1.Buffer Overflow

O objetivo de um ataque de buffer overflow é encontrar uma falha relacionada à memória do sistema em um servidor e explorá-la sobrecarregando-a com valores inesperados, geralmente causando um DoS. Um ataque de buffer overflow ocorre quando um invasor escreve mais dados em uma área de memória do que o esperado, fazendo com que essa informação excedente transborde para áreas adjacentes da memória, potencialmente modificando o comportamento do programa. Normalmente, os desenvolvedores de aplicativos implementam verificações de limites para impedir que qualquer usuário escreva mais do que o espaço alocado permite. No entanto, atacantes buscam brechas nesses sistemas de segurança, testando várias partes do aplicativo para encontrar formas de manipular sua execução.

Apesar de ser um ataque bastante conhecido, explorá-lo não é simples. Mesmo que um invasor encontre uma vulnerabilidade de buffer overflow, adicionar dados inesperados à memória pode simplesmente fazer o sistema ou a aplicação falhar. Entretanto, se o ataque for bem planejado, ele pode modificar o funcionamento do programa de forma vantajosa para o invasor. O objetivo principal dos atacantes é encontrar um buffer overflow que possa ser repetido e utilizado de maneira confiável para obter acesso privilegiado ou executar comandos maliciosos.

Um exemplo clássico desse ataque envolve a elevação de privilégios dentro de um sistema. Imagine que há duas variáveis armazenadas na memória: a variável A, que pode armazenar 8 bytes de informação, e a variável B, que ocupa 2 bytes. Inicialmente, a variável A está vazia e a variável B contém o valor 1979, o que significa que o usuário tem permissões básicas dentro do sistema. Para conseguir privilégios administrativos, o invasor precisa modificar a variável B para que seu valor ultrapasse 24.000, algo que, em condições normais, não pode ser alterado dentro da própria aplicação.

Ao identificar que a variável A permite um buffer overflow, o atacante insere 9 caracteres em seu espaço. Como A só pode armazenar 8 caracteres, o nono acaba invadindo o espaço da variável B, alterando seu valor original. Se esse valor for modificado corretamente, ele pode ultrapassar o limite de 24.000, concedendo ao atacante direitos administrativos sem a necessidade de credenciais.