Gestão da Tecnologia da Informação

Auditoria e Segurança da Informação

Francisco José Tosi

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Semana 5
Aula 09/10
Ataques cibernéticos

14/09

Francisco José Tosi

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Categoria de Ataques:

Ataque passivo: tem o objetivo a descoberta ou a utilização de informações do sistema sem afetar os recursos desse sistema.

Ataque Ativo: além de obter as informações, modifica os recursos do sistema, influenciando na operação.

Silva, 2023, p. 75.

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

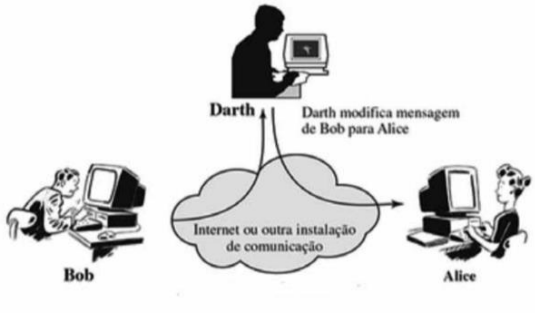
Categoria de Ataques:

Ataque passivo:

Liberação do conteúdo de uma mensagem sem autorização

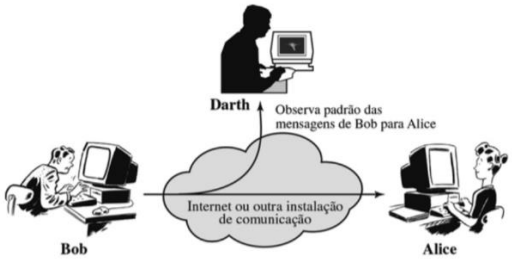
Seja em conversa telefônica, texto ou arquivo.

Figura 11 – Ataque passivo de liberação de conteúdo da mensagem



Fonte: (STALLINGS, 2008, p. 6).

Figura 12 – Ataque passivo de análise de tráfego.



Fonte: (STALLINGS, 2008, p. 6).

Análise de tráfego, as informações estão protegidas, mas é levantado as informações do padrão de mensagem, frequência de envio tamanho da mensagem, envolvidos.

Silva, 2023, p. 76.

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Categoria de Ataques:

Ataque Ativos:

Ocorre a modificação no fluxo de dados ou criação de um fluxo falso.

- ✓ Repetição;
- ✓ Disfarce;
- ✓ Modificação de mensagens;
- ✓ Negação de serviço;

Silva, 2023, p. 76.

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Categoria de Ataques:

Ataque Ativos:

Repetição: inicialmente os dados são capturados de forma passiva e posteriormente serão transmitidos para produzir um efeito não autorizado.

Disfarce: uma entidade finge ser outra, visando permitir o ataque a execução de ação em nome da entidade, conseguindo assim privilégios não autorizados.

Modificação: uma parte da mensagem original é alterada, adiada ou reordenada, visando à produção de efeito não autorizado.

Negação: ocorre o impedimento ou inibição para utilização ou gerenciamento das instalações de comunicação.

Silva, 2023, p. 77 / 78 / 79.

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Categoria de Ataques:

Ataques

Ataque de **Negação** pode possuir um alvo específico ou a rede como um todo, sobrecarregando com mensagens ou desativa-la.

Grande quantidade de trafego – é disparado uma grande quantidade de dados a uma taxa que a rede *host* ou aplicativo não pode manipular causando lentidão aos usuários chegando a interrupção dos serviços.

Pacotes maliciosos formatados – é enviado um pacote formatado maliciosamente para um *host* ou aplicativo que não pode ser manipulado, causando lentidão ou falha n execução do dispositivo.

Silva, 2023, p. 80.

Auditoria e Segurança da Informação

Categoria de Ataques:

Ataques

Ataques **mistos** utilizam mais de uma técnica para infiltrar no sistema.

São os ataques mais modernos.

