Frank Ned Santa Cruz de Oliveira
Responsável pelo Website Verdade
@Absolutahttp://www.absoluta.org
frank@absoluta.org

ARTIGO

Você Precisa de um Teste de Invasão?

Observação:
O objetivo deste artigo é munir os administradores de sistema com algumas informações que possam ajudá-los a melhorar o nível de segurança de sua rede. A primeira parte do artigo, trata dos principais pontos que devem ser observados durante a realização de um teste de invasão. Esta parte foi baseada num texto publicado na revista Internet Security de março de 1999, cujo o autor é Mark Cusick <cusickm@fortrex.com>, porém vários pontos do texto original foram modificados além de terem sido incluídos conceitos que não estão presentes no texto. A segunda parte desse artigo é um pequeno roteiro de um possível teste de invasão.

1. Introdução

Um teste de invasão tem por objetivo verificar a resistência do sistema em relação aos métodos atuais de ataque. Este método pode ser simplesmente um tipo de engenharia social, onde alguém do *Tiger Team* liga para funcionários e pergunta pela identificação do usuário e senha ou mais complexo utilizando técnicas de *buffer overflow* para ganhar acesso de *root*.

Diariamente são descobertos novos furos nos mais variados sistemas, por isso é de fundamental importância que o *Tiger Team* utilize técnicas reais, pois caso isso não ocorra o teste pode tornar-se inválido.

Após o teste temos duas possibilidades:

1. O *Tiger Team* obtêm êxito, logo o sistema de segurança está falho.
2. O *Tiger Team* não obtêm êxito, logo o sistema de segurança está adequado.

A segunda afirmativa pode não ser verdadeira uma vez que seu sistema foi submetido a uma equipe que está sujeita a erros.

O objetivo deste artigo é demonstrar o que você pode esperar de um teste de invasão, esclarecer se você realmente precisa de um e mostrar alguns riscos envolvidos em um teste de invasão.

2. Testando o sistema de detecção de intrusão (IDS)

O Sistema de Detecção de Intrusão (*IDS - Intrusion Detection Systems*) permite a notificação quando há a ocorrência de tentativas de intrusão segundo a verificação de certos padrões de ataque que podem ser configurados dependendo da ferramenta que se está utilizando.

Se sua casa possui um sistema de alarmes contra ladrões, você possui um sistema de *IDS* relativamente sofisticado. Ele pode detectar tentativas de invasão e tomar alguma ação baseado na detecção.

Infelizmente, devido a grande variedade de vulnerabilidades, detectar uma intrusão em sua rede não é algo simples. É praticamente impossível que uma pessoa detecte uma invasão de rede em tempo real (*on-the-flay*) e tome alguma ação de imediato.

Os maiores problema com as atuais ferramentas de *IDS* são: [1]

- A alta taxa de ***false-positive*** ocorre quando a ferramenta classifica uma ação como uma possível intrusão, porém trata-se de uma ação legítima.
- A ***false-negative*** ocorre quando uma intrusão real acontece mas a ferramenta permite que ela passe como se fosse uma ação legítima.
- Erro de ***subversion*** ocorre quando o intruso modifica a operação da ferramenta de IDS para forçar a ocorrência de ***false-negative.***

Um bom exemplo de *false-positive* é o ataque de *SYN FLOOD*. O simples fato de acessar um determinado tipo de página pode gerar uma detecção da ocorrência desse tipo de ataque. Você certamente não quer que suas páginas fiquem fora do ar a todo momento que um usuário acessar seu site :). É muito difícil definir regras que diferenciem entre atividades hostis e autorizadas. O teste de invasão pode ser utilizado com a finalidade de demonstrar efetivamente se sua ferramenta de *IDS* está operando conforme o esperado e ajudá-lo no refinamento das regras de forma a reduzir a taxa de *false-positive*.

