PENTEST

AULA 02

Por Luiz Alvarenga

Sumário

PENTEST

Você sabia que vários milhões de sites WordPress são invadidos diariamente?

Por mais falso que possa parecer, os sites WordPress não são os únicos sites atacados por hackers, outros sites e computadores pessoais também são uma das razões pelas quais alguns desses sites são invadidos com tanta facilidade é porque não foi realizado um " teste de penetração", ou mais conhecido como **PENTEST**.
Geralmente o Pentest funciona para verificar o nível de vulnerabilidade.
Aqui está uma visão geral sobre o teste de penetração, por que é necessário, benefícios, tipos e etapas envolvidos e tudo o que você precisa para dar o pontapé no mundo Hacker etc.

O que é Pentest?

O pentest ou teste de penetração, também chamado de "Pentest" ou " **teste de segurança** ", é o ato de atacar os sistemas de TI dos seus clientes ou de seus clientes para imitar um ataque de um hacker, a fim de detectar falhas de segurança no sistema e tomar as medidas apropriadas para consertá-los.

O Pentest é um tipo de teste de segurança usado para testar a insegurança de um aplicativo. É conduzido para encontrar o risco de segurança que pode estar presente no sistema.

Se um sistema não estiver protegido, qualquer invasor poderá interromper ou obter acesso autorizado a esse sistema. O risco de segurança normalmente é um erro acidental que ocorre durante o desenvolvimento e a implementação do software.

Por exemplo, erros de configuração, erros de design e erros de software, etc.

Nos módulos a seguir você irá aprender sobre o Pentest e os possíveis testes.

Por que é necessário o Pentest?

O Pentest **normalmente** avalia a capacidade de um sistema de proteger suas redes, aplicativos, terminais e usuários contra ameaças externas ou internas.

O Pentest também é necessário para proteger os controles de segurança e garante apenas o acesso autorizado.

O Pentest é necessário porque:

- Identifica um ambiente de simulação, ou seja, como um invasor pode atacar o sistema através do **ataque de chapéu branco** .
- Ajuda a encontrar áreas fracas onde um invasor pode atacar para obter acesso aos recursos e dados do computador.
- Suporta para evitar **ataques de Blackhat** e protege os dados originais.
- Ele estima a magnitude do ataque a negócios em potencial.
- Ele fornece evidências para sugerir, por que é importante aumentar os investimentos no aspecto de segurança da tecnologia.

Causas de Vulnerabilidade 

- **Erros de design e desenvolvimento** : pode haver falhas no design de hardware e software. Esses erros podem colocar os dados críticos da empresa em risco de exposição.

- **Má configuração do sistema** : essa é outra causa de vulnerabilidade. Se o sistema estiver mal configurado, poderá introduzir brechas através das quais os invasores podem entrar no sistema e roubar as informações.

- **Erros humanos** : fatores humanos, como descarte inadequado de documentos, deixar os documentos sem supervisão, erros de codificação, ameaças internas, compartilhamento de senhas em sites de phishing, etc. podem levar a violações de segurança.

- **Conectividade** : se o sistema estiver conectado a uma rede não segura (conexões abertas), ele estará ao alcance dos hackers.

- **Complexidade** : a vulnerabilidade de segurança aumenta proporcionalmente à complexidade de um sistema. Quanto mais re cursos um sistema tiver, mais chances de ataque do sistema.

- **Senhas** : as senhas são usadas para impedir o acesso não autorizado. Eles devem ser fortes o suficiente para que ninguém consiga adivinhar sua senha. As senhas não devem ser compartilhadas com ninguém a qualquer custo e as senhas devem ser alteradas periodicamente. Apesar dessas instruções, às vezes as pessoas revelam suas senhas para outras pessoas, as escrevem em algum lugar e mantêm senhas fáceis de serem adivinhadas.

- **Entrada do usuário** : Você deve ter ouvido falar em injeção SQL, estouros de buffer etc. Os dados recebidos eletronicamente por esses métodos podem ser usados para atacar o sistema receptor.

- **Gerenciamento** : a segurança é difícil e cara de gerenciar. Às vezes, as organizações perdem o gerenciamento adequado de riscos e, portanto, a vulnerabilidade é induzida no sistema.

- **Falta de treinamento para a equipe** : isso leva a erros humanos e outras vulnerabilidades.

- **Comunicação** : Canais como redes móveis, internet e telefone abrem o escopo de roubo de segurança.

Quais os benefícios do Pentest?

