MBA USP ESALQ

Fundamentos da Segurança da Informação

Rodolfo Ipolito Meneguette

*A responsabilidade pela idoneidade, originalidade e licitude dos conteúdos didáticos apresentados é do professor.

AGENDA

- Apresentação do professor;
- Introdução;
- conceitos sobre segurança;
- tipos de ataques;
- princípios de uma política de segurança.

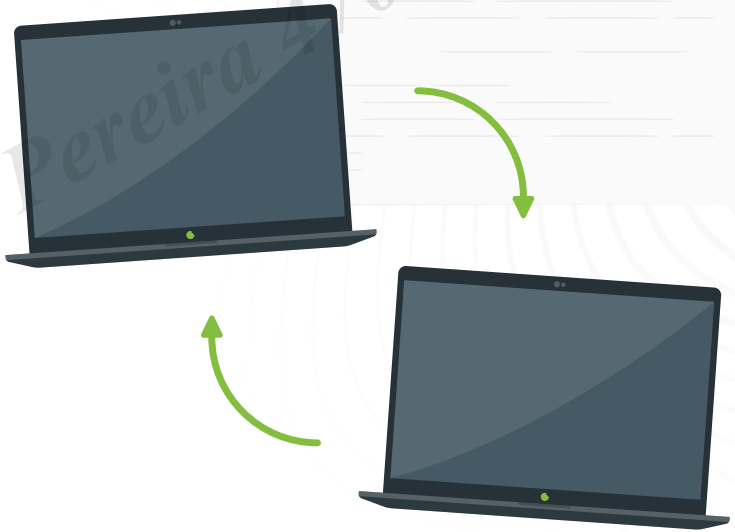
APRESENTAÇÃO DO PROFESSOR

- Formação;
- Experiência com segurança;
- Linha de Pesquisa.

INTRODUÇÃO

Computadores são mais úteis ligados em rede, compartilhando informação e recursos.

- Com mais de 7 bilhões de dispositivos IoT conectados hoje, os especialistas esperam que esse número cresça para 10 bilhões em 2020 e 22 bilhões em 2025. [1]



[1] https://www.oracle.com/br/internet-of-things/what-is-iot/#:~:text=Com%20mais%20de%207%20bilhões,e%2022%20bilhões%20em%202025

Microsoft nega violação e roubo de 30 milhões de contas de usuários

Responsável pela suposta violação e roubo de dados, grupo hacktivista Anonymous Sudan já fez a Microsoft de vítima antes

