Part 1: Introduction to Linux Exploit Development

Hello and welcome! As I'm sure you know by know, if your reading this, I have a passion for exploit development. My journey into Windows exploit development has even taken me into the depths and insanity of Ring0 exploitation [Thx Ryujin for expanding the pain!]. I will continue to write and publish Windows exploit development tutorials but the time has come for FuzzySecurity to branch out into Linux exploitation! A good friend and colleague of mine Donato Capitella (aka kyuzo) has graciously offered to share his knowledge on this subject matter with us and I know we can all learn a lot from his experience. I won't bore the reader with an overly long introduction, I will just mention that these tutorials require a certain familiarity with general Operating System Internals (nothing that a good Google-search won't teach you). Now go forth and get yourself a shell!!

Tools Of The Trade

A Brain/Persistence
Keep your head cool, read up on subject matter topics, enjoy bending your OS to your strength and pop a shell!

Linux GDB Debugger - Quick reference guide
GNU debugger or more typically referenced as gdb is the default debugger on Linux and is also the defacto debugger we will be using in these tutorials. The command line interface can be a bit daunting at first but once you get used to it you will not regret the effort. If you want to use a graphical debugger you can try edb (Evan's Debugger) which is skinned to be similar to OllyDBG on windows.

Virtualization Software

Basically there are two options here VirtualBox which is free and Vmware which isn't. If its possible I would suggest using Vmware; a clever person might not need to pay for it ;)).

Comments

There are no comments posted yet. Be the first one!

Post a new comment

Enter text right here!

Name

Displayed next to your comments.

Email

Not displayed publicly.

Subscribe to None ▾

Submit Comment