O Pentest oferece os seguintes benefícios -

- **Aprimoramento do sistema de gerenciamento** - fornece informações detalhadas sobre as ameaças à segurança. Além disso, também categoriza o grau de vulnerabilidades e sugere qual é o mais vulnerável e qual é o menor. Portanto, você pode gerenciar seu sistema de segurança com facilidade e precisão, alocando os recursos de segurança adequadamente.
- **Evitar multas** - O Pentest mantém as principais atividades da sua organização atualizadas e em conformidade com o sistema de auditoria. Portanto, o Pentest protege você de aplicar multas.
- **Proteção contra danos financeiros** - Uma simples violação do sistema de segurança pode causar milhões de dólares em danos. O Pentest pode proteger sua organização de tais danos.
- **Proteção do cliente** - A violação de dados de um único cliente pode causar grandes prejuízos financeiros e danos à reputação. Ele protege as organizações que lidam com os clientes e mantém seus dados intactos.

O Pentest é uma combinação de técnicas que considera vários problemas dos sistemas e testa, analisa e fornece soluções. É baseado em um procedimento estruturado que executa o Pentest passo a passo.

Este capítulo descreve várias etapas ou fases do método de Pentest.

Quando realizar Pentest?

O Pentest é um recurso essencial que precisa ser executado regularmente para garantir o funcionamento de um sistema.

Quando fazer:

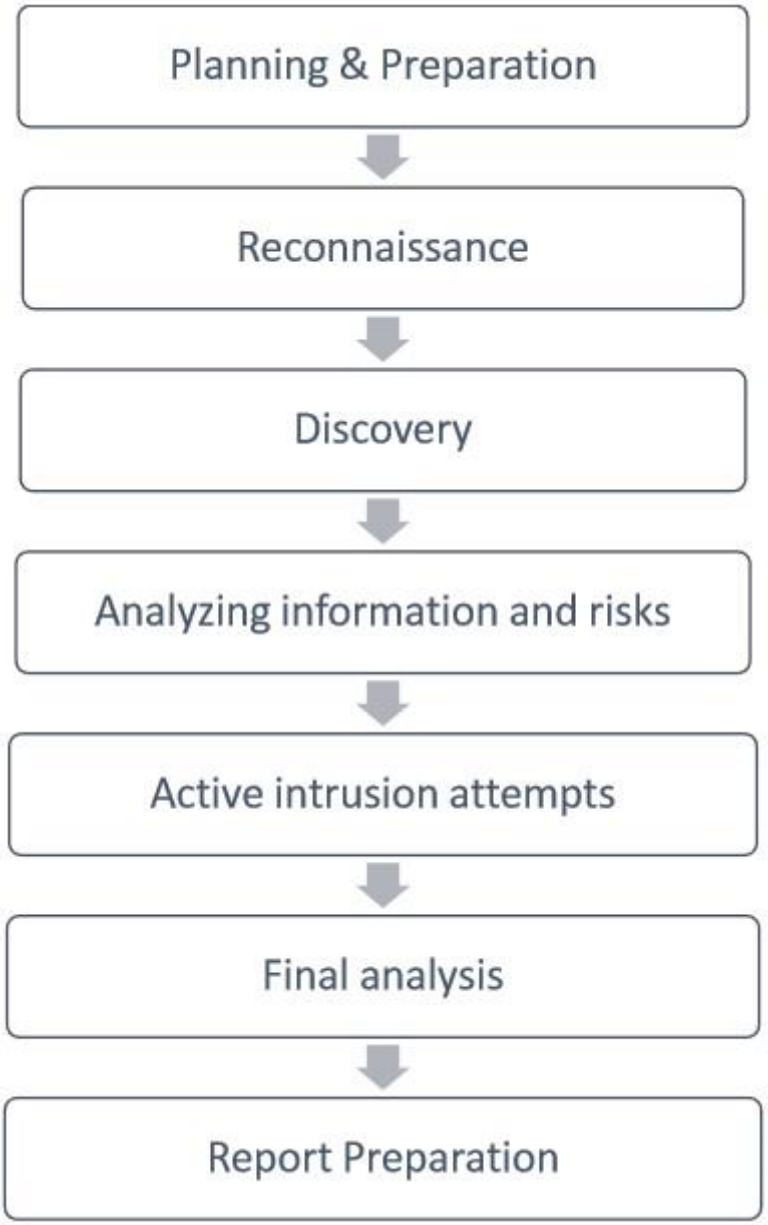
- O teste de penetração é necessário para garantir a segurança dos dados nos setores financeiros, como bolsas de valores, bancos e bancos de investimento.
- Fazer testes de penetração proativamente é a melhor maneira de garantir que seu sistema não seja invadido.
- Em uma situação em que o sistema de software já foi hackeado, o teste de penetração se torna a melhor maneira de determinar se ainda existem brechas nas quais hackers em potencial podem lucrar para repetir uma invasão futura.

Além disso, deve ser realizado sempre que -

- O sistema de segurança descobre novas ameaças dos atacantes.
- Você adiciona uma nova infraestrutura de rede.
- Você atualiza seu sistema ou instala um novo software.
- Você muda seu escritório.
- Você configurou um novo programa / política para o usuário final.

Etapas do método de Pentest

A seguir, são apresentadas as sete etapas do Pentest -



Planejamento e Preparação

O planejamento e a preparação começam com a definição das metas e objetivos do Pentest.

