# Segurança da Informação

Unidade 1 *Hackers*, *crackers* e os sistemas

computacionais



#### **Diretor Executivo**

DAVID LIRA STEPHEN BARROS

**Gerente Editorial** 

CRISTIANE SILVEIRA CESAR DE OLIVEIRA

Projeto Gráfico

TIAGO DA ROCHA

**Autoria** 

DANIEL CARLOS NUNES

# **AUTORIA**

#### **Daniel Carlos Nunes**

Olá! Sou Mestre em Desenvolvimento de Processos pela UNICAP, com experiência na elaboração de rotinas e processos para a otimização de operações e redução do custo operacional, executando atividades por cerca de 20 anos. Docente de Pós-Graduação na Universidade Estácio, fui professor formador, modalidade à distância, do Sistema Escola Aberta do Brasil - UAB, Instituto Federal de Educação, Ciências e Tecnologia de Pernambuco (IFPE). Fui Professor Líder de Projeto no Centro de Estudos e Sistemas Avançados do Recife, CESAR / HANIUM. Consultor de Custos em Sistemas de Saúde com foco em Gestão Hospitalar, da empresa Essencial TI. Já realizei trabalhos em várias instituições privadas, entre elas, Diname Factoring e Lojas Tentação. Na Área de Saúde, destacamse trabalhos já realizados no Centro Hospitalar Albert Sabin, Hospital de Olhos de Pernambuco, HOPE), Centro Hospitalar São Marcos, Laboratório Boris Berenstein. Estou muito feliz em poder ajudar você nesta fase de muito estudo e trabalho. Conte comigo!

# **ICONOGRÁFICOS**

Olá. Esses ícones irão aparecer em sua trilha de aprendizagem toda vez que:



OBJETIVO: para o início do desenvolvimento de uma nova competência:



NOTA: quando forem necessários observações ou complementações para o seu conhecimento:



EXPLICANDO MELHOR: algo precisa ser melhor explicado ou detalhado:



SAIBA MAIS: textos, referências bibliográficas e links para aprofundamento do seu conhecimento:



ACESSE: se for preciso acessar um ou mais sites para fazer download, assistir vídeos, ler textos, ouvir podcast;



ATIVIDADES: quando alguma atividade de autoaprendizagem for aplicada;



DEFINIÇÃO: houver necessidade de se apresentar um novo conceito;



IMPORTANTE: as observações escritas tiveram que ser priorizadas para você:



VOCÊ SABIA? curiosidades e indagações lúdicas sobre o tema em estudo, se forem necessárias:



REFLITA: se houver a necessidade de chamar a atenção sobre algo a ser refletido ou discutido sobre:



RESUMINDO: quando for preciso se fazer um resumo acumulativo das últimas abordagens;



TESTANDO: quando o desenvolvimento de uma competência for concluído e questões forem explicadas;

# **SUMÁRIO**

Unidades básicas de um computador	12
A máquina, o sistema e a segurança	12
O Computador	12
Dispositivos de entrada e saída de dados	
Teclado	14
Monitor	15
Mouse	15
Roteador Wi-Fi	16
Interfaces "Él"	16
Pen drive	17
USB	17
Bluetooth (tecnologia)	18
Portas paralelas	18
Os barramentos	18
Disco Rígido - HD	18
Memória do computador	19
Unidade Central de Processamento (CPU)	20
Tipos de sistemas operacionais	22
O que é um Sistema operacional?	22
O que um sistema operacional é capaz de fazer?	22
Gerenciamento dos processos	23
Gerenciamento da memória	23
Gerenciamento dos recursos	23
Gerenciamento de entrada e de saída de dados	23
Gerenciamento do sistema de arquivos	24
Como um sistema operacional funciona?	24
A Estrutura de um sistema operacional	25

Distribuição e licenças dos sistemas operacionais	26
Sistema operacional fechado	26
Sistema operacional aberto	26
Sistema operacional freeware	26
Conhecendo o Windows	27
Sistema Operacional Windows	27
As Versões recentes do Windows	28
Windows 95	28
Windows 98	28
Windows XP	28
Windows Vista	29
Windows 7	29
Windows 8	30
Windows 10	30
Windows 11	31
Conhecendo o Linux	31
O Sistema Operacional Linux	31
Interface do Linux	31
Características do Linux	32
Distribuições do Linux	33
Debian	33
Fedora	33
Ubuntu	34
Mageia	34
Red Hat Enterprise Linux (Chapéu Vermelho)	35
Hackers e crackers	36
O que é um <i>hacker</i>	36
Tipos de hackers e crackers	37
White hat	37
Gray hat	38

Black hat ou craker	38
Phreaker	39
Diferença entre hacker e cracker	39
Métodos de testes de segurança e de invasão	40
XSSPLOIT/CROSS-SITE SCRIPTING	41
SQLMAP/SQL INJECTION	41
METASPLOIT	42
W3AF	43
Falha de Segurança Wordpress STORED XSS	43
Manageengine Supportcenter Plus V. 7.9	44
Princípios de segurança e tipos de vulnerabilidade	45
O que são vírus	45
Tipos de vírus	46
Vírus de boot	46
Worms (Vermes)	47
Time bomb (bomba-relógio):	47
Trojans (Cavalos de Troia)	47
Hijackers (sequestradores)	48
Vírus de macro	48
Estado de zoombie	50
Facilitadores para os vírus	50
Usar um sistema antigo e não o atualizar corretamer	nte50
Abrir e-mails e fazer downloads de	remetentes
desconhecidos	50
Não utilizar cópias de segurança	51
Os vírus mais conhecidos na história	51
Chernobyl	51
Melissa	52
I Love You	52
Cabir	53

# UNIDADE



# INTRODUÇÃO

Nesta unidade, vamos estudar o computador e sua conexão com a segurança da informação. No início veremos os componentes básicos do computador, seguiremos com os conceitos de segurança da informação e seus princípios, e ainda as definições básicas de *hackers* e *crackers*, explorando também a vulnerabilidade dos sistemas, para que, por fim, possamos compreender como se defender dos vírus e como evitar que eles infectem o computador. Entendeu? Ao longo desta unidade letiva você vai mergulhar neste universo!

# **OBJETIVOS**

Olá, seja muito bem-vindo à **Unidade 1 - Hackers, crackers e os sistemas computacionais**. Até o término desta etapa de estudos nosso objetivo é auxiliar você no desenvolvimento das seguintes competências profissionais:

- Identificar as unidades que compõem o funcionamento de um computador, bem como o processo de conexão desses componentes com a máquina; distinguir os princípios do funcionamento desses dispositivos; e entender qual seu principal papel dentro desse processo.
- 2. Entender a definição, a finalidade e os principais conceitos em relação aos sistemas operacionais Linux e Windows.
- 3. Compreender os princípios básicos da Segurança da Informação e entender como estes são adotados pelos profissionais que atuam na área; e observar os tipos de vulnerabilidades dos dispositivos e sistemas.
- 4. Identificar as diversas nuances dos hackers e dos crackers, para que, por meio dessa compreensão, possa ser efetuada uma melhor segurança contra crackers e um melhor teste de segurança pelos hackers éticos.

Então? Preparado para adquirir conhecimento sobre um assunto fascinante e inovador como esse? Vamos lá!

# Unidades básicas de um computador



#### **OBJETIVO:**

Ao término deste capítulo, você será capaz de identificar as unidades que compõem o funcionamento de um computador e o processo de conexão desses mesmos componentes com a máquina. Você saberá distinguir os princípios do funcionamento desses dispositivos, e qual seu principal papel dentro deste processo. Terá também uma visão geral das novidades em relação à tecnologia e quanto ao uso dos computadores. E então? Motivado para desenvolver esta competência? Então vamos lá. Avante!

# A máquina, o sistema e a segurança

Os sistemas operacionais requerem um conhecimento muito mais aprofundado sobre os periféricos e equipamentos. Afinal, esses equipamentos e dispositivos são os verdadeiros alvos das funcionalidades básicas de um sistema operacional, independente do seu fabricante ou montador. Ao longo deste encontro, estudaremos alguns conceitos e conheceremos os principais dispositivos que se conectam a computadores de um modo geral. Ao estudá-los, conheceremos as métricas de unidades computacionais, que serão bastante úteis na rotina da administração de sistemas operacionais, como a capacidade de armazenamento em memória, velocidade de transmissão, entre outros indicadores extremamente importantes para este entendimento.

