1.Testes de penetração

Muitas vezes pensamos em testes de penetração como algo feito digitalmente pela internet, mas os testes de penetração físicos também são uma ferramenta importante de segurança. Isso ocorre porque é extremamente fácil contornar a segurança de um sistema operacional quando se tem acesso físico ao dispositivo. Com esse acesso, é possível modificar o processo de inicialização, inicializar o sistema a partir de outra mídia ou alterar arquivos do sistema operacional. Por essa razão, servidores costumam ser mantidos em data centers altamente seguros, onde a segurança física é essencial.

Quando uma empresa realiza um teste de penetração físico, o objetivo é tentar obter acesso às suas instalações. Os testadores tentam entrar no prédio sem uma chave, avaliar os acessos disponíveis dentro do edifício e explorar todas as formas possíveis de entrada, incluindo portas, janelas e elevadores.

Os testes de penetração costumam ser vistos como uma ação ofensiva, mas há diferentes abordagens. A equipe vermelha (red team) é responsável por atacar os sistemas, identificar vulnerabilidades e explorá-las. Já a equipe azul (blue team) trabalha na defesa, identificando ataques em tempo real e bloqueando-os. A melhor abordagem é a integração dessas equipes para criar um sistema de segurança que constantemente se autoavalia: a equipe vermelha ataca, encontra brechas e passa essas informações para a equipe azul, que corrige e fortalece a defesa.

Os testes de penetração podem ser realizados com diferentes níveis de informação sobre o ambiente. Se o testador recebe todos os detalhes do sistema antes do teste, ele trabalha com um ambiente conhecido. Em um ambiente parcialmente conhecido, apenas algumas informações são fornecidas. Já no ambiente desconhecido (ou teste cego), o testador precisa descobrir tudo por conta própria.

Independentemente do tipo de teste, o processo sempre começa com a fase de reconhecimento, onde os testadores coletam o máximo de informações sobre o ambiente. Isso inclui identificar ferramentas de segurança, servidores e aplicativos em uso. Com essas informações, é possível mapear a rede, listar os endereços IP e entender a infraestrutura.

O reconhecimento pode ser passivo ou ativo. **No reconhecimento passivo, os testadores coletam informações sem interagir diretamente com a rede da empresa**, utilizando fontes como redes sociais, sites corporativos, fóruns e até engenharia social, onde tentam obter dados de funcionários ou parceiros da organização. Em casos extremos, podem até buscar documentos descartados no lixo (dumpster diving).

Já o reconhecimento ativo envolve interagir diretamente com a rede da empresa, como realizar varreduras de portas e serviços, consultas a servidores

DNS ou fingerprinting de sistemas operacionais. Esse tipo de reconhecimento é mais arriscado, pois deixa rastros em arquivos de log, podendo alertar os administradores da rede.

Os testes de penetração são essenciais para identificar vulnerabilidades e fortalecer a segurança das organizações, seja no ambiente digital ou físico.