1.Técnicas utilizadas na classificação de ameaças

1.1 Avaliações de segurança

O reconhecimento e descoberta de rede são usados para identificar hosts, topologia de rede e serviços/portas abertas, estabelecendo uma superfície de ataque geral. Vários tipos de avaliações de segurança podem ser usados para testar vulnerabilidades em hosts e serviços. Existem muitos modelos e frameworks para a realização de avaliações de segurança.

Um bom exemplo é a Special Publication SP 800-115, do NIST, que identifica três atividades principais dentro de uma avaliação:

- Testar o objetivo em avaliação para descobrir vulnerabilidades ou comprovar a eficácia dos controles de segurança
- Examinar objetos de avaliação para compreender o sistema de segurança e identificar quaisquer pontos fracos e lógicos. Isso pode destacar a falta de controles de segurança ou uma configuração incorreta comum
- Entrevistar pessoal para recolher informações e sonar atitudes e compreensão da segurança

Os principais tipos de avaliação de segurança são geralmente classificados como verificação de vulnerabilidade, caça a ameaças e testes de penetração. Essencialmente, a avaliação de vulnerabilidade determina se a configuração atual corresponde à configuração ideal. Elas podem envolver a inspeção manual dos controles de segurança, mas são mais frequentemente realizadas por meio de scanners automatizados de vulnerabilidade.

A verificação de vulnerabilidade é uma parte essencial da gestão de riscos de segurança cibernética e ajuda as organizações a entender e reduzir os riscos à medida que mantêm a integridade e a confidencialidade de seus sistemas e dados. As descobertas da verificação de vulnerabilidade são geralmente usadas para priorizar a implementação de medidas de segurança, como correções de software, configurações seguras e políticas de acesso.

1.2 Técnicas de verificação de vulnerabilidades

A verificação de vulnerabilidade, ou avaliação de vulnerabilidade, é o processo de identificação, avaliação e análise das fraquezas e falhas de segurança em sistemas, redes, aplicativos ou infraestrutura de tecnologia da informação.

O objetivo da verificação é identificar e documentar as vulnerabilidades existentes, avaliar seu impacto e probabilidade de exploração e, em seguida, recomendar medidas para mitigar ou corrigir essas falhas. Isso ajuda a fortalecer a segurança dos sistemas e a reduzir o risco de incidentes de segurança.

As técnicas de verificação de vulnerabilidades podem ser categorizadas em dois grupos principais descritos mais abaixo.

1.3 Varreduras automatizadas

Elas envolvem o uso de software especializado que examina sistemas e redes em busca de vulnerabilidades conhecidas. Essas ferramentas são eficientes para identificar uma ampla gama de vulnerabilidades em um curto espaço de tempo. No entanto, elas podem não ser capazes de detectar vulnerabilidades novas ou personalizadas. Uma varredura automatizada deve ser configurada com assinaturas e scripts que possam correlacionar software conhecido e vulnerabilidades de configuração com dados coletados de cada host. Consequentemente, existem vários tipos de scanners de vulnerabilidade otimizados para diferentes tarefas. A seleção da ferramenta adequada depende dos requisitos específicos de verificação de vulnerabilidade e do ambiente em questão. Algumas destas ferramentas são: Nmap, OpenVAS, Nessus, Burp Suite e Wireshark.

1.4 Testes e varreduras manuais

Elas envolvem a análise minuciosa de sistemas por profissionais de segurança cibernética. Eles usam suas habilidades e conhecimentos para identificar vulnerabilidades que as ferramentas automatizadas podem não detectar. Os testes manuais são particularmente úteis para avaliar a segurança de sistemas complexos e personalizados.

Um scanner automatizado precisa ser mantido atualizado com informações sobre vulnerabilidades conhecidas. Essas informações costumam ser descritas como feed de vulnerabilidade, os quais utilizam identificadores comuns para facilitar o compartilhamento de dados de inteligência entre diferentes plataformas.

O Common Vulnerabilities and Exposures (CVE), ou Vulnerabilidades e Exposições Comuns, é um sistema internacional de identificação e nomeação de vulnerabilidades de segurança cibernética em sistemas de software e hardware. O CVE é mantido e gerenciado pela organização MITRE Corporation, em colaboração com diversas entidades de segurança cibernética em todo o mundo. É uma iniciativa global que conta com a colaboração de muitos especialistas em segurança cibernética em todo o mundo para identificar, nomear e documentar vulnerabilidades.

O sistema de nomeação do CVE segue um padrão bem definido, facilitando a comunicação e referência a vulnerabilidades de forma consistente em todo o setor de segurança cibernética. Seu principal objetivo é fornecer uma lista padronizada de identificadores únicos para vulnerabilidades conhecidas, tornando mais fácil para as organizações e os profissionais de segurança cibernética compartilharem informações sobre vulnerabilidades, coordenarem esforços de correção e facilitarem a integração de informações de segurança em sistemas de segurança e ferramentas de verificação de vulnerabilidades.

