PEN-TEST (PENETRATION TEST)

Introducão ao Pen-Test

Consiste em uma avaliação de maneira realista da segurança empregada no ambiente computacional de uma empresa. Esse teste é capaz de descobrir na prática quais são as falhas do ambiente e também quais danos elas podem causar caso fossem exploradas por um Cracker (atacante mal intencionado).

Este profissional trabalha de maneira muito semelhante a um Cracker , porém, o que o diferencia o Pen Tester do Cracker é a maneira ética de lidar com a intrusão. O objetivo final do Pen Tester é apontar as falhas do ambiente para que possam ser corrigidas, diferente do objetivo final de um Cracker cuja intensão é roubar ou destruir dados.

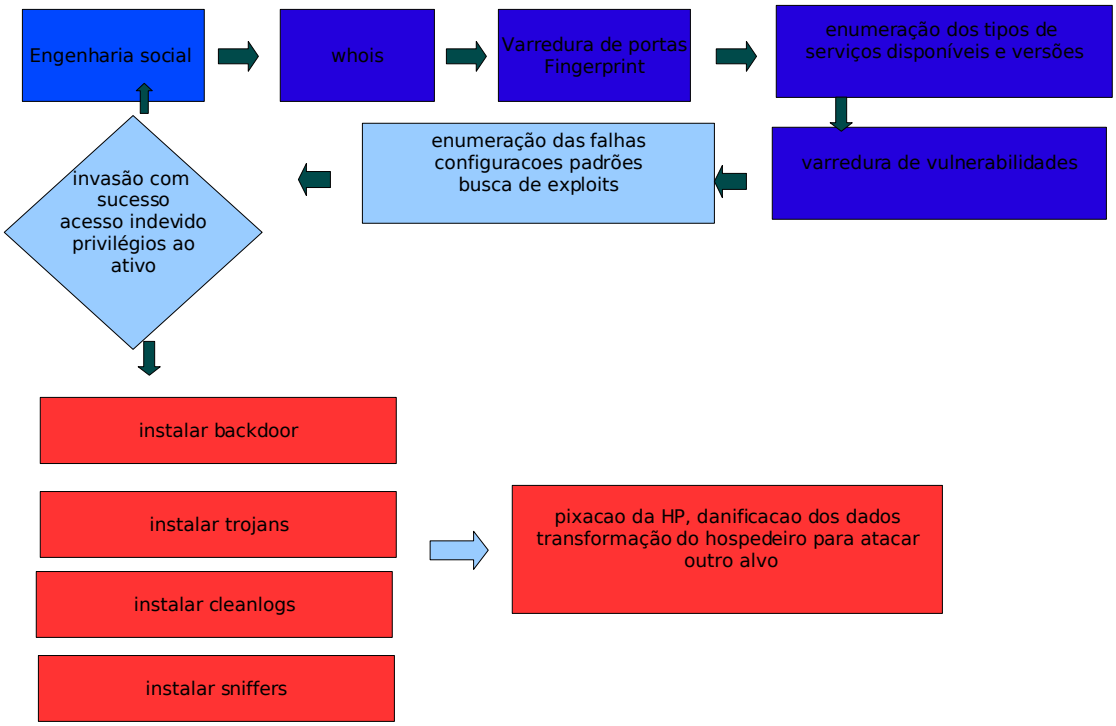
Problemas no Universo da segurança da Informação

Atualmente sofremos diversos problemas quando tentamos garantir a segurança de um ambiente. A cada dia, aumenta consideravelmente o numero de servidores e serviços operantes em rede.

Em contrapartida, se torna cada vez mais fácil o uso dos computadores domésticos. Isso faz com que a grande maioria dos usuários domésticos não se preocupem em entender realmente como funcionam os recursos disponiveis e a maneira certa de utilizá-los.

São poucos os usuários que entendem que o computador que eles possuem em casa, pode ser usado por Cracker para realização de ataques de negação de serviços (DOS/DDOS) que prejudicam milhares de empresas a cada ano. Além disso, quando um Cracker domina a máquina de um usuário, ele pode ter acesso aos dados bancários do mesmo, o que leva a um grande prejuízo financeiro principalmente por parte das empresas de cartão de crédito.

