

Red & blue Team tools

Search Engines



Red Team



RedTeam TOOLKIT

OSINT Tools

- Spiderfoot
- OSINT
- Maltego

Reconnaissance

- Shodan
- Nmap
- sqlmap
- OpenVAS
- Nikto
- RustScan

Phishing

- Gophish
- King Phisher
- EvilURL

C&C

- Empire Project
- Pupy
- Cobalt Strike

Privilege Escalation

- BloodHound
- BeRoot

Exfiltration

- SharpExfiltrate
- DNSExfiltrator
- Egress-Assess

Credential Dumping

- Mimikatz
- Dumpert
- nanodump
- LaZagne
- Forkatz
- Pypykatz



cybersecurity-news

www.cybersecuritynews.com

Blue Team



Blue Team T O O L K I T

Network Analysis

- Wireshark
- pfSense
- Arkime
- Snort

Incident Management

- TheHive
- GRR Rapid Response

Threat Intelligence

- Misp
- MSTICPY

EDR

- Cortex XDR
- Cynet 360
- FortiEDR

OS Analysis

- HELK
- Volatility
- Wazuh
- RegRipper
- OSSEC
- osquery

Honeypots

- Kippo
- Cowrie
- Dockpot
- HonSSH

SIEM

- OSSIM
- Splunk
- LogRhythm

Docs

Autopsy

autopsy.pdf

Assessments

- <https://github.com/freelabz/secator>

From:

<https://wiki.fortier-family.com/> - **Warnaud's Wiki**

Permanent link:

<https://wiki.fortier-family.com/cybersecurity/tools?rev=1776572189>

Last update: **2026/04/19 06:16**

