Módulo 3 - Aulas 1 e 2

Módulo 3: Técnicas utilizadas na identificação de ameaças

Aula 1: Gerenciamento de vulnerabilidades

Objetivos

- [x] Compreender os conceitos-chave do gerenciamento de vulnerabilidades.
- [x] Assimilar as técnicas e os métodos de verificação.
- [x] Conhecer avaliações e interpretar resultados de varreduras de segurança.

Conceitos

- [x] Verificação de vulnerabilidades, técnicas e tipos.
- [x] Avaliação de segurança.
- [x] Varredura credenciada/não credenciada e falsos positivos/falsos negativos.

Introdução

Bem-vindos à aula sobre gerenciamento de vulnerabilidades. Nosso propósito é explorar um dos temas fundamentais da segurança cibernética: a identificação e o tratamento de vulnerabilidades em sistemas e redes. Em um cenário onde a cibersegurança desempenha um papel crucial na proteção de informações sensíveis e na garantia da integridade de sistemas críticos, compreender e gerenciar vulnerabilidades é essencial. A exploração de vulnerabilidades é um dos métodos mais comuns usados por cibercriminosos para comprometer sistemas e causar danos.

Nesta aula, abordaremos uma série de tópicos-chave, desde as técnicas de verificação de vulnerabilidades até a análise de resultados de varreduras de segurança. Você aprenderá sobre vulnerabilidades e exposições comuns e explorará os diferentes métodos de verificação, incluindo varreduras intrusivas e não intrusivas.

Além disso, discutiremos a importância das avaliações de segurança e como elas desempenham um papel crítico na identificação de vulnerabilidades. Você também entenderá a diferença entre varreduras credenciadas e não credenciadas, juntamente com a análise de falsos positivos e falsos negativos, que são conceitos fundamentais para a precisão das verificações de vulnerabilidade.

Por fim, abordaremos a revisão de configurações, uma etapa importante no processo de garantir a segurança dos sistemas. Ao final desta aula, você terá uma compreensão mais clara dos princípios do gerenciamento de vulnerabilidades e estará mais preparado para contribuir para a segurança de sistemas e redes.

