🔍

Search Skills

Creado por	 Ammi González
Etiquetas	TryHackMe
Fecha de creación	@2 de febrero de 2026 13:32

🟢 Introduction

A quick Google search for “learn cyber security” returned around 600 million hits, while a search for “learn hacking” returned more than double that number! The number might have grown even further with time.

📋 Evaluation of Search Results

On the Internet, everyone can publish their writings. It can be in the form of blog posts, articles, or social media posts. It can be even in more subtle ways, such as by editing a public wiki page. This ability makes it possible for anyone to voice their unfounded claims. Everyone can express their opinion about best cyber security practices, future programming trends, and how to best prepare for a DevSecOps interview.

It is our job, as readers, to evaluate the information. What to consider when evaluating information:

- **Source**: Identify the author or organization publishing the information. Consider whether they are reputable and authoritative on the subject matter. Publishing a blog post does not make one an authority on the subject.
- **Evidence and reasoning**: Check whether the claims are backed by credible evidence and logical reasoning. We are seeking hard facts and solid arguments.

- **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.

🐍 Snake Oil

A cryptographic method or product considered bogus or fraudulent.

⌨️ ss (socket statistics)

Is the name of the command replacing `netstat` in Linux systems.

🖥️ netstat (network statistics)

Is a classic command-line utility in Linux used for monitoring network connections, viewing routing tables, and displaying network interface statistics. It is a versatile tool for system administrators to diagnose network issues and perform security analysis.

🛜 Search Engines

Operators supported by Google.

- `"exact phrase"`: Double quotes indicate that you are looking for pages with the exact word or phrase. For example, one might search for `"passive reconnaissance"` to get pages with this exact phrase.
- `site:`: This operator lets you specify the domain name to which you want to limit your search. For example, we can search for success stories on TryHackMe using `site:tryhackme.com success stories`.
- `-`: The minus sign allows you to omit search results that contain a particular word or phrase. For example, you might be interested in learning about the

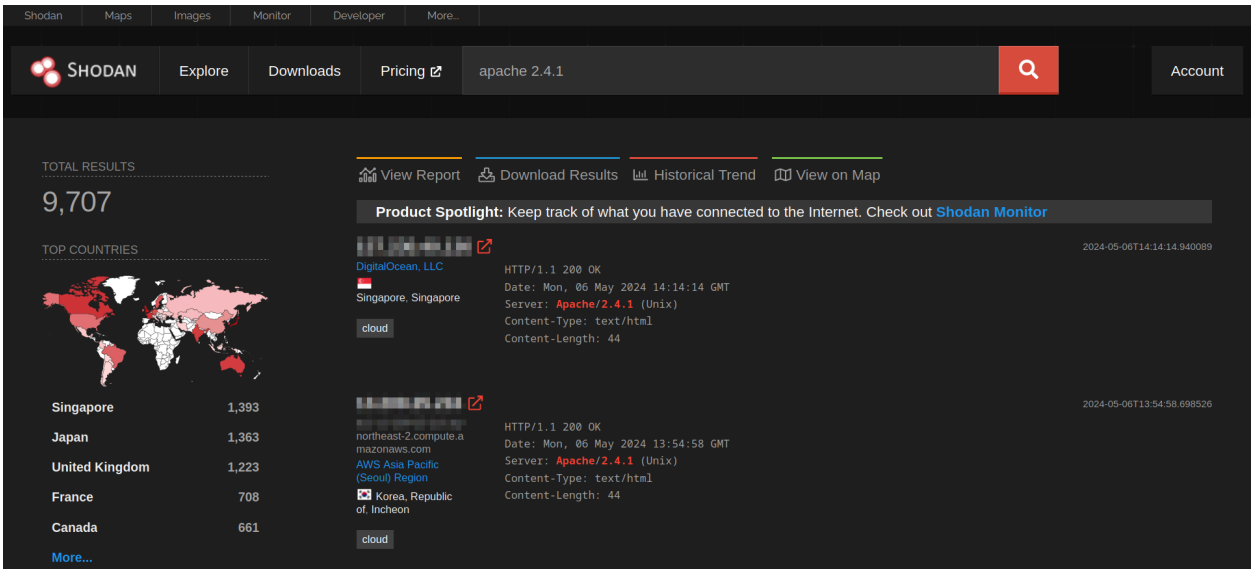
pyramids, but you don't want to view tourism websites; one approach is to search for `pyramids -tourism` or `tourism pyramids`.

