Segurança da Informação

Aula 06

Aula 06

Em Segurança da Informação, o que vem a ser:

- Cracking de Senhas
- Buffer Overflow
- IP Spoofing
- Denial of Service
- Sniffer
- Trojan
- Engenharia Social
- Consolidação de Poder

Aula 06

Segurança da Informação

Cracking de Senhas

Conceito

Fazer “crack” de uma senha significa descobrir qual é a senha para uma determinada conta.

Métodos empregados

- Adivinhação
- Programas de Cracking

Aula 06

Segurança da Informação

Cracking de Senhas

Adivinhação

Este é um método bastante primitivo, contudo eficiente. Trata-se de utilizar o bom senso junto com algumas informações sobre a conta atacada. Muitos usuários utilizam senhas fáceis (times de futebol, conta acrescido de um digito, datas especiais, nomes de familiares) que são fáceis de serem adivinhadas.

Um outra possibilidade de adivinhação está relacionada com softwares que vem com "senhas de fábrica". Por exemplo, quando um banco de dados é instalado o mesmo vem com alguns contas de administração padrão, as quais possuem algumas senhas padrões. Se estas senhas não forem alteradas pelo administrador, fica-se vulnerável a qualquer hacker que tenha uma lista de senhas padrões. Este problema ocorre para roteadores, sistemas operacionais, softwares básicos (ex: backup), etc.

Aula 06

Segurança da Informação

Cracking de Senhas

Programas de Cracking

Este método consistem em empregar programas que "descobrem" as senhas utilizando tentativa e erro. Para isto, os programas utilizam dicionários de senhas básica, aplicando variações, ou então utilizam força bruta (tentam todas as senhas possíveis).

Este processo normalmente é efetuado após o hacker ter conseguido obter um arquivo contendo o hash code das senhas. Este arquivo contém uma representação das senhas, não as senhas propriamente ditas. O programa de cracking começa então a gerar senhas, e quando uma senha gerada produzir o mesmo hash code ele terá encontrado a senha.

Uma vez que é muito simples obter via internet um bom programa de cracking, esta técnica de ataque será muito efetiva caso o arquivo de hash da sua empresa caia nas mãos dos hackers.

Aula 06

Segurança da Informação

Buffer Overflow

Conceito

Falha de programação que faz com que haja um “transbordamento” da área de memória de uma determinada variável invadindo a área de memória contígua.

Conseqüência

Softwares podem ser derrubados ou forçados a executar outras funções (código arbitrário).

Abrangência

Atinge todos os tipos de software, sistemas operacionais, Serviços (ex: Web Servers), aplicativos (scripts CGI).

Aula 06

Segurança da Informação

Buffer Overflow

Como os hackers exploram esta vulnerabilidade ?

Hackers técnicos desenvolvem programas para explorar um buffer overflow (exploits) em um determinado software/versão. Estes programas são extremamente sofisticados, exigindo que se "mescle" em tempo de execução dois códigos de máquina. Uma vez desenvolvido estes exploits e divulgados na internet, qualquer hacker pode se utilizar dos mesmos para fazer um ataque contra um servidor que utilize o software com problema de buffer overflow.

Aula 06

Segurança da Informação

Buffer Overflow

Como funciona o buffer Overflow ?

Este bug ocorre quando o programador esquece de validar se os dados de entrada recebidos por uma variável estão dentro dos limites máximos de tamanho reservado para aquela variável. Um buffer overflow ocorre quando uma área destinada a uma variável transborda. Ou seja, foi recebido uma quantidade de bytes para ser armazenado maior do que o espaço reservado para aquela variável. Normalmente as variáveis pertencem a funções, e por terem escopo local foram criadas na pilha. Deve-se lembrar que a pilha contém o endereço de retorno de uma função, e valores de registradores que serem restaurados quando a função encerra. Portanto, se o atacante for capaz de trocar estes valores, será capaz de mudar o comportamento de um programa.

Aula 06

Segurança da Informação

Buffer Overflow

Como funciona o buffer Overflow ? (continuação)

Um hacker pode utilizar uma falha de buffer overflow para paralisar um programa, forçando-o a executar instruções ilegais, ou então danificando a sua área de dados a tal ponto que o estado do programa fique tão inconsistente a ponto de causar um auto cancelamento. Desta forma, o buffer overflow pode ser utilizado para causar denial of service (DoS), indisponibilizando o serviço prestado por uma programa que foi paralisado.