Microsoft confirma ataque hacker que afetou milhões de usuários

A Microsoft confirmou ter sofrido ataque hacker por falhas no Azure e Outlook

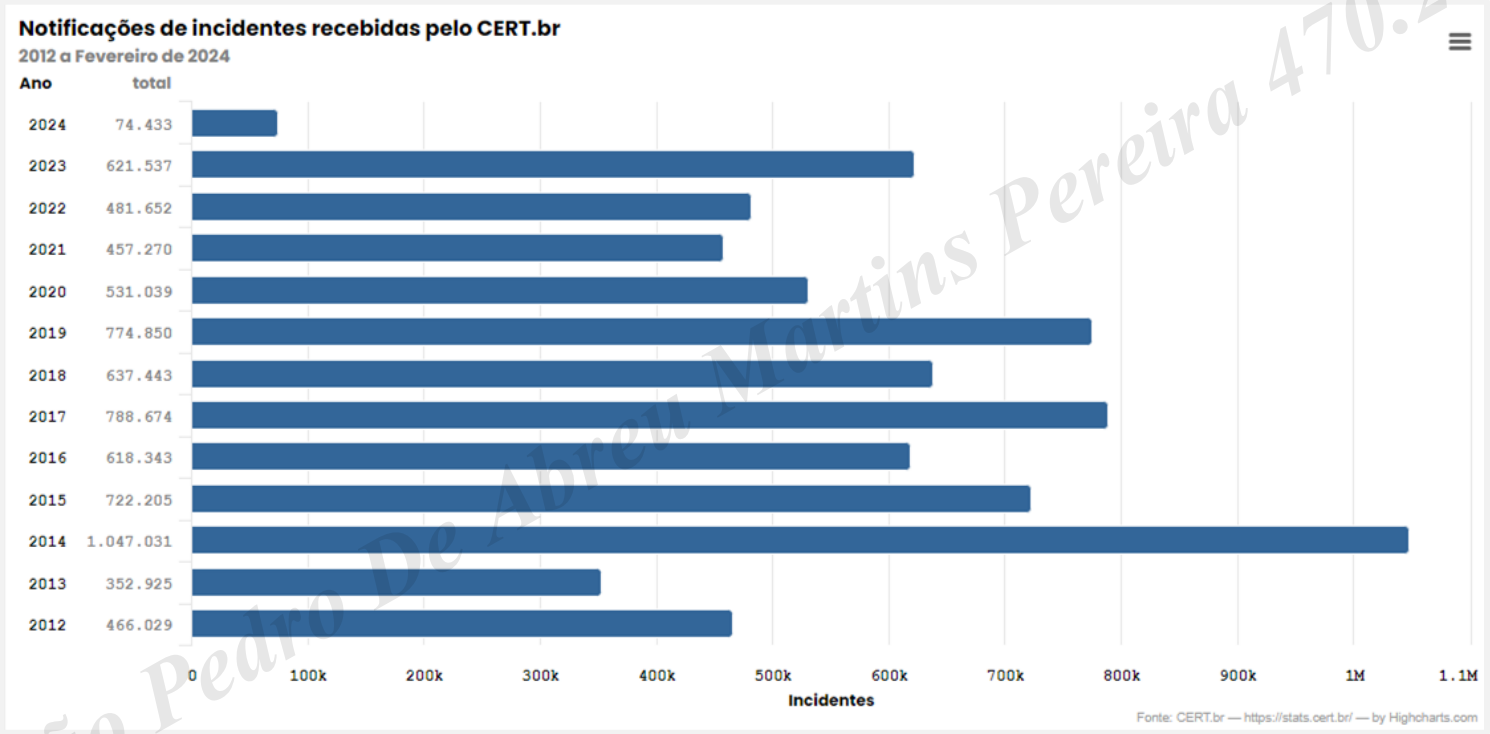
SEGURANÇA

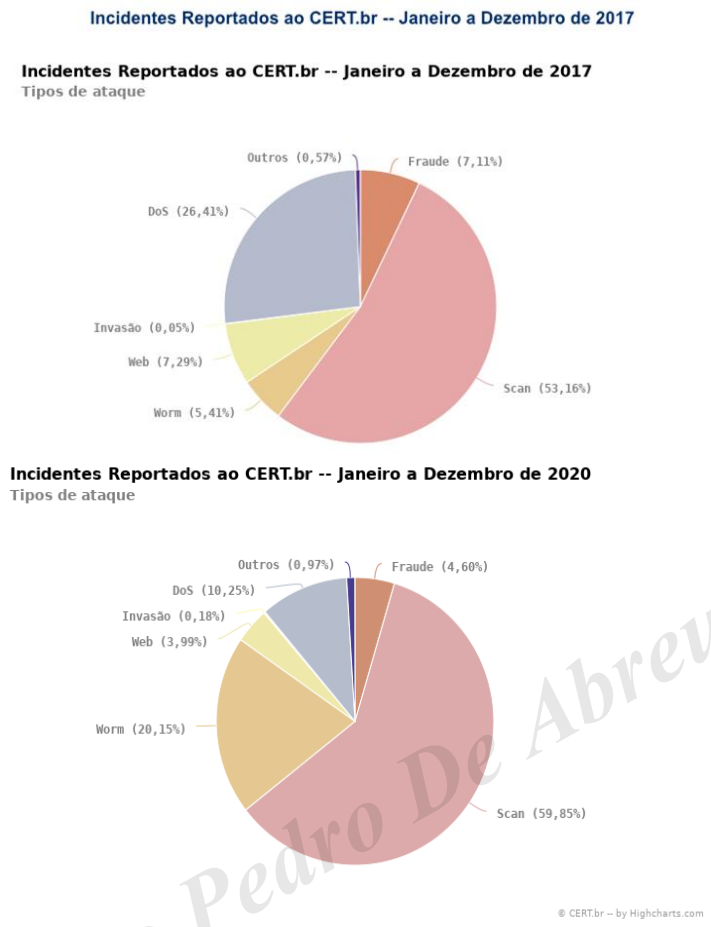
Carro da Tesla foi hackeado: entenda os riscos para os carros autônomos

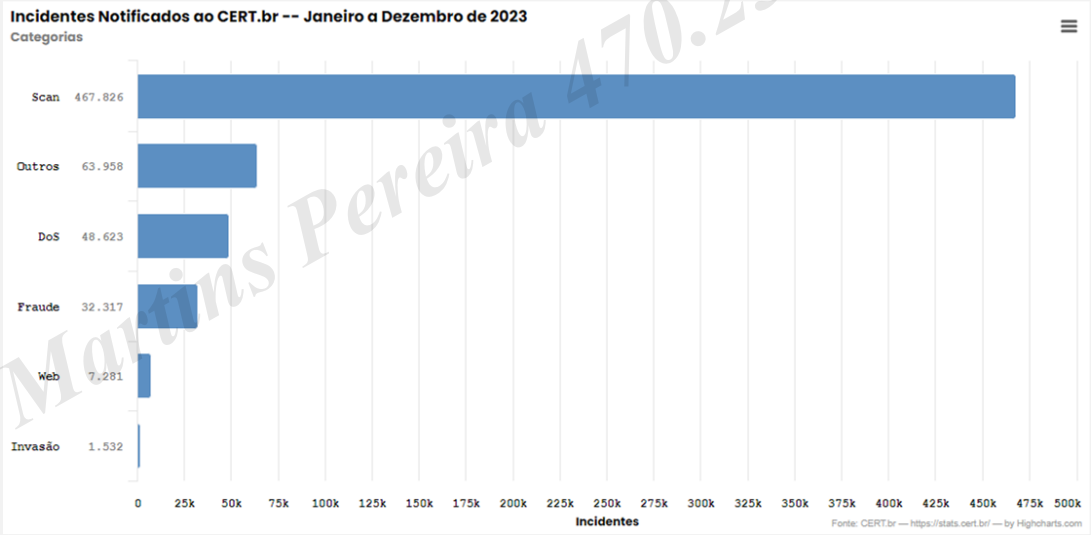
Airbus inicia investigação após hacker vazar dados da empresa

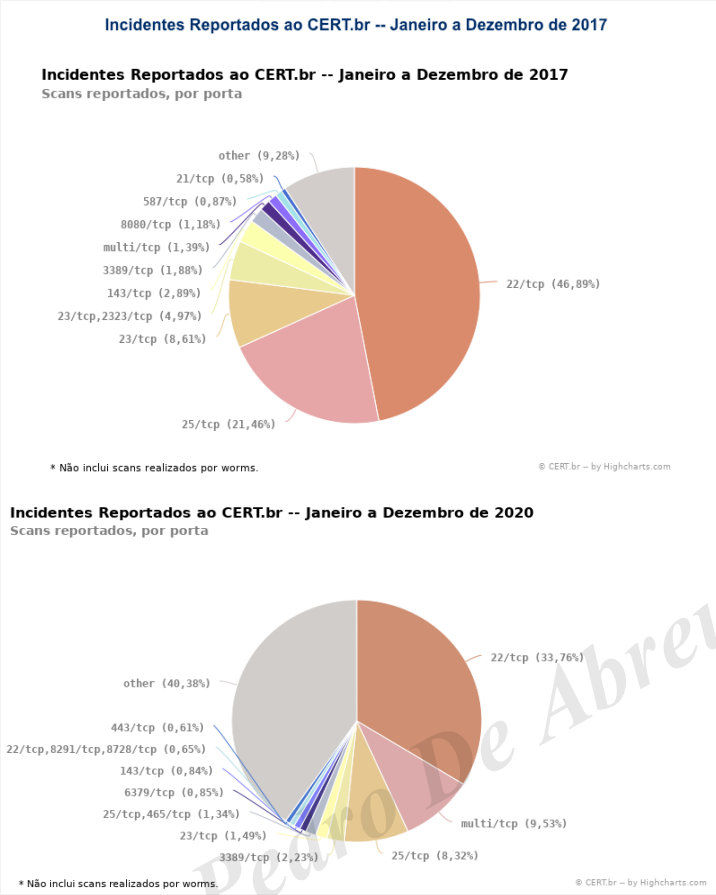
A fabricante de aviões iniciou uma investigação depois que um hacker afirmou ter violado os sistemas da empresa e vazado alguns documentos comerciais

