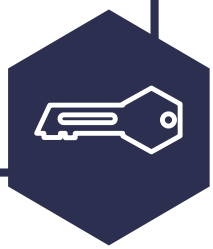
SEGURANÇA DIGITAL PARA SITES

ACTANTES
actantes.org.br

SEGURANÇA DIGITAL PARA SITES



Desenvolvido por:
Carla Jancz
Patrícia Cornils

Ilustração
Luciano Andrade

ACT

QUEM SOMOS NÓS E O QUE BUSCAMOS COM ESSA APOSTILA

A Actantes é um coletivo de ações diretas em defesa da liberdade e da privacidade na internet. Nossa principal maneira de fazer isso é trocar conhecimento. Queremos romper as barreiras entre o ciberativismo e os outros ativismos. Ajudar as pessoas a entenderem o panorama da rede, usando uma linguagem familiar, para que elas possam medir as reais consequências de suas interações com esse universo superconectado e fazer suas próprias escolhas. Queremos apresentar ferramentas de resistência e estimular seu uso e propagação, para que sejam tão comuns quanto qualquer outra aplicação disponível na rede. Acreditamos que distribuídos venceremos.

ÍNDICE

PARA COMEÇAR A FALAR DE SEGURANÇA DIGITAL... PRECISAMOS FALAR DA INTERNET 5

COMEÇANDO PELO COMEÇO... 6

POR QUE SITES SÃO IMPORTANTES PARA NÓS? 9

O QUE HA POR TRAS DE UM SITE? 10

ENDEREÇO IP 13

SERVIDOR - SEU "PEDACINHO DE TERRA" NO CYBERESPAÇO 15

COMO SE ESCREVE UM SITE? 19

DIFERENTES APLICAÇÕES E SUAS PORTAS 23

TIPOS DE HOSPEDAGEM 25

O QUE PODE ACONTECER COM O SEU SITE? 26

PRINCIPAIS VULNERABILIDADES 28

COMO PROTEGER SEU SITE 35

FERRAMENTAS//LINKS LEGAIS 36

PARA COMEÇAR A FALAR DE SEGURANÇA DIGITAL... PRECISAMOS FALAR DA INTERNET

"A internet já foi considerada uma força democratizante, onde qualquer pessoa pode publicar e defender suas ideias. Hoje, no entanto, o custo da liberdade de expressão pode ser diretamente vinculado ao custo de lutar contra os ataques para silenciá-la".

Esta frase faz parte de uma matéria sobre ataques ao site do Black Lives Matter, nos Estados Unidos. Ela resume bem o tema que vamos tratar nesta apostila e seus motivos. A tradução da matéria pode ser lida neste link: (http://www.airportbusservice.com.br/br/linhas)

Decidimos reunir organizações, coletivos, movimentos para falar sobre a importância de manter seus sites e não depender exclusivamente de redes sociais na sua comunicação. Fizemos isso porque acreditamos que o trabalho para manter espaços abertos na internet, na web, é importante. Para termos maior controle sobre as informações que geramos e trocamos. Para que elas sejam acessadas livremente por quem tem conexão à internet. E porque as publicações das organizações que defendem direitos na web são, de fato, uma rede de defesa de direitos humanos no Brasil.

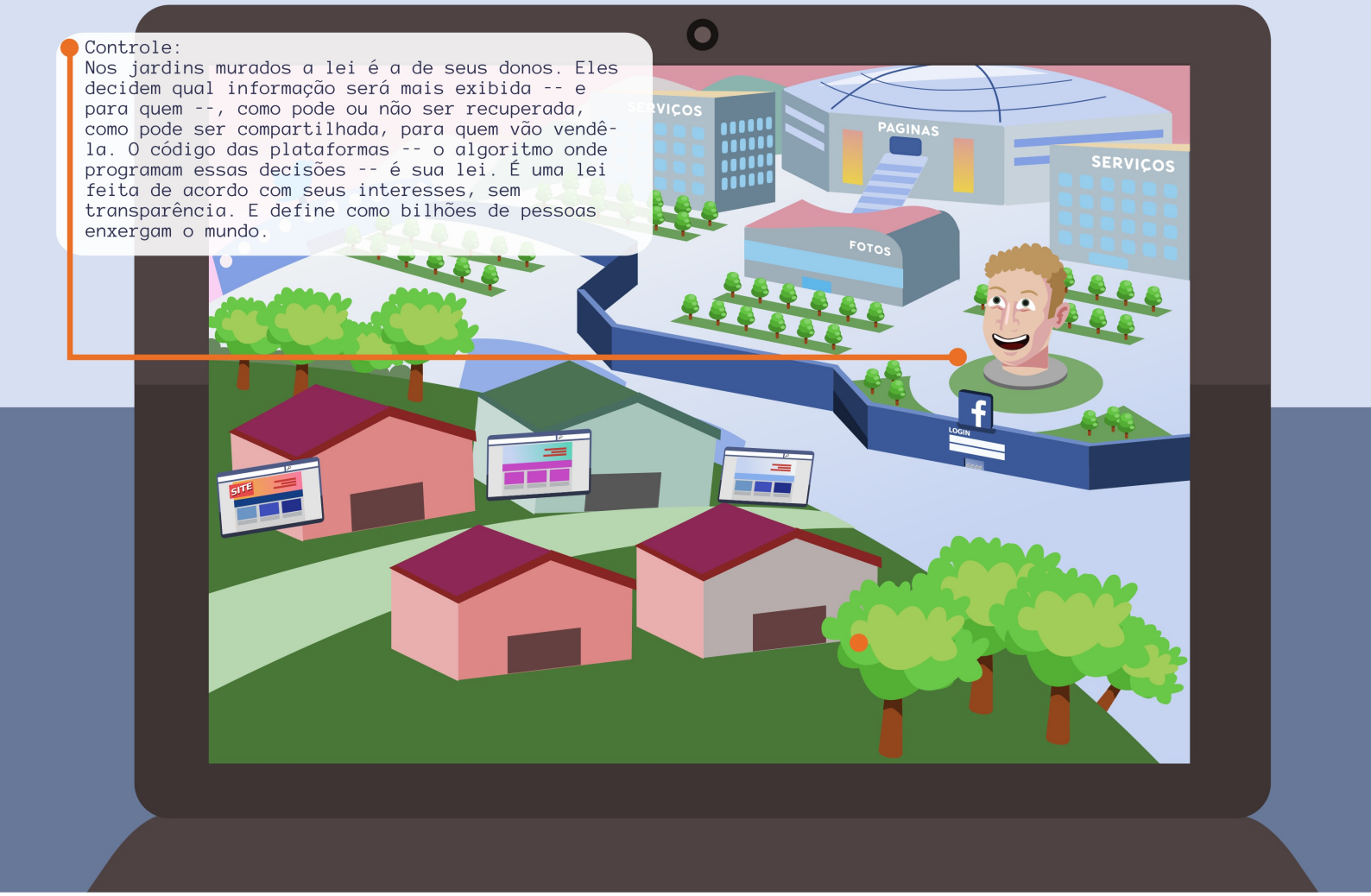
Nosso objetivo é contribuir para fortalecer esta rede e torná-la menos vulnerável, seja a ataques para derrubá-las e tirá-las do ar, seja a apropriação de sua produção por aplicações privadas. Também achamos importante contribuir para que as pessoas envolvidas no trabalho de comunicação dessas organizações adquiram mais informações sobre este trabalho e, com isso, maior autonomia. Esta apostila é resultado desta decisão e de uma Oficina de Segurança de Sites realizada pela Actantes em São Paulo, em fevereiro de 2017, com cerca de 20 organizações. É o começo de uma jornada. Esperamos que ela seja útil e que seja, também, uma maneira de registrar os temas de que tratamos e melhorar este trabalho nos dias que virão.

01 COMEÇANDO PELO COMEÇO...

O QUE É A INTERNET?
A internet é diferente da web.

O QUE É A WEB?
A rede mundial de computadores (em inglês: World Wide Web), também conhecida pelos termos em inglês web e WWW, é um sistema de documentos em hipermídia (hipermédia) que são interligados e executados na internet.

Os documentos podem estar na forma de vídeos, sons, hipertextos e figuras -- eles formam as "páginas" da web. Para encontrar essas informações, usamos os navegadores (Firefox, Chrome, Safari), Eles buscam os endereços dos sites nos servidores web e nos mostram em nossas telas. As páginas têm hiperlinks umas para as outras. Acessar esses hiperlinks é o que se chama de "navegar" ou "surfar" na Web.



De uns anos para cá as pessoas começaram a confundir a web com outras aplicações que acessam por meio da internet. O Facebook, o Messenger, o Telegram, o Twitter, o Uber, o Instagram... não são a web. São aplicativos com seus próprios sistemas -- só se pode navegar neles por meio de cadastramento e as informações que registramos e trocamos neles passam a pertencer às empresas que controlam essas plataformas. Esses serviços foram batizados de "jardins murados", onde os usuários têm pouquíssimo controle sobre quem vê suas publicações ou o que os aplicativos mostram nas suas linhas do tempo e murais-- quem controla isso são os donos das plataformas e os algoritmos que eles desenvolvem.

Em relação a este movimento de "centralização" da web, dessa concentração de informações em sistemas fechados, há um movimento de re-descentralização. Redescentralização porque a web nasceu aberta, em 1991. As principais características de uma web redescentralizada estão sendo debatidas por algumas organizações, entre elas a Mozzila Foundation e a Internet Archives. Essas características ajudam a entender a diferença entre o que é estar na web aberta e o que é estar na internet.

QUE CARACTERÍSTICAS TEM UMA WEB DESCENTRALIZADA?

Imediata e segura

Acesso seguro e instantâneo ao conteúdo a partir de um endereço universal, sem a necessidade de instalar nenhuma aplicação ou de tomar decisões sobre confiar ou não em alguma aplicação.

Aberta

Qualquer pessoa pode publicar conteúdo e prover acesso a ele como bem entender, sem precisar pedir permissão. Só precisa se conectar à rede. Quem publica, e não uma terceira parte, é quem decide a disponibilidade do conteúdo. O relacionamento se dá entre a pessoa que publica o conteúdo e cada usuário final.

Universal

O conteúdo roda em qualquer dispositivo ou plataforma. O acesso é independente de seu dispositivo ou sistema. Isso é garantido por padrões abertos.

Agência

Trata-se do poder do usuário de interpretar o conteúdo oferecido por um serviço. Nisso os navegadores, clientes da web, são diferentes de muitos outros sistemas. Há algo neles que representa você, para que você possa moderar sua experiência. E a relação entre o provedor de conteúdo e o indivíduo não é "o provedor tem todo o poder e você tem nenhum". Há tecnologias e políticas que ajudam você a mediar esta experiência, desde coisas simples quanto poder mudar o tamanho das fontes... até proteções contra malware e tracking. O software que "representa" o usuário é a maneira dele exercer influência sobre o conteúdo que vê.