3. Testando o plano de resposta a incidentes

As ações da sua ferramenta de *IDS* devem estar diretamente relacionadas com o plano de resposta a incidentes. Na verdade a definição de um plano de resposta a incidentes é um fator tão crítico que caso você não tenha um, provavelmente um teste de invasão não irá ajudá-lo muito. Seu plano de resposta a incidentes deve abranger, basicamente, os seguintes pontos:

- Qual o objetivo do plano de resposta para cada tipo de incidente?
- Quais as ações legais existentes?
- Serão tomadas ações legais no caso de um incidente?
- Que tipo de publicidade (a respeito do ataque) é permitida?
- Quem é responsável por conduzir a resposta ao incidente?
- Quem fará parte do grupo de resposta a incidente?
- Que nível de autoridade é requerida para o grupo de resposta a incidente?

Como você conduz uma resposta a um incidente está diretamente relacionado ao tipo de negócio da sua instituição. Os bancos por exemplo, devem tomar algumas ações junto a federação nacional de bancos.

Após você ter seu plano de resposta a incidente montado, você pode testá-lo efetivamente e refiná-lo utilizando o teste de invasão. É uma boa idéia anunciar a realização do primeiro teste, uma vez que seu propósito é ajustar o plano de resposta e verificar se ele funciona. Após o refinamento do plano, faça um novo teste sem avisar. [danadinho] :)

4. Testando o firewall

O *firewall* é um sistema de proteção, porém, como qualquer sistema, pode ser vulnerável. Na verdade várias instituições instalam o *firewall* com o objetivo de se proteger da abertura que a Internet proporciona, porém elas mesmas criam regras (brechas) para permitir conexões com vendedores e parceiros. Além disso, muitos *firewalls* são instalados com a configuração básica

e nunca são testados para verificar sua eficiência. Um bom teste de invasão consegue identificar os buracos de forma que você saberá que eles existem.:)

5. Identificando as vulnerabilidades de alto risco

Um teste de invasão pode dar um boa idéia sobre as vulnerabilidades de alto risco presente em seu sistema. Financeiramente não é interessante utilizar o teste de invasão para identificar todas as possíveis vulnerabilidades do seu sistema. Se seu objetivo é simplesmente identificar as vulnerabilidades, considere a utilização de uma ferramenta de *SCAN*, como: *nmap* [2], *SATAN* [3], *ISS scanner* [4]. Lembre-se: você está pagando por um teste de invasão pelo conhecimento e *expertise* do *Tiger Team* além da habilidade em explorar as vulnerabilidades. As ameaças e vulnerabilidades que não conseguirem explorar podem ser identificadas pela ferramenta de *scan*, pense nisso antes de contratar um teste de invasão.

6. Riscos envolvidos em um teste de invasão

Um importante aspecto referente ao teste de invasão é que ele pode gerar uma falsa sensação de segurança. A idéia de que "eles fizeram o melhor que podiam e não obtiveram êxito" não é valida. Sua rede pode ter vulnerabilidades que o *Tiger Team* não tenha encontrado ou talvez elas não existam no momento do teste, mas podem vir a existir após alguma mudança na configuração da rede.

Um importante ponto a ser lembrado é: "Você terá o que pagou". Existem algumas pessoas que executam teste de invasão e acham que seu trabalho é entrar na rede - sem identificar as vulnerabilidades. É recomendável que a pessoa que vai realizar o teste de invasão apresente um documento detalhando exatamente quais são os resultados finais a serem alcançados. Além disso, você deve considerar a realização do teste de invasão em vários momentos do seu sistema.

Lembre-se: você deve estar atento o tempo todo, a um intruso basta somente uma olhada.:). O fato de você ter realizado um teste de invasão não significa que sua rede está segura. A segurança absoluta só é alcançada em um sistema que esteja a trinta metros abaixo da terra e sem acesso para o mundo exterior. [essa é antiga :)]

7. Danos ao sistema durante o teste

Um fator que deve ser levado em consideração são os possíveis danos causados: o sistema pode ser afetado durante o teste ou arquivos importantes podem ser perdidos. É importante a definição de parâmetros que identifiquem os pontos onde o teste tem validade. Você pode ignorar qualquer tipo de *DoS* (*Denial Of Service*) conhecido. As pessoas que realizam o teste de invasão, por definição, não são usuários legítimos. O bom teste de invasão não pode ficar preso a um único aspecto do seu sistema. Muitas pessoas que realizam teste de invasão requerem que seja indicado um departamento que assuma as responsabilidades no caso de ocorrer algum dano ao sistema.

