PenTeste

PenTeste são testes de intrusão/invasão, realizados por especialistas em cibersegurança, com intuito de identificar vulnerabilidades em sistemas.

Em resumo PenTeste são invasões consentidas contra sistemas informatizados, para verificar se é ou não possível invadir tais sistemas. De posse dos resultados do PenTest, as equipes de cibersegurança podem tomar decisões melhores a respeito da segurança dos sistemas/informações.

Segundo CARDWELL 2022, em seu livro **Building Virtual Pentesting Labs for Advanced Penetration Testing**, testes de segurança são processos ou métodos para determinar se sistemas protegem e mantém as informações como planejado. Desta forma, *PenTeste é uma metodologia e não um produto*.

Ao final do PenTeste, deve ser emitido um diagnóstico a respeito da segurança do sistema testado. Tal diagnóstico, deve ser utilizado para eliminar vulnerabilidade e mitigar ciberameaças, melhorando assim a segurança do cliente.

> Atenção!!! Um PenTeste realizado sem o consentimento da vítima, pode ser considerado crime.

Os passos realizados em PenTestes, podem variar dependendo do profissional realizando o PenTeste ou dos objetivos a serem alcançados. Todavia, esses passos basicamente são:

- 1) **Determinar o Escopo do PenTeste** - esse passo consiste em entender onde o PenTeste será executado e quais são os objetivos do PenTeste. Neste passo, algumas perguntas devem ser realizadas e respondidas:

    - O que deve ser testado? -
    - Como deve ser testado?
    - Em quais condições?
    - Qual é o limite aceitável para o teste?
    - etc...

  Aqui também pode ser combinado qual é o tipo de PenTeste que será realizado, tal como:

    - **Blind** ou **black box** - no qual o PenTeste é realizado sem qualquer conhecimento a respeito do alvo. É um teste às cegas;
    - **Double blind** - idem ao anterior, mas neste o alvo também não sabe que o teste vai acontecer;
    - **Gray box** - quem realiza o PenTeste tem algumas informações a respeito do ambiente a ser testado e o alvo também sabe que o teste será realizado;
    - **Double gray box** - idem ao anterior, mas o alvo também tem informações parciais a respeito do teste;
    - **Tandem** ou **white box** - neste estilo de PenTeste o atacante recebe informações antecipadas e detalhadas a respeito do alvo e também o alvo sabe que será testado;
    - **Reversal** - similar ao anterior, todavia o alvo não sabe que será testado.

    > Essas definições podem variar um pouco, mas basicamente a ideia é essa.

  É necessário notar, que todos os detalhes do PenTeste devem ser combinados com o cliente (alvo). É altamente recomendável (se não obrigatório) ter um contrato entre o cliente e o realizador do PenTeste, de forma que o PenTeste não seja considerado crime em um segundo momento. No caso de testes a cegas e suas variações, grande parte da equipe que trabalha no cliente/alvo não sabe dos testes, entretanto é necessário que alguém (chefe, gerente, responsável, etc) saiba e aceite previamente o PenTeste, caso contrário isso poderá ser considerado crime.

- 2) **Obtendo Informações a Respeito do Alvo** - esse passo tenta obter a maior quantidade possível de informações a respeito do alvo. Isso pode ser feito utilizando várias técnicas e ferramentas, mas basicamente esse passo consiste em obter informações que dizem respeito a: empresas, pessoas, serviços e tudo que está ligado direta ou indiretamente com o alvo. Por exemplo: (i) o executor do teste, pode obter informações de domínios da vítima na Internet, URLs, *hosts*, etc; (ii) vasculhar as redes sociais das pessoas ligadas ao alvo ou informações publicadas em outras fontes (*blogs*, justiça, etc).

- 3) **Escaneamento** - esse passo faz uma análise mais profunda e detalhada da estrutura alvo. Principalmente em *hosts* descobertos no passo anterior. Nesta fase são identificadas informações detalhadas a respeito de redes, *hosts*, sistema operacional. Também, nos *hosts* descobertos, são identificados, portas de redes abertas, serviços em execução e suas possíveis vulnerabilidades (alguns livros tratam isso como outros passos, chamados de **Enumeração do Alvo** e **Mapeamento de Vulnerabilidades** - mas aqui deixaremos dentro do Escaneamento).

