Building Communities for Open Source Security Tools

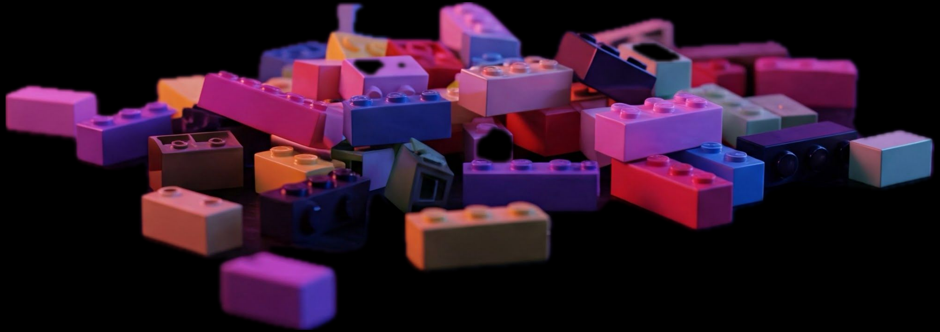
HD MOORE
Founder & CEO

Building

I’ve always liked making things and sharing them

I struggle with drawing, writing, & crafts

But I love building software



Security

Infosec software is incredibly fun to write

Treat the world as a large video game

With real consequences

Open Source

Building in the open is terrifying and exciting

A huge potential audience for your work

A great way to learn fast

And make friends!

Why Build OSS?

Solve a need that you or your organization has

Great for personal & career development

Effectively a startup with similar work

Fame? Spite? No bad reasons!

METASPLOIT
USSR
www.metasploit.com

The Metasploit Project

Created to make penetration testing safer

Initial focus was shellcode, not exploits

Shifted to exploits, scanners, payloads

A way to maintain research tools

A loud voice for disclosure

Just me in 2002

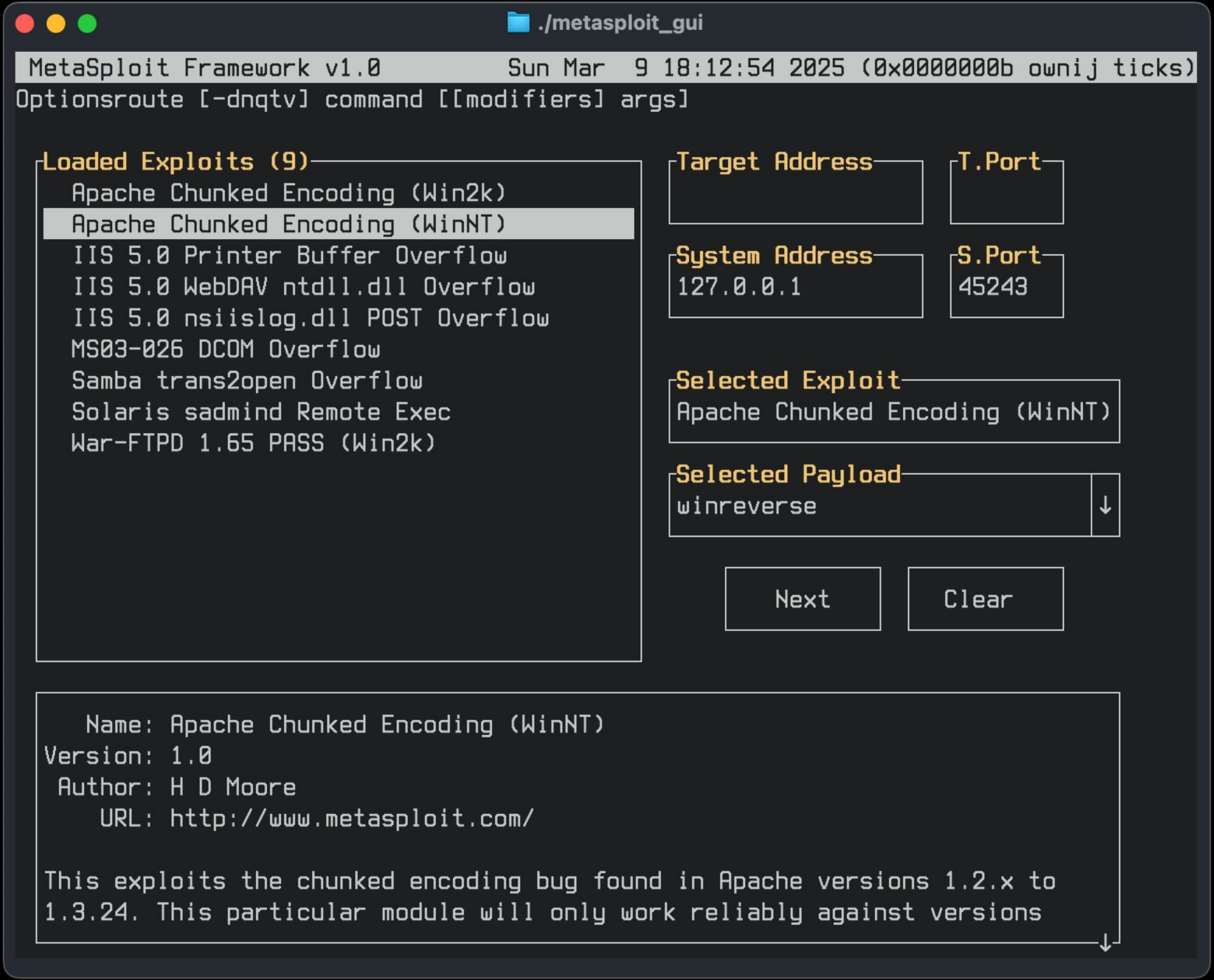
Metasploit 1 Was Terrible

Dinky Perl scripts with 9 shoddy exploits

Released in 2002 at HitB (Malaysia)

