ADHD Tools Usage Document

ADHD
HoneyDrive
Windows

(ADHD/ADHD_logo.jpg)

ADHD Version: **0.7.2** | Github Page (https://github.com/adhdproject) | Sourceforge Page (http://sourceforge.net/projects/adhd/)

Black Hills Information Security (http://www.blackhillsinfosec.com)

ADHD

[↑]

- Credentials
- Artillery
    - Example 1: Running Artillery
    - Example 2: Triggering a Honeyport
    - Example 3: Adding a File to a Watched Directory
- Bear Trap
    - Example 1: Basic Usage
- BeEF
    - Example 1: Hooking a Web Browser
    - Example 2: Browser Based Exploitation With BeEF
- Cowrie

    - Example 1: Running Cowrie
    - Example 2: Cowrie In Action
    - Example 3: Viewing Cowrie's Logs
- Cryptolocked
    - Example 1: Debug Mode
    - Example 2: Arming Cryptolocked
    - Example 3: Cryptolocked's Tentacles
    - Example 4: Email Alerts
- Cryptolocked-ng
    - Example 1: Debug Mode
    - Example 2: Arming Cryptolocked-ng
    - Example 3: Cryptolocked-ng's Tentacles
    - Example 4: Cryptolocked-ng's Huntr
    - Example 5: Email Alerts
- Decloak
    - Example 1: Compiling Flash and Java Objects
    - Example 2: Setting Up the Decloak DNS Server
    - Example 3: Browsing to a Decloak Activated Website
    - Example 4: Viewing the Decloak Database
    - Example 5: Tearing Down the Decloak DNS Server
- DenyHosts
    - Example 1: Installing DenyHosts
    - Example 2: Enabling DenyHosts
    - Example 3: Basic Configuration
- Docz.py
    - Usage: Basic Usage
    - Example 1: Creating a Webbug for Honeybadger
    - Example 2: Creating a Webbug for Webbugserver
- Gcat
    - Example 1: Deploying an Implant
    - Example 2: Running a Command & Retrieving Output
- Ghostwriting.sh
    - Example 1: Obfuscating an executable with Ghostwriting.sh
- Honey Badger
    - Example 1: Web Browser Share Location
    - Example 2: Creating a Honey Badger User
    - Example 3: Viewing the Honey Badger Map
    - Example 4: Using Java to Find Nearby Wireless APs
- Honey Ports
    - Example 1: Monitoring A Port With HoneyPorts
    - Example 2: Blacklisting In Action
    - Example 3: Spoofing TCP Connect for Denial Of Service
- Human.py
    - Example 1: Setting up Monitoring on a service account
    - Example 2: Cancelling monitoring and purging records.
- Invisiport
    - Example 1: Customizing the Configurations

- Jar-Combiner
    - Example 1: Finding the Entrypoints
    - Example 2: Combining Two jars
    - Example 3: Signing Finished.jar
    - Example 4: Launching Your Jar Via HTML
    - Example 5: Changing Java Security Settings
- Java Applet Web Attack
    - Example 1: Cloning a URL
    - Example 2: Weaponizing a Web Page
    - Example 3: Starting the Attack Server
    - Example 4: Stopping the Attack Server
    - Example 5: Customizing the Payloads
- Kippo
    - Example 1: Running Kippo
    - Example 2: Kippo In Action
    - Example 3: Viewing Kippo's Logs
- Lockdown
    - Example 1: Customizing the Configurations
    - Example 2: Triggering the failsafe
- Molehunt
    - Example 1: Configuring Molehunt
    - Example 2: Running a Campaign
    - Example 3: Opening a File
    - Example 4: Monitoring for Leaks
- OpenBAC
    - Example 1: Initialization
    - Example 2: Generate a Hash
    - Example 3: Authentication
    - Example 4: Implementing in Code
- OpenCanary
    - Example 1: Deploying OpenCanary as a Service
- OsChameleon
    - Example 1: Scanning Yourself
- PHP-HTTP-Tarpit
    - Example 1: Deployment
- Portspoof
    - Example 1: Starting Portspoof
    - Example 2: Spoofing Service Signatures
    - Example 3: Cleaning Up
- PSAD
    - Example 1: Installing PSAD
    - Example 2: Iptables Configuration
    - Example 3: Checking for Messages
    - Example 4: Email Alerts
    - Example 5: Updating Signatures
- Pushpin
    - Example 1: Find Tweets Sent from Times Square
- Recon-ng

    - Example 1: Finding Hosts With Bing
    - Example 2: Viewing Stored Data
    - Example 3: Reporting From Within Recon-ng
- Rubberglue
    - Example 1: Setting a Trap
- SET
    - Example 1: Look over SET's features
- Simple-Pivot-Detect
    - Usage
- Spidertrap
    - Example 1: Basic Usage
    - Example 2: Providing a List of Links
    - Example 3: Trapping a Wget Spider
- Sqlite Bug Server
    - Example 1: Initializing the database
    - Example 2: Setting up the Web Bug Doc
    - Example 3: Viewing Bug Connections in the Database
- Sweeper
    - Example 1: Setting a Trap
- TALOS
    - Example 1: Running a Honeyport
    - Example 2: Backgrounding Modules & Reading Notifications
    - Example 3: Aliases & Autocomplete
    - Example 4: Basic Scripting
    - Example 5: Tripcodes
    - Example 6: Advanced Scripting
    - Example 7: Phantom Basics
- TcpRooter
    - Example 1: Increasing Coverage
- Web Bug Server
    - Example 1: Setting up the Web Bug Doc
    - Example 2: Viewing Bug Connections in the Database
- Weblabyrinth
    - Example 1: Basic Usage
    - Example 2: Viewing the Database with Adminer
    - Example 3: Wget Gets Lost in the Labyrinth
- Wordpot
    - Example 1: Running a fake Wordpress install

HoneyDrive

[↑]

- Conpot
    - Example 1: Usage
- Dionaea
    - Example 1: Usage
- Thug
    - Example 1: Usage

Windows

[↑]