O cliente e o testador definem conjuntamente os objetivos para que ambas as partes tenham os mesmos objetivos e entendimento. Os objetivos comuns dos Pentest são:

- Identificar a vulnerabilidade e melhorar a segurança dos sistemas técnicos.
- Confirme a segurança de TI por terceiros externos.
- Aumente a segurança da infraestrutura organizacional / pessoal.

Reconhecimento

O reconhecimento inclui uma análise das informações preliminares. Muitas vezes, um testador não possui muitas informações além das informações preliminares, ou seja, um endereço IP ou bloco de endereços IP. O testador começa analisando as informações disponíveis e, se necessário, solicita mais informações, como descrições do sistema, planos de rede etc. do cliente. Este passo é o Pentest passiva, mais ou menos. O único objetivo é obter informações completas e detalhadas dos sistemas.

Descoberta

Nesta etapa, um testador de penetração provavelmente usará as ferramentas automatizadas para varrer os ativos de destino em busca de vulnerabilidades. Essas ferramentas normalmente têm seus próprios bancos de dados, fornecendo os detalhes das vulnerabilidades mais recentes. No entanto, o testador descobre

- **Descoberta de rede** - como a descoberta de sistemas, servidores e outros dispositivos adicionais.
- **Descoberta de host** - Determina portas abertas nesses dispositivos.
- **Interrogação de Serviço** - **Interroga as** portas para descobrir os serviços reais que estão sendo executados nelas.

Analisando informações e riscos

Nesta etapa, o testador analisa e avalia as informações coletadas antes das etapas de teste para penetrar dinamicamente no sistema. Devido ao maior número de sistemas e tamanho da infraestrutura, consome muito tempo. Ao analisar, o testador considera os seguintes elementos -

- Os objetivos definidos do Pentest.
- Os riscos potenciais para o sistema.
- O tempo estimado necessário para avaliar possíveis falhas de segurança nos Pentest ativos subsequentes.

No entanto, na lista de sistemas identificados, o testador pode optar por testar apenas aqueles que contêm vulnerabilidades em potencial.

Tentativas de intrusão ativas

Este é o passo mais importante que deve ser realizado com o devido cuidado. Esta etapa envolve até que ponto as possíveis vulnerabilidades identificadas na etapa de descoberta possuem os riscos reais. Esta etapa deve ser executada quando uma verificação de possíveis vulnerabilidades é necessária. Para os sistemas com requisitos de integridade muito altos, a vulnerabilidade e o risco em potencial precisam ser cuidadosamente considerados antes de realizar procedimentos críticos de limpeza.

Analise Final

Esta etapa considera principalmente todas as etapas realizadas (discutidas acima) até aquele momento e uma avaliação das vulnerabilidades presentes na forma de riscos potenciais. Além disso, o testador recomenda eliminar as vulnerabilidades e riscos. Acima de tudo, o testador deve garantir a transparência dos testes e as vulnerabilidades que divulgou.

Preparação de relatórios

A preparação do relatório deve começar com procedimentos gerais de teste, seguidos de uma análise de vulnerabilidades e riscos. Os altos riscos e vulnerabilidades críticas devem ter prioridades e serem seguidos pela ordem inferior.

No entanto, ao documentar o relatório final, os seguintes pontos precisam ser considerados -

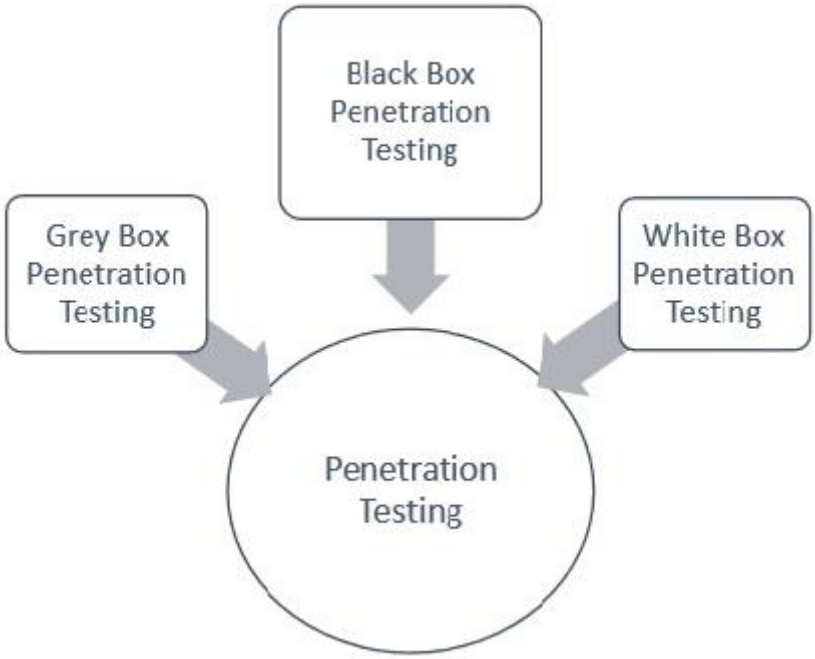
- Resumo geral dos Pentest.
- Detalhes de cada etapa e as informações coletadas durante o teste da caneta.
- Detalhes de todas as vulnerabilidades e riscos descobertos.
- Detalhes de limpeza e fixação dos sistemas.
- Sugestões para segurança futura.

