DumpsterFire Toolset

Generating Network & System Shenanigans to Manipulate Blue Teams

Presenter: TryCatchHCF

 @TryCatchHCF

Presenter Background

Principal Security Researcher & Red Team member at a Fortune 500

Prior roles: Principal Infosec Engineer, Pentest Lead, AppSec Team Lead, Shrubber of Fine Shrubberies

Former USMC intelligence analyst, counterintelligence specialist

Cmdr. Sisko was best Star Trek leader (Fight me)

Bachelors - Cognitive Science; Masters - Information Assurance

Certs - Various Acronyms, some of which hit me up for money each year

DumpsterFire Toolset

Presentation Roadmap

- Background: Red Team Goals & Operations
- Challenges & Roadblocks
- Shenanigans / Examples
- DumpsterFire Toolset Walkthrough

Background

Red Team Goals & Operations

DumpsterFire Toolset

Red Team Tasks

- Simulate full range of attackers
    - From loud “skiddie at the gates” to advanced “low and slow” pivoting & exfiltration, extended campaigns (months) as well as “smash & grab”
- Simulate “Errant Users”
    - Downloading, installing, and running unauthorized apps (file sharing, scanning tools, “malicious” utilities)
    - Running unauthorized services (FTP, Web servers, etc.)
- Purple Team
    - Tabletop exercises, coordinated SIEM config validation
- Physical security (not covered here)

DumpsterFire Toolset

Red Team Tasks (cont.)

- Focus on rank-prioritized threats per analysis of organization's risk profile
- All for the purpose of helping Blue Team improve security (defenses, policies, procedures)
  - SIEM (Security Information & Event Management) tools
    - Tuning for best signal-to-noise ratios
    - Prioritizing alerts by type & volume
    - Identify gaps in detection, collection, alerting (settings & tools)
  - SOC/CIRT Response
    - Policies and procedures
    - Drills for teams & individuals (training & assessment)

Challenges & Roadblocks

DumpsterFire Toolset

Red Team Dilemmas

- So much attack surface
  - So little time
  - So few resources

- Most organizations don't have Red Teams
  - Those that do, usually have small teams in high operational demand

- Difficult to scale Red Team even when you have one

DumpsterFire Toolset

Red Team Dilemmas

- Common for corporate assets to be located worldwide
  - Multiple timezones to support
- SOCs are 24/7 with multiple shifts / teams
  - How to provide live exercise support for all shifts?
- Providing consistent, repeatable engagements
  - Want to compare “apples to apples” to track improvements & identify chronic problem areas

DumpsterFire Toolset

Caffeine can only help so much.

DumpsterFire Toolset

Not Just Red Team's Dilemmas

- 3rd-party pentesters suffer similar constraints
    - Limited windows of engagement
    - Often small team (or just one person)
    - Need to show maximum return on engagement
        - Single path to DC is useful, but limited
- Blue Teams don't have expertise in creating attacks
    - And even if they did… time & resource limitations
    - Internal bias towards existing configs & experiences

DumpsterFire Toolset

Blue Team Dilemmas

- Orgs without Red Teams leave their Blue Teams untested
  - Stuck with “Annual 3rd-Party Nessus Assessment”
  - Tabletop exercises
    - Only test policy & procedures
    - Typically only one or two scenarios
  - No realtime operational tests of sensor thresholds or incident response edge cases

DumpsterFire Toolset

SOC/CIRT Reaction:

DumpsterFire Toolset

SOC/CIRT Reaction (cont.)

“Hey! I’m tested every single day with real world scenarios!”

- Sure, but missing some key things
  - Repeatability across shifts, using same live scenarios
  - Customized scenarios that simulate events your team hasn’t encountered yet, but should be ready for
  - Scenarios tailored to methodically test SIEM coverage & alerting
- You can only respond to what you’re already collecting & alerting on
  - “Don’t know what you don’t know” about gaps in sensors / alerting

