

Blue Team Tools by Joas and Fabacab

Windows-based defenses

- Hardentools - Utility that audits a number of risky Windows features.
- NotRuler - Detect both client-side rules and VBScript enabled forms used by the Ruler attack tool when attempting to compromise a Microsoft Exchange server.
- PlumKloud - More effectively use BloodHoundAD in continual security life-cycles by utilizing its pathfinding engine to identify Active Directory security vulnerabilities.
- Sandboxie - Free and open source general purpose Windows application sandboxing utility.
- Sigcheck - Audit a Windows host's root certificate store against Microsoft's Certificate Trust List (CTL).
- Sticky Keys Slayer - Establishes a Windows RDP session from a list of hostnames and scans for accessibility tools lockdowns, alerting if one is discovered.
- Windows Secure Host Baseline - Group Policy objects, compliance checks, and configuration tools that provide an automated and flexible approach for securely deploying and maintaining the latest releases of Windows 10.
- WMI Monitor - Log newly created WMI consumers and processes to the Windows Application event log.

macOS-based defenses

- BlockBlock - Monitors common persistence locations and alerts whenever a persistent component is added, which helps to detect and prevent malware installation.
- LuLu - Free macOS firewall.
- Santa - Keep track of binaries that are naughty or nice in an allow/deny-listing system for macOS.
- Stronghold - Easily configure macOS security settings from the terminal.
- macOS Fortresses - Automated configuration of kernel-level, OS-level, and client-level security features including privatizing proxying and anti-virus scanning for macOS.

Threat signature packages and collections

- ESET's Malware IoTCS - Indicators of Compromise (IOC) derived from ESET's various investigations.
- FireEye's Red Team Tool Countermeasures - Collection of Snort and YARA rules to detect attacks carried out with FireEye's own Red Team tools, first released after FireEye disclosed a breach in December 2020.
- FireEye's Sunburst Countermeasures - Collection of IOC in various languages for detecting backdoored SolarWinds Orion NMS activities and related vulnerabilities.
- YARA Rules - Project covering the need for IT security researchers to have a single repository where different Yara signatures are compiled, classified and kept as up to date as possible.

Threat intelligence

- Active Directory Control Paths - Visualize and graph Active Directory permission configs ('control relations') to audit questions such as "Who can read the CEO's email?" and similar.
- AttackerKB - Free and public crowdsourced vulnerability assessment platform to help prioritize high-risk patch application and combat vulnerability fatigue.
- DATA - Credential phish analysis and automation tool that can accept suspected phishing URLs directly or trigger on observed network traffic containing such a URL.
- Forager - Multi-threaded threat intelligence gathering built with Python3 featuring simple text-based configuration and data storage for ease of use and data portability.
- GRASSMARLIN - Provides IP network situational awareness of industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) by passively mapping, accounting for, and reporting on your ICS/SCADA network topology and endpoints.
- MLSec Combine - Gather and combine multiple threat intelligence feed sources into one customizable, standardized CSV-based format.
- Malware Information Sharing Platform and Threat Sharing (MISP) - Open source software solution for collecting, storing, distributing and sharing cyber security indicators.
- Open Source Vulnerabilities (OSV) - Vulnerability database and triage infrastructure for open source projects aimed at helping both open source maintainers and consumers of open source.
- Sigma - Generic signature format for SIEM systems, offering an open signature format that allows you to describe relevant log events in a straightforward manner.
- ThreatIntegrator - Extendable tool to extract and aggregate IOCs from threat feeds including Twitter, RSS feeds, or other sources.
- Unfetter - Identifies defensive gaps in security posture by leveraging MITRE's ATT&CK framework.
- Viper - Binary analysis and management framework enabling easy organization of malware and exploit samples.