Os autores das ameaças utilizam várias ferramentas para realizar os ataques.

Silva, 2023, p 81.

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Categoria de Ataques:

Ataques

A escuta	Escutar trafego da rede
Modificação de dados	Captura o trafego da empresa e altera os dados nos pacotes sem conhecimento do remetente ou receptor
Calcificação do endereço IP	Construção do pacote IP parecido com o original de um endereço válido dentro da internet corporativa
Baseados em senhas	Obter as credenciais de uma conta de usuário válida, utilizando a conta para obter informações da rede, ou alterar configurações de servidor

Silva, 2023, p 81.

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Categoria de Ataques:

Ataques

Negação de serviço (DoS)	Impede o uso normal de um computador ou rede por usuários válidos. Após obter acesso a rede o ataque pode travar aplicativos ou serviços da rede. Pode inundar
Manin-the-Middle (MItM)	Os agentes de ameaça se posicionam entre a origem e o destino, monitorando e controlando ativamente a comunicação.
Chave comprometida	Obter a chave secreta utilizando a chave para obter acesso a uma comunicação segura sem que o remetente ou destinatário esteja ciente.
Sniffer	Um aplicativo ou dispositivo que pode ler, monitorar e capturar troca de dados de rede e ler pacotes de rede.

Silva, 2023, p 81.

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Domínio de Ameaças:

É uma área de controle, autoridade ou proteção que atacantes pode explorar para ganhar acesso ao sistema através de *exploits*.

Exploits são um subconjunto de malware. Normalmente, são programas maliciosos com dados ou códigos executáveis capazes de aproveitar as vulnerabilidades de sistemas em um computador local ou remoto.

- Acesso físico direto ao sistema ou redes.
- Redes sem fio dentro do domínio da empresa.
- Equipamentos com comunicação via *bluetooth*.
- Anexos de e-mails maliciosos.
- Contas de mídias sociais.
- Mídias removíveis.
- Aplicação baseada em nuvem.

Silva, 2023, p 81.

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Ataques Dia Zero:

Explora a vulnerabilidade do software antes que se torne conhecida ou antes de ser divulgada pelo fabricante.

A rede é extremamente vulnerável entre o tempo que o *exploits* é descoberto.

Hora Zero é o tempo que o fornecedor de software leva para desenvolver um *patch* que conserta o e*xploits.*

Para se defender é necessário de profissionais de segurança de rede que adotam uma visão sofisticada e holística de qualquer arquitetura de rede.

EDUCAÇÃO METODISTA

Silva, 2023, p 83.

Auditoria e Segurança da Informação

Códigos Maliciosos:

Ou *Malwares* são desenvolvidos com a finalidade de executar ações danosas e atividades maliciosas em um sistema ou computador.

Pode ser utilizado para obter informações sensíveis ou excluir e modificar arquivos.

De acordo com o Panorama de Ameaças da Kaspersky de 2022 (KASPERSKY, 2022), ocorreram mais de 1.500 ataques de *malware* por minuto no Brasil entre janeiro/2022 e agosto/2022 .

EDUCAÇÃO METODISTA

Silva, 2023, p 83.

Auditoria e Segurança da Informação

Códigos Maliciosos:

Virus:

Virus é um programa de computador ou parte dele, que se propaga inserindo cópias dele mesmo.

O vírus depende da execução do programa ou arquivo hospedeiro, para se tornar ativo.

O primeiro registro de vírus foi Creeper, programado pelo pesquisador Bob Thomas em 1971.

O vírus se anexa em algum tipo de código executável e quando um programa contaminado é executado os arquivos acessados são contaminados.

EDUCAÇÃO METODISTA

Silva, 2023, p 86.

Auditoria e Segurança da Informação

Códigos Maliciosos:

Worm:

Em português verme.

Se multiplica pela rede, enviando cópias de si mesmo entre os computadores.

