Malware Analysis (CS6038)

Week 07.1 Document Analysis

Scott Nusbaum
nusbausa@ucmail.uc.edu

February 26, 2019

University of CINCINNATI

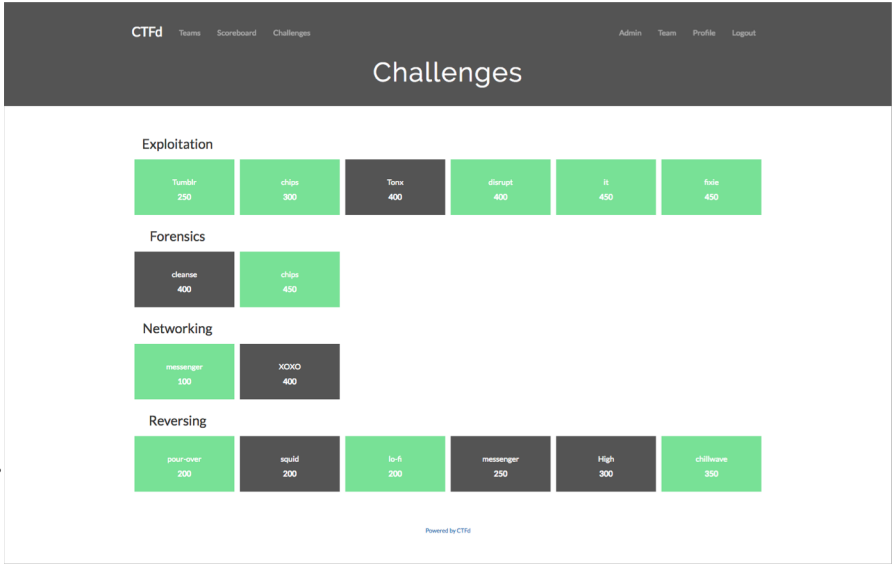
Overview

- Schedule
- Homework
- Network Analysis
- GDB

University of CINCINNATI

Schedule

- 6 More weeks of lectures
- The three lectures after Break will be similar to prior lectures but more in depth. More in class problems
- Final
  - Begins: April 14, 2019 Sunday at 00:00.
  - Ends: April 28, 2019 Sunday at 23:59.
  - Format Jeopardy CTF style



University of CINCINNATI

Homework

- Homework 2:
  - Graded and in Blackboard
- Homework 3:
  - Due Feb 28, 2019
- Homework 4:
  - Network Analysis
  - Assigned Feb 28, 2019
  - Due Mar 14, 2019

University of CINCINNATI

Network Analysis

- Tools
  - Wireshark
  - Tshark
  - TCPDump
  - Bro (Zeek)
  - Security Onion

University of CINCINNATI

Wireshark

- Overall GUI
- Filtering
- Streams (TCP)
- SSL Decrypting
- Packet | Stream Exporting

University of CINCINNATI

TShark

- Packaged with Wireshark
- Filtering
- Streams. -- tcp.stream eq #

University of CINCINNATI

TCPDump

- Manual Page
- Examples

University of CINCINNATI

Zeek

- Demo the parsing of the Pcap File
- https://www.zeek.org/bro-exchange-2013/exercises/faf.html
- https://www.sans.org/reading-room/whitepapers/detection/onion-zeek-rita-improving-network-visibility-detecting-c2-activity-38755

University of CINCINNATI

GDB

- Starting GDB
  - gdb <filename>
  - gdb <filename> <dump file>

GDB

- Commands
  - run (r)
  - continue (c)
  - break (b)
    - break $eax
    - break *0x401000
  - step (s) | step instruction (si)
  - next (n) | next instruction (ni)
  - i r – Show Registers
  - i b – Show Breakpoints
  - d # -- Delete Breakpoints
  - layout next
  - x/x | x/10x | x/10wx
  - x/s | x/10s
  - x/i | x/10i
  - disassemble

University of CINCINNATI

GDB

- follow-child-fork | follow-parent-fork
- attach <pid>
- shell (sh) <command>
- pwntools (gdb)
- Search Memory