PERGUNTA 42 (GERENCIAMENTO DE SEGURANÇA DO SO)	PERGUNTA 42 (GERENCIAMENTO DE SEGURANÇA DO SO)
Por que há a necessidade de manter os computadores seguros?	Computadores são **fontes de informação,** se uma informação poder ser **alterada ou compartilhada** com quem não deve, essa informação não é segura. Portanto existe uma grande necessidade de proteger as informações dos computadores.
Quais são os Sistemas Operacionais mais utilizados nos dias de hoje e como eles podem ser classificados no quesito Segurança?	**Windows:** possuí uma **Segurança Baixa,** além disso, por ser o SO mais popular, ele é alvo fácil de hackers; **Mac OS X:** possuí uma **Segurança Mediana,** por não ser tão popular devido o preço, não é um alvo prioritário; **Linux:** possuí **Segurança Maior,** não é muito utilizado por pessoas comuns, é mais usado por desenvolvedores. Porém, é um risco se instalado num servidor, por ser open source.
O que é um Vírus de Computador de como eles agem?	Vírus são **programas criados com o objetivo de infectar outros programas e causar algum tipo de dano.** Eles se aproveitam de **falhas na segurança e brechas deixadas por desenvolvedores** para se instalar e infectar máquinas que **estejam conectadas na mesma rede.**
Qual é a maneira mais comum dos Vírus agirem?	Eles têm **3 funções básicas:** **Primeiro** eles tentam **se esconder** da melhor maneira possível; **Segundo** eles tentam **se replicar** invadindo outros programas ou computadores que estejam na mesma rede; **Terceiro** cumprem o **papel para o qual foram criados:** roubar dados, espionar ou até mesmo danificar o equipamento.
O que é um Vírus de Programa Executável?	Um **Vírus de Programa Executável** é um vírus que é **executado quando o usuário abre um programa.** Eles fazem isso usando uma **técnica chamada sobreposição, eles sobrepõem o seu código sobre o código da aplicação.** Outra tática, é se **mascarar no atalho de um programa,** quando o usuário executa o programa, **antes ele abre o vírus sem perceber** e depois ele abre o programa. Quando agem, **se multiplicam e se anexam a outros programas.**
O que é um Vírus de Memória?	Um **Vírus de Memória** é um vírus que procura se **alocar na memória do computador, ele procura pelas partes da memória que raramente são utilizadas pelo sistema para não serem encontrados.** Alguns têm até a capacidade de **disfarçar o espaço de memória como se o espaço estivesse em execução, para evitar que o SO realocasse o seu espaço.** O objetivo deles é **alterar o controle do Sistema Operacional à sua vontade, entrando no Kernel.**
O que é um Vírus de Setor de Boot?	Como a maioria dos computadores modernos utilizam ROM´s com programas da **BIOS que podem ser reescritos**, abriu-se uma brecha para a entrada de vírus. E é justamente ai que o **Vírus de Boot ataca, ele se aloja na ROM e consegue reescrever o programa BIOS danificar o setor de Boot, impedido que o Sistema Operacional carregue ou que um vírus maliocioso seja carregado toda vez que o computador é iniciado.**
O que é um Vírus de Drivers de Dispositivo?	É um Vírus que consegue **infectar um Driver de Dispositivo.** O que é muito **perigoso,** pois os **drivers são carregados em modo Kernel, o que dá ao vírus acesso as instruções privilegiadas.** Ou seja, ele **pode controlar todo o Sistema Operacional.**
O que é um Vírus de Macro?	Programas como o **Word, Excel e Power Point da Microsoft permitem a criação de macros usando linguagem Visual Basic. (Linguagem de programação completa.)** As Macros permitir que um usuário carregue comandos gravados. Porém, isso é **uma brecha para Vírus de Macro que são codificados em Visual Basic.** Se um usuário executar uma **Macro maliciosa, esse vírus pode apagar arquivos e modificar propriedades dos programas.**
O que é um Vírus de Código Fonte?	São Vírus enviados via rede que **procuram arquivos escritos em Código Fonte, como C por exemplo, e fazem a alterações no arquivo escrevendo o seu próprio código no contexto do código original.** Quando o arquivo original é carregado, o vírus também é, agindo e se multiplicando no computador. Nesse momento as **boas práticas de programação se fazem necessárias, pois é muito difícil encontrar esses vírus em códigos mal organizados.**

PERGUNTA 42 (GERENCIAMENTO DE SEGURANÇA DO SO)		PERGUNTA 42 (GERENCIAMENTO DE SEGURANÇA DO SO)
Qual a diferença entre um Hacker e um Cracker?		**Crackers são os responsáveis por crimes digitais,** seu nome vem de **"Quebra"** em inglês. **Hackers são decifradores de códigos.** Existe a confusão sobre os dois termos por que no final da **década de 80 e início de 90, alguns Hackers resolveram praticar atos ilícitos e causar prejuízos.** Por isso, outros **Hackers os nomearam de Crackers para que sua imagem não fosse afetada.**
Qual é a classe de computadores que nunca foi invadida por Crackers?		São os **Mainframes,** isso se dá ao fato deles utilizarem um **Sistema Operacional Único e serem dedicados a apenas uma aplicação.** Além de possuírem um **sistema de segurança rígido e caro de ser implementado.**