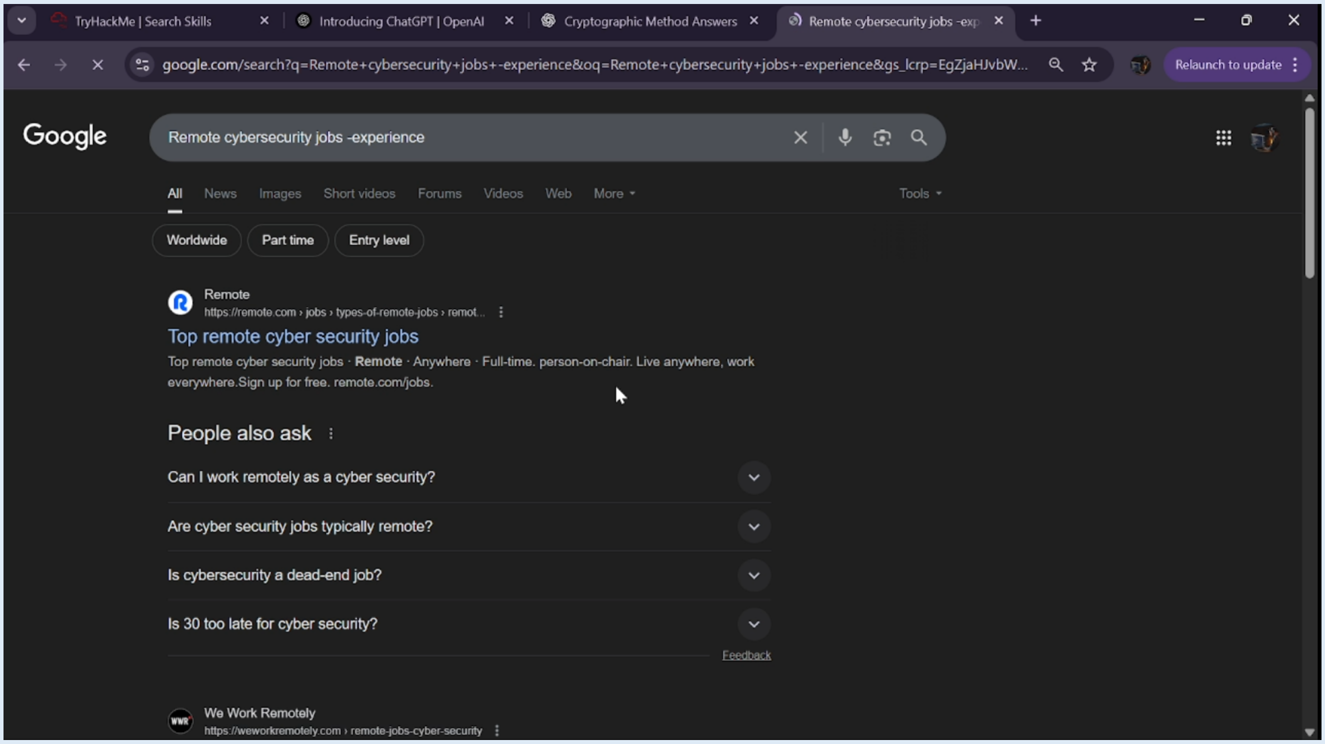
People also ask

What is SS in Linux?

What does SS stand for in Linux?

What is the SS command in Linux man?

“Phrase” -“phrase”


TryHackMe | Search Skills
Introducing ChatGPT | OpenAI
Cryptographic Method Answers
Remote cybersecurity jobs -exp
Relaunch to update
All
News
Images
Short videos
Forums
Videos
Web
More
Tools
Worldwide
Part time
Entry level
Feedback

google.com/search?q=Remote+cybersecurity+jobs+-experience&oq=Remote+cybersecurity+jobs+-experience&gs_lcrp=EgZjaHJvbW...

Google

Remote cybersecurity jobs -experience

Remote
https://remote.com › jobs › types-of-remote-jobs › remot...
Top remote cyber security jobs
Top remote cyber security jobs · **Remote** · Anywhere · Full-time. person-on-chair. Live anywhere, work everywhere.Sign up for free. remote.com/jobs.

People also ask

Can I work remotely as a cyber security?

