1.Vulnerabilidades de virtualização

Com a infraestrutura baseada em nuvem, é possível criar máquinas virtuais em questão de segundos e em grande quantidade simultaneamente. Enquanto a gestão de computadores físicos já apresenta desafios de segurança, administrar um ambiente em nuvem, onde máquinas virtuais são constantemente criadas e desativadas ao longo do dia, torna essa tarefa ainda mais complexa. Além disso, essas máquinas podem ter diferentes configurações, variando em número de CPUs, memória e capacidade de armazenamento, o que dificulta a padronização e a aplicação uniforme de medidas de segurança.

Assim como em dispositivos físicos, as máquinas virtuais operam com sistemas como Windows e Linux, exigindo a aplicação das mesmas práticas de segurança. No entanto, há vulnerabilidades específicas dos ambientes virtuais, como escalonamento de privilégios, injeção de comandos e vazamento de informações. Em teoria, uma máquina virtual deveria ser completamente isolada das outras no mesmo hipervisor, garantindo que seus recursos, como CPU e memória, não possam ser acessados por outras VMs. **No entanto, ataques conhecidos como VM escape já demonstraram que é possível explorar falhas para mover-se de uma máquina virtual para outra dentro do mesmo hipervisor**.

Um exemplo prático desse tipo de ataque ocorreu em março de 2017, no concurso de segurança **Pwn2Own**, onde pesquisadores conseguiram escapar de uma máquina virtual e acessar outra no mesmo ambiente. Utilizando uma falha no motor JavaScript do navegador Microsoft Edge, os invasores conseguiram contornar a sandbox do navegador. Em seguida, exploraram uma vulnerabilidade no kernel do Windows 10 para obter acesso total ao sistema operacional convidado. A partir daí, aproveitaram uma falha na simulação de hardware do VMware para pular de uma máquina virtual para outra no mesmo hipervisor. Felizmente, essa vulnerabilidade foi revelada durante a competição, permitindo que a VMware corrigisse o problema antes que ele pudesse ser explorado em larga escala.

Outro grande problema em ambientes virtuais é o **reuso de recursos**. Um hipervisor gerencia a alocação de memória, armazenamento e poder de processamento para diversas máquinas virtuais. Entretanto, como esses recursos são compartilhados, erros na alocação podem permitir que uma VM acesse inadvertidamente a memória de outra. Por exemplo, um hipervisor pode ter apenas 4 GB de RAM físicos, mas permitir que três máquinas virtuais utilizem 2GB cada, totalizando 6 GB virtualmente alocados. Para que isso funcione, o hipervisor precisa gerenciar dinamicamente a memória conforme a demanda. Se houver uma falha nesse gerenciamento, uma máquina pode acabar acessando dados que pertencem a outra, comprometendo a segurança.

Dessa forma, a segurança em ambientes virtuais depende tanto das práticas aplicadas às máquinas individuais quanto da integridade do próprio hipervisor. Manter

os sistemas operacionais atualizados, corrigir vulnerabilidades conhecidas e garantir que os hipervisores estejam sempre protegidos contra ataques são medidas essenciais para evitar violações e acessos não autorizados.