TEMA 10
Testes de Penetração e Vulnerabilidades

Habilidades:

- Identificação de vulnerabilidades.
- Exploração de vulnerabilidades.
- Análise de riscos.
- Relatórios técnicos e comunicação efetiva.

Testes de Penetração/PenTest/Testes de Intrusão, **são métodos e técnicas realizadas por profissionais da área de cibersegurança com o intuito de identificar e avaliar a segurança operacional de uma infraestrutura de redes e aplicações de uma organização**.

Os testes de penetração (também conhecidos como ***PenTests***) são atividades de avaliação de segurança que têm como objetivo identificar e explorar vulnerabilidades em sistemas, redes, aplicativos e infraestruturas de TI. O propósito é simular um ataque realista para avaliar a eficácia das medidas de segurança existentes e reconhecer as áreas de melhoria. Aqui estão os principais **tópicos relacionados aos testes** de penetração e vulnerabilidades:

- **Definição de Testes de Penetração**: Explicação sobre o que são testes de penetração e como são conduzidos para identificar vulnerabilidades e avaliar a segurança de sistemas e redes.
- **Objetivos dos Testes de Penetração**: Discussão sobre os principais objetivos dos testes de penetração, incluindo a identificação de vulnerabilidades, avaliação da postura de segurança, redução de riscos e melhoria contínua da segurança.
- **Fases dos Testes de Penetração**: Explicação das etapas comuns de um teste de penetração, como o levantamento de informações, identificação de vulnerabilidades, exploração, obtenção de acesso e documentação dos resultados.
- **Metodologias e Abordagens**: Apresentação das metodologias e abordagens normalmente utilizadas em testes de penetração, como as metodologias OSSTMM, OWASP e PTES, e a importância de adaptá-las para atender às necessidades do ambiente alvo.
- **Tipos de Testes de Penetração**: Exploração dos diferentes tipos de testes de penetração, incluindo testes de caixa-preta, caixa-cinza e caixa-branca, e como eles se diferenciam em termos de acesso à informação do sistema.
- **Ferramentas de Teste de Penetração**: Visão geral das ferramentas comumente usadas em testes de penetração, como scanners de vulnerabilidades, ferramentas de exploração, sniffers e ferramentas de análise de tráfego.
- **Documentação e Relatórios**: Discussão sobre a importância da documentação e relatórios em testes de penetração, e abrange a descrição dos testes realizados, as vulnerabilidades identificadas, os riscos associados e as recomendações para mitigação.
- **Ética e Legalidade**: Exploração das considerações éticas e legais envolvidas nos testes de penetração, incluindo a obtenção de autorização prévia, o respeito às políticas e leis de privacidade, e a importância de manter a confidencialidade dos dados obtidos.
- **Benefícios dos Testes de Penetração**: Destaque dos benefícios de realizar testes de penetração, como a melhoria da postura de segurança, a identificação proativa de vulnerabilidades e a redução do risco de ataques cibernéticos.
- **Melhores Práticas em Testes de Penetração**: Apresentação de algumas melhores práticas a serem seguidas em testes de penetração, como a definição de escopo claro, o envolvimento das partes interessadas, a comunicação eficaz dos resultados e a realização de testes regulares para garantir a segurança contínua.

Os testes de penetração são uma parte importante da avaliação e melhoria da segurança, mas devem ser realizados por profissionais experientes e seguindo as melhores práticas e considerações éticas.

Os **hackers éticos**, normalmente, são desenvolvedores de alto nível que contam com habilidades com infraestrutura de redes e sistemas de informação em geral. Estes profissionais usam de suas destrezas para algo que impactará positivamente à organização e de modo geral prestam serviços de forma autônoma.

A função do hacker não é apenas realizar os testes, mas canalizar e imaginar como um criminoso agiria vendo este sistema e de quais artimanhas usaria para realizar algum ataque. Ele deve pensar de que maneira um usuário pode encontrar e percorrer diversos caminhos que não poderiam ser utilizados e notados por eles.

Níveis de Testes de Penetração

Existem três níveis de *PenTests* que poderão ser definidos e usados conforme a necessidade e tem como objetivo preparar os procedimentos da forma que um atacante enxerga a empresa. Cada um possui uma aplicabilidade diferente. São elas:

White Box

Nesta abordagem, os **testes serão realizados com todas as informações de infraestrutura e aplicações disponíveis**. É o processo mais completo e por ter o acesso de todas as operações e costuma ser realizado pelos próprios analistas de T.I. e S.I. da organização, no intuito de testar um agente interno tentando realizar algum tipo de crime cibernético.

