Tekeli-li

The Great Deep Project

Team Members

Michael Weatherby
Michael Fitch
Blake Janes
Eric Del Valle

Tasks Accomplished - Summer

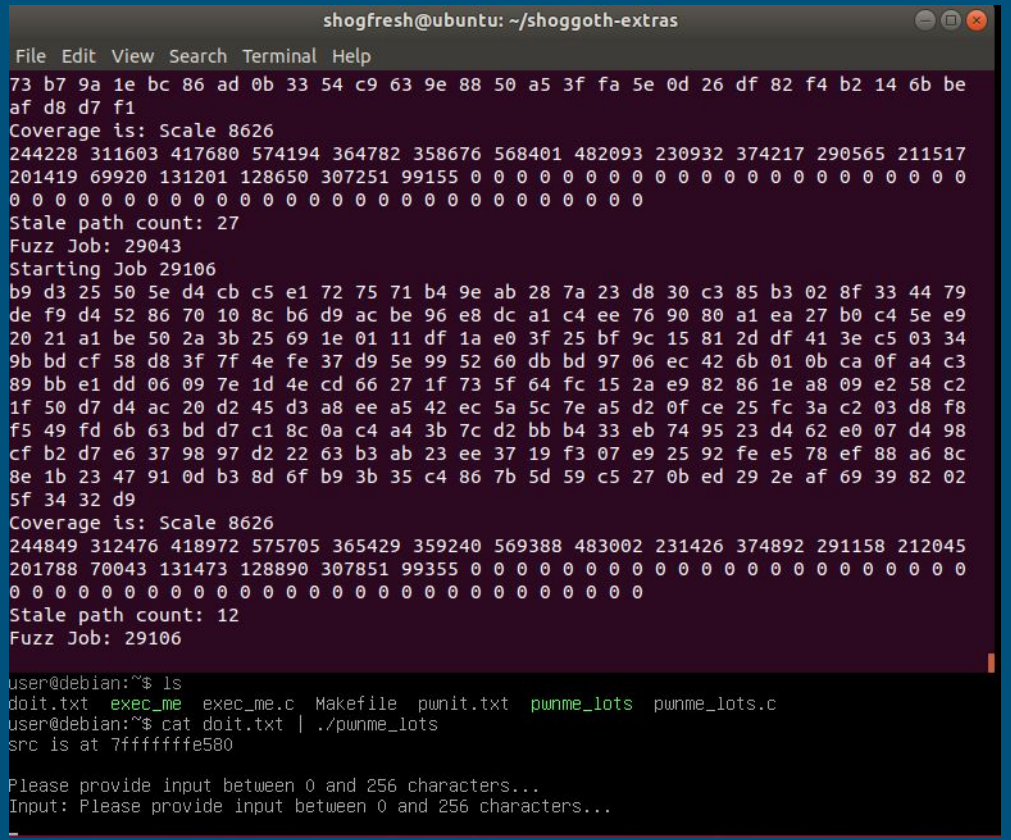
- Each team member:
  - Wrote a personal fuzzer plugin
  - Wrote a personal pwnme plugin
  - Created a .qcow2 (qemu OS image) and installed the OS
- Made a ‘getting started’ guide for:
  - Creating & installing .qcow2 files
  - Coding and running plugins

Tasks Accomplished

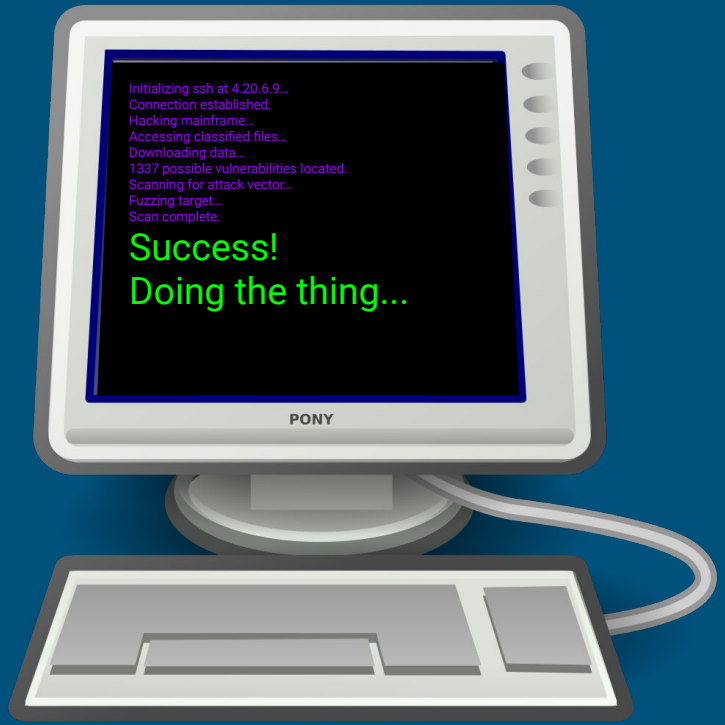
- Created modified OS handler designed to work on a linux VM with Untangle NG Firewall
- Created a Coverage Guided Fuzzer plugin in python for an existing target packaged with shoggoth-extras
- Expanded on plugin documentation

CGF

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



Live Demo


Initializing ssh at 4.20.6.9...
Connection established.
Hacking mainframe...
Accessing classified files...
Downloading data...
1337 possible vulnerabilities located.
Scanning for attack vector...
Fuzzing target...
Scan complete.
Success!
Doing the thing...
PONY

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