

# HOSTS

“A host is any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. Some examples include, but are not limited to, computers, personal electronic devices, thin clients, and multi-functional devices.” ⇒ [NIST CSRC](#)

## TOOLS:

- <https://browserleaks.com/>
- <https://urlscan.io/>
- <https://urlquery.net/>
- <https://urldna.io/>
- <https://mxtoolbox.com/>
- <https://dnschecker.org/>
- <https://whatsmydns.me/>
- <https://www.whatsmydns.net/>
- <https://whatismyipaddress.com/>
- <https://ipfingerprints.com/>
- <https://iamroot.tech/>
- <https://www.ipvoid.com/>
- <https://www.urlvoid.com/>
- <https://www.whatsmyip.org/>
- <https://who.is/>
- <https://www.whois.com/>
- <https://crt.sh/>
- <https://dnsdumpster.com/>
- <https://bash.ws/>
- <https://www.findip-address.com/>
- <https://http.dev/>
- <https://httpheader.io/>
- <https://tools.keycdn.com/>
- <https://gsuite.tools/>
- <https://traceroute-online.com/>
- <https://nikto.online/>
- <https://nmap.online/>
- <https://nmap.org/>
- <https://sqlmap.org/>
- <https://github.com/sullo/nikto>
- <https://github.com/jekyc/wig>
- <https://www.whatweb.net/>
- <https://wapiti-scanner.github.io/>
- <https://github.com/wpscanteam/wpscan>
- <https://github.com/Dionach/CMSmap>
- <https://www.metasploit.com/>
- <https://offsec.tools/>

## WEB VULNERABILITY SCANNERS:

- <https://ns.tools/>

- <https://observatory.mozilla.org/>
- <https://www.scyscan.com/web-scanner/>
- <https://wpscan.com/>
- <https://wpsec.com/>
- <https://securewp.net/security-checker/>

#### WEB MALWARE SCANNERS:

- <https://www.virustotal.com/gui/home/url>
- <https://quttera.com/website-malware-scanner>
- <https://www.scyscan.com/virus-scanner/>
- <https://www.garyshood.com/virus/>
- <https://webav.io/>
- <https://github.com/rguziy/clamav-web-client>

#### SEARCH ENGINES:

- <https://www.shodan.io/>
- <https://search.censys.io/>
- <https://www.zoomeye.ai/>
- <https://viz.greynoise.io/>

#### DNS BLACKLISTS:

- <https://www.abuseipdb.com/>
- <https://talosintelligence.com/>
- <http://lookup.abusix.com/>
- <https://barracudacentral.org/>
- <https://www.spamcop.net/>
- <https://www.surbl.org/>
- <https://dronebl.org/>
- <https://www.spamhaus.org/>
- > <https://check.spamhaus.org/>
- <https://www.spamhaus.com/>
- <https://abuse.ch/>
- > <https://urlhaus.abuse.ch/>
- > <https://threatfox.abuse.ch/>
- > <https://sslbl.abuse.ch/>
- <https://gridinsoft.com/website-reputation-checker>
- <https://socradar.io/labs/>
- <https://www.dnsbl.info/>

#### BLOCKLISTS:

- <https://github.com/StevenBlack/hosts>
- <https://easylist.to/>
- <https://pgl.yoyo.org/>
- <https://someonewhocares.org/>
- <https://github.com/amitambekar510/Malicious-Domain-Threat-List>

#### VDP/BOUNTIES:

- <https://firebounty.com/>

From:  
<https://servzero.net/rwiki/> - **RECON-WIKI**

Permanent link:  
<https://servzero.net/rwiki/doku.php/hosts>

Last update: **2026/04/22 21:21**