A “spoonm” emailed me to complain

I said ok, do it better…



```
./metasploit_gui

MetaSploit Framework v1.0          Sun Mar  9 18:12:54 2025 (0x0000000b ownij ticks)
Optionsroute [-dnqtv] command [[modifiers] args]

 ┌Loaded Exploits (9)──────────────────────────┐  ┌Target Address──┐  ┌T.Port─┐
 │  Apache Chunked Encoding (Win2k)            │  │                │  │       │
 │  Apache Chunked Encoding (WinNT)            │  └────────────────┘  └───────┘
 │  IIS 5.0 Printer Buffer Overflow            │  ┌System Address──┐  ┌S.Port─┐
 │  IIS 5.0 WebDAV ntdll.dll Overflow          │  │127.0.0.1       │  │45243  │
 │  IIS 5.0 nsiislog.dll POST Overflow         │  └────────────────┘  └───────┘
 │  MS03-026 DCOM Overflow                     │
 │  Samba trans2open Overflow                  │  ┌Selected Exploit───────────────┐
 │  Solaris sadmind Remote Exec                │  │Apache Chunked Encoding (WinNT)│
 │  War-FTPD 1.65 PASS (Win2k)                 │  └───────────────────────────────┘
 │                                             │  ┌Selected Payload─────────────┬─┐
 │                                             │  │winreverse                   │↓│
 │                                             │  └─────────────────────────────┴─┘
 │                                             │     ┌──────────┐  ┌──────────┐
 │                                             │     │   Next   │  │  Clear   │
 │                                             │     └──────────┘  └──────────┘
 └─────────────────────────────────────────────┘

 ┌────────────────────────────────────────────────────────────────────────────┐
 │   Name: Apache Chunked Encoding (WinNT)                                    │
 │Version: 1.0                                                                │
 │ Author: H D Moore                                                          │
 │    URL: http://www.metasploit.com/                                         │
 │                                                                            │
 │This exploits the chunked encoding bug found in Apache versions 1.2.x to    │
 │1.3.24. This particular module will only work reliably against versions     │
 └───────────────────────────────────────────────────────────────────────────↓┘
```

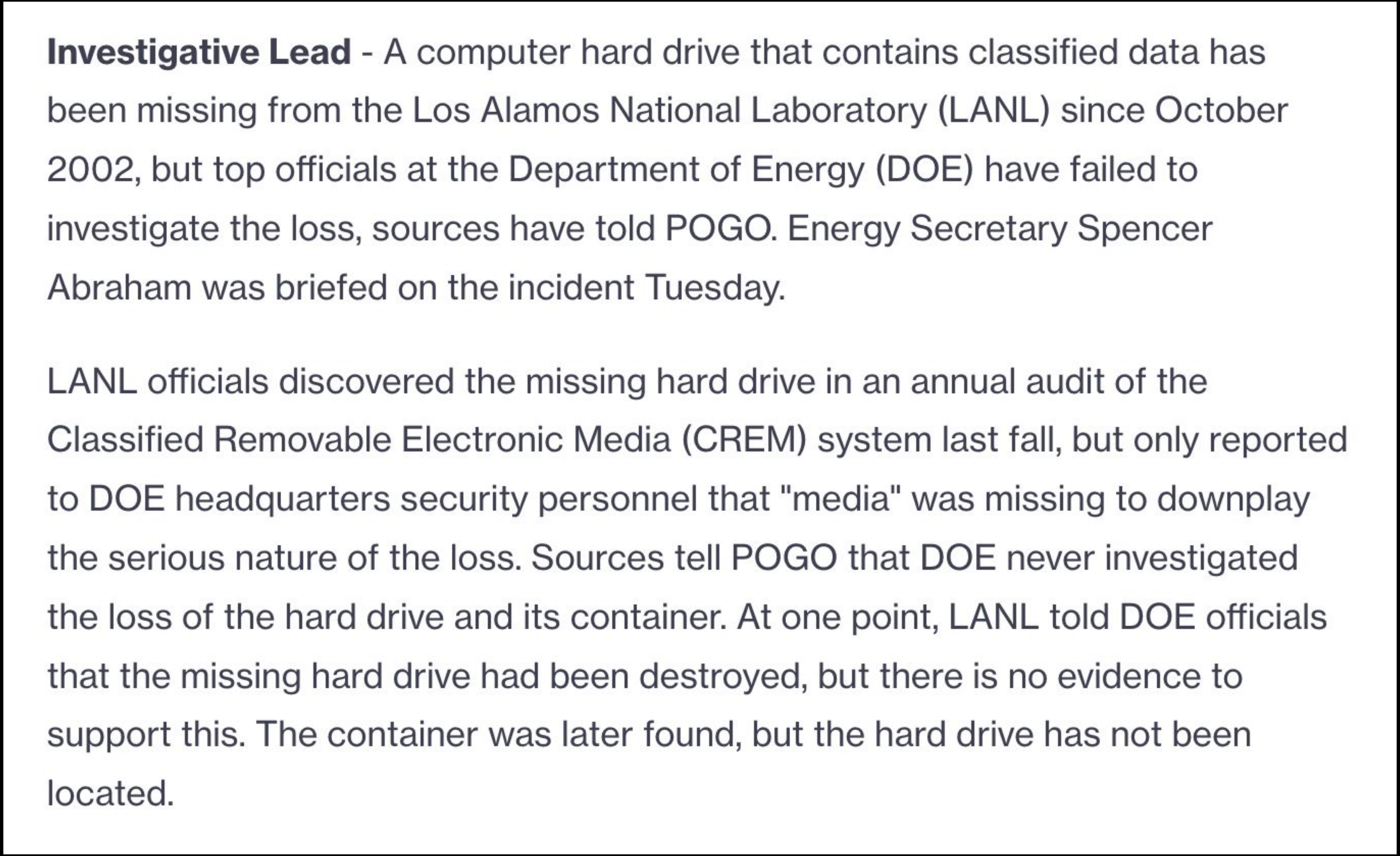
Metasploit 2 Got Better

Team became 3 with the addition of “skape”