São semelhantes a vírus, mas não se programa pela inclusão de cópias, e sim pela execução direta das suas cópia ou exploração da vulnerabilidade existente nos computadores.

Um worm podem realizar muitas cópias de si mesmo e consumir muitos recursos computacionais e afetar o desempenho de redes.

O worm dispertou a necessidade de manter as máquinas atualizadas com sistema de segurança e realização de *backup*.

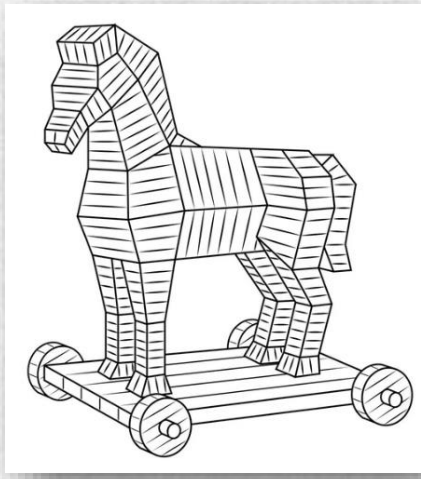
EDUCAÇÃO METODISTA

Silva, 2023, p 86.

Auditoria e Segurança da Informação

Códigos Maliciosos:

Trojan:



É uma *malware* que funciona com um cavalo de troia.

Utiliza a sua aparência externa de forma a enganar o usuário a executa-lo.

Ao ser executado, as instruções de ataque são realizadas com permissão do usuário.

O programa tem que ser executado pelo usuário.

São classificados pelo tipo de dano que causa ou pela forma que violam o sistema.

Um tipo de cavalo de troia é o que permite o acesso remoto não autorizado.

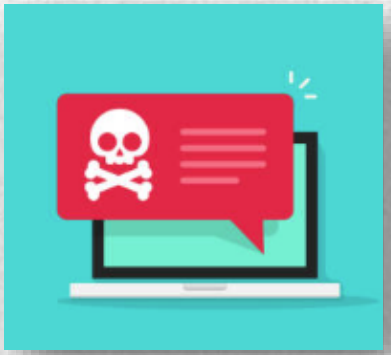
EDUCAÇÃO METODISTA

Silva, 2023, p 88.

Auditoria e Segurança da Informação

Códigos Maliciosos:

Spyware:



Tem o objetivo de coletar informações sobre um usuários por meio de conexão pela internet sem consentimento.

Retira a confidencialidade da informação.

Após sua instalação o aplicativo monitora as atividades do usuário na internet.

Funciona como programa executável independente e pode realizar operações como varredura de arquivos de disco rígido, leitura de *cookies*, alteração da página inicial do navegador, monitoração dos toques de teclas.

EDUCAÇÃO METODISTA

Silva, 2023, p 91.

Auditoria e Segurança da Informação

Códigos Maliciosos:

Adware:

É um tipo de *malware* muito conhecido na internet.

Software que exibe anúncios e coleta de dados.

São baixados quando se concorda com termos de serviço de software gratuitos em troca de da exibição de anúncios.

Algumas vezes são instalados sem permissão e realizam outras ações prejudiciais .

Adware é qualquer programa que automaticamente executa, mostra, ou baixa publicidade no computador.

EDUCAÇÃO METODISTA

Silva, 2023, p 91.

Auditoria e Segurança da Informação

Códigos Maliciosos:

Scareware:

É projetado para persuadir o usuário a executar uma ação específica com base no medo.

Simula janelas *pop-up* que se assemelham a janelas de diálogo do sistema operacional.

Transmitem mensagens falsificadas que afirmam que o sistema está em risco ou precisam de um programa específico para retornar a à operação normal.

Se o usuário concordar e executar o programa seu sistema será infectado.

Silva, 2023, p 92.

Auditoria e Segurança da Informação

Códigos Maliciosos:

Botnet:

Possui recursos de comunicação com o invasor que permite que ele seja controlado de forma remota.