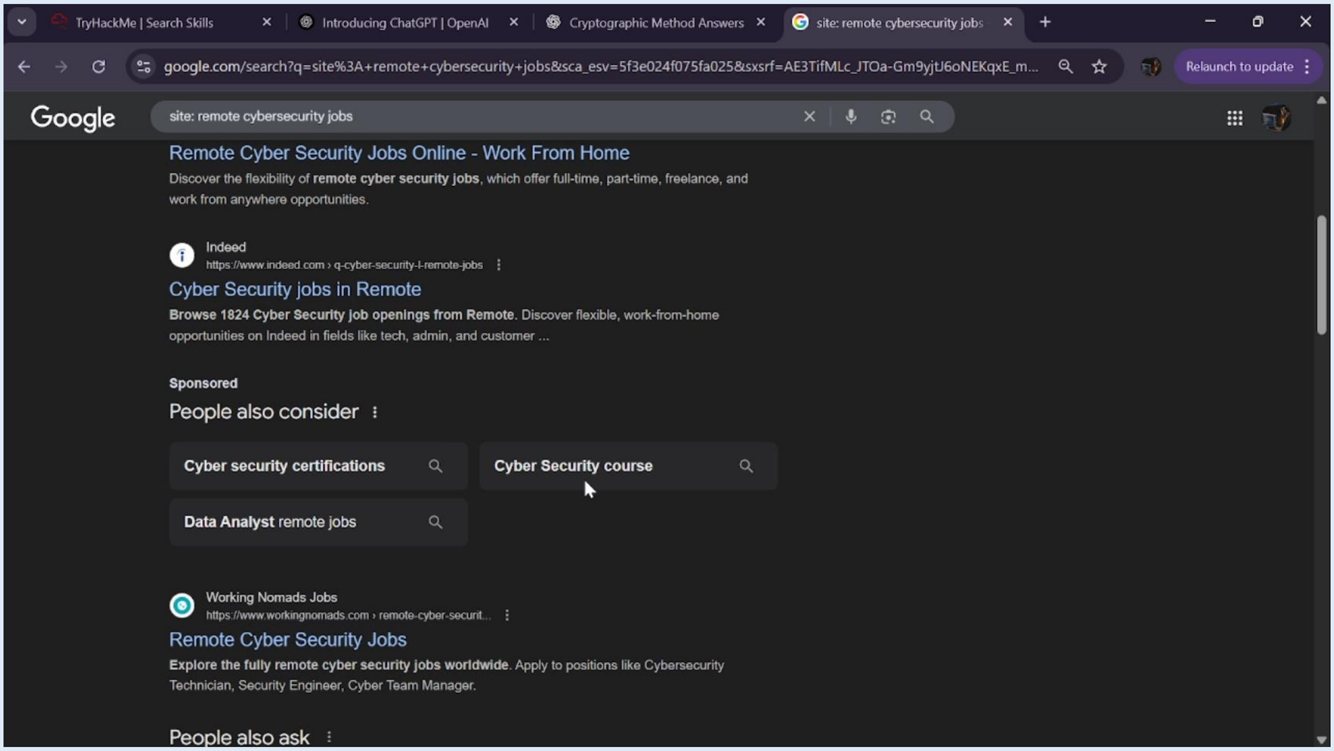
Are cyber security jobs typically remote?

Is cybersecurity a dead-end job?

Is 30 too late for cyber security?

We Work Remotely
https://weworkremotely.com › remote-jobs-cyber-security

Site:


TryHackMe | Search Skills
Introducing ChatGPT | OpenAI
Cryptographic Method Answers
site: remote cybersecurity jobs
Relaunch to update

google.com/search?q=site%3A+remote+cybersecurity+jobs&sca_esv=5f3e024f075fa025&sxsrf=AE3TifMLc_JTOa-Gm9yjU6oNEKqxE_m...

Google

site: remote cybersecurity jobs

Remote Cyber Security Jobs Online - Work From Home
Discover the flexibility of **remote cyber security jobs**, which offer full-time, part-time, freelance, and work from anywhere opportunities.

Indeed
https://www.indeed.com › q-cyber-security-l-remote-jobs
Cyber Security jobs in Remote
Browse 1824 Cyber Security job openings from Remote. Discover flexible, work-from-home opportunities on Indeed in fields like tech, admin, and customer ...

Sponsored

People also consider

Cyber security certifications

Cyber Security course

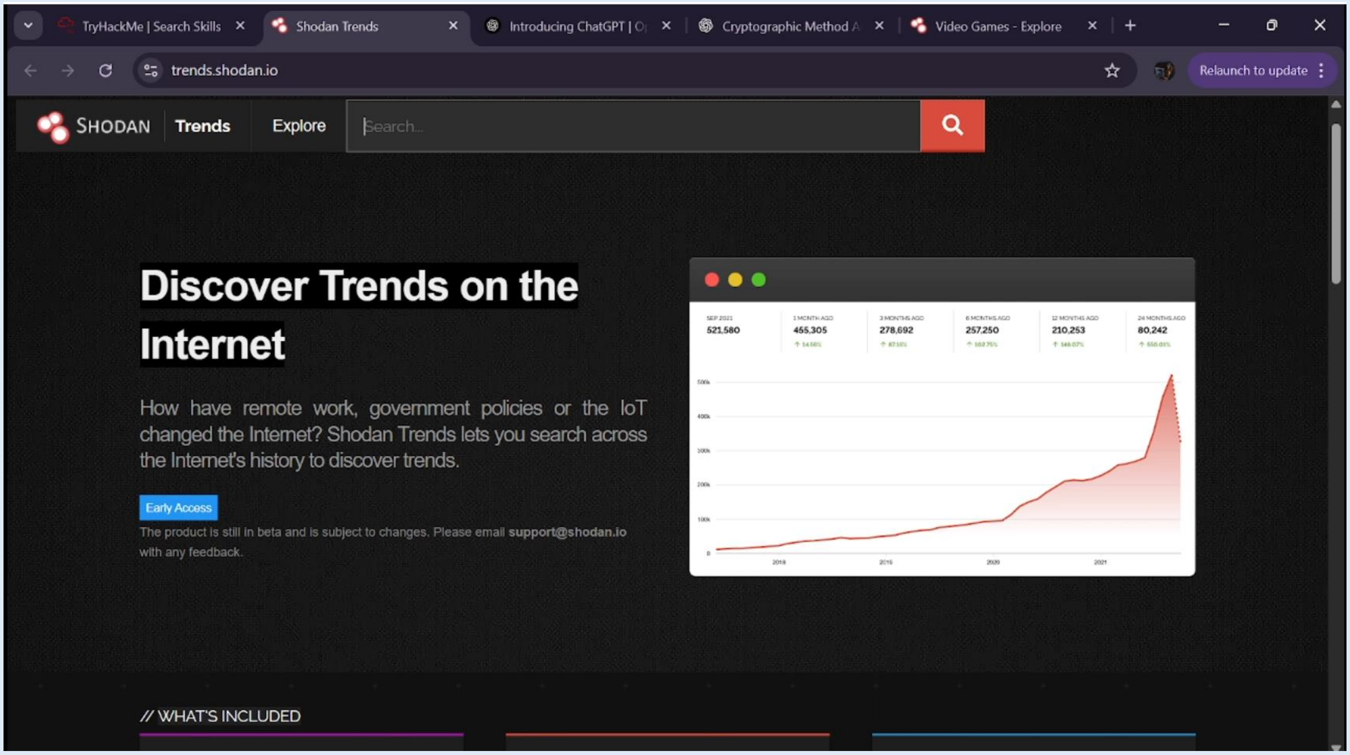
Data Analyst remote jobs

Working Nomads Jobs
https://www.workingnomads.com › remote-cyber-securit...
Remote Cyber Security Jobs
Explore the fully remote cyber security jobs worldwide. Apply to positions like Cybersecurity Technician, Security Engineer, Cyber Team Manager.