O tipo de Pentest normalmente depende do escopo e dos desejos e requisitos organizacionais. Este capítulo discute sobre diferentes tipos de Pentest. Também é conhecido como **Pentest** .

Tipos de Pentest

A seguir, estão os tipos importantes de Pentest

- Pentest de caixa preta
- Pentest de caixa branca
- Pentest na caixa cinza



Para um melhor entendimento, vamos discutir cada um deles em detalhes -

Pentest de caixa preta (Blackbox)

Nos Pentest de caixas pretas ou Blackbox, o testador não tem idéia dos sistemas que ele irá testar. Ele está interessado em reunir informações sobre a rede ou sistema de destino. Por exemplo, neste teste, um testador sabe apenas qual deve ser o resultado esperado e não sabe como os resultados chegam. Ele não examina nenhum código de programação.

Vantagens do Pentest de caixa preta

Tem as seguintes vantagens -

- O testador não precisa necessariamente ser um especialista, pois não exige conhecimento específico de idioma
- O testador verifica as contradições no sistema real e as especificações
- O teste geralmente é realizado com a perspectiva de um usuário, não do designer

Desvantagens dos Pentest de caixa preta

Suas desvantagens são -

- Particularmente, esses tipos de casos de teste são difíceis de projetar.
- Possivelmente, não vale a pena, caso o designer já tenha realizado um caso de teste.
- Não conduz tudo.

Pentest de caixa branca

Este é um teste abrangente, pois o testador recebeu toda uma gama de informações sobre os sistemas e / ou rede, como Esquema, Código-fonte, detalhes do SO, endereço IP etc. É normalmente considerado como uma simulação de um ataque por um fonte interna. Também é conhecido como estrutural, caixa de vidro, caixa transparente e teste de caixa aberta.

O Pentest de caixa branca examina a cobertura do código e faz o teste de fluxo de dados, teste de caminho, teste de loop, etc.

Vantagens dos Pentest na caixa branca

Possui as seguintes vantagens -

- Ele garante que todos os caminhos independentes de um módulo tenham sido exercidos.
- Ele garante que todas as decisões lógicas foram verificadas junto com seu valor verdadeiro e falso.
- Ele descobre os erros tipográficos e faz a verificação de sintaxe.
- Ele encontra os erros de design que podem ter ocorrido devido à diferença entre o fluxo lógico do programa e a execução real.

Pentest na caixa cinza

Nesse tipo de teste, um testador geralmente fornece informações parciais ou limitadas sobre os detalhes internos do programa de um sistema. Pode ser considerado um ataque de um hacker externo que obteve acesso ilegítimo aos documentos de infraestrutura de rede de uma organização.

Vantagens do Pentest na caixa cinzenta

Tem as seguintes vantagens -

- Como o testador não requer o acesso ao código-fonte, ele não é intrusivo e imparcial
- Como existe uma clara diferença entre um desenvolvedor e um testador, há menos risco de conflito pessoal
- Você não precisa fornecer informações internas sobre as funções do programa e outras operações

Áreas do Pentest

O Pentest é normalmente realizado nas três áreas a seguir:

- **Pentest de rede** - Nesse teste, a estrutura física de um sistema precisa ser testada para identificar a vulnerabilidade e o risco que garantem a segurança em uma rede. No ambiente de rede, um testador identifica falhas de segurança no design, implementação ou operação da rede da empresa / organização respectiva. Os dispositivos testados por um testador podem ser computadores, modems ou até dispositivos de acesso remoto, etc.
- **Pentest de aplicativos** - Nesse teste, a estrutura lógica do sistema precisa ser testada. É uma simulação de ataque projetada para expor a eficiência dos controles de segurança de um aplicativo, identificando vulnerabilidade e risco. O firewall e outros sistemas de monitoramento são usados para proteger o sistema de segurança, mas, em algum momento, ele precisa de testes focados, especialmente quando o tráfego é permitido passar pelo firewall.
- **A resposta ou fluxo de trabalho do sistema** - Esta é a terceira área que precisa ser testada. A engenharia social reúne informações sobre a interação humana para obter informações sobre uma organização e seus computadores. É benéfico testar a capacidade da organização respectiva de impedir o acesso não autorizado aos seus sistemas de informação. Da mesma forma, este teste foi projetado exclusivamente para o fluxo de trabalho da organização / empresa.
- O Pentest normalmente consiste em coleta de informações, análise de riscos e vulnerabilidades, explorações de vulnerabilidades e preparação de relatórios finais.
- Também é essencial conhecer os recursos de várias ferramentas disponíveis no Pentest. Este capítulo fornece informações e idéias sobre esses recursos.
- O que são ferramentas de Pentest?