Anatomia do ataque



footprint

rootkit

Um Pen Test possui começo, meio e fim. Portanto, Pen Testers e Crackers trabalham de forma semelhante com algumas diferenças:

1a. fase -> l**evantamento informação**: nesta fase do ataque cabe a um Pen Tester encontrar os principais ativos da empresa. Todos os seus alvos serão levantados nessa fase do ataque. Quando mais potenciais alvos ele encontrar, maior será a chance do mesmo encontrar alguma falha que possibilite ao mesmo entrar no ambiente computacional da empresa.

2a. fase -> **varreduras**: essa fase consiste em descobrir quais são as portas abertas dos alvos previamente selecionados, e descobrir a versão dos aplicativos que estão rodando nas mesmas. Isso é importante principalmente para escolha das vulnerabilidades que serão exploradas na terceira fase.

3a. fase -> **ganhando acesso**: nesta fase do ataque , cabe ao Pen Tester realizar a intrusão no sistema. Existem várias maneiras de se atacar um sistema, porém, as que têm se mostrado mais efetivas são: ataque ao sistema operacional e suas aplicações, captura de tráfego de rede em busca de senhas que tragam por protocolos inseguros e negação de serviços.

as fases seguintes diferenciam um Pen Tester dos Cracker

4a. fase-> **mantendo o acesso:** em um ataque real um cracker insere uma backdoor ou um rootkit na máquina que foi comprometida, para que possa voltar quando quiser, mesmo se a falha usada para atacar, tenha sido corrigida. O Pen Tester .....

5a. fase -> **Limpando rastros:** toto Pen Tester tem autorizacao para realizar o ataque sobre o alvo. E devido a esse motivo, não precisa ocultar rastros.

Tipo de Pen Test

BLIND -> nessa modalidade o auditor não conhece nada sobre o alvo que irá atacar, porem 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 sabe quais testes serão realizados.

DOUBLE GRAY BOX -> nessa modalidade o auditor tem conhecimento parcial do alvo e o alvo sabe que será atacado porem 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.

REVERSAL -> nessa modalidade o auditor tem conhecimento total do alvo, porem o alvo não sabe que será atacado, e tão pouco sabe quais testes serão executados.

Engenharia Social

A engenharia social é um dos meios mais utilizados de obtenção de informações sigilosas e importantes. Isso porque explora com muita sofisticação as "falhas de segurança dos humanos". As empresas investem fortunas em tecnologias de segurança de informações e protegem fisicamente seus sistemas, mas a maioria não possui métodos que protegem seus funcionários das armadilhas de engenharia social. A questão se torna mais séria quando usuários domésticos e que não trabalham com informática são envolvidos.

Uma definição aceitável do que é a engenharia social é a seguinte: engenharia social é qualquer método usado para enganação ou exploração da confiança das pessoas para a obtenção de informações sigilosas e importantes. Para isso, o enganador pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, etc.

Exemplo 1: você recebe uma mensagem *e-mail*, onde o remetente é o gerente ou alguém em nome do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de *Internet Banking* está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem. A execução deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso a conta bancária, aguardando que você digite sua senha. Na verdade, este aplicativo está preparado para furtar sua senha de acesso a conta bancária e enviá-la para o atacante.

Os 6 tipos de ataques

Reciprocidade
Validação Social
Consistência
Autoridade
Amizade
Escassez

Importância do Lixo

Todos os dias são jogados no lixo de empresas vários documentos por terem perdido sua utilidade. Porém para um atacante esses documentos são informações úteis para entender o funcionamento, a história e a maneira de operação da empresa.

Engenharia Social baseada em pessoas

As técnicas de engenharia social baseada em pessoas possuem diversas características que são utilizadas para que o atacante consigas as informacoes que deseja, dentre elas podemos citar:

- disfarces
- representações
- uso de cargos de alto nível
- ataque ao serviço de help desk
- observações

Engenharia Social baseada em computadores

Esses ataques são caracterizados por utilizarem técnicas de ataque baseadas no desconhecimento do usuário com relação ao uso correto da informática. Ex:

- cavalos de Tróia
- e-mails falsos
- websites falsos

Engenharia Social reversa

Este tipo de engenharia social tem três pontos chaves:

- sabotagem
- anuncio
- ajuda

imaginem o seguinte cenário: o atacante causa um problema em computador de uma empresa. Deixa um folheto de propaganda, de uma prestadora de suporte técnico, com a recepcionista da empresa. Alguém liga e pede ajuda ao atacante, e enquanto ele te ajuda, pega todas as informações que necessita do seu sistema.

UM CONCEITO IMPORTANTE

informações soltas não tem valor, porém o trabalho de um atacante é juntar as informações que conseguiu e montá-las como em um quebra cabeça para que as mesmas tenham valor e façam diferença dentro do contexto de ataque.

