1.Introdução à invasão de computadores

1.1 Reconhecimento ativo

O reconhecimento ativo envolve a interação direta com o alvo. Isso pode incluir varredura de portas, solicitações de DNS, pings e outras atividades que geram tráfego e podem ser detectadas pelo sistema ou pela equipe de segurança. O reconhecimento ativo apresenta maior risco de detecção. As técnicas ativas podem envolver a obtenção de acesso físico às instalações ou o uso de ferramentas de varredura nos serviços da web e em outras redes do alvo. Exemplos estão descritos abaixo

- **Engenharia social:** Refere-se à obtenção de informações, acesso físico às instalações ou mesmo acesso a uma conta de usuário através da arte da persuasão. Embora a quantidade de interação possa variar, isso pode ser classificado como uma técnica ativa.
- **Footprinting:** Usando ferramentas de software, como Nmap (nmap.org), para obter informações sobre um host ou topologia de rede. As varreduras podem ser iniciadas em hosts da web ou em segmentos de rede com ou sem fio, se o investigador puder obter acesso físico a eles.
- **Varredura de portas:** Identificar quais portas estão abertas e quais serviços estão em execução.
- **Solicitações de DNS:** Descobrir informações sobre a infraestrutura de rede.
- **Ping sweeps:** Identificar hosts ativos na rede.
- **Banner grabbing:** Coletar informações dos banners de serviços em execução.

Vantagens incluem fornecer informações detalhadas e em tempo real, úteis para identificar vulnerabilidades específicas. É útil para testar a resiliência do alvo a varreduras ativas. Desvantagens incluem poder ser detectado pelo alvo, resultando em bloqueio ou alerta de segurança. Pode ser invasivo e perturbar as operações normais.

1.2 Reconhecimento passivo

Em contraste, o reconhecimento passivo é mais discreto e envolve a coleta de informações sem interação direta com o alvo. Isso pode incluir monitoramento de tráfego de rede, análise de logs, pesquisa de informações publicamente disponíveis (OSINT), entre outras técnicas que não perturbam o alvo. Exemplos estão descritos abaixo.

- **Monitoramento de tráfego de rede:** Observar o tráfego para identificar padrões e sistemas ativos.
- **Análise de logs:** Examinar logs de eventos e registros de sistemas em busca de informações úteis.
- **Pesquisa OSINT:** Ferramentas de agregação OSINT, como theHarvester, coletam e organizam esses dados de diversas fontes. OSINT quase não requer acesso privilegiado, pois depende da localização de informações que a empresa disponibiliza publicamente, intencionalmente ou não. Coleta informações disponíveis publicamente sobre alvos, como endereços de IP, nomes de domínio, informações de registro WHOIS etc.

Vantagens geralmente incluem passar despercebido e não perturbar o alvo. É útil para coletar informações gerais sobre a infraestrutura do alvo. Desvantagens incluem poder fornecer informações menos detalhadas e mais antigas, não sendo ideal para identificar vulnerabilidades específicas.

2.Pentest (teste de penetração)

Um teste de penetração, também conhecido como pentest, é uma simulação controlada de um ataque cibernético realizado em um sistema, rede ou aplicação para avaliar sua segurança. Os testes de penetração são uma parte crítica da estratégia de segurança cibernética, permitindo que as organizações avaliem sua postura de segurança e tomem medidas proativas para mitigar riscos.

A importância dos testes de penetração reside em sua capacidade de identificar vulnerabilidades antes que atacantes maliciosos o façam. Isso permite que as organizações fortaleçam suas defesas e protejam informações confidenciais. A ética e a conformidade em testes de penetração são fundamentais. Isso inclui o respeito às leis e regulamentações, a obtenção de autorização adequada, notificação das partes interessadas e a importância de documentar e relatar todas as atividades.

Os testes de penetração incluem:

- Identificar vulnerabilidades, fraquezas e deficiências na segurança de um ambiente. Mapear pontos fracos em sistemas, redes e aplicativos
- Avaliar a eficácia das medidas de segurança existentes
- Medir a capacidade de uma organização de detectar e responder a ameaças cibernéticas
- Fornecer recomendações para melhorar a segurança e reduzir riscos

As fases de um pentest incluem:

- **Planejamento:** Nesta fase, são definidos os objetivos do teste, o escopo e a metodologia a ser utilizada. É essencial obter a aprovação da alta administração e garantir a legalidade do teste.
- **Coleta de informações:** Os testadores reúnem informações sobre o alvo, incluindo sistemas, redes e aplicativos a serem avaliados. Isso pode envolver varredura de DNS, coleta de informações WHOIS e identificação de alvos potenciais.
- **Análise:** Durante essa fase, os testadores analisam as informações coletadas e desenvolvem estratégias de ataque. São identificadas possíveis vulnerabilidades e fraquezas que serão exploradas.
- **Exploração:** Esta é a fase em que as técnicas de ataque são implementadas para explorar as vulnerabilidades identificadas. Os testadores tentam ganhar acesso não autorizado ou explorar fraquezas de segurança.
- **Documentação:** Todos os detalhes do teste são registrados de forma detalhada, incluindo os métodos, resultados e descobertas. Essa documentação é crucial para o próximo passo.

- **Relatório:** Um relatório abrangente é gerado com todas as descobertas, riscos identificados e recomendações para correção. Este relatório é entregue à equipe de segurança e à alta administração.