O buffer overflow também pode ser utilizado para fazer com que um programa passe a executar uma seqüência de código determinada pelo hacker. Neste caso, os dados que serão enviados contém uma seqüência de instruções de máquina que irão substituir o código de máquina original. Isto permite ao buffer overflow criar uma porta de entrada, abrindo por exemplo um shell para entrada de comandos.

Aula 06

Segurança da Informação

Buffer Overflow

Exemplo de buffer Overflow

Vamos ilustrar como funciona um buffer overflow através de um exemplo que mostra um overflow de áreas de dados (uma variável preenchendo ilegalmente dados de outra variável). Observe o programa abaixo:

```
#include <stdio.h>

char s1[10];
char s2[10];

int main()
{
printf("\ns2 antes = %s",s2);
printf("\nDigite s1: ");
gets(s1);
printf("\ns2 depois = %s",s2);

}
```

Trata-se de um programa extremamente simples, que lê um string de caracteres (s1), e em seguida exibe um outro string de caracteres (s2), o qual não recebeu nenhum valor. O resultado esperado deste programa é exibir s2 como um string vazio (nenhum caractere). Contudo, em nenhum instante este programa valida se a quantidade de caracteres lido em s1 ultrapassa o tamanho da variável. Isto abre condições para um buffer overflow.

Aula 06

Segurança da Informação

Buffer Overflow

Abaixo podemos ver o mesmo programa com as suas instruções em código de máquina:

```
8:    printf("\ns2 antes = %s",s2);
00401028   push        offset _s2 (004237d0)
0040102D   push        offset string "\ns2 antes = %s" (00420040)
00401032   call        printf (00401160)
00401037   add         esp,8
9:    printf("\nDigite s1: ");
0040103A   push        offset string "\nDigite s1: " (00420030)
0040103F   call        printf (00401160)
00401044   add         esp,4
10:   gets(s1);
00401047   push        offset _s1 (004237b0)   s1
0040104C   call        gets (00401090)
00401051   add         esp,4
11:   printf("\ns2 depois = %s",s2);
00401054   push        offset _s2 (004237d0)   s2
00401059   push        offset string "\ns2 depois = %s" (0042001c)
0040105E   call        printf (00401160)
00401063   add         esp,8
12:
13:   }
```

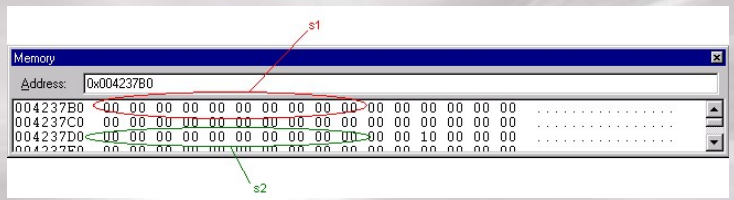
Pode-se verificar que a variável s1 está num endereço mais alto do que a variável s2. Logo, se s1 transbordar, s2 receberá um conteúdo.

Aula 06

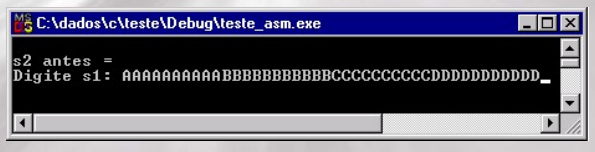
Segurança da Informação

Buffer Overflow

Inicialmente ambas as variáveis estão preenchidas com zero binário, conforme mostrado abaixo.



Vamos imaginar que na entrada de dados foram digitados mais do que 9 caracteres, como mostra a tela abaixo:

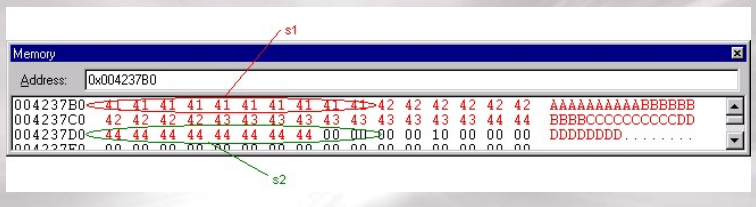


Aula 06

Segurança da Informação

Buffer Overflow

Gerando a seguinte configuração de memória:



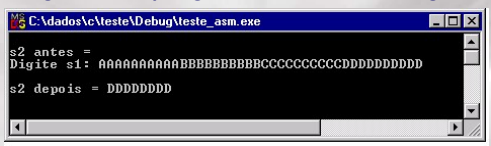
Deve-se observar que o buffer overflow já ocorreu. A área reservada para s1 era capaz de armazenar apenas 9 caracteres (último para \0). Como foi lido uma seqüência de 40 caracteres, estes caracteres adicionais foram armazenados nas posições consecutivas de memória, invadindo o espaço de memória da variável s2.

