Ética, Profissão e Cidadania

BCC.

Segurança Digital.

25 / 03 / 2021.

Segurança Digital

O conceito de Segurança Computacional "Capacidade de assegurar a prevenção ao acesso e à manipulação ilegítima da informação, ou ainda, de evitar a interferência indevida na sua operação normal"

Objetivos de Segurança

Segurança Digital

Objetivos da Segurança

Confidencialidade — *Garantir que as informações não serão reveladas a pessoas não autorizadas;*

Integridade — *Garantir a consistência dos dados, prevenindo a criação não autorizada e a alteração ou destruição dos dados;*

Disponibilidade — *Garantir que usuários legítimos não terão o acesso negado a informações e recursos;*

Autenticidade — *Garantir que um sujeito usando uma identificação é seu verdadeiro detentor*

Não repudiação — *Garantir que o participante de uma comunicação não possa negá-la posteriormente*

Segurança Digital

Violações

Quando os objetivos de segurança não são alcançados – propriedades não são garantidas – há uma violação da segurança !

- **Revelação não autorizada da informação**
  - Violação da Confidencialidade
- **Modificação não autorizada da informação**
  - Violação da Integridade
- **Negação indevida de serviço**
  - Violação da Disponibilidade

Segurança Digital

Ataques na Internet

Segurança Digital

Motivos de ataques na Internet

Demonstração de poder: mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente

Prestigio: vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar sites considerados visados ou difíceis de serem atacados; disputar com outros atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo.

Segurança Digital

Motivos de ataques na Internet

Motivações financeiras: coletar e utilizar informações confidenciais de usuários para aplicar golpes.

Motivações ideológicas: tornar inacessível ou invadir sites que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia.

Segurança Digital

Motivos de ataques na Internet

Motivações comerciais: tornar inacessível ou invadir sites e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas.

Segurança Digital

Exploração de vulnerabilidades

Vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança

Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.

Segurança Digital

Exploração de vulnerabilidades

Ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas:

Como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível

Segurança Digital

Exploração de vulnerabilidades

Varredura em redes (Scan)

É uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles

Por exemplo, serviços disponibilizados e programas instalados.

Segurança Digital

Exploração de vulnerabilidades

Varredura em redes (Scan)

Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

Segurança Digital

Exploração de vulnerabilidades

Varredura em redes (Scan)

Legítima: por pessoas devidamente autorizadas, para verificar a segurança de computadores e redes e, assim, tomar medidas corretivas e preventivas.

Maliciosa: por atacantes, para explorar as vulnerabilidades encontradas nos serviços disponibilizados e nos programas instalados para a execução de atividades maliciosas.

Segurança Digital

Exploração de vulnerabilidades

Interceptação de tráfego (Sniffing)

Interceptação de tráfego, ou sniffing, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de sniffers.

Segurança Digital

Exploração de vulnerabilidades

Interceptação de tráfego (Sniffing)

Legítima: por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados.

Maliciosa: por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

Segurança Digital

Exploração de vulnerabilidades

Força bruta (Brute force)

Um ataque de força bruta, ou brute force, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário.

Segurança Digital

Exploração de vulnerabilidades

Força bruta (Brute force)

Se um atacante tiver conhecimento do seu nome de usuário e da sua senha ele pode efetuar ações maliciosas em seu nome como, por exemplo:

trocar a sua senha, dificultando que você acesse novamente o site ou computador invadido;
invadir o serviço de e-mail que você utiliza e ter acesso ao conteúdo das suas mensagens e à sua lista de contatos, além de poder enviar mensagens em seu nome;

Segurança Digital

Exploração de vulnerabilidades

Força bruta (Brute force)

acessar a sua rede social e enviar mensagens aos seus seguidores contendo códigos maliciosos ou alterar as suas opções de privacidade;
invadir o seu computador e, de acordo com as permissões do seu usuário, executar ações, como apagar arquivos, obter informações confidenciais e instalar códigos maliciosos.

Segurança Digital

Exploração de vulnerabilidades

Desfiguração de página (Defacement)

Desfiguração de página, defacement ou pichação, é uma técnica que consiste em alterar o conteúdo da página Web de um site.

As principais formas:

- **explorar erros da aplicação Web;**
- **explorar vulnerabilidades do servidor de aplicação Web;**
- **explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação Web;**

Segurança Digital

Exploração de vulnerabilidades

Desfiguração de página (Defacement)

As principais formas:

invadir o servidor onde a aplicação Web está hospedada e alterar diretamente os arquivos que compõem o site;

furtar senhas de acesso à interface Web usada para administração remota.