People also ask

- Explored specialized search engines:

Shodan



Discover Trends on the Internet

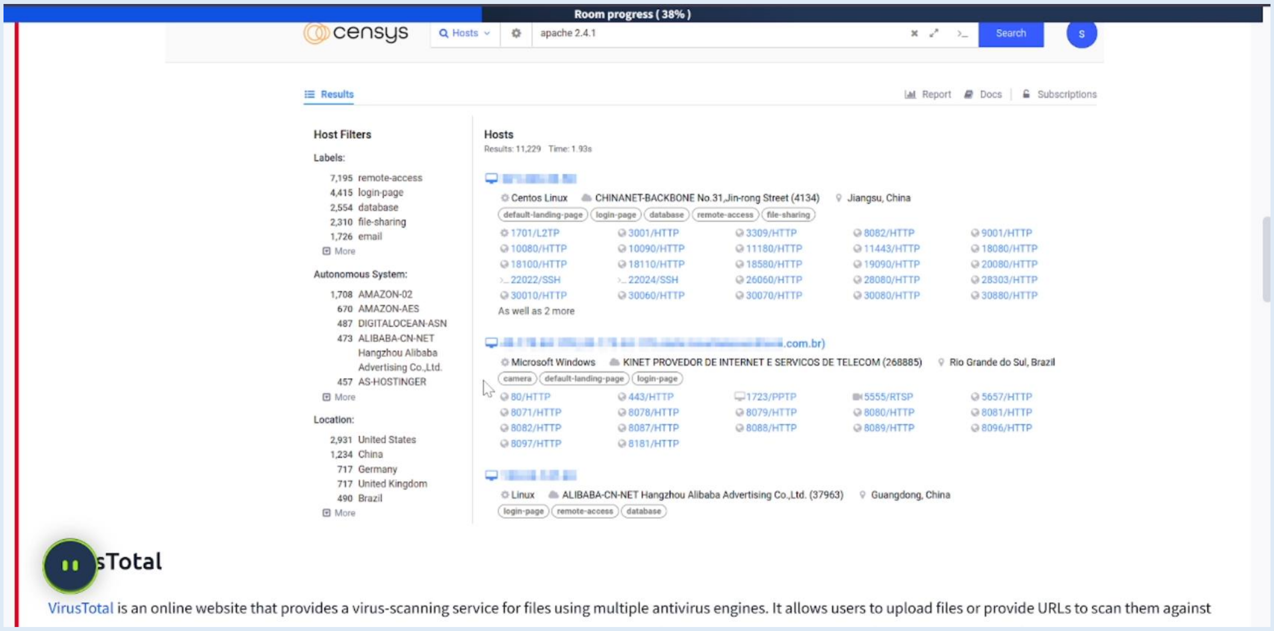
How have remote work, government policies or the IoT changed the Internet? Shodan Trends lets you search across the Internet's history to discover trends.

Early Access

The product is still in beta and is subject to changes. Please email **support@shodan.io** with any feedback.

// WHAT'S INCLUDED

Censys



apache 2.4.1

Host Filters

Labels:

7,195	remote-access
4,415	login-page
2,554	database
2,310	file-sharing
1,726	email

More

Autonomous System:

1,708	AMAZON-02
670	AMAZON-AES
487	DIGITALOCEAN-ASN
473	ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd.
457	AS-HOSTINGER

More

Location:

2,931	United States
1,234	China
717	Germany
717	United Kingdom
490	Brazil

More

Hosts

Results: 11,229 Time: 1.93s

[redacted]

Centos Linux CHINANET-BACKBONE No.31,Jin-rong Street (4134) Jiangsu, China

default-landing-page login-page database remote-access file-sharing

```
1701/L2TP    3001/HTTP    3309/HTTP    8082/HTTP    9001/HTTP
10080/HTTP   10090/HTTP   11180/HTTP   11443/HTTP   18080/HTTP
18100/HTTP   18110/HTTP   18580/HTTP   19090/HTTP   20080/HTTP
22022/SSH    22024/SSH    26060/HTTP   28080/HTTP   28303/HTTP
30010/HTTP   30060/HTTP   30070/HTTP   30080/HTTP   30880/HTTP
```

As well as 2 more

[redacted].com.br)

Microsoft Windows KINET PROVEDOR DE INTERNET E SERVICOS DE TELECOM (268885) Rio Grande do Sul, Brazil

camera default-landing-page login-page

```
80/HTTP      443/HTTP     1723/PPTP    5555/RTSP    5657/HTTP
8071/HTTP    8078/HTTP    8079/HTTP    8080/HTTP    8081/HTTP
8082/HTTP    8087/HTTP    8088/HTTP    8089/HTTP    8096/HTTP
8097/HTTP    8181/HTTP
```

[redacted]

