Trường Đại học Công nghệ Thông tin (UIT)
Đại Học Quốc Gia Tp. HCM

BÀI TẬP 3

Môn học: Lập trình an toàn & Khai thác lỗ hổng phần mềm

Tên chủ đề: **Overflow-based Exploitation**

Mã môn học: NT521

1. NỘI DUNG THỰC HIỆN

Thực hiện các yêu cầu khai thác lỗ hổng liên quan tới ***chuỗi định dạng***, ***tràn bộ nhớ ngăn xếp/BSS*** của chương trình.

Thông tin chi tiết về yêu cầu như bên dưới:

[1] ELF x86 - Format string bug basic 1: https://www.root-me.org/en/Challenges/App-System/ELF-x86-Format-string-bug-basic-1

[2] ELF x86 - Format string bug basic 2: https://www.root-me.org/en/Challenges/App-System/ELF-x86-Format-string-bug-basic-2

[3] ELF x86 Stack overflow basic 1: https://www.root-me.org/en/Challenges/App-System/ELF-x86-Stack-buffer-overflow-basic-1

[4] ELF x86 Stack overflow basic 2: https://www.root-me.org/en/Challenges/App-System/ELF-x86-Stack-buffer-overflow-basic-2

[5] ELF x86 - Stack buffer overflow basic 3: https://www.root-me.org/en/Challenges/App-System/ELF-x86-Stack-buffer-overflow-basic-3

[6] ELF x86 - Stack buffer overflow basic 4: https://www.root-me.org/en/Challenges/App-System/ELF-x86-Stack-buffer-overflow-basic-4

[7] ELF x86 - Stack buffer overflow basic 5: https://www.root-me.org/en/Challenges/App-System/ELF32-Stack-buffer-overflow-basic-5

[8] ELF x86 - Stack buffer overflow basic 6: https://www.root-me.org/en/Challenges/App-System/ELF-x86-Stack-buffer-overflow-basic-6

[9] ELF x86 - BSS buffer overflow: https://www.root-me.org/en/Challenges/App-System/ELF-x86-BSS-buffer-overflow

2. GỢI Ý – THAM KHẢO

Một số gợi ý thực hiện:

- Sử dụng gdb, IDA Pro,… để gỡ lỗi, phân tích bộ nhớ chương trình.
- Tham khảo bài giảng môn học.
- Sách "The art of software security assessment identifying and preventing software vulnerabilities"
- Sách "Hacking: The Art of Exploitation"

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT