Level 0x0e

Game of Life / File Permissions

Topics

- Cyberquest
- Hacking History
- Bugs

Upcoming Events

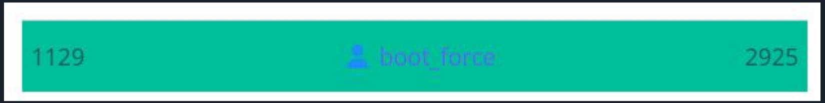
LOCKHEED MARTIN
CYBERQUEST®
COMPETITION

- Lockheed Martin Cyber Quest
  - Saturday, March 23rd
  - 3 hours. Free Breakfast and Lunch
  - Teams are 3-5 students
    - 3 laptops per team
  - Arrive at 8 AM
  - Pickup at 2PM
- Breakfast - IHOP
  - Pancakes, eggs, bacon, sausage, ham, potatoes
- Lunch - 4 Rivers
  - Brisket / Pulled Pork / Chicken sandwiches
  - Mac & Cheese, Corn Bread, Potatoes, Rice And beans, cookies, snacks
- CyberQuest Internships Available
- Challenge Overview Slides from Lockheed
- Emergency Phone: 407-256-0147

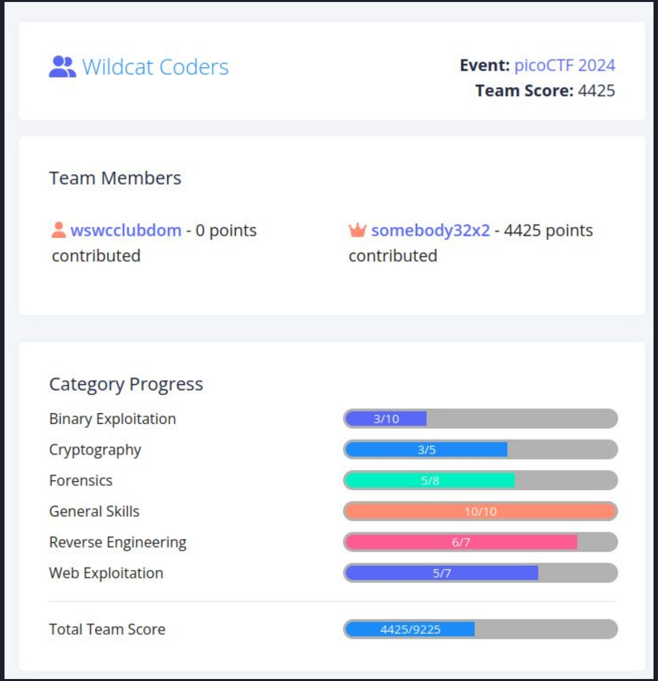
Wildcat Hackers 1	Wildcat Hackers 2
~~Dominick M~~ Jay J Parker W Sam S Zachary W	Eshan V Saaketh K Shoaib A ~~Dylan G~~ Justin T

PicoCTF

- Sam crushing it
- 550th of over 10,000 participants
- Where was everyone else?



1129 boot_force 2925



Wildcat Coders

Event: picoCTF 2024
Team Score: 4425

Team Members

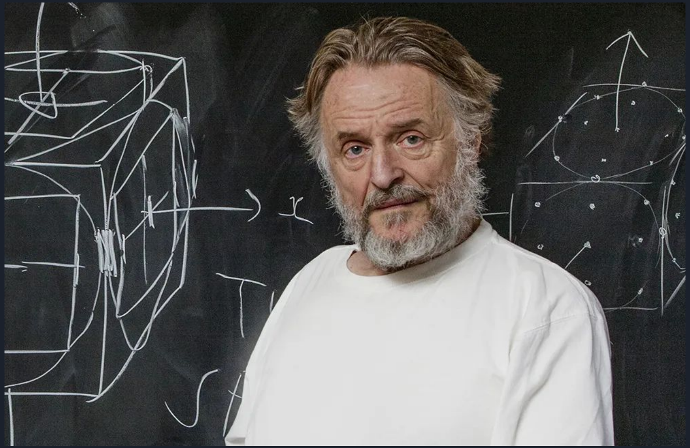
wswcclubdom - 0 points contributed

somebody32x2 - 4425 points contributed

Category Progress

Binary Exploitation	3/10
Cryptography	3/5
Forensics	5/8
General Skills	10/10
Reverse Engineering	6/7
Web Exploitation	5/7
Total Team Score	4425/9225

