PCS 3446 – Sistemas Operacionais

Prof. João José Neto

Aula 27

Segurança em Sistemas Operacionais


010001 001011 110100
» SECURITY «


infected
trojan
VIRUS
malicious
attack

CONCEITOS

Objetivos deste estudo em S.O.

- Atender os requisitos de ***integridade*** (de dados e do sistema), ***disponibilidade*** e ***confidencialidade*** dos recursos dos sistemas de informação (confidencialidade dos dados, e privacidade), incluindo hardware, software, firmware, dados/informação e telecomunicações.
- Para isso, o sistema deve garantir que seus usuários sejam ***autenticados*** e que os autores de quaisquer acessos ao sistema possam ser identificados de forma segura.

Situações de Quebra de Segurança em um Sistema Computacional

Efeito (sintoma)	Ação (ataque)
Abertura não autorizada (acesso a dados por parte de uma entidade que não tem esse direito)	**Exposição** (liberação para entidade não autorizada) **Interceptação** (acesso não autorizado a dados em trânsito) **Inferência** (dedução de informação sigilosa a partir de dados obtidos em acesso não autorizado) **Intrusão** (entidade não autorizada burla a segurança)
Decepção (entidade autorizada recebendo dados falsos como se fossem autênticos)	**Mascaramento** (entidade indevida passa por autorizada) **Falsificação** (passar dados falsos a entidade autorizada) **Repúdio** (prejudicar uma entidade por parte de outra que falsamente nega a sua responsabilidade por um ato)
Desrupção (algo interrompe ou impede o funcionamento correto do sistema)	**Incapacitação** (desabilitar algum componente de sistema) **Corrupção** (deterioração deliberada de funções ou dados) **Obstrução** (interrupção de serviço devido a algum bloqueio da operação do sistema)
Usurpação (entidade não autorizada assume o controle de serviços)	**Apropriação indevida** (assumir indevidamente o controle lógico ou físico de um recurso do sistema) **Mau uso** (levar o sistema a uma ação que lhe seja prejudicial)

Danos Causados por Malware a um Sistema Computacional

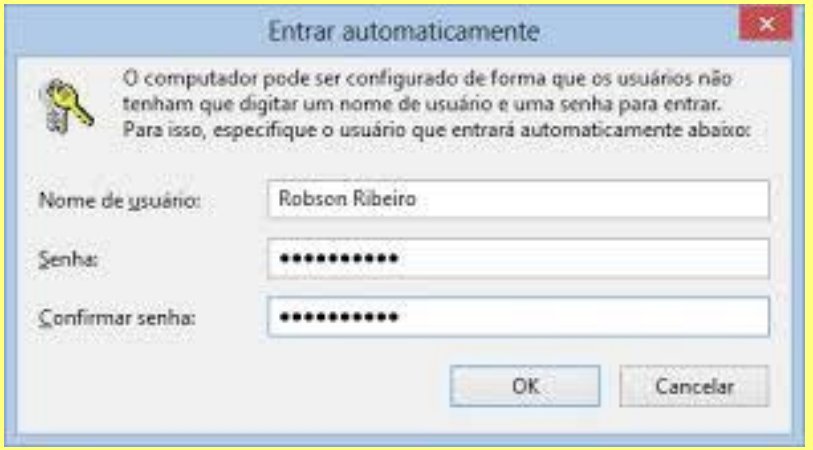
	Disponibilidade	Confidencialidade	Integridade
Hardware	Equipamento roubado ou inutilizado		Inutilização de um equipamento pelo malware
Software	Programa apagado	Cópia não autorizada	Programa modificado para operar incorretamente ou executar função indevida
Dados	Arquivos apagados	Leitura ou análise estatística de dados não autorizada	Alteração não autorizada de arquivos ou criação indevida de outros novos
Comunicação	Mensagens destruídas ou apagadas, ou linhas de comunicação ou redes indisponibilizadas	Leitura não autorizada ou observação indevida do tráfego de mensagens	Alteração, reordenação, atraso, duplicação de mensagens ou criação de falsas mensagens

Padrões de Comportamento de Intrusos

	Hacker	Atividade criminosa	Interno
1	Acesso a um IP através de ferramenta de espionagem	Ação rápida e precisa para passar desapercebido e dificultar detecção	Criação de contas na rede para si e para seus amigos
2	Mapear a rede em busca de serviços acessíveis	Explorar a periferia do computador em busca de portas vulneráveis	Acesso a contas ou programas não muito utilizados no dia-a-dia
3	Identificar potenciais serviços vulneráveis	Usar cavalos de tróia (software escondido) para deixar portas dos fundos abertas para novos acessos	Envio de e-mails para antigos e potenciais novos interessados
4	Tentativa e erro para adivinhar senhas	Usar ferramentas para capturar passwords	Usar chats para passar mensagens furtivas
5	Instalação de ferramenta de administração remota	Não permanecer ativo nas imediações para não ser percebido	Visitar páginas web corporativas para espionar sua utilização
6	Aguardar login de administrador para roubar sua senha	Cometer poucos ou nenhum erro	Executar longos downloads e cópias de arquivos
7	Usar senha roubada p/ acessar o resto da rede		Acessar a rede em horas de baixo tráfego

