


This repository | Search

Pull requestsIssuesMarketplaceGist

 paralax / awesome-honeypots

Watch165

Star1,475

Fork318

<> Code

Issues3

Pull requests2

Projects0

Wiki

Insights

an awesome list of honeypot resources

honeypot

awesome-list

awesome

list

honeyd

173 commits

1 branch

0 releases

28 contributors

Artistic-2.0

Branch: masterNew pull request

Create new fileUpload filesFind fileClone or download

paralax committed on GitHub add honeytrap, portlurkerLatest commit 5a67267 7 days ago

CONTRIBUTING.md

Create CONTRIBUTING.md

2 years ago

LICENSE

Initial commit

2 years ago

README.md

add honeytrap, portlurker

7 days ago


awesome-check.py

checks URLs

a year ago

README.md

# Awesome Honeypots



A curated list of awesome honeypots, tools, components and much more. The list is divided into categories such as web, services, and others, focusing on open source projects.

There is no pre-established order of items in each category, the order is for contribution. If you want to contribute, please read the [guide](#).

Discover more awesome lists at [sindresorhus/awesome](#).

## Sections

- Honeypots
- Honeyd Tools
- Network and Artifact Analysis
- Data Tools
- Guides

## Related Lists

- [awesome-pcaptools](#), useful in network traffic analysis.
- [awesome-malware-analysis](#), with some overlap here for artifact analysis.

## Honeypots

- Database Honeypots
  - [MongoDB-HoneyProxy](#) - A MongoDB honeypot proxy.
  - [Elastic honey](#) - A Simple Elasticsearch Honeypot.
  - [mysql](#) - A mysql honeypot, still very very early stage.
  - [NoSQLpot](#) - The NoSQL Honeypot Framework.
  - [ESPot](#) - An Elasticsearch honeypot written in NodeJS, to capture every attempts to exploit CVE-2014-3120.

- [Delilah](#) - An Elasticsearch Honeypot written in Python.
- Web honeypots
  - [Glastopf](#) - Web Application Honeypot.
  - Snare/Tanner - successors to Glastopf
    - [Snare](#) - Super Next generation Advanced Reactive honEypot
    - [Tanner](#) - Evaluating SNARE events
  - [phpmyadmin\\_honeypot](#) - A simple and effective phpMyAdmin honeypot.
  - [servlet](#) - Web application Honeypot.
  - [Nodepot](#) - A nodejs web application honeypot.
  - [basic-auth-pot](#) - http Basic Authentication honeyPot.
  - [Shadow Daemon](#) - A modular Web Application Firewall / High-Interaction Honeypot for PHP, Perl & Python apps.
  - [Servletpot](#) - Web application Honeypot.
  - [Google Hack Honeypot](#) - designed to provide reconnaissance against attackers that use search engines as a hacking tool against your resources.
  - [smart-honeypot](#) - PHP Script demonstrating a smart honey pot.
  - [Bukkit Honeypot](#) Honeypot - A honeypot plugin for Bukkit.
  - [Laravel Application Honeypot](#) - Honeypot - Simple spam prevention package for Laravel applications.
  - [stack-honeypot](#) - Inserts a trap for spam bots into responses.
  - [EoHoneyPotBundle](#) - Honeypot type for Symfony2 forms.
  - [shockpot](#) - WebApp Honeypot for detecting Shell Shock exploit attempts.
  - [django-admin-honeypot](#) - A fake Django admin login screen to notify admins of attempted unauthorized access.
  - WordPress honeypots
    - [HonnyPotter](#) - A WordPress login honeypot for collection and analysis of failed login attempts.
    - [HoneyPress](#) - python based WordPress honeypot in a docker container.
    - [wp-smart-honeypot](#) - WordPress plugin to reduce comment spam with a smarter honeypot.
    - [wordpot](#) - A WordPress Honeypot.
- Service Honeypots
  - [honeynip](#) - NTP logger/honeypot.
  - [honeypot-camera](#) - observation camera honeypot.
  - [troje](#) - a honeypot built around lxc containers. It will run each connection with the service within a separate lxc container.
  - [HoneyPy](#) - A low interaction honeypot.
  - [Ensnares](#) - Easy to deploy Ruby honeypot.
  - [RDPy](#) - A Microsoft Remote Desktop Protocol (RDP) honeypot in python.
  - [Honeyprint](#) - Printer honeypot.
  - [Tom's Honeypot](#) - Low interaction Python honeypot.
  - [Honeyport](#) - A simple honeypot written in Bash and Python.
  - [AMTHoneypot](#) - Honeypot for Intel's AMT Firmware Vulnerability CVE-2017-5689.
- Distributed Honeypots
  - [DemonHunter](#) - Low interaction Honeypot Server.
- Anti-honeypot stuff
  - [kippo\\_detect](#) - This is not a honeypot, but it detects kippo. (This guy has lots of more interesting stuff)
- ICS/SCADA honeypots
  - [Conpot](#) - ICS/SCADA honeypot.
  - [gridpot](#) - Open source tools for realistic-behaving electric grid honeynets .
  - [scada-honeynet](#) - mimics many of the services from a popular PLC and better helps SCADA researchers understand potential risks of exposed control system devices.
  - [SCADA honeynet](#) - Building Honeypots for Industrial Networks.
  - [GasPot](#) - Veeder Root Guardian AST, common in the oil and gas industry.