Antes de iniciarmos os nossos estudos sobre a segurança da informação especificamente, vamos conhecer mais sobre o computador em si, analisando os principais componentes.

# O Computador

O que é um computador? O computador pode ser definido como um conjunto de peças que trabalham se comunicando umas com as outras criando a capacidade de realizar múltiplas tarefas e obedecer a vários comandos para o processamento de dados.



Figura 1 - Segurança da Informação

Fonte: Freepik.

O computador pode processar inúmeros cálculos matemáticos, armazenar muitas informações e realizar diversas operações, tudo em grande escala. Hoje o mundo não pode mais existir sem a presença dessas incríveis máquinas.

# Dispositivos de entrada e saída de dados

Os dispositivos de entrada e saída funcionam como a porta comunicadora do computador, entre eles temos:

- Dispositivos de entrada e de saída de dados são as peças de hardware que utilizamos de duas formas, tanto para a comunicação com o computador, como também, o meio de comunicação do computador conosco. Por exemplo: tela de touched screen, pen drives, o roteador de acesso à Internet e outros.
- Dispositivos de saída de dados (Output) são as peças de hardware que o computador usa para a comunicação com o usuário. Por exemplo: fones de ouvido, tela de computador e qualquer outra forma de saída de informações.

 Dispositivos de entrada de dados (Input) – são as peças de hardware utilizadas para a comunicação do usuário com o computador. Por exemplo: o mouse, o teclado, a caneta ótica, e qualquer outra forma de entrada de informações.



#### NOTA:

Na segurança da informação é preciso ter muita atenção com o que é conectado ao computador, pois os dispositivos de entrada e saída de dados podem ser responsáveis por grandes infecções de vírus e ataques de *crackers*, como veremos nas aulas seguintes.

#### **Teclado**

O teclado é um dos componentes que conhecemos e usamos muito. Ele é um "dispositivo de entrada de dados" para o computador, usado para inserir textos, informações, teclas de atalho, teclas de função, macros, letras e números.



Figura 2 - Teclado

Fonte: Freepik.

#### Monitor

O monitor de vídeo é um dos principais, se não for o principal, "dispositivo de saída de dados", que o computador usa para se comunicar com você, exibindo na tela por meio de uma interface gráfica tudo aquilo que você faz, pelo mouse, pelo teclado ou na "tela de toque". A tela do monitor de vídeo pode ser de *CRT* (tubo catódico), *LCD* (cristal), de *LED* (luz), ou de "plasma".



Figura 3 - Monitor

Fonte: Freepik.

Os primeiros modelos de monitor eram em CRT, hoje em dia eles não são mais utilizados, já que a tecnologia evoluiu a ponto deles se tornarem ultrapassados.

# Mouse

O *mouse*, um dos principais dispositivos de entrada do computador, é o dispositivo apontador, usado para mover o cursor na tela do computador. Foi criado em 1968, pela empresa americana Xerox, e comercializado em 1980, pela empresa americana Apple.



Figura 4 - Mouse

Fonte: Freepik.

Em inglês, "mouse" significa "rato". Você acha semelhante a um ratinho?

#### Roteador Wi-Fi

O roteador é um dispositivo de entrada e de saída de dados, usando como ponto de acesso à Internet, ou para uma rede de computadores. O roteador é o dispositivo que possibilita a escolha da melhor "rota" para enviar as mensagens na rede, ou seja, o melhor caminho para acessar, enviar e navegar.

# Interfaces "Él"

As interfaces são as portas, físicas ou lógicas, que fazem a ligação, conexão, entre os muitos dispositivos que formam o computador, sendo responsáveis pela comunicação entre esses dispositivos. Você já observou a parte de trás do seu computador? Percebeu as entradas e as portas de conexão? São justamente elas. Além disso, temos alguns outros exemplos de conexão e de interfaces para a comunicação, tais como:

- Interface gráfica é a área de trabalho "gráfica" do computador, usada pelo usuário, com o uso de programas e serviços.
- Interface de rede pode ser um *hardware* ou um *software* que serve para conectar os dispositivos à rede, e para oferecer serviços.
- Interface do usuário é a área de trabalho do usuário no computador, como o mouse, o teclado, os ícones de atalhos etc.

Das interfaces do tipo él, temos alguns exemplos que são mais conhecidos do grande público e se destacam pelo seu uso e pela praticidade que oferecem.

#### Pen drive

O *pen drive* é um exemplo de dispositivo de entrada e saída de dados, que usa uma conexão com o computador de entrada USB, entrada universal e serve a todo dispositivo que usa essa conexão. Todo mundo tem ou usou um "*pen drive*" para copiar arquivos, fotos, músicas etc.



Figura 5 – Pen drive

Fonte: Freepik.



#### REFLITA:

Você usaria um *pen drive* que achou no chão de seu prédio só por curiosidade? Se sim, você acha que é seguro trazer um dispositivo desconhecido para ligar-se diretamente com o seu computador?

#### USB

Universal Él Bus (USB) é a conexão de porta única que usa a mesma entrada para vários dispositivos diferentes, como mouse sem fio, teclado sem fio, *smartphones*, caixas de som, entre outros. A proposta da conexão USB é unificar e acabar com muitas outras portas que existiam antes do seu surgimento, uma para cada dispositivo, atrapalhando a rotina dos usuários.

# Bluetooth (tecnologia)

O *Bluetooth* é a tecnologia de comunicação sem fio que conecta dispositivos para a transmissão de dados, como smartphones, notebooks, impressoras e câmeras digitais. O "*Bluetooth*" não é exatamente uma porta do tipo "él", mas uma tecnologia de conexão em rede sem fio, que atua de forma prática e rápida.

## Portas paralelas

As portas paralelas são as interfaces de conexão entre o computador e certos dispositivos mais específicos, como as impressoras, os *scanners*, algumas câmeras de vídeo, entre outros.

#### Os barramentos

Quando você liga uma impressora, a energia elétrica passa do botão para os dispositivos através dos fios. Dentro de um computador, os barramentos são justamente essa ligação (condutores elétricos), que ligam os dispositivos ao sistema do computador. Os barramentos têm a função de transportar sinais elétricos dos dispositivos para o computador e outros periféricos.

Existem vários tipos de barramentos que se diferem pela forma de conexão entre dispositivos, como barramento do processador, barramento de cache, barramento de memória, de entrada e de saída, e os barramentos de dados.

A taxa de transferência é a velocidade de transmissão dos dados entre os dispositivos com o computador.

# Disco Rígido - HD

O disco rígido, ou o HD que é a sigla de "hard disk", é a parte do computador que armazena, boa parte, e em alguns casos todas as informações do computador. Os dados armazenados no HD são medidos em *Gigabytes* ou em *Terabytes*.





Fonte: Freepik.

Temos também, no mercado, o HD externo, equipamento que serve para guardar os arquivos de dados da mesma forma que um HD comum, só que como o próprio nome já diz, ele não fica na parte interna de um computador.

# Memória do computador

Você tem uma boa memória? E o que você faz para lembrar de alguma coisa que esqueceu? A memória do computador guarda dados de uma forma temporária ou permanente, e permite que você recupere essas informações quando precisar. A memória do computador é dividida em dois tipos, conforme a seguir:

- Memória não volátil: é aquela que guarda os dados, mesmo quando computador estiver desligado, como a memória FLASH, a memória do pen drive, e a memória ROM (Read Only Memory), que é a memória só de leitura, para guardar instruções de funcionamento do sistema.
- Memória volátil: é aquela que existe quando o computador estiver ligado, como a memória RAM (Random Access Memory), que é uma memória dinâmica, de acesso aleatório. O bom exemplo para o uso da memória RAM são os "pentes de memória", medidos em Megabytes.



#### NOTA:

Boa parte dos vírus se instalam na memória não volátil e, por isso, permanecem mesmo quando o computador é desligado, não sabe o que é vírus ainda? Leia o capítulo 4.