Threat hunting

- YARA - Tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples, described as 'the pattern matching swiss army knife' for file patterns and signatures.
- Chimblee - Suite of C/C++/PHP-based tools enabling remote incident response and hunting operations across all versions of Windows.
- DeepBlueCLI - PowerShell module for hunt learning via Windows Event logs.
- GRF Rapid Response - Incident response framework focused on remote live forensics consisting of a Python agent installed on suspect and/or Kubelet server infrastructure enabling analysts to quickly triage attacks and perform analysis remotely.
- Hunting ELK (HELK) - All-in-one Free Software threat hunting stack based on Elasticsearch, Logstash, Kafka, and Kibana with various built-in integrations for analysts including Jupyter Notebook.
- ModDef - Automate the security incident handling process and facilitate the real-time activities of incident handlers.
- PSHunt - PowerShell module designed to scan remote endpoints for indicators of compromise or survey them for more comprehensive information related to state of those systems.
- PSRecon - PSHunt-like tool for analyzing remote Windows systems that also produces a self-contained HTML report of its findings.
- PowerForensics - All in one PowerShell-based platform to perform live hard disk forensic analysis.
- rustsec2 - Multi-platform tool for triaging suspected IOCs on many endpoints simultaneously and that integrates with antivirus consoles.
- Redline - Firmware endpoint auditing and analysis tool that provides host-based investigative capabilities, offered by FireEye, Inc.

Preparedness training and wargaming

- APTSimulator - Toolset to make a system look as if it was the victim of an APT attack.
- Atomic Red Team - Library of simple, automatable tests to execute for testing security controls.
- BadBlood - Fills a test (non-production) Windows Domain with data that enables security analysts and engineers to practice using tools to gain an understanding and prescribe to securing Active Directory.
- DumppsterFire - Modular, menu-driven, cross-platform tool for building repeatable, time-delayed, distributed security events for Blue Team drills and sensor/alert mapping.
- Metta - Automated information security preparedness tool to do adversarial simulation.
- Network Flight Simulator (FlightSim) - Utility to generate malicious network traffic and help security teams evaluate security controls and audit their network visibility.
- RedTriton OS - Ubuntu-based Open Virtual Appliance (OVA) preconfigured with several threat emulation tools as well as a defender's toolkit.

Phishing awareness and reporting

- CertSpotter - Certificate Transparency log monitor from SSLMate that alerts you when a SSL/TLS certificate is issued for one of your domains.
- Gophish - Powerful, open-source phishing framework that makes it easy to test your organization's exposure to phishing.
- King Phisher - Tool for testing and promoting user awareness by simulating real world phishing attacks.
- NotifySecurity - Outlook add-in used to help your users to report suspicious e-mails to security teams.
- Phishing Intelligence Engine (PIE) - Framework that will assist with the detection and response to phishing attacks.
- Swordfish - Platform allowing to create and manage (fake) phishing campaigns intended to train people in identifying suspicious mails.
- mailspoofer - Scans SPF and DMARC records for issues that could allow email spoofing.
- phishing_catcher - Configurable script to watch for instances of suspicious TLS certificates by domain name in the Certificate Transparency Log (CTL) using the CertStream service.

Operating System distributions

- Computer Aided Investigative Environment (CAINE) - Italian GNU/Linux live distribution that packages numerous digital forensics and evidence collection tools.
- Security Onion - Free and open source GNU/Linux distribution for intrusion detection, enterprise security monitoring, and log management.
- Qubes OS - Desktop environment built atop the Xen hypervisor project that runs each end-user program in its own virtual machine intended to provide strict security controls to constrain the reach of any successful malware exploit.

Network perimeter defenses

- Gatekeeper - First open source Distributed Denial of Service (DDoS) protection system.
- fwknop - Protects ports via Single Packet Authorization in your firewall.
- ssh-audit - Simple tool that makes quick recommendations for improving an SSH server's security posture.
- IPFire - Hardened GNU/Linux based router and firewall distribution forked from ICSop.
- pfSense - Hardened FreeBSD based firewall and routing platform forked from pfSense.
- pfSense - FreeBSD firewall and router distribution forked from m0n0wall.

