

Metasploit Minus Metasploit

Building APIs and abstractions for the future

Adam Cammack and James Barnett

Who We Are

- Engineers on the Metasploit team
- Made possible by our awesome community

Top Contributors

[View All Contributors >](#)

LAST 12 MONTHS 



msf5 > banner

```
. :ok000kdc'                'cdk000ko: .  
.x0000000000000000c        c000000000000000x .  
:0000000000000000k,      ,k00000000000000000:  
'000000000k000000: :00000000000000000000'  
o00000000.MMMM.o0000o0000l.MMMM,00000000o  
d00000000.MMMMMM.c00000c.MMMMMM,00000000x  
l00000000.MMMMMMMMM;d;MMMMMMMMM,00000000l  
.00000000.MMM.;MMMMMMMMMMMM;MMM,00000000.  
c0000000.MMM.OOc.MMMMM'o00.MMM,0000000c  
o000000.MMM.0000.MMM:0000.MMM,000000o  
l00000.MMM.0000.MMM:0000.MMM,00000l  
;0000'MMM.0000.MMM:0000.MMM;0000;  
.d00o'WM.0000occcx0000.MX'x00d.  
,k0l'M.00000000000000.M'd0k,  
:kk;.00000000000000.;Ok:  
;k0000000000000000k:  
,x00000000000000x,  
.l0000000l.  
,d0d,  
.
```

msf5 > banner

```
      . :ok000kdc'          'cdk000ko: .  
      .x0000 0000000c      c00  0000000x .  
      :000          00000k, ,k00000  000000:  
'000000          00000: :00          00'  
o0000          0o00          000000o  
d0000          00x  
100000000.          000001  
.00          00.  
c0          .00c. MMM          000c  
o000000. .0000.MMM:000          0 000o  
100000.MMM.00  MMM:0000.MMM  0001  
;0000'MMM          MMM:0000.MMM;0000;  
.d00o'WM          cccx0000.MX'x00d.  
      ,k0l          M.d0k,  
      :k          00000.c0k:  
      ;k0000          :  
      ,x000          ,  
      .100          .  
      ,d0d,  
      .
```

msf5 > banner

```
      . :ok000kdc'          'cdk000ko: .  
      .x000000000000000c      c00000000000000x .  
      :0000000000000000k,      ,k00000000000000000:  
'0000000000kkk00000: :00000000000000000000'  
o00000000.      .o0000o0000l.      ,00000000o  
d00000000.      .c00000c.      ,00000000x  
l00000000.      ;d;      ,00000000l  
.00000000.      .;      ;      ,00000000.  
c00000000.      .00c.      'o00.      ,0000000c  
o0000000.      .0000.      :0000.      ,000000o  
l000000.      .0000.      :0000.      ,00000l  
;0000'      .0000.      :0000.      ;0000;  
.d00o      .0000occcX0000.      x00d.  
      ,k0l      .000000000000000.      .d0k,  
      :kk; .000000000000000.c0k:  
      ;k0000000000000000k:  
      ,x0000000000000x,  
      .l0000000l.  
      ,d0d,  
      .
```

Be Flexible

Handle ALL the Cases

- Different types of tasks
 - Scanning
 - Exploiting
 - Post-exploit gathering
- Network traffic should be re-routable
- Exploit traffic should be malleable
- Payloads should support transformations

Separate Modules and Payloads

- Modules should only know enough to trigger the exploit
- Maintain a wide library of payloads
- C2 for a wide library of payloads
- Large number of module/payload combinations

Current Architecture

Everything Touches the DB

- Very Rails-oriented
- Tightly coupled to the database
- ONE MSF per database
- Searching and filtering haphazardly organized

Modules Are Plugins

- Read into memory, modified, and eval'd
- Loaded multiple times at startup
- Everything executes in the context of everything else
- Shared functionality via mixins
- And then there's the datastore...