Aula 06

Segurança da Informação

Buffer Overflow

Portanto, prosseguindo o programa teremos o seguinte resultado:



De forma "inesperada", s2 apareceu com um seqüência de caracteres. Isto é o resultado do buffer overflow.

Este é um buffer overflow em que o transbordamento ocorreu na área de dados. Foi apenas um exemplo simplificado para que o conceito fosse esclarecido.

Obs.: Em casos reais, este transbordamento ocorre na pilha, que contém variáveis locais de subrotinas, endereços de retorno, e valores de registradores. Quando o hacker consegue substituir esta área de memória, consegue modificar o fluxo de execução, fazendo com que o computador atacado passe a executar um novo código (por exemplo, uma chamada ao shell para receber comandos). É desta forma que os hackers conseguem "controlar" softwares que apresentam problemas de buffer overflow.

Aula 06

Segurança da Informação

IP Spoofing

Conceito

Cada máquina que está se comunicando na internet tem um identificador único: o endereço IP. Contudo, este endereço pode ser forjado, permitindo que uma máquina utilize o endereço de uma outra máquina. Esta técnica é denominada IP Spoofing.

Conseqüências

1) Atacante anônimo: Utilizando o IP Spoofing o atacante pode esconder a sua verdadeira identidade (IP de origem).
2) Sobrecarregar servidores/roteadores: O IP spoofing faz com que os roteadores/servidores fiquem sobrecarregados ao ter de responder mensagens com endereços IPs falsos. Se isto for aplicado em grande escala, possibilita ataques de denial of service.

Aula 06

Segurança da Informação

IP Spoofing

Como são elaborados programas com o IP Spoofing ?

Para construir um programa com IP spoofing, o hacker ignora a camada de protocolo IP do sistema operacional e gera os seus próprios pacotes (modo RAW). Esta técnica dá ao hacker um controle total sobre os pacotes IP.

Quando este programa com IP Spoofing for executado, permitirá a escolha dos endereços IP de origem. O programa pode permitir ao usuário especificar um endereço IP, um grupo de endereços IP, ou ainda solicitar ao programa que gere endereços IP aleatoriamente.

Aula 06

Segurança da Informação

IP Spoofing

O que acontece quando se utiliza o IP Spoofing

Quando um servidor/roteador tenta responder a um pacote com endereço spoofado (endereço falso), poderá acontecer duas coisas:

- Se existir uma máquina ativa com o endereço IP indicado, esta máquina responderá que não está interessada em receber dados deste servidor, uma vez que ela não solicitou nenhuma comunicação com este host. Isto é feito através de um pacote com flag RST.
- Se não existir nenhuma máquina com o endereço IP indicado, o servidor/roteador acabará recebendo da rede uma mensagem de "Host Unreacheable".

Obs.: Tanto um caso quanto o outro fazem com que haja um consumo de CPU e de banda neste servidor. Este é um dos artifícios empregados nos ataques de denial of service. Neste ataques o servidor recebe milhares de pacotes com IP Spoofing e o resultado do tratamento a estes pacotes gera uma sobrecarga no host, ocasionando um denial of service.

Aula 06

Segurança da Informação

Denial of Service (DoS)

Conceito

Ataques de denial of service tem como objetivo paralisar (derrubar) um serviço em um servidor, ou então tornar os serviços tão lentos que o usuário legitimo não consegue acessá-los.

Quais vulnerabilidades são exploradas?

- Falhas em softwares

Softwares que possuem falhas de buffer overflow podem ser paralisados (derrubados) caso recebam um string que ultrapasse a capacidade de seu buffer. Isto causa um denial of service com paralisação do serviço que foi derrubado, exigindo um restart neste serviço. Outras falhas de software que causem o seu cancelamento e possam ser induzidas externamente também produzem o efeito de denial of service.

Denial of Service (DoS)

Quais vulnerabilidades são exploradas? (continuação)

- Falhas de Protocolo

  Alguns sistemas operacionais se desestabilizam quando recebem pacotes TCP/IP mal formados. Isto pode levar a uma queda completa do host, exigindo um shutdown.

