CiberSegurança

Escola José Carlos celestino gomes

Miguel Aveiro, 11\2023

Trabalho realizado pelo aluno Miguel Eugénio , da turma 12ºE2 , sob orientação do Professor, Sérgio Heleno, no ano letivo 2023/2024.

CiberSegurança

Nome da Escola

nome cidade, mês ano

Trabalho realizado pelo alun....., da turma ..... , sob orientação do Professor, Sérgio Heleno, no ano letivo 2020/2021.

Índice

1 Introdução

Este trabalho surgiu no âmbito de Redes de Comunicação/FCT com a finalidade de aprender mais sobre a segurança na Internet. Trabalho realizado em fevereiro de 2021 na cidade de Esmoriz.

2 O que é a CiberSegurança

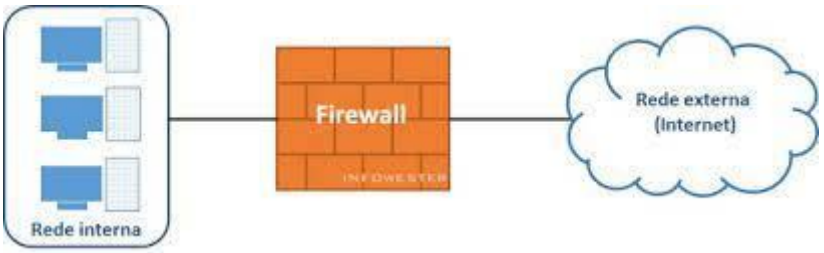
A cibersegurança, ou segurança cibernética, é um campo que se dedica a proteger sistemas, redes, dispositivos e dados contra ameaças digitais. O termo refere-se às práticas, tecnologias e processos que são empregados para garantir a confidencialidade, integridade e disponibilidade das informações em ambientes digitais.

3 O que é a Darkweb

A dark web, ou "web obscura", refere-se a uma parte da internet que não é indexada pelos motores de busca convencionais e que, portanto, não é facilmente acessível através de navegadores comuns. Diferentemente da "surface web" (web superficial), que é a parte da internet que a maioria das pessoas usa diariamente e que é acessível por meio de motores de busca padrão, a dark web é intencionalmente obscurecida e muitas vezes requer software específico para acesso.

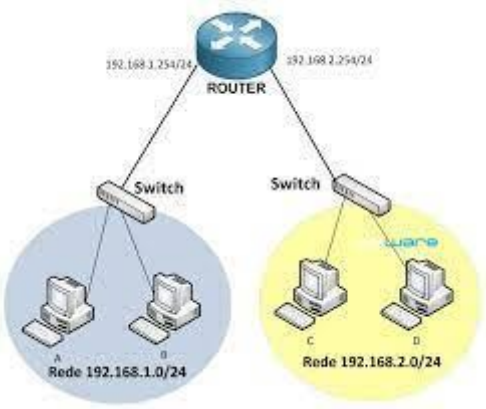
4 O que é uma Firewall

Uma firewall é um componente de segurança de rede que monitora e controla o tráfego de dados entre redes, decidindo permitir ou bloquear com base em um conjunto de regras predeterminadas. O objetivo principal de uma firewall é proteger uma rede ou dispositivo contra acessos não autorizados, ataques cibernéticos e outros riscos de segurança.



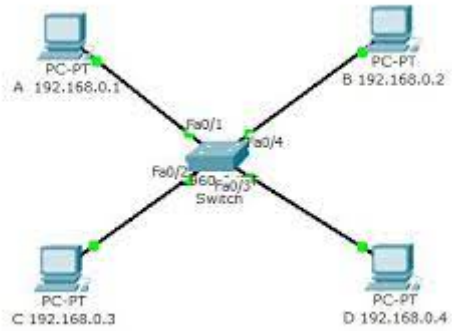
5 O que é um router

Um roteador (também conhecido como "router" em inglês) é um dispositivo de rede que encaminha dados entre diferentes redes de computadores. Sua principal função é tomar decisões sobre a rota mais eficiente para enviar pacotes de dados de uma rede para outra. Os roteadores são fundamentais para a operação da Internet e redes locais (LANs).



