Group 3

Group Presentation

CS444/544
Spring 2017

*Jessica Dudek *Jonathan Kring *Katrina Mosimann *Edgar Salas *Sheng Zhong

Moderating The Game

Setup

To set up our game, we gave every group the execution rights to the folders that store the pipes. This allowed them to use the stat() command to check the inodes of those pipes.

Based on the time that inode was last modified people were able to guess which teams were the werewolves.

Results

Our method was mostly successful as several groups actually found the identity of the werewolves by using this method with our setup.

Moderating The Game

Issues with stat() function vulnerability

While moderating, we found that this method does not always reveal werewolves with 100% accuracy because:

1) Sometimes the number of pipes that had been modified during the night was more than the number of werewolves. This was likely caused by some townspeople trying to find other vulnerabilities during the night.

2) This method won't work if werewolves choose to keep silent to avoid detection.

Exploits Used by Group During GamePlay

- Race Condition --Log File Access
- File Permissions
- Command injection vulnerabilities
- Social Engineering and Other Strategies

Race condition

While working with the race condition, we used the group provided command:

```
tail -f /home/moderator/log/#m.log &
```

This command was run prior to the start of the game to successfully get the log file information about the game players at startup.

We learned that this is a good example to implement the covert channel attack by taking the advantage of this classic filesystem race condition vulnerability.

While running this exploit we were able to see which roles were assigned to each team and successfully win our games.

File permission by other group

We learned SUID, SGID and Sticky Bit.

Run executable with permission of the authorized users.

Modify the files with SUID set using temporary privilege of the user who has r/w permission for that file.

Command injection vulnerabilities by other group

We learned how to use the commands:

“xxxx; <command>”

Where the commands involved changing the log and config files along with another one called “sneaky_script.sh” as:

“xxxx; chmod -R 777 /home/moderator/log”

“Xxxx; chmod 777 /home/moderator/config”

“xxxx” is the text being entered and changed by the commands above

Social Engineering and Other Survival Strategies

Although not one of the methods discussed in the presentations, our team members also used Social Engineering to attempt to win during gameplay.

As Werewolves-- When a game started before we were able to work with the listed exploit, we would wait until the first team correctly identified us and our partner werewolf team then would convince the other groups to eliminate the teams that had seen the logs.

As Townspeople-- When we were townspeople we would usually stay silent and observe the other teams behaviors. If we noticed any unusual behavior or threatening behavior towards our team we would convince the other teams to kill the attacking team

As the Witch- To survive as the witch, we saved our potion for ourselves. If we were unable to convince the other teams to kill a team that was acting strangely we used our poison potion on the team that we assumed to be a wolf.

This method was actually quite successful and lead to more wins than we were expecting.