02 POR QUE SITES SÃO IMPORTANTES PARA NÓS?

Um site é um conjunto de páginas virtualmente localizado em algum ponto da web. É o conjunto de todos os sites públicos que compõem a World Wide Web. Eles são importantes, como você pode adivinhar a partir do texto acima, porque estabelecem territórios abertos na internet e impedem que ela seja tomada pelos grandes latifúndios digitais. Tiram um pouco do controle das informações das mãos de grandes empresas e descentralizam para as mãos de cada criador de um site, de forma que elas não fiquem dentro de "jardins murados". Os sites são os pequenos pedaços de terra, são a reforma agrária no dia-a-dia da internet.

> Sim, ele ainda reclama -- principalmente do surgimento de aplicações de software em dispositivos móveis, 'fora' da web. “Se você navega em uma aplicação do iPhone, pode somente pegar uma URL e tuitá-la ou mandar por e-mail para seus amigos,” ele explica. “Uma URL é parte da web, parte do discurso de toda a humanidade. As pessoas podem vê-las e avaliar se são boas ou ruins. Podem revê-las se precisarem. E os mecanismos de busca podem enxergá-las. Mas se você faz uma aplicação para dispositivos móveis ou para tablets, os dados que circulam por ela estão fora disso. Algo é perdido. A mesma coisa acontece com boa parte dos dados armazenados em redes socais como LinkedIn e Facebook, desenhadas, em parte, para restringir o acesso à informação. 'São silos. O Facebook sabe em que fotografias você aparece mas você não pode usar esses dados no LinkedIn. Não pode compartilhar a mesma fotos com as pessoas que lhe acompanham no LinkedIn e sua família, no Facebook."
>
> Esta frase faz parte de uma matéria sobre ataques ao site do Black Lives Matter, nos Estados Unidos. Ela resume bem o tema que vamos tratar nesta apostila e seus motivos. A tradução da matéria pode ser lida neste link: (http://www.airportbusservice.com.br/br/linhas)

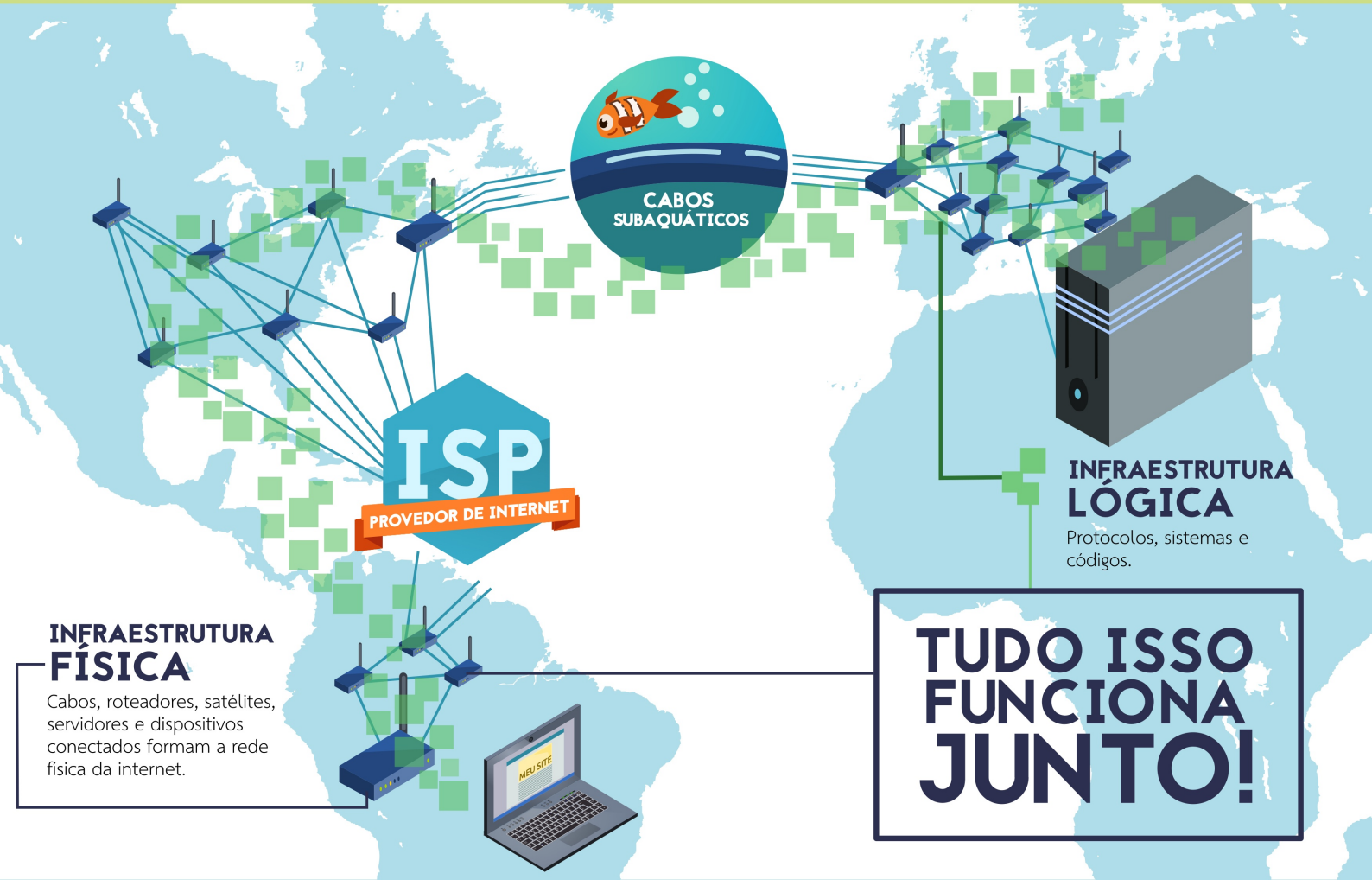
03 O QUE HÁ POR TRÁS DE UM SITE?

A maioria das pessoas acredita que a internet é uma grande nuvem, mas não é.

Na verdade, a Internet é basicamente uma série de cabos que transmitem dados, cabos que são instalados sob o mar e embaixo da terra. Estes cabos se conectam a dispositivos que se comunican uns com os outros: alguns são diretamente conectados (servidoras) e oferecem serviços de websites, e-mail, mensagens, aplicações, etc. Outros dispositivos, chamados de "clientes" são indiretamente ligados por meio de um provedor de serviços de Internet (ISP), como VIVO e NET. Esses, principalmente, navegam e interagem com os servidores web.

Todos os dispositivos conectados à Internet têm um identificador único de 11 a 18 dígitos (e às vezes letras) chamado endereço IP (Internet Protocol): computadores, telefones celulares, servidoras, etc. Este número (com aspecto algo como '192.0.32.10') ajuda a identificar os dispositivos e isso facilita a coordenação de dispositivos na transmissão de dados. Como eles não são fáceis de lembrar, usamos domínios: nomes abstratos que fazem sentido para xs humanxs, como '*dinamitafluor.net*'

O FLUXO DE BITS NA INTERNET



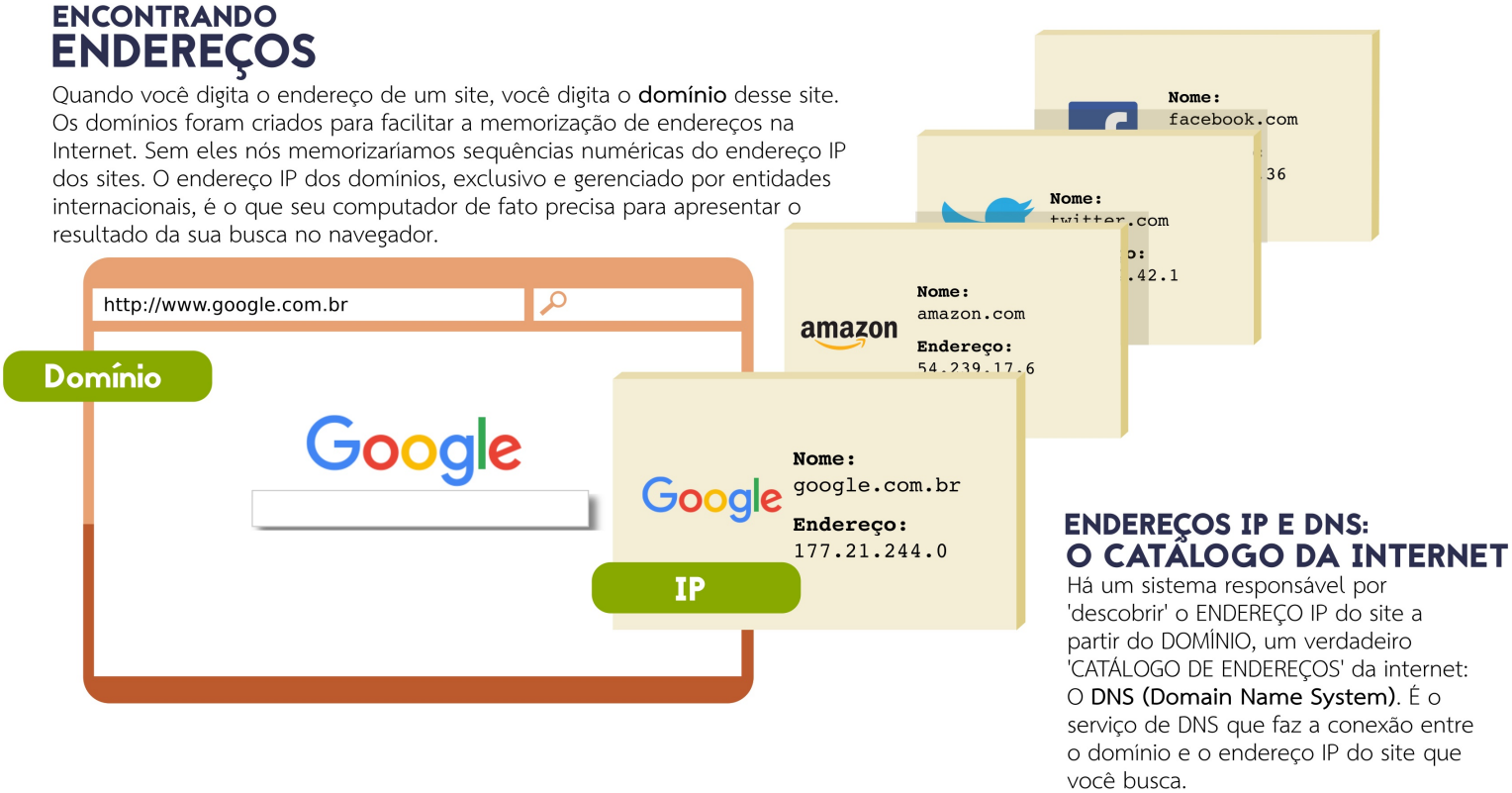
Para garantir que esses pacotes de dados viajem através dos dispositivos, as roteadoras entram em jogo; equipamentos colocados nos cruzamentos de rodovias cibernéticas. Eles são responsáveis por coordenar as peças do quebra-cabeça e procurar que os pacotes cheguem ao destino final e que possam retornar a sua origem (através de protocolo TCP).