- Other/random
  - [NOVA](#) uses honeypots as detectors, looks like a complete system.
  - [Open Canary](#) - A low interaction honeypot intended to be run on internal networks.
  - [OFPot](#) - OpenFlow Honeypot, redirects traffic for unused IPs to a honeypot. Built on POX.
  - [OpenCanary](#) - Modular and decentralised honeypot.
- Botnet C2 tools
  - [Hale](#) - Botnet command & control monitor.
  - [dnsMole](#) - analyse dns traffic, and to potentially detect botnet C&C server and infected hosts.
  - [botsnoopd](#) - Botnet C2 monitoring
- IPv6 attack detection tool
  - [ipv6-attack-detector](#) - Google Summer of Code 2012 project, supported by The HoneyNet Project organization.
- Dynamic code instrumentation toolkit
  - [Frida](#) - Inject JavaScript to explore native apps on Windows, Mac, Linux, iOS and Android.
- Tool to convert website to server honeypots
  - [HIHAT](#) - Transform arbitrary PHP applications into web-based high-interaction Honeypots.
- Malware collector
  - [Kippo-Malware](#) - Python script that will download all malicious files stored as URLs in a Kippo SSH honeypot database.
- Distributed sensor deployment
  - [Smarthoneypot](#) - custom honeypot intelligence system that is simple to deploy and easy to manage.
  - [Modern Honey Network](#) - Multi-snort and honeypot sensor management, uses a network of VMs, small footprint SNORT installations, stealthy dionaeas, and a centralized server for management.
  - [ADHD](#) - Active Defense Harbinger Distribution (ADHD) is a Linux distro based on Ubuntu LTS. It comes with many tools aimed at active defense preinstalled and configured.
- Network Analysis Tool
  - [Tracexploit](#) - replay network packets.
- Log anonymizer
  - [LogAnon](#) - log anonymization library that helps having anonymous logs consistent between logs and network captures.
- Low interaction honeypot (router back door)
  - [Honeypot-32764](#) - Honeypot for router backdoor (TCP 32764).
- honeynet farm traffic redirector
  - [Honeymole](#) - deploy multiple sensors that redirect traffic to a centralized collection of honeypots.
- HTTPS Proxy
  - [mitmproxy](#) - allows traffic flows to be intercepted, inspected, modified and replayed.
- System instrumentation
  - [Sysdig](#) - open source, system-level exploration: capture system state and activity from a running Linux instance, then save, filter and analyze.
  - [Fibratus](#) - tool for exploration and tracing of the Windows kernel.
- Honeypot for USB-spreading malware
  - [Ghost-usb](#) - honeypot for malware that propagates via USB storage devices.
  - [Honeystick](#) - low interaction honeypot on USB stick