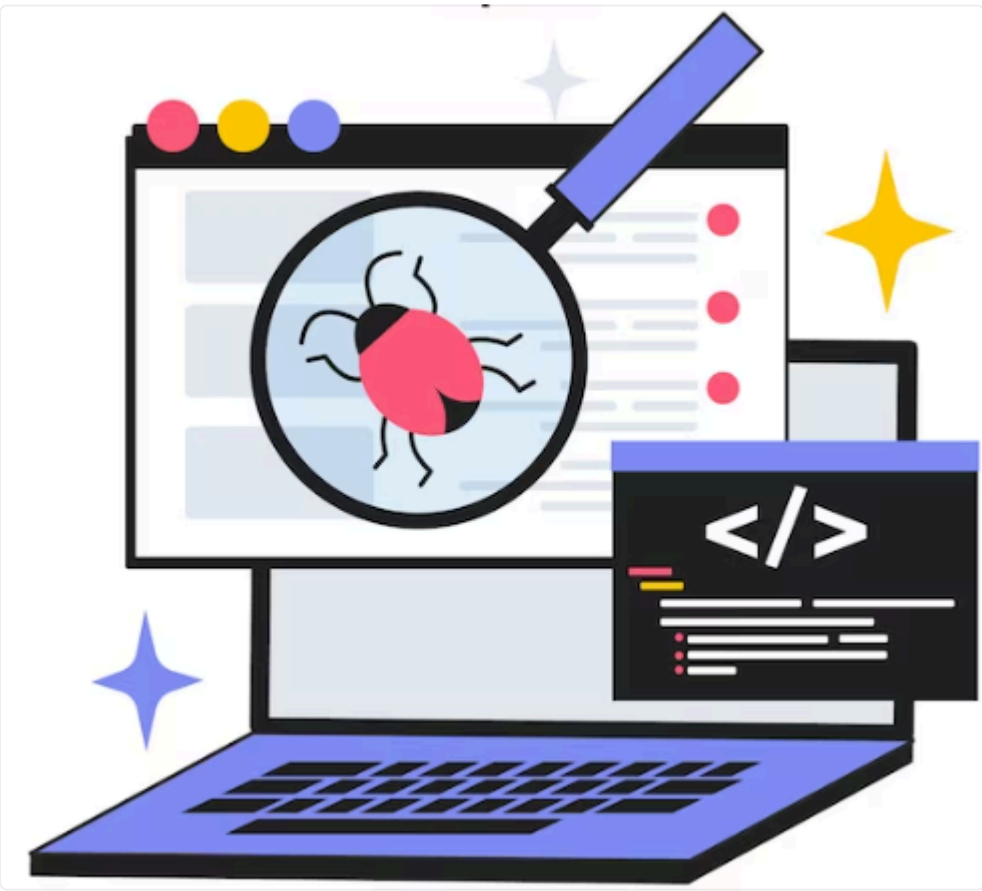
Avaliações de segurança

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 objeto 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 lógicos. Isso pode destacar a falta de controles de segurança ou uma configuração incorreta comum.
- Entrevistar pessoal para recolher informações e sondar 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. Trataremos neste momento da verificação de vulnerabilidades, cujo conceito pode ser definido como uma avaliação da segurança e da capacidade de um sistema de atender aos requisitos de conformidade com base no estado de configuração do sistema. Essencialmente, a avaliação de vulnerabilidade determina se a configuração atual corresponde à configuração ideal (a linha de base). 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.



Verificação de vulnerabilidades.

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. Essas fraquezas, conhecidas como "vulnerabilidades", podem ser exploradas por indivíduos mal-intencionados, como hackers, para comprometer a segurança dos sistemas e acessar informações confidenciais ou causar danos.

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: varreduras automatizadas e testes manuais. Ambas as abordagens têm seu lugar na caixa de ferramentas de segurança cibernética e são frequentemente usadas em conjunto para garantir uma cobertura abrangente. As características principais de cada abordagem são:

1. **Varreduras automatizadas**: 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. Além disso, é importante manter essas ferramentas atualizadas, pois novas vulnerabilidades são descobertas regularmente. Existem muitas ferramentas populares disponíveis para realizar varreduras automatizadas em sistemas e redes. Algumas delas incluem:

- **Nmap (Network Mapper)**: ferramenta de código aberto usada para descobrir dispositivos em redes e verificar quais portas estão abertas e quais serviços estão em execução.

- **OpenVAS (Open Vulnerability Assessment System)**: estrutura de verificação de vulnerabilidades que inclui um scanner de código aberto.
- **Nessus**: ferramenta de varredura de vulnerabilidades amplamente utilizada, que ajuda a identificar vulnerabilidades em sistemas e redes.
- **Burp Suite**: ferramenta de teste de segurança de aplicativos da web que ajuda a encontrar vulnerabilidades em sites e aplicativos da web.
- **Wireshark**: ferramenta de análise de tráfego de rede que pode ser usada para examinar o tráfego em busca de anomalias e potenciais vulnerabilidades.

2. **Testes manuais**: 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.

Vulnerabilidades e exposições comuns

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.

Trata-se de um dicionário de vulnerabilidades em sistemas operacionais e softwares aplicativos publicado (cve.mitre.org). 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:

1. **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.
2. **Descrição da vulnerabilidade**: cada entrada CVE contém informações sobre a vulnerabilidade, incluindo uma descrição do problema, seu impacto potencial, as

3. **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.
versões afetadas do software ou hardware e quaisquer soluções ou correções disponíveis.
4. **A data em que a entrada de vulnerabilidade foi criada**.

CVE.

Verificação intrusiva e não intrusiva

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. Aqui está uma explicação de cada uma delas:

1. **Varreduras intrusivas**: as varreduras intrusivas (ou ativas) 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. A varredura baseada em agente também é uma técnica ativa.

