CETEPI - I
PAULO AFONSO

EDUCAÇÃO PROFISSIONAL DA BAHIA
Trabalho, Educação e Desenvolvimento

SEGURANÇA DE SISTEMAS E REDES

TÁSSIO JOSÉ GONÇALVES GOMES
www.tassiogoncalves.com.br
tassiogoncalvesg@gmail.com

CONTEÚDO

Visão geral sobre o Pentest

Tipos de Pentest

As fases de um ataque

Categorias de ataques

Metodologias existentes

Como conduzir um teste de invasão

Aspectos Legais

VISÃO GERAL SOBRE O PENTEST

O Teste de Intrusão é um processo de análise detalhada do nível de segurança de um sistema ou rede usando a perspectiva de um infrator.

Trata-se de um teste realista ao nível de segurança das infraestruturas e da informação que estas detêm.

VISÃO GERAL SOBRE O PENTEST

O objetivo principal é simular de forma controlada um ataque real que normalmente é executado por criminosos.

TIPOS DE PENTEST

Blind

Double blind

Gray Box

Double Gray Box

Tandem

Reversal

BLIND

Nessa modalidade o auditor não conhece nada sobre o alvo que irá atacar, porém o alvo sabe que será atacado e o que será feito durante o teste.

DOUBLE BLIND

Nessa modalidade o auditor não conhece nada sobre o alvo, e o alvo não sabe que será atacado e tão pouco sabe quais testes o auditor irá realizar.

GRAY BOX

Nessa modalidade o auditor tem conhecimento parcial do alvo, e o alvo sabe que será atacado e também sabe quais testes serão realizados.

Aproxima-se de um teste onde é simulado o ataque de dentro de um ambiente completamente monitorado e controlado.

DOUBLE GRAY BOX

Nessa modalidade o auditor tem conhecimento parcial do alvo, e o alvo sabe que será atacado, porém, não sabe quais testes serão executados.

TANDEM

Nessa modalidade o auditor tem total conhecimento sobre o alvo, o alvo sabe que será atacado e o que será feito durante o ataque. Também conhecido como “caixa de cristal”.

REVERSAL

Nessa modalidade o auditor tem conhecimento total do alvo, porém o alvo não sabe que será atacado, e tão pouco sabe quais testes serão executados.

Esse formato de teste é ideal para testar a capacidade de resposta e como está o timing de ação da equipe de resposta a incidentes do alvo.

AS FASES DE UM ATAQUE

Levantamento de Informações

Varredura

Mantendo acesso

Limpando rastros

AS FASES DE UM ATAQUE

Um ataque, ou teste de invasão, é composto por uma série de fases, onde em cada uma determinadas operações são realizadas.

O que vai definir a diferença de um teste de invasão e um ataque realizado por um cracker, são justamente a intenção, o escopo e o espaço de tempo disponível para o mesmo.

LEVANTAMENTO DE INFORMAÇÕES

Essa é a fase mais importante de um ataque e de um teste de invasão.

Podemos dizer que essa é a fase abrangente, e a fase seguinte detalha as informações adquiridas nessa primeira fase.

LEVANTAMENTO DE INFORMAÇÕES

Qualquer informação que seja vinculado ao alvo é considerada de valor nesse primeiro passo:

- Concorrentes
- Nome de funcionários
- Endereços
- Telefones
- Sites
- Empresas
- Comunidades sociais
- Empresas do mesmo grupo e etc.

VARREDURA

Nessa fase o atacante busca informações mais detalhadas o alvo, que posam permitir definir seus vetores de ataque e enxergar as possibilidades que podem permitir ganhar acesso ao sistema, através da exploração de alguma falha encontrada.

VARREDURA

Aqui buscamos informações que respondam algumas perguntas, como por exemplo:

- Qual sistema operacional o alvo utiliza?
- Quais os serviços estão sendo executados no alvo?
- Quais serviços estão disponíveis para acesso?
- Qual a versão de cada serviço sendo executado?
- Há IDS/IPS na rede?
- Há honeypots na rede?
- Há firewalls na rede?
- Existe uma rede interna e outra externa, como uma DMZ?
- Há serviços com acesso público rodando em alguma máquina?
- Há algum software malicioso já sendo executado em alguma máquina?

GANHANDO ACESSO

Aqui o atacante coloca em prática tudo aquilo que planejou a partir das informações obtidas previamente.

Dependendo de seus vetores de ataque, ele pode realizar uma série de ataques buscando ganhar acesso ao sistema alvo.

GANHANDO ACESSO

Exemplos:

- Ataques de força bruta local
- Ataques de força bruta remoto
- Captura de tráfego de rede
- Ataque de engenharia social
- Ataques às aplicações WEB
- Exploração de serviços
- Exploração de sistema operacional

MANTENDO ACESSO

Após conseguir o acesso, o atacante busca, de alguma forma, manter o acesso conseguido através de seus ataques.

Essa fase, quando realizada durante um teste de invasão, precisa de extremo cuidado e planejamento para não trazer comprometimentos e prejuízos desnecessários ao alvo.