Widely ridiculed by the security scene

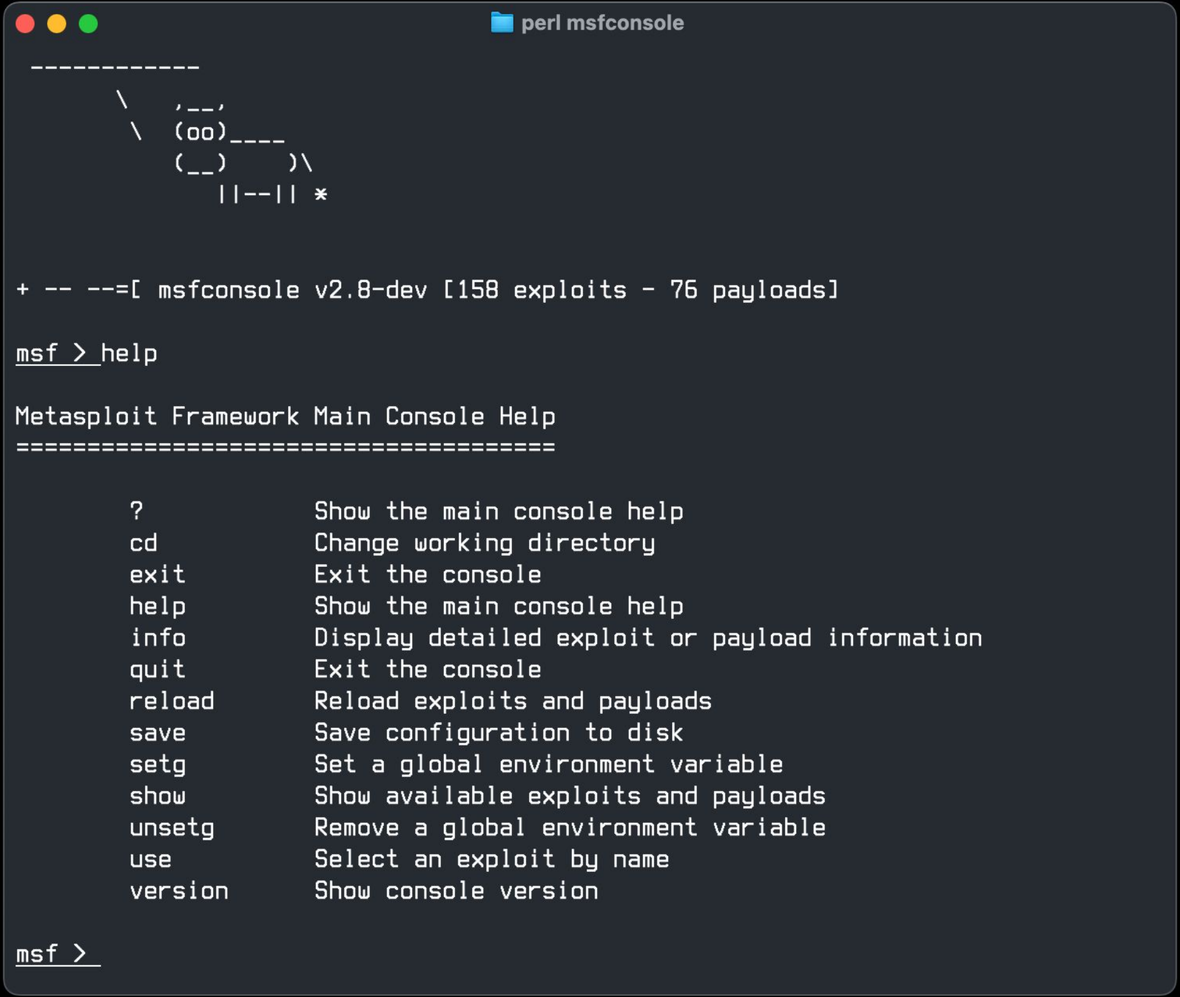
Meterpreter, VNC, IDS & AV evasion

Good enough to be stolen



Investigative Lead - A computer hard drive that contains classified data has been missing from the Los Alamos National Laboratory (LANL) since October 2002, but top officials at the Department of Energy (DOE) have failed to investigate the loss, sources have told POGO. Energy Secretary Spencer Abraham was briefed on the incident Tuesday.