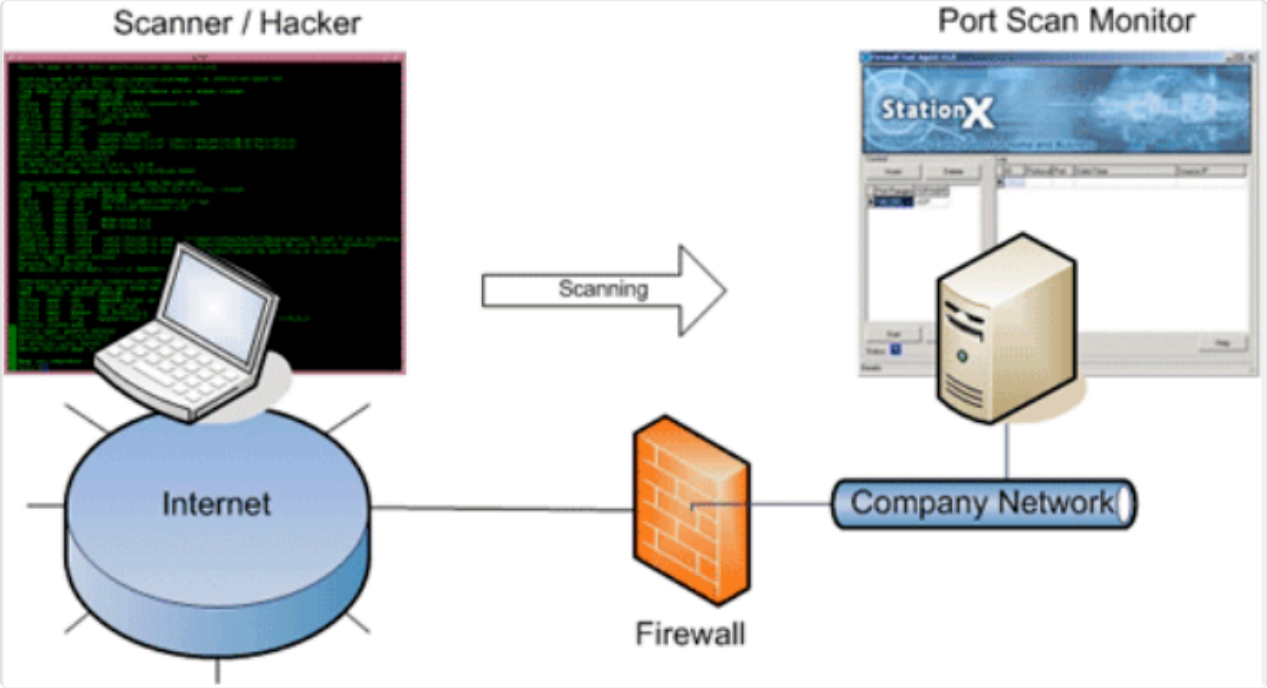
- **Exemplo de verificação intrusiva**: o tipo mais intrusivo de scanner de vulnerabilidade não para na detecção de uma vulnerabilidade. As estruturas de exploração contêm scripts padrão para tentar usar uma vulnerabilidade para executar código ou obter acesso ao sistema. Um exemplo de uma varredura intrusiva é uma tentativa de autenticação com credenciais incorretas para testar a resistência a tentativas de login não autorizadas. Outro exemplo é o uso de exploits ou técnicas de invasão para verificar se uma vulnerabilidade é realmente explorável.
- **Vantagens**: 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.

2. **Varreduras não intrusivas**: 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. Um scanner passivo, sendo o Zeek Network Security Monitor (zeek.org) um exemplo, analisa uma captura de rede e tenta identificar desvios de política ou correspondências de CVE. 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.

- **Exemplo de verificação não intrusiva**: 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.



Varredura de portas.

Varredura credenciada versus não credenciada

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. A seguir, veremos as diferenças entre varreduras credenciadas e não credenciadas em contextos de verificação de vulnerabilidades e avaliações de segurança:

1. **Varredura 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. Também mostra o que um ataque interno, ou aquele em que o invasor comprometeu uma conta de usuário, pode conseguir. Uma verificação credenciada é um tipo de verificação mais intrusiva do que a verificação não credenciada.

- **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.

2. **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. As rotinas de teste podem incluir coisas como o uso de senhas padrão para contas de serviço e interfaces de gerenciamento de dispositivos, mas não recebem acesso privilegiado. A verificação não credenciada costuma ser a técnica mais apropriada para avaliação externa do perímetro da rede ou ao executar a verificação de aplicativos da web.

- **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.

Scanner de rede.