# Unidade Central de Processamento (CPU)

A Central Processing Unit (CPU) é o cérebro do computador, a parte que executa todas as funções de instrução do sistema, como os cálculos e os comandos, a entrada e a saída de dados, além de toda a programação de execução. O processador é, portanto, o motor do computador, que realiza várias funções. Além disso, ele é responsável por manter todo o sistema, do computador. Ele é medido em *Hertz* (Hz), pela frequência do relógio do sistema, o "Clock".

A CPU é dividida entre os seguintes componentes:

Unidade de Gerenciamento de Memória (MMU): a MMU divide o uso da memória principal do computador entre seus programas em execução.

- Unidade de Controle (UC): a UC controla as ações feitas no computador e de todos os componentes que formam o computador.
- Unidade Lógica e Aritmética (ULA): a ULA executa as instruções lógicas de todos os programas em execução, no sistema.
- Registradores: São memórias rápidas que guardam os comandos usados no processo de cada instrução, como o apontador, o registrador e a pilha.
- Os principais fabricantes de processadores no mundo são dois especificamente: a empresa americana Intel, com os modelos "Core i3", "Core i5", "Core i7 e a empresa americana AMD. E eles são em 32, e em 64 bits.



#### RESUMINDO:

Neste capítulo, você pôde compreender sobre o computador, seu sistema e sua segurança. Assim, você conheceu todos os componentes de entrada e de saída do computador, como o teclado, o mouse, o pen drive, o HD, entre tantos outros, podendo compreender para que serve cada um desses elementos e a sua importância. Vimos também que o computador possui memória, sendo ela dividida em dois tipos de processamento, que contém diferentes componentes. Deste modo, podemos compreender a importância de cada um dos itens existentes.

# Tipos de sistemas operacionais



#### OBJETIVO:

Ao término deste capítulo, você será capaz de compreender a definição, finalidade e os principais conceitos em relação aos sistemas operacionais, Linux e Windows. E então? Motivado para desenvolver esta competência? Então vamos lá. Avante!

# O que é um Sistema operacional?

O sistema operacional (SO) é o ponto de partida para todo e qualquer profissional de *help-desk* ou suporte à segurança da informação, já que, para assegurá-la é preciso conhecer o sistema que está operando, conhecendo bem seus principais pontos fracos e fortes. Veremos, ao longo desse encontro as definições dos principais sistemas operacionais, bem como suas funções básicas, e como elas devem ser usadas.



#### **DEFINIÇÃO**:

O sistema operacional – "operating system" (O.S.) – é um programa especial que comanda todas as tarefas e todos os recursos que um computador é capaz de fazer e usar.

O sistema operacional funciona como uma "ponte" entre o *Hardware* e o *Software* do computador, realizando as atividades para que o computador responda corretamente às demandas que o usuário requisita.

# O que um sistema operacional é capaz de fazer?

O SO cuida, de maneira geral, do funcionamento das operações, dos comandos que são executados em um computador e como essas informações se comunicam entre si.

Vamos observar, a seguir, as principais funções desenvolvidas pelos sistemas operacionais de maneira geral:

## Gerenciamento dos processos

Trata-se do comando das ações que serão executadas, e do tempo necessário para que elas sejam realizadas, na ordem de sequência em que elas tiveram o seu pedido de comando. Esses comandos podem ser alternados na "fila", dependendo da necessidade.

#### Gerenciamento da memória

São "permissões" para que cada instrução de comando, ou programa em uso, possa usar o seu espaço de memória reservado para a sua execução. Ou seja, é a organização, em tempo real, do espaço de memória necessário para se realizar os comandos do sistema e se armazenar os dados temporários que ficam armazenados na memória real do computador (também conhecido por RAM - Random Access Memory ou memória de acesso aleatório.).

#### Gerenciamento dos recursos

Trata-se dos comandos que permitem o uso correto dos recursos dos dispositivos de *hardware* e os programas que estão instalados no computador, determinando a ordem de execução dos comandos. Por exemplo: monitor de vídeo, mouse, teclado, entradas/saídas USB, HD (*hard-disk*) etc. Como vimos na aula anterior, esses componentes são fundamentais para a integração do usuário com a máquina e o gerenciamento de recursos, sendo assim, tais componentes são essenciais para que o computador responda adequadamente às necessidades e demandas do usuário.

#### Gerenciamento de entrada e de saída de dados

São as ações de controle e de gerenciamento dos dispositivos que estão conectados com o computador, possibilitando ao usuário que ele possa mexer na configuração destes dispositivos. O sistema operacional abre e fecha portas de acesso a esses dispositivos de acordo com as requisições dos programas que estão sendo executados. Por exemplo: quando você aciona o comando "Imprimir" no MS-*Word* ou em seu navegador, você está requisitando o acesso de seus dados a um dispositivo denominado "impressora".

# Gerenciamento do sistema de arquivos

Trata-se das ações que permitem salvar e armazenar os arquivos diretamente no disco rígido, ou em outro disco de armazenamento, e que podem ler estes arquivos, organizá-los e recuperá-los depois, dependendo da necessidade do usuário.

# Como um sistema operacional funciona?

Em termos de estrutura e de funcionamento, os sistemas operacionais podem processar e administrar grandes quantidades de informações, tudo ao mesmo tempo, utilizando todos os recursos disponíveis no computador. Nesse contexto, os sistemas operacionais podem ser classificados quanto à sua forma de executar tarefas, podendo ser:

 Monotarefa – também conhecidos como "monotask". Trata-se de um sistema operacional que só pode fazer uma única instrução de tarefa por vez, obedecendo a um só comando até poder começar outro, como o MS-DOS e o BIOS.



#### SAIBA MAIS:

MS-DOS foi o primeiro sistema operacional da Microsoft, lançado no final da década de 1970 para microcomputadores pessoais da IBM. A sigla DOS significa *Disk Operational System* ou sistema operacional de discos.

BIOS (Basic Input/Output System ou Sistema Básico de Entrada e Saída), é o sistema operacional nativo dos computadores, ainda mais básico que o sistema operacional propriamente dito (como o Windows ou Linux), e funciona para coordenar o acesso dos dados às suas portas de entrada e de saída.

Multitarefa – chamados também de sistemas operacionais multitask, eles podem executar mais de uma instrução de comando por vez, por um tempo específico, ou seja, podem aceitar "concorrência" entre tarefas. Mas, caso aconteça algum erro de comando, todo o sistema pode "travar". As primeiras versões do Windows (3.0, 3.1 e 95) podem ser considerados sistemas operacionais multitarefas.

- Multitarefa preemptivo trata-se de um sistema operacional que pode executar vários comandos ao mesmo tempo, controlando o processo e escolhendo qual será o comando a ser executado inicialmente. Neste caso, se ocorrer algum erro, o sistema não para, como era o caso das primeiras versões do Windows.
- Multiprocessador são SO que conseguem gerenciar máquinas com mais de um processador simultâneo. Eles distribuem as suas muitas instruções de tarefas entre dois ou mais processadores, disponíveis na mesma máquina. Esses processadores podem estar fortemente ou fracamente acoplados. As versões mais recentes do Windows, MacOS e Linux conseguem gerenciar multiprocessamentos.

# A Estrutura de um sistema operacional

E quando você observa uma casa em construção? Você sabe qual é a sua "base", e a sua estrutura de construção? (Uma casa simples, uma casa de 1º andar). Da mesma forma, os sistemas operacionais, que são as bases de todo o sistema computacional, podem ser capazes de realizar pequenas ou grandes tarefas, depende de como seja a sua arquitetura.

Andrew Stuart Tanenbaum é um dos mais proeminentes bacharéis em computação dos EUA, com diversos livros publicados na área. Para Tanenbaum, um sistema operacional pode ser classificado, quanto à sua estrutura (ou arquitetura), da seguinte forma:

- Monolítico quando o núcleo do sistema operacional é um "único" processo que está sendo executado na memória "protegida", realizando as tarefas.
- Micronúcleo modelo tipo Cliente-Servidor, no qual o núcleo do sistema é formado por funções mínimas, chamadas de "serviços" (comunicação e gerência de processos), e de "clientes" (aplicações ou programas).