Networking Is Complicated

- All listeners go through the switch board
- Pivoting through sessions and proxies
- Socket, service, and client abstractions
- Ring buffers for sessions

Isolating Modules

Modules as Processes

- Enhanced isolation
- Parallelism
- Support for any language



Modules as Processes



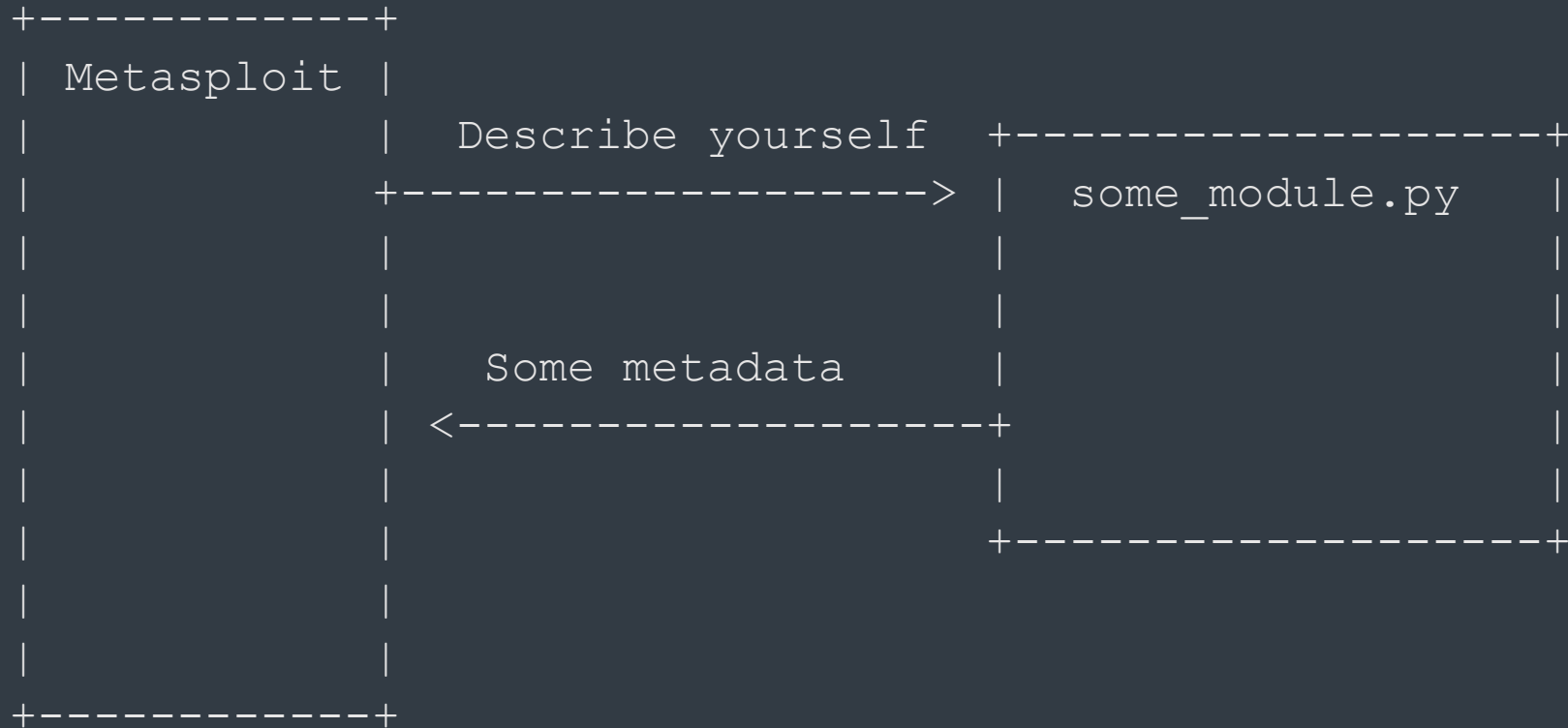
Full Isolation

- OS process per task
- Communicates via JSON over stdin/stdout
- Network transparency