Honeypots

- CanaryTokens - Self-hostable honeypot generator and reporting dashboard; demo version available at CanaryTokens.org.
- Kushaka - Sustainable all-in-one honeypot and honeypot orchestrator for under-resourced blue teams.
- Endless - SSH target that slowly sends an endless banner.
- Labrea - Program that answers ARP requests for unused IP space, creating the appearance of fake machines that answer further requests very slowly in order to slow down scanners, worms, etcetera.

Policy enforcement

- Conftest - Utility to help you write tests against structured configuration data.
- Open Policy Agent (OPA) - Unified toolset and framework for policy across the cloud native stack.
- Tang - Server for binding data to network presence; provides data to clients only when they are on a certain (secured) network.

Compliance testing and reporting

- Chef InSpec - Language for describing security and compliance rules, which become automated tests that can be run against IT infrastructures to discover and report on non-compliance.
- OpenSCAP Base - Both a library and a command line tool (oscap) used to evaluate a system against SCAP baseline profiles to report on the security posture of the scanned system(s).

Application or Binary Hardening

- Dynatrace - Tools for binary instrumentation, analysis, and modification; useful for binary patching.
- DynamRIO - Runtime code manipulation system that supports code transformations on any part of a program, while it executes implemented as a process-level virtual machine.
- Equalito - Binary recomplier and instrumentation framework that can fully disassemble, transform, and regenerate ordinary Linux binaries designed for binary hardening and security research.
- Valgrind - Instrumentation framework for building dynamic analysis tools.

Communications security (COMSEC)

- GPFSync - Centralize and automate OpenPGP public key distribution, revocation, and updates amongst all members of an organization or team.
- Genova (Genetic Evasion) - Novel experimental genetic algorithm that evolves packet-manipulation-based censorship evasion strategies against nation-state level censors to increase availability of otherwise blocked content.
- GlobaLeaks - Free, open source software enabling anyone to easily set up and maintain a secure whistleblowing platform.
- SecureDrop - Open source whistleblower submission system that media organizations and NGOs can install to securely accept documents from anonymous sources.
- Teleport - Allows engineers and security professionals to unify access for SSH servers, Kubernetes clusters, web applications, and databases across all environments.

Kubernetes

- KubeSec - Static analyzer of Kubernetes manifests that can be run locally, as a Kubernetes admission controller, or as its own cloud service.
- Kyverno - Policy engine designed for Kubernetes.
- Linkerd - Ultra light Kubernetes-specific service mesh that adds observability, reliability, and security to Kubernetes applications without requiring any modification of the application itself.
- Managed Kubernetes Inspection Tool (MKIT) - Query and validate several common security-related configuration settings of managed Kubernetes cluster objects and the workloads/resources running inside the cluster.
- Polaris - Validates Kubernetes best practices by running tests against code commits, a Kubernetes admission request, or live resources already running in a cluster.
- certificate-expiry-monitor - Utility that certifies the expiry of TLS certificates as Prometheus metrics.
- k-rail - Workload policy enforcement tool for Kubernetes.
- kube-forensics - Allows a cluster administrator to dump the current state of a running pod and all its containers so that security professionals can perform off-line forensic analysis.
- kube-hunter - Open source tool that runs a set of tests ('hunters') for security issues in Kubernetes clusters from either outside ('attacker's view') or inside a cluster.
- kubernetes-event-exporter - Allows exporting the often missed Kubernetes events to various outputs so that they can be used for observability or alerting purposes.

Fuzzing

- Atheris - Coverage-guided Python fuzzing engine based off of libFuzzer that supports fuzzing of Python code but also native extensions written for CPython.
- Fuzztrench - Free service that evaluates fuzzers on a wide variety of real-world benchmarks, at Google scale.
- OneFuzz - Self-hosted Fuzzing-as-a-Service (FaaS) platform.

Distributed monitoring

- Cortex - Provides horizontally scalable, highly available, multi-tenant, long term storage for Prometheus.
- Jaeger - Distributed tracing platform backend used for monitoring and troubleshooting microservices-based distributed systems.
- OpenTelemetry - Observability framework for cloud-native software, comprising a collection of tools, APIs, and SDKs for exporting application performance metrics to a tracing backend (formerly maintained by the OpenTracing and OpenCensus projects).
- Prometheus - Open-source systems monitoring and alerting toolkit originally built at SoundCloud.
- Zigbee - Distributed tracing system backend that helps gather timing data needed to troubleshoot latency problems in service architectures.

