CS 544/444

Lab 3 Final

Group 5: Christopher Wu, Haleh Falakshahi, Qian Hao, Dipendra Humagain, Keith Swalin

Command Line Injection

- What we tried when we played ‘;cat /home/moderator/log/some_log’, ‘;su group5’, ‘;vi /home/moderator/log/some_log’, etc. ... all attempts failed
- What we did when we hosted - 3 Servers prepared (modifications to config and to communications.py)
  - #1 did not sanitize chmod
    - #1 we anticipated ‘;chmod 777 /home/moderator/log/*’ or something like that to be able to read the log file in an effort to win the game
  - #2 sanitized chmod but left other commands open, i.e. cp, cat, etc.
    - #2 we anticipated ‘;cp /home/group5/bash_script /home/moderator/’ then execution of a script that would do chmod itself or ‘;cat /home/moderator/log/some_log > /home/group5/some_folder/some_log’
  - #3 sanitized chmod, cp & mv but left other commands open, i.e. cat, nano, vi, etc.
    - #3 we prepared a way for users to gain root privs through an accessible log file with a password to an unused group → this group was in the sudoers file and wheel group

File Permissions

- **Stat() function:**
  - while : ; do stat /home/moderator/pipes/#tosD/#tos | grep Change; \sleep 1; done
    - this is the Stat() function command we used during the game.
  - All the groups are given the execute permission for the directory that stores in the pipe.
    - this is modified by moderator
  - So users can use Stat() function to check Inode.
    - Run the command during the game and we can see who is typing during that time. (Based on the changes of last modified time)
- **SUID & SGID**
  - Set User ID & Set group ID
  - Unix access rights flags that allow users to run an executable with the permissions of the executable's owner or group respectively and to change behaviour in directories.

Race Conditions

- Used a premade script provided by the group
- Ran the script prior to game start

```
#!/usr/bin/env bash while true; do tail -f "/home/moderator/log/${1}m.log" 2>
/dev/null \ || true done
```

- On success, the beginning of the log file will be outputted to the terminal.
- What we learned - Taking advantage of race opportunities means that we can gain information the original developer did not intend by taking advantage of order of operations opportunities.

Extras/Interesting/Winning strategy

- Playing the game normally. If you are a werewolf, hang the other one and then eat people at night. They are too busy with computer magic than moon magic.
- Physically stealing passwords.