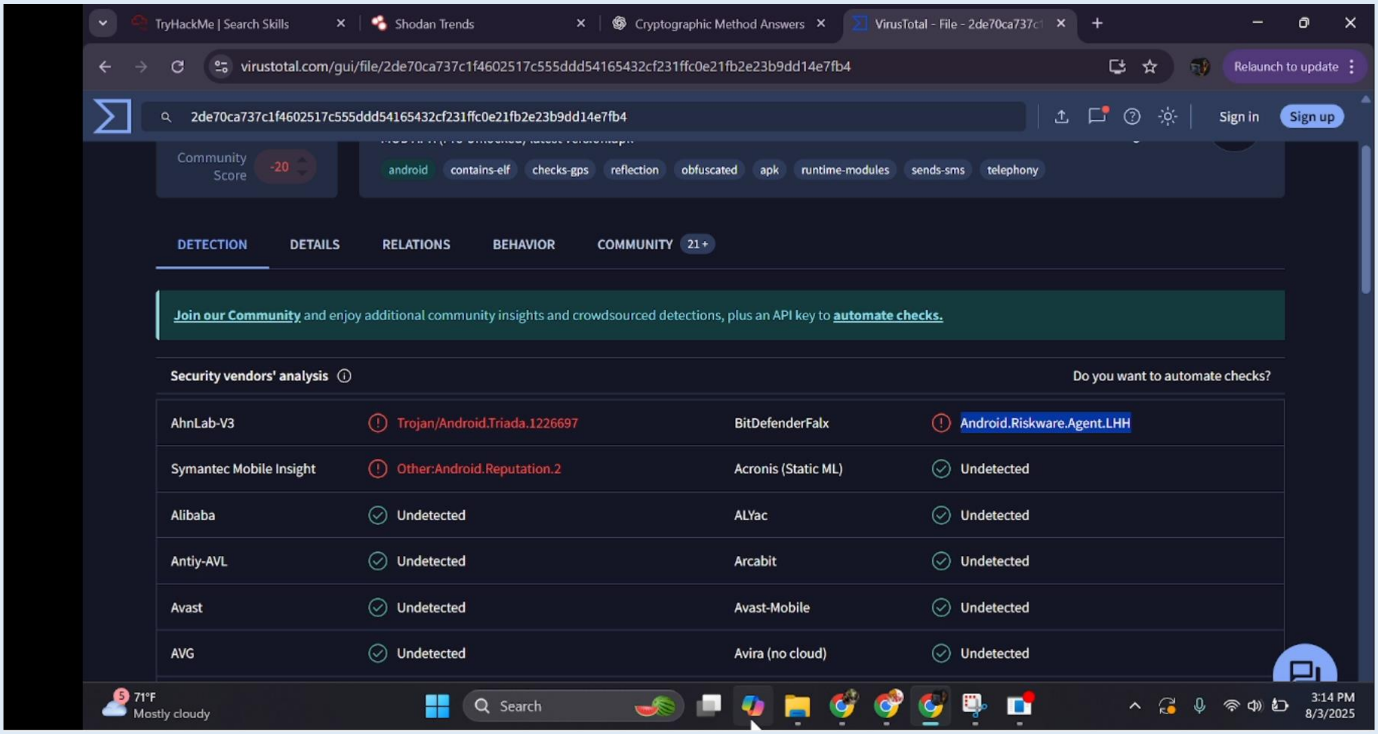
Linux ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd. (37963) Guangdong, China

login-page remote-access database

sTotal

VirusTotal is an online website that provides a virus-scanning service for files using multiple antivirus engines. It allows users to upload files or provide URLs to scan them against

Virus.Total



TryHackMe | Search Skills
Shodan Trends
Cryptographic Method Answers
VirusTotal - File - 2de70ca737c
virustotal.com/gui/file/2de70ca737c1f4602517c555ddd54165432cf231ffc0e21fb2e23b9dd14e7fb4
Relaunch to update
2de70ca737c1f4602517c555ddd54165432cf231ffc0e21fb2e23b9dd14e7fb4
Sign in
Sign up
Community Score
-20
android
contains-elf
checks-gps
reflection
obfuscated
apk
runtime-modules
sends-sms
telephony
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 21+