Terminologia Associada a Programas Maliciosos

Nome	Descrição
Vírus	Cria cópias de si próprio dentro de um programa executável
Verme	Roda isoladamente, e propaga clones para outras máquinas/redes
Bomba lógica	Inserido em aplicativo por intruso, aguarda evento para ativar-se
Cavalo de Tróia	De aparência útil e inofensiva, ao ser ativado viola a segurança
Backdoor	Burla a verificação de segurança e proporciona acessos indevidos
Código móvel	Script, macro ou software portátil, eficaz em variadas plataformas
Exploits	Código específico p/ explorar dado conjunto de vulnerabilidades
Downloaders	Enviado por e-mail instala elemento indevido na máquina atacada
Auto-roteador	Ferramentas de hacker, usado para invasões remotas indevidas
Kit (gerador de vírus)	Ferramenta de geração automática de novos vírus.
Spammers	Envia grandes quantidades de e-mails indesejados
Flooders	Força tráfego volumoso, p/ provocar a recusa de serviço na rede
Keyloggers	Captura teclas digitadas pelos usuários do sistema contaminado
Rootkit	Ferramentas instaladas após invasão, para hacking da máquina
Robô (zumbi, bot)	Prog. ativado em máquina infectada p/ promover outros ataques
Spyware	Coleta informações de uma máquina, e envia-as para outras
Adware	Propaganda embutida em software: pop-ups e redirecionamentos



TÉCNICAS DE SEGURANÇA EM S.O.

Motivação

- Pode-se perceber a necessidade e a importância de que haja no sistema algum **mecanismo de proteção** que impeça que programas intrusos e que outras formas de quebra de segurança venham a causar maiores danos no sistema computacional.

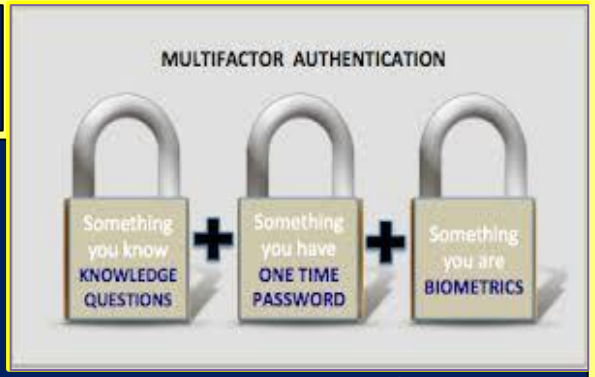
Principais técnicas de segurança no sistema computacional

- Para impedir, ou ao menos minimizar os danos provocados pela quebra de segurança em um sistema computacional têm sido adotadas algumas **técnicas**, entre as quais as mais importantes, e que serão discutidas a seguir, são:
  - **autenticação**
  - **controle de acesso**
  - **detecção de intrusos**
  - **defesa contra malware**
  - **cuidados com ataques de buffer overflow**

Autenticação

- A **verificação de identidade** é usada para garantir que a entidade esteja autorizada a usar os recursos do sistema, e para isso considera dois passos:
  - Passo de **identificação** – a entidade apresenta um "passaporte" ao sistema de segurança.
    Identificar uma entidade como válida é base para o esquema de segurança e abre portas para os demais serviços do sistema, logo requer muito cuidado.
  - Passo de **verificação** – ocorre quando da autenticação do "passaporte" apresentado, procurando assim associar de forma segura a entidade com a sua identificação.

Formas de Autenticação



- Principais **formas de autenticação**:
  - algo que só a entidade deveria saber (***senha***, ***número de identificação pessoal*** , ***respostas a perguntas predeterminadas***);
  - algo que só a entidade possui (***tokens*** tais como ***chaves eletrônicas***, ***cartões inteligentes***, ***chaves físicas***);
  - algo que a entidade é (***biometria estática: impressão digital, imagem de retina, imagem do rosto***);
  - algo que a entidade é capaz de fazer (***biometria dinâmica: ritmo de digitação, padrão de voz, análise grafológica do manuscrito***).
- O custo da utilização dessas técnicas varia. Reconhecimentos menos rigorosos, em custo crescente:
  - Os mais econômicos: de **voz**, de **face**, de **assinatura**, de **mão**;
  - Intermediários: dos **dedos** e da **retina**;
  - O mais preciso e oneroso: de **íris**.