LANL officials discovered the missing hard drive in an annual audit of the Classified Removable Electronic Media (CREM) system last fall, but only reported to DOE headquarters security personnel that "media" was missing to downplay the serious nature of the loss. Sources tell POGO that DOE never investigated the loss of the hard drive and its container. At one point, LANL told DOE officials that the missing hard drive had been destroyed, but there is no evidence to support this. The container was later found, but the hard drive has not been located.



```
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


+ -- --=[ msfconsole v2.8-dev [158 exploits - 76 payloads]

msf > help

Metasploit Framework Main Console Help
======================================

        ?               Show the main console help
        cd              Change working directory
        exit            Exit the console
        help            Show the main console help
        info            Display detailed exploit or payload information
        quit            Exit the console
        reload          Reload exploits and payloads
        save            Save configuration to disk
        setg            Set a global environment variable
        show            Show available exploits and payloads
        unsetg          Remove a global environment variable
        use             Select an exploit by name
        version         Show console version

msf > 
```

Metasploit 3 Hit Critical Mass

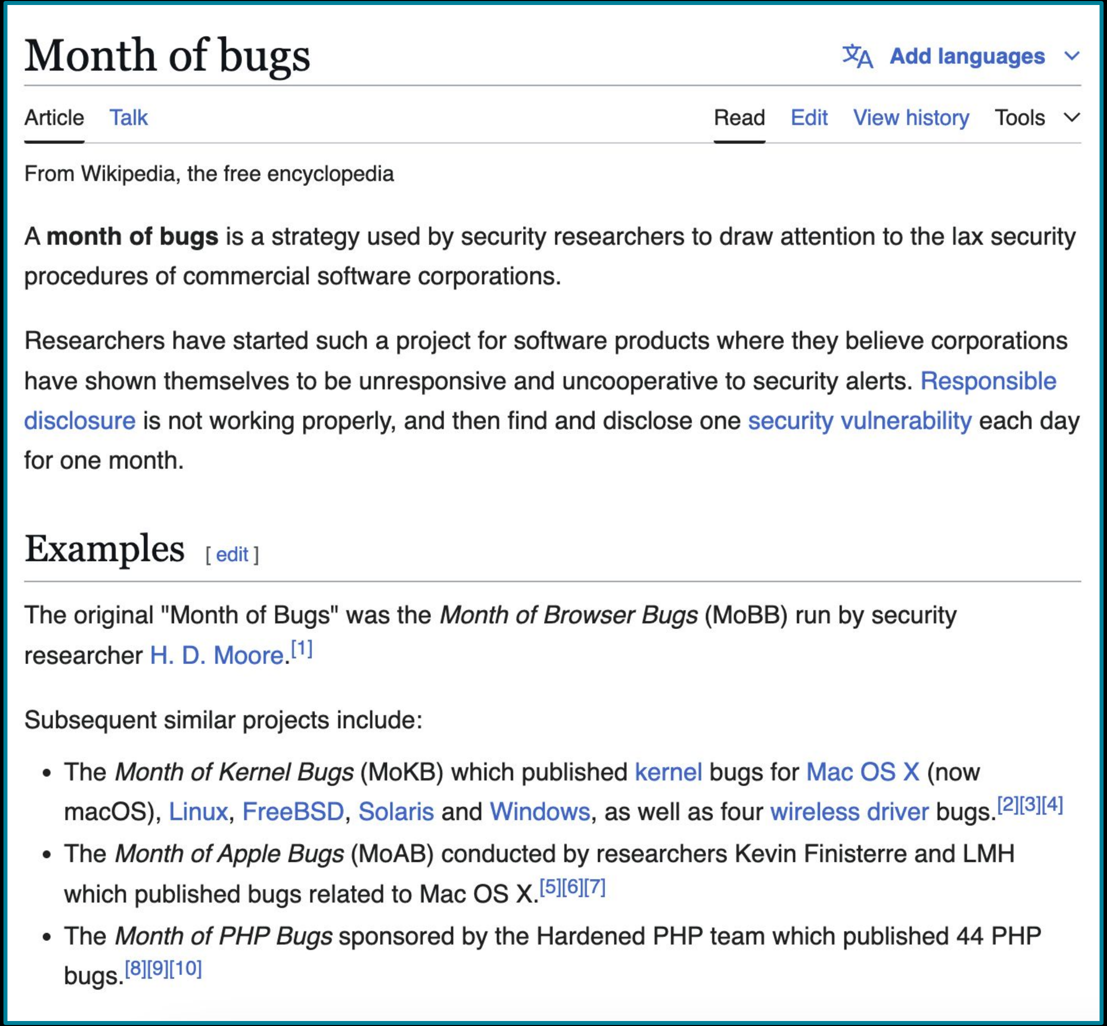
Grew to a half-dozen active developers

Completed a rewrite from Perl to Ruby

Hundreds of contributors over time

Many research side projects

Conferences & training



Month of bugs

From Wikipedia, the free encyclopedia

A **month of bugs** is a strategy used by security researchers to draw attention to the lax security procedures of commercial software corporations.

Researchers have started such a project for software products where they believe corporations have shown themselves to be unresponsive and uncooperative to security alerts. Responsible disclosure is not working properly, and then find and disclose one security vulnerability each day for one month.