- A tabela a seguir reúne algumas das ferramentas de penetração mais significativas e ilustra seus recursos -

Nome da ferramenta	**Objetivo**	**Portabilidade**	**Custo esperado**
Hping	Port Scanning Impressão digital remota de OC	Linux, NetBSD, FreeBSD, OpenBSD,	Livre
Nmap	Digitalização em rede Port Scanning OS Detection	Linux, Windows, FreeBSD, OS X, HP-UX, NetBSD, Sun, OpenBSD, Solaris, IRIX, Mac, etc.	Livre
SuperScan	Executa consultas, incluindo ping, whois, pesquisas de nome de host etc. Detecta portas UDP / TCP abertas e determina quais serviços estão sendo executados nessas portas.	Windows 2000/XP/Vista/7	Livre
p0f	Os fingerprinting Detecção de firewall	Linux, FreeBSD, NetBSD, OpenBSD, Mac OS X, Solaris, Windows e AIX	Livre
Xprobe	Remote active OS fingerprinting Port Scanning	Linux	Livre

	Impressão digital TCP		
Httprint	Detecção de impressões digitais do servidor da Web SSL Detectar dispositivos habilitados para web (por exemplo, pontos de acesso sem fio, comutadores, modems, roteadores)	Linux, Mac OS X, FreeBSD, Win32 (linha de comando e GUI	Livre
Nessus	Detectar vulnerabilidades que permitem que o cracker remoto controle / acesse dados confidenciais	Mac OS X, Linux, FreeBSD, Apple, Oracle Solaris, Windows	Edição gratuita e limitada
GFI LANguard	Detectar vulnerabilidades de rede	Windows Server 2003/2008, Windows 7 Ultimate / Vista, Windows 2000 Professional, Business / XP, Servidor 2000/2003/2008	Apenas versão de teste grátis
Iss Scanner	Detectar vulnerabilidades de rede	Windows 2000 Professional com SP4, Windows Server 2003 Standard com SO1, Windows XP Professional com SP1a	Apenas versão de teste grátis
Shadow Security Scanner	Detectar vulnerabilidades de rede, proxy de auditoria e servidores LDAP	Windows, mas verifica servidores criados em qualquer plataforma	Apenas versão de teste grátis

Estrutura Metasploit	Desenvolver e executar código de exploração em um destino remoto Testar vulnerabilidade de sistemas de computador	Todas as versões do Unix e Windows	Livre
Brutus	Cracker de senha Telnet, ftp e http	Windows 9x / NT / 2000	Livre

HACKER

Quem são os hackers éticos?

Hackers éticos são especialistas em computadores que têm permissão legal para invadir um sistema de computador com o objetivo de se proteger dos hackers criminosos. Um hacker ético identifica as vulnerabilidades e os riscos de um sistema e sugere como eliminá-los.

Quem são os hackers criminais?

Hackers criminais são aqueles especialistas em programação de computadores que cortam outros sistemas com a intenção de roubar dados, roubar dinheiro, difamar o crédito de outros, destruir outros, chantagear alguém etc.

O que os criminosos hackers podem fazer?

Depois que um sistema é invadido, um hacker criminoso pode fazer qualquer coisa com esse sistema. As duas imagens a seguir, CC Palmer, publicadas em pdf.textfiles.com, ilustram um exemplo simples de uma página invadida -

Quais são os conjuntos de habilidades de hackers éticos?

Os hackers éticos especialistas têm os seguintes conjuntos de habilidades para invadir o sistema com ética

- Eles devem ser confiáveis.
- Quaisquer que sejam os riscos e vulnerabilidades, eles descobrem ao testar o sistema, eles precisam mantê-los confidenciais.
- Os clientes fornecem informações confidenciais sobre a infraestrutura do sistema, como endereço IP, senha etc. Os hackers éticos precisam manter essas informações em sigilo.
- Os hackers éticos devem ter um bom conhecimento de programação de computadores, redes e hardware.

- Eles devem ter boas habilidades analíticas para analisar a situação e especular o risco antecipadamente.
- Eles devem ter a habilidade de gerenciamento juntamente com paciência, pois o Pentestpode levar um dia, uma semana ou até mais.

O que os hackers éticos fazem?

Os hackers éticos, enquanto realizam Pentest, basicamente tentam encontrar as respostas para as seguintes perguntas -

- Quais são os pontos fracos que um hacker criminoso pode atingir?
- O que um hacker criminoso pode ver nos sistemas de destino?
- O que um hacker criminoso pode fazer com essas informações confidenciais?

