Sistemas Operacionais

Segurança

Prof. José Roberto Bezerra

Conteúdo

- Conceitos básicos de segurança de sistemas
- Autenticação de usuários
- Ataques internos
- Ataques externos
- Mecanismos de Proteção

Objetivos gerais

- Confidencialidade dos dados
- Integridade dos dados
- Disponibilidade do sistema
- Privacidade

Invasores

Aqueles indivíduos que acessam informações que não lhe pertece ou não foi permitido acesso

Tipos de Invasores

- Curiosos
- Espiões internos
- Ladrões
- Espiões profissionais

Autenticação de Usuário

Processo de identificação de um usuário permitindo que tenha acesso ao sistema

Autenticação

- Como autenticar?
  - Alguma coisa que o usuário sabe
  - Alguma coisa que o usuário possui
  - Alguma coisa que o usuário é
- *Hackers* são aqueles indivíduos que conseguem passar pelo procedimento de autenticação do sistema fazendo-se passar por um usuário autorizado

Senhas

- A forma mais comum de autenticação, devido a simplicidade de implementação e fácil entendimento do usuário
- Compõe-se de nome de usuário e senha
  - O nome é buscado em uma lista
  - A senha informada é comparada com o valor armazenado
  - Se coincidentes o usuário é autenticado

Formas de invasão

- Tentativas com várias combinações de nome e senha (força bruta)
  - Nome a partir do Nome completo do usuário
    - João da Silva: joao, silva, jsilva,...
  - Senhas com valores de data de nascimento, endereço, senhas fáceis, nomes ao contrário, palavras de dicionário
  - Uso de *softwares* específicos
- Telnet
- *Packet sniffer*

Ataques de dentro do sistema

- Cavalos de Tróia
- Conexão Impostora (*login spoofing*)
- Bombas lógicas
- Alçapões
- Transbordo de *buffer*

Cavalos de Tróia

- Programa que aparentemente é inocente ou útil realiza uma função inesperada e indesejável
  - Remover, modificar ou criptografar arquivos do usuário
  - Copiar para locais que onde o invasor possa recuperá-los
  - Roubar senhas
- É necessário que o próprio usuário execute o código do Cavalo de Tróia
  - Não é necessário que haja a invasão do sistema
-

Conexão impostora

- O programa invasor apresenta uma tela semelhante a tela de *login* original.
- O usuário digita o nome e a senha certo de que está realizando o login normalmente
- Ao final, um arquivo é gravado com o login e a senha do usuário e enviado para um local pré-estabelecido
- Um sinal é enviado para matar o processo do programa invasor e permitindo que o programa correto seja chamado
- O usuário tem a impressão de que errou a senha e o sistema fez uma nova solicitação para login

Bombas lógicas

- Código escrito por um funcionário da empresa e secretamente colocado no sistema operacional
- Periodicamente a bomba (o programa) é alimentada com uma senha ou similar. Enquanto isto acontecer, a bomba não é “detonada”
- Caso o programador seja demitido ou transferido e não possa mais retardar a “explosão” a mesma ocorre

- A Explosão representa alguma ação destrutiva para o sistema
  - Apagar todo o disco
  - Apagar arquivos aleatórios
  - Fazer alterações difíceis de detectar em arquivos
  - Criptografar arquivos de sistema

Alçapões (*trap door*)

- Semelhante a bomba lógica que é criada por um programador do próprio sistema
- Consiste em alterar/inserir um código que permita a conexão de um usuário mesmo que não digite uma senha
- A única maneira de prevenir-se contra *trap doors* é fazer revisões periódicas de código
-

Vírus

Programa capaz de se disseminar anexando seu código a um outro programa e produzindo efeitos danosos ao sistema

Potenciais danos

- Os vírus podem realizar tarefas similares a outros programas para desviar a atenção do usuário aos danos que pode causar
  - Criptografar dados do usuário
  - Tornar o sistema inacessível (*denial of service*)
  - Danificar o hardware (BIOS em *flash* ROM)
  - Apagar arquivos
  - Mudar nomes de arquivos vitais para o sistema

Tipos de Vírus

- Companheiro
- Programas executáveis
- Residentes em memória
- De *boot*
- De macro
- Código-fonte