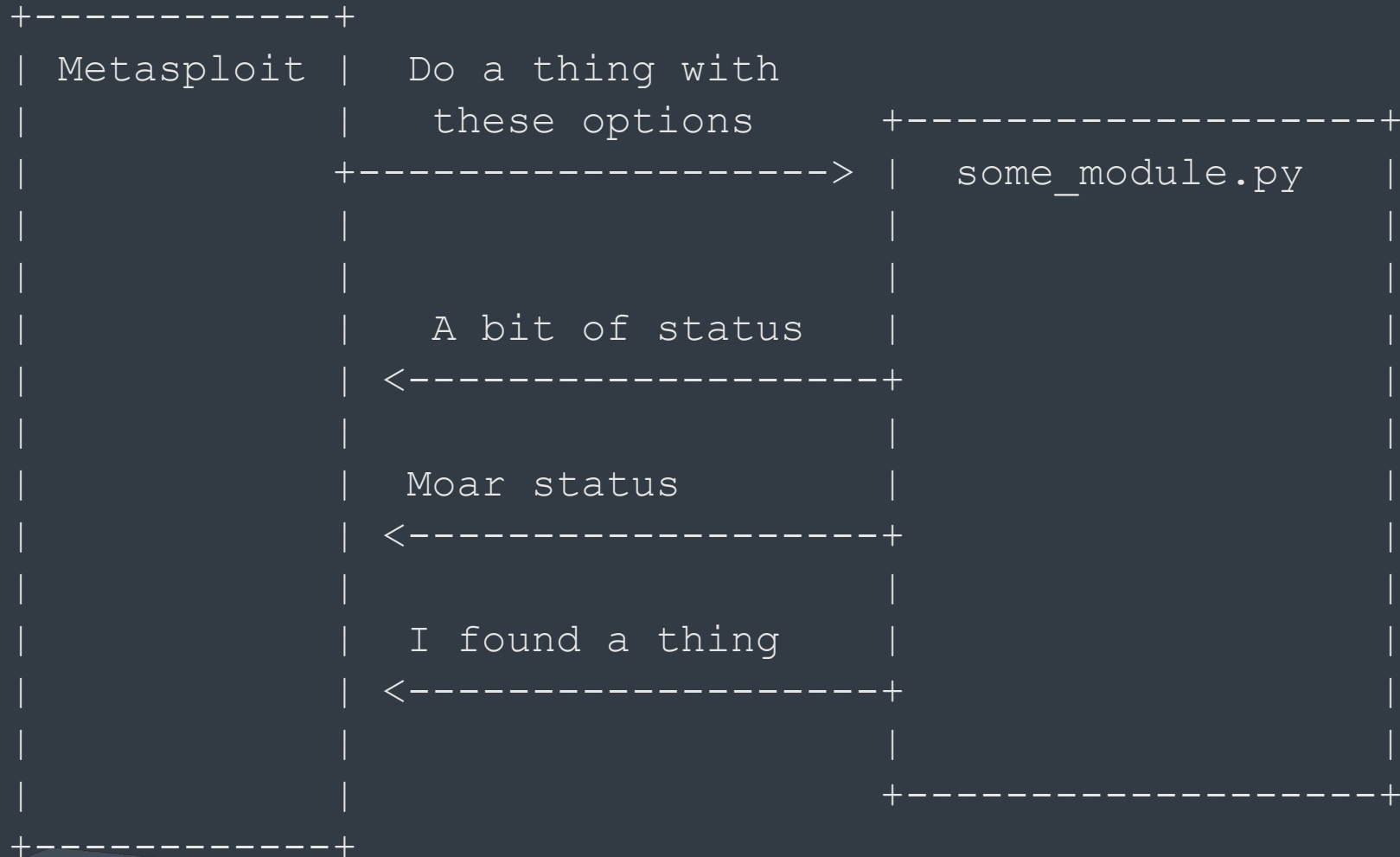
Better Performance

- Separate file descriptor pool
- Separate memory space
- No GIL - separate
- Horizontal scaling