- Data Collection
  - [Kippo2MySQL](#) - extracts some very basic stats from Kippo's text-based log files (a mess to analyze!) and inserts them in a MySQL database.
  - [Kippo2ElasticSearch](#) - Python script to transfer data from a Kippo SSH honeypot MySQL database to an ElasticSearch instance (server or cluster).
- Passive network audit framework parser
  - [pnaf](#) - Passive Network Audit Framework.
- VM monitoring and tools
  - [VIX virtual machine introspection toolkit](#) - VMI toolkit for Xen, called Virtual Introspection for Xen (VIX).
  - [vmscope](#) - Monitoring of VM-based.
  - [vmitools](#) - C library with Python bindings that makes it easy to monitor the low-level details of a running virtual machine.
  - [Antivmdetect](#) - Script to create templates to use with VirtualBox to make vm detection harder.
  - [VMCloak](#) - Automated Virtual Machine Generation and Cloaking for Cuckoo Sandbox.
- Binary debugger
  - [Hexgolems - Schem Debugger Frontend](#) - A debugger frontend.
  - [Hexgolems - Pint Debugger Backend](#) - A debugger backend and LUA wrapper for PIN.
- Mobile Analysis Tool
  - [APKInspector](#) - APKInspector is a powerful GUI tool for analysts to analyze the Android applications.
  - [Androguard](#) - Reverse engineering, Malware and goodware analysis of Android applications ... and more.
- Low interaction honeypot
  - [Honeypoint](#) - platform of distributed honeypot technologies.
  - [Honeyperl](#) - Honeypot software based in Perl with plugins developed for many functions like : wingates, telnet, squid, smtp, etc.
- Honeynet data fusion
  - [HFlow2](#) - data coalescing tool for honeynet/network analysis.
- Server
  - [LaBrea](#) - takes over unused IP addresses, and creates virtual servers that are attractive to worms, hackers, and other denizens of the Internet.
  - [Honeysink](#) - open source network sinkhole that provides a mechanism for detection and prevention of malicious traffic on a given network.
  - [KFSensor](#) - Windows based honeypot Intrusion Detection System (IDS).
  - [Honeyd](#) Also see [more honeyd tools](#).
  - [UDPot Honeypot](#) - Simple UDP / DNS honeypot scripts.
  - [Conpot](#) - ow interactive server side Industrial Control Systems honeypot.
  - [Bifrozt](#) - High interaction honeypot solution for Linux based systems.
  - [Beeswarm](#) - Honeypot deployment made easy.
  - [Bait and Switch](#) - redirects all hostile traffic to a honeypot that is partially mirroring your production system.
  - [Artillery](#) - open-source blue team tool designed to protect Linux and Windows operating systems through multiple methods.
  - [slipm-honeypot](#) - A simple low-interaction port monitoring honeypot.
  - [HoneyWRT](#) - low interaction Python honeypot designed to mimic services or ports that might get targeted by attackers.
  - [Amun](#) - vulnerability emulation honeypot.
  - [TelnetHoney](#) - A simple telnet honeypot.
  - [Hontel](#) - Telnet Honeypot.
  - [MTPot](#) - Open Source Telnet Honeypot, focused on Mirai malware.
  - [Heralding](#) - A credentials catching honeypot.

- [VNC-Pot](#) - A low interaction VNC honeypot.
- [vnclowpot](#) - A low interaction VNC honeypot.
- [SIREN](#) - Semi-Intelligent HoneyPot Network - HoneyNet Intelligent Virtual Environment.
- [telnetlogger](#) - A Telnet honeypot designed to track the Mirai botnet.
- [honeytrap](#) - a low-interaction honeypot and network security tool written to catch attacks against TCP and UDP services.
- [mwcollectd](#) - a versatile malware collection daemon, uniting the best features of nepenthes and honeytrap.
- [portlurker](#) - Port listener / honeypot in Rust with protocol guessing and safe string display.
- IDS signature generation
  - [Honeycomb](#) - Automated signature creation using honeypots.
- Lookup service for AS-numbers and prefixes
  - [CC2ASN](#) - A simple lookup service for AS-numbers and prefixes belonging to any given country in the world.
- Web interface (for Thug)
  - [Rumal](#) - Thug's Rumāl: a Thug's dress & weapon.
- Data Collection / Data Sharing
  - [HPfriends](#) - data-sharing platform.
  - [HPFeeds](#) - lightweight authenticated publish-subscribe protocol.
- central management tool
  - [PHARM](#) - Manage , Report, Analyze your distributed Nepenthes instances.
- Network connection analyzer
  - [Impost](#) - a network security auditing tool designed to analyze the forensics behind compromised and/or vulnerable daemons.
- Honeypot deployment
  - [Modern Honeynet Network](#) - makes deploying and managing secure honeypots extremely simple.
  - [SurfIDS](#) - an open source Distributed Intrusion Detection System based on passive sensors.
- Honeypot extensions to Wireshark
  - [Wireshark Extensions](#) - support applying Snort IDS rules and signatures against pcap files.
- Telephony honeypot
  - [Zapping Rachel](#)
- Client
  - [Pwnypot](#) - High Interaction Client Honeypot
  - [MonkeySpider](#)
  - [Capture-HPC-NG](#)
  - [Wepawet](#)
  - [URLQuery](#)
  - [Trigona](#)
  - [Thug](#)
  - [Shelia](#)
  - [PhoneyC](#)
  - [Jsunpack-n](#)
  - [HoneyC](#)
  - [HoneyBOT](#)
  - [CWSandbox / GFI Sandbox](#)
  - [Capture-HPC-Linux](#)
  - [Capture-HPC](#) - a high interaction client honeypot (also called honeyclient).