Existem vários elementos que compõem a entrada de uma vulnerabilidade no CVE:

- **Um identificador no formato:** CVE-YYYY-####, onde YYYY é o ano em que a vulnerabilidade foi descoberta e #### tem pelo menos quatro dígitos que indicam a ordem em que a vulnerabilidade foi descoberta.

- **Descrição da vulnerabilidade:** Cada entrada CVE contém informações sobre a vulnerabilidade, incluindo uma descrição do problema, seu impacto potencial, as versões afetadas do software ou hardware e quaisquer soluções ou correções disponíveis.
- **Uma lista de referência de URLs:** Fornecem mais informações sobre a vulnerabilidade. As informações listadas no CVE são de acesso público e podem ser consultadas por qualquer pessoa, incluindo profissionais de segurança, desenvolvedores de software e pesquisadores.
- **A data de entrada da vulnerabilidade:** O dia em que a vulnerabilidade foi posta no banco de dados CVE.

1.5 Verificação intrusiva (ativa)

As varreduras intrusivas envolvem ações que podem impactar o sistema ou rede verificados. Isso significa que o processo de verificação pode interromper o funcionamento normal dos sistemas, causar quedas de serviço ou potencialmente explorar vulnerabilidades de maneira ativa. A varredura ativa significa testar a configuração do dispositivo usando algum tipo de conexão de rede com o alvo. Consome mais largura de banda da rede e corre o risco de travar o alvo da varredura ou causar algum outro tipo de interrupção.

O tipo mais intrusivo de scanner de vulnerabilidade não para na detecção de uma vulnerabilidade. As estruturas de exploração contêm scripts padrão para tentar usar uma vulnerabilidade para executar código ou obter acesso ao sistema. Um exemplo de uma varredura intrusiva é uma tentativa de autenticação com credenciais incorretas para testar a resistência a tentativas de login não autorizadas.

- **Vantagens:** As varreduras intrusivas podem identificar vulnerabilidades que varreduras não intrusivas podem perder, já que elas exploram ativamente as fraquezas. São úteis para verificar a exploração real de vulnerabilidades e avaliar a resistência a ataques.
- **Desvantagens:** O principal inconveniente das varreduras intrusivas é o potencial para causar impacto adverso nos sistemas verificados, como interrupções de serviço. Portanto, devem ser realizadas com cautela e geralmente em ambientes controlados.

1.6 Verificação não intrusiva

São projetadas para serem não perturbadoras e não causar impacto nos sistemas verificados. Elas observam os sistemas e redes de fora, sem tentar explorar ativamente vulnerabilidades. A varredura não intrusiva (ou passiva) significa analisar evidências indiretas, como os tipos de tráfego gerados por um dispositivo.

Esse tipo de verificação tem o menor impacto na rede e nos hosts, mas é menos provável que identifique vulnerabilidades de forma abrangente. Você pode usar a varredura passiva como uma técnica onde a varredura ativa representa um sério risco à estabilidade do sistema, como a varredura de dispositivos de impressão, dispositivos VoIP ou sistemas de rede integrados.

Uma varredura não intrusiva pode incluir a coleta de informações por meio de análise de tráfego de rede, pesquisa de informações publicamente disponíveis, análise de configurações de sistemas e verificação de portas abertas.

- **Vantagens:** Varreduras não intrusivas são seguras e não causam interrupções. São ideais para monitorar a superfície de ataque e identificar vulnerabilidades sem perturbar o funcionamento normal dos sistemas.
- **Desvantagens:** Podem não detectar vulnerabilidades que requerem exploração ativa. A verificação passiva pode ser usada por um agente de ameaça para verificar uma rede furtivamente. Em alguns casos, informações limitadas podem estar disponíveis para avaliar completamente o risco

Varreduras intrusivas e não intrusivas são duas abordagens diferentes usadas na verificação de vulnerabilidades e na avaliação de segurança de sistemas e redes. Elas diferem em sua natureza e no impacto que têm nos sistemas e na infraestrutura durante o processo de verificação. A intrusividade da varredura é uma medida de quanto o scanner interage com o alvo.

1.7 Varreduras credenciada

Nas varreduras credenciadas, o processo de verificação de vulnerabilidades envolve o uso de credenciais válidas, como nomes de usuário e senhas, para autenticar-se nos sistemas ou dispositivos sendo analisados, além de quaisquer outras permissões apropriadas para as rotinas de teste. O acesso com credenciais permite que a ferramenta de verificação acesse áreas mais profundas e restritas dos sistemas, como arquivos e configurações sensíveis. Isso resulta em uma verificação mais completa e precisa.