6 O que é um switch

Um switch é um dispositivo de rede que opera na camada de enlace de dados (camada 2) do modelo OSI (Open Systems Interconnection). Sua função principal é encaminhar pacotes de dados entre dispositivos em uma rede local (LAN), com base nos endereços MAC (Media Access Control) dos dispositivos conectados.



7 O que é um antivírus

Um antivírus é um programa de software projetado para detectar, prevenir e remover software malicioso (malware) de um computador ou sistema. O malware inclui vírus, worms, cavalos de Troia, spyware, adware e outras formas de software indesejado que podem causar danos ao sistema, roubar informações ou comprometer a segurança e o desempenho do dispositivo.

8 Tipos de Hacker

Hacker Ético (White Hat Hacker):

Motivação: Trabalham para melhorar a segurança de sistemas, redes e aplicativos.

Atividades: Realizam testes de segurança, identificam vulnerabilidades e ajudam a corrigi-las. São frequentemente contratados por organizações para fortalecer a segurança.

Cracker ou Black Hat Hacker:

Motivação: Realizam atividades maliciosas, explorando vulnerabilidades para ganho pessoal ou prejudicar sistemas.

Atividades: Invadem sistemas, roubam dados, distribuem malware, realizam ataques de negação de serviço (DDoS) e outras atividades ilegais.

Hacker Grey Hat:

Motivação: Possuem características tanto de hackers éticos quanto de crackers, podendo realizar atividades questionáveis sem permissão, mas com a intenção de alertar sobre vulnerabilidades.

Atividades: Podem invadir sistemas sem autorização, mas geralmente divulgam as falhas encontradas para alertar os proprietários.

Hacktivista:

Motivação: Buscam promover causas sociais ou políticas por meio de atividades online.

Atividades: Realizam ataques cibernéticos para chamar a atenção para questões específicas, **vazar informações ou interromper operações online relacionadas a causas que defendem.**

Script Kiddie:

Motivação: Possuem pouco conhecimento técnico e geralmente realizam atividades de hacking usando ferramentas desenvolvidas por outros. Atividades: Praticam hacking de baixa complexidade, muitas vezes sem compreender completamente as técnicas envolvidas.

Hacker de Chapéu Azul (Blue Hat Hacker):

Motivação: Trabalham em prol de uma organização específica, geralmente para testar a segurança de seus sistemas.

Atividades: Realizam testes de penetração e avaliações de segurança em sistemas internos, semelhante a hackers éticos.

8.1 O que é um Hacker

Os termos "hacker" e "hacking" têm várias conotações e podem referir-se a diferentes tipos de atividades online. É importante observar que nem todos os hackers estão envolvidos em atividades maliciosas; muitos deles contribuem para a segurança da informação e desenvolvem habilidades em programação para fins legítimos.

8.2 White Hats

Os "White Hats" (chapéus brancos) são hackers éticos que utilizam suas habilidades em cibersegurança para propósitos legítimos, visando melhorar a segurança de sistemas, redes e aplicativos. Diferentemente dos hackers maliciosos, os White Hats atuam de maneira legal e ética, muitas vezes sendo contratados por organizações para realizar testes de segurança, avaliações de vulnerabilidades e outras atividades para fortalecer a postura de segurança.

8.3 Gray Hats

Os "Gray Hats" (chapéus cinza) são hackers que não se enquadram estritamente nas categorias de "White Hats" (chapéus brancos), que são éticos e buscam melhorar a segurança, nem nas categorias de "Black Hats" (chapéus pretos), que são maliciosos e buscam explorar vulnerabilidades para ganho pessoal ou prejudicar sistemas.

8.4 Black Hats

Os "Black Hats" (chapéus pretos) referem-se a hackers que realizam atividades cibernéticas maliciosas e ilegais, muitas vezes visando explorar vulnerabilidades em sistemas, roubar dados, causar danos ou interromper operações. Esses hackers agem com motivações pessoais, financeiras ou prejudiciais.