Além disso, é necessário um hacker ético para lidar adequadamente com as vulnerabilidades e riscos, que ele descobriu existir no (s) sistema (s) de destino. Ele precisa explicar e sugerir os procedimentos de prevenção. Por fim, prepare um relatório final de todas as suas atividades éticas que ele realizou e observou ao realizar Pentest.

Tipos de hackers

Os hackers normalmente são divididos em três categorias.

Black Hat Hackers

Um "hacker de Blackhat" é um indivíduo que possui um extenso software de computador, além de hardware, e seu objetivo é violar ou ignorar a segurança da Internet de outra pessoa. Os hackers de Blackhat também são populares como crackers ou hackers do lado escuro.

White Hat Hackers

O termo "hacker de chapéu branco" refere-se a um hacker de computador ético, especialista em segurança de computadores, especializado em Pentest e em outras metodologias de testes associadas. Seu papel principal é garantir a segurança do sistema de informações de uma organização.

Hacker de chapéu cinza

O termo "hacker de chapéu cinza" refere-se a um hacker de computador que quebra o sistema de segurança de computadores cujos padrões éticos se situam entre algo puramente ético e apenas malicioso.

Pentest vs. Hacking Ético

O Pentest está intimamente relacionado ao hacking ético, portanto esses dois termos são frequentemente usados de forma intercambiável. No entanto, há uma fina linha de diferença entre esses dois termos. Este capítulo fornece informações sobre alguns conceitos básicos e diferenças fundamentais entre Pentest e hackers éticos.

Pentest

O Pentest é um termo específico e se concentra apenas na descoberta de vulnerabilidades, riscos e ambiente de destino com o objetivo de proteger e assumir o controle do sistema. Ou, em outras palavras, o Pentest visa os sistemas de defesa da organização respectiva, consistindo em todos os sistemas de computadores e sua infraestrutura.

Hacking Ético

Por outro lado, hacking ético é um termo extenso que abrange todas as técnicas de hacking e outras técnicas de ataque de computador associadas. Portanto, além de descobrir as falhas e vulnerabilidades de segurança e garantir a segurança do sistema de destino, está além de invadir o sistema, mas com uma permissão para salvaguardar a segurança para fins futuros. Portanto, é possível que seja um termo genérico e o Pentest seja uma das características do hacking ético.

A seguir, estão as principais diferenças entre o Pentest e o hacking ético, listadas na tabela a seguir -

Como as técnicas de penetração são usadas para proteger contra ameaças, os possíveis invasores também estão se tornando cada vez mais sofisticados e inventando novos pontos fracos nos aplicativos atuais. Portanto, um tipo específico de Pentest única não é suficiente para proteger sua segurança dos sistemas testados.

De acordo com o relatório, em alguns casos, uma nova brecha de segurança é descoberta e um ataque bem-sucedido ocorre imediatamente após o

Pentest. No entanto, isso não significa que o Pentest seja inútil. Isso significa apenas que, é verdade que, com Pentest completos, não há garantia de que um ataque bem-sucedido não ocorra, mas definitivamente, o teste reduzirá substancialmente a possibilidade de um ataque bem-sucedido.

Veja a seguir a diferença entre PENTEST E Hacking Ético

Pentest	Hacking Ético
Um termo restrito se concentra no Pentest apenas para proteger o sistema de segurança.	Um termo abrangente e Pentest é um dos seus recursos.
Um testador essencialmente precisa ter um conhecimento abrangente de tudo o que é necessário para ter o conhecimento apenas da área específica para a qual ele realiza o teste com caneta.	Um hacker ético precisa essencialmente ter um conhecimento abrangente de programação de software e hardware.
Um testador não precisa necessariamente ser um bom redator de relatórios.	Um hacker ético precisa essencialmente ser um especialista em elaboração de relatórios.
Qualquer testador com algumas entradas de Pentest pode executar o teste com caneta.	É necessário ser um profissional especialista no assunto, que possua a certificação obrigatória de hackers éticos para ser eficaz.
Trabalho de papel em menos do que o hacking ético.	São necessários trabalhos detalhados em papel, incluindo acordo legal etc.
Para executar esse tipo de teste, é necessário menos tempo.	O hacking ético envolve muito tempo e esforço em comparação com o Pentest.
Normalmente, a acessibilidade de sistemas de computadores inteiros e sua infraestrutura não exige. A acessibilidade é necessária apenas	De acordo com a situação, normalmente requer toda uma gama de acessibilidade a todos os sistemas de computadores e sua infraestrutura.

para a parte para a qual o testador está realizando o teste com caneta.	

Limitações do Pentest

Devido ao ritmo acelerado dos desenvolvimentos no campo da informação e da tecnologia, a história de sucesso dos Pentest é comparativamente curta. Quanto mais proteção aos sistemas for necessária, mais frequentemente do que você precisará executar Pentest, a fim de diminuir a possibilidade de um ataque bem-sucedido ao nível apreciado pela empresa.