Examples [edit]

The original "Month of Bugs" was the *Month of Browser Bugs* (MoBB) run by security researcher H. D. Moore.[1]

Subsequent similar projects include:

- The *Month of Kernel Bugs* (MoKB) which published kernel bugs for Mac OS X (now macOS), Linux, FreeBSD, Solaris and Windows, as well as four wireless driver bugs.[2][3][4]
- The *Month of Apple Bugs* (MoAB) conducted by researchers Kevin Finisterre and LMH which published bugs related to Mac OS X.[5][6][7]
- The *Month of PHP Bugs* sponsored by the Hardened PHP team which published 44 PHP bugs.[8][9][10]

Metasploit Track at DEFCON 17

Rapid7 Acquires Metasploit

I join Rapid7, bring on egyp7, we hire a team

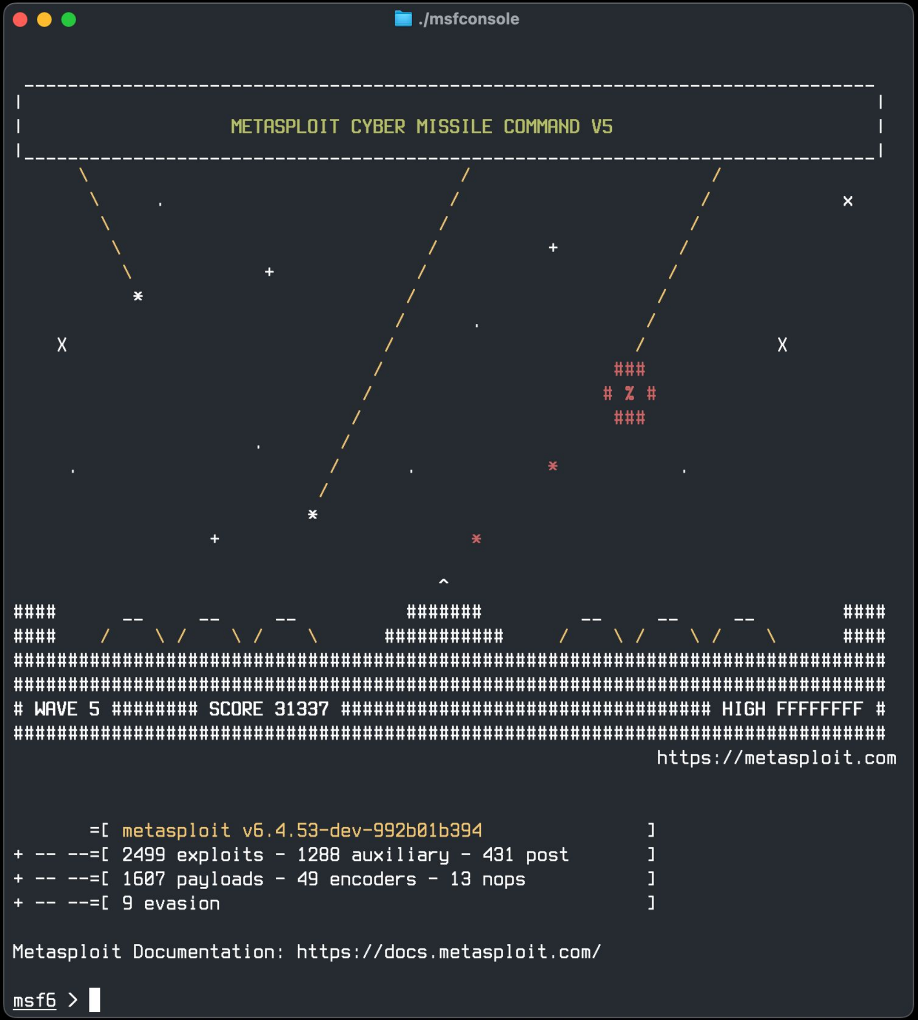
Expand OSS & launch commercial product

Incredibly busy, but mostly succeeds

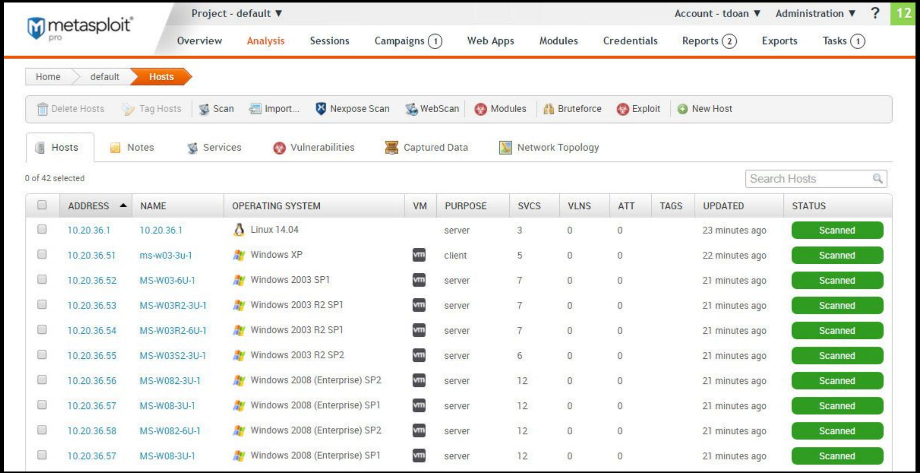
Merge into Rapid7 engineering in 2013

I officially left the project in 2017

* See BHDC 2010 “Metasploit and Money” for details and lessons learned.