Segurança Digital

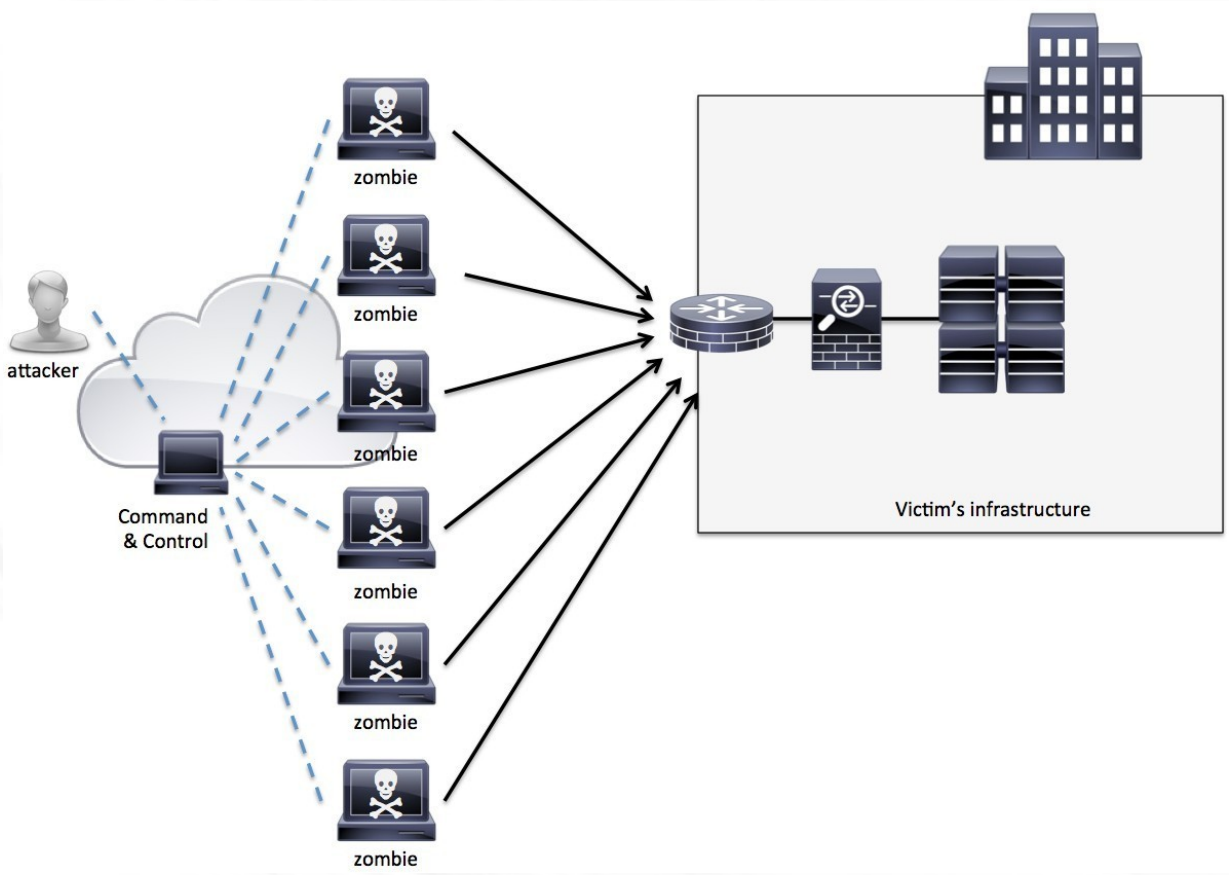
Exploração de vulnerabilidades

Negação de serviço (DoS e DDoS)

Negação de serviço, ou DoS (Denial of Service), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (Distributed Denial of Service).

Segurança Digital



The Case for Securing Availability and the DDoS Threat https://
www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html

Segurança Digital

Exploração de vulnerabilidades

Negação de serviço (DoS e DDoS)

O objetivo destes ataques não é invadir e nem coletar informações, mas sim exaurir recursos e causar indisponibilidades ao alvo.

Quando isto ocorre, todas as pessoas que dependem dos recursos afetados são prejudicadas, pois ficam impossibilitadas de acessar ou realizar as operações desejadas.

Segurança Digital

Exploração de vulnerabilidades

Negação de serviço (DoS e DDoS)

Uma pessoa pode voluntariamente usar ferramentas e fazer com que seu computador seja utilizado em ataques.