2.1 Ciclo de vida do ataque de pentest

A fase do ciclo de vida do ataque de pentest é fundamental para a realização de testes de penetração de forma organizada e eficaz. A kill chain é um termo comumente utilizado em segurança cibernética e defesa cibernética para descrever as etapas sequenciais que um atacante segue durante um ataque cibernético, desde o planejamento inicial até a execução e exploração bem-sucedida de um sistema ou rede. Essas etapas são projetadas para representar o ciclo de vida típico de um ataque e podem ser usadas para entender, analisar e defender-se contra ameaças cibernéticas. A ideia por trás da kill chain é que, se uma organização for capaz de identificar e interromper uma etapa da cadeia, poderá impedir um ataque cibernético antes que ele tenha sucesso.

2.2 Cyber Killchain - Reconhecimento

Nesta fase, o testador de penetração reúne informações sobre o alvo, como redes, sistemas e aplicativos a serem testados, identificação de vulnerabilidades, sistemas em uso, funcionários, parceiros e outros detalhes relevantes. Isso pode incluir varredura de DNS, pesquisa de informações publicamente disponíveis (OSINT) e outras técnicas.

2.3 Cyber Killchain - Exploração

O testador busca vulnerabilidades nos sistemas e aplicativos identificados durante a fase de reconhecimento. Isso pode envolver a exploração de falhas de segurança conhecidas ou a busca por fraquezas específicas. Nesse momento, uma ferramenta de software é usada para obter algum tipo de acesso à rede do alvo. Isso pode ser feito usando um e-mail e payload de phishing ou obtendo credenciais por meio de engenharia social.

2.4 Cyber Killchain - Persistência

Após a exploração bem-sucedida, o testador estabelece uma presença persistente no sistema, geralmente por meio da instalação de backdoors ou outras ferramentas. Trata-se da capacidade do testador de se reconectar ao host comprometido e usá-lo como uma ferramenta de acesso remoto (RAT) ou backdoor. Para fazer isso, o testador deve estabelecer uma rede de comando e controle (C2 ou C&C) usando para controlar o host comprometido, carregar ferramentas de ataque adicionais e baixar dados exfiltrados. A conexão com o host comprometido normalmente exigirá que um executável de malware seja executado após eventos de desligamento/logoff e que uma conexão com uma porta de rede e o endereço IP do invasor estejam disponíveis.

2.5 Cyber Killchain - Escalonamento de privilégios

A persistência é seguida por um reconhecimento adicional, onde o pen tester tenta mapear a rede interna e descobrir os serviços em execução nela e as contas configuradas para acessá-la. Mover-se dentro da rede ou acessar ativos de dados provavelmente exigirá níveis de

privilégio mais elevados. Outra exploração pode permitir que o malware seja executado com privilégios de sistema/root ou use privilégios de administrador de rede em outros hosts, como servidores de aplicativos. Se o objetivo for obter acesso privilegiado, o testador busca maneiras de aumentar suas permissões e níveis de acesso.

2.6 Cyber Killchain - Movimento lateral/pivotagem

Ganhando controle sobre outros hosts. O testador explora a rede, procurando outros sistemas para se movimentar lateralmente dentro da organização. Isso é feito em parte para descobrir mais oportunidades de ampliar o acesso, em parte para identificar onde ativos de dados valiosos podem estar localizados e em parte para evitar a detecção. O movimento lateral geralmente envolve a execução de ferramentas de ataque em compartilhamentos de processos remotos ou o uso de ferramentas de script, como o PowerShell. Se o pentester conseguir uma posição segura em um servidor de perímetro, um pivô permitirá que ele contorne um limite de rede e comprometa servidores em uma rede interna. Um pivô normalmente é realizado usando protocolos de acesso remoto e tunelamento, como Secure Shell (SSH), rede privada virtual (VPN) ou área de trabalho remota.

2.7 Cyber Killchain - Ações baseadas em objetivos

Esta é a fase em que o testador executa ações maliciosas planejadas, como roubo de dados, danos ao sistema, interrupção de operações ou outros objetivos específicos. Para um agente de ameaça, isso significa roubar dados de um ou mais sistemas (exfiltração de dados).

2.8 Cyber Killchain - Fases de limpeza

Após concluir o teste de penetração, o testador remove todos os vestígios de sua presença no sistema, garantindo que não deixe rastros indesejados. Para um autor da ameaça, isso significa remover evidências do ataque, ou pelo menos evidências que possam implicar o autor da ameaça. Para um pentester, essa fase significa remover quaisquer backdoors ou ferramentas e garantir que o sistema não seja menos seguro do que o estado de pré-engajamento.

3.Importância de relatórios detalhados e documentação

A documentação adequada é um aspecto crucial de um teste de penetração. Os relatórios detalhados não apenas registram as atividades realizadas, mas também fornecem informações essenciais para que a organização possa corrigir vulnerabilidades e melhorar sua segurança cibernética. Os relatórios de testes de penetração devem ser claros, concisos e fornecer informações relevantes. Eles geralmente incluem:

- Uma visão geral do escopo do teste
- Detalhes das atividades realizadas em cada fase
- Vulnerabilidades identificadas e seu impacto
- Recomendações para mitigação
- Evidências que comprovam as descobertas
- Informações sobre a conformidade com as regras de engajamento
- Uma análise de riscos e impacto