As fases de um processo de teste de invasão (Pentest)

Tempo estimado de leitura: 7 mins

Diego Macêdo 26 de junho de 2016 2 Comments

vulnerabilidade, o analista não só descobre as vulnerabilidades que podem ser usadas pelos atacantes mas também exploram as vulnerabilidades, onde possivelmente, para avaliar o que os atacantes ganhariam após uma exploração com sucesso.

De tempos em tempos, surgem notícias de grandes empresas tendo informações vazadas devido a ciberataques. Maioria das vezes, os atacantes não usam as vulnerabilidades mais recentes ou zero-day (vulnerabilidades sem patch de correção publicada pelo fabricante do software). Maioria das empresas com orçamento considerável para para Segurança da Informação são vítimas de SQL Injection (SQLi) em seus sites, ataques aos seus funcionários através de engenharia social, serviços expostos na internet com senhas fracas, etc. Em outras palavras, empresas estão perdendo dados proprietários e os de seus clientes, através de brechas de segurança que poderiam ser corrigidos. Em um pentest, achamos estes problemas antes dos atacantes e recomendamos como corrigir, evitando futuras vulnerabilidades.

O escopo de um penteste vai variar de cliente para cliente. Alguns deles terão uma postura excelente em segurança da informação, enquanto outros terão vulnerabilidades que permitirão os atacantes invadir o perímetro e ganhar acesso aos sistemas internos.

Você também poderá ter a tarefa de avaliar algumas aplicações web. Você poderá realizar alguns ataques de engenharia social ou ganhar acesso pelo lado do cliente a uma rede interna. Alguns pentestes irão requerer que atuem como um insider (funcionário fraudador ou um atacante que já tenha invadido o perímetro) enquanto você realiza testes internos de invasão. Alguns clientes solicitarão um teste de invasão externo, onde você simulará um ataque via Internet. Alguns solicitarão a avaliação da segurança das redes wireless da empresa. Em alguns casos, será necessário avaliar os controles de segurança físico.

Resumo das fases

O penteste inicia com a fase de pré-compromisso, a qual envolve conversar co mo cliente sobre os objetivos do penteste, definir o escopo (a extensão e os parâmetros do teste), e assim por diante. Quando um pentester e o cliente acordam sobre o escopo, o formato do relatório e outros tópicos, os testes começam.

Na fase de coleta de informações, o pentester busca por informações públicas disponíveis sobre o cliente e identifica potenciais meios para se conectar aos seus sistemas.

Na fase de modelagem das ameaças, um pentester utiliza as informações para determinar o valor de cada achado e o impacto para o cliente se isto permite um atacante invadir o sistema. Esta avaliação

Antes do pentester poder iniciar os ataques aos sistemas, ele irá realizar uma análise de vulnerabilidade. Nesta fase, ele tentará descobrir vulnerabilidades nos sistemas que podem ser úteis na fase de exploração. Uma exploração de sucesso poder levar a fase de pós-exploração, onde o resultado da exploração é aproveitar para encontrar informações adicionaris e sensíveis, acesso a outros sistemas, e assim por diante.

A última fase é a emissão do relatório, onde o pentester resume o que foi encontrado, tanto na visão executiva, como na técnica.

Pré-Compromisso

Antes do pentest iniciar, o analista faz um pré-compromisso com o cliente para garantir que todos estão alinhados sobre o teste que será realizado. Falha na comunicação entre o analista e o cliente, que espera um simples escanner de vulnerabilidade, poderia levar a uma situação desagradável com um teste mais intrusivo.

A fase de pré-compromisso é quando você deve ter um tempo para entender os objetivos do negócio do cliente com este pentest. Se for o primeiro pentest deles, o que os fizeram procurar um pentester? Com qual exposição ele estão mais preocupados? Eles tem algum dispositivo frágil que deve-se ter cuidado durante os testes? Pergunte tudo sobre os negócios do cliente. O que mais importa para eles? Por exemplo, para uma loja de vendas online, horas de downtime pode significar milhares de reais em perdas de vendas. Para um banco local, ter o site deles fora do ar por algumas horas pode aborrecer alguns clientes, mas seria mais devastador se comprometessem o banco de dados dos cartões de créditos dos clientes. Para um fornecedor de segurança da informação, ter o seu site “pichado” com mensagens rudes poderiam danificar a reputação e acabar com as vendas deles. Outros pontos importantes para se discutir e acordar durante esta fase são

1) Escopo

Qual endereço de IP ou host estão no escopo, e o que não está no escopo? Que tipo de ações o cliente espera que você realize? Você tem permissão para usar exploits e correr o risco de derrubar o serviço do dispositivo, ou deve se limitar ao ponto de simplesmente detectar possíveis vulnerabilidades? O cliente entende que mesmo um simples escaneamento de portas poderá derrubar um servidor, roteador ou firewall? Você tem a permissão para realizar ataques de engenharia social?