A grande maioria dos computadores, porém, participa dos ataques sem o conhecimento de seu dono, por estar infectado e fazendo parte de botnets

Segurança Digital

Exploração de vulnerabilidades

Negação de serviço (DoS e DDoS)

Podem ser realizados por diversos meios, como:

pelo envio de grande quantidade de requisições para um serviço, consumindo os recursos necessários ao seu funcionamento (processamento, número de conexões simultâneas, memória e espaço em disco, por exemplo) e impedindo que as requisições dos demais usuários sejam atendidas;

Segurança Digital

Exploração de vulnerabilidades

Negação de serviço (DoS e DDoS)

Podem ser realizados por diversos meios, como:

pela geração de grande tráfego de dados para uma rede, ocupando toda a banda disponível e tornando indisponível qualquer acesso a computadores ou serviços desta rede;

Segurança Digital

Exploração de vulnerabilidades

Negação de serviço (DoS e DDoS)

Podem ser realizados por diversos meios, como:

pela exploração de vulnerabilidades existentes em programas, que podem fazer com que um determinado serviço fique inacessível

Segurança Digital

Códigos maliciosos (Malware)

Segurança Digital

Códigos maliciosos (Malware)

São programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

Algumas das diversas formas:

- **pela exploração de vulnerabilidades existentes nos programas instalados;**
- **pela autoexecução de mídias demovíveis infectadas, como Pen- drives;**

Segurança Digital

Códigos maliciosos (Malware)

Algumas das diversas formas:

pelo acesso a páginas Web maliciosas, utilizando navegadores vulneráveis;
pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;

Segurança Digital

Códigos maliciosos (Malware)

Algumas das diversas formas:

pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

Segurança Digital

Vírus

É um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

O vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado.

Segurança Digital

Vírus

Vírus propagado por e-mail: recebido como um arquivo anexo a um e-mail cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado.

Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os e-mails encontrados nas listas de contatos gravadas no computador.

Segurança Digital

Vírus

Vírus de script: escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página Web ou por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML.

Pode ser automaticamente executado, dependendo da configuração do navegador Web e do programa leitor de e-mails do usuário.

Segurança Digital

Vírus

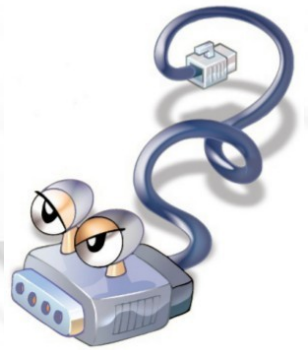
Vírus de macro: tipo específico de vírus de script, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros).

Segurança Digital

Worm

É um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o worm não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores.



Segurança Digital

Worm

Worms são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores.

Segurança Digital

O que são vírus de computador e worm de computador?

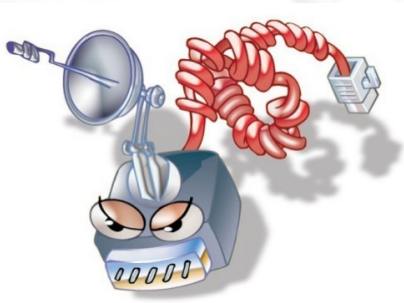
https://www.kaspersky.com.br/resource-center/threats/computer-viruses-vs-worms

Segurança Digital

Bot e botnet

Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente.

Possui processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.



Segurança Digital

Bot e botnet

A comunicação entre o invasor e o computador infectado pelo bot pode ocorrer via canais de IRC, servidores Web e redes do tipo P2P, entre outros meios.

Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar spam.

Segurança Digital

Bot e botnet

Um computador infectado por um bot costuma ser chamado de zumbi (zombie computer), pois pode ser controlado remotamente, sem o conhecimento do seu dono.