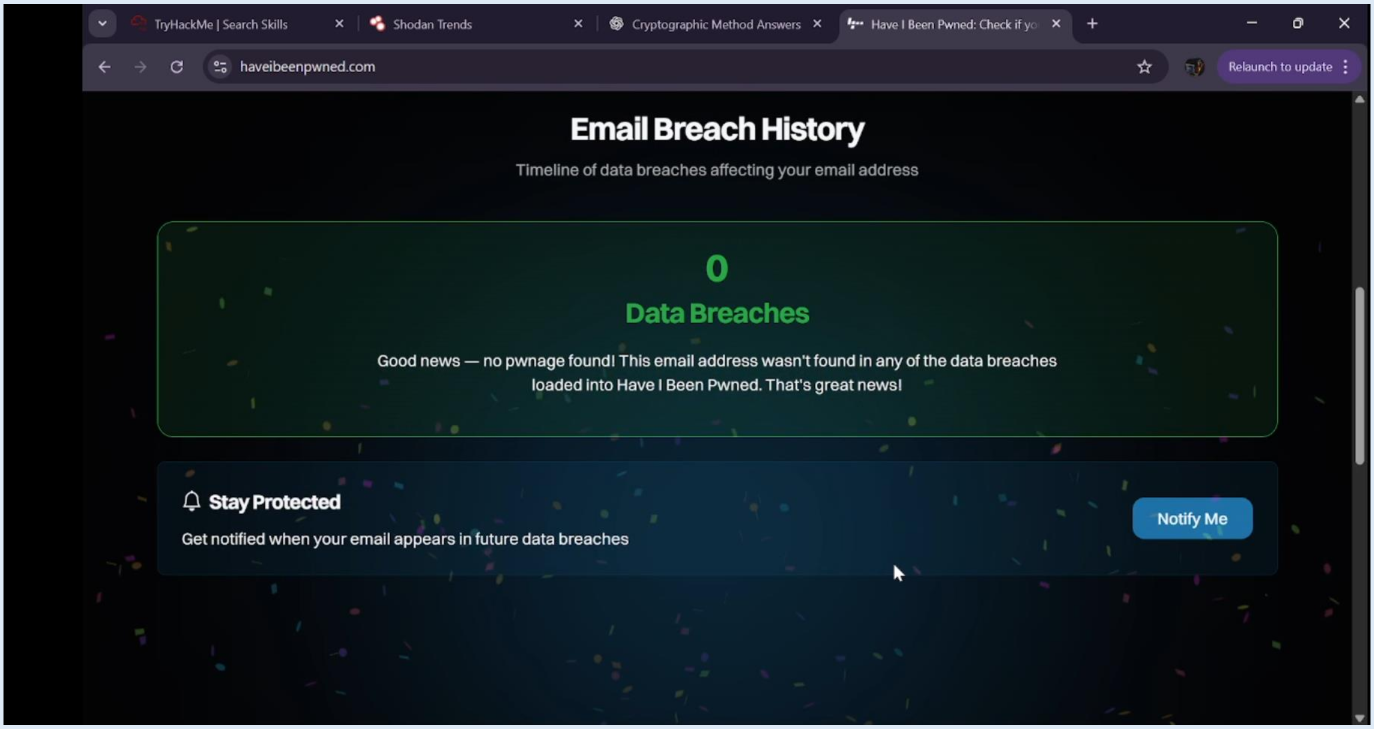
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Android.Triada.1226697	BitDefenderFalx	Android.Riskware.Agent.LHH
Symantec Mobile Insight	Other:Android.Reputation.2	Acronis (Static ML)	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
AVG	Undetected	Avira (no cloud)	Undetected

Have I Been Pwned



TryHackMe | Search Skills
Shodan Trends
Cryptographic Method Answers
Have I Been Pwned: Check if yo
haveibeenpwned.com
Relaunch to update

Email Breach History

Timeline of data breaches affecting your email address

0

Data Breaches

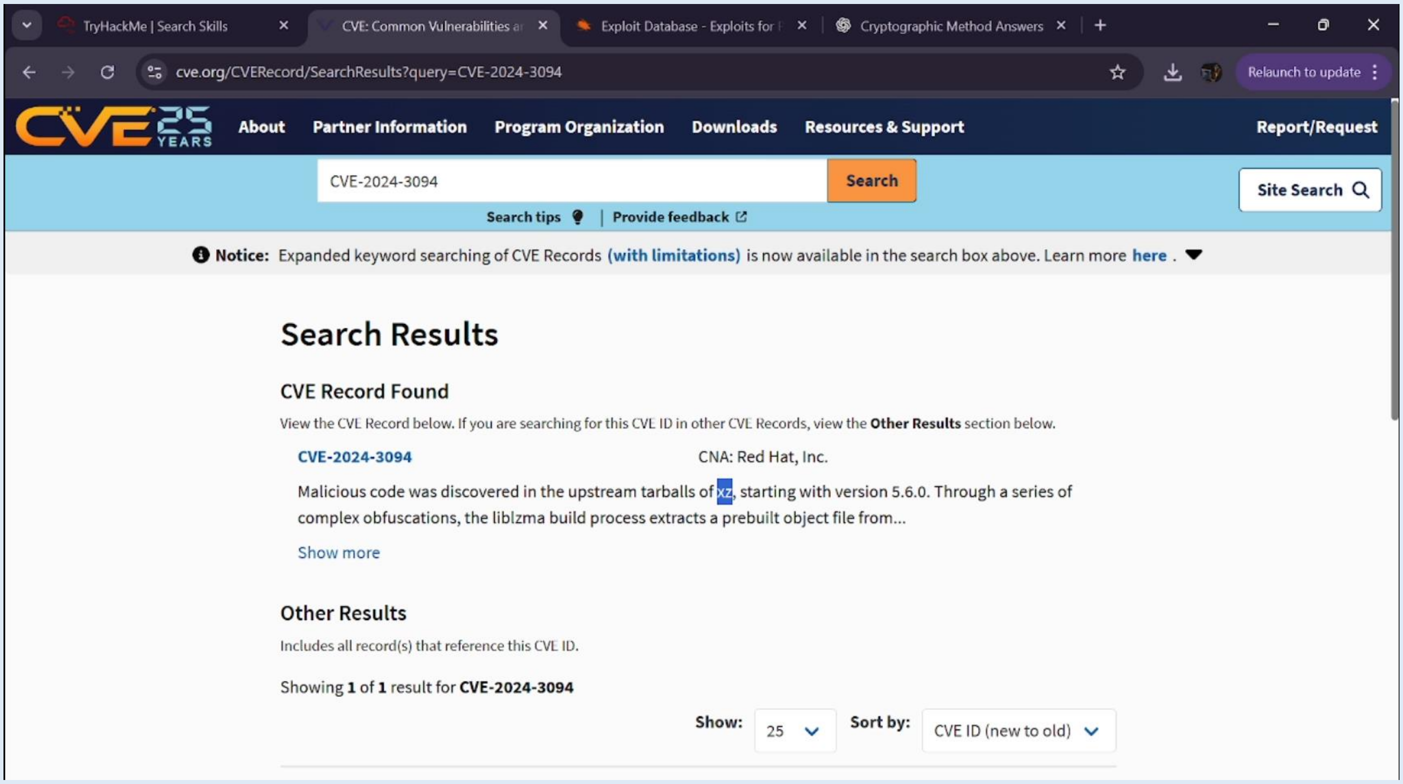
Good news — no pwnage found! This email address wasn't found in any of the data breaches loaded into Have I Been Pwned. That's great news!

