APRESENTAÇÃO DO MATERIAL

Queridos alunos!!

Sabemos que os **resumos** das disciplinas **são fundamentais para fixação de conteúdos** e, também, para **realização de revisões**. Um resumo bem feito garante que os principais pontos de cada matéria sejam revisados de forma rápida, **aumentando a produtividade dos estudos e a eficiência das revisões**.

Além disso, sabemos que, principalmente para os grandes concursos, o número de matérias cobradas no edital é muito grande. Dessa forma, além de revisar os pontos marcados em seus materiais, um bom resumo pode encurtar o tempo de revisão, garantindo, assim, que todo o material possa ser revisado em um período de tempo mais curto.

Com isso em mente, apresentamos a vocês o **Resumo de Informática - SegInfo - Parte 3 - Antimalwares**. Trata-se de um material pensado para lhe ajudar em todo esse processo, visando, inclusive, uma economia de tempo de confecção de materiais, tempo que é o bem mais precioso de um concurseiro, não é mesmo?

Esperamos poder ajudá-los!

Conte sempre com o Estratégia em sua caminhada!

Estratégia Concursos

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 11.

Esse é um material resumido. Em momento algum ele substitui o estudo do material completo. Trata-se de um complemento aos estudos e um facilitador de revisões!

Resumo de Informática

SegInfo - Parte 3 - Antimalwares

Ferramentas Antimalware

- Ferramentas Antimalware são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador (Ex: Antivírus, Antispyware, Antirootkit e Antitrojan). Apesar de inicialmente eles terem sido criados para atuar especificamente sobre vírus, com o passar do tempo, passaram também a englobar as funcionalidades dos demais programas, fazendo com que alguns deles caíssem em desuso. Há diversos tipos de programas antimalware que diferem entre si sob diversos critérios.

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 11.

- **Método de detecção**: assinatura (uma lista de assinaturas é usada à procura de padrões), heurística (baseia-se nas estruturas, instruções e características do código) e comportamento (baseia-se no comportamento apresentado) são alguns dos métodos mais comuns.
- **Forma de obtenção**: podem ser gratuitos, experimentais ou pagos. Um mesmo fabricante pode disponibilizar mais de um tipo de programa, sendo que a versão gratuita costuma possuir funcionalidades básicas ao passo que a versão paga possui funcionalidades extras e suporte.
- **Execução**: podem ser localmente instalados no computador ou executados sob demanda por intermédio do navegador Web. Também podem ser online, quando enviados para serem executados em servidores remotos, por um ou mais programas.
- **Funcionalidades apresentadas**: além das funções básicas (detectar, anular e remover códigos maliciosos) também podem apresentar outras funcionalidades integradas, como a possibilidade de geração de discos de emergência e firewall pessoal.

FASES	DESCRIÇÃO
DETECÇÃO	Uma vez que a infecção do vírus tenha ocorrido em algum programa de computador, localize o vírus.
IDENTIFICAÇÃO	Uma vez que o vírus tenha sido detectado, identifique qual vírus específico que infectou um programa.
REMOÇÃO	Uma vez o vírus tenha sido identificado, remova todos os traços do vírus do programa infectado e restaure-o ao seu estado original.

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 11.

NÃO É RECOMENDÁVEL UTILIZAR MAIS DE UM ANTIMALWARE SIMULTANEAMENTE

POSSÍVEIS CUIDADOS
Tenha um antimalware instalado em seu computador (programas online, apesar de bastante úteis, exigem que seu computador esteja conectado à Internet para que funcionem corretamente e podem conter funcionalidades reduzidas).
Utilize programas online quando suspeitar que o antimalware local esteja desabilitado/comprometido ou quando necessitar de uma segunda opinião (quiser confirmar o estado de um arquivo que já foi verificado pelo antimalware local).
Configure o antimalware para verificar toda e qualquer extensão de arquivo.
Configure o antimalware para verificar automaticamente os discos rígidos e as unidades removíveis (como pen-drives, CDs, DVDs e discos externos).
Mantenha o arquivo de assinaturas sempre atualizado (configure o antimalware para atualizá-lo automaticamente pela rede, de preferência diariamente).
Mantenha o antimalware sempre atualizado, com a versão mais recente e com todas as atualizações existentes aplicadas.

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 11.

TIPOS DE ANTIVÍRUS	DESCRIÇÃO
1º GERAÇÃO	Também chamada de Detecção Baseada em Assinatura, ele busca por um trecho único do código do vírus (estrutura ou padrão de bits) chamado de assinatura. Procurando por esse trecho, o antivírus pode detectar o vírus sem precisar analisar o arquivo inteiro. É realizada uma engenharia reversa no software malicioso para entendê-lo. Então é desenvolvida uma maneira de detectá-lo, depois ele é catalogado em uma base de dados e distribuído para todos os clientes do antivírus.
2º GERAÇÃO	Também chamada de Detecção Baseada em Heurística, ele utiliza um conjunto de técnicas para identificar vírus desconhecidos de forma proativa chamada heurística – sem depender de assinatura. Nesta linha, a solução de segurança analisa a estrutura de um arquivo e compara o seu comportamento com certos padrões que podem indicar a presença de uma ameaça.
3º GERAÇÃO	Também chamada de Interceptação de Atividade, ele utiliza uma tecnologia que identifica um vírus por suas ações, em vez de sua estrutura em um programa infectado. Esses programas têm a vantagem de não ser necessário desenvolver assinaturas e heurísticas para uma ampla variedade de vírus. É diferente da heurística porque só funciona com programas em execução, enquanto a heurística analisa o próprio arquivo sem a necessidade de executá-lo.
4º GERAÇÃO	Também chamado de Proteção Completa, São pacotes compostos por uma série de técnicas antivírus utilizadas em conjunto. Estas incluem componentes de varredura e de interceptação de atividades. Ademais, esse tipo de pacote inclui recurso de controle de acesso, que limita a capacidade dos vírus de penetrar em um sistema e, por consequência, limita a capacidade de um vírus de atualizar arquivos a fim de passar a infecção adiante. Trata-se da geração da maioria dos antivírus atuais.