How it Works



How it Works



Isolating Data Storage

Objectives of Project Goliath

- Make the Metasploit datastore portable
- Improve the data model
- Make sessions shareable

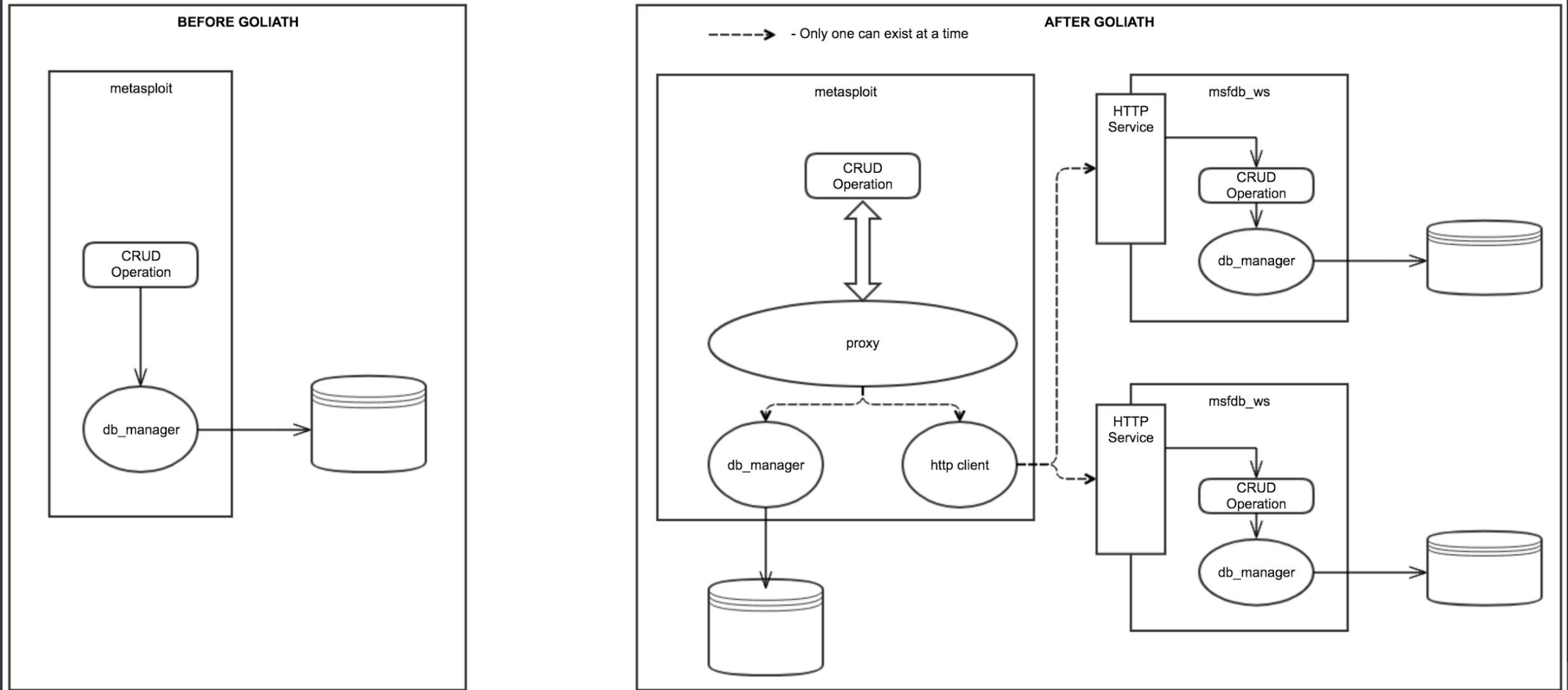


Datastore As a Service

- Collaborate with others
- Host data store anywhere
- Integrate with other tools