- [YALIH \(Yet Another Low Interaction Honeyclient\)](#) - a low Interaction Client honeypot designed to detect malicious websites through signature, anomaly and pattern matching techniques
- Binary Management and Analysis Framework
  - [Viper](#)
- Honeypot
  - [Single-honeypot](#)
  - [Honeyd For Windows](#)
  - [IMHoneypot](#)
  - [Deception Toolkit](#)
- PDF document inspector
  - [peepdf](#)
- Distribution system
  - [Thug Distributed Task Queuing](#)
- HoneyClient Management
  - [HoneyWeb](#)
- Network Analysis
  - [HoneyProxy](#)
- Hybrid low/high interaction honeypot
  - [HoneyBrid](#)
- SSH Honeypots
  - [Kojoney](#)
  - [Kojoney2](#) - low interaction SSH honeypot written in Python. Based on Kojoney by Jose Antonio Coret
  - [Kippo](#) - Medium interaction SSH honeypot
    - [LongTail Log Analysis @ Marist College](#) - analyzed SSH honeypot logs
    - [DRG SSH Username and Password Authentication Tag Clouds](#) - live updated word clouds of SSH login honeypot data
  - [Cowrie](#) - Cowrie SSH Honeypot (based on kippo)
  - [sshlowpot](#) - Yet another no-frills low-interaction ssh honeypot in Go.
  - [sshhipot](#) - High-interaction MitM SSH honeypot
  - [DShield docker](#) - Docker container running cowrie with DShield output enabled.
  - [hornet](#) - Medium interaction SSH Honeypot that supports multiple virtual hosts
  - [ssh-honeypot](#) - Fake sshd that logs ip addresses, usernames, and passwords.
- Distributed sensor project
  - [DShield Web Honeypot Project](#)
  - [Distributed Web Honeypot Project](#)
- A pcap analyzer
  - [Honeysnap](#)
- Client Web crawler
  - [HoneySpider Network](#)
- Network traffic redirector
  - [Honeywall](#)
- Honeypot Distribution with mixed content

- [HoneyDrive](#)
- Honeypot sensor
  - [Dragon Research Group Distro](#)
  - [Honeeeepi] (<https://redmine.honeynet.org/projects/honeeeepi/wiki>) - Honeeeepi is a honeypot sensor on Raspberry Pi which based on customized Raspbian OS.
- File carving
  - [TestDisk & PhotoRec](#)
- Sebek
  - [Sebek](#) - data capture
  - [Qebek](#) - QEMU based Sebek. As Sebek, it is data capture tool for high interaction honeypot.
  - [xebek](#) - Sebek on Xen
- SSH proxy
  - [HonSSH](#)
- Anti-Cheat
  - [Minecraft honeypot](#)
- behavioral analysis tool for win32
  - [Capture BAT](#)
- Live CD
  - [DAVIX](#)
- Spamtrap
  - [Mailoney](#) - SMTP honeypot, Open Relay, Cred Harvester written in python.
  - [Spampot.py](#)
  - [Spamhole](#)
  - [spamd](#)
  - [Mail::SMTP::Honeypot](#) - perl module that appears to provide the functionality of a standard SMTP server
  - [honeypot](#) - The Project Honey Pot un-official PHP SDK
  - [SpamHAT](#) - Spam Honeypot Tool
  - [SendMeSpamIDS.py](#) Simple SMTP fetch all IDS and analyzer
  - [Shiva](#) - Spam Honeypot with Intelligent Virtual Analyzer
    - [Shiva The Spam Honeypot Tips And Tricks For Getting It Up And Running](#)
- Distributed spam tracking
  - [Project Honeypot](#)
- Commercial honeynet
  - [Specter](#)
  - [Netbait](#)
  - [HONEYPOINT SECURITY SERVER](#) - distributed honeypot, includes IT and SCADA emulators
- Server (Bluetooth)
  - [Bluepot](#)
- Dynamic analysis of Android apps
  - [Droidbox](#)
- Dockerized Low Interaction packaging
  - [Manuka](#)