2) A janela de teste

3) Informações de contato

Com quem você deve entrar em contato caso aconteça algo sério? O cliente espera que você entre em contato com alguém 24 horas por dia? Você prefere utilizar criptografia ao enviar o e-mail?

4) Um cartão de "fique livre da cadeia"

Tenha certeza que você tem autorização para realizar um teste de invasão naquele alvo. Se o alvo não pertence à empresa, tenha certeza de verificar se o cliente tem aprovação formal do terceiro para realizar teste de invasão. Independentemente, tenha certeza que seu contrato inclua uma cláusula que limite sua responsabilidade nos casos não esperados, e tenha por escrito uma permissão para realizar os testes.

5) Termos do pagamento

Como e quando você será pago, e quanto será? Finalmente, inclua uma cláusula de "nondisclosure agreement" em seu contrato. Clientes vão apreciar este termo, o qual mantém o teste de invasão e qualquer achado de forma confidencial

Coleta de informações

Esta é a próxima fase, onde você vai analisar de forma livre as fontes de informações sobre o seu alvo, utilizando um processo chamado Open Source Intelligence (OSINT). Você também pode começar a utilizar ferramentas como port scanners para ter uma ideia de quais sistemas estão voltados para internet ou redes internas, assim como saber quais softwares os dispositivos estão rodando neles. Iremos ver mais detalhes sobre esta fase em outra postagem.

Modelagem das Ameaças

baseados em informações coletadas. Por exemplo, se um cliente desenvolve um software proprietário, um atacante poderia devastar com a empresa ao obter acesso a rede interna de desenvolvimento do sistema, onde o código-fonte é desenvolvido e testado, e vender as informações secretas para uma empresa concorrente. Baseado nos dados achados durante a fase de coleta de informações, nós desenvolvemos as estratégias de invasão no sistema do cliente.

Análise de Vulnerabilidade

Nesta etapa, começamos a descobrir ativamente as vulnerabilidades para determinar quão sucedido será explorar as vulnerabilidades poderão ser. Falhas ao explorar certas vulnerabilidades pode causar um crash no sistema, desligar alertas de Intrusion Detection System (IDS), e por outro lado arruinar as suas chances de fazer uma exploração com sucesso.

Sempre durante esta fase, os pentesters rodam escaneres de vulnerabilidades, os quais possuem um banco de dados de vulnerabilidades conhecidas para fazer diversas checagens e identificar possíveis vulnerabilidades presentes no sistema do cliente. Apesar dos escaneres de vulnerabilidades serem ferramentas poderosas, elas não dispensam o pensamento crítico, então também devemos realizar análises manuais e verificar os resultados por nós mesmos nesta fase. Iremos explorar mais detalhes sobre esta fase em outra postagem.

Exploração

Agora a parte mais divertida, a exploração do sistema. Aqui podemos rodar alguns exploits em sistemas vulneráveis que descobrimos (as vezes utilizando ferramentas como o Metasploit) na tentativa de acessar o sistema do cliente. Como veremos adiante, algumas vulnerabilidades serão fáceis de explorar, como logar utilizando senhas padrões do sistema. Veremos com mais detalhes futuramente em outra postagem.

Pós-Exploração

Alguns dizem que os pentestes somente começam após a fase de exploração, ou seja, na pós-exploração. Você entrou, mas o que a invasão realmente significa para o cliente? Se você invadiu um sistema legado sem correção que não é parte de um domínio ou esteja de conectado aos alvos de alto valor, e o sistema não tem informações de interesse de um atacante, o risco daquela vulnerabilidade é significantemente baixa em relação a um ataque ao controlador do domínio ou um sistema em desenvolvimento do cliente.

para acessos adicionais aos sistemas. Podemos utilizar ainda uma máquina explorada para atacar sistemas não disponíveis antes para nós, simplesmente pivotando dentro deles. Veremos como fazer isto nas próximas postagens.

Relatório

A fase final do teste de invasão é o relatório. É onde juntamos tudo o que achamos e é significante para o cliente de alguma forma. Contaremos a ele o que estão fazendo corretamente, onde eles necessitam melhorar sua postura de segurança, como você entrou, o que você achou e as recomendações para corrigir os problemas.

Escrever um bom relatório de penteste é uma arte que necessita de prática. Você pode precisar resumir seus achados de forma clara para todos, desde o pessoal da TI responsáveis por ajustar as vulnerabilidades, até a alta gestão que contratam os auditores externos. Por exemplo, se um não-técnico ler algo como “E então usei um MS08-067 para pegar uma shell” ele poderá não entender. Uma forma melhor de dizer isto seria dizer que dados sensíveis e privados poderiam ser acessados ou modificados. Uma frase como “Fui capaz de ler seu e-mail” vai causar efeito em qualquer um. O relatório do penteste deve incluir tanto um sumário executivo e um relato técnico, assim como será discutido nas próximas seções.

Fonte:
Weidman, Georgia. Penetration Testing: A Hands-On Introduction to Hacking. 2014.

Diego Macêdo