- Esgotamento de recursos

  Todo máquina tem um conjunto de recursos limitado (CPU, memória, banda de comunicação). Se estes recursos forem esgotados, o servidor fica extremamente lento, ou pode cair. Este é o princípio utilizado pelos ataques de denial of service do tipo distribuido.

Denial of Service (DoS)

Tipos de ataques denial of service

- Denial of Service comum (DoS)

  Neste ataque, uma máquina ataca a outra. Normalmente exploram as vulnerabilidade de "Falha de Softwares" e "Falhas de Protocolo".

- Distributed Denial of Service (DDoS)

  Este ataque utiliza várias máquinas para atacar uma máquina alvo. O objetivo do ataque é esgotar algum recurso da máquina alvo.

Aula 06

Segurança da Informação

Denial of Service (DoS)

Como ocorre um ataque DDoS ?

1. Um hacker técnico desenvolve um sistema para explorar alguma vulnerabilidade dos protocolos TCP/IP. Este sistema é composto por dois programas: Master e Zumbi.
2. Para um hacker vândalo disparar um ataque é necessário primeiro "plantar" os programas zumbis nos computadores atacantes. Para isto o hacker vândalo invade computadores que tenha uma boa largura de banda e uma segurança fraca. Neste computadores eles instalam o programa zumbi.
3. Quando o hacker vândalo já tem uma quantidade suficiente de computadores comprometidos com o programa zumbi, ele dispara o ataque. Para isto ele utiliza o programa Master, o qual é capaz de se comunicar de forma direta (e normalmente criptografada) com os Zumbis. Através deste programa Master o hacker identifica o alvo do ataque, e como será feito o ataque.

Aula 06

Segurança da Informação

Denial of Service (DoS)

Como ocorre um ataque DDoS ?

4. Uma vez recebido o comando de ataque, todos os computadores Zumbis começam simultaneamente a atacar o computador alvo.
5. Normalmente os programa DDoS utilizam IP Spoofing. Desta forma a equipe responsável pela administração do Site que está sendo atacado não tem como saber quais os IPs fazem parte do ataque, pois os IPs são falsos. Isto dificulta as tentativas de filtragem. A única saída é tentar descobrir alguma característica nos pacotes recebidos que possa permitir separar os pacotes de ataque dos pacotes de acesso legítimo. Isto não é fácil, e exige que a equipe responsável pela segurança esteja bem treinada e preparada para este tipo de ataque.

Aula 06

Segurança da Informação

Sniffer

Conceito

Computadores em uma rede local (Ethernet) compartilham um meio físico. Normalmente, uma placa de rede "le" os pacotes destinados a ela, e descarta os demais. Um programa Sniffer coloca a placa de rede em modo promiscuo, possibilitando que um computador receba todos os pacotes que circulam no segmento de rede (domínio de colisão) a que pertence. Isto possibilita ao hacker obter informações privilegiadas (ex: senhas que circulam sem criptografia) que facilitem um ataque.

Aula 06

Segurança da Informação

Trojan

Conceito

O nome Trojan vem de "Trojan Horse": Cavalo de Tróia. Trata-se de um programa que finge realizar uma certa tarefa, e secretamente realiza uma outra tarefa maliciosa.

Características técnicas

1. Não detectáveis: Trojans sob medida (feitos especificamente para atacar uma certa empresa) não são detectados por antivírus, uma vez que não possuem uma assinatura que os identifique como vírus.

Aula 06

Segurança da Informação

Trojan

Características técnicas (continuação)

2. Executam de forma camuflada: Trojans normalmente se instalam como serviços, ou se instalam no startup com um programa sem janela. Os trojans se comunicam com o mundo exterior através de TCP ou UDP, empregando portas que estão abertas no firewall. Os Trojans mais sofisticados criptografam toda a sua comunicação para evitar que seja compreendia.

3. Backdoors: Uma das principais finalidades dos trojans é criar uma backdoor, permitindo ao hacker controlar a máquina comprometida, e poder assumir uma posição interna na rede. Isto abre novas possibilidades de ataque.

Aula 06

Segurança da Informação

Trojan

Tendências

Existe uma tendência de aumentar a utilização de Trojans em invasões de ambientes complexos, pois:

1. Elo Fraco: Exploram um elo fraco (curiosidade humana), permitindo uma instalação com muita facilidade. A grande maioria dos usuários atualmente considera seguro abrir um arquivo que recebeu em anexo em e-mails. Tais usuários acreditam que o sistema de antivirus irá bloquear qualquer arquivo nocivo.