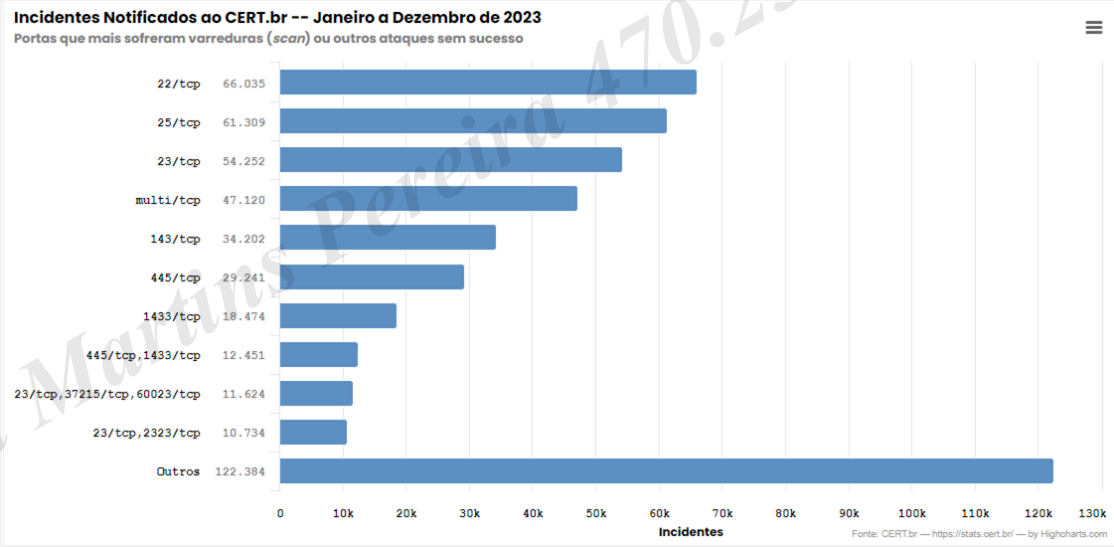
NÚMEROS DE 2012-2024

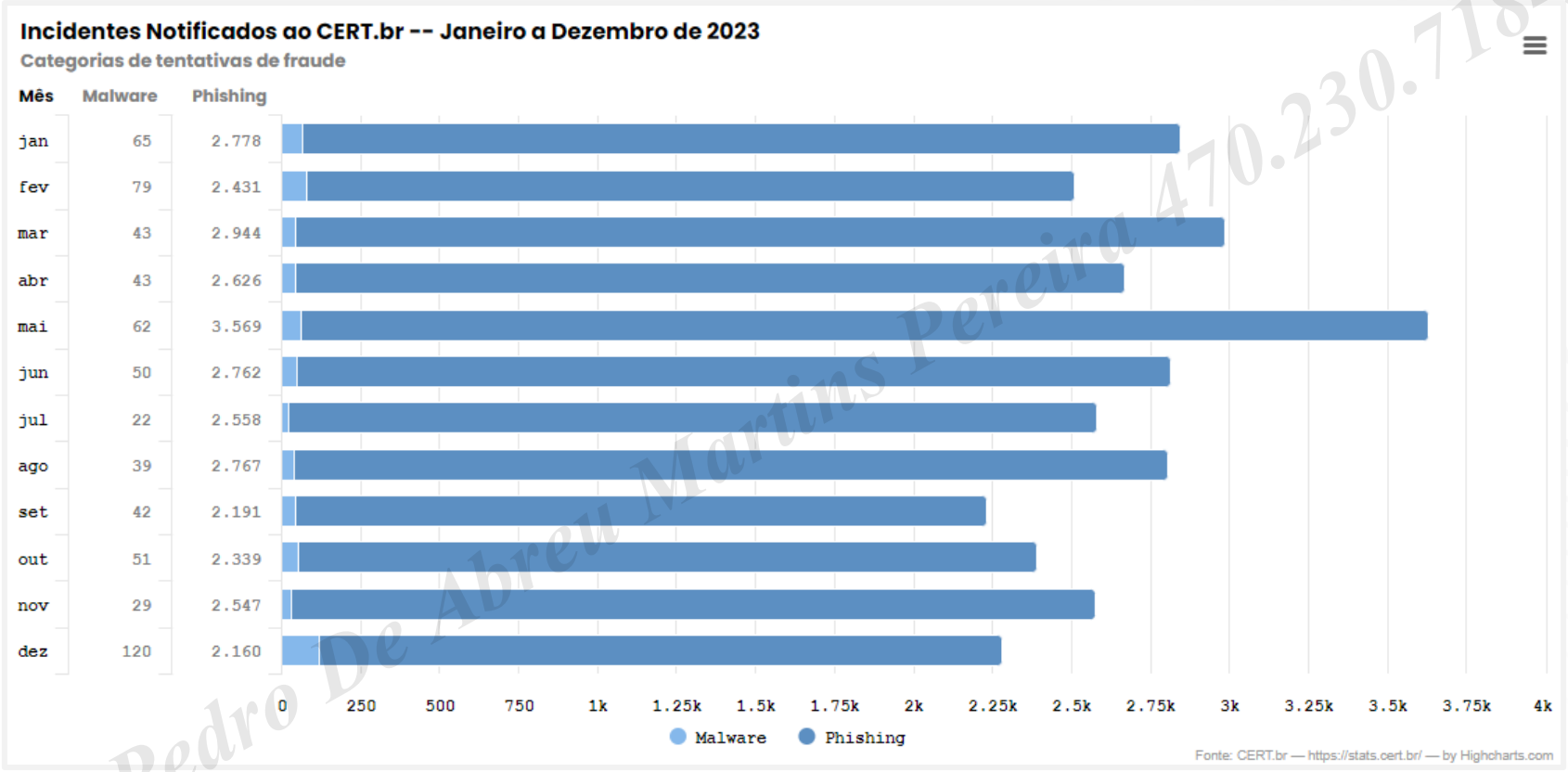












SEGURANÇA

O QUE É SEGURANÇA?

A segurança de um sistema, aplicação ou protocolo é sempre relacionada à:

- Conjunto de propriedades desejadas;
- Um adversário com capacidades específicas.

SEGURANÇA

IMPORTÂNCIA DA SEGURANÇA

- Proteção de patrimônio (em especial: informação);
- Vantagem competitiva;
- Cumprimento de responsabilidades;
- Continuidade de operação/atividade.

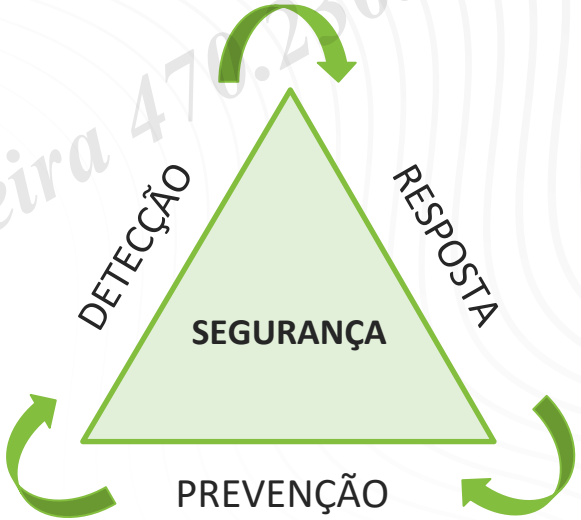
Segurança da informação = proteção + integridade + disponibilidade + autenticação.

SEGURANÇA

PRÁTICA: Prevenção, Detecção e Resposta.

Toda segurança é relativa, pode ser tomada em níveis e deve ser um balanceamento:

- Custo da segurança × valor do patrimônio.
- Provável × possível.
- Necessidades de segurança × do negócio.



SEGURANÇA

ANÁLISE DE RISCO

- Identificar e priorizar valores (patrimônio);
- Identificar vulnerabilidades;
- Identificar ameaças e suas probabilidades;
- Identificar contramedidas (respostas);
- Desenvolver análise de custo-benefício;
- Planejar políticas e procedimentos de segurança.
  - Políticas e procedimentos de segurança.

SEGURANÇA

ELEMENTOS E REQUISITOS DE SEGURANÇA

Confidencialidade: proteção da informação contra descoberta ou interceptação não autorizada; privacidade.

Integridade: impedir informação/transmissão de ser alterada/danificada de forma ñ-autorizada, imprevista ou acidental.

Disponibilidade: confiabilidade de redes, sistemas e equipamentos sobre evitar ou se recuperar de interrupções.