8.5 Hackeres organizados

Hackers organizados são grupos de indivíduos que colaboram de maneira estruturada para realizar atividades cibernéticas. Esses grupos podem ter diferentes motivações, metas e níveis de sofisticação. Aqui estão alguns tipos de hackers organizados:

9 Tipos de Malware

Existem vários tipos de malware, que são programas maliciosos desenvolvidos para causar danos, roubar informações ou realizar atividades indesejadas em um sistema. Aqui estão alguns dos principais tipos de malware:

Vírus:

Propaga-se ao anexar seu código a programas legítimos. Uma vez executado, pode se espalhar para outros programas e sistemas.

Worms:

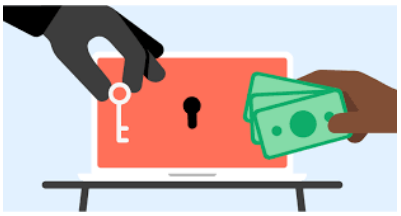
Diferentemente dos vírus, os worms não precisam se anexar a programas existentes. Eles se espalham automaticamente pela rede, explorando vulnerabilidades.

Trojans (Cavalos de Troia):

Apresentam-se como programas legítimos, mas têm funcionalidades maliciosas ocultas. Podem ser usados para roubo de dados, controle remoto ou instalação de outros malwares.

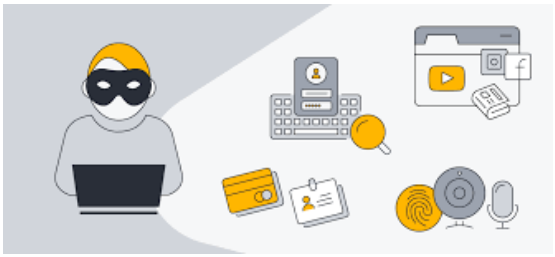
Ransomware:

Criptografa arquivos no sistema da vítima e exige um resgate em troca da chave de descriptografia. É projetado para extorquir dinheiro das vítimas.



Spyware:

Monitora atividades do usuário sem o seu conhecimento, coletando informações pessoais, senhas e dados confidenciais.

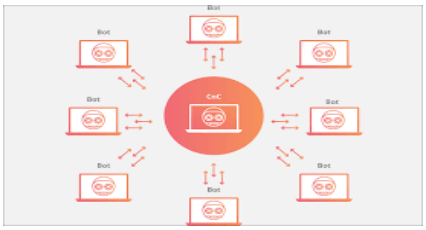


Adware:

Exibe anúncios indesejados no sistema da vítima. Pode ser incorporado em software legítimo e exibir publicidade excessiva.

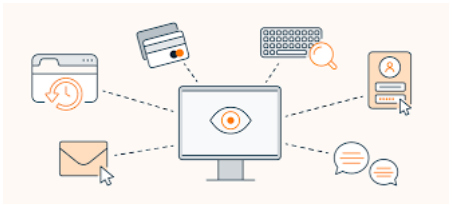
Botnets:

Conjunto de dispositivos infectados que são controlados remotamente por um invasor. Geralmente usado para realizar ataques distribuídos de negação de serviço (DDoS) ou outras atividades maliciosas em larga escala.



Keyloggers:

Registram as teclas digitadas pelo usuário, permitindo que os invasores capturem senhas e outras informações confidenciais.



Rootkits:

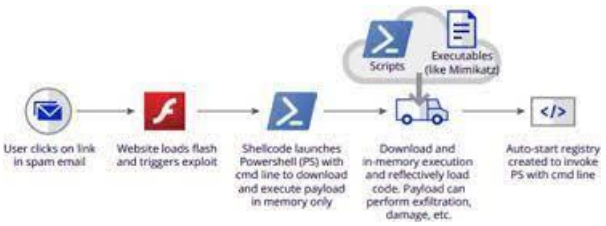
Modificam o sistema operacional para esconder a presença de outros malwares. Podem ser difíceis de detectar e remover.