- `filetype:`: This search operator is indispensable for finding files instead of web pages. Some of the file types you can search for using Google are Portable Document 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`.

🎏 Specialized Search Engines

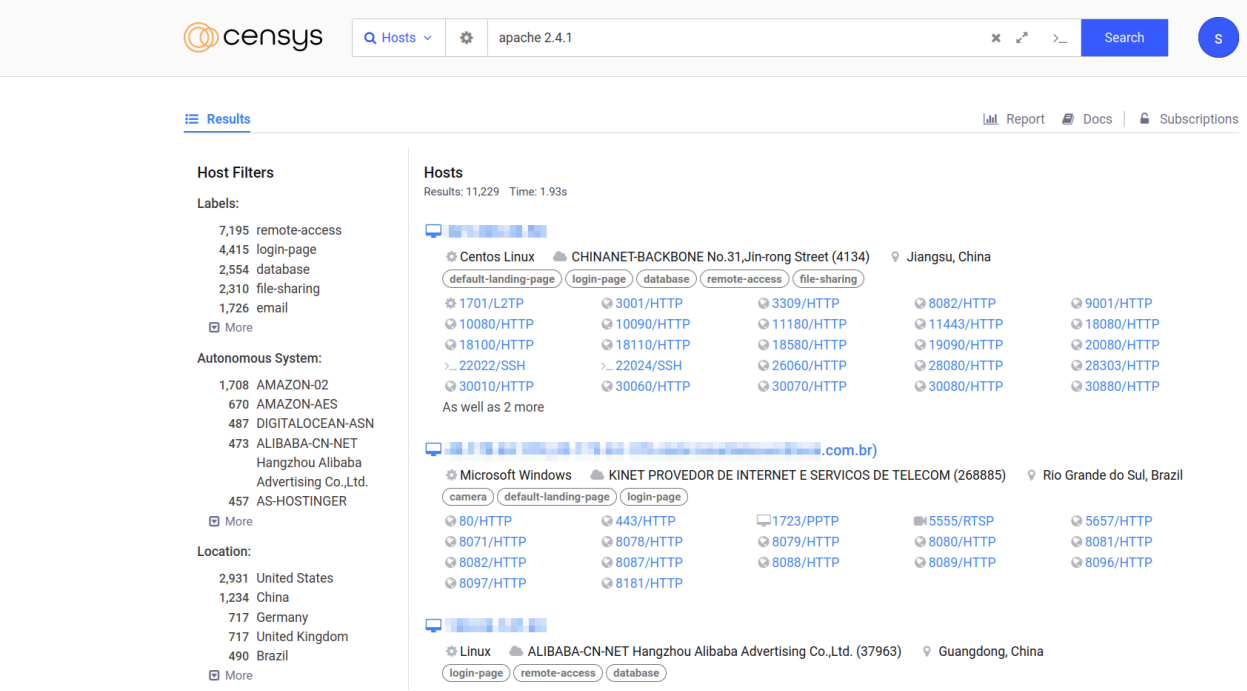
💻 Shodan

a search engine for devices connected to the Internet. It allows you to search for specific types and versions of servers, networking equipment, industrial control systems, and IoT devices. You may want to see how many servers are still running Apache 2.4.1 and the distribution across countries. To find the answer, we can search for `apache 2.4.1`, which will return the list of servers with the string "apache 2.4.1" in their headers.