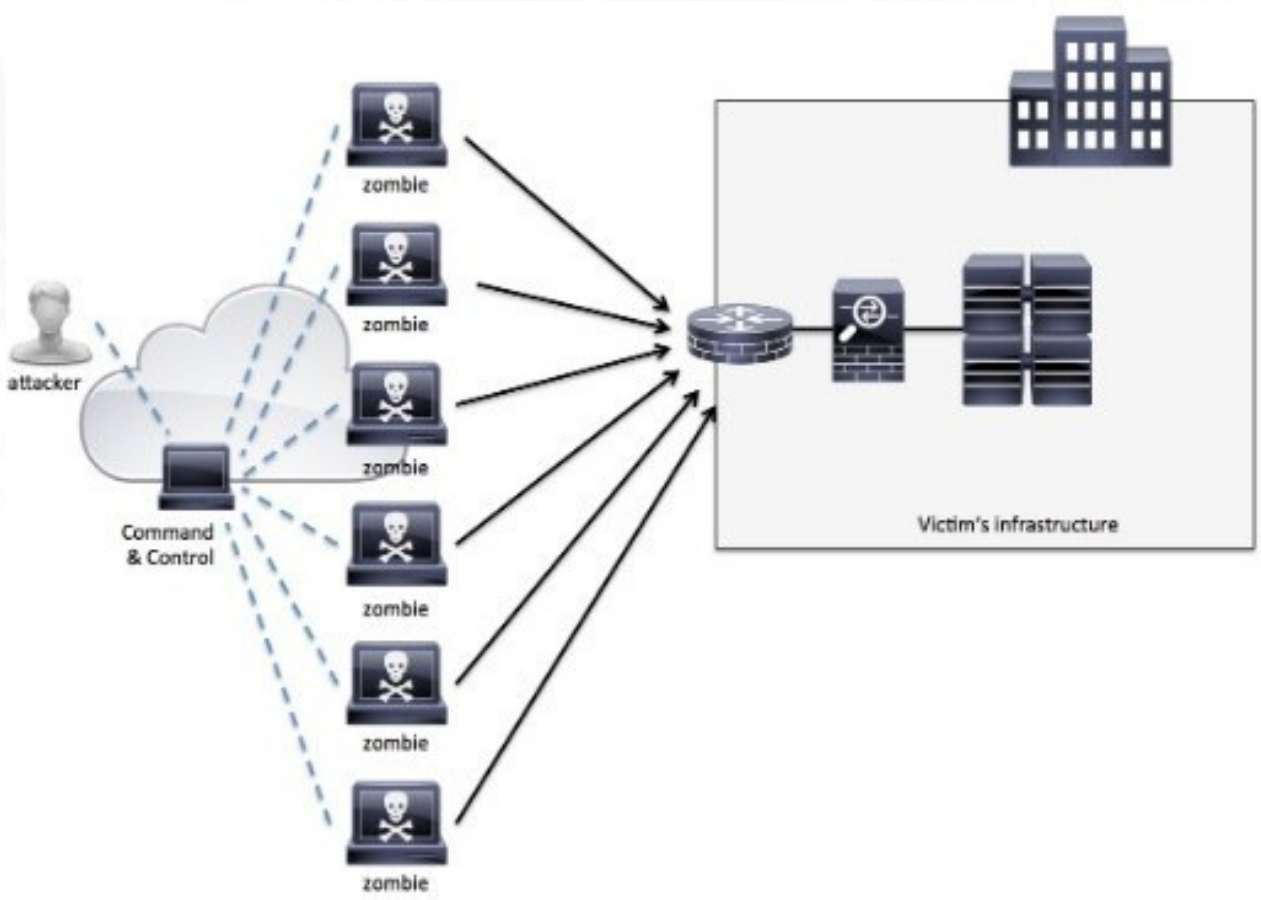
Também pode ser chamado de spam zombie quando o bot instalado o transforma em um servidor de e-mails e o utiliza para o envio spam.

Segurança Digital

Bot e botnet

Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots.

Segurança Digital



The Case for Securing Availability and the DDoS Threat https://
www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html

Segurança Digital

Spyware

Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Segurança Digital

Spyware

***Keylogger*:** capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um *site* específico de comércio eletrônico ou de *Internet Banking*.

Segurança Digital

Spyware

***Screenlogger*:** similar ao *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou a região que circunda a posição onde o *mouse* é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em *sites* de *Internet Banking*.

Segurança Digital

Spyware

***Adware*:** projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.

Segurança Digital

Backdoor

É um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados par

Segurança Digital

Cavalo de troia (Trojan)

É um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Segurança Digital

Rootkit

É um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

Segurança Digital

Acesso não autorizado

Um acesso autorizado a um sistema computacional é considerado autorizado quando a pessoa que o executou tem um conta válida no sistema

Conta criada pelo administrador do sistema por força de um relacionamento maior e anterior: usuário é um empregado de uma empresa ou um estudante de uma escola

Segurança Digital

Acesso não autorizado

Além da posse de uma conta válida a pessoa usa o computador respeitando as regras existentes, inclusive éticas

Tentar executar funções do administrador, ler ou danificar arquivos de outros usuários ou usar o computador para obter acesso não autorizado a outros computadores, são exemplos de desrespeito a essas regras.

Segurança Digital

Acesso não autorizado

O que é considerado Hacking?

Um hacker é uma pessoa que acessa sistemas computacionais sem autorização

O hacker pode ter uma intenção criminosa ou pelo simples prazer de invadir um sistema

Segurança Digital

Acesso não autorizado

O que é considerado Hacking?

A conotação da palavra hacker tem um sentido mais pejorativo, mas há uma conotação um pouco mais antiga

Hacker foi usado para designar um profissional extremamente talentoso e dedicado, que procura vencer desafios relacionados aos computadores, desenvolver projetos altamente complexos e conhecer todos os detalhes internos dos computadores e de seu software básico

Referências

Masiero, Paulo Cesar. Ética em Computação. EDUSP: São Paulo, SP, Brasil. 2000, 213p.

Livro da Cartilha de Segurança para Internet – Cert.br

https://cartilha.cert.br/livro/