CONFIDENCIALIDADE

SEGREDO, OCULTAÇÃO, ENCOBRIMENTO DE INFORMAÇÕES OU RECURSOS

Necessária em áreas sensíveis:

- Instituições civis ou militares (governamentais) compartimentalizam informações -> need to know.
- Acesso restrito àqueles que necessitam dela.

Ex.: companhias com projetos proprietários.

CONFIDENCIALIDADE

- Mecanismo de suporte:
  - Criptografia.
- Implementação do mecanismo de suporte:
  - Criptografia.
- A chave controla o acesso;
- Precisa-se proteger a confidencialidade da chave!
- Problemas... Ex.: WEP;
- Aplica-se à existência de dados.
  - Comunicações cifradas de extra-terrestres.

CONFIDENCIALIDADE

ASPECTO IMPORTANTE: ocultação de informações

- Equipamentos de uma organização;
- Configurações;
- Versões de sistemas e aplicações.

Mecanismos para garanti-la dependem de **Serviços de suporte confiáveis e premissas**:

- Kernel é capaz de lidar com o serviço;
- Agentes provêm dados corretos;
- Ambiente não comprometido.

INTEGRIDADE

- Confiança nos dados ou recursos;
- Relacionada à prevenção de mudanças;
- impróprias ou não-autorizadas;
- Integridade dos dados:
  - O conteúdo da informação não foi alterado.

INTEGRIDADE DA ORIGEM:

- Fonte de dados (autenticação).
  - Precisão, credibilidade e confiança na informação.

INTEGRIDADE

ASPECTO IMPORTANTE: credibilidade!

Ex.: jornal imprime informação obtida de um vazamento do Palácio do Planalto e atribui à fonte errada (integridade dos dados, mas não da origem).

Mecanismos podem ser divididos em **2 classes**:

- **Prevenção;**
- **Detecção.**

INTEGRIDADE

MECANISMOS DE PREVENÇÃO:

- Mantêm a integridade pelo bloqueio de qualquer tentativa não-autorizada de modificação dos dados ou tentativas de modificar o dado de maneira não autorizada.

Usuário tenta mudar dado sem autoridade para tal.

Usuário autorizado tenta mudar dado de outras maneiras não correspondentes a sua autorização.

Ex.: intruso mexer nos registros de um contador vs. contador sonegar impostos.

INTEGRIDADE

MECANISMOS DE DETECÇÃO:

- Alertam que a integridade dos dados não foi preservada (sem credibilidade).

Garantia depende de premissas sobre a fonte e confiança nesta fonte.

Avaliação inclui corretude e confiança do dado.

- Como e de quem foi obtido?
- O caminho do dado foi protegido?
- O destino do dado é protegido?

DISPONIBILIDADE

Habilidade de se usar a informação ou recurso desejado.

Aspecto importante da confiabilidade e projeto de um sistema:

- Sistema indisponível é tão ruim quanto um sistema inexistente;
- Alguém pode deliberadamente negar acesso a um dado ou serviço, tornando-o indisponível.

DISPONIBILIDADE

Ex.: projetos de sistemas podem assumir um modelo estatístico para analisar padrões de uso esperado (garantidos por mecanismos).

Se esse uso é manipulado (tráfego de rede), a premissa não é mais válida -> falha.

- Mecanismo para manter o recurso/dado disponível não suporta um ambiente para o qual ele não foi projetado.
- *Ex.: conexões do Apache*.

DISPONIBILIDADE

Tentativas de bloquear a disponibilidade são difíceis de se detectar:

- O padrão de acesso incomum é uma anomalia momentânea, uma falha de dispositivo/recurso ou um ataque proposital?

Se um sistema indisponível é essencial para o funcionamento de outro, a negação do serviço ocorre em cascata (e.g., interface de consulta e banco de dados remoto).

SEGURANÇA

ELEMENTOS E REQUISITOS DE SEGURANÇA

Identificação e Autenticação: distinguir, determinar e validar a identidade do usuário/entidade (se é quem diz ser).

Controle de acesso: limitar/controlar nível de autorizações de usuários/entidades a uma rede, sistema ou informação.

Não-repúdio: impedir que seja negada a autoria ou ocorrência de um envio ou recepção de informação.

AMEAÇAS E ATAQUES

VULNERABILIDADE

- Fraqueza inerente de um elemento do sistema;
- Brecha: ponto fraco ou falha que pode ser explorado.

AMEAÇA

- Qualquer coisa que possa afetar ou atingir o funcionamento, operação disponibilidade, integridade da rede ou sistema.

ATAQUE

- Técnica específica usada para explorar uma vulnerabilidade.

CONTRAMEDIDAS

- Técnicas ou métodos usados para se defender contra ataques, ou para fechar ou compensar vulnerabilidades.

AMEAÇAS E ATAQUES

VULNERABILIDADES

Principais origens:

- Deficiência de projeto: brechas no hardware/software;
- Deficiência de implementação: instalação/configuração incorreta, por inexperiência, falta de treinamento ou desleixo;
- Deficiência de gerenciamento: procedimentos inadequados, verificações e monitoramento insuficientes.

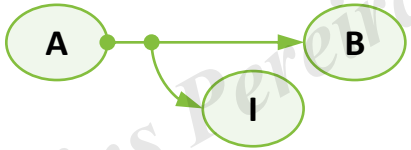
Exemplos:

- Instalação física: má proteção física de equipamentos e mídia;
- Hardware e Software: situações não previstas, limites, bugs no projeto, deixando brechas que podem ser exploradas.

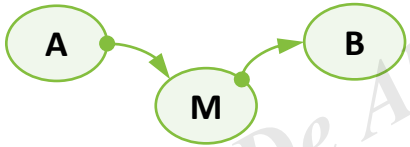
Humana: desleixo, preguiça, estupidez, ganância, revolta etc.

AMEAÇAS NA SEGURANÇA

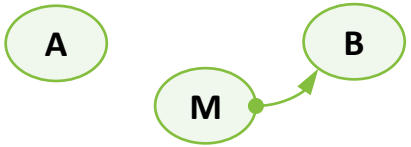
Interrupção



Intercepção



Modificação



Fabricação

FLUXO NORMAL

Fonte de Informação

Destino da Informação

AMEAÇAS E ATAQUES

ATAQUES

Ataques sobre o fluxo de informação.

- **Interrupção:** ataca a disponibilidade;
- **Interceptação:** ataca a confidencialidade;
- **Modificação:** ataca a integridade;
- **Fabricação:** ataca a autenticidade.

PASSIVO

Interceptação, monitoramento, análise de tráfego (origem, destino, tamanho, frequência).

ATIVO

Adulteração, fraude, reprodução (imitação), bloqueio.

MOTIVAÇÃO PARA UM ATAQUE

DINHEIRO
- Venda dos dados;
- Extorsão.

PODER
- Insegurança;
- Medo.

VINGANÇA
- Ciúmes.

FAMA E CURIOSIDADE
- Facilidade de iniciar.

OPORTUNIDADE E DIFICULDADE FINANCEIRA
- Aumento de ataques a pessoas;
- Sobrevivência;
- Novo emprego.

