Tekeli-li

The Great Deep Project

Team Members

Michael Weatherby

Michael Fitch

Blake Janes

Eric Del Valle

Challenges Faced

- Previously very little documentation on how to create a pwnme, qcow2 save, and a plugin for fuzzing. There was lots of small pieces to the puzzle that needed to be determined to write a proper guide.
- Lots of the existing code didn’t have documentation.
- Errors with running Shoggoth sometimes were only findable after many minutes of runtime.

Tasks Accomplished - Team

- Built Shoggoth
- Wrote a personal fuzzer
- Wrote a personal pwnme
- Created a .qcow2 file and installed an OS
- Wrote a “Getting Started” guide
  - Added instructions for plugin compilation, including where to place compiled plugins
  - Wrote the commands for creating a .qcow2 and installing an OS from an image file
  - Added instructions for setting up a snapshot to fuzz from, and how to run from it

Tasks Accomplished - Blake

- Wrote guide on getting started in Shoggoth
- Successfully got chosen fuzzing target running under Shoggoth
- Identified issue with OS handler preventing automated fuzzer development
- In Progress: Determining where in QEMU the C3 Register is

Tasks Accomplished - Michael F.

- Assisted in a guide to create a pwnme and plugin to emulate and fuzz a shoggoth save state.
- Studied plugin system to help provide support.
- Added python support to the plugin creator wizard
- In Progress: Continue studying plugin system to assist in writing plugins for finding (hopeful) 0day. (Potentially with untangled)

Tasks Accomplished - Michael W.

- Added to existing plugin documentation
- Studying back-end C code to information on messaging API
  - Plugins simple, documented callback functions
  - The example plugin sends a message to the VM to set a memory address range to a certain value
  - There are +30 message commands, all with no documentation- including no parameter information

Tasks Accomplished - Eric

- Wrote the guide to creating, installing, and running the .qcow2
- Wrote preliminary documentation
- Added the instructions for plugins
- Studied the OS Handler
- In Progress - Find where the c3 register is assigned in the source