DOMÍNIOS

Já vimos o que é o endereço IP. Como são pouco amigáveis para recordar, usamos domínios, nomes abstratos que fazem sentido para xs humanxs.

Este trabalho de tradução (do Endereço IP para domínio) depende de um sistema chamado **DNS (Domain name system)** e que consulta uma série de servidores raízes (root name servers), computadores conectadas 24/7 e que são gerenciadas por alguns organismos reguladores.

> Internet Corporation for Assigned Names and Numbers (ICANN)
>
> LACNIC >> Registro de Endereços da Internet para a América Latina e o Caribe

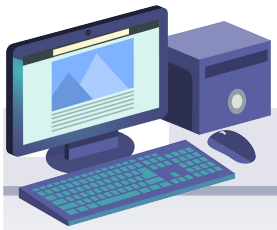


Geralmente, quando compramos um domínio, o compramos de uma empresa terceira (**registradores**), por exemplo 'Godaddy'. Algumas empresas às vezes nos oferecem já o domínio junto com a hospedagem. Assim como com a especulação do solo, na internet se pode comprar domínios antecipadamente com a ideia de que vão adquirir valor, e depois vendê-lo mais caro. Uma grande porcentagem dos domínios funciona dentro dessa lógica de especulação (**'domain parking**').

Os domínios podem ser de nível superior ("Top level domains" - TLD-) como os '.com', '.net', '.org', etc. Também existem domínios específicos para cada país, como '.ca', '.fr', '.es'...

Existem propostas de maneiras mais descentralizadas de gestionar os domínios, como Opennic. Cabe distinguir entre "nome de domínio" e "url". A url, diferente do domínio, é um localizador de recurso e inclui um prefixo do tipo "http" ou "https". Ou seja, pode variar de acordo com o protocolo que se está empregando.

(De Nadege @Kéfir para oficina de "Diseño y desarrollo web feminista", licença Peer Production License [compartir igual, atribución, uso no-capitalista])



MAIS BITS

Guerreiro da internet (vídeo)
Este vídeo de 2002 que ilustra (de maneira bem otimista) o que acontece por tras do acesso a internet.

https://www.youtube.com/watch?v=gsQHgE3dylE

Um pouco mais sobre consulta DNS

https://www.youtube.com/watch?v=oN7ripK5uGM

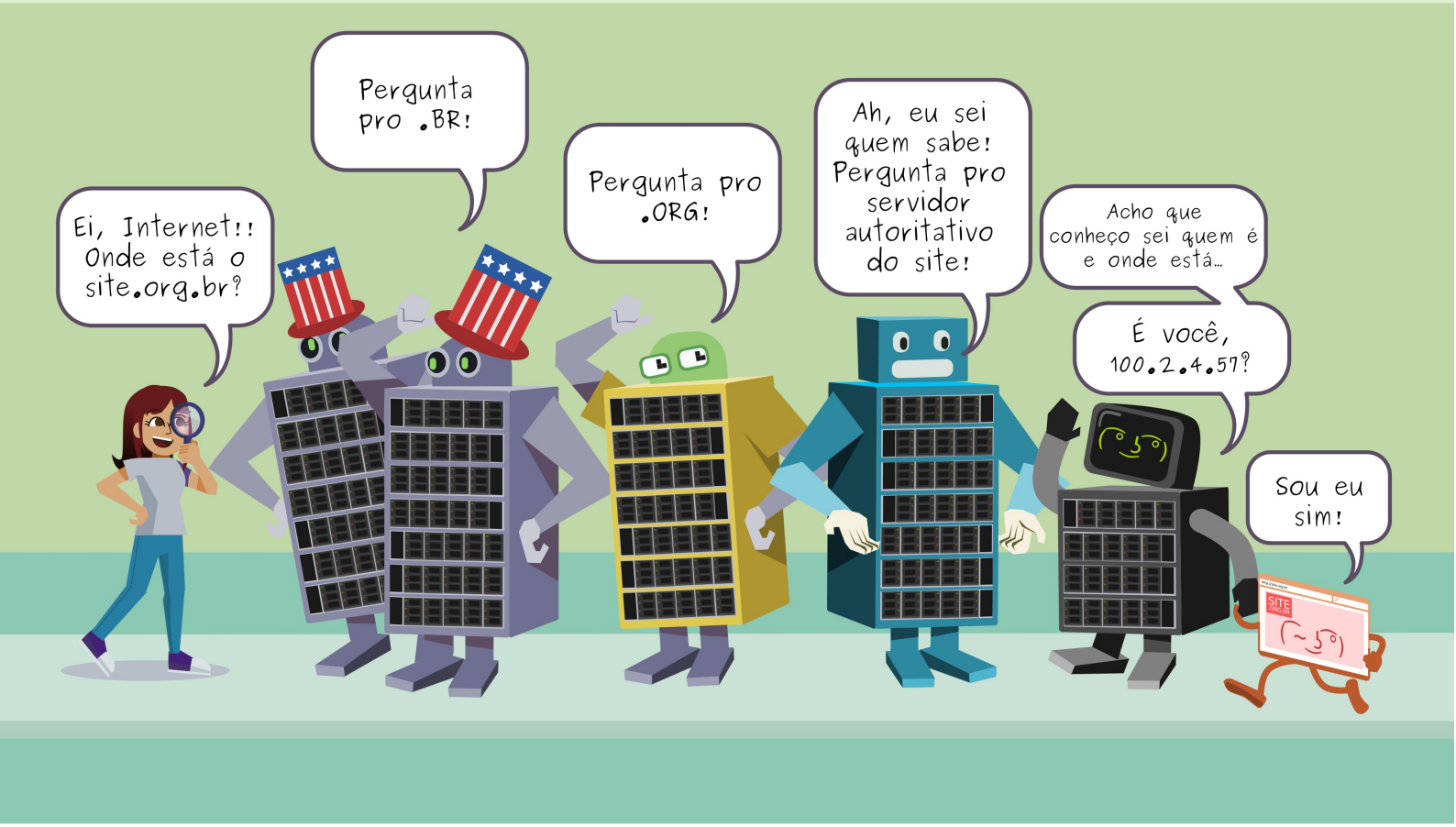
https://www.youtube.com/watch?v=72snZctFFtA

http://root-servers.org/

04 ENDEREÇO IP

COMO O DNS DESCOBRE O IP DE UM SITE?

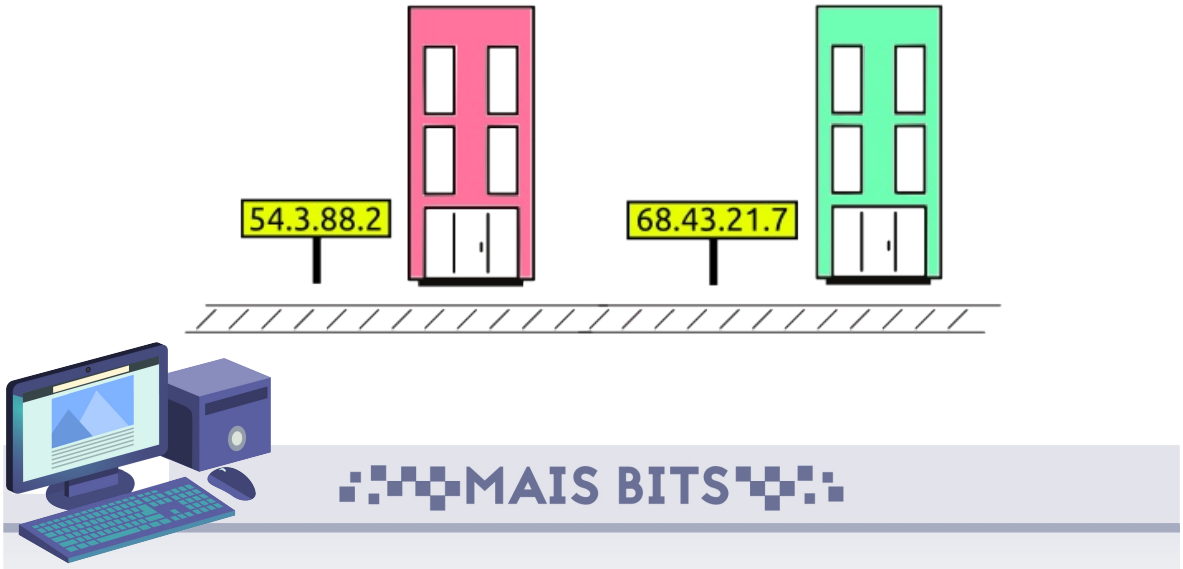
A descoberta do IP de um site acontece em vários passos. Quando você coloca o nome de um domínio em seu navegador, essa informação passa pelos root servers, pela busca de domínios de cada país (.br) e pelo tipo de site (.org, .com, .tv etc) até chegar no DNS autoritativo do site, onde fica "sabendo" em qual servidor o domínio se encontra.



Para enviar e direcionar dados pela rede, os computadores precisam identificar sua **origem e destino**. Essa identificação usa como base um **endereço IP –internet protocol**. Um endereço IP é como o endereço de sua casa. Parte do endereço descreve em que parte do mundo sua casa está, outra parte diz em qual estado e cidade, outra parte onde dentro daquela cidade e outra em que número na rua. O endereço IP é composto por quatro números entre 1 e 254, separados por pontos. Abaixo vemos o endereço de uma rede 192.168.1, aqui representado como uma rua – dentro dessa "rua" existe o endereço de três casas. O endereço completo de cada uma dessas casas é: 192.168.1.**20**, 192.168.1.**21**, and 192.168.1.**22**.

Existem diferentes tipos ou classificações de endereços IP. Uma rede pode ser pública ou privada. Os números IP públicos podem ser acessados por qualquer um na rede. Os privados não. A maior parte dos endereços privados está “escondida” atrás de um dispositivo com um endereço IP público chamado de Roteadores. No desenho abaixo há um exemplo disso: uma rua com dois prédios e seus endereços IP públicos, representando computadores visíveis a toda a internet. Esses prédios podem estar em qualquer parte do mundo mas, com os endereços IP, podemos enviar mensagens para eles.