PASSOS DE UM ATAQUE

Um ataque consiste de um **conjunto de etapas** para ter sucesso:

- Reconhecimento e enumeração;
- Ganho de acesso (intrusão);
- Manutenção do controle (persistência);
- Ocultação de traços (limpeza);
- Fazer o alvo trabalhar para o atacante.

Mapeamento entre sistema e Indivíduo.

RECONHECIMENTO E ENUMERAÇÃO

LEVANTAMENTO DE DADOS DO ALVO:

SISTEMA

Footprint

- *Scan – nmap;*
- Topologia da rede, serviços, SO, Versões;
- Funcionamento da empresas (funcionários, acessos).

Fingerprint

- Versão de protocolo;
- Buscar explot *https://www.exploit-db.com*

CLASSES DE ATAQUES

DISSEMINAÇÃO/EXPOSIÇÃO (*Disclosure*)

- Acesso não autorizado à informação;
- Ataques:
  - Phishing;
  - Sniffer.

ENGANAÇÃO (*Deception*)

- Aceitação de dados falsos/forjados;
- Ataques:
  - Roubo de identidade;
  - Repúdio (falar que pagou a mercadoria para receber).

CLASSES DE ATAQUES

DISRUPÇÃO (*Disruption*)

- Interrupção da operação “normal”;
- Ataques.
  - Atraso;
  - Negação de serviço;
  - Manter a pessoa ocupada.

USURPAÇÃO (*Usurpation*)

- Controle não autorizado de um sistema (ou parte dele);
- Ataques.
  - Roubo de identidade;
  - Atraso e negação de serviço.

TIPOS DE ATAQUES

OBTENÇÃO DE INFORMAÇÕES

- Engenharia Social;
- Phishing;
- Packet Sniffing;
- Scanning;
- Spoofing.

TIPOS DE ATAQUES

CÓDIGOS MALICIOSOS (*Malware*)

- Vírus;
- Worms;
- Cavalos de Tróia;
- Adware e Spyware Backdoors;
- Keyloggers e Screenloggers;
- Bots e Botnets Rootkits.

TIPOS DE ATAQUES

NEGAÇÃO DE SERVIÇO (DoS)
E ATAQUES COORDENADOS (DDoS)

- Sobrecarga no poder; computacional;
- Sobrecarga na rede;
- Sobrecarga nos atendimentos; de conexão simultânea.

ENGENHARIA SOCIAL

Método de ataque onde alguém **faz uso da persuasão**, explorando a ingenuidade ou a confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Pessoas se passando por empresas ou pessoas conhecidas para capturar informações.

- Ataques tipo “força bruta”.
  - Montar dicionário.

PHISHING

Tipo de fraude que se dá por meio do **envio de mensagem não solicita**da, passando-se por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários. Também conhecido como phishing scam ou phishing/scam.

- Mensagens que contêm links para programas maliciosos;
- Páginas de comércio eletrônico ou Internet Banking falsificadas.

PACKET SNIFFING

Técnica que consiste na **captura de informações valiosas diretamente pelo fluxo de pacotes**. Também conhecida como passive eavesdropping.

Sniffer – dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores.

- Há diversos softwares com essa capacidade, como o tcpdump, fornecido com o Linux, o Ethereal e o Wireshark.

SCAN

São ferramentas utilizadas para **obtenção de informações referentes aos serviços** que são acessíveis e definidas por meio do mapeamento das portas **TCP** e **UDP**.

O intuito desse tipo de ataque é evitar o desperdício de esforço com ataques a serviços inexistentes.

- O **nmap** é um dos port scanners mais utilizados e pode ser empregado para realizar a auditoria do firewall e do IDS.

SPOOFING

Ataque onde o sujeito autentica um host para outro se utilizando da técnica de **forjar pacotes originários de um host confiável**.

Os principais e mais largamente utilizados tipos de *spoofing* são:

- IP Spoofing;
- ARP Spoofing;
- DNS Spoofing.

IP SPOOFING

A pessoa que irá realizar o spoofing tem então dois problemas na verdade:

- Alterar o IP origem;
- Manter a seqüência de números.

Como exemplo, tem-se o spoofit, o mendax, o seq_number, o ipspoof e outros, todos em C, o que significa que **podem ser executados em várias plataformas**, dependendo apenas de uma compilação correta.

ARP SPOOFING

Variação do IP spoofing que se aproveita do mesmo tipo de vulnerabilidade, diferenciando-se apenas por **utilizar o endereço físico ou MAC** (*Media Access Control*).

O host atacante envia um mapa com informações erradas ao ARP cache remoto.

- O tempo em que uma entrada dinâmica permanece no ARP cache, que é muito curto, desfazendo então a informação errada inicialmente implantada.

DNS SPOOFING

É uma fraude na **associação entre os nomes e os identificadores dos computadores/serviços na Internet**.

Nome.

*Ex. um host está em uma rede que "sofre" de envenenamento de DNS pode ser **redirecionado para uma página fraudulenta** quando solicitar o identificador de www.bancodobrasil.com.br para um servidor.*

DNS SPOOFING

IDENTIFICADORES (mensagem)

- Esta técnica é muito simples e não requer grandes conhecimentos do TCP/IP.

- Consiste em se alterar as tabelas de mapeamento de *host name – IP address* dos servidores DNS, de maneira que os servidores, ao serem perguntados pelos seus clientes sobre um hostname qualquer, informam o IP errado, ou seja, o do host que está aplicando o DNS spoofing.

Tipos de Ataques - Códigos Maliciosos

Código malicioso ou Malware (Malicious Software) – termo que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador.

EXEMPLOS:

- Vírus;
- Worms;
- Backdoors.

Tipos de Ataques - Códigos Maliciosos

CLASSIFICAÇÕES:

Dependência de hospedeiro:

- Dependentes (vírus, bombas lógicas e backdoors);
- Independentes (worms e zumbis).

Replicação:

- Não se replicam (bombas lógicas, backdoors e zumbis);
- Se replicam (vírus e worms).

Tipos de Ataques - Vírus

Programa ou parte de programa que **se propaga infectando**, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador.

O vírus **depende da execução do programa ou arquivo hospedeiro** para que possa se tornar ativo e dar continuidade ao processo de infecção.

Tipos de Ataques - Vírus

Normalmente o vírus tem **controle total sobre o computador**, podendo fazer de tudo, desde mostrar uma mensagem de "feliz aniversário", até alterar ou destruir programas e arquivos do disco.

Para que um computador seja infectado por um vírus, é preciso que um programa previamente infectado seja executado. Isto pode ocorrer de diversas maneiras, tais como:

Tipos de Ataques - Vírus

Existem vírus que procuram permanecer ocultos, infectando arquivos do disco e **executando uma série de atividades sem o conhecimento do usuário**.

Um vírus propagado por e-mail (*e-mail borne vírus*) normalmente é recebido como **um arquivo anexado** à uma mensagem de correio eletrônico.

- O conteúdo dessa mensagem procura induzir o usuário a clicar sobre o arquivo anexado, fazendo com que o vírus seja executado.

Tipos de Ataques - Vírus

VÍRUS DE MACRO

- Para que o vírus possa ser executado, o arquivo que o contém precisa ser aberto e, a partir daí, o vírus pode executar uma série de comandos automaticamente e infectar outros arquivos no computador.