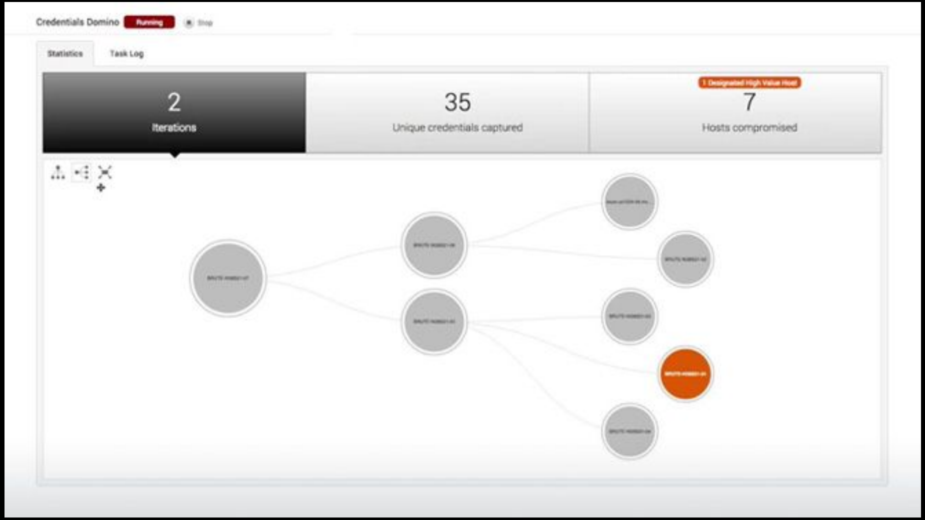


```
 -----------------------------------------------------------------------------
|                                                                             |
|                      METASPLOIT CYBER MISSILE COMMAND V5                    |
|_____________________________________________________________________________|

####      __     __     __          #######          __     __     __        ####
####    /    \ /    \ /    \      ###########      /    \ /    \ /    \      ####
#################################################################################
#################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
#################################################################################
                                                           https://metasploit.com


       =[ metasploit v6.4.53-dev-992b01b394                ]
+ -- --=[ 2499 exploits - 1288 auxiliary - 431 post       ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                        ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```



0 of 42 selected

	ADDRESS	NAME	OPERATING SYSTEM	VM	PURPOSE	SVCS	VLNS	ATT	TAGS	UPDATED	STATUS
☐	10.20.36.1	10.20.36.1	Linux 14.04		server	3	0	0		23 minutes ago	Scanned
☐	10.20.36.51	ms-w03-3u-1	Windows XP	vm	client	5	0	0		22 minutes ago	Scanned
☐	10.20.36.52	MS-W03-6U-1	Windows 2003 SP1	vm	server	7	0	0		21 minutes ago	Scanned
☐	10.20.36.53	MS-W03R2-3U-1	Windows 2003 R2 SP1	vm	server	7	0	0		21 minutes ago	Scanned
☐	10.20.36.54	MS-W03R2-6U-1	Windows 2003 R2 SP1	vm	server	7	0	0		21 minutes ago	Scanned
☐	10.20.36.55	MS-W03S2-3U-1	Windows 2003 R2 SP2	vm	server	6	0	0		21 minutes ago	Scanned
☐	10.20.36.56	MS-W082-3U-1	Windows 2008 (Enterprise) SP2	vm	server	12	0	0		21 minutes ago	Scanned
☐	10.20.36.57	MS-W08-3U-1	Windows 2008 (Enterprise) SP1	vm	server	12	0	0		21 minutes ago	Scanned
☐	10.20.36.58	MS-W082-6U-1	Windows 2008 (Enterprise) SP2	vm	server	12	0	0		21 minutes ago	Scanned
☐	10.20.36.57	MS-W08-3U-1	Windows 2008 (Enterprise) SP1	vm	server	12	0	0		21 minutes ago	Scanned



Rapid7's Continued Improvements

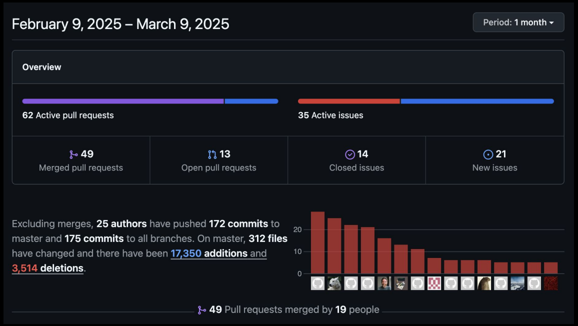
Thriving community and frequent updates

Great per-module docs (+ AttackerKB)

Multi-language modules (Python!)

Modules with hardware interfaces

Big thanks to Caitlin Condon!



February 9, 2025 – March 9, 2025

Period: 1 month

Overview

62 Active pull requests

35 Active issues

49	**13**	**14**	**21**
Merged pull requests	Open pull requests	Closed issues	New issues

Excluding merges, **25 authors** have pushed **172 commits** to master and **175 commits** to all branches. On master, **312 files** have changed and there have been **17,350 additions** and **3,514 deletions**.

49 Pull requests merged by **19** people

Metasploit is 23 Years Old

Nmap is 28, Kismet is 23, ZAP is 20

What made these successful?

Why are these still around?

* ZAP was forked from Paros Proxy 3.2.12

Key Traits

Deep focus on a technically difficult problem

Friendly path for community contributions

Clear boundaries on project scope

Extensive documentation

Consistent leadership

Create

Preamble

It’s your project and only your opinion matters

It’s 100% OK to retire a project, no guilt!

The goal is to learn things and have fun

Mistakes are mostly* fixable

1. Choose a Name

Two great options

<Your Org> [Non-Unique Name]	[Unique Name]
“Garth’s VPN Scanner”	“VeepScan”

Check for conflicts

Domains	Socials	Packages	Trademarks	Offensive Terms

2. Choose a License

Two safe options

MIT / BSD / Apache	Source Available
Permissive and safe to relicense	Technically not "Open Source"
Simple community engagement	Difficult community engagement
Many free packaging options	Trickier to support packaging
No abuse protection	Still safer than using GPL variants

Why Avoid GPL Variants?

GPL can prevent *you* from relicensing later

Commercially toxic for embedding

Limited abuse protection

3. Pick a Forge

Choose a service provider or self-host

Practically, just use GitHub

Otherwise mirror to it

4. Issues and Contributions

Setup a bug tracker, create templates

Document how to contribute code

Set expectations for response

Disable other forge features

5. Discussion and Support

Publish some form of contact information

Document your security policy

Direct folks to a shared forum

Publish a Code of Conduct

Read your messages

6. Security Best Practices

Leverage CI/Forges for security monitoring

- Dependency tracking and updates
- Security source scanning
- Secret scanning

OpenSSF is a great resource

- https://openssf.org/technical-initiatives/developer-best-practices/
- https://www.bestpractices.dev/en/criteria/0

Grow

Growing Your Project

Marketing time! Get users! Promote!

Style and polish matter! Excite folks!