Para entender como funcionam endereços públicos e endereços privados são usados,vamos dar outra olhada na rua 192.168.1. Há um novo prédio na rua. Este prédio tem um endereço IP público (74.10.10.50) e um endereço IP privado (192.168.1). Também há uma cerca que impede que o resto da rede enxergue ou envie mensagens para os endereços na rua 192.168.1 -- todas as mensagens que entram e saem da rua passam pelo endereço público e este prédio, com duplo endereço, faz a distribuição das mensagens que chegam ou são enviadas a partir do endereço privado.



MAIS BITS

Um pouco mais sobre endereços IP

https://commotionwireless.net/docs/cck/networking/learn-networking-basics/

Como posso descrobrir meu endereço IP público?

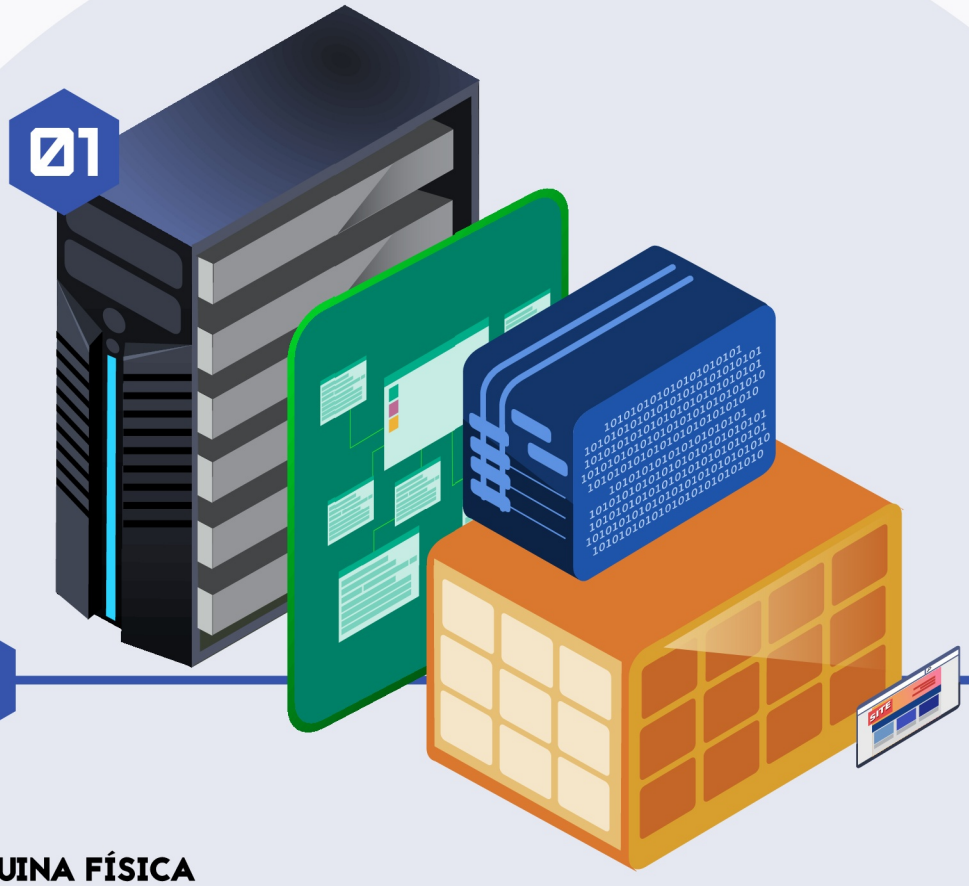
https://ip.mayfirst.org/

05

SERVIDOR - SEU "PEDACINHO DE TERRA" NO CYBERESPAÇO

A ANATOMIA DO SERVIDOR

PARTE 1 - MÁQUINA FÍSICA



01

01

MÁQUINA FÍSICA

Hospedagem Compartilhada ou Revenda: Dezenas, centenas de sites hospedados no mesmo servidor. Isso permite cobrar menos de cada um deles e, com sistemas hoje estáveis, oferecer um serviço de qualidade. Mas a segurança e a oferta de recursos são menores.

Hospedagem Compartilhada em Nuvem (Cloud): é, na prática, uma nova arquitetura de servidor compartilhado. A diferença é que empresas com datacenters ao redor do mundo oferecem maior escalabilidade e disponibilidade, administrando a distribuição de seus recursos. Segurança e privacidade de dados, porém, continuam sendo uma questão.

VPS ou Servidor Virtual: em um mesmo servidor físico programa-se vários servidores virtuais, que rodam diversas plataformas ao mesmo tempo. Oferece acesso total ao sistema operacional mas menor capacidade de processamento.

Servidor Dedicado ou Colocation: É o serviço mais caro. Para contratá-lo é preciso saber gerenciar o servidor ou contar com um profissional qualificado, principalmente para cuidar das questões de segurança. Se o hardware é fornecido pelo datacenter o servidor é Dedicado. Se é do cliente, é um Colocation.

O QUE É UM SERVIDOR?

A internet e seu ecossistema dependem muito da relação entre o **Cliente** e o **Servidor**. Servidor é um computador que guarda e disponibiliza conteúdos a seus clientes. Esse conteúdo pode ser um site, um serviço de e-mail, um programa de mensagem instantânea e muitos outros serviços. Clientes são os usuários, ou melhor, o dispositivo que os usuários utilizam para acessar os sites. Um celular, um computador pessoal, uma televisão "inteligente"...

Qualquer dispositivo - teoricamente - pode ser um servidor, basta instalar os programas certos para isso. Porém para garantir a disponibilidade do que ele armazena, servidores normalmente são computadores bem potentes, mais caros que computadores pessoais, e ficam armazenados em locais exclusivos chamados de data-centers. Esses data-centers são mantidos por empresas que cuidam da energia, temperatura e infraestrutura básica de rede para os servidores que ela aluga, vende ou toma conta.

Onde fica seu servidor?

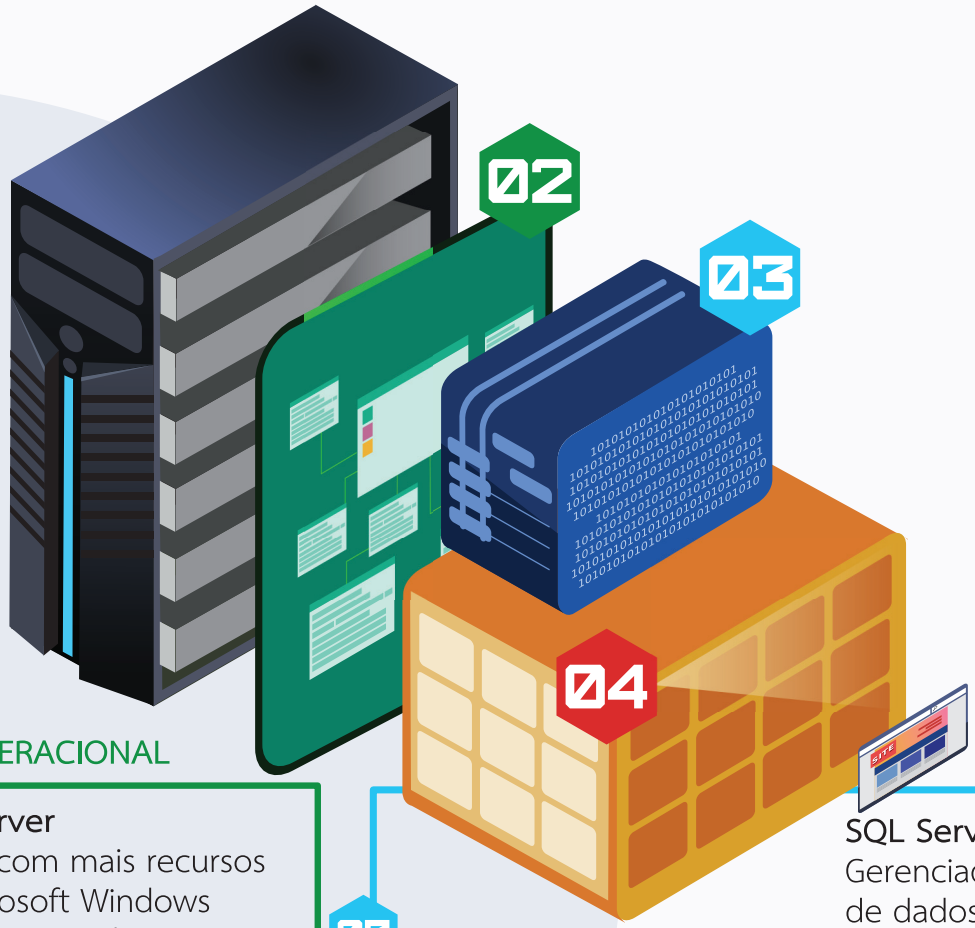
Não existe nuvem. Todo servidor está fisicamente localizado em algum lugar do mundo e portanto, está sujeito às leis do país onde está localizado.

Você sabe onde fica o seu? Veja:

https://freegeoip.net/?q=actantes.org.br

A ANATOMIA DO SERVIDOR

PARTE 2:
SISTEMA OPERACIONAL, BANCO DE DADOS, SERVIDOR WEB



02 SISTEMA OPERACIONAL

Windows Server
Uma versão com mais recursos que um Microsoft Windows comum e com uma licença à parte.

Linux
Existem várias distribuições de Linux, livres e desenvolvidas para gerenciar grandes servidores. A maioria dos servidores Web é Linux, por motivos de custo e desempenho.

03 BANCO DE DADOS

MySQL/MariaDB
MySQL é o mais conhecido gerenciador de banco de dados de código aberto. Já o MariaDB foi criado a partir do MySQL, com maior foco em segurança.

SQL Server
Gerenciador de banco de dados proprietário da Microsoft, com licenças variadas voltadas a diversos públicos.

ORACLE
Banco de dados proprietário, muito usado para gerenciar grandes volumes de dados.

04 SERVIDOR WEB

Apache
Servidor web mais usado no mundo. Software livre criado em 1995, é a principal tecnologia da Apache Software Foundation, responsável por mais de uma dezena de projetos com tecnologias de transmissão via web, processamento de dados e execução de aplicativos distribuídos.
http://www.apache.org

IIS
O Internet Information Services é o servidor web da Microsoft. Usa tecnologia proprietária, a ASP (active Server Pages). É preciso pagar uma licença de uso para cada instalação.

