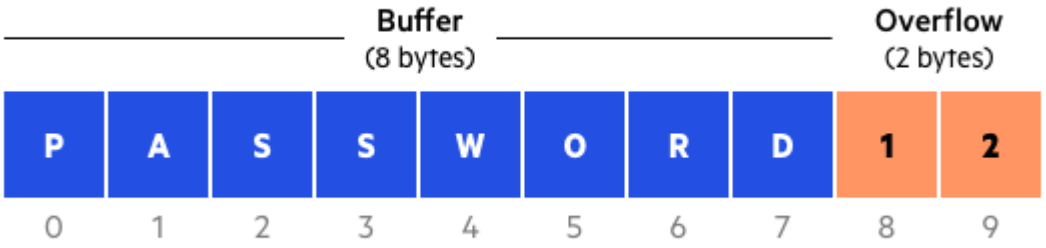
Programowanie niskopoziomowe – Lab 4

Czym jest buffer overflow? Jest to sytuacja, w której program zapisuje dane poza przydzieloną dla bufora pamięcią. Gdy zbyt dużo danych jest wpisywanych do bufora, może to spowodować nadpisanie sąsiednich obszarów pamięci, co prowadzi do nieprzewidywalnego zachowania aplikacji, a w niektórych przypadkach umożliwia atakującemu wykonanie nieautoryzowanego kodu.

Najczęściej spotykane przyczyny exploatacji buffer overflow obejmują:

- **Błędy programistyczne:** Niepoprawne obliczenia długości danych wprowadzanych przez użytkownika mogą prowadzić do przepełnienia bufora.
- **Brak walidacji danych:** Niewystarczająca kontrola nad danymi wejściowymi pozwala na wprowadzenie złośliwych ładunków.
- **Zastosowanie przestarzałych lub nieodpowiednich funkcji:** Funkcje takie jak strcpy nie sprawdzają długości danych, co zwiększa ryzyko.



Materiały dodatkowe

- https://owasp.org/www-community/attacks/Buffer_overflow_attack
- https://medium.com/offensive-security-walk-throughs/how-to-perform-buffer-overflow-attacks-253f4eb35b74
- https://astralabs-co.medium.com/exploit-tutorial-understanding-buffer-overflows-d017108edc85
- https://tcm-sec.com/practice-assembly-with-a-buffer-overflow-exercise/
- https://www.youtube.com/watch?v=FthE3WhMUuw
- https://d0nut.medium.com/week-13-introduction-to-buffer-overflows-5f15c0d5b5c1
- https://medium.com/purple-team/buffer-overflow-c36dd9f2be6f
- https://medium.com/nerd-for-tech/buffer-overflow-attacks-b5e62a522e6e
- https://snyk.io/blog/buffer-overflow-attacks-in-c/
- https://medium.com/techloop/understanding-buffer-overflow-vulnerability-85ac22ec8cd3
- https://www.cobalt.io/blog/overflow-vulnerabilities
- https://www.cobalt.io/blog/pentester-guide-to-exploiting-buffer-overflow-vulnerabilities
- https://www.youtube.com/watch?v=ncBblM920jw
- https://www.jsums.edu/nmeghanathan/files/2015/05/CSC437-Fall2013-Module-5-Buffer-Overflow-Attacks.pdf
- https://github.com/muhammet-mucahit/Security-Exercises
- https://web.ecs.syr.edu/~wedu/seed/Book/book_sample_buffer.pdf
- https://steflan-security.com/tryhackme-buffer-overflow-prep/
- https://infosecwriteups.com/tryhackme-oscp-buffer-overflow-prep-overflow-2-57c22b51a91f
- https://anilcelik.medium.com/en-buffer-overflow-prep-overflow2-walkthrough-ed6d9447595b
- https://medium.com/@zycc2727/buffer-overflow-prep-overflow-1-778304795902
- https://bevijaygupta.medium.com/tryhackme-oscp-buffer-overflow-prep-overflow-1-9d134d15a8cb

Zadania praktyczne – Buffer overflows

1) Zarejestruj się na stronie tryhackme:

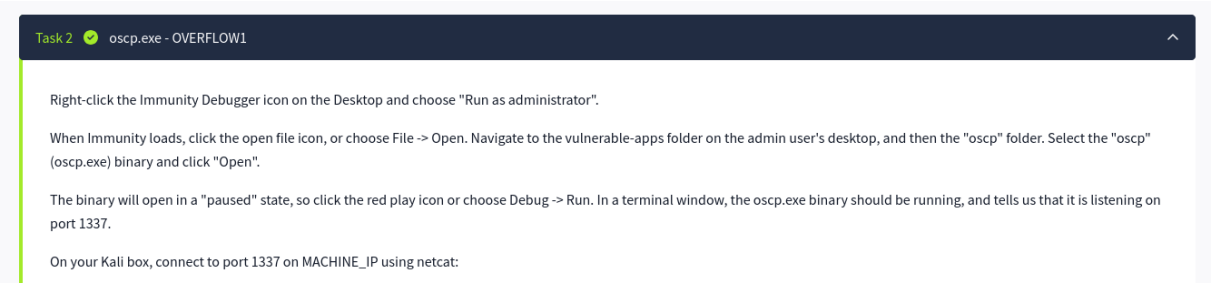
https://tryhackme.com/

2) Następnie uruchom zadanie **Buffer Overflow Prep**

https://tryhackme.com/room/bufferoverflowprep

3) Rozwiąż 10 zadań dostępnych w pokoju
   - Po każdym etapie sprawdzaj, czy poprawnie identyfikujesz adres powrotu i przesunięcie (offset).
   - W razie potrzeby korzystaj z podpowiedzi na platformie (sekcja *Hints*).

Proces rozwiązania zadania OVERFLOW1 proszę udokumentować i przesłać w formie krótkiego sprawozdania



Zadanie dodatkowe - Sudo Buffer Overflow (CVE-2019-18634)

Otwórz pokój **Sudo Buffer Overflow**

- https://tryhackme.com/room/sudovulnsbof

Przeprowadź atak na podatną wersję sudo

- Zapoznaj się z opisem podatności oraz warunkami jej wyzwolenia (pwfeedback=1 w konfiguracji).
- Wygeneruj odpowiedni ładunek (*payload*) powodujący przepełnienie bufora i eskalację uprawnień.
- Odpowiedz na pytania kontrolne, aby ukończyć zadanie.