DumpsterFire Toolset

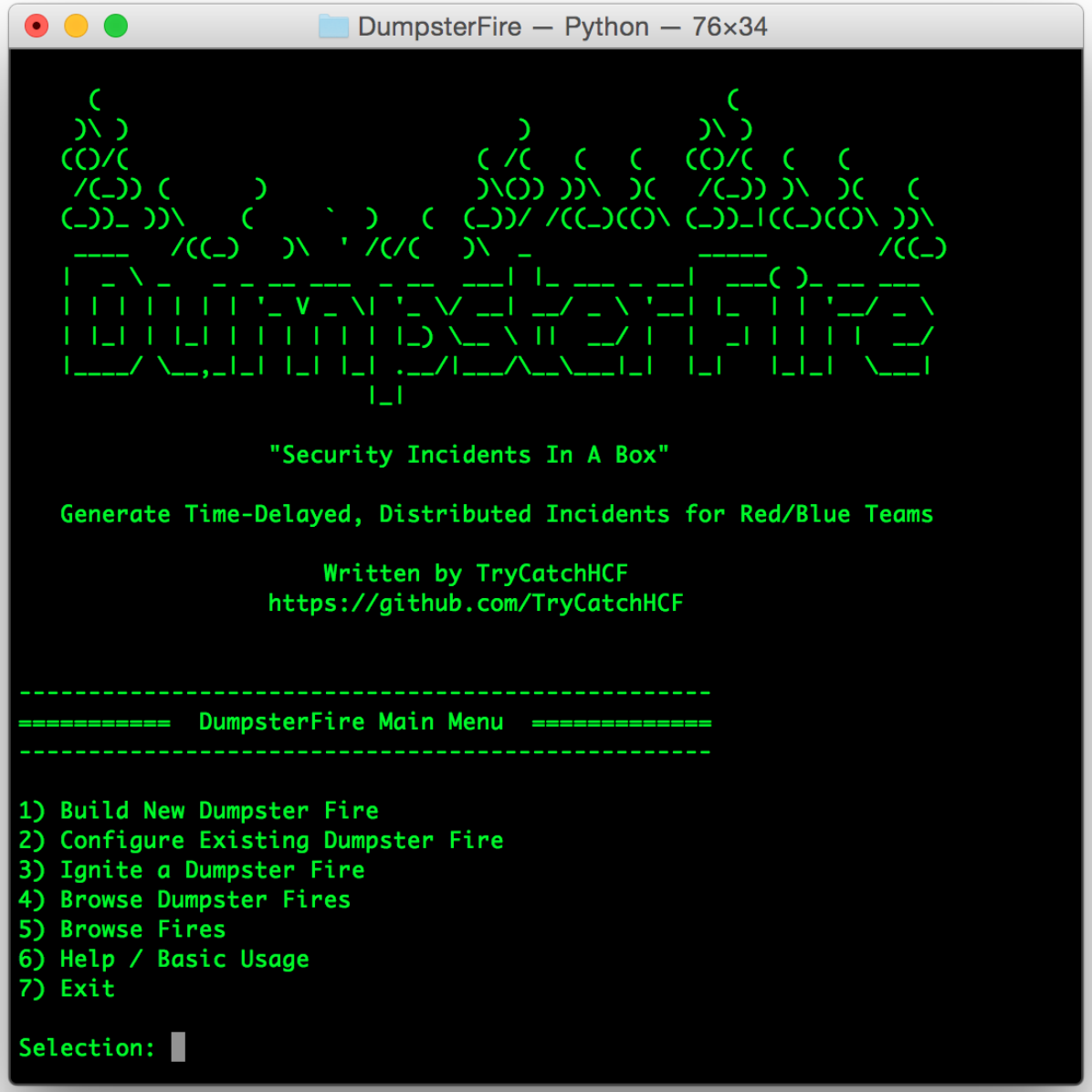
Great, so the Red Team can’t scale (or doesn’t even exist)

“What now?”

DumpsterFire Toolset

Automation to the rescue!

DumpsterFire Toolset



DumpsterFire Toolset

Ever wondered how your Blue Team would respond to Mirai botnet activity on your internal network?

Let’s find out!

DumpsterFire Toolset

Don’t have a Red Team but wish you had an easy way to run controlled drills against all of your SOC shift teams?

Plug-n-spray!

DumpsterFire Toolset

Wish you could support a Red Team engagement against that remote team that's 8 timezones away, without waking up at 3:00am?

Hit that snooze button!

DumpsterFire Toolset

Wish you could simultaneously rickroll all of your opponents' sub-networks during your annual cyberwarfare exercise?

DumpsterFire Toolset

And while we're at it…

DumpsterFire Toolset

Why settle for just one automated friend?

DumpsterFire Toolset

DumpsterFire Toolset

But first…

Let’s talk about Shenanigans

DumpsterFire Toolset

Staying Employed & Out of Federal Prison

- Standard rules-of-engagement boilerplate may not cover additional activities
    - If it's not in writing, it's not happening
- Simulate, don't destroy / corrupt
    - Goal is help Blue Team tune & improve, not impact business
- No automated pivoting
    - Too hard to control, can't guarantee you're still in scope
    - Building & deploying a worm **will never be in scope**

DumpsterFire Toolset

DumpsterFire Toolset

Red Team Shenanigans

- Go beyond the standard attack chain we all know & love
  - Recon -> Scan -> Attack -> Persist -> Pivot
- Advantages in manipulating Blue Team
- 3 Categories
  - Distract
  - Lure onto Compromised System
  - Overwhelm

DumpsterFire Toolset

Advantages in Manipulating Blue Team

- Move beyond the standard attack chain scenarios
- Better reflects evolving advanced attacks that follow up original attack chains with secondary infections & attacks meant to cover up the initial campaign
- Create parallel security events that provide SOC analysts with an easier investigative path to pursue (and close)
    - Generate the Occam's Razor you wish them to find
- Lure privileged users into your credential traps

DumpsterFire Toolset

Goals in Manipulating Blue Team

- Move beyond the standard attack chain scenarios
  - Sound familiar yet?

- Give Blue Teams direct experience in managing layered attack scenarios, hands-on in their operational environment

- Help Blue Teams get to the next level, which in turn forces Red Team to get to their next level

  - Positive security feedback loop
  - Help analysts think strategically, not just tactically
  - Prepare analysts for evolving real-world threats

DumpsterFire Toolset

Distract

DumpsterFire Toolset

Manipulating Blue Team - Distraction

- Create distractions to throw Blue Team off your trail
- Build & execute complete parallel competing narratives
- Alternate points of compromise
  - Visits website; malicious app installed; loud activity
- Create scapegoats & decoys, mimicking methodologies and C&C infrastructure of known campaigns
  - Lead Blue Team down enticing (& utterly false) paths

DumpsterFire Toolset

DumpsterFire Toolset

(But seriously, you really don't want your activities associated with an APT's methodologies / external C&C infrastructure / etc.)

(No, seriously. Just don't.)

(Unless it's in scope. In writing. And signed by people with authority to handle inquiries from the Feds.)

(Remember, we operate in a world where an externally sourced default nmap scan will make some orgs scream "APT!" and get your proxy provider subpoenaed.)

DumpsterFire Toolset

Lure

DumpsterFire Toolset

("Pearls Before Swine" is an amazing comic strip, btw)

DumpsterFire Toolset

Manipulating Blue Team - Lure

- Sometimes admin credentials are hard to come by
- Credential traps are like fishing off a dock
  - “Hurry up and wait”
- Move from dock fishing to chumming the waters
  - Create events to lure admin users onto the network & systems that are hosting your credential traps
  - Use lower privilege accounts to socially engineer IT dept.

DumpsterFire Toolset

Manipulating Blue Team - Lure (cont.)

- Using an unprivileged user's account, send email / Slack chat to admin(s) with a URL you're trying to access (compromised and hooked, of course)
- Fill a local or shared directory to capacity, requiring privileged user to access and cleanup
- Generate faulty network activity that interferes with users
- Any activity that will likely cause a privileged user to remotely authenticate to the resource (login, fileshare, etc.)

DumpsterFire Toolset

Overwhelm

DumpsterFire Toolset

Manipulating Blue Team - Overwhelm

- Create a volume of security events that overwhelm available resources, useful in various circumstances
    - Tactical Feint (e.g. loudly attack exposed Website login page while quietly exploiting RDP on adjacent network)
    - When you're ready to burn your operation
    - When Blue Team is hot on your trail & you need more time
- Each event requires fixed overhead of resources
    - Ticket Management - Open / Investigate / Close
    - Ties up at least one analyst
    - Simulating severe events raises priority & necessitates immediate attention

DumpsterFire Toolset

Manipulating Blue Team - Overwhelm (cont.)

- Playing a numbers game
    - If staff can handle X critical events at a time, then generating 3X events means 2/3rds of those events will lay idle until the other events are investigated and closed out
    - If your staged distractions are perceived to be higher criticality than evidence of your actual operations, you can buy your team some critical time to complete your goals
- Best to only use “Overwhelm” during wargames or other exercises where operational SOC/CIRT teams will not be pulled away from critical duties

DumpsterFire Toolset

Manipulating Blue Team - Overwhelm (cont.)

- Separate waves of events by time
  - Battlestar Galactica “Every 33 Minutes” effect
  - Just as responders are getting a handle on the current wave of events, the next series triggers
  - Only works if the event trigger mechanisms remain undiscovered
  - Fun to make each successive wave generate increasingly severe events

DumpsterFire Toolset

Manipulating Blue Team - Overwhelm (cont.)

- Separate waves of events by time (cont.)
  - Example Scenario: Organization has Port 22 open on most systems for remote admin access. Network is segmented, but compromised credentials that give attackers access to all subnets.
  - Target multiple subnets for time-delayed, sequenced brute-force login attempts over SSH on Port 22 on local subnet. (Credentials are purposely chosen to fail.)
  - Select a system on each targeted subnet, login remotely and attempt to download payload from Red Team controlled external endpoints (Whack-a-Mole!)

DumpsterFire Toolset

Shenanigans Bonus Round

Sometimes you just want to make things extra interesting

DumpsterFire Toolset

Shenanigans Bonus Round

Linux/Unix: Edit global .bashrc / .cshrc / .bash_profile

Locations: /etc/bash.bashrc /etc/bashrc (check your baseline)

- `stty s erase`
  - ’s’ key is now the backspace key, annoys in random ways
  - Try typing ‘ls’ / ‘netstat’ / ‘stty’ / ‘erase’
- `alias ls=‘echo’`
  - Blank line printed instead of directory listing

DumpsterFire Toolset

Shenanigans Bonus Round (cont.)

Linux/Unix: Edit global .bashrc / .cshrc / .bash_profile

- `alias pwd='echo "Directory not found"'`
- `alias cd='echo "Directory not found"'`
- `alias df='echo "Error accessing device"'`
- `alias du='echo "Error accessing device"'`
- `alias vi='echo "Could not allocate inode"'`

Troll emacs users while you're at it:

- `alias emacs='echo "vi refusing to allow emacs"'`

(.cshrc uses different format but you get the idea)

DumpsterFire Toolset

Shenanigans Bonus Round (cont.)

Cross-Platform

- Take screenshot of active desktop, install as desktop background
- Hide all other open apps

