

Tekeli-li

The Great Deep Project

Team Members

Michael Weatherby

Michael Fitch

Blake Janes

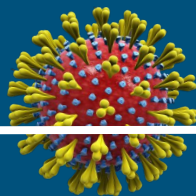
Eric Del Valle



Tasks Accomplished

- Build and Compile Shoggoth
- Begin adding to and re-working Shoggoth's documentation- internal documentation in particular is very messy
- Attempted to use Shoggoth's fuzzing tool with a simulated vulnerability.

That One *Little* Problem...



- Prevented in-person collaboration, which was our team's primary form of collaboration
- Delayed communication between team members and corporate client
- Slowed down progress

Shoggoth fuzzing

The image shows a Kali Linux virtual machine environment. At the top, there are several window tabs: 'Home', 'revm', 'Kali Linux 2020.1-vmware-a...x', 'lab9 - p3.py', 'QEMU', 'kali@kali: ~/Progr...', '[kali@kali: ~/Progr... String_Encrypt_E...', 'kali@kali: ~/Progr...', and 'Tekeli-li/shoggoth-... 08:44 PM'. The main window is a terminal titled 'kali@kali: ~/Downloads/lab9' with a sub-window 'kali@kali: ~/P...hoggoth-extras'. The terminal output shows a fuzzing job for 'p3.py' with the following details:
- Fuzzing job: 1261
- Starting job: 1324
- Input is: 19 6e aa bb 8b 43 3f 8f 8f 81 0d 7c 05 64 02 ee 1f 6a 39 5c 97 f2 97 57 62
- de 48 f6 53 ad a9 44 18 c0 39 72 f6 98 05 8a 8f 8a b5 dd 72 bc 76 d2 93 28 2a 53 64
- ab 21 5a b8 8d 9a 4f 88 63 9b 61 a0 a4 b0 ae 40 27 e6 31 04 43 d9 96 a1 83 d6 55 dc
- ae af 96 0d 03 3f ac 97 cb 7d af 99 27 5f 09 54 e5 c0 5e d6 36 65 de 63 c3 b6 e3
- Coverage is: scale is 8626
- 11290 14045 18650 26792 16345 16709 24558 19491 9242 14196 10798 7651 6770 2340 4025
- State path count: 20
- Fuzzing job: 1324
- Starting job: 1387
- Input is: ce b8 c0 73 75 87 32 7f 8e f3 0c e4 63 ae d4 69 65 3a 8e 4f ae 6b 87 d5 6c
- f8 12 70 de 71 24 ae 33 86 43 5e c1 1c 19 65 de 3f 84 76 d2 34 72 98 dc e6 60 49 8a
- 95 81 90 d3 69 ae 77 31 0c 9f 6f 3d fc 1f 06 35 b6 3a b6 47 7c 28 dc c4 9b 08 ef 80
- 2b fe 50 c2 aa 9f 5e 8c a5 35 25 83 89 e6 2d a1 42 e0 a9 1f c2 56 08 68 27 8f 47 88
- Coverage is: scale is 8626
- 11794 14612 19576 28209 17390 17497 25877 20409 9701 14961 11463 8101 7255 2519 4313
- State path count: 41
- Fuzzing job: 1387
- Starting job: 1450
- Input is: 28 1c b3 07 df 6d 94 50 f3 a1 95 b6 56 ad cd 7e 38 d1 f0 d5 43 6d c7 a8 e8
- 7f 7d 5f 47 7b 0b c6 d1 66 12 a5 f9 31 69 61 93 9b 90 9d b6 8c 6f 44 24 0b 87 7c 8d
- 33 fc 80 d5 fe f5 d9 94 06 6d c7 ce 8d 6a da d2 1a 6d 94 57 31 f2 6a a6 6a b4 13 78
- 7c 3e 84 b4 5b 85 c6 4b a0 45 cf 12 f6 45 ee 4e 26 7f ba 7f 50 65 c4 94 c4 76 21 6c
- Coverage is: scale is 8626
- 12298 15179 20322 29414 18451 18358 27298 21594 10360 15656 12028 8369 7417 2573 442
- State path count: 3
- Fuzzing job: 1450
- Starting job: 1513
- Input is: 1c 1b 97 d2 a4 ba 9d c0 7e c3 c7 9e 93 b3 b6 33 a1 08 2a c0 68 df 03 4d fe
- 39 ed a5 7a 02 e7 59 aa dd a4 86 74 f8 8c b5 72 25 c0 56 50 22 56 55 7e c6 3c ef
- f1 4a 95 e9 32 19 ac dd 10 94 2f 5c cd af 00 5c ae 68 26 9c 0f c7 a4 2d 2d b0 3c 5a
- 7d c7 7f 93 8d 43 a9 a5 b6 27 e9 c5 b6 f4 79 72 d2 97 6b c1 8f fb 4d 50 6c 69 c4 f2
- Coverage is: scale is 8626
- 12799 15737 21272 30796 19313 19198 28419 22341 10702 16404 12489 8666 7714 2672 464
- State path count: 1
- Fuzzing job: 1513
- Starting job: 1576
- Input is: 7f 4c 80 c7 cb 3a 5b c9 15 83 92 42 1d bc 4a 72 d1 b7 56 1a 9a dd 73 21 21
- d6 5f 82 6d 30 2d 4f 1f 95 60 7f cf 6f 35 23 be c8 e0 56 7c 35 81 b6 2b fd bc 4b 17
- 71 62 ef 06 b0 b0 bf bb 39 63 1e 40 3d 02 fc 42 e4 75 92 dd rd 3f 56 6c a9 d2 2d 00
- 0c 93 66 89 e8 00 03 7f 3d f2 a9 79 de 13 0b 37 27 6f bd 3b 51 cd b4 23 ca 80 e9 62
- Coverage is: scale is 8626
- 13303 16475 22197 32002 20093 19906 29762 23748 11395 17242 12969 9070 8074 2812 487
- State path count: 54
- Fuzzing job: 1576
The terminal also shows a list of discovered vulnerabilities, including 'doit.txt' [converted] IL, 47C written, user@debian: '\$ cat doit.txt', and 'doit.txt exec_me exec_me.c Makefile punlit.txt punme_lots punme_lots.c'. The user is prompted to provide input between 0 and 256 characters...

