Pwning Your System

Binary Exploitation using Ghidra

by Luke Thurston

All About The Pwn

“Slang term meaning ‘to completely defeat (something).’ Originally a mistyping of ‘own’, since ‘p’ and ‘o’ are next to each other on QWERTY keyboards. PWN is part of leetspeak, a modified spelling system used by hackers and video gamers.” (NordVPN)

In the context of CTF competitions, the term ‘pwn’ is commonly used to refer to challenges that deal with Binary Exploitation.

Distinction between Binary Exploitation and Reverse Engineering (CTF101)

- Reverse Engineering is focused on understanding “the functionality of a given program such that you can identify deeper issues.”
- Binary Exploitation is about “finding a vulnerability in the program and exploiting it to gain control of a shell or modifying the program's functions.”

Technical Background

Tools for Binary Exploitation

(1.) Hypervisor, Virtual Machine, and Guest OS

- ★ Ubuntu, Kali, Parrot Sec, Windows 10, etc.

(2.) Reverse Engineering Software

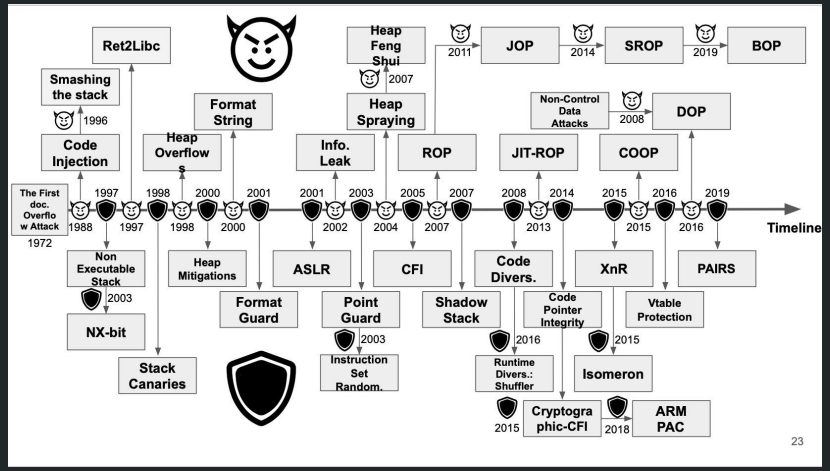
- ★ Ghidra IDA Pro, Valgrind, Binary Ninja, Radare, Hopper, etc.

(3.) Binary Exploitation

- ★ PwnTools, Pwndbg, GEF, Peda, Codium, Checksec, etc.

Biting the Bullet: Binex Attack Space

- Buffer Overflow Attacks
- Shell Code Injection & Stack Smashing
- Non-exec Stack vs. Return to Libc
- Stack Canaries vs. Heap Overflow
- Address Space Layout Randomization vs. Info Leaking and Heap Spraying
- Overwriting GOT (Global Offset Table)



(Roppers Intro)

Demo Preview

Step 1: Download and Install Virtualbox
Step 2: Spin up a Kali Machine
Step 3: Download Executables from Crackmes.one
Step 4: Try Running the Executable
Step 5: To understand the program flow, open the binary in ghidra
Step 6: Use any additional binex tools to complete the hack.

Demo Summary and Takeaways

- Ghidra is a powerful tool for SRE that can be used to carry out numerous exploits on unsuspecting victims.
- Make sure that your binary executables have been stripped of any identifiers which could lead a hacker to more quickly detect the functionality of your program.
- Binex attacks take experience to fully master. Resources to stay up to date include:
  - pwn.college Blue Belt by Arizona State University
  - Roppers Roadmap
  - Crackmes.one

Citations

- https://nordvpn.com/cybersecurity/glossary/pwn/
- https://www.hoppersroppers.org/roadmap/training/pwning.html
- https://ctf101.org/binary-exploitation/overview/