🟠 Censys

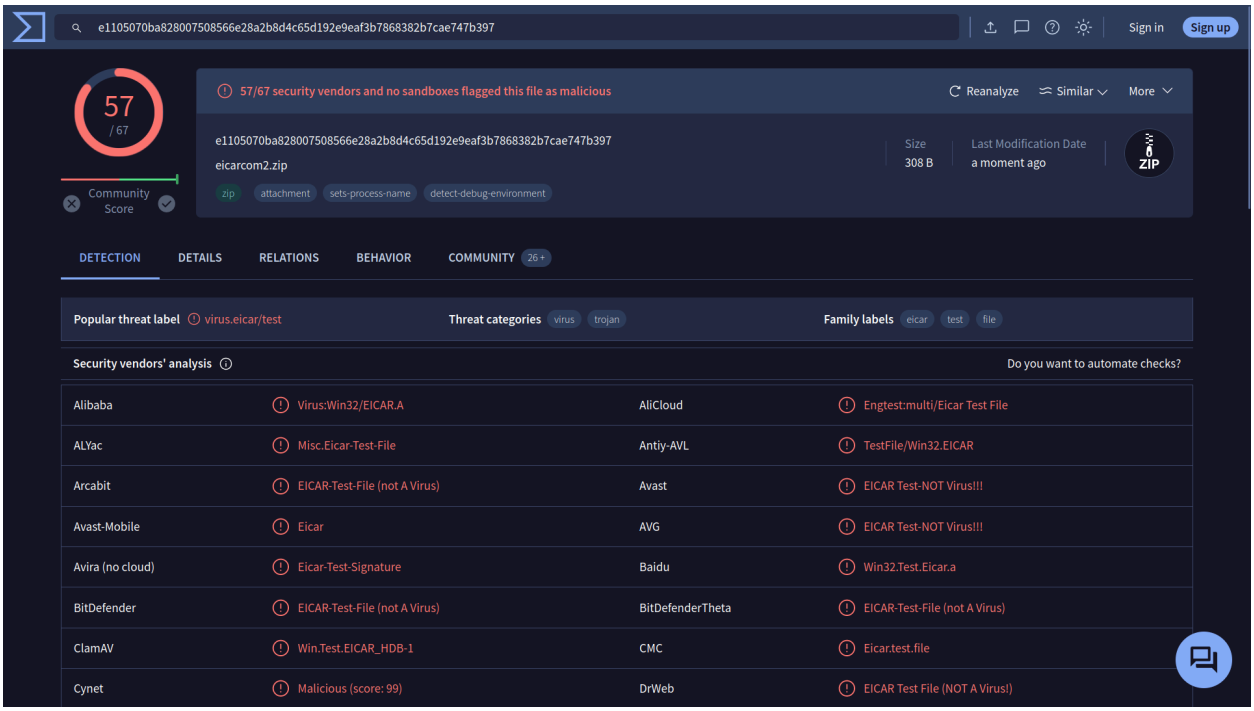
Focuses on Internet-connected hosts, websites, certificates, and other Internet assets. Some of its use cases include enumerating domains in use, auditing open ports and services, and discovering rogue assets within a network.