Conference talks? ahem

Reduce Friction For Users

A one-liner is best, cloud demo even better

Leverage packaging frameworks

Show a fast time-to-value

Reduce Friction For Contributors

Public CoC, create issue and PR templates

Write up “easy” issues for first-timers

Create modules, scripts, or plugins

Simplify documentation updates

Give The Community a Space

Mailing lists, forums, slacks, and discords

Preferably something searchable

Encourage questions!

Run surveys!

Make Your Community Look Good

Give credit generously, showcase contributors

Highlight interesting use cases

Write up case studies

Track usage stats

Tell The World Your Plans

State your goals and publish a roadmap

Provides a compass for decisions

Document what you won’t do

Shininess in 2025

The minimum bar for pretty has been raised

Lots of tools help, but they require effort

Want to succeed? Polish!

It still feels silly

Look For Helpers

Deputize friendly folks who can help the project

Invite them to help respond to the community

Limit their access, keep an eye out for abuse

Help them out in return

Challenges

Back Of The House

Register a business entity for the project

Assign © and domains to the entity

Register trademarks to the entity

$500 – $1500 (!)

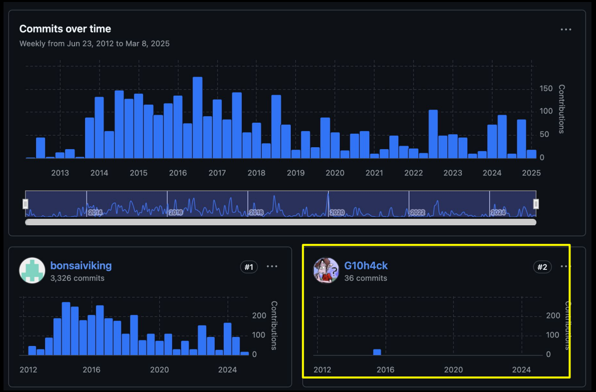
Hard Truths

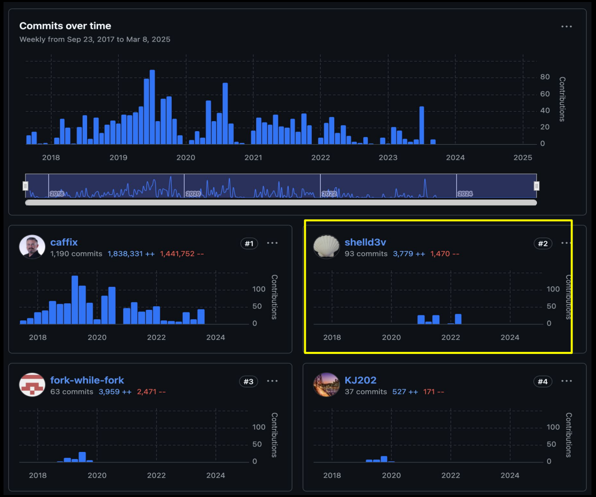
Nobody will care more than you

Code won’t make you money

You’re likely the owner for life

It will likely die without you




Commits over time
Weekly from Sep 23, 2017 to Mar 8, 2025
Contributions
caffix
1,190 commits 1,838,331 ++ 1,441,752 --
#1
shelld3v
93 commits 3,779 ++ 1,470 --
#2
fork-while-fork
63 commits 3,959 ++ 2,471 --
#3
KJ202
37 commits 527 ++ 171 --
#4

Conflicts

Give folks the benefit of the doubt, once

Trolls always exist, you can’t fix them

You also don’t owe them anything

Consider limiting interactions

- Offer commercial support contracts
- Disable issues, use email

Workload

A full–time job jammed into your spare time

Feels a lot like commercial product work

Folks often bring up “sustainability”

OSS runs on free time and fumes

Commercialization

Making money from OSS is counter-intuitive

OSS maintenance conflicts with paid work

Nothing you already do helps

What to do instead?

Difficult Commercial Models

Relicensing (*GPL, SSPL) and charging businesses

Paid feature development

Corporate sponsorship

Acquisition

Better Commercial Models

Support contracts with a monthly retainer

Offering a hosted turnkey solution

Build a separate product

Afterlives

Document a “living will” for your project

Decide on archiving vs handing off

Define a forking policy (need ™)

Defense

Transfer to a company that depends on the code

Transfer to a bigger project or foundation

Consider archiving it instead

Avoid getting “Jia Tan”ed

Introducing excrypto & SSHamble

Go: excrypto & sshamble

TLS is part of the stdlib (Go 1.24.1, etc)

SSH is part of the x/crypto stdlib

Great code, but not super flexible

Challenging for security uses

sshamble

A customized version of x/crypto/ssh

Designed for deep protocol tweaks

Also a CLI for auditing SSH

Drops lots of shells!

excrypto

A fork + tweaks to zcrypto (a fork of stdlib)

Speaks SSL 3.0 and TLS 1.3 (+PQC)

Co-resides with stdlib and FIPS

Lenient certificate parsing

Create

Name:	excrypto (lib) & sshamble (lib/cli)
License:	BSD (2–clause)
Code/Forge:	GitHub.com/runZeroInc/excrypto GitHub.com/runZeroInc/sshamble
Bugs/Contribs:	Issues and Pull Requests
Discussion/Support:	GopherSlack #excrypto & #sshamble
Security:	GitHub (Dependabot, Secret Scanner, Security Policy) golangci-lint + gosec + govet

Grow

Launch:	sshamble launched at BH/DC 2024 excrypto at BSidesSF 2025
Branding:	Logo and domain (sshamble.com)
Deploy:	go install github.com/runZeroInc/sshamble@latest go get github.com/runZeroInc/excrypto@latest

Roadmap

Introduce excrypto into other OSS projects

Align maintenance with corporate interests

Package sshamble into popular distros

Document internal maintenance tasks

Automate as much as possible

- A research tool for SSH implementations
- Interesting attacks against authentication
- Post-session authentication attacks
- Pre-authentication state transitions
- Post-session enumeration
- Easy timing analysis

https://SSHamble.com

Built-in checks

bypass	auth=none	skip=auth	auth=success
	method=null	method=empty	skip=pubkey-any
publickey	pubkey-any	pubkey-any-half	user-key
	half-auth-limit	pubkey-hunt	—
password	pass-any	pass-empty	pass-null
	pass-user	pass-change-empty	pass-change-null
keyboard	kbd-any	kbd-empty	kbd-null
	kbd-user	—	—
gss-api	gss-any	—	—
userenum	timing-none	timing-pass	timing-pubkey
vulns	vuln-tcp-forward	vuln-generic-env	vuln-softserve-env
	vuln-gogs-env	vuln-ruckus-password-escape	—

Getting started