Scareware:

Apresenta falsos alertas de segurança para assustar os usuários e induzi-los a comprar software falso ou desnecessário.

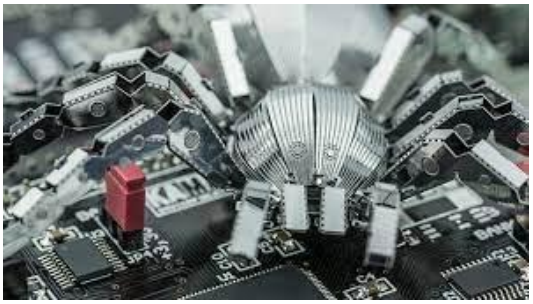
Fileless Malware:

Opera na memória do sistema, sem deixar rastros físicos em disco. Pode ser mais difícil de detectar por soluções antivírus tradicionais.



Macrovírus:

Explora macros em documentos, como planilhas e documentos do Word, para executar código malicioso.



9.1 O que é o Malware

"Malware" é uma contração das palavras "malicious" (malicioso) e "software" (software). Portanto, malware refere-se a qualquer software projetado para causar danos, explorar recursos ou realizar ações indesejadas em um computador, dispositivo móvel, rede ou sistema de computadores.

9.2 Spyware

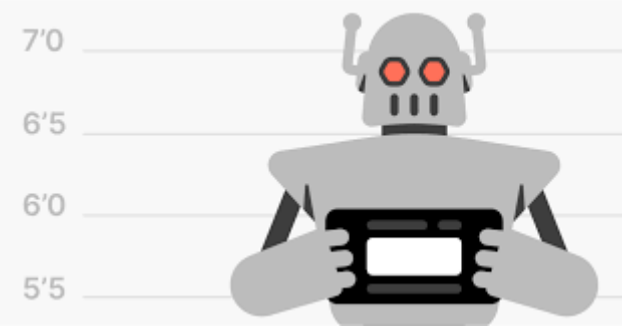
O spyware é um tipo de software malicioso projetado para coletar informações sobre as atividades de um usuário sem o seu conhecimento ou consentimento. Esse tipo de malware é conhecido por espionar os usuários, monitorando suas atividades online e offline e coletando dados pessoais sensíveis.

9.3 Adware

Exibe anúncios indesejados no sistema da vítima. Pode ser incorporado em software legítimo e exibir publicidade excessiva.

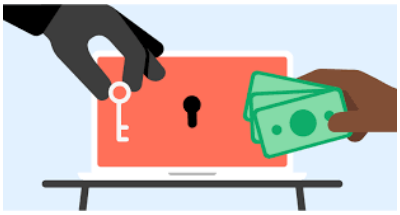
9.4 Bot

O termo "bot" refere-se a um programa de software automatizado que realiza tarefas específicas na internet. A palavra "bot" é uma abreviação de "robot" (robô). Existem diferentes tipos de bots, cada um projetado para executar funções específicas.



9.5 Ransomware

Criptografa arquivos no sistema da vítima e exige um resgate em troca da chave de descriptografia. É projetado para extorquir dinheiro das vítimas.



9.6 Scareware

Apresenta falsos alertas de segurança para assustar os usuários e induzi-los a comprar software falso ou desnecessário.

9.7 Rootkit

Modificam o sistema operacional para esconder a presença de outros malwares. Podem ser difíceis de detectar e remover.

9.8 Vírus

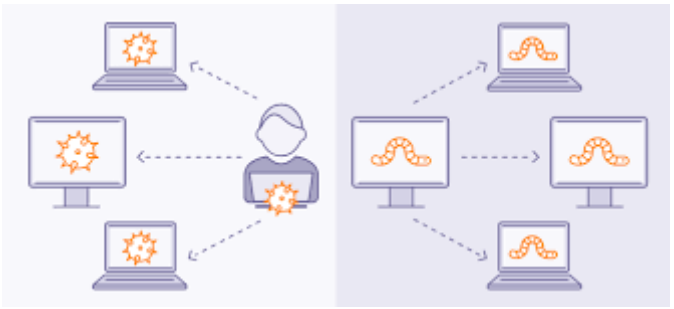
Propaga-se ao anexar seu código a programas legítimos. Uma vez executado, pode se espalhar para outros programas e sistemas.