Cloud Platform Security

- Checkov - Static analysis for Terraform (infrastructure as code) to help detect OS policy violations and prevent security misconfiguration.
- Falco - Behavioral activity monitor designed to detect anomalous activity in containerized applications, hosts, and network packet flows by auditing the Linux kernel and enriched by runtime data such as Kubernetes metrics.
- Kata Containers - Secure container runtime with lightweight virtual machines that feel and perform like containers, but provide stronger workload isolation using hardware virtualization technology as a second layer of defense.
- Prowler - Tool based on AWS-CLI commands for Amazon Web Services account security assessment and hardening.
- Scout Suite - Open source multi-cloud security-auditing tool, which enables security posture assessment of cloud environments.
- gVisor - Application kernel, written in Go, that implements a substantial portion of the Linux system surface to provide an isolation boundary between the application and the host kernel.

DevSecOps

- Bane - Custom and better AppArmor profile generator for Docker containers.
- BlackBox - Safety store secrets in Git/ Mercuria/Subversion by encrypting them 'at rest' using GnuPG.
- Cilium - Open source software for transparently securing the network - connectivity between application services deployed using Linux container management platforms like Docker and Kubernetes.
- Clair - Static analysis tool to probe for vulnerabilities introduced via application container (e.g., Docker) images.
- CodeQL - Discover vulnerabilities across a codebase by performing queries against code as though it were data.
- DefectDojo - Application vulnerability management tool built for DevOps and continuous security integration.
- Countit - Pinned applications during routine continuous integration build pipelines.
- Git Secrets - Prevents you from committing passwords and other sensitive information to a git repository.
- SOPS - Editor of encrypted files that supports YAML, JSON, ENV, INI and binary formats and encrypts with AWS KMS, GCP KMS, Azure Key Vault, and PGP.
- Snyk - Finds and fixes vulnerabilities and license violations in open source dependencies and container images.
- SonarDocker - Continuous inspection tool that provides detailed reports during automated testing and alerts on newly introduced security vulnerabilities.
- Trivy - Simple and comprehensive vulnerability scanner for containers and other artifacts, suitable for use in continuous integration pipelines.
- Vault - Tool for securely accessing secrets such as API keys, passwords, or certificates through a unified interface.
- git-crypt - Transparent file encryption in git: files which you choose to protect are encrypted when committed, and decrypted when checked out.
- helm-secrets - Helm plugin that helps manage secrets with Git workflow and stores them anywhere, backed by SOPS.

Automation

- Ansible Lockdown - Curated collection of information security themed Ansible roles that are both vetted and actively maintained.
- Clevis - Plugable framework for automated decryption, often used as a Timg client.
- DShell - Extensible network forensic analysis framework written in Python that enables rapid development of plugins to support the dissection of network packet captures.
- Dei-Sec.io - Server hardening framework providing Ansible, Chef, and Puppet implementations of various baseline security configurations.
- peepdf - Scriptable PDF file analyzer.
- PyREBox - Python-scriptable reverse engineering sandbox, based on QEMU.
- Watchtower - Container-based solution for automating Docker container base image updates, providing an unattended upgrade experience.

Code libraries and bindings

- MultiScanner - File analysis framework written in Python that assists in evaluating a set of files by automatically running a suite of tools against them and aggregating the output.
- Push-VirusTotal - PowerShell interface to VirusTotal.com APIs.
- censys-python - Python wrapper to the Censys REST API.
- liberalfx - High level C++ network packet sniffing and crafting library.
- python-dshield - Pythonic interface to the Internet Storm Center/DShield API.
- python-sandboxapi - Minimal, consistent Python API for building integrations with malware sandboxes.
- python-stix2 - Python APIs for serializing and de-serializing Structured Threat Information Expression (STIX) JSON content, plus higher-level APIs for common tasks.