VirusTotal

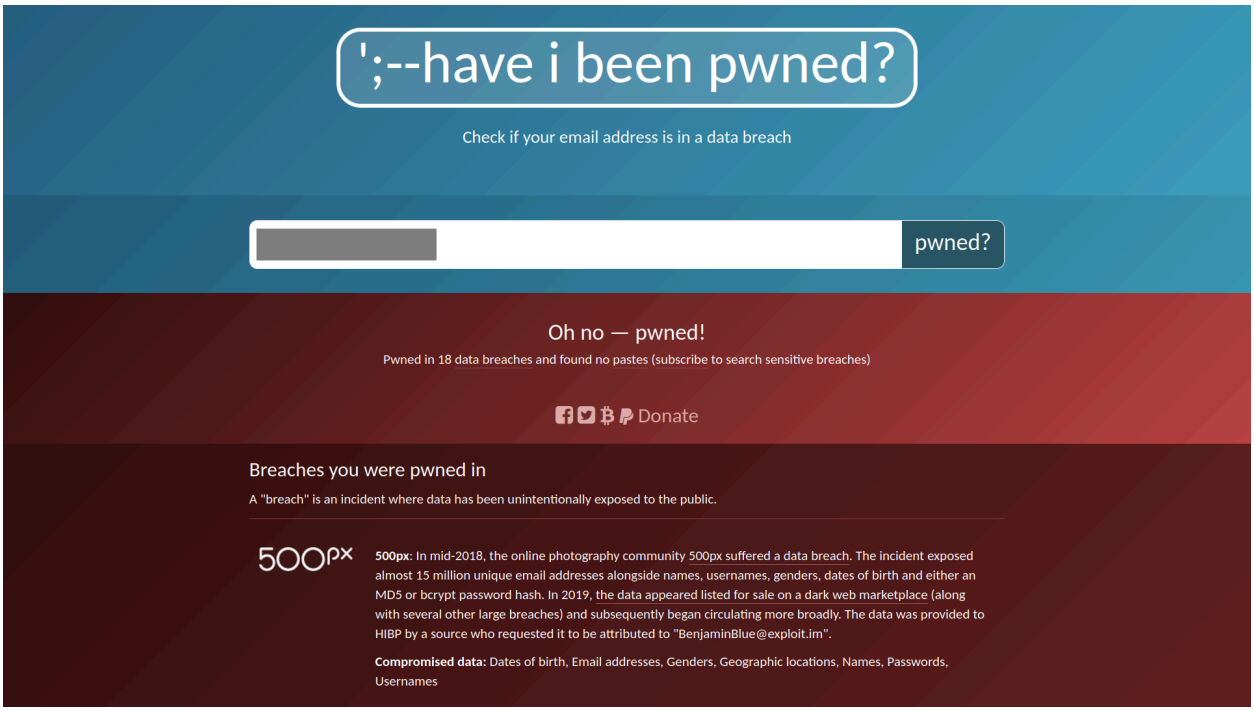
Is an online website that provides a virus-scanning service for files using multiple antivirus engines. It allows users to upload files or provide URLs to scan them against numerous antivirus engines and website scanners in a single operation. They can even input file hashes to check the results of previously uploaded files.

The screenshot below shows the result of checking the submitted file against 67 antivirus engines. Furthermore, one can check the community's comments for more insights. Occasionally, a file might be flagged as a virus or a Trojan; however, this might not be accurate for various reasons, and that's when community members can provide a more in-depth explanation.



❔ Have I Been Pwned

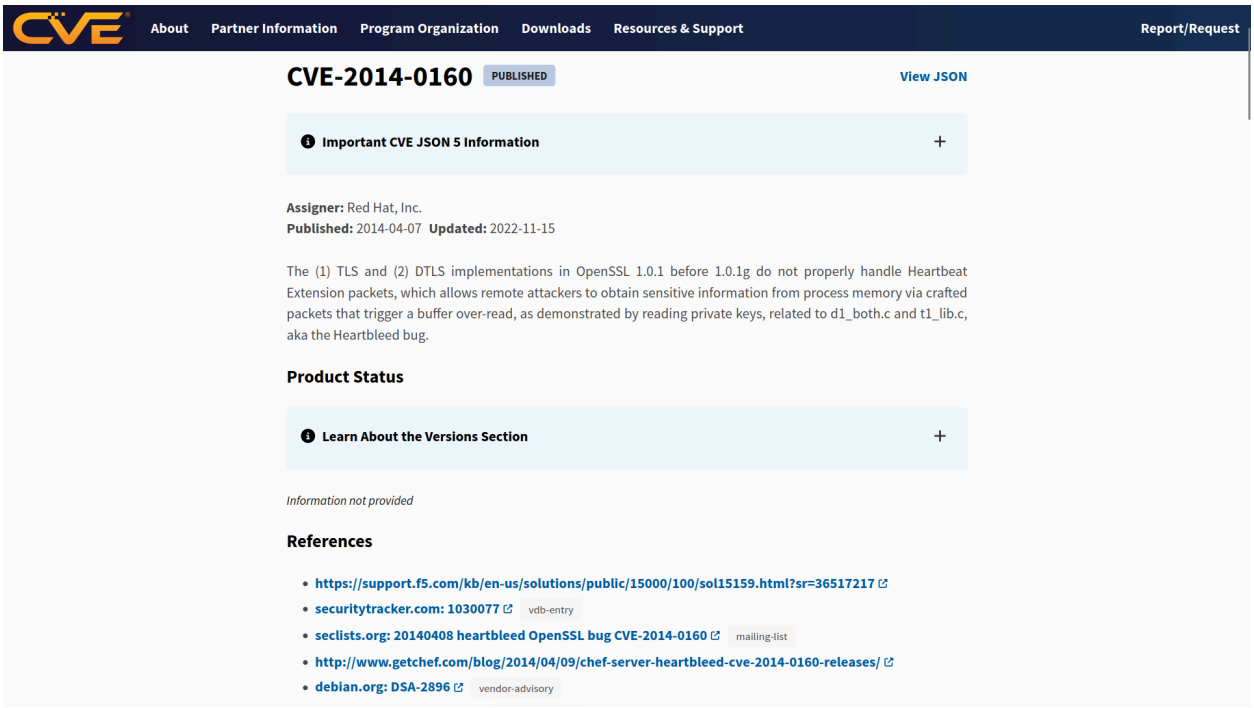
Have I Been Pwned (HIBP) does one thing; it tells you if an email address has appeared in a leaked data breach. Finding one's email within leaked data indicates leaked private information and, more importantly, passwords. Many users use the same password across multiple platforms, if one platform is breached, their password on other platforms is also exposed. Indeed, passwords are usually stored in encrypted format; however, many passwords are not that complex and can be recovered using a variety of attacks.