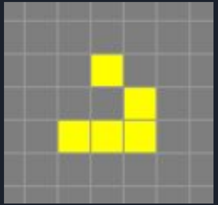
John Conway



- Mathematician (1937 - 2020)
- Invented Game of Life in 1970
    - Zero player game
    - Turing complete

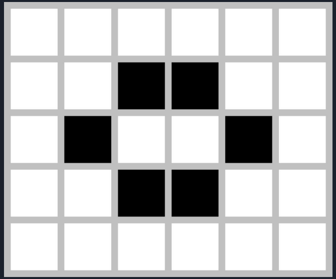
Rules for Conway's Life

1. Any live cell with fewer than two live neighbors dies, as if by underpopulation.
2. Any live cell with two or three live neighbors lives on to the next generation.
3. Any live cell with more than three live neighbors dies, as if by overpopulation.
4. Any dead cell with exactly three live neighbors becomes a live cell, as if by reproduction.

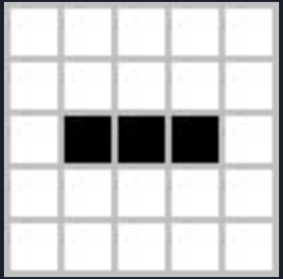


John Conway Explaining Life

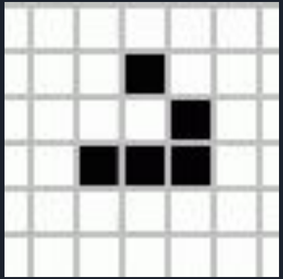
Game of Life Patterns



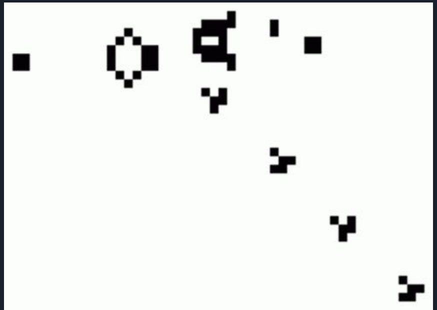
Bee hive
(stationary)



Blinker
(period 2)