- [Dockerized Thug](#)
  - [Dockerpot](#) A docker based honeypot.
  - [Docker honeynet](#) Several Honeynet tools set up for Docker containers
- Network analysis
  - [Quechua](#)
- SIP Server
  - [Artemnesia VoIP](#)
- Malware collection
  - [Honeybow](#)
- IOT Honeypot
  - [HoneyThing](#) - TR-069 Honeypot
- Honeytokens
  - [Honeybits](#) - A tool that can be used to create and place breadcrumbs and honeytokens to lead the attackers to honeypots (in production environment)
  - [CanaryTokens](#)
  - [dcept](#) - A tool for deploying and detecting use of Active Directory honeytokens

## Honeyd Tools

---

- Honeyd plugin
  - [Honeycomb](#)
- Honeyd viewer
  - [Honeyview](#)
- Honeyd to MySQL connector
  - [Honeyd2MySQL](#)
- A script to visualize statistics from honeyd
  - [Honeyd-Viz](#)
- Honeyd UI
  - [Honeyd configuration GUI](#) - application used to configure the honeyd daemon and generate configuration files
- Honeyd stats
  - [Honeydsum.pl](#)

## Network and Artifact Analysis

---

- Sandbox
  - [RFISandbox](#) - a PHP 5.x script sandbox built on top of [funcall](#)
  - [dorothy2](#) - A malware/botnet analysis framework written in Ruby
  - [COMODO automated sandbox](#)
  - [Argos](#) - An emulator for capturing zero-day attacks
  - [libemu](#) - Shellcode emulation library, useful for shellcode detection.
  - [Pylibemu](#) - A Libemu Cython wrapper.
  - [imalse](#) - Integrated MALware Simulator and Emulator.
  - [Cuckoo](#) - the leading open source automated malware analysis system.
- Sandbox-as-a-Service



- [malwr.com](#) - free malware analysis service and community.
- [detux.org](#) - Multiplatform Linux Sandbox.
- [Joebox Cloud](#) - analyzes the behavior of malicious files including PEs, PDFs, DOCs, PPTs, XLSs, APKs, URLs and MachOs on Windows, Android and Mac OS X for suspicious activities.
- [VirusTotal](#)
- [Hybrid Analysis](#) - a free malware analysis service powered by Payload Security that detects and analyzes unknown threats using a unique Hybrid Analysis technology.

## Data Tools

---

- Front Ends
  - [Tango](#) - Honeypot Intelligence with Splunk.
  - [Django-kippo](#) - Django App for kippo SSH Honeypot.
  - [Wordpot-Frontend](#) - a full featured script to visualize statistics from a Wordpot honeypot.
  - [Shockpot-Frontend](#) - a full featured script to visualize statistics from a Shockpot honeypot.
  - [honeypotDisplay](#) - A flask website which displays data I've gathered with my SSH Honeypot.
  - [honeyalarmg2](#) - Simplified UI for showing honeypot alarms.
  - [DionaeaFR](#) - Front Web to Dionaea low-interaction honeypot.
- Visualization
  - [Kippo-Graph](#) - a full featured script to visualize statistics from a Kippo SSH honeypot.
  - [Kippo stats](#) - Mojolicious app to display statistics for your kippo SSH honeypot.
  - [HoneyStats](#) - A statistical view of the recorded activity on a Honeynet.
  - [HoneyMap](#) - Real-time websocket stream of GPS events on a fancy SVG world map.
  - [HoneyMalt](#) - Maltego tranforms for mapping Honeypot systems.
  - [Glastopf Analytics](#)
  - [Afterglow Cloud](#)
  - [Afterglow](#)
  - [ovizart](#) - visual analysis for network traffic.
  - [HpfeedsHoneyGraph](#) - a visualization app to visualize hpfeeds logs.
  - [Acapulco](#) - Automated Attack Community Graph Construction.
  - [Sebek Dataviz](#) - Sebek data visualization

## Guides

---

- [T-Pot: A Multi-Honeypot Platform](#)
- [Honeypot \(Dionaea and kippo\) setup script](#)
- Deployment
  - [Dionaea and EC2 in 20 Minutes](#) - a tutorial on setting up Dionaea on an EC2 instance
  - [honeypotpi](#) - Script for turning a Raspberry Pi into a Honey Pot Pi
- Research Paper
  - [vEYE](#) - behavioral footprinting for self-propagating worm detection and profiling.