1.Teste de penetração

O **Penetration Testing (Pen Test)** é um processo de simulação de ataques a sistemas próprios para identificar vulnerabilidades de segurança. Diferente de uma simples varredura de vulnerabilidades, o Pen Test envolve a exploração real dessas falhas para verificar se um invasor conseguiria acesso. Muitas organizações realizam testes periódicos por boas práticas de segurança ou por exigências regulatórias. O **NIST (National Institute of Standards and Technology)** disponibiliza um guia técnico para testes e avaliações de segurança, útil para compreender esse processo.

Antes de iniciar um Pen Test, é essencial definir as **regras de engajamento** (rules of engagement), que especificam os limites do teste, como horários permitidos, sistemas que podem ser testados e contatos de emergência. Algumas empresas restringem testes a horários fora do expediente para evitar impactos nos sistemas de produção. Além disso, deve-se documentar como lidar com informações sensíveis encontradas durante o teste.

Durante a execução do Pentest, o objetivo principal é explorar vulnerabilidades conhecidas para obter acesso aos sistemas. Entretanto, algumas técnicas, como **buffer overflow**, podem causar falhas nos sistemas, o que reforça a importância das regras de engajamento. Existem diferentes métodos de ataque, como **força bruta de senhas, engenharia social, injeção de banco de dados** e **exploração de falhas de software**.

Caso um invasor consiga acessar um sistema, ele pode usar essa máquina como um **ponto de pivô**, permitindo movimentação lateral dentro da rede. Para manter o acesso, atacantes frequentemente instalam **backdoors**, criam contas ocultas ou alteram senhas de administradores. Muitas redes possuem firewalls para impedir acessos externos, mas, uma vez dentro, invasores podem usar máquinas comprometidas como **relays** para explorar outros dispositivos.

A descoberta e correção de vulnerabilidades seguem um processo longo. Inicialmente, um pesquisador de segurança identifica uma falha e notifica o desenvolvedor do software. A correção envolve análise, testes e lançamento de uma atualização. Somente após a disponibilização do patch a vulnerabilidade é tornada pública e registrada em listas como o **CVE (Common Vulnerabilities and Exposures)**. Esse processo pode levar semanas ou meses.

Para incentivar a descoberta responsável de falhas, muitas empresas oferecem **bug bounties** (recompensas por vulnerabilidades encontradas). Nesses programas, pesquisadores identificam e reportam falhas para que possam ser corrigidas antes que sejam exploradas por criminosos. Dessa forma, os **bug bounties** ajudam a fortalecer a segurança cibernética, beneficiando tanto as empresas quanto os usuários.