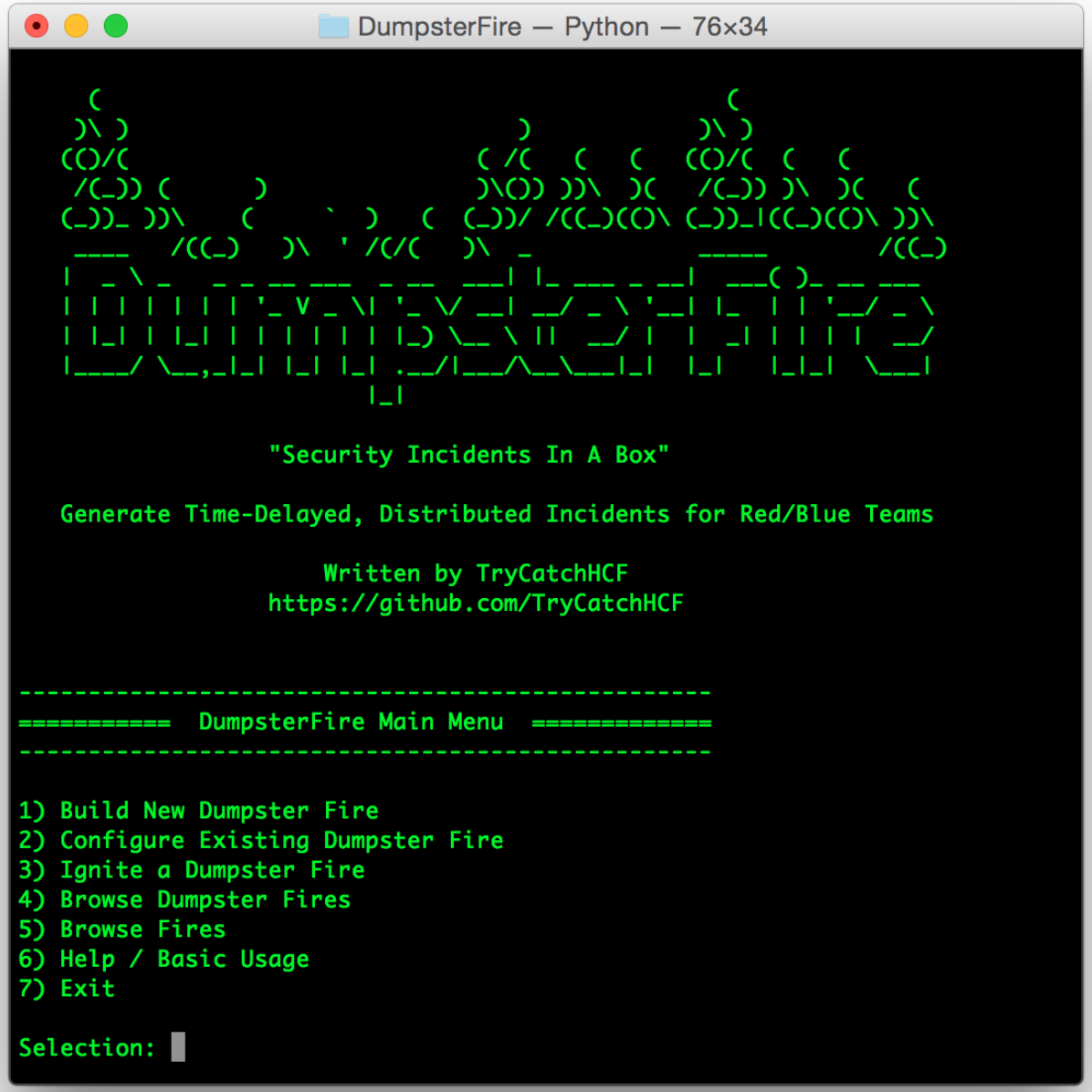
or

- Download screen-grab of ransomware lock screen, install as desktop background
- Hide all other open apps

DumpsterFire Toolset

Back to DumpsterFire!

DumpsterFire Toolset



DumpsterFire Toolset

- “Security Incidents In A Box!”
- Build & execute custom event chains to generate incident narratives / activities
- Time-Date Delayed Execution
  - Allows you to generate automated, sequenced events
  - Converts to Universal Coordinated Time (UTC) internally to avoid timezone confusion across global sites
- Parallel Deployments
  - Generate security incidents at scale, anytime, anywhere
- Numerous Fires plus pre-configured DumpsterFires to jumpstart your activities

DumpsterFire Toolset

- Lightweight, easy to use, easy to deploy
  - Menu-driven
  - Written in Python for cross-platform support
  - Quick start, immediate results

- Extensible - Customize for your unique threat space
  - Create your own Fire modules, add to Fires directory, start DumpsterFire Factory, burn away!

- No 3rd-party dependencies

- Open Source (MIT License)
  - “Free as in No Budget Approval Needed”

DumpsterFire Toolset

“That’s a lot of word salad. Details please.”

DumpsterFire Toolset

DumpsterFires

- Fires are modular events
  - Ex. Download a file; Scan a network; Login attempts
- DumpsterFires are collections of Fires
  - Chained together to create sequences of events
  - Functionality inspired by *nix command line utilities
- Tremendous power by chaining simple tools

DumpsterFire Toolset

DumpsterFires (cont.)

Chained Linux Tools:

```
% cat log.txt | cut -d ‘;’ -f3,5- | grep -i “login” | sort -un
```

Chained Fires for an Insider Threat DumpsterFire:

```
Visit Webpage about revenge -> Download Metasploit -> Scan
local subnet for Top 20 ports -> Brute force attacks against
Port 22 SSH -> Upload random data tarball to Red Team
controlled external node -> Visit Webpage about modifying logs
```

DumpsterFire Toolset

DumpsterFires (cont.)

- Building DumpsterFires is fun & fast, the tool guides you
- Modular process
  - Create a list of Fires in whatever order you want
  - Assign optional time-delta triggers to each Fire
  - Configure settings for selected Fires
  - Assign optional DateTime trigger to new DumpsterFire
  - Distribute & Ignite!

DumpsterFire Toolset

Just Like Building a Teddy Bear!