9.9 Trojan horse

Apresentam-se como programas legítimos, mas têm funcionalidades maliciosas ocultas. Podem ser usados para roubo de dados, controle remoto ou instalação de outros malwares.

9.10 Worm

Diferentemente dos vírus, os worms não precisam se anexar a programas existentes. Eles se espalham automaticamente pela rede, explorando vulnerabilidades.



10 Engenharia Social

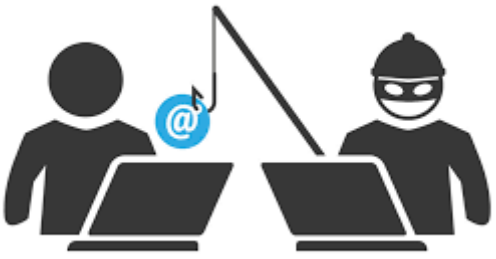
A engenharia social é uma prática que envolve manipular pessoas para realizar ações específicas ou divulgar informações confidenciais. Ao contrário de ataques cibernéticos que exploram vulnerabilidades técnicas, a engenharia social explora aspectos psicológicos e sociais para obter acesso não autorizado a informações, sistemas ou recursos.

10.1 O que é a engenharia social

A engenharia social é uma prática que envolve a manipulação de pessoas para obter informações confidenciais, acesso a sistemas ou realizar ações que possam comprometer a segurança. Diferentemente dos ataques que exploram vulnerabilidades técnicas em software ou hardware, a engenharia social explora aspectos psicológicos e sociais para enganar as pessoas.

10.2 Pretexting

Pretexting é uma técnica de engenharia social na qual um indivíduo cria um pretexto ou narrativa falsa para obter informações de uma pessoa. O objetivo é manipular a vítima para que ela revele detalhes pessoais, financeiros ou informações confidenciais. Diferente do phishing, que muitas vezes envolve mensagens eletrônicas fraudulentas, o pretexting geralmente ocorre através de interações mais elaboradas e diretas.



10.3 Tailgating

Tailgating, também conhecido como "piggybacking" (carona), é uma técnica de engenharia social na qual um indivíduo não autorizado segue de perto uma pessoa autorizada para obter acesso a uma área restrita. Essa prática explora a cortesia comum em ambientes físicos, onde as pessoas têm a tendência de manter portas abertas para colegas ou mesmo desconhecidos que estão próximos.

11 Segurança

O termo "segurança" refere-se à proteção contra riscos, ameaças, perigos ou danos. Em diversos contextos, a segurança pode abranger uma ampla gama de áreas e preocupações.

11.1 Segurança do posto de trabalho

A segurança do posto de trabalho refere-se às medidas e práticas implementadas para garantir a segurança e o bem-estar dos trabalhadores em seus ambientes de trabalho. Isso abrange uma variedade de aspectos, desde a prevenção de acidentes físicos até a segurança da informação e a promoção do bem-estar emocional dos funcionários.

11.2 Segurança de email

A segurança de e-mail é crucial para proteger as comunicações eletrônicas contra ameaças como phishing, malware e ataques de engenharia social.

12 Conclusão

Com a realização deste trabalho fiquei a saber um pouco mais sobre cibersegurança.

Tive dificuldade em nada

Gostei de elaborar em esta pesquisa, em especial de falar sobre os virus

13 Para pensar

Será que daqui a .....

14 Webgrafia

Chatgpt

Wikipedia.

Cibersegurança
Miguel Eugénio
Escola José Carlos Celestino Gomes
Aveiro, Novembro de 2023