Supply chain security

- Grafeas - Open artifact metadata API to audit and govern your software supply chain.
- Helm GPG (GnuPG) Plugin - Chart signing and verification with GnuPG for Helm.
- Notary - Aims to make the internet more secure by making it easy for people to publish and verify content.

Host-based tools

- Antiray - Combination honeypot, filesystem monitor, and alerting system designed to protect Linux and Windows operating systems.
- chkrootkit - Locally checks for signs of a rootkit on GNU/Linux systems.
- CrowdInspect - Free tool for Windows systems aimed to alert you to the presence of malware that may be communicating over the network.
- Fall3n - Intrusion prevention software framework that protects computer servers from brute-force attacks.
- Open Source HIDS Security (OSSEC) - Fully open source and free, feature-rich, host-based Intrusion Detection System (HIDS).
- Rootkit Hunter (rkhunter) - POSIX-compliant Bash script that scans a host for various signs of malware.

Sandboxes

- Bubblewrap - Sandboxing tool for use by unprivileged Linux users capable of restricting access to parts of the operating system or user data.
- Dangerzone - Take potentially dangerous PDFs, office documents, or images and convert them to a safe PDF.
- Firejail - SUID program that reduces the risk of security breaches by restricting the running environment of untrusted applications using Linux namespaces and seccomp-bpf.
- Anyrun

Security monitoring

- Wazuh - Open source, multipplatform agent-based security monitoring based on a fork of OSSEC HIDS.
- ChaosShop - Framework to aid analysts in the creation and execution of pyrit-based decoders and detectors of APT tradecraft.
- Maltrail - Malicious network traffic detection system.
- Moloch - Augments your current security infrastructure to store and index network traffic in standard PCAP format, providing fast, indexed access.
- DuWH - Helps manage network IDS at scale by visualizing Suricata, Zeek, and Moloch life cycles.
- Real Intelligence Threat Analysis (RTA) - Open source framework for network traffic analysis that ingests Zeek logs and detects beaconing, DNS tunneling, and more.
- Responder - Detects the presence of the Responder LLNMR/NBT-NS/MDNS poisoner on a network.
- Snort - Widely-deployed, Free Software IPS capable of real-time packet analysis, traffic logging, and custom rule-based triggers.
- SpoofSpotter - Catch spoofed NetBIOS Name Service (NBNS) responses and alert on an email or log file.
- Stenographer - Full-packet-capture utility for buffering packets to disk for intrusion detection and incident response purposes.
- Suricata - Free, cross-platform, IDS/IPS with on- and off-line analysis modes and deep packet inspection capabilities that is also scriptable with Lua.
- Tsunami - General purpose network security scanner with an extensible plugin system for detecting high severity vulnerabilities with high confidence.
- VAST - Free and open-source network telemetry engine for data-driven security investigations.
- Wireshark - Free and open-source packet analyzer useful for network troubleshooting or forensic netflow analysis.
- Zeek - Powerful network analysis framework focused on security monitoring, formerly known as Bro.
- netniff-ng - Free and fast GNU/Linux networking toolkit with numerous utilities such as a connection tracking tool (floodtop), traffic generator (trafgen), and autonomous system (AS) trace route utility (astraceoute).

Security information and Event Management (SIEM)

- AlienVault OSSIM - Single-server open source SIEM platform featuring asset discovery, asset inventory, behavioral monitoring, and event correlation, driven by AlienVault Open Threat Exchange (OTX).
- Prelude SIEM OSS - Open source, agentless SIEM with a long history and several commercial variants featuring security event collection, normalization, and alerting from arbitrary log input and numerous popular monitoring tools.