Falsos positivos, falsos negativos e análise de log

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. O relatório deve incluir ou vincular detalhes específicos sobre cada vulnerabilidade e como os hosts podem ser corrigidos.

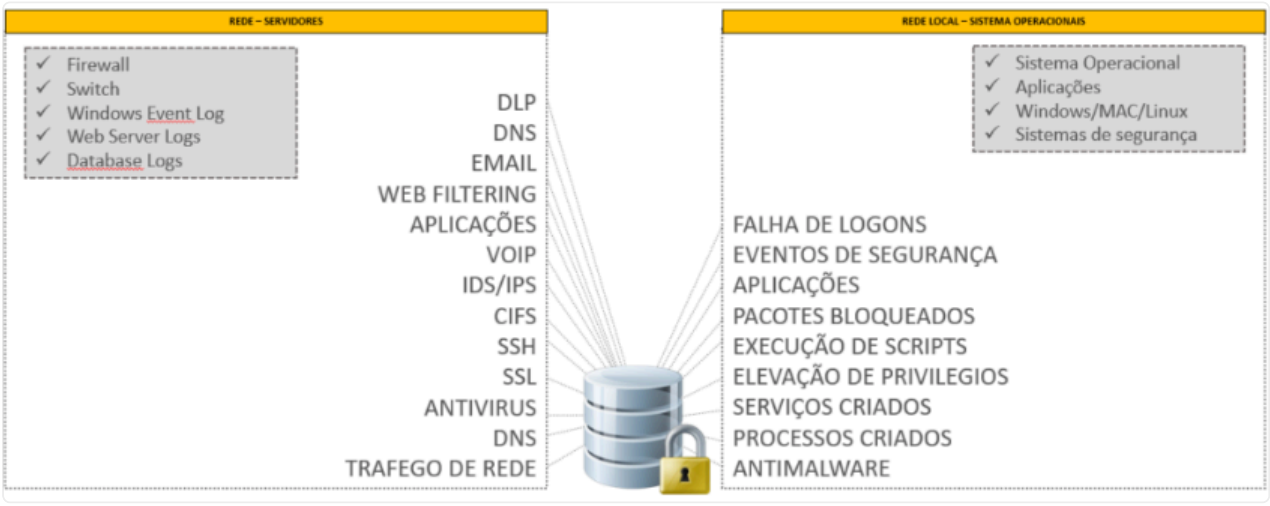
1. **Falso positivo**: em varreduras de vulnerabilidades, um falso positivo ocorre quando a ferramenta de verificação identifica erroneamente uma vulnerabilidade que na realidade não existe no sistema ou rede. Isso pode

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. Por exemplo, num teste de detecção de um antivírus, se o software identifica corretamente um arquivo malicioso como sendo malicioso, isso é considerado um verdadeiro positivo.

2. **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. Esse risco pode ser mitigado de alguma forma executando varreduras repetidas periodicamente e usando scanners de mais de um fornecedor. O verdadeiro negativo, por sua vez, ocorre quando um teste indica corretamente a ausência de uma condição ou característica que realmente não está presente. Por exemplo, num teste de detecção de um antivírus, se o software corretamente determina que um arquivo não possui ameaças, isso é considerado um verdadeiro negativo.
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. Para realizar uma análise de logs eficaz, é importante que os sistemas estejam configurados para registrar informações relevantes de maneira adequada e que os administradores de segurança tenham as habilidades necessárias para interpretar os registros.

- **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. Além disso, a análise de logs pode revelar possíveis falsos negativos. 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. A correlação de eventos de logs de diferentes fontes pode se tornar complexa e complicada. A análise de logs requer conhecimento e habilidades especializadas.