Controle de acesso

- Estabelece os tipos, circunstâncias e agentes dos acessos permitidos, e pode ser efetuado de três modos (eventualmente aplicados em conjunto):
  - **Discricionário** – Acessos aos recursos do sistema são concedidos ou não por decisão unilateral do sistema de controle.
  - **Mandatório** – Acessos são concedidos só se o nível de segurança do requisitante for compatível com as permissões de acesso ao recurso, estabelecidas para o requisitante.
  - **Baseado no papel da entidade** – Baseia-se na compatibilidade entre a função desempenhada no sistema pelo requisitante e regras preestabelecidas para o acesso.
- **Matrizes e listas de controle de acesso** costumam ser utilizadas para a implementação desta técnica, e relacionam as informações sobre os direitos do requisitante com as restrições que o sistema impõe quanto ao acesso dos usuários ao recurso solicitado.

Detecção de intrusos

- Para a presente discussão, são relevantes dois conceitos:
  - **Intrusão na segurança** – evento ou combinação de eventos que caracteriza um incidente de segurança de acesso ao sistema, ocorrido sem autorização.
  - **Detecção da intrusão** – monitorando e analisando os eventos do sistema, um serviço localiza e denuncia tentativas ou ocorrências de acessos não autorizados ao sistema.

Requisitos

- Este grupo de técnicas se concentra em determinar a presença de intrusos e o seu efeito no sistema. Para isso, deve contar com:
  - ***Sensores***, responsáveis pela coleta de dados, compreendendo pacotes de rede, arquivos de log, relações de chamadas de sistema.
  - Os sensores enviam os dados coletados aos ***analisadores***, que também podem receber dados provenientes de outros analisadores, indicando se foi detectada a presença de algum intruso no sistema.
  - Como saída, os analisadores enviam a uma ***interface com o usuário*** o diagnóstico realizado, e as evidências encontradas que levaram a tal diagnóstico.

Técnicas de detecção usuais

- As técnicas usuais de detecção de intrusos abrangem
  - detecção de **anomalias de comportamento**
  - detecção de **assinaturas de intrusos**.
- Ferramentas essenciais para esta família de técnicas de segurança são os **registros de auditoria**, que podem ser
  - ***Nativos***
    (coletam informação sobre a atividade normal do sistema)
  - ***Específicos*** (exclusivos para alguma particular ocorrência)

  e indicam:
  - o *sujeito*, a *ação*, o *objeto*
  - a *condição de exceção*, o *recurso* afetado e o *uso* dele efetuado
  - uma *identificação temporal* única da ocorrência

Defesas contra malware

- Nesta classe incluem-se as medidas profiláticas contra intrusões.
  Antivírus envolvem:
  - **Detecção** – uma vez infectado, ***identificar*** essa situação e ***localizar*** sua causa.
  - **Identificação** – após constatar sua existência, ***descobrir a praga atuante específica***
  - **Remoção** – ***restaurar o sistema*** a seu estado original pela ***destruição*** do fator contaminante
  - **Reinstalação** – Detectando a praga, mas falhando nas outras ações, é instalada uma cópia não contaminada do programa.
  - **Ações específicas** – Particulares, para cada tipo de praga (vírus, vermes, *bots*, etc), sempre com a finalidade profilática de ***neutralizar sua ação*** e, preferencialmente, de ***erradicá-la***.

Ataques de *buffer overflow*

- *Overflow* de *buffers* é frequente, fácil de detectar e de ser usado indevidamente para fins escusos.
- Ações corretivas usuais nesse sentido ***inserem defesas*** no programa em tempo de compilação;
- A ***escolha de uma linguagem*** de programação adequada pode melhorar o cenário, bem como o ***uso de extensões de linguagem*** e de ***bibliotecas seguras***;
- Mecanismo de ***proteção*** de pilha;
- Mecanismos de ***proteção contra ataques*** em tempo de execução.

Comentários

- O material aqui discutido foi apenas um rápido estudo de um tópico cada vez mais importante no software básico dos sistemas computacionais, particularmente nos sistemas operacionais e nos sistemas de comunicação e de administração de rede, que são os responsáveis pela gestão de recursos físicos e lógicos mais sujeitos à invasão por agentes maliciosos externos.
- Recomenda-se aos interessados um aprofundamento maior, que pode ser feito com o auxílio de boas publicações específicas, muitas disponíveis na Internet.

Apresentação baseada em

Stallings

Operating Systems – Internals and Design Principles

6ª. ed. Pearson, 2009, cap. 14 e 15