Werewolves Out Briefing

Lessons Learned

Joshua Donckels, Audarius Goins, Jenniffer Estrada,
Banafsheh Khosravi, Bentley Laaksonen

Department of Computer Science
University of New Mexico

Cyber Security: CS444/544

Outline

Interesting Points
What We Learned

What We Learned

- Command injections in SQL seem to demonstrate fundamental architecture flaws? Sanitizing input may work, but seems like a patch on a more fundamental problem. Enabling the equivalent of a matlab "eval" in a database is a bit crazy!
- The Linux OS exposes quite a bit of information to unprivileged users via /proc, etc. It's kind of shocking how much information can be leaked by poking in the right places.
- Setting file permissions properly can be challenging. Linux has a reasonably simple model. Windows ACLs are so insanely complex they seem utterly unmanageable. "KISS," keep it simple stupid, seems appropriate.

Outline

Lessons Learned
Our Take Aways

From Our Moderation

- Our race exploit was coded in C and compiled -O2 to be as fast as possible. The inner loop was kept as simple as it could possibly be. This made the exploit more reliable, after testing demonstrated extra care was needed.
- It is a bad idea to enable all exploits in the game as a moderator.
- The race condition exploit required knowing what file was to-be created – not always possible.

Outline

Lessons Learned
Our Take Aways

From Playing Games

- Reading the moderator log file is the coolest way to cheat in the game. Moderator log file doesn't have necessary permission. But we try to export the race condition and able to access it. You should be able to change the permission once you get its access. So,that everyone can access moderator file.
- Many protections can be made, but one can still walk around the room and sample screens!
- The TCP socket info attack may have been the most fun because it was indirect. While one could pollute the channel to make it harder, this wouldn't be practical in real life.
- Even when the werewolves were found out, the hardest part was convincing other people.

Lingering Questions
After thoughts

Would have been cool

- If you have physical access to a server, opportunities are opened! It would have been fun to try and find the VM disk images, mount them with root access from another VM, and exploit away!

Lingering Questions

- Do hardened Linux distributions attempt to protect side channels (against things like the TCP socket information attack)?
- Has an OS been designed from the ground up with security as the first priority?