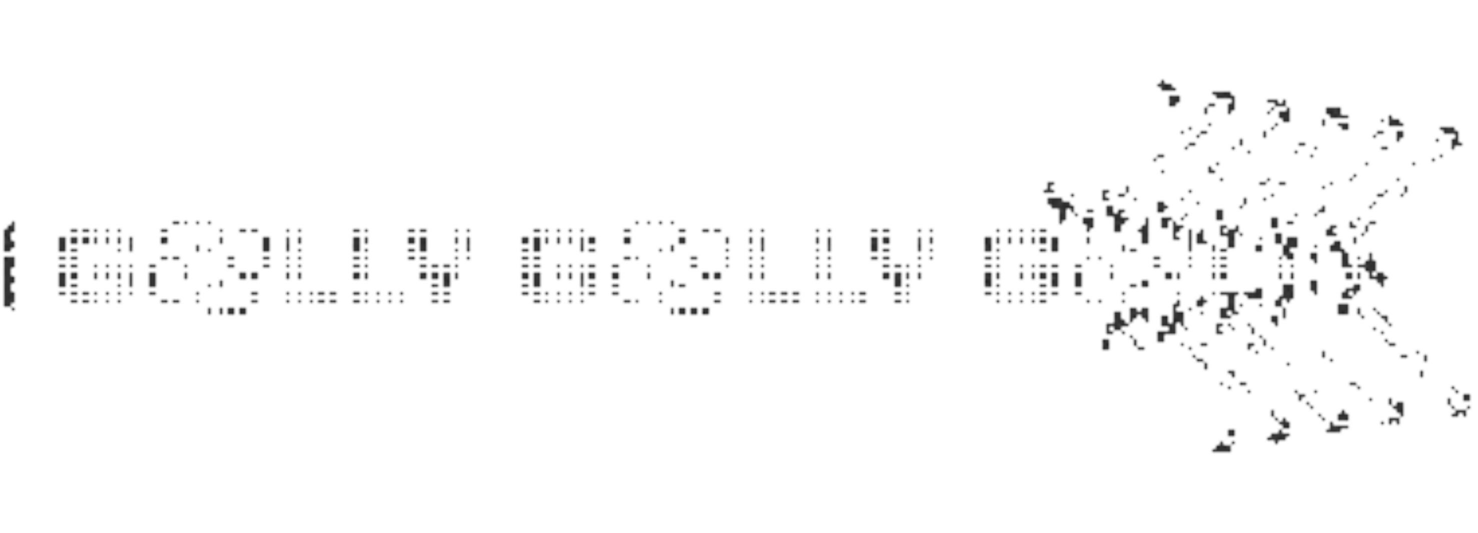


Glider (c/4 speed)

