nnamon / linux-exploitation-course

A Course on Intermediate Level Linux Exploitation

32 commits 1 branch 0 releases 1 contributor CC-BY-4.0

Branch: master New pull request Find file Clone or download

nnamon Update Vagrantfile Latest commit 23dba47 4 days ago

lessons	Update lessonplan.md	18 days ago
.gitignore	Finished sections 6 and 7.	a year ago

LICENSE	Create LICENSE	a year ago
README.md	Update README.md	19 days ago
Vagrantfile	Update Vagrantfile	4 days ago
builddocker.sh	Completed section 3	a year ago
cleanup.sh	Added the advanced exercises, sections 9 and 10	a year ago
deploydocker.sh	Completed section 3	a year ago
makeall.sh	Added more to the Introduction to PEDA and Pwntools section on PEDA	a year ago

README.md

linux-exploitation-course

A Course on Intermediate Level Linux Exploitation

Pre-Requisites

The course is designed as a continuation of the Windows Exploit Development workshops by the people at Null Singapore and some pre-requisite knowledge is expected of the following topics:

1. An Understanding of x86-64 Assembly
2. Familiarity with GDB
3. Familiarity with C and Python
4. Familiarity with the Standard Jump to Shellcode Exploits

Please do view this 15 minute 'Introduction to Return Oriented Programming' video as a refresher. If you have time, please go through the lesson plan for the video.

Syllabus

1. Setting Up the Environment
2. How Does a Linux Binary Work? - Skipped for Now
3. Introduction to PEDA and Pwntools
4. Classic Exploitation Technique
5. Linux Binary Protections
6. Bypassing NX with Return Oriented Programming
7. Bypassing NX with Ret2Libc
8. ASLR in Depth
9. Bypassing ASLR/NX with Ret2PLT
10. Bypassing ASLR/NX with GOT Overwrite
11. Memory Leaks - Skipped for Now
12. Multi-Stage Exploits
13. Format String Vulnerabilties
14. Advanced Exercises