💣 Vulnerabilities and Exploits

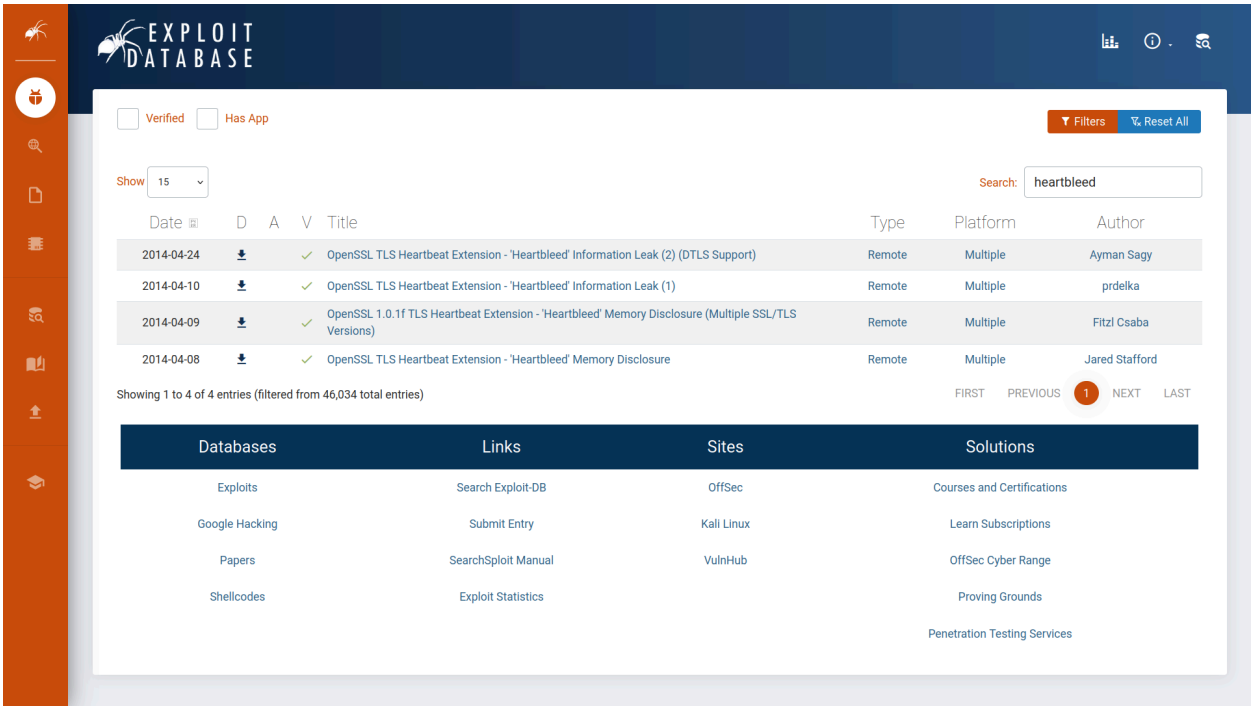
🥊 Common Vulnerabilities and Exposures (CVE)