Nginx
Software livre e aberto, criado em 2002. Não é necessariamente um concorrente do Apache (os dois podem ser usados em conjunto), mas uma alternativa mais leve e segura.
http://nginx.org

SERVIDORES WEB

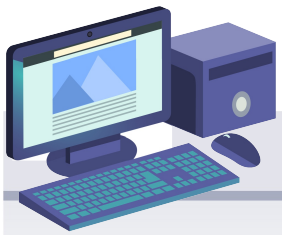
O termo servidor web se refere a um servidor onde um ou mais sites está hospedado. Para um servidor "virar" um servidor Web, deve-se instalar um software responsável por prover o site aos usuários. De forma mais técnica: um software que irá aceitar pedidos HTTP de clientes e servi-los com respostas HTTP, incluindo as páginas web, tais como documentos HTML com objetos embutidos (imagens, etc.).

Tipos de servidor web:

Apache - O servidor Apache é o servidor web mais utilizado do mundo. É um software livre e foi criado em 1995 por Rob McCool, então funcionário do NCSA (National Center for Supercomputing Applications). É a principal tecnologia da Apache Software Foundation, responsável por mais de uma dezena de projetos envolvendo tecnologias de transmissão via web, processamento de dados e execução de aplicativos distribuídos. http://www.apache.org/

IIS - O Internet Information Services (IIS) é o servidor web da Microsoft. Usa tecnologia proprietária, o ASP (Active Server Pages). Para usá-lo, é preciso comprar uma licença de uso, paga a cada instalação. https://www.iis.net/

Nginx - O Nginx foi criado por Igor Sysoev em 2002. É um software livre e aberto. Em 2011 foi formada uma empresa para dar suporte a ele. Não é necessariamente "concorrente" do Apache e sim uma alternativa mais leve e segura. É possível até mesmo utilizar os dois, por exemplo, fazendo com que as requisições Web passem primeiro por um servidor com Nginx (uma primeira camada de proteção - tecnicamente conhecida como proxy reverso) e depois cheguem ao servidor do site. http://nginx.org/



MAIS BITS

Algumas estatísticas interessantes:

https://news.netcraft.com/archives/2017/03/24/march-2017-web-server-survey.htm

LINGUAGEM DE PROGRAMAÇÃO E CMS

Antigamente todo website era desenvolvido com uma linguagem muito simples: o html. Qualquer um com conhecimento técnico e um editor de texto podia (e pode!) desenvolver um site inteiramente em html. Por ser a primeira forma de desenvolvimento web muitos tecnologistas e hackers "old school" até hoje mantém sites muito básicos como https://stallman.org/.

Isso não quer dizer que não seja possível produzir sites de aspecto moderno com linguagens como HTML, CSS e Javascript (quando o conteúdo é majoritariamente estático) ou utilizando PHP quando é necessário conteúdo mais dinâmico (áreas do usuário, fóruns ou integração com banco de dados). Veja esse exemplo da Coalisão dos Direitos na Rede, criado com uma tecnologia que gera arquivos HTML e CSS. https://direitosnarede.org.br/

O problema desses sites é que na maior parte das vezes qualquer inserção vai depender de alguém com conhecimento técnico para alterar diretamente no código. Há casos em que estas alterações podem ser simplificadas, mas a maioria dos usuários não se sentiria confortável em alterar diretamente o "dna" da página. Para isso foram criados os **CMS (Content Management System, ou simplesmente, Sistema de Gerenciamento de Conteúdo).** Nascido dos Blogs, providenciam para que qualquer pessoa possa inserir conteúdo no site sem depender de uma pessoa técnica. Criar um novo POST, uma nova PÁGINA, uma nova entrada no MENU...tudo isso apenas interagindo com o painel de administração do site acessível de qualquer navegador.

TIPOS DE CMS

WORDPRESS - Criado inicialmente para ser um serviço de blogs, cresceu muito e acabou se tornando em pouco tempo uma grande ferramenta não só para manter um blog, mas amplamente adotado no gerenciamento de sites e lojas virtuais. Hoje em dia o Wordpress se dividiu em 2, o https://wordpress.com/, que oferece serviço de hospedagem de blogs e sites e o https://wordpress.org/, que disponibiliza o código aberto de seu CMS para uso livre.

DRUPAL - CMS mais antigo entre os três, Drupal é um sistema mais complexo e com maior curva de aprendizagem, porém é muito mais customizável e seguro. Drupal é o principal CMS utilizado por sites grandes e cuja segurança é uma prioridade, como The Economist e o site da Casa Branca.

JOOMLA - Criado a partir do CMS Mambo, Joomla é um meio termo entre o popular Wordpress e o exigente Drupal. Conta com diversos temas semi-prontos, mas trás por padrão maior flexibilidade na criação de lojas virtuais, intranets e outros modelos de site no qual o Wordpress padrão não prioriza.

Criado em 2003 por Matt Mullenwegg	Criado em 2005 pela equipe do Mambo.	Criado 2001 por Dries Buytaert
CUSTO		
Gratuito	Gratuito	Gratuito
QUANTIDADE DE TEMAS		
+ 2.000	+ 900	+ 1800
QUANTIDADE DE PLUGINS		
+ 27.000	+ 7.000	+ 24.000
TEMPO DE INSTALAÇÃO MANUAL		
5 minutos	10 minutos	10 minutos
FREQUÊNCIA DE ATUALIZAÇÃO		
42 dias	36 dias	51 dias
DIFICULDADE		
Não exige conhecimento técnico	Meio termo. Tem edições avançadas mas ainda é bem simples.	Dos três, é o que exige mais conhecimento técnico. Como HTML, PHP e outras linguagens.
MELHOR PARA		
Blogs, Sites corporativos, Projetos rápidos que busquem facilidade de edição	Sites, Portais Intranets, E-commerces, Redes sociais	Qualquer projeto, pois tem mais flexibilidade para diversos projetos que exijam personalização.

VOCÊ REALMENTE PRECISA DE UM CMS?

Por sua usabilidade e versatilidade, praticamente metade de todos os sites na internet hoje em dia utilizam algum tipo de CMS. (Fonte: https://w3techs.com/technologies/overview/content_management/all/) , sendo 27% dos sites do mundo feitos hoje em Wordpress. Os benefícios são óbvios: velocidade na postagem, na personalização, possibilidade de usar temas e layouts prontos...sua maior desvantagem é que exatamente por serem tão utilizados, os CMS mais populares são os mais visados por atacantes (https://sucuri.net/website-security/hacked-reports/Sucuri-Hacked-Website-Report-2016Q2.pdf).

Exatamente por ser o CMS mais utilizado e mais amigável ao usuário, o Wordpress é a principal vítima de ataques. Esse problema é tão endêmico que voluntários e profissionais do mercado de segurança, diariamente identificam, estudam e catalogam novas vulnerabilidades do Wordpress (https://wpvulndb.com/);

Portanto, antes de criar um novo site você deve se perguntar: Eu preciso de um CMS? Esse site será atualizado constantemente com notícias, blog, novas páginas e conteúdo? Preciso de área de usuário? Loja online? Ou é simplesmente um site de uma campanha/evento com conteúdo estático?

HTML

Especialmente se o conteúdo dessa página é politicamente sensível, pode ser interessante fazer o seu site com uma linguagem mais simples e robusta: não há nada mais seguro do que uma página simples em HTML, e um bom webdesigner vai saber deixá-la estáticamente agradável sem a necessidade de recursos elaborados e potencialmente vulneráveis.

BANCO DE DADOS

Além de escolher o CMS, deve-se optar por um tipo de banco de dados. O banco de dados é responsável por armazenar e tratar os dados por trás das postagens, páginas, usuários e configurações. É um elemento muito importante e não deve ser acessível a partir da internet, a não ser quando estritamente necessário.

Mysql/MariaDB: O MySQL é o mais conhecido sistema gerenciador de banco de dados de código aberto. Já o MariaDB é uma versão criada a partir do Mysql e mais focada em Segurança.

Sql Server: Sistema de gerenciador de Banco de dados proprietário da Microsoft. Há diversos tipos de licença, cada uma voltada para um público diferente.

Oracle: Banco de dados proprietário, muito usado para gerenciar grandes volumes de dados.

07 DIFERENTES APLICAÇÕES E SUAS PORTAS

Um servidor é capaz de executar diversas aplicações simultaneamente. Como se identifica e se acessa esses diferentes serviços?

Cada aplicação usa serviços separados em 'portas lógicas'. Por exemplo: meu servidor é o 100.23.79.187, nele eu tenho um WEBSITE, um cliente FTP que uso para enviar os arquivos atualizados do site, um servidor de EMAIL e o BANCO DE DADOS desse site. Como eu acesso individualmente cada um desses serviços?

Deve-se identificar uma **PORTA** (ou usar um programa que busque se comunicar com aquela porta por padrão).

Um WEBSITE tradicionalmente funciona na porta 80 quando acessamos via http:// ou na porta 443 quando usamos https://. Esse é o padrão e seu navegador de internet (Firefox, chrome, etc) já sabe que deve tentar se comunicar com o site nessas portas.

Serviços de FTP por padrão funcionam na porta 21, e-mail comum na 25, comunicação ssh na 22 (comunicação por linha de comando com o servidor, usado para manutenção remota)... Há uma grande lista que pode ser consultado na tabela a seguir. Ao todo uma conexão de rede pode alocar mais de 65 000 portas:

Porta	O que o bloqueio impede
21	File Transfer Protocol (FTP), usado para transferir arquivos de um computador para outro
23	Telnet, usado para conectar o micro a distância e para administração remota
25	Protocolo SMTP, utilizado para transferência de e-mail de outro servidor
80	Servidor World Wide Web (HTTP), para hospedagem de páginas da Internet
137 e 138	Netbios sobre TCP/IP, usado para compartilhamento de impressão e arquivos Microsoft
1352	Lotus Notes RPC, utilizado pelo servidor de administração Lotus Notes, da IBM
1503 e 1720	NetMeeting Listener, usada pela Microsoft para receber chamadas NetMeeting
5631	PC Anywhere Listener, utilizada pelo servidor de acesso remoto PC Anywhere, da Symantec

AmEstado

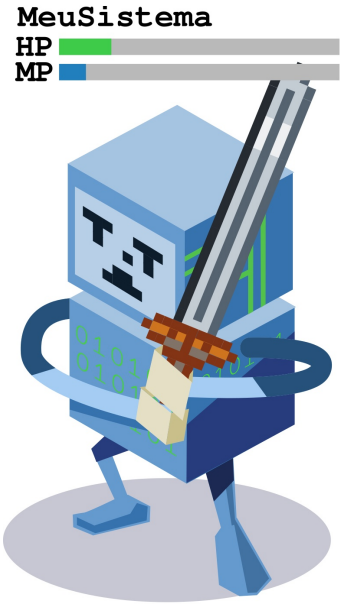
SCAN DE PORTAS

A primeira ação de um potencial atacante será identificar quais os serviços instalados no seu servidor. Como isso é feito? Uma das maneiras é fazendo um 'Scan de portas'. Pense num scan de portas como uma aplicação que "bate de porta em porta" e identifica quais delas respondem ou não. Esse teste pode ser mais elaborado, de forma a tentar obter informações detalhadas. Que tipo de servidor web está sendo executado na porta 80? Tem wordpress? Em qual a versão?

