

Tekeli-li

The Great Deep Project

Team Members

Michael Weatherby

Michael Fitch

Blake Janes

Eric Del Valle



Tasks Accomplished - Summer

- Each team member:
 - Wrote a personal fuzzer plugin
 - Wrote a personal pwnme plugin
 - Created a .qcow2 (qemu OS image) and installed the OS
- Made a 'getting started' guide for:
 - Creating & installing .qcow2 files
 - Coding and running plugins

Tasks Accomplished

- Created modified OS handler designed to work on a linux VM with Untangle NG Firewall
- Created a Coverage Guided Fuzzer plugin in python for an existing target packaged with shoggoth-extras
- Expanded on plugin documentation

CGF

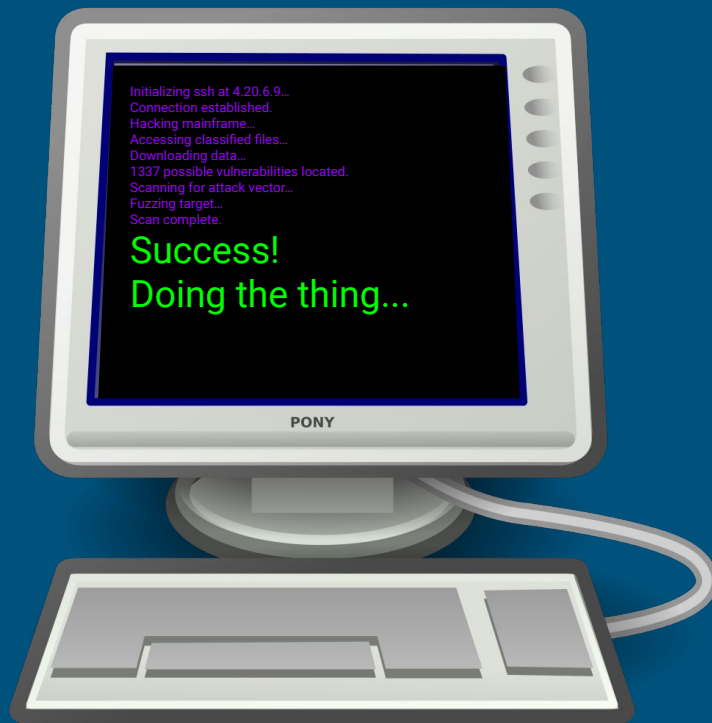
Snapshot of python CGF
running on the target packaged
with shoggoth-extras.

```
shogfresh@ubuntu: ~/shoggoth-extras
File Edit View Search Terminal Help
73 b7 9a 1e bc 86 ad 0b 33 54 c9 63 9e 88 50 a5 3f fa 5e 0d 26 df 82 f4 b2 14 6b be
af d8 d7 f1
Coverage is: Scale 8626
244228 311603 417680 574194 364782 358676 568401 482093 230932 374217 290565 211517
201419 69920 131201 128650 307251 99155 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Stale path count: 27
Fuzz Job: 29043
Starting Job 29106
b9 d3 25 50 5e d4 cb c5 e1 72 75 71 b4 9e ab 28 7a 23 d8 30 c3 85 b3 02 8f 33 44 79
de f9 d4 52 86 70 10 8c b6 d9 ac be 96 e8 dc a1 c4 ee 76 90 80 a1 ea 27 b0 c4 5e e9
20 21 a1 be 50 2a 3b 25 69 1e 01 11 df 1a e0 3f 25 bf 9c 15 81 2d df 41 3e c5 03 34
9b bd cf 58 d8 3f 7f 4e fe 37 d9 5e 99 52 60 db bd 97 06 ec 42 6b 01 0b ca 0f a4 c3
89 bb e1 dd 06 09 7e 1d 4e cd 66 27 1f 73 5f 64 fc 15 2a e9 82 86 1e a8 09 e2 58 c2
1f 50 d7 d4 ac 20 d2 45 d3 a8 ee a5 42 ec 5a 5c 7e a5 d2 0f ce 25 fc 3a c2 03 d8 f8
f5 49 fd 6b 63 bd d7 c1 8c 0a c4 a4 3b 7c d2 bb b4 33 eb 74 95 23 d4 62 e0 07 d4 98
cf b2 d7 e6 37 98 97 d2 22 63 b3 ab 23 ee 37 19 f3 07 e9 25 92 fe e5 78 ef 88 a6 8c
8e 1b 23 47 91 0d b3 8d 6f b9 3b 35 c4 86 7b 5d 59 c5 27 0b ed 29 2e af 69 39 82 02
5f 34 32 d9
Coverage is: Scale 8626
244849 312476 418972 575705 365429 359240 569388 483002 231426 374892 291158 212045
201788 70043 131473 128890 307851 99355 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Stale path count: 12
Fuzz Job: 29106

user@debian:~$ ls
doit.txt  exec_me  exec_me.c  Makefile  pwnit.txt  pwnme_lots  pwnme_lots.c
user@debian:~$ cat doit.txt | ./pwnme_lots
src is at 7fffffff500

Please provide input between 0 and 256 characters...
Input: Please provide input between 0 and 256 characters...
```

Live Demo



Milestone 5 Goals

- Write fuzzers targeting several attack surfaces in Untangle
- Create guide for Coverage Guided Fuzzing
- Fix Linux OS Handler for kernel versions 4.x