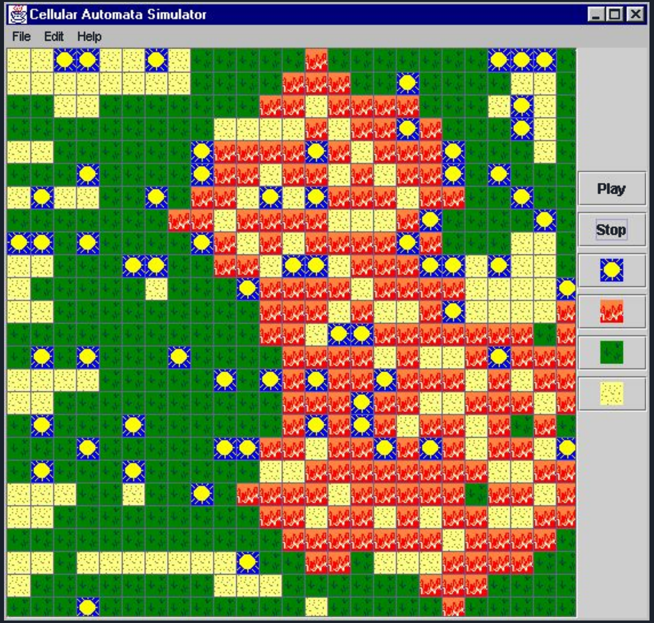


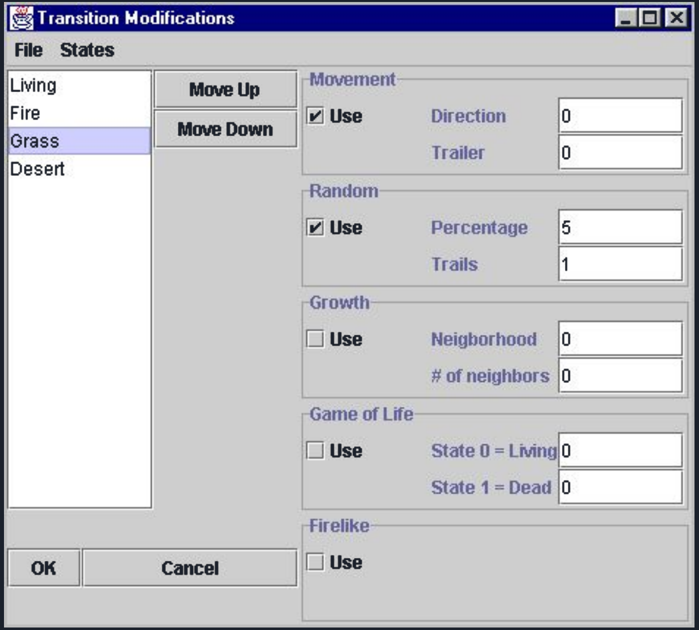
Emitter / Glider
Gun

Game of Life Computers



Spacial Entity Simulator





Living
Fire
Grass
Desert

Movement

☑ Use Direction 0

Trailer 0

Random

☑ Use Percentage 5

Trails 1

Growth

☐ Use Neighborhood 0

# of neighbors 0

Game of Life

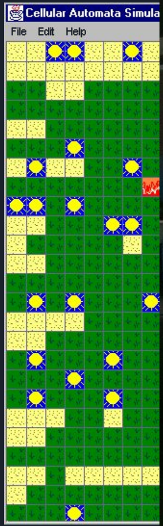
☐ Use State 0 = Living 0

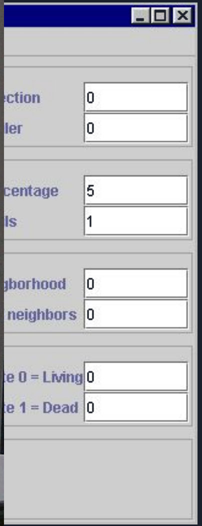
State 1 = Dead 0

Firelike

☐ Use

Spacial Entity Simulator





ection 0

ler 0

centage 5

ls 1

gborhood 0

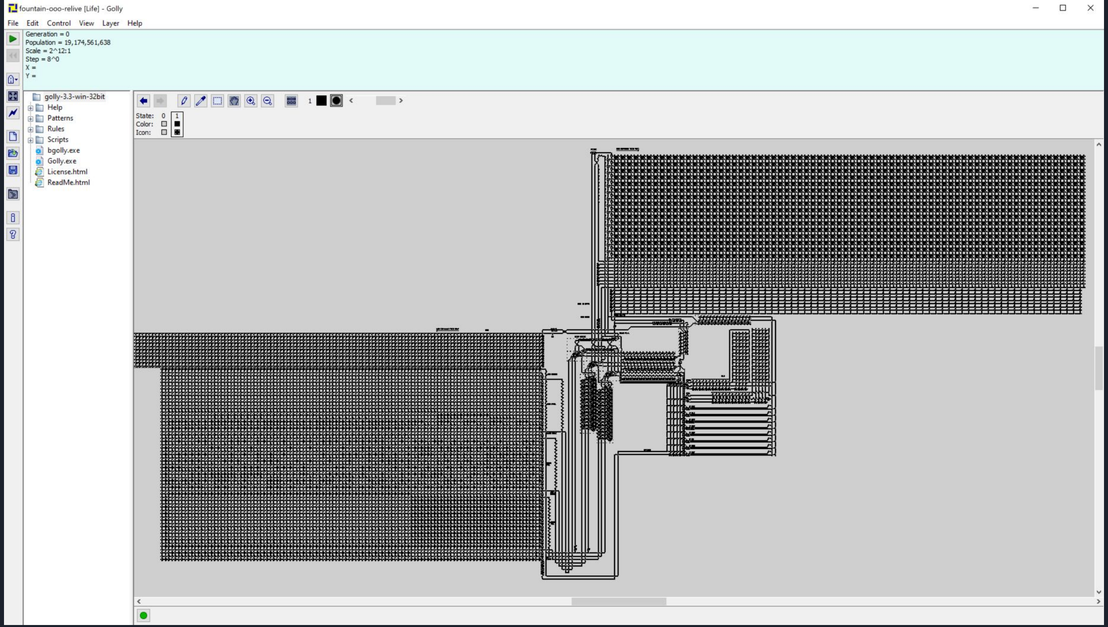
neighbors 0

te 0 = Living 0

te 1 = Dead 0

Game of Life and CTFs

DEFCON Quals 2020

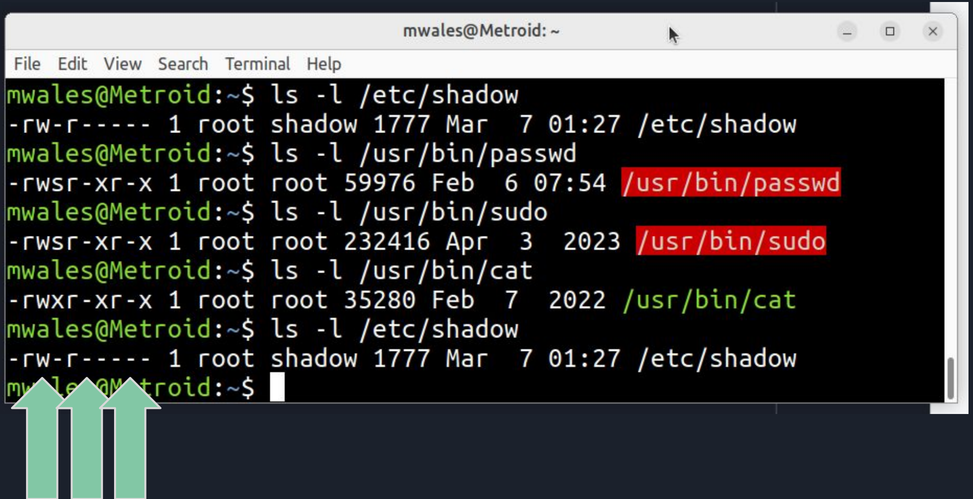


fountain-ooo-relive [Life] - Golly

```
Generation = 0
Population = 19,174,561,638
Scale = 2^12:1
Step = 8^0
X =
Y =
```

File Permissions

- File permissions have 3 groups (from left to right)
  - user / Owner
  - group
  - others
- **`chmod a+x filename`**: change file mode, all add execute



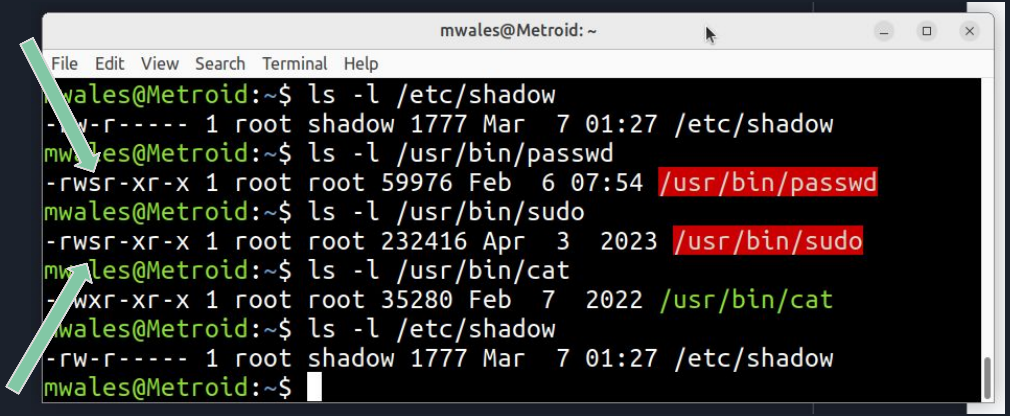
```
mwales@Metroid:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1777 Mar  7 01:27 /etc/shadow
mwales@Metroid:~$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 59976 Feb  6 07:54 /usr/bin/passwd