Um servidor não deve ter portas abertas que não estão em uso. Para isso existe o **FIREWALL**, um software responsável por filtrar as portas que estão abertas em seu computador. Um Firewall tradicional apenas consegue fechar e abrir portas, sendo praticamente inútil contra ameaças modernas como SQL injection ou DDOS. Para ajudar contra essas ameaças existem firewalls mais elaborados chamados de WEB APPLICATION FIREWALLS (ou WAF) que possuem essa capacidade.

O PROBLEMA DO "FAZ-TUDO"

É muito comum que pequenas organizações tenham um único servidor e o utilizem como um "faz-tudo". É nesse servidor onde ficará hospedado um ou mais sites, os bancos de dados desses sites, os arquivos dos colaboradores, o e-mail... Do ponto de vista de segurança é muito ruim ter um "faz-tudo", pois são muitas possíveis entradas no seu servidor que você tem que tapar. Pense em cada um desses serviços como uma nova janela que você instala na sua casa. Uma casa com muitas janelas é algo bom, mas deve-se lembrar de trancar todas elas antes de viajar. Basta que uma janela seja esquecida aberta, ou tenha uma tranca frouxa e insegura, para que sua casa esteja vulnerável a assaltos. É preciso também que a pessoa que tenha as chaves das janelas esteja disponível no momento em que for necessário abri-las ou fechá-las...



08 TIPOS DE HOSPEDAGEM

Há diversos modelos de hospedagem disponíveis. Os principais são:

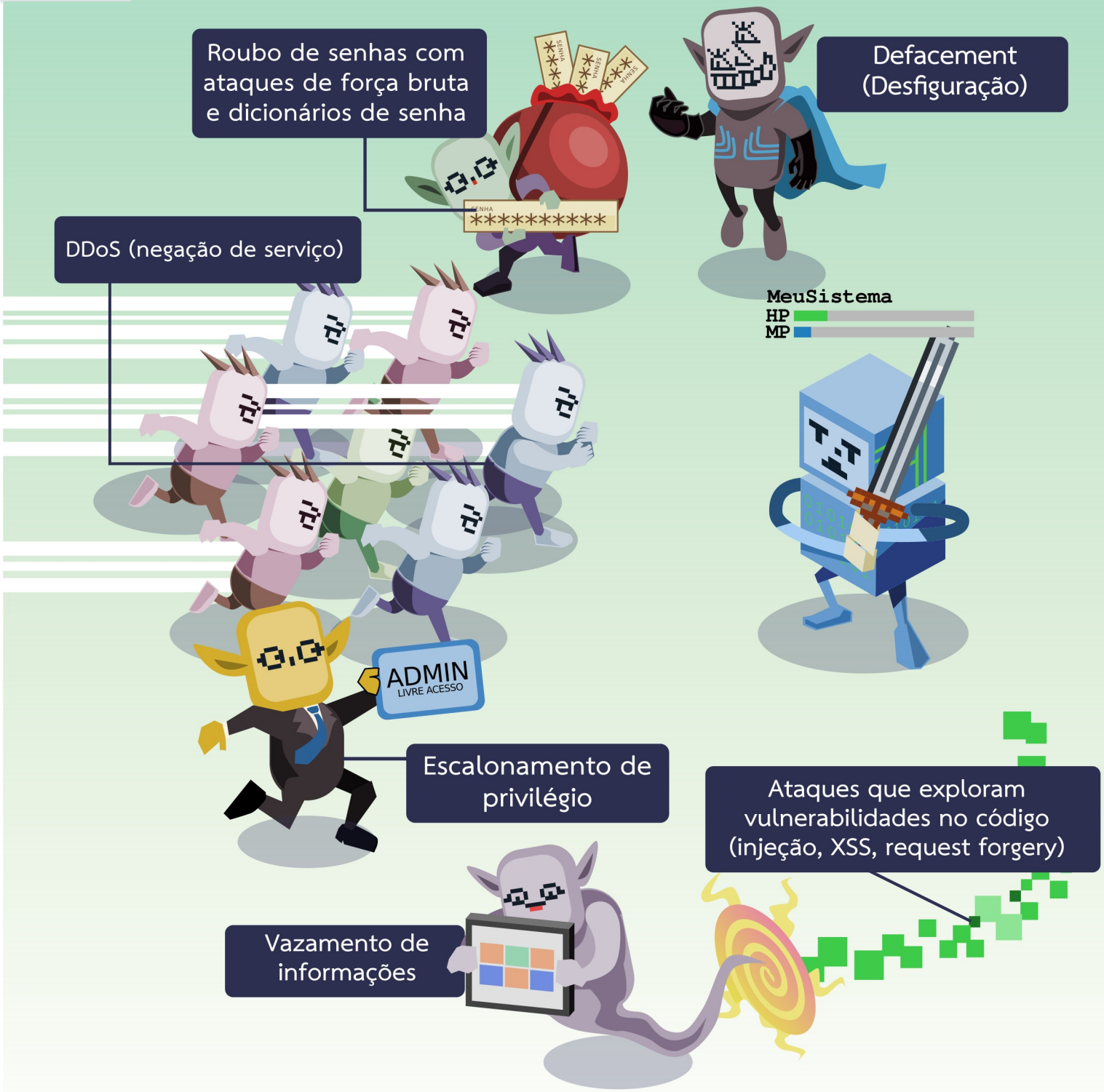
Hospedagem Compartilhada ou Revenda: dezenas a centenas de sites são hospedados num mesmo servidor, o que garante o melhor custo-benefício. Hoje os sistemas são estáveis o suficiente para permitir um serviço de qualidade mesmo nessas condições, porém com menos segurança e sem garantia de recursos.

Hospedagem compartilhada em Cloud: Na prática a "cloud" é somente uma nova arquitetura de um servidor compartilhado. A diferença é que grandes empresas com datacenters ao redor do mundo conseguem prover mais escalabilidade e disponibilidade, controlando melhor a distribuição de recursos. A segurança e privacidade de dados, porém, continua sendo uma questão.

Servidor Virtual (VPS): utilizando virtualização, um mesmo servidor é capaz de executar diversas plataformas simultaneamente, oferecendo na prática "Servidores virtuais" para os . É indicado para aplicações que precisam acesso total ao sistema operacional mas que não precisem de muita capacidade de processamento.

Servidor Dedicado ou colocation: é o serviço mais caro, porém, superior a Hospedagem Compartilhada e ao Servidor Virtual, pois pode-se controlar melhor o servidor. Além de contratar um servidor, é também necessário saber que se necessita gerenciá-lo, o que requer um profissional qualificado, principalmente para gerenciar a segurança do servidor contra crackers. O hardware quando fornecido pelo data center é chamado de Servidor Dedicado, e quando é do cliente é chamado de Colocation.

09 O QUE PODE ACONTECER COM O SEU SITE?



- Seu site pode ficar fora do ar
- Suas informações e as informações de seus usuários podem ser roubadas
- Seu site pode ser alterado para virar uma fonte de malwares e infectar seus usuários
- Seu site pode ser alterado para te ridicularizar ou passar uma mensagem criminosa

FORA DO AR
Silenciamento. Censura. Negação de conteúdo. Essa é a decorrência de um a**taque de Negação de Serviço (o famoso DOS ou DDOS)**.

INFORMAÇÕES VAZADAS
Um site inseguro pode ter várias brechas que permitam a alguém obstinado obter dados sensíveis. Esses dados podem ser divididos em duas categorias: **Vazamento de informação** sobre o site; dados importantes como nome de usuários, senhas, versão de serviços utilizados e acesso não autorizado a dados armazenados em servidor ou no banco de dados. (Esse acesso não autorizado a um banco de dados ou sistema pode ser conseguido **escalonando privilégios** ou adivinhando a senha de um usuário com **ataques de força bruta e dicionário**). Um atacante que consiga acesso ao banco de dados ou ao servidor vai ter acesso irrestrito aos dados dos seus usuários.

SEU SITE PODE SER ALTERADO PARA VIRAR UMA FONTE DE MALWARE
Se aproveitando da falhas na programação do seu site, um atacante pode Injetar comandos e informações maliciosas no seu site, ou até mesmo scripts (o famoso **XSS: Cross Site Scripting**). Com isso os atacantes podem obter informações sensíveis de usuários, senhas e outras características da sessão para acessar e adulterar arquivos não-autorizados. É muito comum atacantes fazerem isso para, a partir do seu servidor, atacar outras pessoas e redes ou servir como uma fonte de malwares cuja finalidade é roubar credenciais financeiras, mandar SPAM ou outros fins que possam gerar ganhos financeiros para o atacante.

SEU SITE PODE SER MODIFICADO
Usando as mesmas técnicas citadas como **XSS, Injeção, request forgery** ou quaisquer técnicas de controle do servidor através de acessos ilegítimos (**escalonamento de privilégios**) um atacante pode alterar o conteúdo do seu site. Isso é conhecido como **Defacement**, ou "Desfiguração" de websites.

MAIS BITS

Que tipo de informações públicas sobre falhas de segurança estão disponíveis para "facilitar" esses ataques?:
Banco de dados de vulnerabilidades: https://cve.mitre.org/
Vulnerabilidades de sites em Wordpress: https://wpvulndb.com/
Banco de dados de scripts prontos para explorar vulnerabilidades: https://www.exploit-db.com/
Scanner de vulnerabilidades para Wordpress: https://wpscan.org/

10 PRINCIPAIS VULNERABILIDADES

Vulnerabilidades são falhas ou atributos específicos de um sistema que são suscetíveis a uma ameaça.

Nenhum sistema está 100% livre de vulnerabilidades, mas sempre que uma vulnerabilidade é identificada deve-se fazer o possível para mitigá-la.

Um exemplo para fixar esses conceitos:

Um GALÃO DE COMBUSTÍVEL é uma **VULNERABILIDADE**

O fogo é a **AMEAÇA**

MITIGAÇÕES
são regras para armazenar material inflamável, ter extintores de incêndio, portas corta-fogo e planos de evacuação.

VULNERABILIDADES MAIS COMUNS

"FORÇA BRUTA" E DICIONÁRIOS DE SENHA

Como funciona esse tipo de ataque

Esses ataques têm como objetivo adivinhar sua senha. Depois que um atacante descobrir ou "chutar" o nome de um usuário (por exemplo, 'Admin'), pode-se configurar um "robô" para ficar tentando adivinhar a senha desse usuário.