- Existem alguns aplicativos que possuem arquivos base (modelos) que são abertos sempre que o aplicativo é executado. Caso este arquivo base seja infectado pelo vírus de macro, toda vez que o aplicativo for executado, o vírus também será.

Tipos de Ataques – Cavalo de Tróia

Programa, normalmente recebido como um "presente" (um cartão virtual, um álbum de fotos, um protetor de tela, um jogo, etc), que além de executar funções para as quais foi aparentemente projetado, **executa outras normalmente maliciosas e sem o conhecimento do usuário**.

Algumas das funções maliciosas que podem ser executadas por um cavalo de Tróia são:

- instalação de ***keyloggers*** ou ***screenloggers***;
- furto de senhas e outras informações sensíveis, como números de cartões de crédito.

Tipos de Ataques – Cavalo de Tróia

Por definição, o cavalo de Tróia distingue-se de um vírus ou de um worm por **não infectar outros arquivos**, nem propagar cópias de si mesmo automaticamente.

Normalmente um cavalo de Tróia consiste em **um único arquivo que necessita ser explicitamente executado**.

Tipos de Ataques – Cavalo de Tróia

- É necessário que o cavalo de Tróia seja executado para que se instale em um computador;

- Ele geralmente vem anexado a um e-mail ou está disponível em algum site na Internet na forma de cartões virtuais animados, álbuns de fotos de alguma celebridade, jogos, protetores de tela, etc;

- Enquanto estão sendo executados, estes programas podem ao mesmo tempo **enviar dados confidenciais para outro computador**.

Tipos de Ataques – Adware e Spyware

ADWARE (*Advertising software*) – tipo de software **especificamente projetado para apresentar propagandas**, seja através de um browser, seja através de algum outro programa instalado em um computador.

São normalmente **incorporados a softwares e serviços**, constituindo uma forma legítima de patrocínio ou retorno financeiro para quem desenvolve software livre ou presta serviços gratuitos.

Exemplo: versão gratuita do Opera.

Tipos de Ataques – Adware e Spyware

SPYWARE – termo utilizado para se referir a uma grande categoria de software que tem o objetivo de **monitorar atividades de um sistema e enviar as informações coletadas para terceiros**.

- Existem adwares que também são considerados um tipo de spyware, pois são projetados para monitorar os hábitos do usuário durante a navegação na Internet, direcionando as propagandas que serão apresentadas.

- Os spywares, assim como os adwares, podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

Tipos de Ataques – Adware e Spyware

Algumas **funcionalidades implementadas** em *spywares*, que podem ter relação com o uso legítimo ou malicioso:

- Monitoramento de URLs acessadas enquanto o usuário navega na Internet;
- Alteração da página inicial apresentada no browser do usuário;
- Varredura dos arquivos armazenados no disco rígido do computador.

Tipos de Ataques – Backdoors

Programa que **permite o retorno de um invasor a um computador comprometido**, utilizando serviços criados ou modificados para este fim.

É comum um atacante procurar garantir uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na invasão.

- Na maioria dos casos, também é intenção do atacante **poder retornar sem ser notado**.

Tipos de Ataques – Backdoors

A forma usual de inclusão de um backdoor consiste na **disponibilização de um novo serviço ou substituição por uma versão alterada**, normalmente possuindo recursos que permitam acesso remoto (através da Internet).

- Pode ser incluído por um invasor ou através de um **cavalo de Tróia**.

Tipos de Ataques – Backdoors

A existência de um *backdoor* não depende necessariamente de uma invasão.

Alguns dos casos onde **não há associação com uma invasão** são:

- instalação através de um *cavalo de Tróia*;
- inclusão como consequência da instalação e má configuração de um programa de administração remota.

Tipos de Ataques – Keyloggers

Programa capaz de **capturar e armazenar a informação das teclas digitadas pelo usuário** em um computador.

Dentre as informações capturadas podem estar um texto de e-mail, dados da declaração de imposto de renda e outras informações sensíveis, como senhas bancárias e números de cartões de crédito.

- Normalmente, a ativação do *keylogger* é **condicionada a uma ação prévia do usuário**, como por exemplo, após o acesso a um site específico de comércio eletrônico ou Internet Banking.

Tipos de Ataques – Keyloggers

Normalmente, o keylogger contém **mecanismos que permitem o envio automático das informações capturadas** para terceiros (por exemplo, através de e-mail).

As instituições financeiras desenvolveram teclados virtuais para evitar que os *keyloggers* pudessem capturar informações sensíveis de clientes. Como resposta, foram desenvolvidos os ***screenloggers***, que são capazes de:

- Armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado.

Tipos de Ataques – Screenloggers

Programas capazes de **escutar, salvar e compartilhar o Estado total ou parcial da tela** (*printscreen*).

A partir de cliques, por exemplo;

- Utilizado para driblar os teclados virtuais.

Tipos de Ataques – Worm

Programa capaz de **se propagar automaticamente através de redes**, enviando cópias de si mesmo de computador para computador.

- Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos **e não necessita ser explicitamente executado para se propagar**.

- Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

Tipos de Ataques – Worm

Geralmente, o *worm* não tem como consequência os mesmos danos gerados por um vírus, como por exemplo a infecção de programas e arquivos ou a destruição de informações. Isto não quer dizer que não represente uma ameaça à segurança de um computador, ou que não cause qualquer tipo de dano.

Worms são notadamente responsáveis por **consumir muitos recursos**. Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar.

Bots e Botnets

BOT – programa capaz se propagar automaticamente (modo similar ao *worm*), explorando vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador.

- Adicionalmente ao *worm*, **dispõe de mecanismos de comunicação com o invasor**, permitindo que o *bot* seja **controlado remotamente**.

Bots e Botnets

- O invasor, ao se conectar ao mesmo *servidor de IRC* e entrar no mesmo canal, envia mensagens compostas por sequências especiais de caracteres, que são interpretadas pelo bot.

- Estas sequências correspondem a instruções que devem ser executadas pelo bot.

Bots e Botnets

Um invasor, ao se comunicar com um bot, pode **enviar instruções** para que ele realize diversas atividades, tais como:

- Desferir ataques na Internet;
- Executar um ataque de negação de serviço.

Bots e Botnets

BOTNETS – redes formadas por computadores infectados com bots.

- Podem ser compostas por centenas ou milhares de computadores;

- Um invasor que tenha controle sobre uma *botnet* pode utilizá-la para **aumentar a potência de seus ataques**, por exemplo, para enviar milhares de e-mails de *phishing* ou *spam*, desferir ataques de negação de serviço, etc.

Bots e Botnets

Identificar a presença de um *bot* em um computador não é uma tarefa simples.

Normalmente, o *bot* é projetado para realizar as instruções passadas pelo invasor **sem que o usuário tenha conhecimento**.

- Embora alguns programas antivírus permitam detectar a presença de bots, isto nem sempre é possível.

Rootkits

ROOTKIT – conjunto de programas que fornece mecanismos para que um invasor possa **esconder e assegurar a sua presença no computador comprometido**.

- O nome *rootkit* não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root ou Administrator*) a um computador, mas sim para mantê- lo.