mwales@Metroid:~$ ls -l /usr/bin/sudo
-rwsr-xr-x 1 root root 232416 Apr  3  2023 /usr/bin/sudo
mwales@Metroid:~$ ls -l /usr/bin/cat
-rwxr-xr-x 1 root root 35280 Feb  7  2022 /usr/bin/cat
mwales@Metroid:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1777 Mar  7 01:27 /etc/shadow
mwales@Metroid:~$
```

File Permissions

3 bits per user-group
Can set permissions with OCTALS!!!

```
chmod 664 other_can_read_but_not_write
chmod 600 only_owner_can_read_write
```

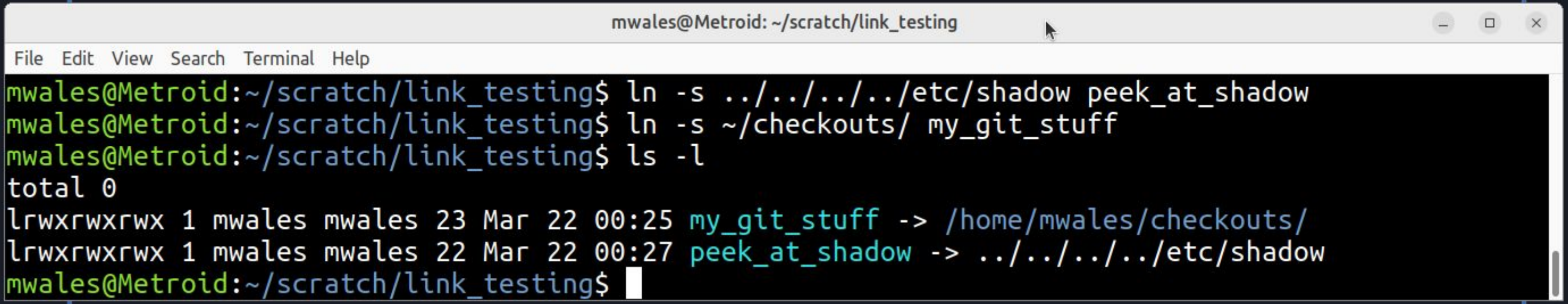
- Each group has:
  - r = read permission
  - w = write permission
  - x = execute
    - s = set uid (execute with the permissions of the owner / group



```
mwales@Metroid:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1777 Mar  7 01:27 /etc/shadow
mwales@Metroid:~$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 59976 Feb  6 07:54 /usr/bin/passwd
mwales@Metroid:~$ ls -l /usr/bin/sudo
-rwsr-xr-x 1 root root 232416 Apr  3  2023 /usr/bin/sudo
mwales@Metroid:~$ ls -l /usr/bin/cat
-rwxr-xr-x 1 root root 35280 Feb  7  2022 /usr/bin/cat
mwales@Metroid:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1777 Mar  7 01:27 /etc/shadow
mwales@Metroid:~$ 
```