A seguir, estão as principais limitações do Pentest -

- **Limitação de tempo** - como todos sabemos, o Pentest não é um exercício vinculado a todo momento; no entanto, especialistas em Pentest alocaram uma quantidade fixa de tempo para cada teste. Por outro lado, os atacantes não têm restrições de tempo, planejam isso em uma semana, mês ou até anos.
- **Limitação de escopo** - Muitas organizações não testam tudo, devido a suas próprias limitações, incluindo restrições de recursos, segurança, orçamento, etc. Da mesma forma, um testador tem escopo limitado e precisa deixar muitas partes dos sistemas que possam ser muito mais vulnerável e pode ser um nicho perfeito para o invasor.
- **Limitação no acesso** - Mais frequentemente, os testadores restringem o acesso ao ambiente de destino. Por exemplo, se uma empresa realizou o Pentest nos seus sistemas DMZ de todas as suas redes da Internet, mas e se os atacantes atacarem através do gateway normal da Internet.
- **Limitação de métodos** - Há chances de o sistema de destino travar durante um Pentest; portanto, alguns dos métodos de ataque específicos provavelmente serão desativados para um testador de penetração profissional. Por exemplo, produzir uma inundação de negação de serviço para desviar um administrador de sistema ou rede de outro método de ataque, geralmente uma tática ideal para um cara realmente ruim, mas é provável que fique fora das regras de envolvimento da maioria dos testadores profissionais de penetração .
- **Limitação dos conjuntos de habilidades de um testador de penetração** - Geralmente, os testadores profissionais de penetração são

limitados, pois possuem habilidades limitadas, independentemente de seus conhecimentos e experiências anteriores. A maioria deles está focada em uma tecnologia específica e com conhecimento raro de outros campos.

- **Limitação de explorações conhecidas** - Muitos dos testadores estão cientes apenas dessas explorações, que são públicas. De fato, seu poder imaginativo não é tão desenvolvido quanto os atacantes. Os atacantes normalmente pensam muito além do pensamento de um testador e descobrem a falha no ataque.
- **Limitação à experiência** - A maioria dos testadores tem um prazo e segue as instruções já fornecidas pela organização ou pelos idosos. Eles não tentam algo novo. Eles não pensam além das instruções dadas. Por outro lado, os atacantes são livres para pensar, experimentar e criar um novo caminho para atacar.

Além disso, o Pentest não pode substituir os testes de segurança de rotina da TI, nem substituir uma política geral de segurança, mas o Pentest complementa os procedimentos de revisão estabelecidos e descobre novas ameaças.

Remediação

Os esforços de Pentest - por mais completos que sejam - nem sempre podem garantir uma descoberta exaustiva de todas as instâncias em que a eficácia de um controle de segurança é insuficiente. A identificação de uma vulnerabilidade ou risco de script entre sites em uma área de um aplicativo pode não expor

definitivamente todas as instâncias dessa vulnerabilidade presentes no aplicativo. Este capítulo ilustra o conceito e a utilidade da correção.

O que é remediação?

A correção é um ato de oferecer uma melhoria para substituir um erro e corrigi-lo. Freqüentemente, a presença de vulnerabilidade em uma área pode indicar fraqueza nas práticas de processo ou desenvolvimento que poderiam ter replicado ou ativado vulnerabilidade semelhante em outros locais. Portanto, durante a correção, é importante que o testador investigue cuidadosamente a entidade ou aplicativos testados com controles de segurança ineficazes em mente.

Por esses motivos, a respectiva empresa deve tomar medidas para corrigir qualquer vulnerabilidade explorável dentro de um período de tempo razoável após o Pentest original. De fato, assim que a empresa concluir essas etapas, o testador de caneta deverá realizar um novo teste para validar os controles recém-implementados, capazes de mitigar o risco original.

Os esforços de correção que se estendem por um período mais longo após o teste inicial da caneta possivelmente exigem a realização de um novo trabalho de teste para garantir resultados precisos do ambiente mais atual. Essa determinação deve ser feita após uma análise de risco de quanta alteração ocorreu desde que o teste original foi concluído.

Além disso, em condições específicas, o problema de segurança sinalizado pode ilustrar uma falha básica no respectivo ambiente ou aplicativo. Portanto, o escopo de um novo teste deve considerar se quaisquer alterações causadas pela correção identificadas no teste são classificadas como significativas. Todas as alterações devem ser testadas novamente; no entanto, se um sistema inteiro é testado novamente ou não, será determinado pela avaliação de riscos das alterações.

Leis e questões legais sobre o Pentest

Antes de permitir que alguém teste dados confidenciais, as empresas normalmente tomam medidas em relação à disponibilidade, confidencialidade e integridade dos dados. Para que este contrato seja estabelecido, a conformidade legal é uma atividade necessária para uma organização.

Os regulamentos legais mais importantes que devem ser observados ao estabelecer e manter sistemas de segurança e autorização são apresentados abaixo no contexto para uso na implementação de Pentest.

