

Forum:[Hack Forums](#)

Thread: [What's One Cybersecurity Tool You Can't Live Without?](#)

Mxstermind - August 3, 2026, 11:22 am

Mine would probably be Wireshark.

It has saved me countless hours when troubleshooting network issues and understanding how protocols actually work.

Other favorites:

- Nmap
- Burp Suite Community
- Ghidra
- Wazuh
- Process Hacker
- CyberChef

What's yours and why?

01001 - August 4, 2026, 12:45 pm

Burp is a popular choice, but Nmap remains the standard for any penetration test, whether for a network or web application.

snadder - August 12, 2026, 9:16 am

Burp. Any other app doesn't come close. Zap is nice but not as usable. Plus the BApp store to add new tools

boondox420 - August 16, 2026, 7:17 pm

For me, it would probably be Process Monitor (ProcMon) from the Sysinternals suite.

Wireshark is incredible for anything network-related, but ProcMon has saved me more time when trying to figure out what a Windows system is actually doing.

You can watch things like:

- file creation/modification
- registry activity
- process behavior
- DLL loading
- permission failures
- persistence-related changes
- * what an installer or suspicious program touches

The filtering is what really makes it useful. Once you learn how to filter by process name, path, operation, result, etc., you can cut through a ridiculous amount of noise.

My other must-haves would probably be:

- Wireshark — packet/network analysis
- Burp Suite — web application testing
- Nmap — network/service discovery

CyberChef — encoding, decoding, hashes, data transformations
Autoruns — Windows persistence/startup investigation
Ghidra — reverse engineering/static analysis

If I could only keep one tool overall, though, I'd probably choose Wireshark simply because understanding what's actually happening on the wire is useful for security, troubleshooting, malware analysis, and learning protocols.

One thing I've learned is that knowing why a tool is giving you a result is a lot more valuable than just knowing the commands/buttons.

That's also why Wireshark and ProcMon are probably my favorites — they force you to understand what's actually happening underneath the GUI.

psycheuser - August 22, 2026, 8:56 pm

Burp Suite Pro for sure. The automation extensions and repeater make web app testing so much faster once you configure your scope right. CyberChef is a close second though, literally the Swiss Army knife for quick decodes.

Young Money - September 19, 2026, 4:32 am

(Aug 3, 2026 11:22 AM)Mxstermind Wrote: [\[CITE\]](#) Mine would probably be Wireshark.

It has saved me countless hours when troubleshooting network issues and understanding how protocols actually work.

Other favorites:

- Nmap
- Burp Suite Community
- Ghidra
- Wazuh
- Process Hacker
- CyberChef

What's yours and why?

I don't have because I'm in a new world:)

Devidwagnor68 - October 7, 2026, 7:36 pm

(Aug 12, 2026 09:16 AM)snadder Wrote: [\[CITE\]](#) Burp. Any other app doesn't come close. Zap is nice but not as usable. Plus the BApp store to add new tools
Jjjsj

Fantaghost33 - October 15, 2026, 10:41 pm

Burp suite

Nmap

Subfinder mas também o ffuf

Metasploit principalmente o msfvenom mas o msfconsole eu uso mais para Labs

Gobuster

Ghidra mas só para Labs porque gera muito log e chama atenção e com proxy fica lento [warn]

ParanoidAndroid - October 16, 2026, 8:56 am

Like most have said the below list; but thought about what tool do i use daily, constantly helping me to quickly check things...its got to be Notepad+++ lol...my quick viewer for all things I can open with

it.

- Burp Suite
- Nmap
- Wireshark
- Ghidra