- **Vantagens:** As varreduras credenciadas tendem a fornecer resultados mais detalhados e precisos, identificando vulnerabilidades que podem não ser visíveis para varreduras não credenciadas. Elas são particularmente eficazes na identificação de problemas de configuração e atualização.
- **Desvantagens:** Exige a cooperação dos proprietários dos sistemas, pois o acesso com credenciais deve ser concedido. Além disso, pode ser mais demorado e complexo de configurar.

1.8 Varredura não credenciada

Nas varreduras não credenciadas, a ferramenta de verificação não faz uso de credenciais válidas. É aquela que direciona pacotes de teste para um host sem ser capaz de fazer logon no sistema operacional ou no aplicativo. Ela examina sistemas e redes de fora, como um observador externo. A visão obtida é aquela que o host expõe a um usuário sem privilégios na rede. A ausência de credenciais restringe o acesso a áreas restritas dos sistemas, o que significa que a verificação é limitada a informações e configurações disponíveis publicamente.

- **Vantagens:** As varreduras não credenciadas são rápidas e não exigem a cooperação dos proprietários dos sistemas, tornando-as mais fáceis de implementar. Elas são úteis para identificar vulnerabilidades que podem ser exploradas por invasores externos.

Embora seja possível descobrir mais pontos fracos com uma verificação credenciada, às vezes pode ser necessário restringir o foco para pensar como um invasor que não possui permissões específicas de alto nível, ou acesso administrativo total.

- **Desvantagens:** As varreduras não credenciadas podem não detectar vulnerabilidades internas devido à falta de acesso com credenciais, como problemas de configuração e atualização, que seriam identificadas em varreduras credenciadas.

A escolha entre varreduras credenciadas e não credenciadas depende dos objetivos da avaliação de segurança e das circunstâncias específicas. Em muitos casos, é recomendável usar ambas as abordagens, permitindo uma análise abrangente que aborde vulnerabilidades internas e externas.

2.Falsos positivos

Em varreduras de vulnerabilidades, um falso positivo ocorre quando a ferramenta de verificação identifica erroneamente uma vulnerabilidade que na realidade não existe no sistema ou rede. Isso pode acontecer devido a falsas interpretações, configurações inadequadas ou limitações da ferramenta de verificação. Falsos positivos podem levar a tempo desperdiçado na investigação e correção de problemas inexistentes.

Por outro lado, o verdadeiro positivo ocorre em um teste de detecção ou classificação quando o resultado indica corretamente a presença de uma condição ou característica que está presente de fato.

2.1 Falsos negativos

Por outro lado, um falso negativo ocorre quando a ferramenta de verificação não detecta uma vulnerabilidade real que está presente no sistema ou rede. Isso pode acontecer devido a falhas na detecção da ferramenta, configurações inadequadas ou falta de visibilidade na varredura. Falsos negativos podem ser particularmente perigosos, pois significam que vulnerabilidades reais não estão sendo tratadas, colocando em risco a segurança.

O verdadeiro negativo, por sua vez, ocorre quando um teste indica corretamente a ausência de uma condição ou característica que realmente não está presente.

3.Análise de logs

A revisão dos logs de rede e do sistema relacionados pode aprimorar o processo de validação do relatório de vulnerabilidade. A análise de logs auxilia na confirmação dos resultados de varreduras. Ela envolve a revisão de registros de eventos e atividades de sistemas, aplicativos e redes para verificar se as vulnerabilidades identificadas pelas ferramentas de verificação são genuínas ou não.

- **Vantagens:** A análise de logs ajuda a distinguir entre falsos positivos e vulnerabilidades reais. Ao examinar registros de eventos, os administradores de segurança podem rastrear a atividade que levou à identificação da vulnerabilidade. Se não houver evidências nos logs de que a vulnerabilidade foi explorada, pode ser um

falso positivo. Se os registros mostrarem tentativas ou atividades suspeitas que não foram identificadas pela ferramenta de verificação, isso pode indicar a presença de vulnerabilidades não detectadas.

- **Desvantagens:** Os registros de logs podem gerar volumes enormes de dados e exigir recursos significativos em termos de hardware e software, incluindo armazenamento, capacidade de processamento e ferramentas de análise. Podem conter uma grande quantidade de informações irrelevantes ou triviais (ruído), como registros de eventos de rotina. Os logs de diferentes sistemas e aplicativos podem usar formatos e estruturas diferentes (falta de padronização), o que torna a análise de logs mais desafiadora. A retenção inadequada de registros pode limitar a capacidade de análise de logs.

Uma ferramenta de verificação vai gerar um relatório resumido de todas as vulnerabilidades descobertas durante a verificação, logo após a conclusão da execução. Esses relatórios codificam as vulnerabilidades por cores em termos de sua criticidade, com o vermelho normalmente denotando uma fraqueza que requer atenção imediata. Geralmente, podemos visualizar vulnerabilidades por escopo (mais críticas em todos os hosts) ou por host.