# Distribuição e licenças dos sistemas operacionais

Alguns sistemas operacionais têm o seu tempo de utilização determinado pelos termos de uma "licença de uso de software". Esta licença estabelece a forma de como você pode usar o seu sistema operacional, entre totalmente gratuito, com o seu código "aberto" ou 100% proprietário. Vejamos então como cada modalidade de licença funciona:

## Sistema operacional fechado

Trata-se daquele sistema operacional totalmente pago e licenciado, com todos os direitos reservados para o fabricante. O Windows e o MAC-OS são os maiores representantes deste tipo de sistema. Uma vez licenciado para um usuário, este poderá utilizar o sistema operacional por um determinado tempo, ou sob algumas certas condições de limitação de uso.

## Sistema operacional aberto

Trata-se daquele sistema operacional que possui seu código-fonte totalmente aberto, o exemplo mais difundido deste tipo de sistema é o LINUX, ele permite que qualquer analista de linguagem (programador) possa mexer em sua estrutura.

#### Sistema operacional freeware

Trata-se daquele sistema operacional que possui sua distribuição de forma totalmente gratuita, com sua total disponibilidade entre os seus usuários. Exemplos: *OpenSolaris* da *Sun Microsystem*;



#### NOTA:

Normalmente, todos os sistemas operacionais do tipo "open source" também são gratuitos (freeware). Porém, nem todos os sistemas gratuitos são open source, pois não disponibilizam o código fonte para o usuário alterar, por exemplo o OpenSolaris.

# Conhecendo o Windows

O sistema operacional mais conhecido e comercializado do mundo é, sem sombra de dúvidas, o Microsoft Windows. Atualmente, ele detém cerca de 90% do mercado mundial de *softwares*, e chegou à sua versão 11 em 2021. O Windows, como visto previamente, é um sistema fechado e pago, mas apesar do custo, quando o assunto é o usuário comum ele ainda ganha em número de utilização do Linux, já na esfera empresarial, pela facilidade do Linux os dois começaram a concorrer de igual para igual.



#### NOTA:

Por ser um sistema de código fechado, o qual o usuário não consegue observar a fundo o que acontece na máquina, a maioria dos vírus são desenhados para esse sistema, e muitas vezes os vírus aproveitam as falhas que já existem neles. Esse é um fator que deve ser levado em consideração na hora de escolher o sistema.

# Sistema Operacional Windows

Desenvolvido em por volta de 1980 por Bill Gates, o Sistema Operacional Windows, como o nome já denota, é um gerenciador de tarefas que faz a "janela" do computador com o usuário.

O Microsoft Windows é um sistema operacional para computadores pessoais, portáteis (laptops), tablets e smartphones com a interface completamente adaptável aos dispositivos sensíveis ao toque (touch screen).



#### ACESSE:

Quer saber ainda mais sobre o SO? Conheça a página oficial do Windows, lá contém informações valiosas sobre o sistema. Para acessar, <u>clique aqui</u>.

#### As Versões recentes do Windows

Vamos observar a seguir as versões do Windows, vendo suas principais funções, prós e contras.

#### Windows 95

O Windows 95 foi lançado em 24 de agosto de 1995. Ele foi o primeiro S.O. da família a ser "totalmente" gráfico. Em termos práticos, com o sistema de arquivos FAT-16, que foi uma revolução para a época, passou a ser possível criar arquivos com nomes extensos, com até 255 caracteres e mais 3 caracteres para sua extensão. Até as versões anteriores do *Windows*, os arquivos só poderiam ter nomes com até 8 caracteres mais 3 de extensão.

Em algumas versões de atualização lançadas logo após o Windows 95, foi implementado o suporte para arquivos FAT-32, possibilitando o surgimento das entradas USB e Ultra DMA.

#### Windows 98

O Windows 98 foi lançando em 25 de junho de 1998. Ele adicionou definitivamente o sistema de arquivos FAT-32, e melhorou a sua implementação com a Web.

O navegador Internet *Explorer* passou a ser um programa nativo do sistema operacional, o que gerou muita insatisfação no mercado mundial de *software*, culminando no desaparecimento de empresas de Internet como o Netscape.

#### Windows XP

O Windows XP, de *eXPerience*, foi lançado em 25 de outubro de 2001, e foi uma revolução total, pois ele vinha com arquitetura de 64 *bits*, além de vários recursos gráficos, novos ícones e uma melhor profundidade de cor. O Windows XP foi seguramente a versão mais estável e bem aceita comparada às anteriores até então, uma vez que a Microsoft era severamente criticada pelos sucessivos "bugs" de suas versões anteriores.

O Windows XP implementou alguns conceitos importantes, como os botões de acionamento dos programas em execução, e a identificação do usuário logado no menu "Iniciar". Por meio da barra de tarefas, que pode ser vista no canto inferior da tela, é possível alternar com extrema facilidade entre os programas em execução no sistema operacional. O Windows XP representou um grande marco na aderência do sistema operacional com os recursos de utilização de serviços em rede, com muitos dos recursos de segurança de dados oferecidos pelo sistema operacional Windows Server (a versão do Windows para servidores de rede).

#### Windows Vista

O Windows Vista foi lançado em 22 de julho de 2005. Ele vinha com a nova interface gráfica do usuário, chama *Windows Aero*, que permitia o *flip* em 3D seguro para a troca entre as janelas, efeitos de transparência, e com um melhor desempenho para o computador.

Apesar de muitas inovações em sua interface, com efeitos 3D e tudo mais, o Windows Vista não foi considerada uma versão exitosa por parte da Microsoft. A altíssima exigência de memória e processamento fez com que poucos usuários ousassem em abandonar o bom e velho *Windows* XP para se aventurar naquela ainda desconhecida versão.

#### Windows 7

Depois do fracasso do Windows Vista, a Microsoft rapidamente lançou o Windows 7, em 22 de julho de 2009. Ele se configurava em um sistema operacional mais prático de ser usado, mais limpo (*clean*) e bem mais eficiente. Muitos o consideram o melhor sistema operacional já lançado pela Microsoft, e ainda hoje ele é bastante utilizado.

O Windows 7 definitivamente uniu o que havia de melhor no Windows XP em termos de estabilidade e usabilidade com o melhor da performance das versões do Windows para servidores de rede. Juntamente com esta versão, a Microsoft lançou algumas variações do sistema, como a versão "Home" para usuários domésticos e "Professional" para empresas e usuários mais experientes.

A integração com a Internet foi outro ponto forte do Windows 7, que guardava todas as configurações e programas instalados pelo usuário na Web, de modo que, ao logar em outro computador, o usuário poderia contar com todas as customizações que havia feito em seu computador original.

#### Windows 8

O Windows 8 foi lançado em 26 de outubro de 2012, e trouxe uma série de inovações, como a interface gráfica "Metro", e seu tempo de inicialização que era muito rápido (Boot), em torno de 2 segundos. Ele vinha junto com o Internet Explorer 10, e com reconhecimento por voz.

O Windows 8 foi desenvolvido para ser totalmente compatível com os dispositivos móveis, como *tablets* e os *smartphones* (Windows Phone). Por isto ele inovou radicalmente sua interface gráfica, implementando o conceito de "Aplicativos", inteiramente compatível com os aplicativos desenvolvidos para o Windows Phone. Os ícones sensíveis ao toque dos dedos foram implementados em substituição ao menu "Iniciar", fato bastante criticado pelos usuários, que exigiram a volta daquele menu, o que só veio acontecer na versão Windows 8.1, uma versão de atualização rapidamente lançada.

#### Windows 10

O Windows 10 foi lançando no dia 29 de julho de 2015, com novos recursos de interfaces gráficas, como a "Live Tiles" (telas para serem postas ao lado do Menu Iniciar), introdução do navegador Microsoft Edge, e com aplicativos renovados para fotos, vídeos e músicas (*Groove*), além da implementação com a Loja da *Microsoft*, e a integração com o Xbox Live.

Com o Windows 10, veio o anúncio da descontinuidade do sistema operacional Windows Phone, fato que não desmerece a consolidação do Windows 10 como sendo o principal sistema operacional para usuários desktop do mundo.

#### Windows 11

O Windows 11 foi lançado em 5 de outubro de 2021, vindo com um visual mais minimalista e limpo, havendo alteração nos seus ícones, nas suas janelas e apresentando uma nova iconografia, ainda, trouxe o seu menu iniciar centralizado. É a forma mais atualizada de Windows no mercado.