Symbolic Links

- Make a link from a path name to a different pathname
  - ln -s /home/user/destfolder specialfolder
  - ln -s ../../../../ am_i_root
- Can link to large files you don’t wan’t to move / copy
- Change between different directories easily
- Attacker can put sym link / path traversal in a tar, gzip, zip container, escape jail
  - DJI Drones were vulnerable for years to this attack (P0VsRedHerring)



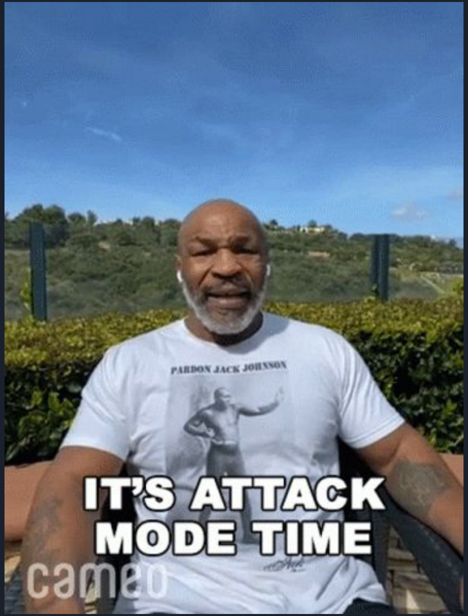
```
mwales@Metroid:~/scratch/link_testing$ ln -s ../../../../etc/shadow peek_at_shadow
mwales@Metroid:~/scratch/link_testing$ ln -s ~/checkouts/ my_git_stuff
mwales@Metroid:~/scratch/link_testing$ ls -l
total 0
lrwxrwxrwx 1 mwales mwales 23 Mar 22 00:25 my_git_stuff -> /home/mwales/checkouts/
lrwxrwxrwx 1 mwales mwales 22 Mar 22 00:27 peek_at_shadow -> ../../../../etc/shadow
mwales@Metroid:~/scratch/link_testing$ 
```

setuid / setgid

- setuid = set user ID
- setgid = set group ID
- Programs like sudo and password need to run as root user, but be run by normal users
  - Program gets to run as user that owns the file (usually root)
- Security Implications
  - A bug in a program running with root permission could give attacker root access
    - Attacker could then add / remove users
    - Attacker could implant / add malicious software to system (keyloggers, spyware)
    - Attacker could access secret files (password hashes)
  - Don’t have many setuid programs on your system, they are very high risk
  - Protect the setuid programs
    - Don’t let other users overwrite them

Attack Methods

- Attack binaries running as root user
  - Exploitation
  - Overwrite / link to my malicious application
- Escape jails / expose secret files with ../../path/traversal
- Which binaries / scripts have root owner / suid bit set?
- What scripts are root users running?
  - Can I redirect execution down malicious path?
  - What files is root executing that I can overwrite?



Links

- https://www.wired.com/2015/09/life-games-playful-genius-john-conway/
- https://en.wikipedia.org/wiki/Conway%27s_Game_of_Life
- https://golly.sourceforge.io/