We can think of the CVE program as a dictionary of vulnerabilities. It provides a standardized identifier for vulnerabilities and security issues in software and hardware products. Each vulnerability is assigned a CVE ID with a standardized format like `CVE-2024-29988`. This unique identifier (CVE ID) ensures that everyone from security researchers to vendors and IT professionals is referring to the same vulnerability, CVE-2024-29988 in this case. The MITRE Corporation maintains the CVE system.

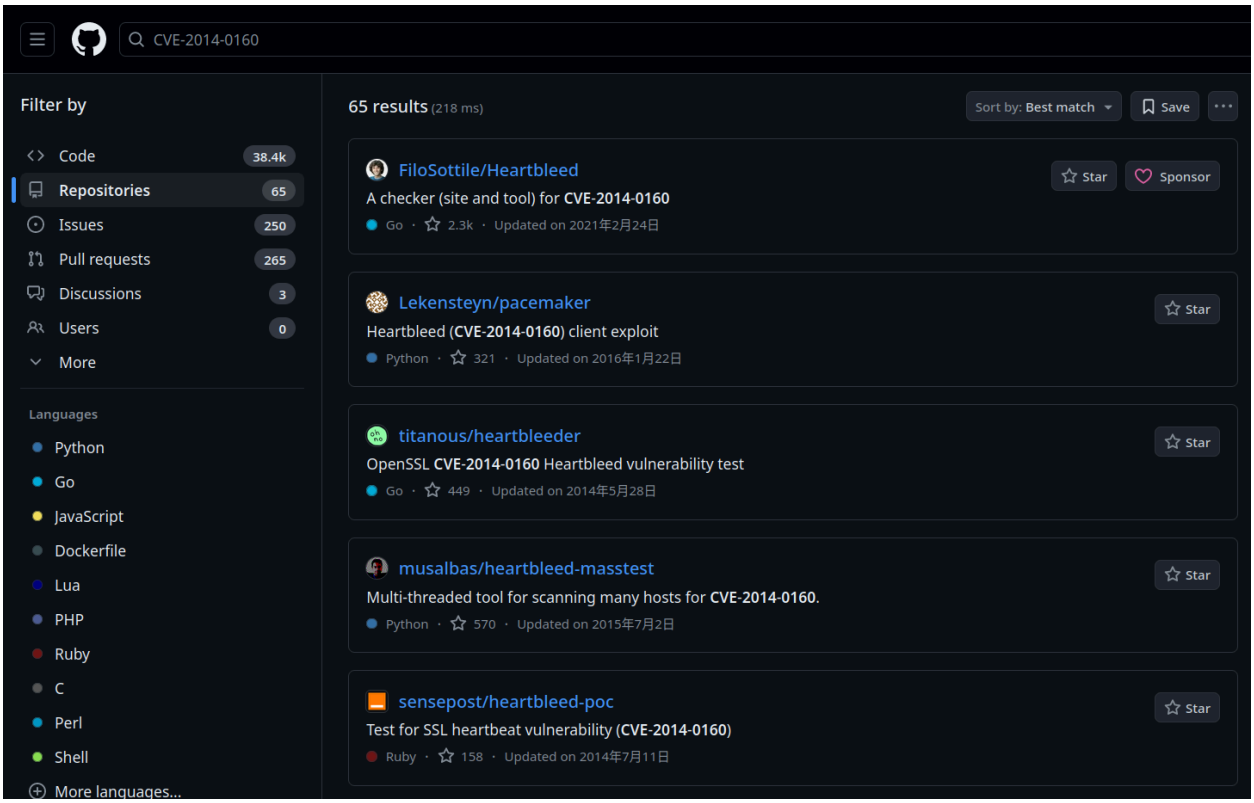


Exploit Database

Lists exploit codes from various authors; some of these exploit codes are tested and marked as verified.