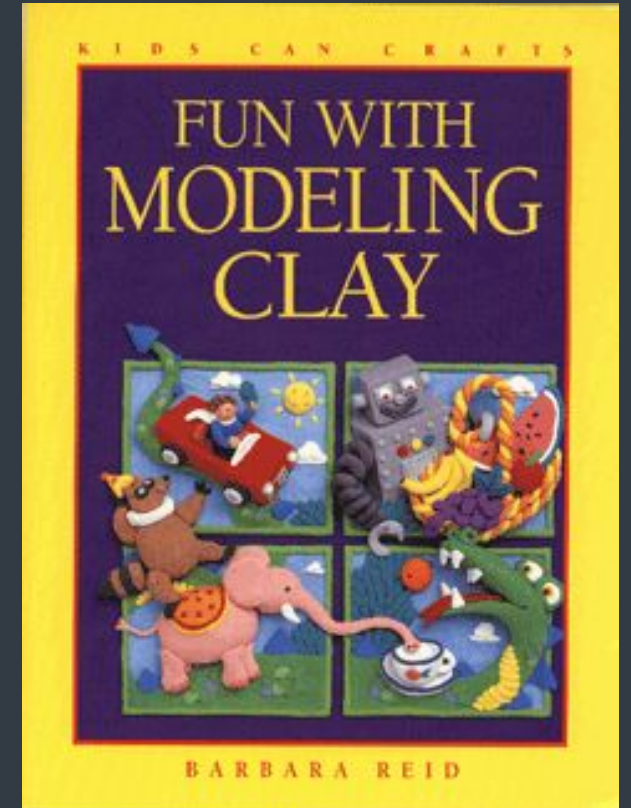


Architecture



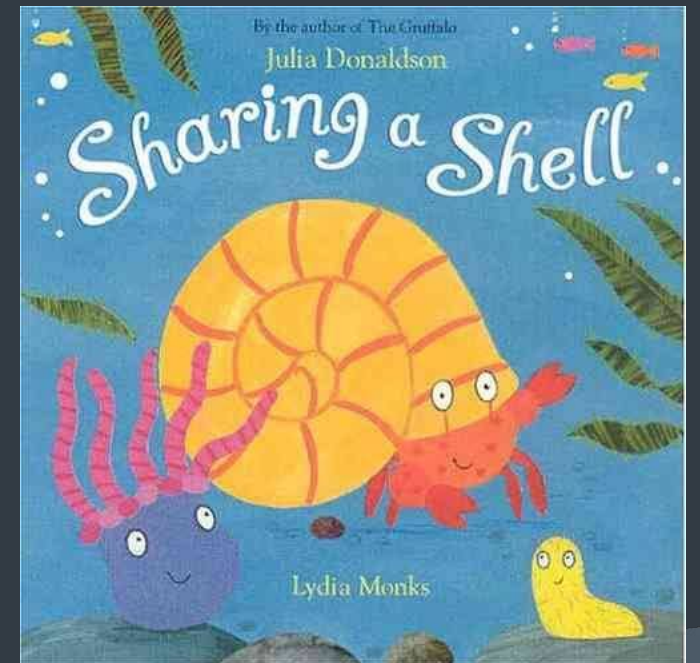
Data Model Improvements

- Flexibility
- Searchability
- Re-usability



Session Sharing

- Separate session management from framework
- Share sessions among team members
- Host session manager in the cloud



Demo



Questions?

<https://blog.rapid7.com/2017/12/28/regifting-python-in-metasploit/>

<https://www.metasploit.com>

<https://github.com/rapid7/metasploit-framework>

<http://garfieldminusgarfield.net>