## Conhecendo o Linux

# O Sistema Operacional Linux

O Linux foi criado para o uso e a implementação de *softwares* livres e gratuitos, com desenvolvimento feito por programadores e empresas de todo o mundo.



#### **DEFINIÇÃO**:

O sistema operacional Linux é um *software* de distribuição plenamente livre, (gratuito) e que possui seu código-fonte totalmente "aberto".

Isso quer dizer que, se você é um programador de linguagem de software (linguagem de programação), poderá modificar toda a estrutura técnica daquele sistema operacional, alterando toda a sua funcionalidade, e ainda personalizar todo o sistema a seu critério. Tudo isso sem pagar nada ou pedir licença a quem quer que seja.

# Interface do Linux

Ao contrário do MAC-IOS e do Windows, o Linux não é considerado um sistema 100% com interface gráfica, visto que seu código é aberto, em muitas funções o usuário deve recorrer ao código para realizar.

Originalmente, a interface do Linux é textual, ou seja, com base em comandos de texto, no entanto esta característica do Linux não era interessante para muitos usuários domésticos, e dificultava até mesmo a vida de quem desejava utilizá-los para fins profissionais, como as empresas e profissionais de informática.

Pensando nisto, empresas e organizações de todo o mundo começaram, no final da década de 1990, a construírem interfaces gráficas para o Linux, tentando torná-lo mais amigável e intuitivo. Os programas de interface gráfica desenvolvidos por essas empresas e profissionais começavam a ganhar corpo no início do século 21. Com a popularidade dessas interfaces crescendo cada vez mais, as mais conhecidas se transformaram em distribuições.



#### ACESSE:

Quer saber ainda mais sobre o Linux e suas funções? Conheça o *site* dessa comunidade que é voltada para ele. Para acessar, <u>clique aqui</u>.

# Características do Linux

O sistema operacional Linux, basicamente, possui um único núcleo, sendo assim um sistema do tipo monolítico, nele são executadas todas as funções, como gerenciamento de memória, operações de entrada e de saída de dados, além do acesso aos arquivos.

A arquitetura monolítica do Linux, associado a outros fatores não técnicos, dificultam o aparecimento de vírus de computador, ou seja, dificilmente uma máquina rodando Linux como sistema operacional será infectada por um vírus de computador.

E para os profissionais que irão lidar com a segurança, esse é um ponto que deve ser levado em consideração quando for escolher o Sistema Operacional a ser adotado. Em síntese, as seguintes características se constituem como diferenciais a favor do Linux:

- **Estabilidade** dificilmente trava ou apresenta variações no desempenho de suas aplicações.
- **Segurança** baixa incidência de vírus de computador.
- Alto desempenho do hardware como o Linux não exige muita memória, ele consegue gerenciar bem os recursos de máquinas com baixa configuração.

# Distribuições do Linux

Como vimos previamente, o código do Linux é livre, ele pode ser alterado por qualquer pessoa que possua domínio de programação, por isso existem tantas distribuições dele.

O Linux faz parte do projeto GNU - "General Public License" (GPL), para qual há um grupo de empresas e de colaboradores que desenvolvem e distribuem uma coleção de softwares "livres", para a sua implementação. Entre essas distribuições, podemos destacar as seguintes:

#### Debian

A distribuição *Debian* é uma das mais antigas e populares do Linux, desde 1993. Tem uma estrutura muito estável e é bastante seguro, sendo ideal para a instalação e configuração de servidores próprios a ambientes de rede.



#### ACESSE:

Para conhecer mais sobre esse sistema e fazer o download, clique aqui.

#### Fedora

A distribuição Fedora é uma das mais populares e estáveis do Linux. Criado pela *Red Hat* (Chapéu Vermelho), outra distribuição que é uma das mais conhecidas e admiradas do Linux, o projeto *Fedora* é bastante robusto e muito estável, além de possuir uma série de recursos gráficos.



#### ACESSE:

Para conhecer e fazer download do Fedora, clique aqui.

# **OpenSUSE**

É uma distribuição bastante completa e intuitiva, e veio para democratizar o uso do Linux por aqueles que não têm conhecimento de programação.

Adistribuição OpenSUSE é um projeto feito pelo grupo Novell, e possui a ferramenta YaST (*Yeah Another Setup Tool*), na qual temos todo o processo de instalação e configuração do sistema.



#### ACESSE:

As principais informações sobre o sistema estão dispostas no *site*. Para acessar, clique aqui.

#### Ubuntu

Sendo hoje uma das mais populares distribuições do sistema Linux, a distribuição Ubuntu foi feita originalmente em cima da distribuição Debian, lançado em 2004, pelo empresário sul-africano Mark Shuttleworth. Entre todas as distribuições disponíveis no mercado mundial, esta é a que mais se assemelha à interface gráfica do Windows, o que facilita ainda mais o contato do usuário com o sistema.



#### ACESSE:

Para conhecer e fazer download do sistema, clique aqui.

# Mageia

A distribuição Mageia é uma das mais novas distribuições do Linux. Lançada em 2010, de origem francesa, foi implementada por cima de outra distribuição do Linux: a Mandriva. Ela é bem estável, e vem sendo muito utilizada.



#### ACESSE:

Para conhecer e fazer download do sistema, clique aqui.

# Red Hat Enterprise Linux (Chapéu Vermelho)

Essa distribuição é, particularmente, a preferida dos usuários programadores, ou profissionais que trabalham com a segurança. A distribuição *Red Hat* (Chapéu Vermelho) é uma das mais conhecidas e uma das mais populares, do Linux. Ele é bastante robusto e bem intuitivo de usar. Notório por sua qualidade e confiabilidade, conquistou um grande público.



#### ACESSE:

Quer conhecer mais sobre essa distribuição? Acesse aqui.



#### RESUMINDO:

E então? Gostou do que mostramos? Aprendeu mesmo tudinho? Agora, só para termos certeza de que você realmente entendeu o tema de estudo deste capítulo, vamos resumir tudo o que vimos. Nesta aula podemos compreender melhor a definição, finalidade e os principais conceitos em relação aos sistemas operacionais, Linux e Windows.

# Hackers e crackers



#### **OBJETIVO:**

Ao término deste capítulo, você será capaz de entender as diversas nuances dos *hackers* e *crackers*, para que por meio desta compreensão possa ser efetuada uma melhor segurança contra *crackers* e um melhor teste de segurança pelos *hackers* éticos. E então? Motivado para desenvolver esta competência? Então vamos lá. Avante!

# O que é um hacker

Descobrindo novas funcionalidades do sistema ou até mesmo atualizando e adaptando as antigas, os hackers trabalham com a criação de softwares e hardwares de máquinas. Eles atuam na segurança de empresas e até de indivíduos, fazendo testes nos sistemas de computadores para detectar possíveis falhas que venham afetar a segurança dos dados e informações armazenados.

Os hackers são muito importantes para que os testes de segurança ocorram de maneira realmente útil e as falhas sejam descobertas, já que é por meio de seus conhecimentos em informática e até no próprio sistema da empresa que os problemas são detectados e reparados.



Figura 7 - Hacker

Fonte: Freepik.



#### EXPLICANDO MELHOR

Imagine que você é o síndico de seu prédio, e compra um novo gerador, para que caso falte energia os elevadores não parem de funcionar. Para testar esse gerador você precisa desligar a energia do prédio, e caso ela seja reestabelecida é porque o gerador está funcionando. O trabalho do *hacker* é parecido com o teste do gerador, já que, quando um sistema de segurança é ligado, o *hacker* vai tentar "desligá-lo", por meio de invasões controladas. O *hacker* atua somente nesse sistema que foi protegido.

## Tipos de hackers e crackers

#### White hat

Conhecido como hacker ético, esse hacker utiliza o seu conhecimento em informática para testar a segurança dos sistemas. Ele realiza o escaneamento de sistemas, no qual identifica erros e os soluciona ou passa a informação para o responsável do sistema, para que ele efetue o reparo na segurança. Em regra, esses hackers trabalham violando e invadindo apenas os sistemas para os quais foram chamados, a fim de verificar a segurança destes. Eles se preocupam, além de invadir, com a parte de conhecimento de programação, ao contrário dos crackers, que de maneira maliciosa se preocupam apenas com a invasão do sistema.