DumpsterFire Toolset

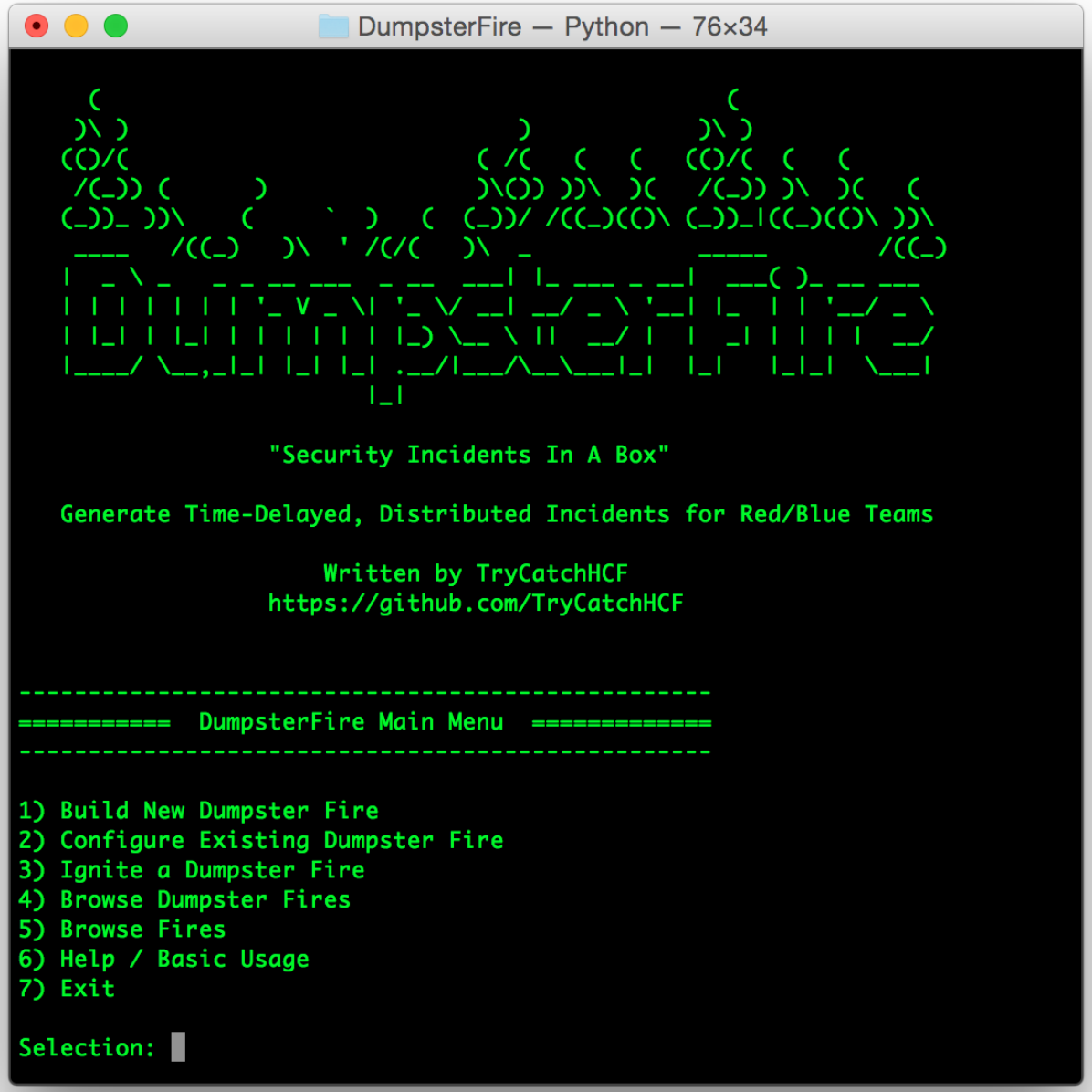
(Except the Teddy Bear is Evil)

