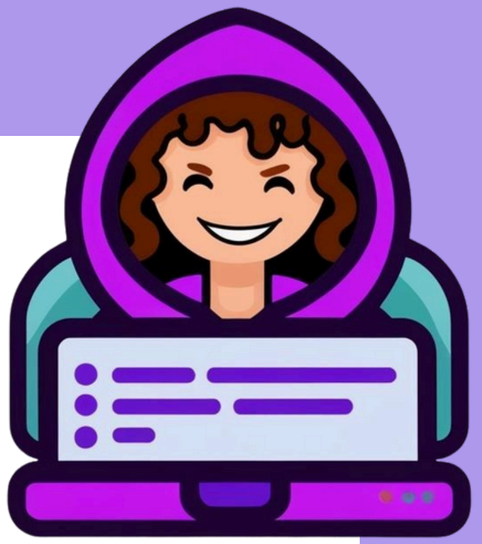
BRINQUEDO DE GENTE GRANDE: POR DENTRO DA MOCHILA DE UM HACKER

Anny Ribeiro

Analista de Infraestrutura com foco em segurança da informação

Anny Ribeiro



- 28 anos, goiana uai
- 2 diplomas pelo IF Goiano Campus Ceres
  - técnica em informática e bacharela em SI - 1º turma
- Pós Graduanda em Cibersegurança pela Faculdade Metropolitana
- 9 anos na área de Tecnologia
- Analista de Infraestrutura com foco em segurança da informação
- 2 PetFilhas, Ioguini, gosto de cozinhar por hobby
- Apaixonada por Café, Vinhos, coisas nerdolas e O NERDOLA com que eu sou casada

O que é Hardware Hacking?

- Diferença entre hacking de software e hardware

Por que isso importa?

- Área em constante crescimento na cibersegurança e tecnologia:
  - **Aplicações práticas:**
    - Testes de invasão (pentest), automação e robótica, programas de bug bounty, CTFs, segurança de IoT.
  - **Mercado crescente**
    - Á medida que os dispositivos se conectam e se tornam inteligentes surge a necessidade de especialistas
  - **Comunidades que apoiam e desenvolvem**

Você já se perguntou o que um hacker carrega na mochila?

- SPOILER: Não é só o notebook!
- Visão geral...

Tudo que vai ser falado a partir de agora é inteiramente para fins didáticos!

Apresentação das ferramentas

- Ferramenta de segurança de RFID (Radio-Frequency Identification) altamente especializada e portátil
- Projetada para emular, clonar, ler e testar cartões e chaves de acesso

RFID

NFC

T-Dongle-S3

- placa de desenvolvimento compacta, do tamanho de um pendrive
- ideal para projetos de Internet das Coisas (IoT) e outras aplicações eletrônicas
- Baixo consumo de energia

Flipper Zero: O Canivete Suíço Digital

- Multi-ferramenta Versátil
  - Interage com sistemas eletrônicos via RFID, NFC, infravermelho e sub-GHz.
  - Clone e teste de controles remotos.
  - Análise de vulnerabilidades em acessos.
- Recursos Principais
  - RFID e NFC para clonagem de cartões.
  - Infrared para controle de dispositivos.
  - Sub-GHz para comunicação sem fio.
  - iButton para sistemas de acesso.

Cardputer: Computador de Bolso

- Microcomputador Compacto
  - Pequeno, mas poderoso, com ESP32, WiFi e Bluetooth.
- Programável
  - Ideal para scan de redes e análise de protocolos.
- Engenharia Reversa
  - Usado em testes de penetração e engenharia reversa.
- Identificação de Vulneráveis
  - Demonstraremos como identificar dispositivos fracos.

Demonstrações práticas

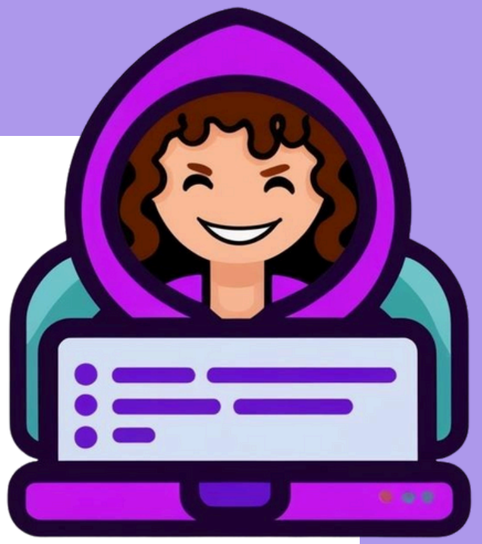
- Hora de brincar:
  - SafeChat
  - Ataque gêmeo do mal
  - Demonstração rápida de cópia de sinais


eu já tô aqui prontinha pra dar
a palestra pra vocês

Aplicações reais

- Descubra usos legítimos.
  - Análise de vulnerabilidades
  - Perícia Forense e Digital
  - Desenvolvimento de Novos produtos
  - Reparo e Custumização
  - Aprendizado e Hobby

Ética e legislação



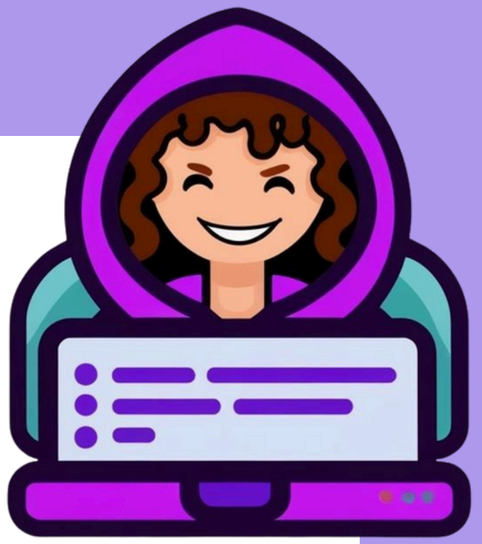
- Ética:
  - Consentimento
  - Divulgação responsável (Bug Bounts)
- Legislação
  - Lei de Crimes Cibernéticos (Lei 12.737/12 - Lei Carolina Dieckmann
    - Divulgação de dados sem autorização
  - LGPD
  - Respeito a propriedade intelectual
    - Copiar um dispositivo para revendê-lo

Outros Brinquedos

você pode criar suas próprias ferramentas usando arduíno, raspberry, um pendrive...

Onde aprender mais?

- (GitHub, YouTube, sites como Hak5, Flipper Labs)
- Comunidades brasileiras de hardware hacking
- Eletrônica
- Arduíno



COMUNIDADES

MULHERESGO

PERGUNTAS?

OBRIGADA!

Outras informações, material da palestra, minhas redes e contatos.

SORTEIO

cilia

SIGAM:

@CILIATECNOLOGIA

www.linkedin.com/company/cilia/