GitHub, a web-based platform for software development, can contain many tools related to CVEs, along with proof-of-concept (PoC) and exploit codes.

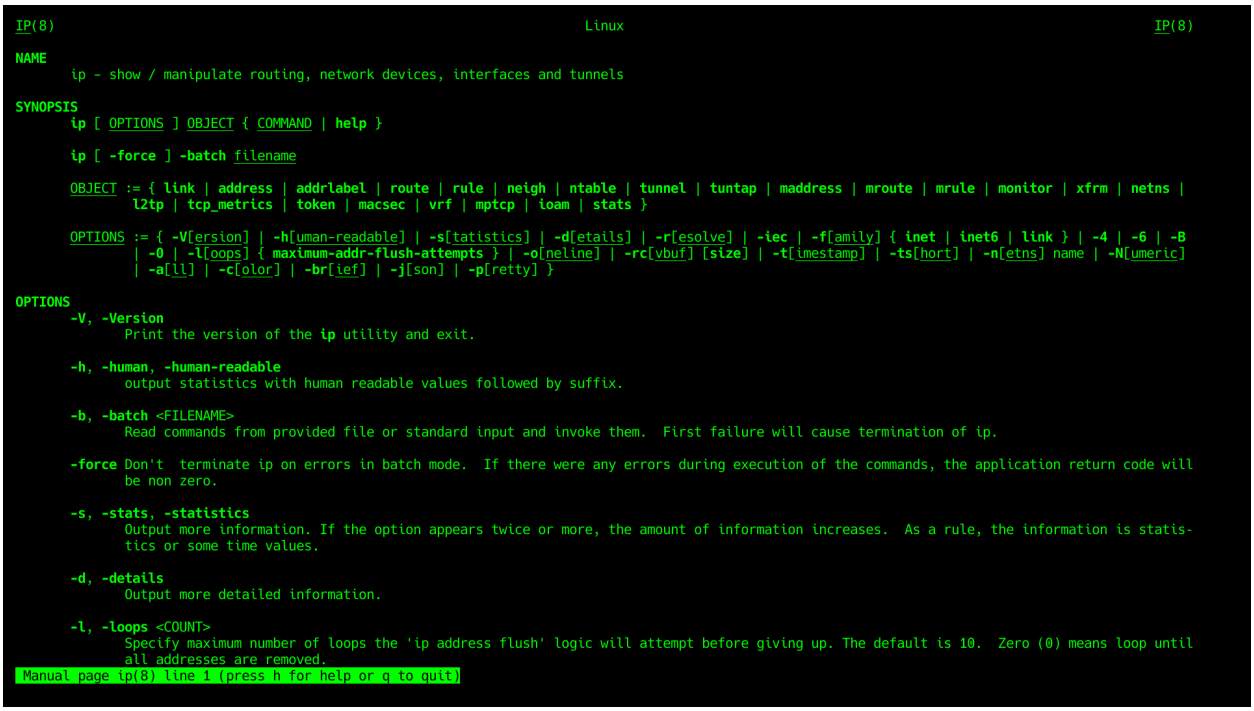


💿 Technical Documentation

📄 Linux Manual Pages

On Linux and every Unix-like system, each command is expected to have a man page. In fact, man pages also exist for system calls, library functions, and even configuration files.

Let's say we want to check the manual page for the command `ip`. We issue the command `man ip`. The screenshot below shows the page we received. You might want to start the AttackBox and run `man ip` on the terminal. Press `q` to quit.

