CharmBUG Meeting

May 29th, 2019

Agenda

- CharmBUG News
- Upcoming BSD Events
- Upcoming CharmBUG Meetups
- Reverse Engineering with BSD

CharmBUG

- Founded: January 2016
  - CharmBUG Organization LLC – June 2018
- CharmBUG Sponsors:

DAEMON SECURITY

OnyxPoint

- CharmBUG Organizers:
  - Michael Shirk
  - Shawn Webb
  - Dylan Cochran
  - JT Pennington
  - Ash Gokhale

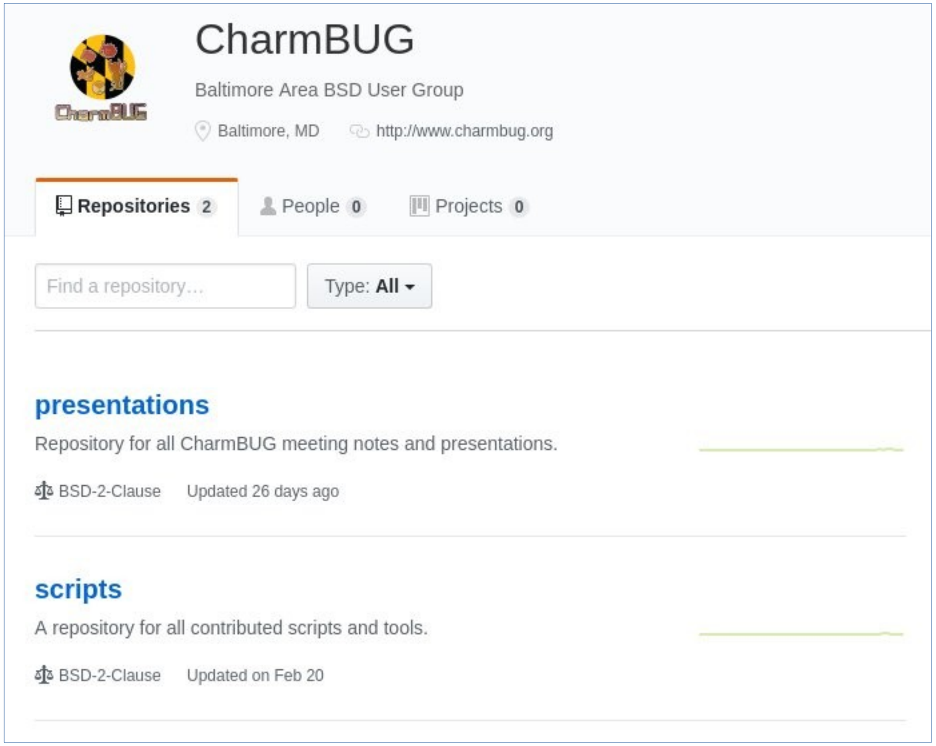
CharmBUG

- Now 70+ BUG members on meetup.com
- Communication for CharmBUG
  - IRC #CharmBUG on irc.freenode.net
  - meetup.com
  - Telegram
- Locations and Schedule
  - Last Week of the month at 7:30PM
    - Wednesday or Thursday
  - Rotating Casual and Formal CharmBUG Meetings
  - Formal meetings will be held at OnyxPoint
    - (See Meetup.com for schedule)
  - Baltimore Casual at Guinness Open Gate Brewery, SouthWest Casual at The Ale House of Columbia

CharmBUG

- CharmBUG Repo

  https://github.com/charmbug



CharmBUG

Baltimore Area BSD User Group

Baltimore, MD http://www.charmbug.org

presentations

Repository for all CharmBUG meeting notes and presentations.

BSD-2-Clause Updated 26 days ago

scripts

A repository for all contributed scripts and tools.