Black Box

Aqui, os testes irão partir do princípio de que o ataque virá de um agente externo, ou seja, que **não tem conhecimento da estrutura da organização e tentará atacar "às cegas"**.

GrayBox

A GrayBox utiliza dos dois métodos citados acima, o Black e o White box. Ele parte da premissa de que o atacante **conseguiu alguma informação relevante a ponto de conseguir uma permissão de acesso e conseguir realizar um ataque**. Ele não tem acesso a tudo como na White Box, mas esta informação ou nível de acesso já consegue ser minimamente suficiente para invadir.

Procedimentos de um Pentest

Existem etapas para se realizar um procedimento de *Pentest*. São elas:

Discovering(Descoberta)

Nesta etapa, o profissional irá planejar seu ataque e levantar seu escopo junto com o cliente. É neste momento que as métricas e estratégias dos testes serão traçadas e o atacante tentará adquirir informações pertinentes à empresa, de modo também a identificar vulnerabilidades a partir daí. Um dos métodos de descoberta mais utilizados pelos hackers é o **FootPrint**, que você já aprendeu no tema anterior**.**

Escaneamento

Assim que o hacker finaliza seu planejamento, segue à segunda fase, que é chamada de escaneamento. São estratégias que têm como objetivo encontrar vulnerabilidades dentro dos códigos da aplicação, partindo de dois tipos de análise:

1. Análise Estática – Avaliação do código da aplicação de modo genérico, para identificar brechas ou falhas sem a necessidade de executar o código. Nessa abordagem, os hackers examinam o código-fonte em busca de padrões ou práticas inseguras, como falta de validação de entrada, erros na implementação de criptografia ou manipulação inadequada de dados sensíveis. Ferramentas de análise estática, como linters e scanners de segurança, podem ser usadas para automatizar essa tarefa e detectar vulnerabilidades conhecidas.

2. Análise Dinâmica – Consiste em avaliar a aplicação em tempo real, enquanto ela está em execução, para identificar vulnerabilidades que só se manifestam durante a execução. Isso inclui testes de penetração e varreduras que simulam ataques reais para observar como a aplicação se comporta sob condições adversas. O objetivo é encontrar falhas que não são evidentes apenas com a análise do código, como problemas de configuração ou vulnerabilidades que surgem com a interação do usuário.

Ambos os tipos de análise são fundamentais para garantir a segurança de uma aplicação, ajudando a identificar e corrigir falhas antes que possam ser exploradas por atacantes. A combinação dessas abordagens oferece uma visão mais abrangente e detalhada das possíveis vulnerabilidades e riscos associados a uma aplicação.

Conseguindo Acesso

Planejamento feito e codificação analisada, finalmente chegou a hora de realizar os testes de penetração baseados nas falhas encontradas. Eles irão explorar todas as vulnerabilidades para conseguir sucesso na simulação de invasão.

Manter o Acesso

Neste estágio, o atacante irá averiguar o andamento de seu ataque, ou seja, vai acompanhar se o ambiente de segurança consegue detectar que houve uma invasão e como ele reage. Caso isso não aconteça, é uma evidência de que a aplicação pode ser violada por tempo suficiente para o agente conseguir informações sigilosas.

Análise e Documentação

Assim que os testes de penetração forem concluídos, o profissional irá documentar todas as vulnerabilidades encontradas no ambiente e anexar todas os comprovantes que validam suas afirmações em um relatório.
Além disso, neste arquivo também conterá **todos os motivos pelos quais estas falhas acontecem**, seja por algum defeito na infraestrutura, colaboradores não cumprindo as políticas de segurança, falta de atualização de sistemas operacionais, ausência de softwares antivírus entre outros.

Correção e Controle

Nesta última fase, serão realizados os procedimentos cabíveis para sanar todas as vulnerabilidades encontradas, como correções em trechos de códigos da aplicação, mudanças na infraestrutura de redes alterações nos filtros de pacotes no firewall, atualizações de sistemas e softwares, inserção e correção de políticas de segurança e orientação dos colaboradores. Feito isso, o *PenTester* irá realizar novamente os testes para assegurar que as correções surtiram efeito.