Na maioria das vezes, o mercado de trabalho reconhece o *hacker* ético com base em seus estudos acadêmicos e na contribuição dada por ele para a segurança de sistemas. Normalmente toda grande companhia de sistemas de informação, *software* e sistemas de informática, já possui uma equipe de *hackers* que trabalha testando o seu sistema.

Existe, ainda, o mercado para hackers autômatos, que podem descobrir falhas em sistemas e ao reportarem as falhas ganham um determinado valor. Normalmente grandes sites já possuem uma tabela de gratificações montadas para esses profissionais, que ao descobrirem as falhas enviam imediatamente um feedback para as empresas que administram o site.



#### VOCÊ SABIA?

Em 2012, um brasileiro chamado Reginaldo Silva descobriu uma falha na rede social Facebook e, ao informar ao *site*, foi recompensado com o valor de R\$ 79.000,00 pela falha encontrada. Ele se denomina "*Hacker* do bem", e já descobriu diversas outras falhas em grandes *sites* e plataformas como Google, Yahoo, Instagram e outros.

## Gray hat

Entre os hackers éticos e os crackers, os gray hat normalmente tem intenções boas, de um hacker ético, mas por vezes utilizam de métodos pouco convencionais ou não éticos para efetuar os seus ataques. Além disso, eles podem também ter outras intenções para testar a segurança e por vezes seguem um código ético diferente do adotado pelos demais. Para eles, dependendo do ataque realizado e para quem foi direcionado, se eles não roubarem, vandalizarem ou mexerem severamente com a vida social de outras pessoas, o seu comportamento é escusável.

Apesar de, a maioria das vezes, possuírem uma boa intenção, as ações realizadas pelos *hackers* de "Chapéu Cinza" são moralmente questionáveis, por vezes eles são considerados *crackers*, já que suas ações podem ir de encontro ao que o administrador do *site* deseja.

### Black hat ou craker

Sendo conhecido também como "Pirata virtual" ou "dark-side", os crackers são agentes, que possuem um grande conhecimento em informática e sistemas, mas, ao contrário do hacker "White hat", se utilizam desse conhecimento para invadir de maneira maliciosa aparelhos de informática. Os crackers, em sua maioria, não possuem um interesse acadêmico ou social por trás de suas ações, eles são pouco voltados para a programação do sistema propriamente dita. Em regra, eles se utilizam de programas já existentes para realizar as suas ações criminosas. Normalmente eles possuem pouca experiência e baixa noção em informática.



#### **VOCÊ SABIA?**

A denominação "cracker" surgiu por volta de 1985, criada pelos próprios profissionais ou amadores hackers, para que houvesse uma distinção entre aqueles que utilizavam seu conhecimento em informática para a segurança, que era o caso dos hackers, e aqueles que utilizassem o conhecimento de maneira maliciosa a fim de prejudicar sistemas e pessoas.

#### Phreaker

O phreaker é o especialista em telefonia, podendo ser fixa ou móvel, ele trabalha na segurança das informações que essa modalidade guarda. Com o crescimento da telefonia móvel, e com o alto desenvolvimento dos aparelhos de telefonia, se torna cada vez mais necessário atentar para a segurança das informações trocadas por esse meio de comunicação.

O *phreaker* pode ser tanto um *hacker* que trabalha para uma empresa de segurança, quanto pode ser um *cracker* que queira usar as informações de maneira maliciosa.



### VOCÊ SABIA?

A primeira forma de *hackear* um aparelho fixo de telefonia foi descrita pelo "Capitão *Crush*", ele descobriu que um brinde que vinha em pacotes de salgadinho, um apito, quando apitado na frente de um tipo de orelhão permitia que se fizesse ligações de graça, já que o apito possuía a mesma frequência que o orelhão.

# Diferença entre hacker e cracker

Apesar de serem palavras similares, o *hacker* e o *cracker* são completamente diferentes quanto a sua atuação na Internet. Como visto previamente, o *hacker* atua, na maioria das vezes, no combate contra os *crackers*, que são os responsáveis pela quebra de sistemas de segurança.





Fonte: Freepik.

Os termos definem, em regra, grupos de pessoas que têm uma habilidade especial em testar sistemas de segurança, a diferença é que, uma testa para ajudar o sistema a melhorar e reparar "bugs", e o outro realiza mais que o teste, ele se infiltra no sistema buscando, de maneira maliciosa, benefício próprio.

# Métodos de testes de segurança e de invasão

Para conseguir o acesso às informações e dados de um sistema, os crackers utilizam de métodos que, muitas vezes, são os mesmos que os hackers (White hat), usam para testar a segurança do sistema. Para que a segurança do sistema seja realizada de maneira eficiente, cabe ao agente que a testa conhecer os métodos, prová-los e compreender como se proteger quando esses procedimentos são utilizados de maneira maliciosa, por esse motivo vamos ver a seguir quais são os métodos mais utilizados dos dois lados.

## XSSPLOIT/CROSS-SITE SCRIPTING

Através da vulnerabilidade de *cross-site scripting* (XSS), os *hackers* inserem a programação *client-side script*, trata-se da programação que roda automaticamente no computador do usuário, e por meio desta programação o agente responsável pelo ataque malicioso consegue injetar *scripts* que tornam as informações da máquina ou sistema atingido, vulneráveis. É através do código JavaScript que o *hacker* efetua esse ataque.

Vamos imaginar que um agente gostaria de realizar um ataque utilizando o XSS em um fórum na Internet, ele iria inserir um texto com um código JavaScript, e por meio desta programação, quando o usuário selecionasse o texto que estaria na página do fórum, por meio deste código, uma nova página seria gerada, sendo esta uma imitação de uma página de "login", e quando o usuário colocasse os dados, eles seriam passados para o *cracker*.

# SQLMAP/SQL INJECTION

Figura 9 - SQL

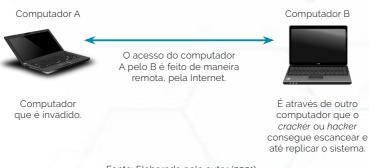
y), function(a){"use strict"; function b(b){return this.each(function()) | Interest wn-menu)"),d-b.data("target");if(d||(d-b.attr("href"),d=d&&d.replace(/.\*(?=#[^\s]\*\$)/,"")), t a"),f-a.Event("hide.bs.tab",{relatedTarget:b[0]}),g=a.Event("show.bs.tab",{relatedTarget:e[0]  $su(t) = (-1) \cdot (-1) \cdot$  $igger(\{type: shown.bs.tab^*, related Target: e[0]\})\}\}\}, c.prototype.activate=function(b,d,e){function}$ > .active").removeClass("active").end().find('[data-toggle="tab"]').attr("aria-expanded",!1) a-expanded",[0],h?(b[0].offsetWidth,b.addClass("in")):b.removeClass("fade"),b.parent(".dropde ().find('[data-toggle="tab"]').attr("aria-expanded",!0),e&&e()]var g=d.find("> .active"),h=e&& ")||!id.find(") .fade").length);g.length&&h?g.one("bsTransitionEnd",f).emulateTransitionEnd war d-a.fn.tab;a.fn.tab-b,a.fn.tab.Constructor=c,a.fn.tab.noConflict=function(){return a.fn.t thow"));a(document).on("click.bs.tab.data-api",'[data-toggle="tab"]',e).on("click.bs.tab.data we strict function b(b) {return this.each(function() {var d=a(this),e=d.data("bs.affix"),f="ob"} typeof  $bbse[b]()\}$ )var c=function(b,d){this.options=a.extend({},c.DEFAULTS,d),this.target=a",a.proxy(this.checkPosition,this)).on("click.bs.affix.data-api",a.proxy(this.checkPositionWi ull, this.pinnedOffset=null, this.checkPosition()};c.VERSION="3.3.7",c.RESET="affix affix-top State-function(a,b,c,d){var e=this.\$target.scrollTop(),f=this.\$element.offset(),g=this.\$target. m"==this.affixed)return null!=c?!(e+this.unpin<=f.top)&&"bottom":!(e+g<=a-d)&&"bottom" locke(=c)\*top::null!=d8&i+j>=a-d&&"bottom"},c.prototype.getPinnedOffset=function(){if(this Reservance of the second secon

Fonte: Pixabay.