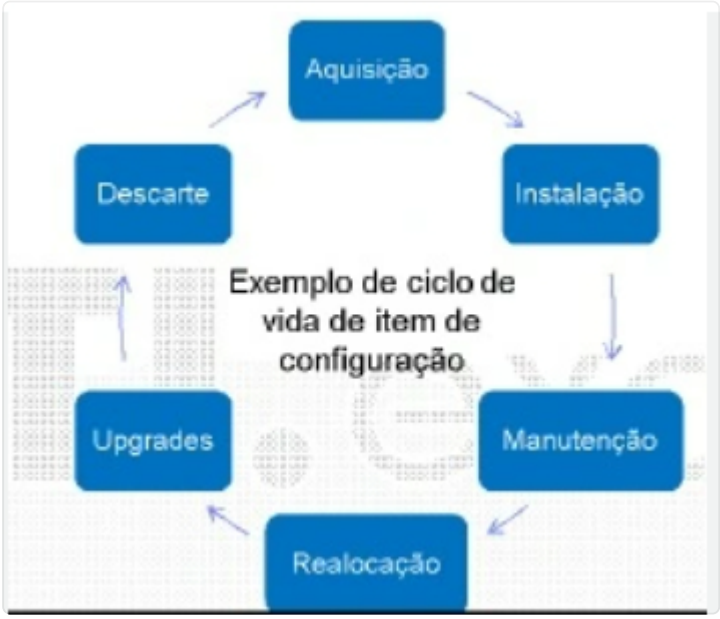
Análise de logs.

Revisão de configurações

A revisão de configurações é uma prática que envolve a análise e aprimoramento das configurações de sistemas, aplicativos e redes para garantir que eles atendam a padrões de segurança e estejam protegidos contra ameaças cibernéticas. As etapas do processo de revisão de configuração contemplam:

1. **Identificação das configurações**: o primeiro passo é identificar as configurações que precisam ser revisadas. Isso pode incluir políticas de segurança, configurações de firewall, permissões de acesso, configurações de criptografia, configurações de aplicativos e muito mais.
2. **Avaliação de conformidade**: depois de identificar as configurações relevantes, é importante avaliar sua conformidade com políticas de segurança, regulamentações e melhores práticas. Ferramentas de avaliação de conformidade podem ser úteis nesse processo.

3. **Análise de vulnerabilidades**: a revisão de configurações também deve incluir a análise de vulnerabilidades potenciais que podem surgir devido a configurações inadequadas. Isso pode incluir a identificação de portas abertas, protocolos fracos, permissões excessivas e assim por diante.
4. **Documentação e registro**: manter registros detalhados das configurações existentes, das alterações realizadas e das justificativas por trás dessas alterações é essencial. Isso ajuda a rastrear o histórico de configurações e simplifica a solução de problemas futuros.
5. **Implementação de correções**: com base na análise realizada, as correções e melhorias nas configurações devem ser implementadas. Isso pode envolver a reconfiguração de sistemas, a aplicação de patches, a atualização de políticas e outras ações corretivas.
6. **Teste e validação**: após implementar as correções, é fundamental testar e validar as novas configurações para garantir que não causem problemas de funcionalidade ou segurança não intencionais. Testes de penetração e verificações de vulnerabilidade podem ser úteis nesse estágio.



Revisão de configuração.

Conclusão

É com grande satisfação que chegamos ao fim desta aula sobre gerenciamento de vulnerabilidades. Parabenizamos a todos vocês pela dedicação e pelo interesse demonstrados em aprimorar seus conhecimentos em segurança cibernética.

Nesta aula sobre gerenciamento de vulnerabilidades, exploramos uma série de tópicos fundamentais da segurança cibernética. A identificação e o tratamento de vulnerabilidades são essenciais para proteger sistemas e redes. Aprendemos sobre técnicas de verificação de vulnerabilidades, abrangendo varreduras automatizadas e testes manuais. Exploramos a diferença entre varreduras intrusivas e não intrusivas, entendendo como cada uma afeta os sistemas verificados e quando usá-las. Discutimos a distinção entre varreduras credenciadas e não credenciadas. Examinamos os conceitos de falsos positivos e falsos negativos, compreendendo sua relevância na avaliação de resultados de varreduras de vulnerabilidades e como a análise de logs pode ajudar a confirmar esses resultados. Finalmente, discutimos a importância da revisão de configurações, destacando práticas recomendadas para manter sistemas, aplicativos e redes seguros.

Este é apenas o começo de sua jornada na segurança cibernética, e o conhecimento adquirido nesta aula será um alicerce sólido para futuros desafios. Parabéns mais uma vez e, como profissionais, desejamos vê-los aplicando essas habilidades em suas carreiras e na proteção do mundo digital.