Tipos de PenTest

Existem diversos tipos de PenTests, cada um para um tipo de aplicação, infraestrutura e ambiente. Veja abaixo os mais comuns:

Na rede:

Serão realizadas simulações de invasão em firewalls e outras ferramentas de segurança que a organização possui. Caso a invasão seja bem-sucedida, qualquer dispositivo que esteja conectado a esta rede-vítima, estará vulnerável e passível de acesso.

Pentests em uma aplicação Web

Em posse da coleta de informações pelo método de Footprint, o atacante consegue ter uma noção de como uma aplicação Web foi desenvolvida e consegue dimensionar um ataque certeiro às vulnerabilidades encontradas nos firewalls, servidores e endereços IP.

Dois exemplos de ataques comuns e que podem ser realizados por hackers éticos são o **SQL Injection e o Ataque de Negação de Serviço DoS e DDoS**, vistos nos temas anteriores.

Pentests Client Side

Nestes testes, o atacante irá analisar a perspectiva de um usuário comum utilizando a aplicação e se ele consegue usar o ambiente com segurança. A proposta é realizar simulações de invasões que não afetem a aplicação em si, mas o usuário/cliente que a utiliza.

Pentests com engenharia social

Neste tipo de teste, o hacker ético abordará o ambiente com métricas de engenharia social no intuito de **analisar o comportamento dos colaboradores** de um ambiente organizacional.

Ferramentas de Pentest

Existem inúmeras ferramentas de testes de penetração existentes, desde dispositivos físicos, para simulação de ataques em hardware, até softwares e sistemas. Neste tópico, você verá o conceito de ambas e exemplos das mais utilizadas atualmente.

Ferramentas de dispositivos físicos (Hardware Hacking)

As ferramentas físicas de testes de penetração são equipamentos de grande valia na exploração e subtração de informações dentro da empresa. Veja abaixo alguns exemplos:

Hardware Keylogger

O Keylogger de hardware é um dispositivo físico, comumente prototipado em portas USB, que é desenvolvido para **captar todas as teclas digitadas pelo usuário**. Ele funciona plugado ao teclado da vítima na porta USB fêmea do dispositivo e ao USB macho no computador. Tem a vantagem de não ser detectado por antivírus, já que funciona como um **extensor do teclado** e ser pequeno, podendo passar despercebido. O log das teclas digitadas pode tanto ser armazenado no dispositivo, quanto transmitido por Wi-Fi, dependendo do modelo.

USB Rubber Ducky

O Rubber Ducky é um dispositivo que tem semelhança com um pen drive, com uma ponta USB macho, e consegue simular um teclado. Tem como o objetivo de simular diversos ataques. No seu interior, há um script que pode ser editado conforme a necessidade. É possível inserir instruções para tentar roubar informações de redes, injetar teclas que possam causar algum tipo de dano ao sistema ou deixar um backdoor.

Shark Jack

Shark Jack é um dispositivo voltado para ataques de rede. Possui uma **porta rj45 na extremidade e**

tem como objetivo coletar diversas informações referentes a infraestrutura e firewall e até mesmo realizar injeções de comandos ao inseri-la em algum ponto de rede.

Cabo O.MG

Este cabo que aparenta ser um simples carregador de celular, na verdade, é um cabo malicioso que, caso conectado a um computador, consegue capturar tudo o que for digitado e encaminhado para o hacker a partir de um ponto de acesso Wi-Fi em uma interface web.

RaspBerry

O Raspberry é um **microcomputador totalmente modular**, capaz de ser atrelado a outros componentes e realizar diversas funções através de uma codificação. Consegue realizar ataques de rastreamento, captação de ondas de rádio e até hackear redes Wi-Fi.

Ferramentas de Softwares/Sistemas

Grande parte das ferramentas de penetração virtual podem ser encontradas em **distribuições do Linux**. Estas distribuições foram totalmente **otimizadas para realizar os mais diversos testes de invasão, além de serem seguras para o hacker ético**.
Vale ressaltar que a escolha de uma distribuição depende da necessidade de cada projeto e também varia de gosto pessoal de cada profissional, já que muitas distribuições, ainda que diferentes, conseguem rodar os mesmos testes.
Dentre as distros mais conhecidas para fins de pentests, podemos citar:

Kali Linux

A **mais famosa e querida entre os hackers éticos**, a Kali é uma distro baseada **no Debian** e reúne mais de 600 ferramentas forenses e pentest pré-instaladas disponíveis para o atacante utilizar e sempre recebem atualizações continuamente. Possui a ferramenta NetHunter, capaz de realizar testes de invasão em dispositivos Android.