O SQLMAP, é um erro de segurança no qual as falhas do código possibilitam aos agentes maliciosos, terem acesso a informações armazenadas, normalmente em bancos de dados. Por meio desta falha, o *cracker* insere instruções no código SQL (*Structured Query Language*, ou Linguagem de Consulta Estrutura, é a linguagem de pesquisa do sistema utilizada em bancos de dados relacionais), que irá fazer com que ele tenha acesso aos dados dispostos neste banco com base nas falsas pesquisas que inseriu. Por meio dessa falha é possível que dados sejam inseridos e retirados, tornando-os incongruentes e falsos.

## **METASPLOIT**

Criada pela desenvolvedora de *software* HD *Moore*, essa ferramenta hoje em dia é uma das mais populares para realizar o teste de segurança de sistemas. Por meio dessa ferramenta é realizado um acesso virtual ao sistema alvo, e quando esse sistema alvo é acessado, é possível que se localize inúmeras falhas e vulnerabilidades na segurança, sendo possível que esse sistema seja aberto, como o LINUX, ou mais fechado como o Windows e o MAC. No *METASLPLOIT* é possível realizar o escaneamento da máquina, bem como uma cópia perfeita de seu sistema, sendo assim uma ferramenta perigosa se utilizada por *crackers*.



Fonte: Elaborada pelo autor (2021)

### W3AF

Utilizada normalmente por *hackers White Had*, essa ferramenta cria um diagnóstico de vulnerabilidades para páginas de Internet, sendo usada para efetuar auditorias profundas, que buscam qualquer falha de segurança no sistema. Essa ferramenta funciona em qualquer plataforma que seja compatível com a linguagem de programação *Python* e pode descobrir duas falhas já citadas, a XSS e a SQL.

# Falha de Segurança Wordpress STORED XSS

Sendo um sistema de gerenciamento de conteúdo voltado para a Internet, o *WordPress* é escrito em PHP e bastante utilizado tanto por empresas quanto por usuários comuns, já que sua aplicabilidade varia desde *sites* até blogs pessoais, e por causa dessa alta aplicabilidade o buraco de segurança do *WordPress* é bastante danoso a quem o utiliza. Através desta falha na segurança, o usuário malicioso é autorizado a injetar códigos nos comentários, e por meio desses códigos o controle da página corre perigo, bem como o controle dos servidores. Algumas dicas para evitar essa falha são:

- Atente sobre a sua postura quanto a segurança do seu site ou blog.
- Ao baixar plug-ins ou temas da Internet, utilize apenas fontes de confianca e certificadas.
- O fator humano pode ser considerado a maior vulnerabilidade quanto a plataforma de WordPress, deve-se sempre atentar que por ser de livre acesso, o *site* deve ser constantemente testado para essas falhas.
- O lugar onde mantem o *site*, que é chamado de *hosting*, é fundamental para a preservação do seu *site*, por isso ele é tão importante quanto o sistema de segurança que é utilizado.
- As senhas que são utilizadas para realizar o log-in do site devem ser únicas e não obvias, por isso deve-se evitar nomes de familiares, datas festivas e qualquer outra que, conhecendo o perfil do criador, o cracker consiga desvendar.

# Manageengine Supportcenter Plus V. 7.9

Navegando por meio de *links* e controles de *software*, que é previamente passado para o *cracker*, é possível que, utilizando das fragilidades de segurança do *SupportCenter*, que é um gerenciador de contas e contatos de páginas de web, ele consiga ter acesso a todas essas informações e também aos dados de contatos das pessoas que acessam a página da *web*.



#### **RESUMINDO:**

E então? Gostou do que mostramos? Aprendeu mesmo tudinho? Agora, só para termos certeza de que você realmente entendeu o tema de estudo deste capítulo, vamos resumir tudo o que vimos. Você deve ter aprendido sobre os hackers e os crackers, assim, vimos que os hackers trabalham com a criação de softwares e hardwares de máquinas e os crackers são aqueles que usam os conhecimentos sobre os sistemas para fazer coisas inadequadas. Vimos ainda os tipos de hackers e os métodos de testes de segurança e de invasão. Assim, concluímos nosso estudo sabendo como entrar no sistema e que é possível usufruir dele tanto para o bem, quanto para o mal.

# Princípios de segurança e tipos de vulnerabilidade



#### OBJETIVO:

Ao término deste capítulo, você será capaz de conhecer mais sobre os tipos de vírus que podem vir a infectar o sistema, observando quais são as ações que podem facilitar que esses vírus infectem a máquina e tornem o sistema inseguro. E então? Motivado para desenvolver esta competência? Então vamos lá. Avante!

# O que são vírus

Vimos previamente que existem diversas maneiras de *crackers* invadirem sistemas, e uma dessas maneiras é por meio do vírus. Podemos dizer que os vírus são usados com maior frequência e possuem milhares de ramificações e códigos distintos.

O vírus de computador, de maneira geral, pode ser definido como um programa que é feito especialmente para danificar uma máquina ou causar prejuízo à máquina infectada.



Figura 10 - Vírus

Fonte: Freepik.

Os vírus, por serem mais comuns que os ataques de *hackers*, de maneira geral, são mais perigosos, visto que existem milhares deles circulando pela Internet, e basta um clique para que todo o sistema seja contaminado.



#### SAIBA MAIS:

A denominação de vírus relacionados a programas danosos de computador surgiu em 1983 com o pesquisador Fred Cohen, que em suas pesquisas chamou programas com códigos perigosos como vírus de computador.

## Tipos de vírus

Novos vírus são criados diariamente, por isso existe a necessidade de se atentar para a segurança de seu sistema, como também para o treinamento de funcionários para evitar que um *software* malicioso o infecte

### Vírus de boot

Esse vírus ataca a máquina durante o processo de inicialização do sistema, quando computador é ligado e o sistema é carregado do "HD" (disco rígido), o vírus faz com que a iniciação do sistema seja afetada, travando a máquina.

Esse tipo de vírus é considerado o primeiro de uma categoria de softwares malignos que atualmente circulam na Internet.

Existem dois métodos básicos para que esse vírus atue:

- Mudando o setor onde o boot (inicialização) do sistema está localizado no disco rígido.
- Adicionando o código do vírus a parte de arquivos executáveis, assim, quando você inicializar o código é iniciado automaticamente.

# Worms (Vermes)

Esse tipo de vírus é bastante danoso ao sistema, uma vez que ele se espalha rapidamente e em uma escala de multiplicação imensa, isso quer dizer que ele domina completamente o sistema.

Muitas vezes o computador precisa ser formatado para se livrar desse vírus, sendo possível que ocorra a perda de informações e dados.



#### VOCÊ SABIA?

Ao contrário dos vírus normais, os *worms* não infectam arquivos, mas sim exploram onde o sistema é vulnerável, não necessitando assim de uma "vítima primária", podendo infectar uma rede toda.

## Time bomb (bomba-relógio):

Chamados de "bomba-relógio" esses vírus são programados para serem ativados em um determinado horário e data. Eles são utilizados quando, por exemplo, se quer fazer um ataque em uma data festiva.

A maioria desses vírus é contraído por conta do usuário que clica ou faz o *download* de algo que o contém em sua estrutura, por isso uma das maneiras mais comuns de se espalhar esse vírus é por *e-mail*.

## Trojans (Cavalos de Troia)

Trojans são aqueles vírus que trazem dentro de si um código que permite ao invasor entrar na máquina de quem acessou ou faça download do arquivo infectado, ele transforma o computador em um "escravo", podendo assim ter acesso a todas as informações, bem como modificálas ou exclui-las direto na máquina.



#### VOCÊ SABIA?

O nome cavalo de troia surgiu em referência ao cavalo enviado pelos gregos aos troianos como, supostamente, um pedido de "paz", mas na verdade esse cavalo foi o ponto decisivo da guerra, já que os troianos estavam escondidos dentro, e o presente, na verdade era uma armadilha. O vírus tem esse nome porque, na prática, é isso que ele se propõe, o usuário acha que está utilizando uma função quando na verdade ele está sendo enganado por um código oculto.