8. Ameaças da Internet

Algumas instituições contratam *crackers* para realizarem os testes de invasão. Este tipo de ação pode ser perigosa pois as pessoas possuem princípios éticos e morais diferentes, então este é um risco que deve ser pesado antes de corrê-lo. Segundo estudos do especialista em segurança Fred Cohen [5], um dos mais respeitados em todo o mundo: "Existe um sério risco de que as informações sejam divulgadas ou utilizada para ganhos financeiros pela pessoa responsável pelos testes". Isso ocorre quando estas pessoas não respeitam os princípios éticos e morais vigente na sociedade. Deve-se formalizar um contrato onde as cláusulas estabelecem que as informações referentes aos testes de invasão não podem ser divulgadas. O que um contrato de invasão deve conter?

- Após os teste deve-se fazer um relatório detalhado das vulnerabilidades encontradas e dar suporte na correção de tais pontos.
- Enquanto você não tiver testado sua ferramenta de *IDS* ou montado seu plano de resposta a incidentes, a pessoa responsável pelo teste não deve receber nenhum tipo de informação sobre o seu sistema, parceiros comerciais. Isso pode protegê-lo quanto

a validade do teste de forma que intrusos verdadeiros não tenha acesso a estas informações.

- Os testes devem ser conduzidos utilizando-se ferramentas previamente definidas.
- Enquanto os pontos acima não forem atendidos, o responsável pelo teste não deve ter acesso a sua rede.
- Informações públicas como: estrutura da empresa, lista de telefones internos, entre outras podem ser passadas para pessoa que vai realizar o teste, justamente para ganhar tempo.
- A pessoa que vai realizar o teste não deve violar a privacidade e os direitos individuais. Lembre-se que trata-se de um teste para avaliar o sistema e não as informações privadas.
- Todos os dados coletados, incluindo os arquivos, senhas e qualquer outro tipo de informação obtida deve devem ser devolvidas a instituição sem que cópias sejam retidas pela organização que realizou os testes.
- Todos os teste devem ser realizado de forma instrutiva.
- Qualquer tipo de teste que possa causar uma dano ao sistema deve ser realizado em períodos de baixa ou sem atividades.
- Um relatório detalhado deve ser entregue contendo todos os passos executados mostrando onde ganhou acesso e onde não. O relatório deve conter recomendações detalhadas para a correção de qualquer vulnerabilidade encontrada.

9. Fase 1: Coleta de dados e planejamento

Nesta fase, o *Tiger Team* vai aprender tudo que puder sobre o alvo e não estará necessariamente preocupado com vulnerabilidades do sistema. Ele tentará obter informações sobre a estrutura da diretoria, número dos telefones/ramais, relação dos parceiros, dos vendedores, ou seja, todo tipo de informação. Muitos testes de invasão obtêm sucesso por que a instituição que está sendo testada fornece as chaves:). Raramente a pessoa que realiza o teste tem que recorrer a mecanismos como *buffer overflow*. A relação de telefones possui muitas informações úteis para o invasor.

Outro tipo de informação importante é a topologia da rede. Conforme a topologia o invasor pode determinar quais os pontos mais vulneráveis.

Durante esta fase um detalhado plano de ataque é construído. Eu, pessoalmente, chamo esta fase de aproximação indireta, um termo utilizado em estratégias militares e planejamento de atos de terrorismo.

10. Fase 2: Pesquisa do sistema

Nesta fase, dentro do que chamo aproximação indireta, podemos colher mais informações sobre a intistuição que está sendo testada. Isso inclui a consulta ao *whois* via web: FAPESP (www.fapesp.br), ao InterNIC (www.inetrnic.net) e ao ARIN (www.arin.net), além destes existem outros servidores de *whois*. Caso utilize um sistema UNIX eu, particularmente, prefiro O *BSD* pois sua implementação é mais elegante e fornece mais opções que o *Linux*. Com estas informações temos uma idéia da rede da instituição e de seus *IPs*.