Pentoo

A Pentoo uma distro conhecida por ter uma gama de testes de invasão e avaliações específicas para redes e infraestruturas. Foi desenvolvida baseando-se na Gentoo e possui versões de 32 e 64 bits.

Parrot Security OS

A Parrot é uma distro **mais leve e amigável** que, assim como o Kali, é baseada **no Debian** e possui inúmeros pentests e ferramentas específicas de mitigação de vulnerabilidades e de computação forense. Ela utiliza repositórios do Kali para rodar as ferramentas, apesar de vir com em menor quantidade. Diferente da Kali, a Parrot não possui suporte para dispositivos Android.

Dentro destas distribuições e de outros sistemas operacionais, podemos encontrar e instalar inúmeras ferramentas de pentest. Veja abaixo algumas das mais populares.

NMap

Já mencionado anteriormente no Footprint, é uma ferramenta extremamente rápida e eficaz capaz de mapear toda a rede e dispositivos, além da utilização do firewall.

Wireshark

A Wireshark é uma das ferramentas com foco em redes mais populares no Linux. Ela consegue realizar uma monitoração dos pacotes de dados que estão trafegando pela rede em tempo real, emitir logs mais complexos e analisar os protocolos de rede.

Nessus

Esta ferramenta é capaz de escanear e detectar vulnerabilidades em um computador de maneira remota. Ela **não tem como objetivo acabar com a falha**, mas sim realizar mais de 1200 verificações predefinidas, identificando problemas e reportando. É uma ferramenta desenvolvida para quebrar senhas(cracking). É possível realizar ataques de força bruta contra as senhas criptografadas e trabalhar com dicionários. Seu ataque é focado em serviços offline.

Hydra

A Hydra permite realizar procedimentos de ataque de força bruta contra serviços de autenticação online, tendo **suporte a dezenas de protocolos**, como por exemplo os FTP's, HTTP, Banco de dados, SHH, entre outros.

Fern Wifi Cracker

É uma ferramenta que tem como objetivo quebrar a segurança de redes sem fio do tipo WPS, WEP e WPA, executando ataques de força bruta e com dicionários.

OBS.: O **Projeto Metasploit** é um projeto de segurança de computadores que fornece informações sobre vulnerabilidades de segurança e ajuda em testes de penetração e desenvolvimento de assinaturas IDS. É propriedade da Rapid7, empresa de segurança sediada em Boston, Massachusetts. Metasploit pode ser integrado com outras ferramentas de segurança, como Nmap para varredura de rede. Sua força reside na extensa base de dados de exploits, payloads, e módulos que permitem a automatização de ataques e exploração de falhas de segurança conhecidas.

RESUMO:

A identificação de vulnerabilidades é um processo crítico em qualquer sistema de segurança da informação, que consiste em descobrir, catalogar e analisar pontos fracos em um sistema que podem ser explorados por invasores. O objetivo é identificar essas vulnerabilidades antes que um invasor possa fazê-lo, permitindo que as organizações tomem medidas proativas para mitigá-las. Isso pode envolver o uso de ferramentas automatizadas, bem como inspeções manuais e auditorias de segurança.

A exploração de vulnerabilidades refere-se ao processo de aproveitar esses pontos fracos identificados para ganhar acesso não autorizado a um sistema ou dados. Uma vez explorada, a vulnerabilidade pode permitir ao invasor executar comandos arbitrários, acessar informações confidenciais ou mesmo comprometer todo o sistema. A análise de riscos, por outro lado, é o processo de identificar e avaliar os riscos associados a estas vulnerabilidades, considerando a probabilidade de um ataque e o impacto potencial para a organização. Finalmente, a elaboração de relatórios técnicos e a comunicação efetiva são vitais para documentar os resultados e as recomendações dessas análises. Esses relatórios ajudam as partes interessadas a entender os riscos e a tomar decisões informadas sobre como abordá-los, seja implementando medidas de segurança adicionais, aceitando o risco ou transferindo-o para outra parte.