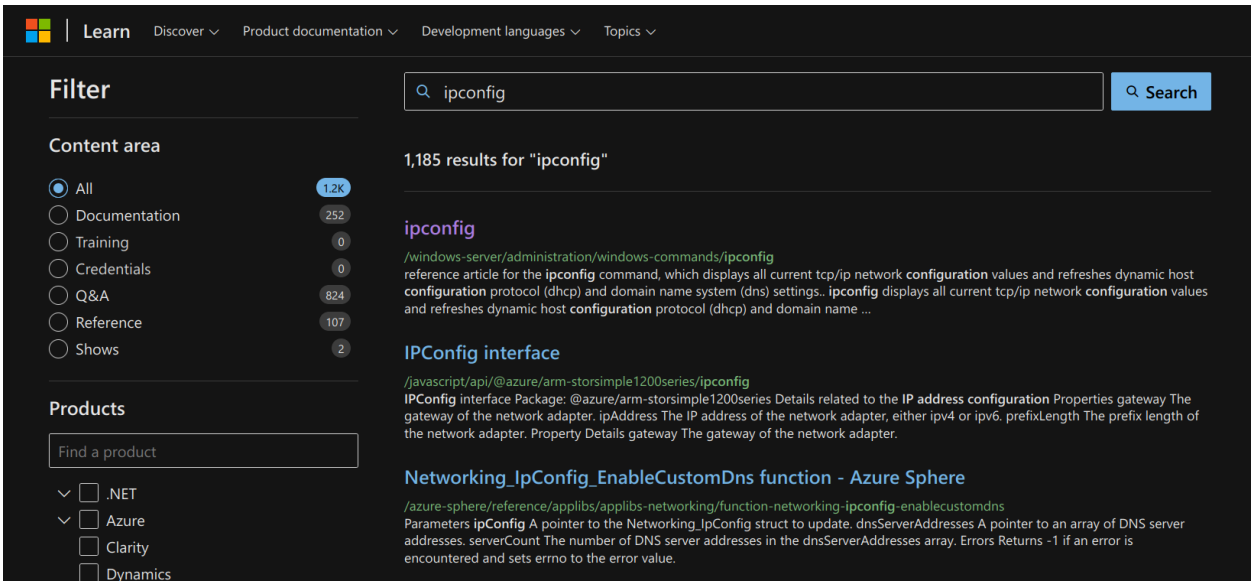


If you prefer to read the man page of `ip` in your web browser, just type `man ip` in your favourite search engine. This page might be at the top of the results.

The **AttackBox** is a Linux system accessible from your browser. Clicking on the **Start AttackBox** button will display the AttackBox in a split screen, making it convenient to read the task text and apply the instructions within the same browser window. If you hide the AttackBox window, you can show it again by clicking the blue Show Split View button at the top. In this task, you can start the AttackBox and use it to try Linux commands such as `man`.

📚 Microsoft Windows

Microsoft provides an official Technical Documentation page for its products. The screenshot below shows the search results for the command `ipconfig`.



📔 Product Documentation

Every popular product is expected to have well-organized documentation. This documentation provides an official and reliable source of information about the product features and functions. Examples include Snort Official Documentation, Apache HTTP Server Documentation, PHP Documentation, and Node.js Documentation.

It is always rewarding to check the official documentation as it is the most up-to-date and offers the most complete product information.

> 💡 The Linux command `cat` stand for *concatenate*.
> The `netstat` parameter in MS Windows that displays the executable associated with each active connection and listening port is *-b*.

📲 Social Media

🛡️ Cybersecurity Best Practices

1. Personnel Security & Social Engineering

It is critical to ensure that employees are mindful of their social media footprint. Oversharing can inadvertently provide adversaries with the building blocks for a breach.

- **The Risk:** Personal details shared online often contain the answers to security "secret questions" (e.g., *"What was the name of your primary school?"*).
- **The Consequence:** Attackers can use this information to perform unauthorized password resets and take over accounts with minimal effort.

> 💡 Conduct regular awareness training on "Digital Hygiene" to prevent the disclosure of sensitive personal data.

---

2. Professional Growth & Networking

As a cybersecurity professional, staying stagnant is not an option. Engaging with the right communities is essential for maintaining a competitive edge.

- **Community Engagement:** Joining specialized groups and channels creates a collaborative environment for sharpening technical expertise.
- **Trend Tracking:** Following industry leaders helps you stay ahead of emerging threats, new technologies, and defensive products.

---

3. Continuous Information Monitoring

Beyond social media, a diversified information diet is necessary to stay informed.

- **Industry News Outlets:** Monitor reputable cybersecurity news websites to get vetted, deep-dive analysis on global vulnerabilities.
- **Primary Sources:** Use a mix of RSS feeds or newsletters to aggregate updates from hundreds of available security platforms.