Antispyware

- É um tipo de software projetado para detectar e remover programas de spyware indesejados. Spyware é um tipo de malware instalado em um computador sem o conhecimento do usuário para coletar informações sobre ele. Isso pode representar um risco de segurança para o usuário, além de degradar o

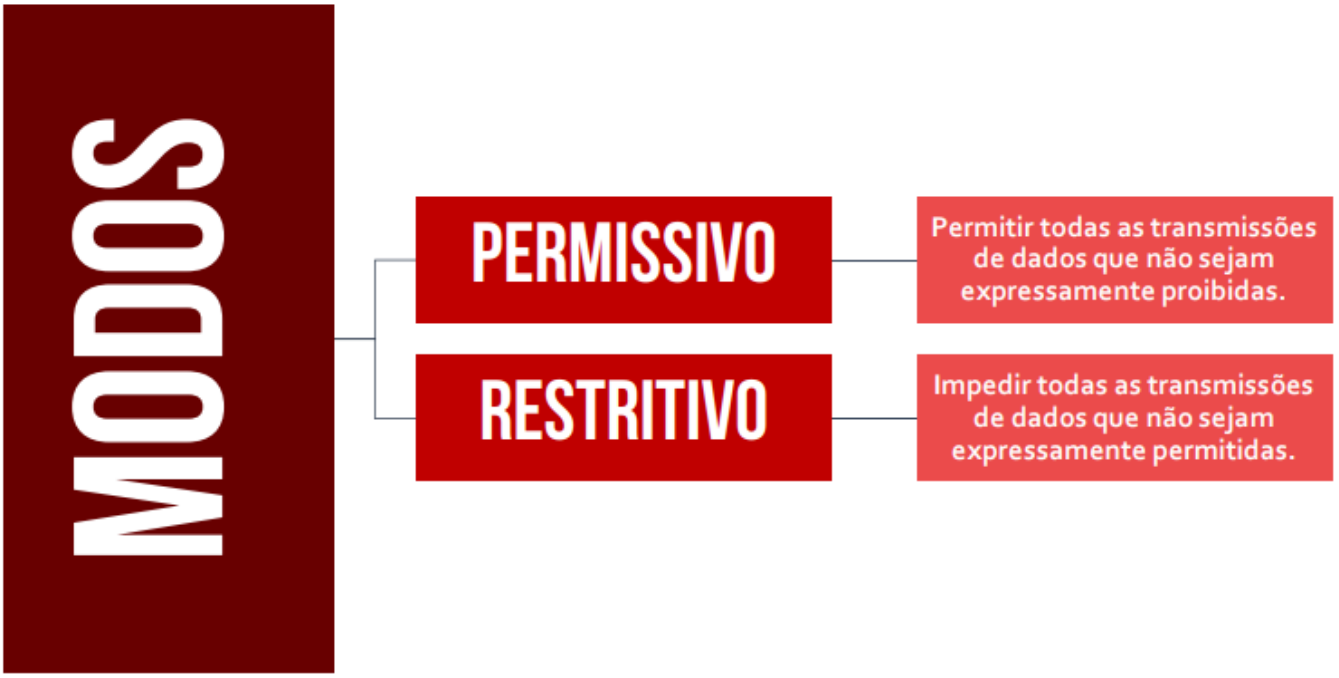
desempenho do sistema, absorvendo o poder de processamento, instalando software adicional ou redirecionando a atividade do navegador dos usuários.

Antispam

- Filtros Antispam já vêm integrados à maioria dos programas de e-mails e permite separar os desejados dos indesejados – os famosos spams. A maioria dos filtros passa por um período inicial de treinamento, no qual o usuário seleciona manualmente as mensagens consideradas spam e, com base nas classificações, o filtro vai "aprendendo" a distinguir as mensagens. Ao detectá-las, essas ferramentas alertam para que ele tome as atitudes adequadas para si.

Firewall

- São dispositivos, em forma de software e/ou de hardware, que possuem a função de regular o tráfego de dados entre redes distintas, impedindo a transmissão e/ou a recepção de acessos nocivos ou não autorizados de uma rede para outra. Ele controla, analisa, registra, polícia, monitora, regula e filtra o tráfego ou movimentação da entrada/saída de dados, detectando ameaças e bloqueando o acesso que não esteja em conformidade com a política de segurança da organização.



TIPOS DE FIREWALL	DESCRIÇÃO
FIREWALL PESSOAL	Software utilizado para proteger um único computador, controlando o tráfego dos dados contra acessos não autorizados provenientes da internet.
FILTRO DE PACOTES	Firewall mais antigo capaz de executar uma política de filtragem com base na combinação de regras específicas (protocolo, porta e lista negra/branca) para examinar cada pacote – sem estado.
FILTRO DE ESTADO DE SESSÃO	Firewall mais moderno que analisa informações dos cabeçalhos dos pacotes de dados e cria uma tabela de estados de conexões para realizar a filtragem baseado nas conexões – com estado.

Proxy

- É um servidor que age como um intermediário para requisições de clientes solicitando recursos de outros servidores. Ele funciona como um Firewall no sentido de que é capaz de impedir que sua rede interna seja exposta à Internet – redirecionando solicitações da/para web quando necessário.