## Hijackers (sequestradores)

Os Hijackers são os vírus de scripts; spywares que invadem a máquina e sequestram as páginas iniciais dos navegadores da Web (home-pages), instalando as barras de navegação, exibindo anúncios de janelas popup, e impedindo a sua remoção. Esses vírus, apesar de muitos serem inofensivos, podem contribuir para que outros vírus infectem a máquina, por isso é importante que alguns passos sejam tomados, são eles:

- A cautela deve ser regra geral para qualquer aplicação em sistemas:
- Quando instalar programas observe todos os passos e só clique em "concordar" ou "prosseguir" quando possuir certeza de que nenhum outro programa será instalado de maneira sorrateira.
- Se quiser instalar programas de terceiros tenha certeza da procedência antes de permitir com o login de usuário do computador.

### Virus de macro

Os vírus "macro" estão dispostos normalmente em textos ou programas de textos, inseridos de maneira maliciosa para trazer dano a quem fez o download ou visualizou. Esse vírus altera um macro (comandos básicos para executar ações que são fundamentais para o sistema executar ações comuns), além de alterar todos os programas ou documentos que foram infectados por eles.



#### SAIBA MAIS

Macros são programas escritos em uma linguagem denominada Visual Basic for Applications (VBA), executados apenas dentro dos programas do pacote MS-Office, como o Word, Excel, Power Point etc. Os macros são bastante utilizados para automatizar rotinas em processamento de documentos. É possível fazer com que um macro seja executado automaticamente quando um determinado documento é aberto no MS-Office. Aí que mora o perigo!!! Os vírus de macro se aproveitam dessa abertura para realizarem operações danosas ao usuário assim que são executados automaticamente em formato de macro.

Os vírus de macro podem ser encontrados em modelos de planilhas para o Excel e em documentos para o Word, além de arquivos de apresentações em PowerPoint. As versões mais recentes do pacote MS-Office oferecem a opção de, ao abrir um arquivo pela primeira vez, colocálo em modo de visualização apenas, o que é um modo de proteção contra esse vírus, impedindo que ele seja iniciado de maneira automática pelo sistema.

Atualmente, a tática mais empregada pelos fabricantes de vírus é a transmissão por *e-mails* e pelas redes sociais. Normalmente esses programas mal-intencionados são enviados como arquivos anexados ou inseridos em postagens. Essas mensagens sempre sugerem que você abra ou baixe (faça *download*) desses arquivos, induzindo-o das maneiras mais criativas possíveis, por exemplo: "Prezado senhor (a), estamos encaminhando apontamento no Serasa/SPC em seu nome, devido a uma conta não paga. Gentileza acessar o link abaixo para confirmar seus dados e ter acesso à empresa credora dentro do prazo de 48 horas...". Nunca clique sobre links como este.

## Estado de zoombie

Esse estado é fruto de um vírus, e ocorre quando o computador está sendo completamente controlado pelo software maligno e pelo agente que o criou e disseminou.

Esse estado é perigoso para o computador e para toda a rede, já que ele pode ser utilizado para espalhar o vírus sem que chame atenção, e em pouco tempo toda a rede estará contaminada.

# Facilitadores para os vírus

# Usar um sistema antigo e não o atualizar corretamente

As atualizações que são feitas em sistemas visam protegê-lo dos vírus que são postos diariamente na Internet, por isso é necessário que o sistema operacional esteja sempre atualizado e seja sempre o mais novo, já que assim ele estará mais moderno e protegido de falhas antigas.

A *Microsoft*, por exemplo, já foi vítima de um vírus que infectou boa parte dos sistemas operacionais, no sistema antigo, o XP, mas, na versão mais atualizada (10) não possuem registros de que tenha corrompido o sistema pelo vírus que antes já foi problema para os diversos usuários do sistema.

# Abrir e-mails e fazer downloads de remetentes desconhecidos

Como visto previamente boa parte dos vírus que hoje circulam pela Internet são repassados por *e-mail*, por isso é preciso que se tenha atenção redobrada quando se conecta com o *e-mail* para ler suas mensagens, algumas dicas de proteção são:

- Conferir sempre o destinatário.
- Caso o destinatário não seja conhecido não abrir o e-mail, e se abrir não clicar em nenhum link.

- Caso esteja no computador da empresa, observar as instruções para abrir e-mails, a fim de não comprometer a segurança das informações da empresa.
- Não clicar em links que venham de destinatários desconhecidos, e caso venha de um conhecido, mas não é de seu feitio mandar o tipo de link, não abrir, perguntar antes.

# Não utilizar cópias de segurança

As cópias de segurança, como o nome já diz, trazem um maior conforto para empresa quanto as suas informações, elas são vitais para que os dados não se percam, caso algum sistema seja corrompido. Quando não se utiliza cópias de segurança os vírus podem permanecer por tempo indeterminado na máquina, causando cada vez mais problemas.

## Os vírus mais conhecidos na história

# Chernobyl

Criado em 1998, era um vírus que possuía um poder de destruição enorme. Cerca de 60 milhões de PC's foram infectados por ele, mas seu principal local de atuação foi na Ásia. Apesar de ser criado em 1998 ele era um vírus "bomba relógio", só foi ativado quando o acidente nuclear que deu nome a ele completou um ano, em 1999, ele apagava todos os dados da BIO, impossibilitando o computador de ligar.

Figura 11 - Chernobyl

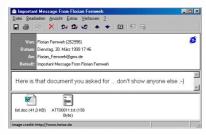


Fonte: Freepik.

### Melissa

Criado em 1999, ele não era destrutivo, mas causou prejuízo às empresas que trabalhavam com tecnologia. Era um vírus macro e abria uma série de ações que, na época, congestionaram os servidores do maior *e-mail*, Outlook. Como um típico vírus macro ele se disseminou por *e-mail* e dava a ilusão que era um arquivo DOC.X.

Figura 12 - Melissa

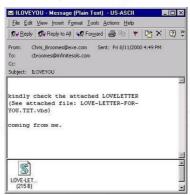


Fonte: TecMundo (2016).

#### I Love You

Como o Melissa ele se disseminou por *e-mail*, mas ao contrário era completamente destrutivo para quem abria a caixa de mensagens eletrônicas. Ele se utilizava da curiosidade das pessoas, achando que alguém tinha mandado uma carta de amor, assim que abria o arquivo que vinha, um *Worm* era aberto, esse vírus substituía todas as fotos pessoais por arquivos inseridos pelo agente que criou, excluindo todas essas informações.

Figura 12 - I Love You



Fonte: Cyber Bezpieczenstwo.

## Cabir

Conhecido como o primeiro vírus de celular, ele foi liberado em 2004. Ele não era destrutivo e fazia unicamente mostrar a palavra "Caribe" quando o celular ligava, ele possuiu uma disseminação enorme, visto que bastava o celular infectado conectar com o Bluetooth de outro celular e esse já era contaminado.

Figura 13 - Cabir



Fonte: TecMundo (2016).



#### RESUMINDO:

E então? Gostou do que mostramos? Aprendeu mesmo tudinho? Agora, só para termos certeza de que você realmente entendeu o tema de estudo deste capítulo, vamos resumir tudo o que vimos. Você deve ter aprendido sobre o que vem a ser vírus de computador e que, assim como os vírus que atingem as pessoas, os vírus de computador também atingem as máquinas e possuem diferentes tipos, entre eles o *boot*, o *worms*, entre outros. Ainda, vimos quais são os facilitadores para os vírus, ou seja, os meios mais fáceis que os vírus usam para entrar no computador e, por fim, vimos quais são os vírus mais conhecidos na história.

# REFERÊNCIAS

CHAVES, E. O. C.; FALSARELLA, O. M. Os sistemas de informação e sistemas de apoio à decisão. **Revista do Instituto de Informática,** v. 3, n. 1, 1995.

FREIRE, I. M.; ARAUJO, V. M. R. H. de. A responsabilidade social da Ciência da informação. **Transinformação**, Campinas, v. 11, n. 1, p. 7-15, jan./abr. 1999.

MARCHIORI, P. A Ciência da Informação: compatibilidade no espaço profissional. **Caderno de Pesquisas em Administração**, São Paulo, v. 9, n. 1, p. 91-101, jan./mar. 2002.

MCGEE, J. V.; PRUSAK, L. **Gerenciamento estratégico da informação**. Rio de Janeiro: Campus, 1994.

