

UERJ Zona oeste

Jonatha Salles Menezes
2211312125

Lista 02 - Sistemas de numeração
INF5312 - Organização de computadores

Rio de Janeiro
2022

Exercício 04)

Buffer Overflow é uma das fraquezas de software mais comuns e perigosas. Pode ocorrer de repente ou através de ataques hackers, que reescrevem o limite de buffers (atribuir a uma variável um valor maior que o seu limite de comprimento, sobrescrevendo acessos anteriores à variável, causando diversos problemas à máquina). para ativar ações como enviar instruções ao aplicativo para, por exemplo, corromper máquinas. O que esse transbordamento de dados faz, na verdade, é, ao estourar o limite da variável, essa memória alocada à variável invade o espaço de outras funções na pilha, permitindo acesso total à máquina invadida, o que permite ao hacker controle sobre toda e qualquer função.

Exercício 08)

O complemento de 1 é a inversão de todos os bits a fim de obter seu complemento. Já o complemento de 2 possui duas etapas, primeiro obtém-se o complemento de 1 do número proposto, após isso, soma-se uma unidade ao número obtido.

O complemento de 2 é utilizado pelo computador para realizar operações de subtração ao somar o número maior ao complemento de 2 do número menor, para obter o complemento de 2 desse número menor, no entanto, iguala-se o número de bits dos dois números antes de invertê-los e somar uma unidade. Além disso, ao obter o resultado da soma, deve-se desconsiderar bits excedentes.

Referências:

[What is a Buffer Overflow Attack? - YouTube](#)

[Running a Buffer Overflow Attack - Computerphile - YouTube](#)

[binários: complemento de 1 e complemento de 2 - YouTube](#)