DumpsterFire Toolset

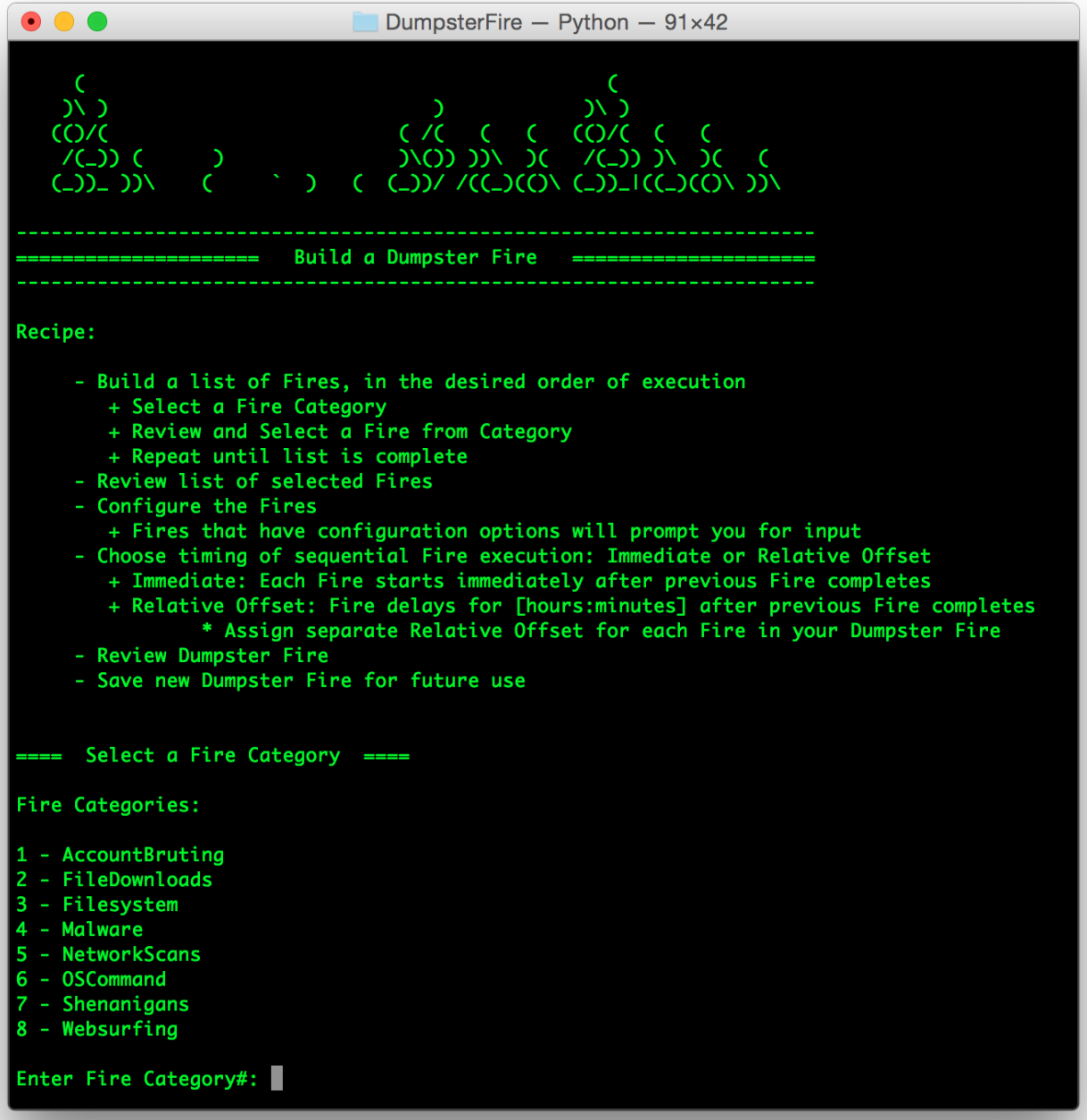
Fire Categories

- Network Scans (Loud & Wide; Targeted; Slow & Narrow)
- File Downloads (Github; Filesharing; Hacking Tools)
- Websurfing (Preconfigured URLs; Custom URLs)
- Account Bruteforcing (e.g. Simulated Mirai botnet activity)
- Filesystem Activities (Fill directory; Create IOC artifacts)
- Malware (Known C&C connects; Sinkholes; Custom)
- Custom OS Commands (Executes string you provide)
- Shenanigans (Annoying entries in shell profiles, etc.)