Shoggoth Debugging

```
File Actions Edit View Help
kali@kali: ~/Downloads/lab9  kali@kali: ~/P...hoggoth-extras  kali@kali: ~/P...hoggoth-extras

0xffffffffffb2a144c8: 90      nop
0xffffffffffb2a144c9: 90      nop
0xffffffffffb2a144ca: 90      nop
0xffffffffffb2a144cb: 90      nop
0xffffffffffb2a144cc: 90      nop
0xffffffffffb2a144cd: 90      nop
0xffffffffffb2a144ce: 90      nop
0xffffffffffb2a144cf: 90      nop
0xffffffffffb2a144d0: 66 66 0f 66 2e      pcmpgtd 0(%rsi), %xmm5
(qemu) info reg
unknown command: 'info reg'
(qemu) reg
unknown command: 'reg'
(qemu) info registers
RAX=ffffffffffb2a141e0 RBX=ffffffffffb3011500 RCX=0000000000000000 RDX=0000000000000000
RSI=0000000000000000 RDI=0000000000000000 RBP=0000000000000000 RSP=ffffffffffb3003ef0
R8 =0100000000000000 R9 =0000000000000000 R10=0000000000000000 R11=fffffa00cbfc19210
R12=ffffffffffb311e00 R13=0000000000000000 R14=0000000000000000 R15=ffffffffffb3011500
RIP=ffffffffffb2a144b2 RFL=00000246 [---Z-P---] CPL=00 II=00 A20=01 SM=00 HLT=01
ES =0000 0000000000000000 00000000 00000000
CS =0010 0000000000000000 00000000 00000000 00af9b00 DPL=00 CS64 [-RA]
SS =0018 0000000000000000 00000000 00000000 00c93000 DPL=00 DS [-WA]
DS =0000 0000000000000000 00000000 00000000
FS =0000 0000000000000000 00000000 00000000
GS =0000 0000000000000000 00000000 00000000
LDT=0000 0000000000000000 00000000 00000000 00002000 DPL=00 LDT
TR =0040 0000000000000000 00000000 00000000 00002087 00008900 DPL=00 TSS64-avl
GDT= 0000000000000000 00000000 00000000
IDT= 0000000000000000 00000000
CR0=00050033 CR2=0000555555758028 CR3=0000000000368bce00 CR4=00000060
DR0=0000000000000000 DR1=0000000000000000 DR2=0000000000000000 DR3=0000000000000000
DR6=0000000000000000 DR7=0000000000000000
EFER=0000000000000001
FCW=037f FSW=0000 [ST=0] FTW=00 MXCSR=00001f80
FPR0=0000000000000000 0000 FPR1=0000000000000000 0000
FPR2=0000000000000000 0000 FPR3=0000000000000000 0000
FPR4=0000000000000000 0000 FPR5=0000000000000000 0000
FPR6=0000000000000000 0000 FPR7=0000000000000000 0000
XMM00=00000000000000000000000000000000 XMM01=00000000000000000000000000000000
XMM02=00000000000000000000000000000000 XMM03=00000000000000000000000000000000
XMM04=00000000000000000000000000000000 XMM05=6374652f207472667065722d2d07374
XMM06=7261702d6e7572202626202f20646320 XMM07=28207c7c206a6f7263616e6172666962
XMM08=20000000200000000000000000000000 XMM09=ffff0000ffff00000000ffff00000000
XMM10=00000000000000000000000000000000 XMM11=00000000000000000000000000000000
XMM12=00000000000000000000000000000000 XMM13=00000000000000000000000000000000
XMM14=00000000000000000000000000000000 XMM15=00000000000000000000000000000000
(qemu)

kali@kali: ~/Programs/shoggoth-extras
Debian GNU/Linux 9 debian tty1
debian login: user
uPassword:
Login incorrect
debian login: user
Password:
Last login: Tue Jan 28 18:36:48 EST 2020 on tty1
Linux debian 4.9.0-7-amd64 #1 SMP Debian 4.9.110-3+deb9u2 (2018-08-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$ ls
exec_me  exec_me.c  Makefile  punint_lots.txt  punme_little  punme_little.c  punme_lots  punme_lots.c
user@debian:~$ ./exec_me
main() is at 555555554780
execbuf is at 7ffff7fe0000
Press any key to continue...
s
I returned!
user@debian:~$ ./exec_me
main() is at 555555554780
execbuf is at 7ffff7fe0000
Press any key to continue...
l
I returned!
user@debian:~$
user@debian:~$ ./exec_me
main() is at 555555554780
execbuf is at 7ffff7fe0000
Press any key to continue...
```

Next Steps

- Finish reworking roadmap: in general recent milestones have been given more time while milestones near the end have been compressed
- Continue adding to and reworking Shoggoth's messy documentation
- Use Shoggoth's fuzzing tool to locate a simulated vulnerability