

Red & blue Team tools

Overview

Top Cybersecurity Tools

©Cyber Threat Intelligence

Social Engineering

1. GoPhish
2. HiddenEye
3. SocialFish
4. EvilURL
5. Evilginx
6. SET (Social-Engineering Toolkit)

Password Cracking

1. Hashcat
2. John the Ripper
3. Hydra
4. Medusa
5. Cain & Abel
6. Ophcrack

Web Application Assessment

1. OWASP ZAP
2. Burp Suite
3. Nikto
4. WPScan
5. Acunetix
6. Arachni

Cloud Security

1. AWS GuardDuty
2. Azure Security Center
3. Google Cloud Security Command Center
4. Prisma Cloud
5. Lacework
6. Wiz

Wireless Hacking

1. Aircrack-NG
2. Wifite
3. Kismet
4. TCPDump
5. Reaver
6. Wireshark

Exploitation

1. Metasploit Framework
2. Burp Suite
3. SQL Map
4. ExploitDB
5. Core Impact
6. Cobalt Strike
7. Empire

Vulnerability Scanning

1. Nessus
2. OpenVAS
3. Nexpose
4. Qualys
5. Acunetix
6. Lynis

Forensics

1. Wireshark
2. Autopsy
3. Volatility
4. SleuthKit
5. Binwalk
6. Foremost
7. EnCase

Network Defense

1. Snort
2. Suricata
3. pfSense
4. Security Onion
5. AlienVault OSSIM

Endpoint Security

1. CrowdStrike Falcon
2. SentinelOne
3. Carbon Black
4. Symantec Endpoint Protection
5. Microsoft Defender for Endpoint

Threat Intelligence

1. ThreatConnect
2. Recorded Future
3. AlienVault OTX
4. IBM X-Force Exchange
5. MISP (Malware Information Sharing Platform)

Information Gathering

1. Nmap
2. Shodan
3. Maltego
4. TheHarvester
5. Recon-NG
6. Amass
7. Censys
8. OSINT Framework
9. Gobuster
10. Spiderfoot

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



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

Best tools



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>

Last update: **2026/04/26 16:24**

