* **Firewall Testing & Evasion Tools Checklist** ■

|  |  |  |
| --- | --- | --- |
| **Category** | **Tool** | **Link** |
| Port scanning | Nmap | <https://nmap.org/> |
| OS fingerprinting | Xprobe2 | <https://sourceforge.net/projects/xprobe/> |
| Packet fragmentation evasion | Ragroute | <https://packetstormsecurity.com/files/31834/ragroute-1.0.tar.gz> |
| IP spoofing | Hping3 | <https://linux.die.net/man/8/hping3> |
| Protocol-specific evasion | Metasploit Framework | <https://www.metasploit.com/> |
| ICMP tunneling | ICMPTX | <http://thomer.com/icmptx/> |
| HTTP tunneling | HTTPTunnel | <http://www.nocrew.org/software/httptunnel.html> |
| ARP spoofing | Ettercap | <https://www.ettercap-project.org/> |
| SSL/TLS interception | SSLstrip | <https://github.com/moxie0/sslstrip> |
| SSL/TLS decryption | Wireshark | <https://www.wireshark.org/> |
| SSH tunneling | OpenSSH | <https://www.openssh.com/> |
| Proxy server evasion | Proxychains | <https://github.com/haad/proxychains> |
| TOR network evasion | Tor Browser | <https://www.torproject.org/> |
| WAF testing | WafW00f | <https://github.com/EnableSecurity/wafw00f> |
| MITM attacks | Bettercap | <https://www.bettercap.org/> |
| VPN detection | Iodine | <https://code.kryo.se/iodine/> |
| Encrypted payload evasion | Veil-Evasion | <https://github.com/Veil-Framework/Veil> |
| SQL injection evasion | SQLMap | <https://sqlmap.org/> |
| XSS evasion | XSSer | <https://github.com/epsylon/xsser> |
| File type evasion | EuzzDB | [https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Upload%20In](https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Upload%20Insecure%20Files/README.md) [secure%20Files/README.md](https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Upload%20Insecure%20Files/README.md) |
| Web service scanning | Nikto | <https://cirt.net/Nikto2> |