Aula 2: Scanner de vulnerabilidades

Objetivos

- [ ] Distinguir as técnicas de reconhecimento ativo e reconhecimento passivo.
- [ ] Entender a finalidade e a importância de um teste de penetração.
- [ ] Compreender as diversas fases do ciclo de vida de um teste de penetração.

Conceitos

- [ ] Reconhecimento ativo e passivo.
- [ ] Pen test ou teste de penetração.
- [ ] Ciclo de vida do ataque de pen test.

Introdução

Bem-vindos à aula sobre "Scanner de vulnerabilidades: ativo x passivo". Nesta aula, abordaremos conceitos relacionados à segurança da informação, focando em tópicos como reconhecimento ativo e passivo, testes de penetração (pen test) e o ciclo de vida de um ataque de pen test.

Vamos entender a diferença entre as abordagens de reconhecimento: ativo e passivo, tão fundamental para identificar vulnerabilidades e riscos em sistemas e redes. Além disso, veremos testes de penetração, uma técnica muito utilizada para avaliar a segurança de um ambiente. Ao longo desta aula, vocês irão descobrir como os especialistas em segurança cibernética simulam ataques reais, identificam falhas de segurança e fornecem orientações para fortalecer a segurança de sistemas e redes.

Vamos nos aprofundar nesse tema da segurança da informação, explorando conceitos, técnicas e ferramentas que ajudarão a fortalecer nossas defesas cibernéticas e garantir um ambiente mais seguro para todos nós.

Reconhecimento ativo vs. passivo

O reconhecimento é o primeiro passo em qualquer avaliação de segurança cibernética. Antes de um atacante ou profissional de segurança explorar uma rede ou sistema, é necessário coletar informações sobre o alvo. É nesse ponto que surgem duas abordagens distintas: o reconhecimento ativo e o reconhecimento passivo.

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 é semelhante a "bater à porta" do alvo para ver como ele responde. 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 de técnicas de reconhecimento ativo**:

1. **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.
2. **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. Embora a busca passiva seja possível (limitando-a a detecção de pacotes), a maioria das técnicas de varredura requer conexões de rede ativas com o alvo que podem ser identificadas pelo software de detecção.
3. **Varredura de portas**: identificar quais portas estão abertas e quais serviços estão em execução.
4. **Solicitações de DNS**: descobrir informações sobre a infraestrutura de rede.
5. **Ping sweeps**: identificar hosts ativos na rede.
6. **Banner grabbing**: coletar informações dos banners de serviços em execução.