BSD-2-Clause Updated on Feb 20

CharmBUG

- Financial Information
  - Potential non-profit status
    - Researching currently
    - Hopefully an update after May 2019
    - No new status
- Scholarships
  - Two $500 dollar scholarships at Harford Community College
    - IT/Computer Science
    - Art

Upcoming BSD Events

- vBSDCon 2019
  - 9/7/2019 – 9/8/2019
  - Reston, Virginia
- EuroBSDCon 2019
  - 9/19/2019 – 9/22/2019
  - Lillehammer, Norway

Upcoming CharmBUG Meetups

- Casual BSD Meetup (SouthWest)
  - 6/27/2019 7:30PM
  - The Ale House of Columbia: Columbia, MD
- CharmBUG Meeting – Tentative Talk
  - 07/25/2019 7:30PM
  - Onyx Point: Hanover, MD

Tonight's Activity

- Reverse Engineering with BSD
  - Ghidra Port
    - Current Status
    - Remember GNU Radio?
  - What other tools do we have?
  - Ash’s binary EEPROM hacking with FreeBSD
    - And other fun...(we will get to this next time)

Thanks for coming.

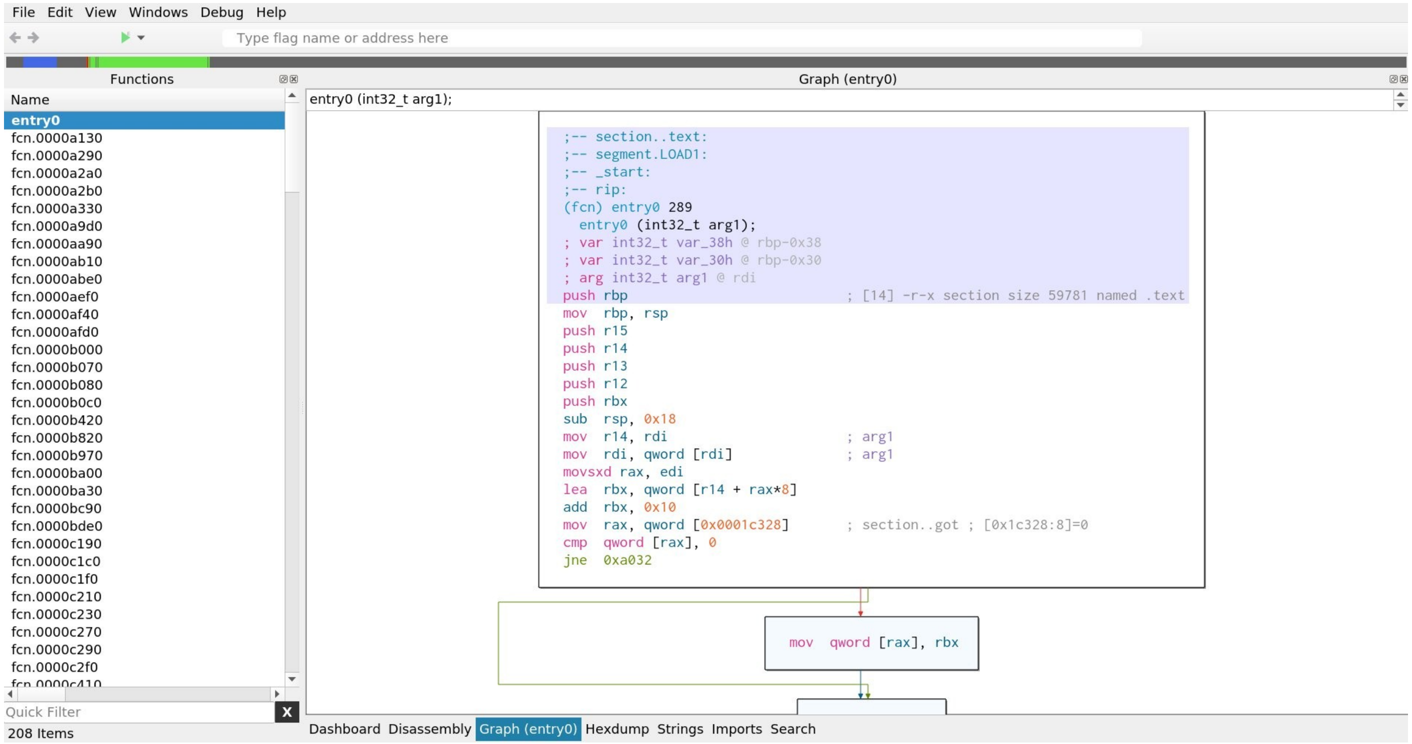
Reverse Engineering on BSD

- Started our informal discussion on what tools do we have available on BSD Operating Systems.
- Ghidra port:
  - Reverse Engineering Tool open-sourced by the NSA
  - Works on Windows/Linux/MacOSX

    https://bugs.freebsd.org/bugzilla/show_bug.cgi?id=237211
  - Port submitted and should at some point be a part of the FreeBSD Ports Tree