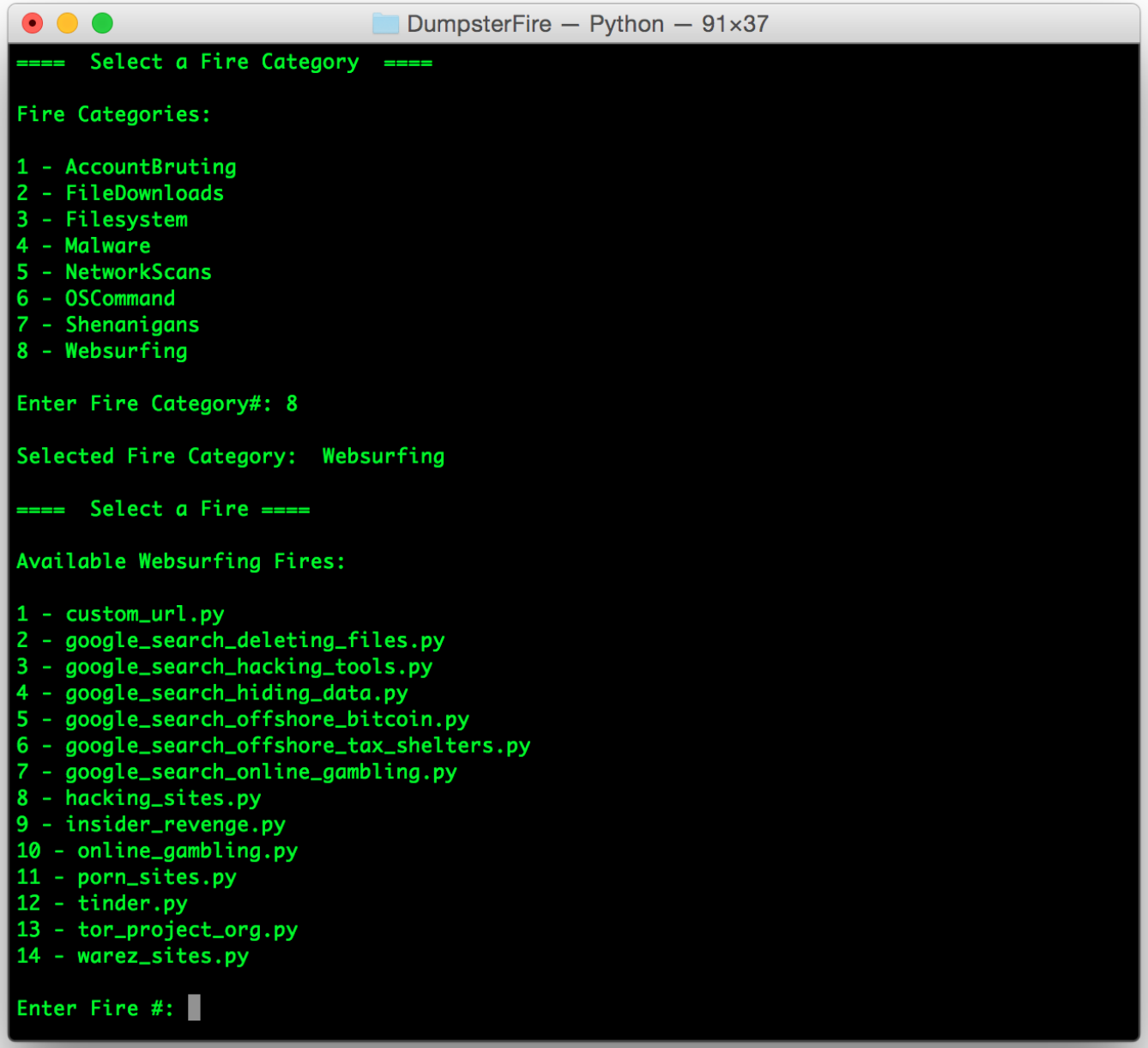
DumpsterFire Toolset



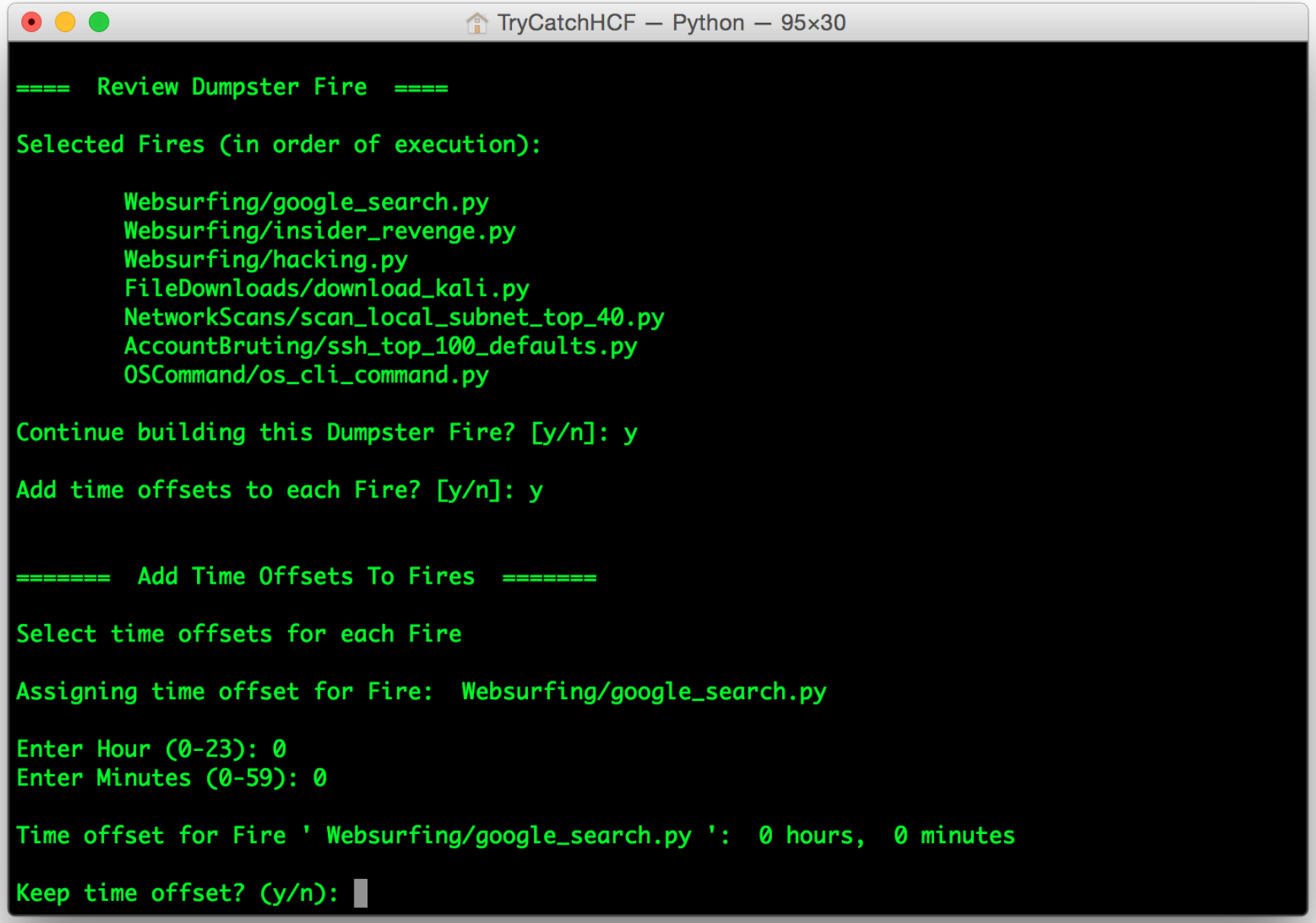
DumpsterFire Toolset



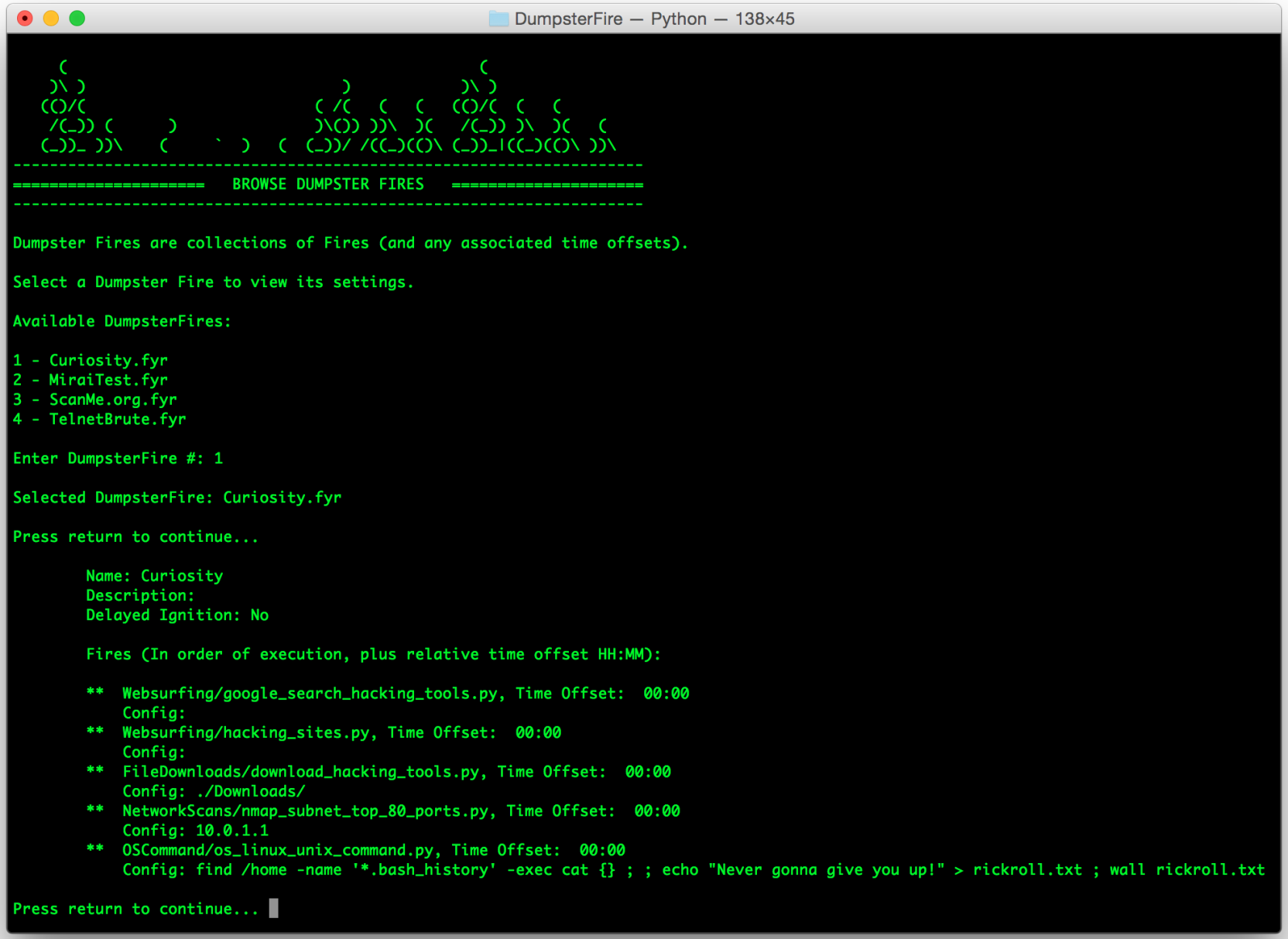
DumpsterFire Toolset



DumpsterFire Toolset



DumpsterFire Toolset



DumpsterFire Toolset

Red Team Benefits

- Scale your Red Team network / system activities
- Reproducible tailored engagements
- Date/Time triggers allow your operations to proceed without you having to enter sleep deprivation
- Logging can be activated, each Fire generating datetimestamps of their activities for later review (and accountability) w/ Blue Team

DumpsterFire Toolset

Blue Team Benefits

- Create and run tailored drills for your analysts
- Train and evaluate analysts in controlled scenarios
- Map & identify gaps in sensor coverage and alerting configuration
- Monitor & measure response
- Build history of results to demonstrate progress

DumpsterFire Toolset

Creating Custom Fires

DumpsterFire Toolset

Extensible Design

- Meant to be used, tailored for your operational needs
- NO HARDCODED CRUD TO MODIFY!
- Create your own custom Fire modules, drop into the collection of Fires, you're ready to go!
- Tool dynamically loads component content at runtime, based on contents of DumpsterFire's "FireModules/" directory
    - Fire Categories (generated from directory names)
    - Names of all Fire modules in each Category directory

DumpsterFire Toolset

Extensible Design (cont.)

- Recommend you keep your custom Fire modules simple and functionally encapsulated
- Minimizing dependencies and complexity allows you to quickly combine your Fire modules in novel sequences to meet operational needs
- In many cases, you may instead be able to do what you need by using existing “OSCommand” Fire modules
  - Include as many as you need in your DumpsterFire