Rootkits

O invasor, após instalar o *rootkit*, terá acesso privilegiado **sem precisar recorrer novamente aos métodos utilizados na invasão**, e suas atividades serão escondidas do responsável e/ou dos usuários do computador.

Um rootkit pode fornecer ferramentas com as mais diversas funcionalidades, podendo ser citados:

- Programas para esconder atividades e informações deixadas pelo invasor (normalmente presentes em todos os *rootkits*), tais como arquivos, diretórios, processos, conexões de rede, etc.

Spam

Termo usado para se referir a mensagens (não Necessariamente e-mail) não solicitadas, mas geralmente enviadas para um grande número de pessoas.

- São utilizados para **propagar malwares ou páginas falsas** (*phishing*) que copiam dados de usuários.

Negação de Serviço (DoS)

NEGAÇÃO DE SERVIÇO (*Denial of Service - DoS*) – o atacante utiliza **um computador** para tirar de operação um serviço ou computador(es) conectado(s) à Internet. Exemplos deste tipo de ataque são:

- Gerar uma **sobrecarga no processamento de um computador**, de modo que o usuário não consiga utilizá-lo;
- Gerar um **grande tráfego de dados para uma rede**, ocasionando a indisponibilidade dela; Indisponibilizar serviços importantes de um provedor, impossibilitando o acesso de seus usuários.

Negação de Serviço (DoS)

DDoS (*Distributed Denial of Service*) – ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.

- Normalmente, procuram **ocupar toda a banda disponível para o acesso a um computador ou rede**, causando grande lentidão ou até mesmo indisponibilizando qualquer comunicação com este computador ou rede.

Negação de Serviço (DoS)

Cabe ressaltar que se uma rede ou computador sofrer um *DoS*, isto não significa que houve uma invasão, pois **o objetivo de tais ataques é indisponibilizar o uso de um ou mais computadores**, e não invadi-los.

No exemplo citado, as empresas não tiveram seus computadores comprometidos, mas ficaram impossibilitadas de vender seus produtos durante um longo período.

EXEMPLOS

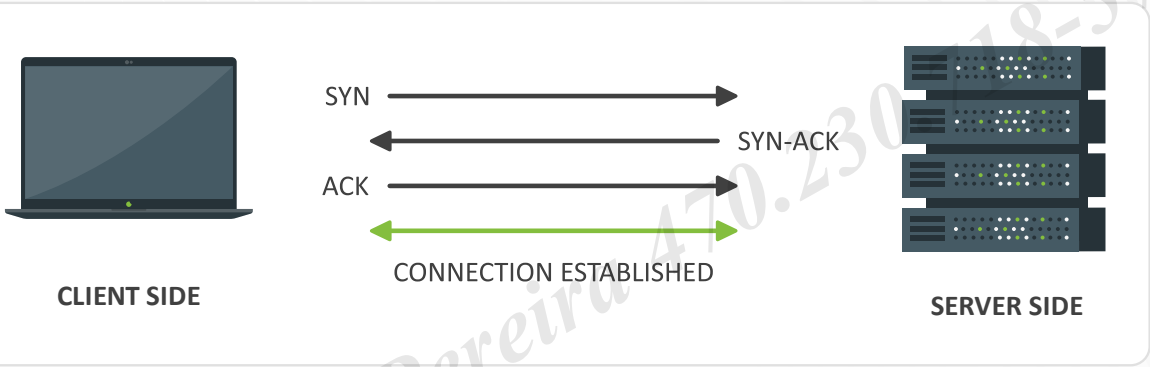
INTERRUPÇÃO DE SERVIÇO (*DoS - Denial of Service*)

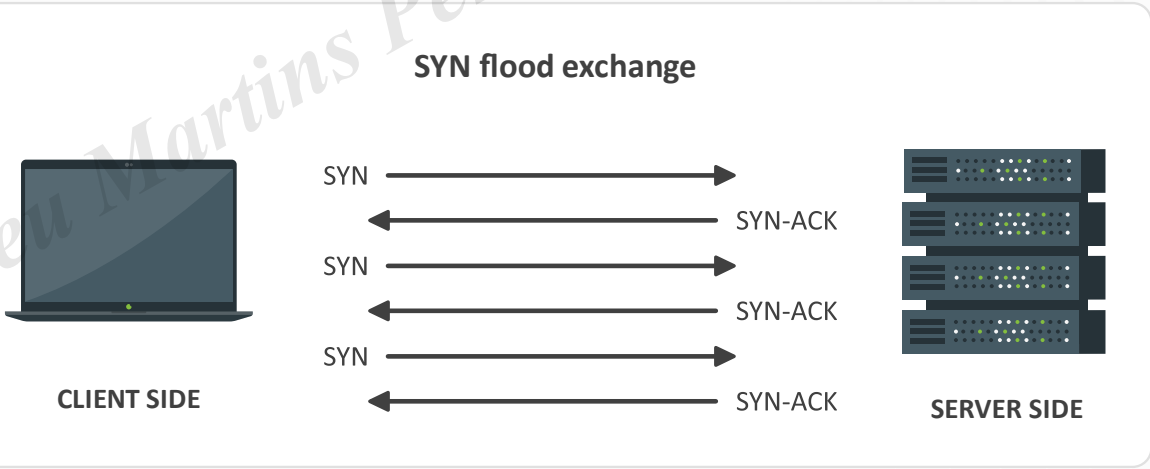
SYN Flooding (Inundação de *SYN*)

- Ataca o handshake de 3-vias do estabelecimento de conexão TCP: cliente envia bit *SYN* (*synchronize sequence number*), servidor reconhece e responde com *SYN-ACK*, cliente reconhece a resposta enviando ACK e inicia a transferência de dados;
- Ataque: enviar *SYNs* e não responder aos *SYN-ACK*, deixando em aberto os estabelecimentos de conexão até ocupar todos os buffers de conexão no servidor;
- Outros clientes não conseguem estabelecer conexões legítimas e o ataque pode derrubar o sistema operacional se a situação consumir toda a memória livre do servidor.

AMEAÇAS E ATAQUES

SYN Flooding (cont.)





EXEMPLOS

INTERRUPÇÃO DE SERVIÇO (*DoS - Denial of Service*)

PING DA MORTE (*Ping of Death*)

- De aplicação simples, baseado em vulnerabilidade;
- Ping: comando TCP/IP que envia um pacote IP p/ um endereço, para testar se existe e está “vivo”;
- Vulnerabilidade: sistemas que não tratam adequadamente pacotes ICMP (pacote de controle a nível de IP) maiores do que o normal;
- Ataque: enviar seqüência de ping com campo ICMP de tamanho máximo (maior que o comum).