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

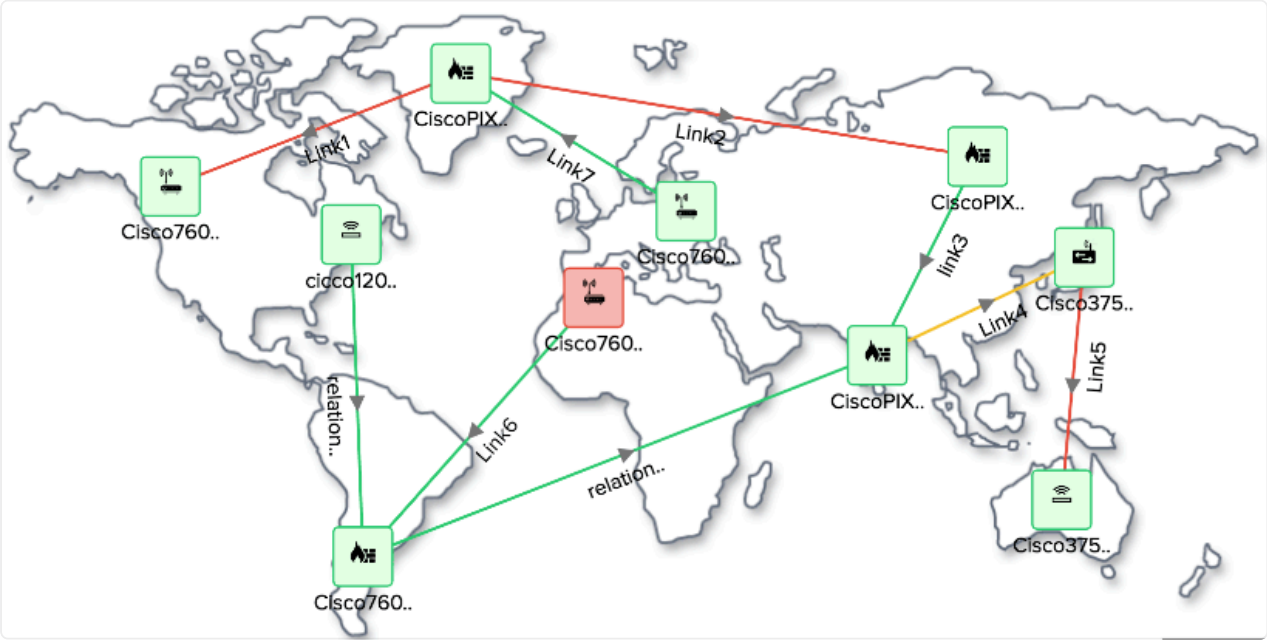
Reconhecimento passivo

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. O reconhecimento passivo provavelmente não alertará o alvo da investigação, pois significa consultar informações publicamente disponíveis.

- **Exemplos de técnicas de reconhecimento passivo**:

1. **Monitoramento de tráfego de rede**: observar o tráfego para identificar padrões e sistemas ativos.
2. **Análise de logs**: examinar logs de eventos e registros de sistemas em busca de informações úteis.
3. **Pesquisa OSINT**: Inteligência de código aberto (OSINT — Open Source Intelligence) — usando ferramentas de pesquisa na web, mídias sociais e sites que verificam vulnerabilidades em dispositivos e serviços conectados à internet para obter informações sobre o alvo. 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 passa despercebido e não perturba o alvo. É útil para coletar informações gerais sobre a infraestrutura do alvo.
- **Desvantagens**: pode fornecer informações menos detalhadas e mais antigas, não sendo ideal para identificar vulnerabilidades específicas.



Reconhecimento ativo de rede.

Teste de penetração (pen test)

Um teste de penetração, também conhecido como pen test, 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. A abordagem ética e legal é crucial para garantir que os testes de penetração sejam realizados de forma responsável e sem prejudicar as operações normais do alvo. Os testes de penetração têm objetivos claros, que 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.

Fases de um pen test

As fases de um pen test incluem:

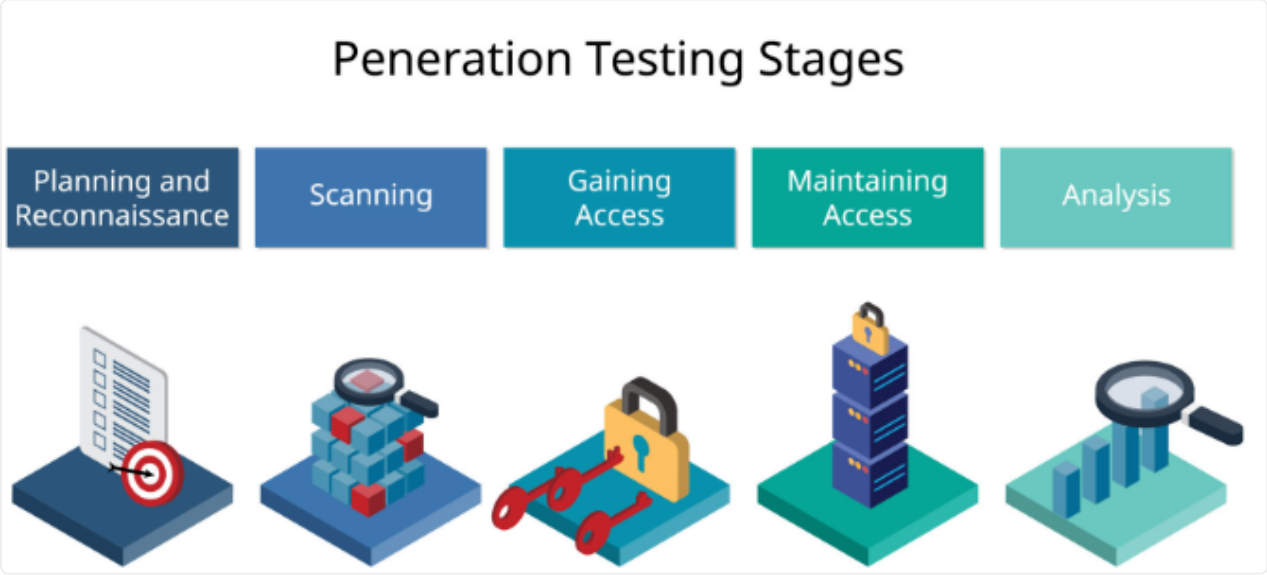
1. **Planejamento**: nesta fase, são definidos os objetivos do teste, o escopo e a metodologia a ser utilizada. É essencial obter a aprovação da alta administração e garantir a legalidade do teste.
2. **Coleta de informações**: os testadores reúnem informações sobre o alvo, incluindo sistemas, redes e aplicativos a serem avaliados. Isso pode envolver varredura de DNS, coleta de informações WHOIS e identificação de alvos potenciais.
3. **Análise**: durante essa fase, os testadores analisam as informações coletadas e desenvolvem estratégias de ataque. São identificadas possíveis vulnerabilidades e fraquezas que serão exploradas.