ATIVIDADES:

1. O que é um Teste de Penetração (Pentest) e seu objetivo principal?

Um Teste de Penetração, ou Pentest, é um processo que simula ataques cibernéticos a um sistema, aplicação ou rede com o objetivo de identificar e explorar vulnerabilidades. O principal objetivo do Pentest é avaliar a segurança de um ambiente de TI, identificando pontos fracos que poderiam ser explorados por atacantes maliciosos. Ele é considerado uma prática essencial porque ajuda a descobrir vulnerabilidades antes que possam ser exploradas em um ataque real, permitindo que as

organizações tomem medidas proativas para mitigar riscos e proteger suas informações.

2. Etapas principais de um Teste de Penetração

Um Pentest geralmente segue um processo estruturado composto por várias etapas:

- Planejamento e Escopo: Define os objetivos do teste, o escopo e as regras de engajamento, assegurando que todas as partes estejam alinhadas sobre o que será testado e como.

- Reconhecimento (Information Gathering): Coleta de informações sobre o alvo para identificar possíveis pontos de entrada. Isso pode incluir a análise de redes, sistemas operacionais, aplicações e outros recursos. Esta fase é crucial porque define a base para as etapas subsequentes.

- Varrimento (Scanning): Análise dos sistemas para identificar portas abertas, serviços em execução e possíveis vulnerabilidades. Ferramentas automatizadas são frequentemente usadas para esta etapa.

- Exploração: Tentativa de explorar as vulnerabilidades identificadas para acessar o sistema ou extrair informações. Essa fase testa a eficácia das medidas de segurança e a extensão dos impactos potenciais.

- Pós-Exploração (Post-Exploitation): Avaliação da persistência do acesso e do impacto de um ataque bem-sucedido. O objetivo é determinar até que ponto um invasor poderia comprometer o sistema ou roubar informações sensíveis.

- Relatório: Documentação dos achados, incluindo vulnerabilidades descobertas, explorações bem-sucedidas e recomendações para mitigação. Um relatório bem-estruturado é vital para comunicar os riscos e as ações corretivas necessárias.

Seguir essas etapas de maneira estruturada garante que o Pentest seja abrangente e que as vulnerabilidades sejam identificadas e tratadas de maneira sistemática.

3. Diferenças entre Pentest de Caixa Preta, Caixa Cinza e Caixa Branca

- Caixa Preta (Black Box): O testador não tem conhecimento prévio do sistema. Simula um ataque real de um invasor externo sem informações internas. **Vantagem:** Reflete ataques reais**. Desvantagem:** Pode não identificar todas as vulnerabilidades, pois o testador não tem contexto suficiente.

- Caixa Cinza (Gray Box): O testador tem algum conhecimento do sistema, como credenciais de usuário ou informações de arquitetura. Simula um ataque de alguém com acesso interno limitado. **Vantagem:** Oferece um equilíbrio entre realismo e profundidade de análise. **Desvantagem:** Pode não ser tão exaustivo quanto o Caixa Branca.

- Caixa Branca (White Box): O testador tem total acesso ao código-fonte, configurações e informações internas. **Vantagem:** Identifica vulnerabilidades profundas e de lógica interna. **Desvantagem:** Pode ser menos realista e requer mais tempo e recursos.

4. Importância da Coleta de Informações na Fase de Reconhecimento

A fase de reconhecimento é essencial em um Pentest porque permite que o testador entenda o

ambiente-alvo e identifique possíveis vetores de ataque. Informações coletadas podem incluir nomes de domínio, endereços IP, estruturas de rede, versões de software e muito mais. Fontes comuns de informações incluem WHOIS, DNS, redes sociais, sites corporativos e ferramentas de varredura de rede. Essa fase ajuda a preparar estratégias de ataque mais eficazes e a maximizar o impacto do Pentest.

5. Tipos de Testes em um Teste de Penetração

Durante um Pentest, vários tipos de testes podem ser realizados:

- Teste de Vulnerabilidade: Utiliza ferramentas automatizadas para identificar vulnerabilidades conhecidas em sistemas e aplicações.

- Teste de Injeção de Código (SQL Injection, XSS): Verifica se é possível injetar código malicioso em aplicações para manipular o comportamento do sistema.

- Teste de Força Bruta: Tenta adivinhar credenciais de login usando combinações de usuários e senhas.

- Teste de Engenharia Social: Avalia a suscetibilidade dos usuários a ataques baseados em manipulação psicológica.

Esses testes ajudam a identificar uma variedade de vulnerabilidades e a avaliar a robustez das medidas de segurança existentes, permitindo que as organizações implementem defesas mais eficazes contra ataques.