LIMPANDO RASTROS

Nessa fase final do ataque, o atacante apaga todos os seus rastros, todos os registros de operações realizadas dentro do sistema comprometido.

CATEGORIAS DE ATAQUES

Há vários tipos de ataque possíveis de serem realizados. Podemos dividir tais ataques em dois grandes grupos:

- Server Side Attacks
- Client Side Attacks

SERVER SIDE ATTACKS

Server Side Attack ou ataque ao servidor foca na tentativa de explorar serviços que estão em execução em um determinado dispositivo. Normalmente não precisam de interação do usuário e provê uma Shell remota para o atacante.

SERVER SIDE ATTACKS

São exemplos de ataques a servidores:

- Ataques a servidores WEB
- Ataques a servidores de e-mail
- Ataques a servidores DNS
- Ataques a serviços RPC

CLIENT SIDE ATTACKS

Client Side Attacks ou ataques ao cliente foca na tentativa de explorar aplicações que são executadas no computador e que normalmente precisam de uma interação da pessoa para que o ataque seja executado.

CLIENT SIDE ATTACKS

São exemplos de ataques ao cliente:

- Exploração de falhas no Internet Explorer
- Exploração de falhas em editores de texto
- Exploração de falhas em Clientes de E-mail
- Exploração de falhas em programas reprodutores de vídeo

Packs como Mpack e IcePack exploram vulnerabilidades em navegadores webs, ou seja, realizam um client side attack.

METODOLOGIAS EXISTENTES

Para um teste de invasão não ficar “solto” e sem uma sequência lógica coerente, a comunidade de segurança, através de alguns órgãos, associações, institutos e pesquisadores, criou uma série de metodologias para servirem como guias básicos para a correta realização de testes de invasão.

METODOLOGIAS EXISTENTES

Isso permite uma certa padronização nos testes realizados seguindo uma outra metodologia.

Podemos citar as seguintes metodologias conhecidas internacionalmente:

METODOLOGIAS EXISTENTES

- OSSTMM
- OWASP Testing Guide
- NIST SP800-115 e SP800-42
- ISSAF
- PenTest Frameworks

COMO CONDUZIR UM TESTE DE INVASÃO

Alguns passos básicos são necessários para a preparação e realização de um teste de invasão, para que o mesmo seja bem sucedido.

PASSOS DE PREPARAÇÃO PARA O PENTEST

Passo 1: Converse com seu cliente sobre as necessidades do teste;

- Esse é um dos passos mais importantes, pois não podemos deixar que existam "zonas cinza" no que foi contratado e acertado, entre o cliente e o pen tester.

Passo 2: Prepare o contrato de serviço e peça ao cliente para assinálos;

- Depois de tudo definido no primeiro passo, é feito um contrato de prestação de serviço, onde está descrito o que será realizado (escopo, horários, equipe de profissionais, permissões, etc) e assinado por contratado e contratante.

PASSOS DE PREPARAÇÃO PARA O PENTEST

Passo 3: Prepare um time de profissionais e agende o teste;

- Aqui reunimos os profissionais que participarão dos testes e lhes passamos todas as informações pertinentes ao que será realizado.

Passo 4: Realize o teste;

- Nesse passo é onde o teste é efetivamente executado. Lembrando sempre de seguir o que foi acordado com o cliente e respeitar as cláusulas do contrato e NDA assinados.

PASSOS DE PREPARAÇÃO PARA O PENTEST

Passo 5: Analise os resultados e prepare um relatório;

- Todas as informações coletadas, resultados obtidos e ocorrências durante a realização do teste são posteriormente reunidas e analisadas.

Passo 6: Entregue o relatório ao cliente.

- O relatório pós-teste, é entregue APENAS para a pessoa responsável pela contratação do teste de invasão, ou definida em contrato. Essa medida extrema é tomada justamente para evitar qualquer vazamento possível de informações.

ASPECTOS LEGAIS

É importante atentarmos para os aspectos legais de um teste de invasão, e se os mesmo estão de acordo com as leis vigentes no país, e principalmente com o que foi assinado no contrato de prestação de serviço.

TESTE DE INVASÃO SEM PERMISSÃO É CRIME!

Portanto, tenha sempre um contrato prévio assinado com o cliente, onde serão definidos os seguintes pontos:

- Limites do teste: até onde pode ir;
- Horários: períodos de menor utilização ou menos críticos;
- Equipe de suporte: caso haja alguém para tomar providências caso alguém ataque tenha efeitos colaterais;
- Contatos: ao menos três contatos, com e-mail, endereço e telefone;
- Permissão assinada: um documento assinado pelo responsável pela empresa, com os nomes das pessoas da equipe autorizadas a realizar os testes.

EXERCÍCIOS TEÓRICOS

1 – Qual o objetivo da OSSTMM?

2 – Qual a necessidade da utilização de uma metodologia para realizar um teste de invasão?

3 – Quais as fases de um ataque?