**overflow1.c**

**A screenshot of a computer program

AI-generated content may be incorrect.**

* Mục đích đoạn code là làm tràn bộ nhớ của biến buffer, ghi đè địa chỉ trả về (return address) của hàm main() bằng địa chỉ của chính buffer, nơi chứa shellcode để thực thi /bin/sh
* Cách hoạt động:
  + Shellcode nằm đầu large\_string → được copy vào đầu buffer
  + Cuối chuỗi là các địa chỉ buffer → return address sẽ bị ghi đè bởi địa chỉ của buffer
  + Khi hàm main() kết thúc → CPU nhảy đến buffer (nơi có shellcode)
  + Shellcode thực hiện execve("/bin/sh", NULL, NULL) → Mở một shell → Khai thác thành công

**A screenshot of a computer

AI-generated content may be incorrect.**

* Khai thác được lỗi thành công, lệnh /bin/bash được thực thi. Tuy nhiên khi build cần tắt các tính năng bảo vệ, vì các compiler hiện đại đều phát hiện được những lỗi cơ bản này, như ở lần build đầu tiên sẽ bị lỗi và bị Aborted

**sp.c**

**A screen shot of a computer code

AI-generated content may be incorrect.**

* Đoạn code này dùng để hiển thị giá trị hiện tại của stack pointer, giúp dự đoán vị trí của shellcode hoặc buffer mà ta muốn thực thi.

**A screen shot of a computer

AI-generated content may be incorrect.**

**exploit2.c**

A screenshot of a computer program

AI-generated content may be incorrect.

* Mục đích chính của đoạn code là đặt shellcode vào biến môi trường $EGG, sau đó thực thi chương trình **vulnerable.c**, với mục đích ép nó nhảy đến shellcode và thực thi /bin/sh
* Cách hoạt động:
  + Ghi shellcode vào một chuỗi buff
  + Lấp đầy chuỗi bằng các RET
  + Đặt shellcode vào giữa bộ nhớ đệm
  + Gán buff làm biến môi trường EGG
  + Thực thi file ./vulnerable đọc biến môi trường và tràn stack.

A computer screen with white text

AI-generated content may be incorrect.

* Sau khi exploit2.c lưu shellcode và đệm chuỗi addr vào biến môi trường $EGG, ./vulnerable sẽ lấy shellcode và chuỗi RET copy vào buffer. RET trong chuỗi này sẽ ghi đè lên EIP. Nhưng RET đã trỏ sai, hoặc shellcode không được thực thi có thể do các nguyên nhân sau:
  + NX bit bật
  + RET không nằm trong vùng NOP/shellcode
  + shellcode chứa byte không hợp lệ (VD: nhảy vào giữa opcode)
* Khi đó CPU thực thi opcode rác -> gây Illegal instruction
* Khi chạy đúng số lượng addr và offset thì sẽ ra kết quả sau:

A screen shot of a computer code

AI-generated content may be incorrect.

**exploit3.c**

A screen shot of a computer code

AI-generated content may be incorrect.

* Mục đích của đoạn code vẫn là đặt shellcode và khai thác buffer overflow để thực thi /bin/bash. Tuy nhiên, cơ chế đã khác với exploit2, ở exploit3 thay vì chèn addr vào trước shellcode ta sẽ chèn một chuỗi NOP sled ở phía đầu, shellcode ở giữa và ret ở cuối. Để miễn là ret nhảy vào vùng NOP sled thì vẫn thành công.
* exploit3.c buffer:

[NOP][NOP][NOP]...[shellcode]...[NOP][addr][addr][addr]...

A screenshot of a computer program

AI-generated content may be incorrect.

* Do có sự khác biệt của hệ thống nên địa chỉ hệ thống thực tế thường cao hơn nhiều so với hệ thống cũ trong hướng dẫn, vì thế giá trị của $EGG sẽ khác để khai thác được buffer
* Khi chạy đúng thì sẽ được kết quả sau

A screenshot of a computer program

AI-generated content may be incorrect.