  - Each “OSCommand” Fire module in your DumpsterFire can have its own unique command string

DumpsterFire Toolset

Extensible Design (cont.)

- For a quick start, copy and modify an existing Fire module that has similar functionality
- In the FireModules/ directory there is a Fire module template file you can copy ("custom_fire_template.py")
  - Contains comments, descriptions, and skeleton of all functions that must be implemented for your custom Fire module to integrate seamlessly with the tool
- Do NOT remove the "__init__.py" files in the subdirectories
  - Required for the tool to be able to dynamically load the Fire modules at runtime (it's a Python package thing)

DumpsterFire Toolset

Extensible Design (cont.)

- To create a new Fire Category, create a new directory under `“FireModules/“`
- When you add new Fire modules to a Fire Category directory, the tool will automatically make them available (**do not use spaces or periods in your Fire names -** messes up package names)
- Have to restart the tool to pick up Fire Category changes
- Your Fire module must implement the following methods
  - Configure()
  - Description()
  - GetParameters()
  - SetParameters()
  - ActivateLogging()
  - Ignite()

DumpsterFire Toolset

FireModule Template

- **Configure()**
  - Prompts user for input, populates FireModule’s parameters
- **Description()**
  - Return a string containing a description of the FireModule
- **GetParameters()**
  - Returns a single string of Fire's parameters
- **SetParameters(string)**
  - Takes a single string & populates Fire's members
- **ActivateLogging(boolean)**
  - Sets flag for Fire to generate a log of its activities (great for review)
- **Ignite()**
  - Executes Fire's actions

DumpsterFire Toolset

https://github.com/TryCatchHCF

@TryCatchHCF