Ataques de força bruta combinam caracteres aleatoriamente. (aaaa, aaab, aaac.....zzz). Apesar de demorado, uma senha como 'arara', 'futebol', 'maria' seria relativamente fácil de ser adivinhada nesse método, mesmo que o atacante não tivesse conhecimentos de língua portuguesa. Já uma senha mais longa e que usa números, caracteres especias e letras maiusculas demoraria muito mais para ser adivinhada nesse método.

Dicionários de senha são mais eficientes, pois trabalham com combinações de palavras existentes na sua língua ou que já foram identificadas como senhas válidas. Não é difícil encontrar listas de senhas vazadas de sites frequentemente hackeados como Sony e Yahoo. É muito mais rápido e eficiente fazer um ataque de dicionário com alguns milhares de senhas que são ou já foram usadas do que um ataque de força bruta com centenas de milhares de combinações aleatórias.

https://www.wired.com/2013/04/massive-wordpress-attack-targets-weak-admin-passwords/

https://blog.sucuri.net/2013/04/mass-wordpress-brute-force-attacks-myth-or-reality.html

Como posso me proteger?

Se seu servidor for compartilhado ou nuvem:

Wordfence Security - limit login access time - https://www.wordfence.com/

https://wordpress.org/plugins/limit-login-attempts/

https://ciphercoin.com/wp-login

Se seu servidor for dedicado ou VPS

(FAIL2BAN)
http://www.fail2ban.org/wiki/index.php/Fail2Ban

INJEÇÃO, XSS, REQUEST FORGERY

Como funciona esse tipo de ataque

INJEÇÃO:
O tipo mais comum de injeção é SQL Injection, ocorre quando a aplicação não verifica os valores ou parâmetros de entrada permitindo que sejam inseridos caracteres especiais que alterem o fluxo da consulta SQL no banco de dados e consequentemente executando comandos arbitrários.

XSS:
XSS (Cross-Site Scripting) permite injetar códigos na aplicação web vulnerável para obter informações sensíveis, como nomes de usuário, senhas, cookies, etc. Neste tipo de ataque normalmente é utilizado códigos em linguagem Javascript.

Request forgery:
A vulnerabilidade de CSRF (Cross-Site Request Forgery) ocorre quando é possível se passar por um usuário do site e inserir uma requisição dentro da requisição deste usuário. Para que isso ocorra é necessário que o site ou aplicação esteja vulnerável e nos permita inserir temporariamente algum código, além disso, é necessário construir uma URL que será enviada para o usuário, que deve clicar sobre ela. Ao clicar nesta URL, a requisição inicial será enviada. Mas como existe a vulnerabilidade, em segundo plano será feita a nossa requisição para executar determinada ação.

Como posso me proteger?
A proteção ideal para injeção de código, XSS ou request forgery é programar as aplicações seguindo as melhores práticas de desenvolvimento seguro, ou seja, 'blindar' o seu código para antecipar esse tipo de tentativa. Caso seu site não tenha tido esse cuidado, ou você use plataformas desenvolvidas por terceiros, como Wordpress ou Joomla, deve-se adicionar camadas de segurança adicionais que ajudarão a fazer esse "filtro" de requisições.

Se seu servidor for dedicado ou VPS:
É possível instalar sistemas de monitoramento de requisições web, por exemplo Maltrail, que em conjunto com o Fail2Ban pode banir atacantes conhecidos ou que estão fazendo chamadas suspeitas

https://github.com/stamparm/maltrail#quick-start

Nesse caso também pode-se instalar uma aplicação de proxy reverso. Ainda que o ideal fosse ter um outro servidor dedicado para essa função, utilizar um proxy reverso local com o Nginx ajuda a filtrar requisições maliciosas, atuando como uma camada antes do servidor web.

https://www.infoq.com/br/news/2010/06/proxy-reverso

Se seu servidor for compartilhado:
Pode-se contratar um **WAF** (Web application firewall) externo como o Cloudflare (https://www.cloudflare.com/) ou Incapsula (https://www.incapsula.com/), ambos proprietários e pagos. No caso do Wordpress pode-se instalar plugins simples que oferecerão uma segurança limitada contra esse tipo de ataque. (Wordfence WAF ou Sucuri WAF) com opções pagas e gratuitas.

VAZAMENTO DE INFORMAÇÕES

Vazamento de informação pode ou não ser uma vulnerabilidade. Há dados públicos que estão disponíveis sobre nossos sites, usuários e serviços. Por exemplo, e-mail do responsável pelo domínio, o IP do site, a localização aproximada do servidor, portas abertas... Outras informações, porém, não deveriam estar disponíveis remotamente, tais quais as versões específicas desses sistemas, nomes de usuários, senhas, e-mails de pessoal relacionado...porém devido a configurações incorretas nos aplicativos e sistemas isso pode acontecer.

Algumas dessas informações públicas podem ser consultadas aqui:

https://who.is/

https://www.shodan.io/ -- Internet of thing search engine for vuln tools

https://hackertarget.com/nmap-online-port-scanner/ - Vazamento de portas e protocolos

Como posso me proteger?

Se seu servidor for dedicado ou VPS:
O processo de hardening ou 'blindagem' do seu sistema operacional e web server pode ocultar diversas informações que favoreceriam um atacante.

http://www.tecmint.com/apache-security-tips/

Se seu servidor for compartilhado:
A enumeração remota de usuários é um dos problemas conhecidos de vazamento de informação no Wordpress. Há alguns plugins que podem mitigar esse comportamento.

Stop-user-enumeration (https://wordpress.org/plugins/stop-user-enumeration/) e Wordfence (https://wordpress.org/plugins/wordfence/).

Também é possível bloquear as requisições diretamente no arquivo .htaccess do servidor.

DDOS - NEGAÇÃO DE SERVIÇO

Como funciona esse tipo de ataque
Um ataque de negação de serviço (ou DoS, Denial of Service), é uma tentativa de tornar os recursos de um sistema indisponíveis. Esse ataque procura tornar as páginas hospedadas indisponíveis na internet a partir de uma inundação de acessos concorrentes. O DDOS é a negação de serviço distribuida (Distributed Denial of Services), pois parte de dezenas, centenas ou milhares de origens distintas -- um grande número de máquinas que foram "sequestradas" por um atacante, formando "redes zumbis" (botnets) que, obedecendo a um comando remoto do atacante, fazem uma inundação de acessos ao site. O impacto deste ataque varia entre deixar o sistema lento, derrubá-lo ou sobrecarregar a banda da rede da vítima.

Alguns sites mantem históricos de grandes ataques DDOS. Esses ataques podem assumir um potencial devastador, pois se aproveitam de dispositivos inseguros conectados na internet (como câmeras de vigilância mal configuradas, computadores e até mesmo outros sites infectados). Alguns ataques DDOS foram poderosos o bastante para deixar pequenos países sem internet, derrubar grandes portais e plataformas governamentais. Esses grandes ataques são registrados e estudados.
http://www.digitalattackmap.com/#anim=1&color=0&country=BR&list=1&time=17035&view=map

Meu site foi usado para participar não-intencionalmente de um DDOS?

http://labs.sucuri.net/?is-my-wordpress-ddosing

Como posso me proteger?
O DDOS é um ataque extremamente difícil de impedir, pois não parte de nenhuma falha de configuração do seu site e sim de uma quantidade abusiva de acessos. Há algumas formas de melhorar a resiliência do seu site.

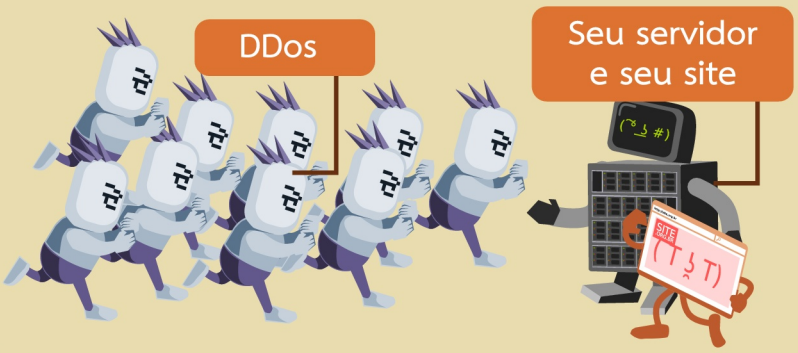
Se seu servidor for dedicado ou VPS:
Há algumas configurações de reforço ou "hardening" do seu sistema operacional e servidor web. Entre eles alguns módulos do apache como mod_security e mod_evasive.

https://techjourney.net/install-mod_evasive-for-apache-to-prevent-ddos-attacks/

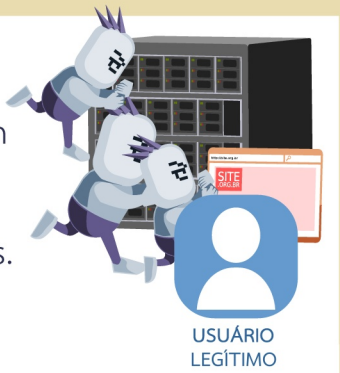
DDoS vs CDN (Content Delivery Network)

CDN (Content Delivery Network) é uma das proteções contra os DDoS, os ataques em massa que derrubam sites para explorar vulnerabilidades.

Ataque DDoS é uma tentativa de derrubar um site através do excessivo tráfego de acesso. São feitos através de "bots", máquinas infectadas que utilizam a rede para sobrecarregar um site.