Stay Protected

Get notified when your email appears in future data breaches

- Demonstrated how to use search for vulnerabilities:

CVE Database


TryHackMe | Search Skills
CVE: Common Vulnerabilities a
Exploit Database - Exploits for
Cryptographic Method Answers
cve.org/CVERecord/SearchResults?query=CVE-2024-3094
Relaunch to update
About
Partner Information
Program Organization
Downloads
Resources & Support
Report/Request
Search
Site Search
Search tips
Provide feedback

CVE-2024-3094

Notice: Expanded keyword searching of CVE Records **(with limitations)** is now available in the search box above. Learn more **here**.

Search Results

CVE Record Found

View the CVE Record below. If you are searching for this CVE ID in other CVE Records, view the **Other Results** section below.

CVE-2024-3094 CNA: Red Hat, Inc.

Malicious code was discovered in the upstream tarballs of xz, starting with version 5.6.0. Through a series of complex obfuscations, the liblzma build process extracts a prebuilt object file from...

Show more

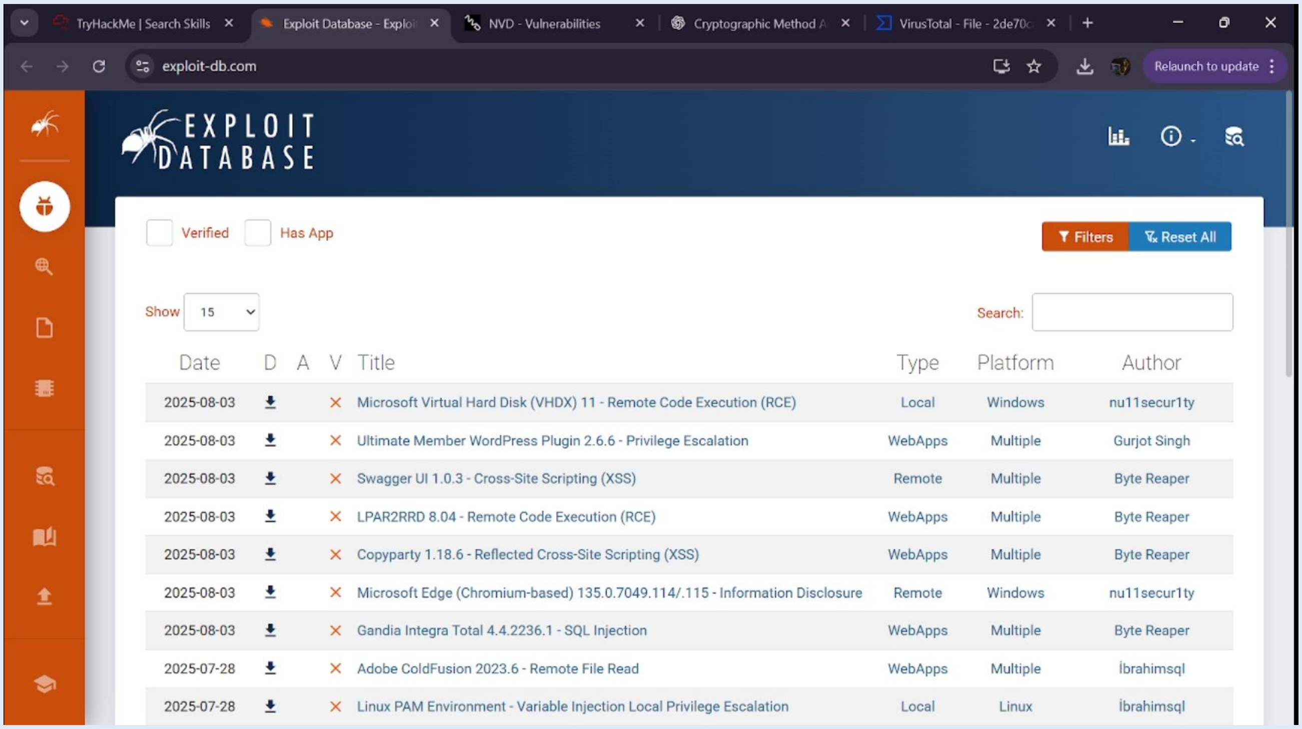
Other Results

Includes all record(s) that reference this CVE ID.

Showing **1** of **1** result for **CVE-2024-3094**

Show: 25 **Sort by:** CVE ID (new to old)