Quais são as questões legais?

A seguir, estão alguns dos problemas que podem surgir entre um testador e seu cliente -

- O testador é desconhecido do cliente - portanto, com que fundamento, ele deve ter acesso a dados confidenciais
- Quem assumirá a garantia de segurança dos dados perdidos?
- O cliente pode culpar pela perda de dados ou confidencialidade ao testador

O Pentest pode afetar o desempenho do sistema e levantar questões de confidencialidade e integridade; portanto, isso é muito importante, mesmo em um Pentest interno, realizado por uma equipe interna para obter permissão por escrito. Deve haver um acordo por escrito entre um testador e a empresa / organização / indivíduo para esclarecer todos os pontos relacionados à segurança, divulgação de dados, etc. antes de iniciar o teste.

Uma **declaração de intenções** deve ser elaborada e devidamente assinada por ambas as partes antes de qualquer trabalho de teste. Deve-se ressaltar claramente que o escopo do trabalho e o que você pode ou não fazer ao executar testes de vulnerabilidade.

Para o testador, é importante saber quem possui os negócios ou sistemas nos quais está sendo solicitado a trabalhar e a infraestrutura entre os sistemas de

teste e seus destinos que podem ser potencialmente afetados pelo teste com caneta. A idéia é ter certeza;

- **o testador** tem permissão por escrito, com parâmetros claramente definidos.
- **a empresa** possui os detalhes de seu testador de caneta e uma garantia de que ele não vazaria nenhum dado confidencial.

Um acordo legal é benéfico para ambas as partes. Lembre-se de que os regulamentos mudam de país para país; portanto, mantenha-se a par das leis de seu país. Assine um contrato somente depois de considerar as respectivas leis.

Ferramentas para o Pentest

Kali Linux

Atualmente a mais conhecida o Kali Linux foi desenvolvido pela Offensive Security assumindo o manto do BACKTRACK. Kali Linux é baseado no Debian. Ele vem com uma grande quantidade de ferramentas de teste de penetração de vários campos de segurança e forense.

A versão mais recente do Kali Linux (2019.4) trocou o ambiente de desktop: em vez do Gnome, ele traz o Xfce por padrão, que consome menos recursos

Kali Linux é uma distribuição GNU/Linux baseada no Debian, considerado o sucessor do Back Track

Nethunter Kex

O NetHunter Kex permite conectar o dispositivo Android a uma saída HDMI, teclado sem fio e mouse Bluetooth para obter uma experiência de desktop.

O Kali Linux é um projeto de código aberto que é mantido e financiado pela Offensive Security, empresa que trabalha com "hacking ético" — ou seja, com ciberataques simulados para testar a segurança de um sistema.

Site Oficial: https://www.kali.org/

HStrike

O **HStrike** é uma plataforma de pentest em nuvem, desenvolvida pela Hacker Security, com objetivo de automatizar e facilitar o trabalho de profissionais da área de segurança da informação e também da área de tecnologia da informação em geral.

Com apenas uma conta e acesso a Internet, você pode realizar um Pentest de qualquer lugar e dispositivo, basta ter um navegador instalado.

O HStrike conta com diversas ferramentas profissionais dentro dele, algumas muito conhecidas, porém a maioria desenvolvida do zero pela equipe Hacker Security.

Site oficial: https://hstrike.com/

Metasploit

Muito conhecido também é o **Metasploit Penetration Testing,** que pode ser encontrado em sua versão gratuita e paga.

Para teste de invasão (pentest) o Metasploit é **a**mplamente utilizado por profissionais de segurança cibernética e hackers éticos esta é uma ferramenta que você tem que conhecer. Metasploit é essencialmente um projeto de segurança de computador (framework) que fornece ao usuário informações vitais sobre vulnerabilidades de segurança conhecidas e ajuda a formular planos, estratégias e metodologias para a exploração de teste de penetração e de ensaio IDS.

Site Oficial: https://www.metasploit.com/

Conclusão

Os testes de penetração oferecem informações incomparáveis sobre a eficácia da segurança de uma organização, bem como um roteiro para aprimorar a segurança. Ao contratar especialistas para simular um ataque cibernético, as vulnerabilidades podem ser identificadas e corrigidas antes de serem exploradas por um hacker ou um membro malicioso.

Aplicações Web são focos de Pentest

São Desenvolvidas em cima do protocolo HTTP e dos Web Servers.

Utilizam diversas linguagens e tecnologias (PHP, ASP, .NET, J2EE, Applets Java, ActiveX, CSS, DOM, SOAP, XML, C#, AJAX, SQL, RMDBS, Perl, Python, Ruby, Cookies, HTML, Javascript, Flash, ISAPI, WebDAV, CGI, ColdFusion, etc).

O crescimento exponencial das aplicações gerou crescimento exponencial dos ataques.

Todo cuidado é pouco!