4. **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.
5. **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.
6. **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.

Demonstração de ferramentas de teste de penetração comuns

Para ilustrar as fases do teste de penetração, é útil apresentar algumas ferramentas comuns usadas em cada etapa do processo. Exemplos de ferramentas incluem:

- **Nmap**: usado para escanear portas e serviços em sistemas.
- **Metasploit**: uma estrutura de teste de penetração que automatiza muitos ataques.
- **Wireshark**: uma ferramenta de análise de tráfego de rede.



Teste de penetração.

Ciclo de vida do ataque de pen test

A fase do ciclo de vida do ataque de pen test é fundamental para a realização de testes de penetração de forma organizada e eficaz. Vamos considerar aqui os testes de penetração usando um ciclo de vida de kill chain estruturado, que envolve várias etapas. 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. As etapas da kill chain geralmente incluem:

1. **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. **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. Tendo conquistado a posição, o pen tester pode então começar a proteger e ampliar o acesso.
3. **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.

4. **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. Por exemplo, o malware original pode ter sido executado com privilégios de administrador local em uma estação de trabalho cliente ou como usuário Apache em um servidor web. 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.
5. **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 (coleta de credenciais, detecção de vulnerabilidades de software e outros), 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 pen tester 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.
6. **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). Da perspectiva de um pen tester, seria uma questão de definição do escopo se isso seria tentado. Na maioria dos casos, é geralmente suficiente mostrar que as ações relativas aos objetivos podem ser alcançadas.
7. **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 pen tester, essa fase significa remover quaisquer backdoors ou ferramentas e garantir que o sistema não seja menos seguro do que o estado de pré-engajamento.

Fases do teste de penetração.

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.

Exemplos de relatórios de pen test e sua estrutura: 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 comprovem as descobertas.
- Informações sobre a conformidade com as regras de engajamento.
- Uma análise de riscos e impacto.

Conclusão

Parabenizamos a todos pela conclusão de mais uma aula de cibersegurança. Durante nossa jornada, exploramos as nuances entre reconhecimento ativo e passivo, reconhecendo que a escolha da abordagem é fundamental para determinar o sucesso de um teste de penetração ou de um ataque cibernético. Compreendemos a importância de obter informações vitais enquanto minimizamos o risco de alertar o alvo.

Além disso, vimos que os testes de penetração são mais do que apenas simulações de ataques cibernéticos. Eles são instrumentos poderosos para avaliar a segurança de sistemas e redes. Aprendemos sobre o ciclo de vida de um teste de penetração, passando pelas fases de planejamento, coleta de informações, análise, exploração, documentação e relatório. Reconhecemos a importância de ética e conformidade nesses testes para garantir que sejam realizados de forma responsável e legal e, por fim, discutimos a importância de relatórios detalhados e documentação para um teste de penetração bem-sucedido.

Obrigado por sua participação nesta aula. Desejamos sucesso a todos em suas jornadas na segurança cibernética e na proteção de informações valiosas em um mundo cada vez mais conectado e digitalizado. Até a próxima aula!