ais

AIS Dynamic Defense Capture the Flag Exercise (Ru5tedBun1ons) 3.0

Assured Information Security, Inc.

Disclaimer

All opinions, statements, or illustrations expressed are mine and do not represent that of my employer or my employer’s customers or partners.

Agenda

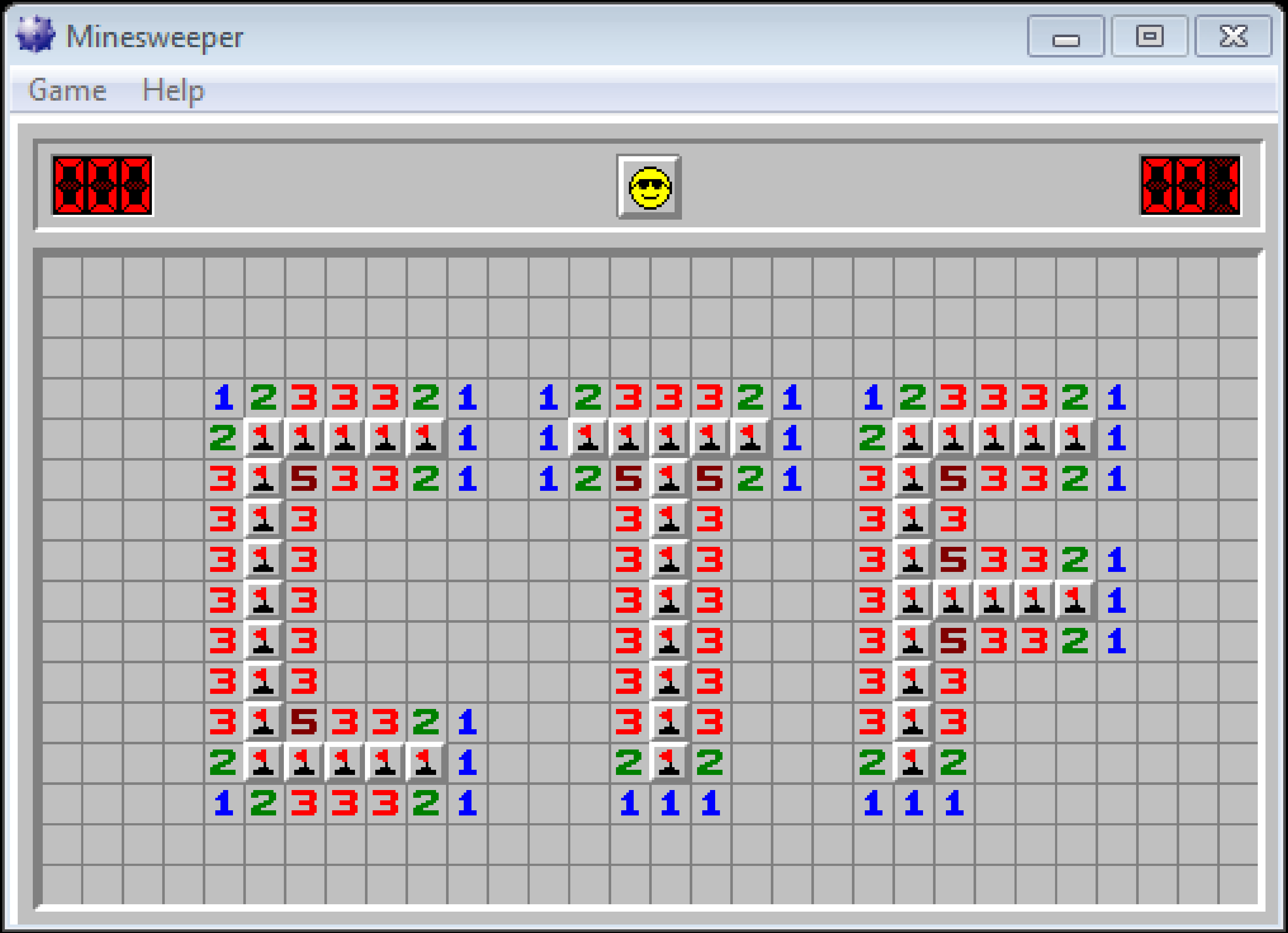
- AIS R&D: Virtual Machine Introspection (VMI)
- Hackathon Capture The Flag Challenges

Background: Virtual Machine Introspection

Essentially provides ‘god-mode’ control over VMs and all from an architectural vantage point

Typical Uses of VMI

- Defenses
  - Anti-Virus scans
  - Live guest patching
  - System Protection
- Malware analysis
- Software analysis
- Reverse engineering

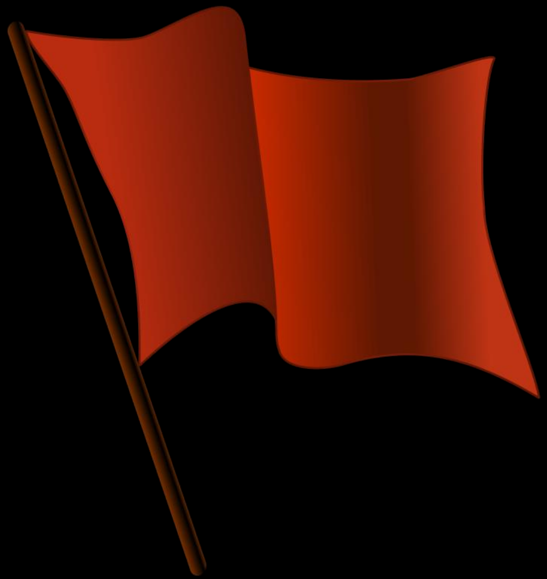


Minesweeper
Game
Help

IntroVirt in the CTF

- You will gain access to multiple VMs running on top of IntroVirt
- IntroVirt will introduce inconsistencies, oddities, or abnormalities into some aspect of system operation
- You will be given hints as to things you can do on these systems to find (or be presented with) the flag
- You submit the flag and get points

On to the challenges!



ais

CTF Challenges

There will be a problem to solve. You have to find any working solution.

INFO?

https://github.com/vix597/Ru5tedBun1ons

Currently being updated. Will be ready at the start of the hackathon tomorrow morning. But the machines are up now. So ya know….

Overview:

Scoring

- Level 1 (Easy): 100 points
- Level 2 (Easy): 100 points
- Level 3 (Medium): 200 points
- Level 4 (Hard): 200 points

Thank You.

ais