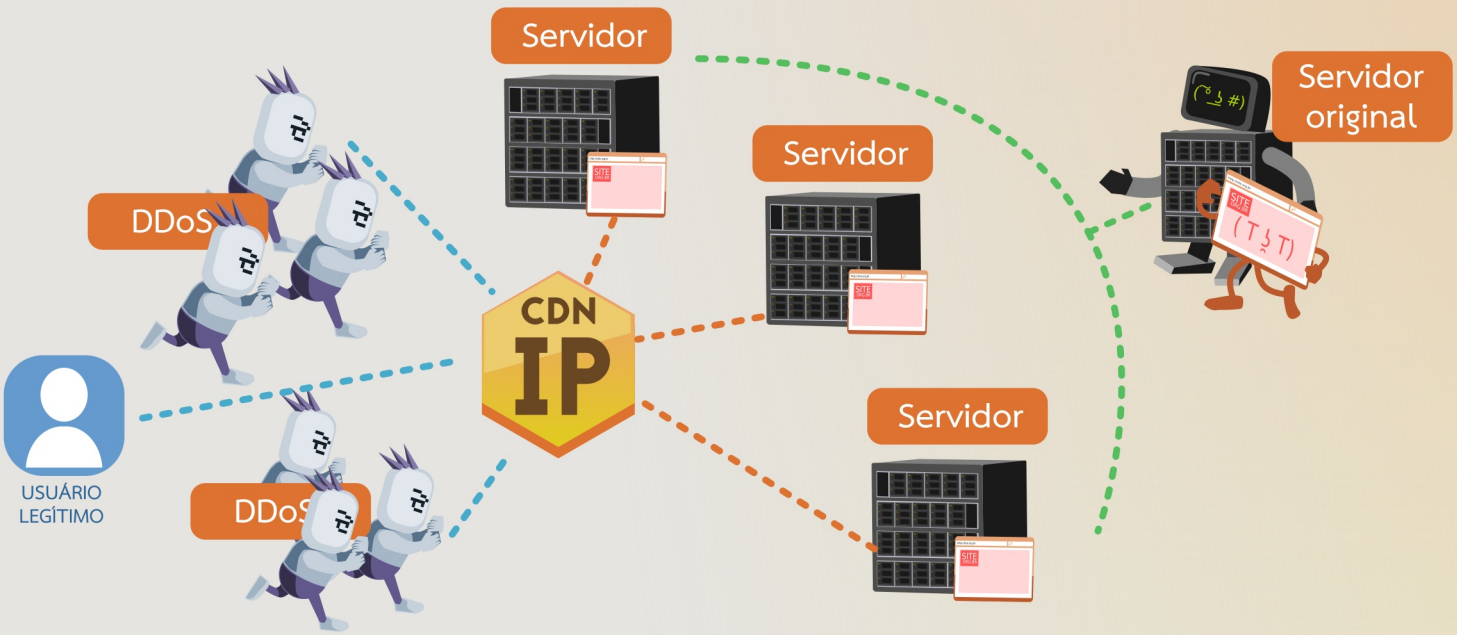
O ataque DDoS mira no servidor de origem do site, derrubando todo tipo de acesso, incluindo os legítimos.



Através de uma CDN (Content Delivery Network) seu site é espelhado e distribuido entre servidores que mantém uma cópia atualizada da última versão.

Essa solução protege seu site e diminui a quantidade de tráfego do seu servidor. Com os usuários sendo direcionados para cópias do site, a origem se mantém protegida dos ataques.

Além de diminuir a latência de reposta do pedido de acesso (os milisegundos para carregar o site), uma CDN redireciona os pedidos de acesso para um endereço IP na rede CDN e entrega o resultado longe da sua verdadeira localização.



Também é possível instalar pacotes de aplicativos livres que monitoram e bloqueiam ativamente conexões suspeitas no caso de um ataque DDOS https://wiki.deflect.ca/wiki/BotnetDBP

Se seu servidor for compartilhado:
Você pode configurar um CDN (content delivery network) para "barrar" a enchente de requisições de um ataque de negação de serviço. Existem planos gratuitos e outros pagos.

http://www.theregister.co.uk/2015/03/11/cloudflare_virtual_dns_ddos_mitigation/

Planos do Cloudflare https://www.cloudflare.com/plans/

CDN Quando sob ataque fica mudando o IP da origem. "Oculta" IP de origem pois adiciona uma camada elástica de proteção

ALTERAÇÕES NÃO AUTORIZADAS NO SITE

Escalonamento de privilégio
O Ataque que visa a escalação de privilégios, normalmente ocorre utilizando-se um erro de lógica na aplicação com o objetivo de obter privilégios para executar alguma tarefa que previamente não estaria autorizados. Estas vulnerabilidades muitas vezes acontecem em aplicações que usam funções para múltiplos usuários.

https://learn.equalit.ie/wiki/Access_Restrictions

11 COMO PROTEGER SEU SITE

SEMPRE MANTENHA OS SISTEMAS ATUALIZADOS!!!

A maioria dos ataques se aproveita de sistemas antigos e desatualizados.

É muito comum que sites Wordpress tenham plugins desatualizados. Por isso é importante que antes de instalar um plugin você faça uma pesquisa para verificar se o plugin é vulnerável ou não. Também sempre os mantenha atualizados e nunca tenha plugins ativos que não estão em uso!

Algumas estatísticas de plugins:
https://sucuri.net/website-security/hacked-reports/Sucuri-Hacked-Website-Report-2016Q2.pdf

https://blog.sucuri.net/2012/03/wordpress-understanding-its-true-vulnerability.html

Servidor VPS ou dedicado:

Hardening do servidor -
https://learn.equalit.ie/wiki/Secure_hosting_guide

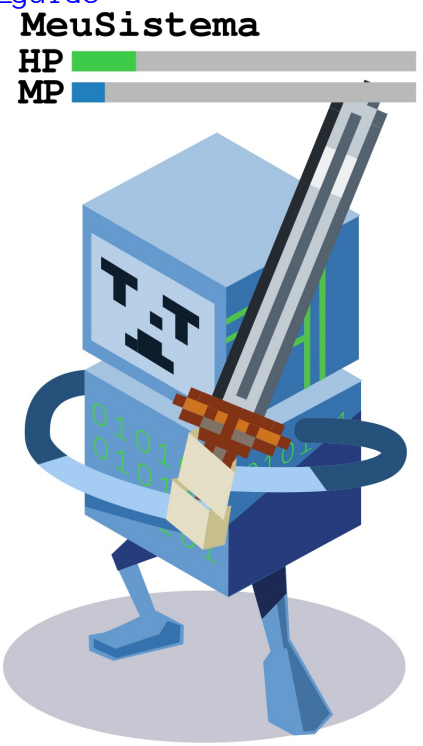
- Sistemas automatizados de backup/clone

Servidor compartilhado:

- Backup (backup do WordPress é diferente do servidor)

- Política de senhas fortes

- Procedimentos e documentações



INFRAESTRUTURA GERAL

https://www.gandi.net/ - **Registrar DNS que não divulga dados desnecessariamente**

https://spideroak.com/ - **Backup criptografado**

https://www.opennicproject.org/ - **Lista de provedores DNS livres**

VPS QUE PERMITEM REINSTALAR E CRIPTOGRAFAR SEU SISTEMA OPERACIONAL

https://tachanka.org/ - **Servidor ativista**

https://greenhost.net/ - **Servidor Holandês com hardware sustentável. Possibilidade de instalar um SO personalizado.**

CDN - CONTENT DELIVERY NETWORKS PARA PROTEÇÃO CONTRA DDOS

https://deflect.ca/ - **CDN distribuida para ativistas e defensores de direitos humanos (Não associada a nenhuma grande empresa)**

http://cloudflare.com - **Serviço comercial com opção gratuita**

https://www.cloudflare.com/galileo/ - **Projeto galileo. CDN gratuito para organizações e atores da sociedade civil mediante aprovação da Cloudflare.**

https://projectshield.withgoogle.com/public/ - **Projeto da Google de CDN gratuita para grupos de mídia, eleições e outras figuras públicas mediante avaliação do projeto.**

WAFS - WEB APPLICATION FIREWALLS (FIREWALLS DE APLICAÇÃO WEB)

http://cloudflare.com - **Serviço comercial, a partir do plano --- tem a opção de WAF**

Sucuri - https://sucuri.net/

FERRAMENTAS DE SEGURANÇA PARA LIDAR COM ATAQUES DE FORÇA BRUTA/DICIONÁRIO/SCANS

Fail2ban - http://www.fail2ban.org/wiki/index.php/Main_Page

BotnetDBP - https://wiki.deflect.ca/wiki/BotnetDBP

Deflect - https://deflect.ca

CRIPTOGRAFIA HTTPS

Certificadora livre (Expira de 3 em 3 meses) - https://letsencrypt.org

Revenda de certificados comerciais para pequenos sites - https://www.namecheap.com/security/ssl-certificates/comodo.aspx

GRANTS E HELPLINES TÉCNICOS

Digital defenders - https://www.digitaldefenders.org/

Frontline defenders - https://www.frontlinedefenders.org/

Access now - https://www.accessnow.org

HARDENING DE SERVIDORES

Configurando servidores Caislean - https://equalit.ie/portfolio/caislean/

LINKS SOCIAIS E BIGDATA

Dataselfie -- Extensão do Chrome que lhe rastreia enquanto você está no Facebook para mostrar a você os dados que gera e como algoritmos de aprendizado de máquina usam esses dados para fazer seu perfil.
http://dataselfie.it/#/

https://facebook.tracking.exposed/ - **Extensão de ff que usa o rastreamento de seus metadado em fb para mostrar como manipula a timeline**

Facebook scanner -- http://stalkscan.com/en/

Matéria sobre Big Data e eleições --
http://outraspalavras.net/posts/big-data-toda-democracia-sera-manipulada/

Matéria questionando a matéria sobre Big Data e eleições --
https://prafalardecoisas.wordpress.com/2017/02/09/nao-provavelmente-o-trump-nao-sabe-mais-sobre-voce-do-que-voce-mesmo/

CONFERÊNCIA ONLINE

https://meet.jit.si/

http://talky.io/

http://hubl.in/

SEGURANÇA

Manual de Facilitação das Brigadas Internacionais de Paz, para compartilhar ferramentas de segurança e proteção a pessoas e organizações de defesas de direitos humanos: http://www.pbi-mexico.org/fileadmin/user_files/projects/mexico/images/News/Reducido_GuiaFacilitacion.pdf

Manual da Tactical Tech sobre Segurança Holística -- muito bacana, sai do modelo de ameaças-proteção simplista usado pelo mercado de segurança para propor uma reflexão mais ampla sobre o que é estar segur@. Se você enviar um e-

mail pedindo uma cópia em papel, a Tactical Tech envia, mas está em inglês. Vamos traduzir? https://holistic-security.tacticaltech.org/

Para botar um linux seguro no USB: https://tails.boum.org/

Holistic Security - https://gendersec.tacticaltech.org/wiki/index.php/Main_Page

http://www.pbi-mexico.org/fileadmin/user_files/projects/mexico/images/News/Reducido_GuiaFacilitacion.pdf

Campanha externa segurança - http://securitycircle.com.br/

Podcast legal sobre segurança da informação --
http://www.segurancalegal.com/
Este episódio fala de endereços DNS, Registro.br e as informações do admnistrador do site a partir do minuto 50min19s. :)
http://www.segurancalegal.com/2016/11/episodio-111-incidente-bancario/

SEGURANÇA DIGITAL PARA SITES

Realização

Apoio

Este projeto foi contemplado pelo Edital
"Redes e Ruas" de Cultura Digital, Inclusão e Cidadania.

Esta apostila foi desenvolvida durante as oficinas de Segurança para Sites de Defesa de Direitos realizadas pela Actantes, com apoio da Open Society Foundation, em fevereiro de 2017.

Está licenciada com uma Licença Creative Commons Atribuição-NãoComercial 4.0 Internacional (http://creativecommons.org/licenses/by-nc/4.0/).