11. Fase 3: Teste do sistema

Agora iniciamos a fase que chamo de aproximação direta, onde temos os seguinte passos:

A) Identificar o caminho para acessar a instituição. Podemos fazer isso com o comando *traceroute*, mas em vez de usar o *traceroute* tradicional, podemos usar uma ferramenta especial para fazer um *traceroute* a uma porta *TCP* ou *UDP* específica, desta forma conseguimos burlar os filtros de *ICMP*. Este fase permite compreender o caminho de acesso à instituição, ou seja, nos dá uma visão lógica do caminho. Nosso objetivo é determinar o caminho e as *ACLs* implementadas nos roteadores e *firewalls*. Para tanto podemos usar a ferramenta *firewalk*. Esta é uma ferramenta muito interessante que permite determinar as *ACLs*implementadas, ou seja, identificar quais serviços são permitidos através da *ACL*.

B) Agora seria uma boa idéia verificar que tipo de informação podemos recuperar do servidor

de *DNS*. Se o servidor estiver mal configurado é possível fazer uma tranferência de zona o que nos fornece muitas informações úteis. Um exemplo é a recuperação do registro *HINFO*, se esta informação estiver disponível, saberemos exatamente o tipo de sistema operacional da instituição. Podemos usar vários comandos diferentes para este fim como *nslookup*, *dig* e *host*. Um dos objetivos é determinar o endereço do *firewall* para que possamos testá-lo. Podemos fazer uma análise destas informações e rapidamente com o auxílio do comando *grep* podemos descobrir todas as máquinas que possuem a palavra **teste** em seu nome, se estas máquinas estiverem mal configuradas é um bom local para tentar um acesso não autorizado, da mesma forma podemos usar o comando *grep* para identificar outros padrões de nome como *linux*, *sun*, *bsd*, etc.

C) Após termos o mapa das máquinas precisamos determinar quais os *hosts* que estão ativos e conectados à Internet, pois as máquinas listadas na resposta do *DNS* não significa estarem ativas. Podemos usar para tal fim ferramentas como *nmap* e o *fping*. O *nmap* permite analizarmos uma determinada faixa de endereços. Enquanto a maioria das ferramentas de *ping* trabalham em cima de *ICMP*, com o *nmap* podemos fazer um *ping* através do *TCP*, ou seja, se os pacotes *ICMP* estiverem sendo filtrados no roteador de borda, com o *nmap* podemos achar os *hosts* ativos usando por exemplo a porta 80.

D) Se uma máquina está ativa e conectada à Internet, chegou o momento de fazer um *port scan*. O *port scan* tem por objetivo determinar quais portas (*TCP/UDP*) estão ativas. A identificação de portas é fundamental para determinar o sistema operacional e as aplicações em uso. Através dos serviços ativos podemos ganhar acesso as máquinas que estão mal configuradas ou rodam versões de programas com vulnerabilidades conhecidas. Existem várias ferramentas que permitem a realização de *port scan: nmap, strobe, tcp_scan, udp_scan, netcat e queso* são algumas delas.

E) Após termos descoberto as portas ativas de cada *host* conectado à Internet, chegou a hora de obtermos mais informações dos *hosts*. Isso inclui *banner* ou qualquer outro tipo de informação. Informações fornecidas pelos serviços de *SNMP, finger, rusers SMTP ou NetBIOS* permitem que montemos uma configuração detalhada além de conseguirmos informações sobre os usuários de cada sistema. Agora podemos conectar a cada uma das portas *TCP/UDP* e analizar as respostas, afim de identificar informações sobre versão e descobrir servidores vulneráveis. Mas não é somente a versão que nos interessa, e sim também informações do sistema como a disponibilidade de serviços como *finger* e *ruser* onde, através destes, podemos obter informações dos usuários do sistema. Através do *SNMP* utilizando uma conexão *UDP* a porta 161 podemos usar *query* com *snmpget*, *snmpwalk* e *snmptest* para obter algumas informações.