EXEMPLOS

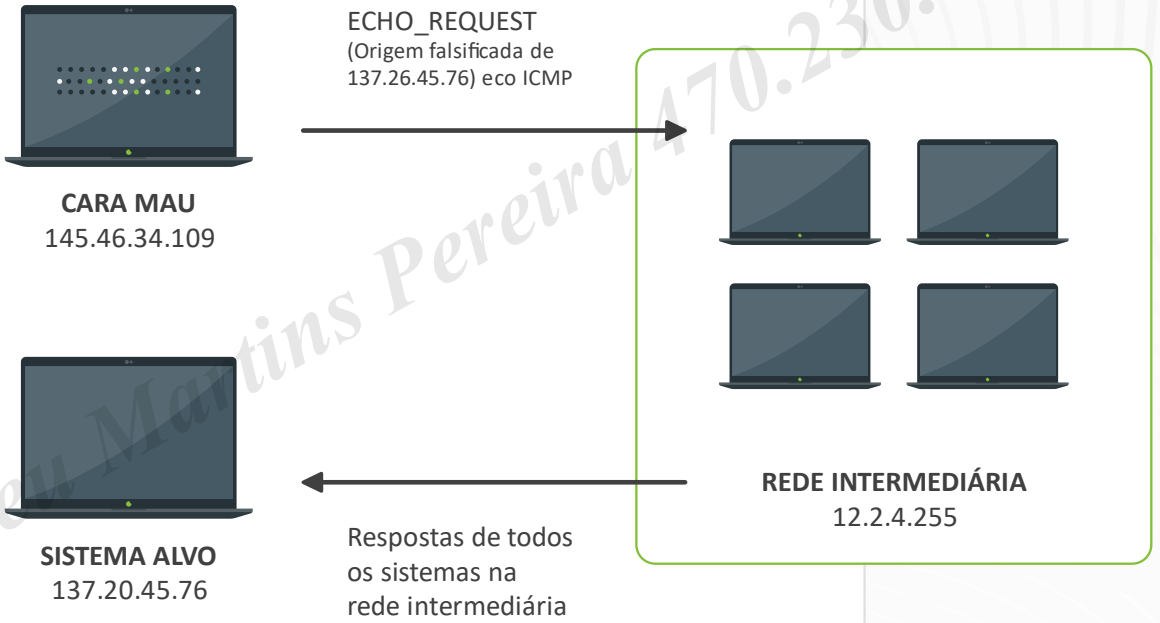
INTERRUPÇÃO DE SERVIÇO (*DoS - Denial of Service*)

SMURF

- Atacante envia um *ECHO_REQUEST ICMP* geral fazendo *spoof* do endereço origem como o endereço IP da máquina alvo = solicita uma resposta (eco) *ICMP* a todas as máquinas de uma rede, fingindo ser a máq. Alvo;
- Todas as máquinas da rede respondem para a máquina alvo real, sobrecarregando a rede e o sistema alvo.

AMEAÇAS E ATAQUES

SMURF (cont.)



FORMAS DE PROTEÇÃO

- Antivírus;
- Anti spam;
- Anti spyware;
- Atualização do sistema;
- Política de segurança.

PRINCÍPIOS DE SEGURANÇA

ECONOMY OF MECHANISM

Esse princípio foca na **simplicidade do projeto e da implementação das medidas de segurança**.

- Enquanto aplicável a maioria dos empreendimentos de engenharia, a noção de simplicidade é especialmente importante no domínio de segurança, uma vez que um simples **framework de segurança** facilita o entendimento aos desenvolvedores e usuários permitindo desenvolvimento e validação eficientes.

FAIL-SAFE DEFAULTS

Esse princípio diz que a configuração padrão (*default*) de um sistema deve ter um **esquema de proteção** conservador.

- Por exemplo, quando adicionar um novo usuário no sistema operacional, o grupo *default* deve conter um mínimo de direitos de acesso a arquivos e serviços. Infelizmente, sistemas operacionais e aplicações frequentemente apresentam opções que focam mais na usabilidade em detrimento a segurança;
- Esse é o caso para um número grande de aplicações populares, tais como *browsers* da web que permitem a execução de códigos baixados de servidores web.

COMPLETE MEDIATION

A ideia por detrás desse princípio é que cada acesso a um recurso deve ser checado para o **cumprimento de um regime de proteção**.

- Como consequência, deve-se ter o cuidado de técnicas de melhoria de desempenho que salvam os resultados dos controles de autorização anteriores, uma vez que as permissões podem mudar ao longo do tempo;
- Por exemplo, um *web site* de um banco on-line deve requerer que usuários façam login novamente após um determinado tempo (em geral 15 minutos é o intervalo definido).

OPEN DESIGN

De acordo com esse princípio, a arquitetura de segurança e **projeto** de um sistema devem ser **disponibilizados ao público**.

- Segurança deve se preocupar apenas em manter as chaves criptográficas secretas;
- Projeto aberto permite que o sistema seja examinado por várias partes, o que leva a **descoberta e correção precoce das vulnerabilidades** de segurança causadas por erros de projeto;
- O princípio de projeto aberto é o oposto da abordagem conhecida como **segurança por obscuridade**, que tenta alcançar a segurança mantendo os algoritmos criptográficos secreto e que tem sido historicamente usando sem sucesso por várias organizações.

SEPARATION OF PRIVILEGE

Esse princípio diz que **condições múltiplas** são requeridas para alcançar acesso a recursos restritos ter um programa que execute uma ação.

LEAST PRIVILEGE

Cada programa e usuário de um sistema de computador deve operar com os **privilégios mínimos** necessários para funcionar corretamente.

- Se este princípio for aplicado, o abuso de privilégios é restrito e os dados causados pelo comprometimento de uma conta de aplicativo ou usuário é minimizado;
- O conceito militar **necessidade de saber** é um exemplo deste princípio.

LEAST COMMON MECHANISM

Em sistemas com múltiplos usuários, mecanismos que permitam que os recursos sejam **compartilhados por mais de um usuários devem ser minimizados**.

- Por exemplo, se um arquivo ou uma aplicação precisa ser acessada por mais de um usuário, então esses usuários devem ter canais separados para cada acesso a esse recurso para prevenir consequências imprevistas que podem ser causadas por problemas de segurança.

PSYCHOLOGICAL ACCEPTABILITY

Este princípio estabelece que interfaces de usuário devem ser **bem projetadas e intuitivas**, e todas as configurações relacionadas à segurança devem aderir ao que um usuário comum poderia esperar.

WORK FACTOR

De acordo com esse princípio, o **custo a ser contornado** por um mecanismo de segurança deve ser comparado com os recursos de um atacante ao projetar um esquema de segurança.

- Um sistema desenvolvido para proteger as notas dos alunos em um banco de dados da Universidade, que pode ser atacado por bisbilhoteiros ou estudantes que queiram mudar suas notas, provavelmente precisa de medidas de segurança menos sofisticadas do que um sistema construído para proteger segredos militares, que podem ser atacados por organizações de inteligência do governo.

COMPROMISE RECORDING

Este princípio estabelece que, por vezes, é mais desejável **gravar os detalhes** de uma intrusão do que adotar medidas sofisticadas para evitá-la.

- Câmeras de vigilância conectadas a internet são um exemplo típico de um sistema de registro que pode ser desenvolvido para proteger um edifício em vez de reforçar portas e janelas;
- Os servidores em uma rede no escritório podem **manter registros de todos os acessos a arquivos**, todos os e-mails enviados e recebidos e todas as sessões dos navegadores.

OBRIGADO!

linkedin.com/in/rodolfo-meneguette-30287329