Exploit Database

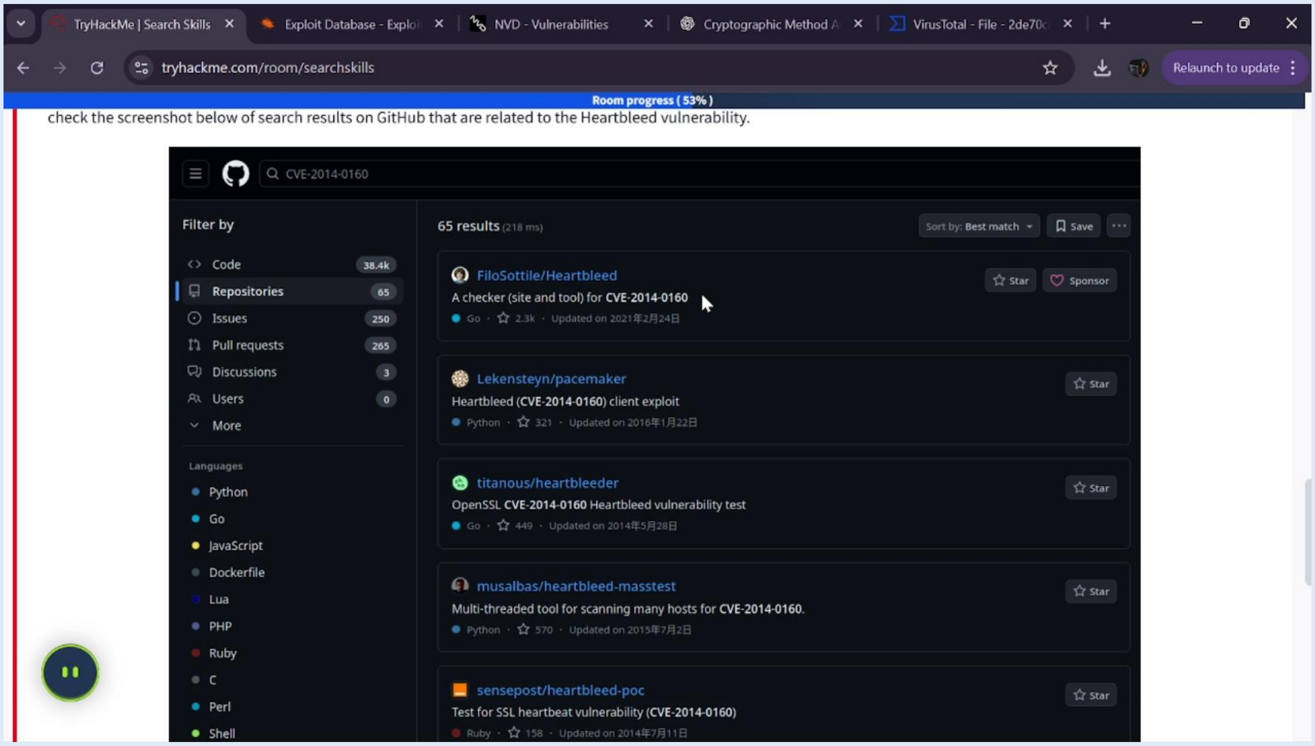


□ Verified □ Has App

Show 15 Search:

Date	D	A	V	Title	Type	Platform	Author
2025-08-03	⬇		✗	Microsoft Virtual Hard Disk (VHDX) 11 - Remote Code Execution (RCE)	Local	Windows	nu11secur1ty
2025-08-03	⬇		✗	Ultimate Member WordPress Plugin 2.6.6 - Privilege Escalation	WebApps	Multiple	Gurjot Singh
2025-08-03	⬇		✗	Swagger UI 1.0.3 - Cross-Site Scripting (XSS)	Remote	Multiple	Byte Reaper
2025-08-03	⬇		✗	LPAR2RRD 8.04 - Remote Code Execution (RCE)	WebApps	Multiple	Byte Reaper
2025-08-03	⬇		✗	Copyparty 1.18.6 - Reflected Cross-Site Scripting (XSS)	WebApps	Multiple	Byte Reaper
2025-08-03	⬇		✗	Microsoft Edge (Chromium-based) 135.0.7049.114/.115 - Information Disclosure	Remote	Windows	nu11secur1ty
2025-08-03	⬇		✗	Gandia Integra Total 4.4.2236.1 - SQL Injection	WebApps	Multiple	Byte Reaper
2025-07-28	⬇		✗	Adobe ColdFusion 2023.6 - Remote File Read	WebApps	Multiple	İbrahimsql
2025-07-28	⬇		✗	Linux PAM Environment - Variable Injection Local Privilege Escalation	Local	Linux	İbrahimsql

GitHub



check the screenshot below of search results on GitHub that are related to the Heartbleed vulnerability.

65 results (218 ms)

FiloSottile/Heartbleed
A checker (site and tool) for CVE-2014-0160
Go · 2.3k · Updated on 2021年2月24日

Lekensteyn/pacemaker
Heartbleed (CVE-2014-0160) client exploit
Python · 321 · Updated on 2016年1月22日

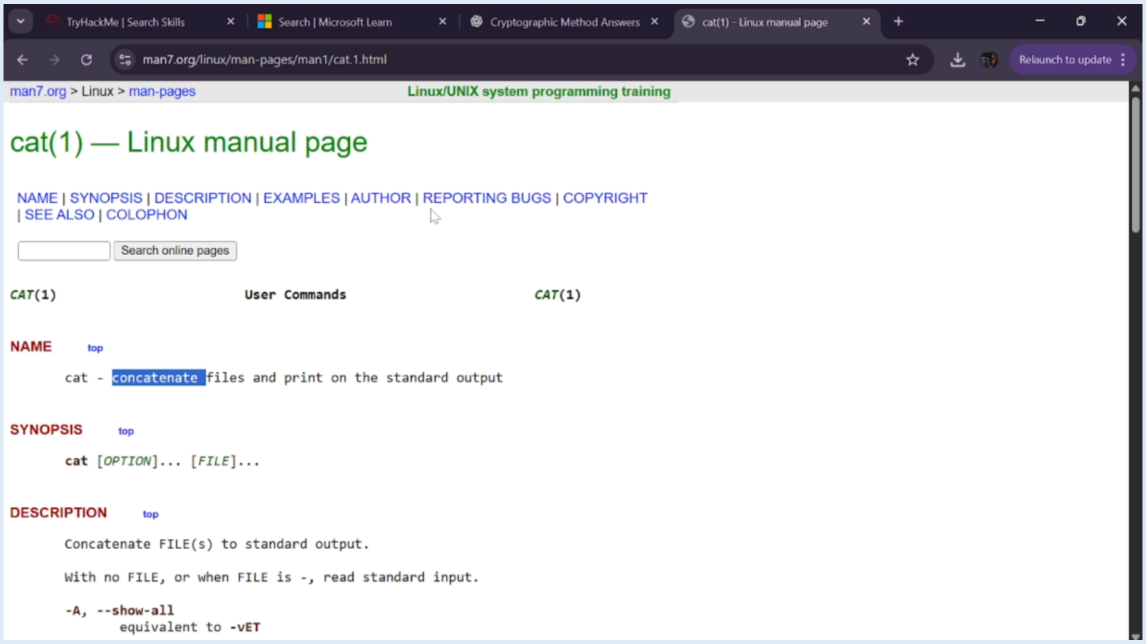
titanous/heartbleeder
OpenSSL CVE-2014-0160 Heartbleed vulnerability test
Go · 449 · Updated on 2014年5月28日