Aula 06

Segurança da Informação

Trojan

Tendências

2. Facilidade de invasão pelo lado de dentro: Na maioria dos casos é mais fácil romper um sistema de segurança partindo de um ponto interno. A maioria das empresas reforça sua segurança na parte periférica da sua rede, e imagina que os usuários internos são "bem comportados".

3. Customização: Trojans podem ser customizados para invasões específicas. Eles podem por exemplo ser programados para executar algum comando que enfraqueça momentaneamente o sistema de segurança, permitindo ao hacker invadir a rede enfraquecida pelo lado externo.

Aula 06

Segurança da Informação

Trojan

Como é feito um ataque com o Trojan ?

1. O hacker tem dificuldade em atacar a rede alvo pelo lado de fora, mas percebe que o sistema de segurança talvez seja fácil de desarmar por dentro.
2. O hacker desenvolve um trojan com a função oculta de enfraquecer o sistema de segurança, ou instalar uma backdoor para permitir ao hacker analisar a rede por dentro.
3. Este trojan é enviado para os usuários da rede alvo, como um arquivo que atraia a curiosidade (imagem, piada). Para isto, o hacker pode inclusive forjar o seu endereço de e-mail, passando-se por um colega da empresa.
4. Os usuários inocentemente executam o trojan. O Trojan dá uma mensagem de despiste (arquivo corrompido), ou executa uma função de disfarce, e simultaneamente se instala na máquina de um forma camuflada (serviço).
5. Secretamente o Trojan passa a executar funções de ataque contra o sistema de segurança, ou então permite ao hacker começar a vasculhar a rede interna como se estivesse localizado numa máquina interna (backdoor).

Aula 06

Segurança da Informação

Engenharia Social

Conceito

O hacker se passa por outras pessoas, enganando os funcionários da empresa. Para poder fazer um "teatro" convincente, o hacker utiliza informações (nomes de usuários, administrador, etc) coletadas previamente. Com isto o hacker consegue obter informações privilegiadas (ex: senhas), ou então induzir funcionários a executar ações que enfraqueçam a segurança (ex: executar um trojan, induzir uma reinicialização de senha).

Aula 06

Segurança da Informação

Engenharia Social

Exemplos de Ataque de Engenharia Social

1. Usuário recebe um e-mail do "administrador" (que é o atacante disfarçado) solicitando para que a sua senha seja alterada para 'x'. Se o usuário proceder conforme solicitado, o hacker saberá qual sua senha, e poderá passar a utilizar a conta deste usuário.
2. Administrador da rede recebe um e-mail/telefonema de um "usuário" (que é o atacante disfarçado), solicitando a reinicialização da sua senha. Isto permite ao atacante logar com a senha deste usuário.
3. Administrador iniciante recebe um e-mail/telefonema de um "administrador de uma outra empresa" (que é o atacante disfarçado), alegando que está recebendo ataques da sua empresa e solicitando a execução de um comando para se certificar. Este comando pode ser um trojan.

Aula 06

Segurança da Informação

Consolidação do Poder

Conceito

Após o hacker ter conseguido invadir o computador alvo, ele procurará se certificar que seja possível voltar a invadir novamente em outra ocasião, de uma forma simples, sem perder tempo. Além disso, ele deve garantir que os rastros da sua invasão sejam apagados, para não correr o risco de ter seu acesso bloqueado. A este conjunto de atividades pós-invasão inicial, damos o nome genérico de consolidação do poder.

Aula 06

Segurança da Informação

Consolidação do Poder

Etapas na consolidação do poder

1. Promoção para Administrador: Caso o hacker tenha feito a sua invasão através de uma conta com poucos privilégios (conta de usuário), ele tentará se promover a administrador. Para isto, existe uma série de técnicas diferentes para cada sistema operacional.
2. Remoção de pistas: Após ter obtido privilégios para manipular os logs do sistema, o hacker eliminará os rastros de sua invasão, de forma a não chamar a atenção.
3. Instalar backdoors: Para poder retornar facilmente à maquina invadida, o hacker procurará instalar backdoors, ou então fará alguma modificação no sistema de segurança para deixá-lo mais aberto. Backdoors é preferida pelos hackers. Os programas que implementam a backdoor são normalmente difíceis de serem localizados, pois instalam-se de forma camuflada.

Segurança da Informação

Termino da Aula 06