Vírus Companheiro

- São vírus que são executados associados a execução de um dado programa
- Por exemplo, a calculadora
- Sempre que o usuário executa a calculadora um outro programa é chamado (vírus) executa alguma ação e em seguida a calculadora original é executada

Vírus de programas executáveis

- Sobrescrevem o código executável de um programa por outro (o vírus)
- Normalmente fazem uma varredura do sistema procurando arquivos executáveis e substituindo pelo código malicioso
- Ao executar um programa, na verdade o usuário estaria executando o vírus. Como foi chamado

Vírus residentes em memória

- São aqueles que permanecem carregados na memória principal durante o funcionamento do sistema
- Funcionam manipulando instruções de controle de fluxo para que seu próprio código seja executado
- Desvia principalmente as chamadas de sistema para ter acesso ao modo núcleo

Vírus de *boot*

- Se instalam na MBR ou alteram seu conteúdo para que sejam carregados junto com o sistema operacional
- São normalmente carregados na memória principal
- Também podem danificar o conteúdo da BIOS do computador, inutilizando-o

Vírus de Macro

- Macros são agrupamentos de comandos de um dado aplicativo como Word e Excel, por exemplo
- Uma macro pode conter programas inteiros que tem a capacidade de executar praticamente qualquer comando no sistema
- Um vírus pode se disfarçar de uma macro e realizar operações destrutivas no sistema

Verificadores de Vírus (anti-vírus)

- Os vírus utilizam artifícios para se tornarem ocultos do usuário
- É necessário a utilização de programas especiais para rastrear a presença de vírus no sistema e removê-los
- Vasculham programas executáveis em busca de padrões de códigos previamente determinados e cadastrados em uma base de dados do anti-vírus

Verificadores de integridade

- São anti-vírus que detectam a presença de vírus através da verificação da integridade dos arquivos executáveis
  - Verfica se o disco está livre de vírus
  - Caso esteja, calcula a soma de verificação de cada arquivo executável e armazena-os
  - Na próxima verificação, refaz os cálculos da som a e compara com o valor previamente armazenado
  - Caso tenha alteração o arquivo é apontado como infectado

Verificadores de comportamento

- O anti-vírus fica residente em memória e monitora possíveis anomalias no comportamento do sistema
- Por exemplo, sobrescrever um arquivo executável é uma atividade incomum e pode ser considerada suspeita e identificar um possível vírus

Recuperação de um ataque de vírus

- Interromper o sistema
- Reiniciar a partir de CDROM ou USB
- Passar o programa antivírus para detectar o vírus no disco
- Converter arquivos não infectados para formatos que os vírus não podem infectar (ASCII)
- Fazer Backup destes arquivos
- Formatar o sistema, inclusive a MBR

Política de segurança

A política de segurança é um mecanismo preventivo de proteção dos dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pelo corpo técnico e gerencial e pelos usuários, internos ou externos

Objetivos

- Descreve o que está sendo protegido e por quê
- Define prioridades sobre o que precisa ser protegido em primeiro lugar e com qual custo
- Permite estabelecer um acordo explícito com várias partes da empresa em relação ao valor da segurança
- Fornece ao departamento de segurança um motivo válido para dizer “não” quando necessário
- Proporciona ao departamento de segurança a autoridade necessária para sustentar o “não”
- Impede que o departamento de segurança tenha um desempenho fútil

Atitutes a evitar na área de informática

Há menos de uma década, bastavam um cadeado, correntes reforçadas no portão e um cachorro feroz para manter a empresa e seus dados protegidos dos gatunos. Hoje, com a maior parte das informações digitalizadas, é preciso ir além.

Não dá para deixar de investir em softwares de segurança e no treinamento dos funcionários para preservar os segredos da empresa. E não são poucas as ocorrências de espionagem industrial. A maioria dos 'piratas' conta com a ajuda dos funcionários da área de informática. Com bons conhecimentos técnicos, facilitam a vida da concorrência por meio da entrega de dados confidenciais da casa.

Bibliografia

- Sistemas Operacionais Modernos
  - Seção 9.1
  - Seção 9.3
  - Seção 9.4
  - Seção 9.5

OBSERVAÇÃO

A disponibilização das notas de aula através de slides serve apenas como apoio aos estudos. Para um bom aproveitamento e aprendizado é necessário a leitura das referências (livro texto) e estar atento às aulas