Reverse Engineering on BSD

- Radare2:
  - Tools to disasm, debug, analyze, and manipulate binary files
  - There is a GUI (radare-cutter) and it works on the CLI


File Edit View Windows Debug Help
Type flag name or address here
Functions
Graph (entry0)
Name
Quick Filter
208 Items
Dashboard Disassembly Graph (entry0) Hexdump Strings Imports Search

```
entry0
fcn.0000a130
fcn.0000a290
fcn.0000a2a0
fcn.0000a2b0
fcn.0000a330
fcn.0000a9d0
fcn.0000aa90
fcn.0000ab10
fcn.0000abe0
fcn.0000aef0
fcn.0000af40
fcn.0000afd0
fcn.0000b000
fcn.0000b070
fcn.0000b080
fcn.0000b0c0
fcn.0000b420
fcn.0000b820
fcn.0000b970
fcn.0000ba00
fcn.0000ba30
fcn.0000bc90
fcn.0000bde0
fcn.0000c190
fcn.0000c1c0
fcn.0000c1f0
fcn.0000c210
fcn.0000c230
fcn.0000c270
fcn.0000c290
fcn.0000c2f0
fcn.0000c410
```

entry0 (int32_t arg1);

```
;-- section..text:
;-- segment.LOAD1:
;-- _start:
;-- rip:
(fcn) entry0 289
  entry0 (int32_t arg1);
; var int32_t var_38h @ rbp-0x38
; var int32_t var_30h @ rbp-0x30
; arg int32_t arg1 @ rdi
push rbp                            ; [14] -r-x section size 59781 named .text
mov  rbp, rsp
push r15
push r14
push r13
push r12
push rbx
sub  rsp, 0x18
mov  r14, rdi                       ; arg1
mov  rdi, qword [rdi]               ; arg1
movsxd rax, edi
lea  rbx, qword [r14 + rax*8]
add  rbx, 0x10
mov  rax, qword [0x0001c328]        ; section..got ; [0x1c328:8]=0
cmp  qword [rax], 0
jne  0xa032
```

```
mov  qword [rax], rbx
```

Reverse Engineering on BSD

- Radare2:
  - Available on FreeBSD and OpenBSD
- Vivisect

  https://github.com/vivisect/vivisect
  - Python static analysis tool
  - Should work with FreeBSD and OpenBSD

Reverse Engineering on BSD

- Munin

  https://github.com/Neo23x0/munin

  - Online Hash Checker for Virus Total and other services
  - Python based and should work with FreeBSD and OpenBSD

Reverse Engineering on BSD

- CyberChef:
  - “Cyber Swiss Army Knife”
  - Web based application developed by GCHQ for working with encryption, encoding, compression and data analysis.
  - Should work if setup on FreeBSD with node.js
  - Live Demo

    https://gchq.github.io/CyberChef/
  - Code Repository

    https://github.com/gchq/CyberChef/

Reverse Engineering on BSD

- VirusTotal:
  - Python API to query VirusTotal with file hashes for malicious behavior
  - Port exists on FreeBSD, code should work fine on OpenBSD
- Yara:
  - Malware identification and classification tool
  - Provides a signature format for host based searching
  - Available as a port with python bindings on FreeBSD and OpenBSD

Reverse Engineering on BSD

- Polichombr:
  - https://github.com/ANSSI-FR/polichombr
  - Python malware analyst framework
  - Discovered while looking for other tools, need to see if it works on any BSD.
- Volatility:
  - Advanced memory forensics framework
  - Available as a port on FreeBSD and OpenBSD

Reverse Engineering on BSD

- This was the first informal view of what is available, there are other tools that assist with reverse engineering that should be in the base OS or a simple port/pkg:
  - objdump
  - Hexedit
  - Strings
  - Hexdump
  - xxd (xxd -r -p to convert hexcode to strings)
- We will review additional tools in the future, including any that make their way into the ports tree.