Sua infecção é similar do *wrom* e tem a capacidade para se programar automaticamente se aproveitando da vulnerabilidades existentes nos softwares ou sistemas instalados.

O computador infectado é conhecido com *sumbie computer,* é controlado sem o conhecimento do seu dono.

Quando os autores da ameaça comprometem muitos *hosts* executam um ataque DoSdistribuído (DDoS).

Silva, 2023, p 92.

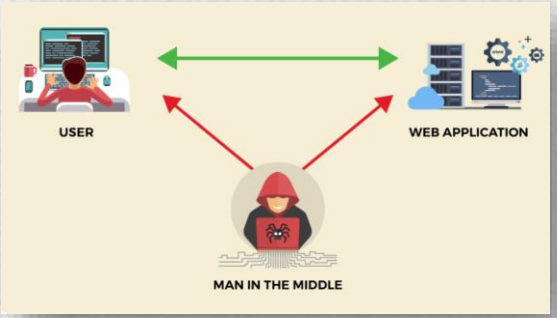
EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Códigos Maliciosos:

Man-In-the-Middle (MitM):

Realiza a interpretação das comunicações entre computadores buscando roubar informações que trafegam pela rede.



Permite que o invasor tenha controle sobre um dispositivo sem conhecimento do usuário.

Pode interceptar e capturar informações do usuário antes de transmiti-las ao seu destino.

São amplamente utilizados para roubar informações financeiras.

Silva, 2023, p 94.

Auditoria e Segurança da Informação

Códigos Maliciosos:

Ransonware:

Aprisiona um sistema de computador ou os dados nele encontrados até que a vítima faça um pagamento para resgate de dados.

Normalmente funciona criptografando dados com chave desconhecida pelo usuário.

Utiliza vulnerabilidade do sistema para bloquear o sistema.

É propagado como um cavalo de troia e resulta em um arquivo baixado ou de um ponto fraco do software.

A meta do criminoso é sempre o pagamento de resgate.

Silva, 2023, p 96.

Auditoria e Segurança da Informação

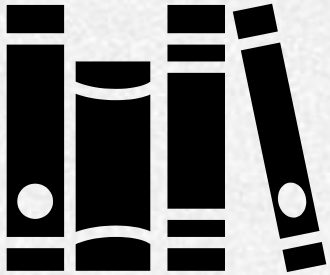
Kahoot

Códigos Maliciosos

https://create.kahoot.it/

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação



Dias Claudia; Segurança e Auditoria da tecnologia da informação Claudia Dias Indaial : Editora Axcel Books, 2000

Gross, Christian Meinecke; Segurança em tecnologia da informação / Christian Meinecke Gross; Jan Charles Gross. Indaial : Uniasselvi, 2013.

Hintzbergen, Julie; Fundamentos de Segurança da Informação: Com base nas normas ISO 27001 e na ISO 27002 / Julie Hintzbergen, Kees Hintzbergen, André Smulders, Hans Baars; Tradução Alan Sá – Rio de Janeiro : Brasport, 2015

Imoniana, Joshua Onome; Auditoria de Sistemas de Informação / Joshua Onome Imoniana; 2. ed. – 2. reimpr; S;ao Paulo : Atlas, 2010

Lyra, Maurício Rocha; Governança da Segurança da Informação / Edição do Autor, 2015

Sêmola, Marcos; Gestão da Tecnologia da Informação: visão executiva da segurança da informação : aplicada a Security Officer / Marcos Sêmola e Módulo Security Solutions S.A. Rio de Janeiro : Elsevier, 2003 – 10ª reimpressão

Silva, Michel Bernardo Fernandes da, Cibersegurança uma visão panorâmica sobre segurança da informação na internet / Michel Bernardo Fernandes da silva. – Rio de Janeiro : Freitas Bastos, 2023.

EDUCAÇÃO METODISTA