F) Agora que já temos um conjunto de informações sobre os *hosts*, como máquinas ativas, os serviços que rodam, informações de usuários entre outras, podemos montar um mapa de vulnerabilidades. O objetivo deste mapa e associar as informações do sistema com as vulnerabilidades conhecidas. Existem alguns métodos para fazer isso:

1. Podemos pegar todas as informações colhidas como versão do sistema operacional, versões dos serviços, arquitetura do sistema e manualmente montar o mapa. Embora seja uma tarefa extremamente chata isso pode ser feito com consultas ao *CERT*, *CIAC*, *BUGTRAQ* entre outros.
2. Outra alternativa é usar os *exploits* escritos por você ou um dos divulgados em várias listas se segurança e *sites*.
3. Pode-se usar uma ferramenta comercial de identificação de vulnerabilidades como o *Cybercop Scanner* (www.nai.com) ou o *Internet Security Scanner* (www.iss.net) ou uma ferramenta *freeware*, do projeto*Nessus* (www.nessus.org).

G) Um dos pontos a serem observados é o *false-positive* e o *false-negative* gerados por estas ferramentas. As ferramentas automáticas geralmente classificam as vulnerabilidades quanto ao risco em baixa, média ou alta, mas não podem determinar o risco no caso de um ataque que combine mais de uma vulnerabilidade. Este tipo de *expertise* é o verdadeiro valor que um

especialista pode fornecer a sua instituição.

Até este momento o invasor não entrou no sistema, mas está colhendo informações adicionais. Podemos começar efetivamente o ataque usando engenharia social, ligando para pessoas da instituição dizendo ser do *ISP*, da companhia telefônica, do representante de tal equipamento ou software e pedindo a identificação do usuário e senha, para que possam realizar alguns testes. Lembre-se: a esta altura o invasor já tem informações sobre quem é quem na instituição e pode falar em nome desta pessoas, por exemplo, se não vai usar esta sua voz de macho né? pode ser uma voz feminina delicada, graciosa, que convida o cabra para um shopinho e tal...:). Após esta fase inicia-se a tentativa de intrusão. Lembre-se: a idéia é entrar e sair sem ser detectado.

Deve-se fazer log detalhado de todos os testes e *scans* bem como de seus resultados. O objetivo do log é permitir que após os testes possa-se fazer uma relação para determinar se eles causaram algum dano ao sistema e garantir que outro intruso não tenham ganho acesso ao sistema durante o teste. Já pensou se seu funcionário entra em um canal de bate-papo e diz que sua empresa vai fazer um teste de invasão, legal né? :).

12. Conclusão

O teste de invasão deve fazer parte do programa de segurança da sua empresa, mas deve-se observar os pontos acima tratados, para que se possa tirar um real aproveitamento do dinheiro empregado em tal atividade. Você deve restringir as informações sobre os testes somente aos departamentos competentes, pois alguns funcionários desavisados ou inocentes podem deixar a informação vazar e alguém pode aproveitar e realizar seu próprios testes. Eu já vi isso acontecer em uma instituição aqui no Brasil, durante o dia eu estava fazendo o levantamento de informações na instituição e para minha supresa ao entar na rede à noite cruzei com uma funcionária que estava comentando em um canal aberto sobre os teste que estavam em andamento dentro da instituição, lógico que ela não estava agindo de má fé, mas uma questão fundamental é a **cultura com relação a segurança da informação**, mas isso é assunto para outro artigo. :)

13. Referências

- [1] - IDS - http://www.cs.purdue.edu/coast/
- [2] - nmap - http://www.insecure.org (ferramenta *freeware*)
- [3] - SATAN - http://www.ensta.fr/internet/unix/sys_admin/satan.html (ferramenta *freeware*)
- [4] - ISS scanner - http://www.iss.net
- [5] - Fred Cohen - http://all.net/
- Invadindo seu site para melhorar a segurança
  -
  - http://www.absoluta.org/absoluta/seguranca/dan_01.html
- Detecção de Sistema Operacional Remotamente via o FingerPrinting da Pilha TCP/IP
  -
  - http://www.absoluta.org/absoluta/seguranca/seg_detect_os.html

O que você achou deste Artigo ?

Qualidade			Abordagem do Assunto		
Excelente	Medio	Fraco	Objetiva	Extensa	Reduzida

Comentário:

Enviar Limpar