Incident Response tools

- LogonTracer - Investigate malicious Windows logs by visualizing and analyzing Windows event log.
- Volatility - Advanced memory forensics framework.
- win_xr - Automates your incident response with zero security preparedness assumptions.
- IR management consoles -
- CERTKIT - Scriptable Digital Forensics and Incident Response (DFIR) toolkit built on Viper.
- Fast Incident Response (FIR) - Cybersecurity incident response framework for easy creation, tracking, and reporting of cybersecurity incidents.
- Rekali - Advanced forensic and incident response framework.
- Thelhive - Scalable, free Security Incident Response Platform (SIRP) designed to make life easier for SOCs, CSIRTs, and CERTs, featuring tight integration with MSP.
- threat_note - Web application built by Defense Point Utility to allow security researchers the ability to add and retrieve indicators related to their research.

Tor Onion service defenses

- AutoMaCTC - Modular, automated forensic triage collection framework designed to process various forensic artifacts on macOS, parse them, and present them in formats viable for analysis.
- OSX Auditor - Free macOS computer forensics tool.
- OSXCollector - Forensic evidence collection & analysis toolkit for macOS.
- i-rescue - Windows Batch script and a Unix Bash script to automate the collection of forensic data during incident response.
- Margarita Shotgun - Command line utility (that works with or without Amazon EC2 instances) to parallelize remote memory acquisition.

Transport-layer defenses

- OnionBalance - Provides load-balancing while also making Onion services more resilient and reliable by eliminating single points-of-failure.
- Vanguards - Version 3 Onion service guard discovery attack mitigation script (intended for eventual inclusion in Tor core).
- Cerbot - Free tool to automate the issuance and renewal of TLS certificates from the Let'sEncrypt Root CA with plugins that configure various Web and e-mail server software.
- MTHEngine - Colling library for server-side detection of TLS interception events.
- OpenVPN - Open source, SSL/TLS-based virtual private network (VPN).
- Tor - Censorship circumvention and anonymizing overlay network providing distributed, cryptographically verified name services (onion domains) to enhance publisher privacy and service availability.

Security monitoring

- Wazuh - Open source, multipplatform agent-based security monitoring based on a fork of OSSEC HIDS.
- ChaosShop - Framework to aid analysts in the creation and execution of pyrit-based decoders and detectors of APT tradecraft.
- Maltrail - Malicious network traffic detection system.
- Moloch - Augments your current security infrastructure to store and index network traffic in standard PCAP format, providing fast, indexed access.
- DuWH - Helps manage network IDS at scale by visualizing Suricata, Zeek, and Moloch life cycles.
- Real Intelligence Threat Analysis (RTA) - Open source framework for network traffic analysis that ingests Zeek logs and detects beaconing, DNS tunneling, and more.
- Responder - Detects the presence of the Responder LLNMR/NBT-NS/MDNS poisoner on a network.
- Snort - Widely-deployed, Free Software IPS capable of real-time packet analysis, traffic logging, and custom rule-based triggers.
- SpoofSpotter - Catch spoofed NetBIOS Name Service (NBNS) responses and alert on an email or log file.
- Stenographer - Full-packet-capture utility for buffering packets to disk for intrusion detection and incident response purposes.
- Suricata - Free, cross-platform, IDS/IPS with on- and off-line analysis modes and deep packet inspection capabilities that is also scriptable with Lua.
- Tsunami - General purpose network security scanner with an extensible plugin system for detecting high severity vulnerabilities with high confidence.
- VAST - Free and open-source network telemetry engine for data-driven security investigations.
- Wireshark - Free and open-source packet analyzer useful for network troubleshooting or forensic netflow analysis.
- Zeek - Powerful network analysis framework focused on security monitoring, formerly known as Bro.
- netniff-ng - Free and fast GNU/Linux networking toolkit with numerous utilities such as a connection tracking tool (floodtop), traffic generator (trafgen), and autonomous system (AS) trace route utility (astraceoute).

Security configurations

- Burkeized-ngrx - Docker image of an Nginx configuration and scripts implementing many defensive techniques for Web sites.

SOAR

- Shuffle - Graphical generalized workflow (automation) builder for IT professionals and blue teams.
- Splunk Phantom
- IBM Resilient
- DFIR Labs InChAn
- Insightconnect
- RespondIX
- Exabeam
- SRP