```
Start a network scan
$ sshamble scan -o results.json 192.168.0.0/24

Analyze the results
$ sshamble analyze -o output results.json

Specify ports, usernames, passwords, public keys, private keys, and
more
$ sshamble scan -o results.json 192.168.0.0/24 \
     --users root,admin,4DGift,jenkins \
     --password-file copilot.txt \
    -p 22,2222 \
     --pubkey-hunt-file admin-keys.pub \

Open an interactive shell for sessions
$ sshamble scan -o results.json 192.168.0.0/24 \
     --interact first --interact-auto pty,env LD_DEBUG=all,shell
```

The interactive shell

```
Enter the sshamble shell with `^E`. Commands:

    exit                     - Exit the session (aliases 'quit' or '.')
    help                     - Show this help text (alias '?')
    env      a=1 b=2         - Set the specified environment variables (-w for wait
mode)
    pty                      - Request a pty on the remote session (-w for wait mode)
    shell                    - Request the default shell on the session
    exec     cmd arg1 arg2   - Request non-interactive command on the session
    signal   sig1 sig2       - Send one or more signals to the subprocess
    tcp      host port       - Make a test connection to a TCP host & port
    unix     path            - Make a test connection to a Unix stream socket
    break    milliseconds    - Send a 'break' request to the service
    req      cmd arg1 arg2   - Send a custom SSH request to the service
    sub      subsystem       - Request a specific subsystem
    send     string          - Send string to the session
    sendb    string          - Send string to the session one byte at a time

sshamble>
```

Recent updates

- Release binaries are now available from GitHub
- Experimental BadKeys.info support in ***analyze***
- Container support (thank you Rial Sloan II!)
- Various small bug fixes & improvements

https://SSHamble.com

Building SSHamble: Library

- SSHamble forks ***x/crypto/ssh*** as an internal package in a weirdly specific way
- Extend existing structs with separate files versus edits
- Wrap and export internal structs and functions
- Some code duplication, but minimal diffs
- Much easier maintenance!

```bash
#!/bin/bash
rm -rf crypto.upstream/ && \
git clone https://github.com/golang/crypto.git crypto.upstream/ && \
LC_ALL=C find ./crypto.upstream/ -type f -exec sed -i '' -e
's@golang.org/x/crypto@github.com/runZeroInc/sshamble/crypto@g' {} \; && \
rm -f ./crypto.upstream/go.mod ./crypto.upstream/go.sum && \
rm -rf crypto.upstream/.git/ && \
rm -rf crypto/ && \
mv crypto.upstream/ crypto/ && \
patch -p0 < crypto.patch
```

Building SSHamble: Client

- The ***x/crypto/ssh*** client provides very little protocol control
- ssh.Dial() does everything in one step
  - Connect, version exchange, key exchange, secure transport, auth!
  - `ssh.Dial("tcp", "host:22", config)`
- Reimplement the client into individual steps with full control
- Provide a config that indicates stopping points & callbacks
- Handle deadlocks through forced socket closes
- Result is a very odd authentication function
  - https://github.com/runZeroInc/sshamble/blob/main/auth/auth.go#L44

Building SSHamble: Gotchas

- → SSH shell Stdin / Stdout / Stderr doesn't work like you would expect
  - Some servers drain input from Stdin before the process starts
  - The remote shell doesn't see your input
  - Send one byte at a time, like a human, or sleep (!)

- → Raw mode terminals (for --interact mode) are a nightmare
  - Concurrency and raw mode TTY is tricky
  - Requires a singleton/global stdio manager
  - Logging has to switch to \r\n from \n for raw
  - Signal handlers break, easy to get stuck
  - https://github.com/runZeroInc/sshamble/blob/main/cmd/interact.go#L85

Thank You!

hdm@runZero.com