musalbas/heartbleed-masstest
Multi-threaded tool for scanning many hosts for CVE-2014-0160.
Python · 570 · Updated on 2015年7月2日

sensepost/heartbleed-poc
Test for SSL heartbeat vulnerability (CVE-2014-0160)
Ruby · 158 · Updated on 2014年7月11日

- Demonstrated the use of technical documentation through:

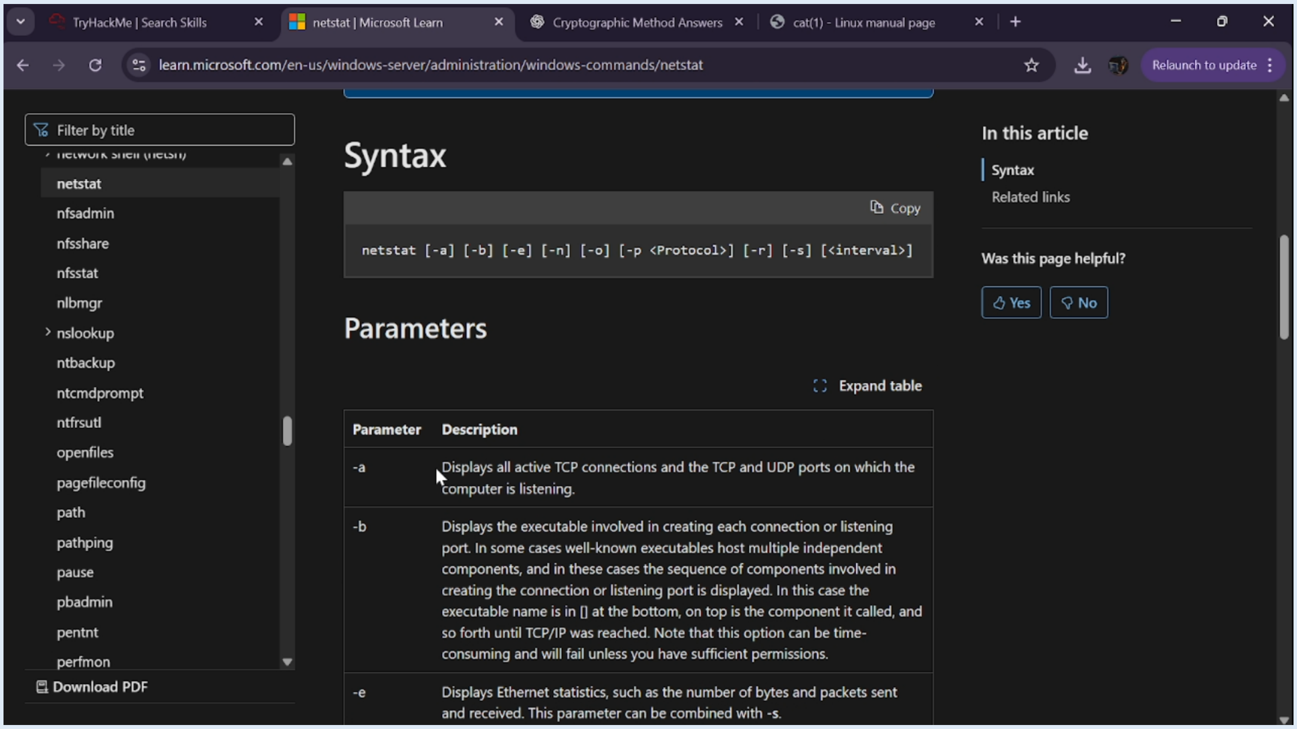
Linux Manual page


TryHackMe | Search Skills
Search | Microsoft Learn
Cryptographic Method Answers
cat(1) - Linux manual page
man7.org/linux/man-pages/man1/cat.1.html
Relaunch to update
man7.org > Linux > man-pages
Linux/UNIX system programming training
NAME | SYNOPSIS | DESCRIPTION | EXAMPLES | AUTHOR | REPORTING BUGS | COPYRIGHT | SEE ALSO | COLOPHON
Search online pages
top

cat(1) — Linux manual page

```
CAT(1)                        User Commands                        CAT(1)

NAME
       cat - concatenate files and print on the standard output

SYNOPSIS
       cat [OPTION]... [FILE]...

DESCRIPTION
       Concatenate FILE(s) to standard output.

       With no FILE, or when FILE is -, read standard input.

       -A, --show-all
              equivalent to -vET
```

Microsoft Windows – Product Documentation



Syntax

```
netstat [-a] [-b] [-e] [-n] [-o] [-p <Protocol>] [-r] [-s] [<interval>]
```

Parameters

Parameter	Description
-a	Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
-b	Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.
-e	Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.

Flag(s):

No flag(s) found

Lessons Learned:

I learned how to:

- Utilize search operators to explore the internet
- Use specialized search engines
- Search for vulnerabilities and exploits
- Fetch information via technical documentation