- 4) **Ganhando Acesso** - é aqui que o profissional realizando o PenTest vai utilizar todas as informações levantadas nos passos anteriores para efetivamente fazer o teste de invasão no alvo. A invasão pode dar-se de várias formas, mas basicamente vai estar dentro dos seguintes contextos:
    - Via Internet - WAN;
    - Via rede local - LAN;
    - Localmente no computador;
    - *Offline*.

  A invasão efetiva, pode ocorrer através de softwares que exploram as vulnerabilidades (*exploits*) descobertas no passo anterior. Neste passo o profissional realizando o teste pode utilizar ferramentas, que automatizam o processo de invasão, ou mesmo aplicar métodos/técnicas manuais que ajudam a demostrar se alguma falha identificada previamente pode ou não ser um risco eminente ao sistema.

  Nesta fase o invasor também pode utilizar de **Engenharia Social**, para conseguir atingir seu objetivo e ganhar o acesso à hosts ou informações do alvo. O uso de Engenharia Social, pode ser considerado um passo do PenTeste, depentendo da metodologia escolhida para o teste.

- 5) **Mantendo o Acesso** - Após conseguir efetivamente explorar alguma vulnerabilidade e invadir o alvo. O profissional realizando o PenTeste pode empregar técnicas para **Escalar Privilégios**, demonstrando, por exemplo, que um invasor poderia acessar o alvo como um usuário comum e depois mudar para um usuário administrador, ou seja, com privilégios. Da mesma forma o profissional por trás do teste de segurança, pode por exemplo, instalar algum software, tal como *backdoor*, para demonstrar que invasores poderiam manter o acesso ao alvo. Algumas pessoas vão considerar que Escalar Privilégios também é mais um passo de PenTeste.

- 6) **Documentação e Relatórios** - Após a realização do PenTest o profissional que o fez, ou a equipe, deve criar um documento dando o diagnóstico obtido depois do PenTeste. Ou seja, é necessário reportar para o cliente/alvo, tudo o que foi descoberto durante os testes. Assim, o cliente pode a partir desses documentos, pensar em formas de sanar ou pelo menos mitigar os problemas apontados pelo PenTest. Note, que pode ser necessário fazer relatórios e documentos distintos dependendo do setor da empresa que deve receber/ler tais resultados. Por exemplo, o gerente vai querer saber dos resultados de forma mais superficial, a nível de negócios (há problemas? quantos? o que eles podem causar?). Já o relatório para equipe de TI, deve informar detalhes mais técnicos (quais falhas foram exploradas? como? softwares? há como sanar?).

Como foi explicado brevemente no texto anterior, o assunto PenTeste é relativamente complexo, exigindo vários passos, métodos e ferramentas. Também o PenTeste exige que o profissional que irá realizá-lo tenha muito conhecimento em várias áreas da informática.

Assim, para nossas aulas, devido a restrições de tempo, vamos nos concentrar apenas em dois passos do PenTeste, que são:

- Escaneamento, mais especificamente iremos nos concentrar no uso do Nmap para escanear redes, *hosts*, serviços e vulnerabilidades.
- Também iremos ver um pouco a respeito do Metasploit para realizar testes de invasão, ou seja, também faremos uma introdução ao passo Ganhando Acesso.

> Indiretamente também iremos acabar abordando superficialmente outros passos e da mesma forma citando outras ferramentas que são utilizadas em PenTeste. Todavia, é altamente recomendável que o leitor deste texto se aprofunde em todos os passos de PenTeste e ferramentas, por isso fica a dica de ler principalmente os livros da seção Referência.

- Escaneamento
- Explorando o Alvo

Referência

- HIMANSHU SHARMA. Kali Linux - An Ethical Hacker's Cookbook : Over 120 Recipes to Perform Advanced Penetration Testing with Kali Linux. Birmingham, UK: Packt Publishing, 2017. ISBN 9781787121829. Disponível em: https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=1617212&lang=pt-br&site=eds-live&scope=site. Acesso em: 26 ago. 2022.

- KEVIN CARDWELL. Building Virtual Pentesting Labs for Advanced Penetration Testing - Second Edition. Birmingham: Packt Publishing, 2016. v. Second editionISBN 9781785883491. Disponível em: https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=1344064&lang=pt-br&site=eds-live&scope=site. Acesso em: 31 ago. 2022.
- LEE ALLEN, *et al* - Kali Linux - Assuring Security by Penetration Testing. Packt Publiching, 2014.
- https://www.spiritsec.com/2021/03/02/pentest-quais-os-tipos-de-ataque/
- https://prosect.com.br/quais-os-principais-tipos-de-pentest/