CONTRAMEDIA:

- formule políticas para procedimentos internos e externos
- verifique se a pessoa que solicita a Informação realmente pode ter acesso aquea informação
- crie uma boa barreira contra códigos maliciosos
- use o correio eletrônico de modo seguro
- treine funcionários e colaboradores

FOOTPRINT & FINGERPRINT

Footprint é a primeira etapa a ser realizada em um teste de intrusão. Durante essa etapa, o Pen-Tester coleta o máximo de informação para alimentar a anatomia de ataque. Podemos dizer que é a fase em que o Pen-Tester se prepará para realizar o ataque.

Em média, um Pen-Tester gasta 85% do tempo analisando um alvo e levantando informações sobre o mesmo. Apenas 15% do tempo é usado para realizar o ataque e avaliar a possibilidade de um atacante realizar procedimentos pós-invasão na máquina-alvo.

Quando estamos realizando um footprint, devemos buscar informações relativas à: topologia da rede, sistemas operacionais, quantidade de máquinas e localização física. Além disso é importante também descobrir informações sobre os funcionários da empresa, como: e-mails, cargos e função específica no ambiente.

Ferramentas

-
- whois
- host
- dnswalk

whois silva.eti.br

é importante saber que além da ferramenta whois, ainda podemos pesquisar informações de domínios usando a ferramenta **xwhois** e também **jwhois** , além disso, o registro.br também fornece estes dados.

outros sites internacionais:

www.ripe.net
www.arin.net
www.apnic.net
www.networksolutions.com

As pesquisas relacionadas, retornam informações importantes como:
Responsável
Endereco
Telefone
E-mail
DNS

Informação sobre DNS

O DNS se configurado de maneira insegura, pode revelar partes importantes da topologia de uma rede. Usando a ferramenta host poderíamos descobrir quais os servidores de nomes de um determinado domínio.

Ex.:
host -t ns silva.eti.br

também usando o comando host podemos descobrir o servidor de e-mail de um determinado domínio.

host -t mx silva.eti.br

também é possivel descobrir toda a base DNS de uma unica vez com o comando host

host -1 -v -t any silva.eti.br

FingerPRINT

Fingerprint é uma das principais técnicas de levantamento de informação (footprint) que é realizada por um Pen Tester antes que o mesmo comece a realizar os ataques em seu alvo.

A função dessa técnica é identificar a versão e distribuicão do ssitema operacional que irá receber a tentativa de intrusão.

Sendo assim, essa técnica é extremamente importante para que atacante consiga desenvolver de maneira mais precisa e menos ruidosa seu ataque.

Usando essa técnica o Pen Tester estará explorando problemas da pilha TCP/IP e verificando características únicas que permitem que o sitema alvo seja identificado.

Só depois que isso for feito, o cracker poderá escolher as melhores ferramentas para explorar o sistema.
Para que o fingerprint apresente resultados confiáveis são necessárias analises complexas, como:

- analise de pacotes que trafegam na rede
- leitura de banners (assinatura do sistema)
- análise de particularidades da pilha TCP/IP

Scanners de fingerprint são softwares usados para realizar tarefas de detecção de sistemas operacionais. Entre os scanners existentes, podemos dividi-los basicamente em dois tipos:

fingerprint passivo: atua como um farejador na rede, ou seja, fica escutando os pacotes que passam por ela, e detectado o formato do pacote que esta passando conseguem detectar o sistema operacional.

fingerprint ativo: o scanner envia pacotes manipulados e forjados, baseado em uma tabela própria de fingerprint. Com isso, ele analisa a resposta do pacote e compara com a tabela, para definir qual o sistema operacional.

Técnicas Clássicas

Para detecção de sistema operacionais, uma técnica clássica e muito usada é através do netcat. Veja usando o comando abaixo (o resultado podera demorar um pouco para retornar).

```
# echo 'GET / HTTP/1.0\n'  | nc www.silva.eti.br 80 | grep '^Server:'
```

ftp

PING

#ping google.com.br

A informação importante esta no campo TTL. A maioria dos sistemas operacionais se diferenciam pelo valor retornado de TTL. Veja a lista abaixo:

- cyclades normalmente 30
- linux normalmente 64
- windows normalmente 128
- cisco normalmente 255
- linux + iptables normalmente 255

para visualizar este valor no linux, use o comando abaixo:

cat /proc/sys/net/ipv4/ip_default_ttl