

# CYBERPUNK GUIDE

## HARDWARE HACKING

IMPLANTES

FERRAMENTAS

PESQUISADORES

FERRAMENTAS!!

ENTREVISTAS

E FERRAMENTAS!!!

VOLUME  
ACUMULATIVO  
COM 16 PAGES



## — nota do editor

# Julio Della Flora



...para ter mais conteúdo gratuito sobre hacking e eletrônica siga meu perfil no Instagram.

The screenshot shows Julio Della Flora's Instagram profile. His bio includes: "Hardware Hacking Criador(a) de conteúdo digital NOVO E-BOOK GRÁTIS AQUI! juliodellaflora.com". Below the bio are two circular icons labeled "Eventos de Sec" and "Dispositivos". At the bottom of the profile screen are navigation tabs for "PUBICAÇÕES", "REELS", "GUIAS", and "MARCADOS". The main area displays a grid of nine images: three in the top row (an Arduino board, a smiling man holding a small device, a close-up of a circuit board), three in the middle row (a man holding a blue microcontroller board, a book cover for "#SYH2", a scope displaying a waveform), and three in the bottom row (a close-up of a circuit board, a license plate, and a blue object).

O conteúdo a seguir foi produzido por mim (Julio Della Flora) com a ideia de reviver as antigas revistas de computação e eletrônica dos anos 90 e 2000.

Infelizmente não da pra anexar um CD Rom com as versões mais recentes do turkojan ou do back orifice mas a ideia continua com o objetivo de criar um revista nessa estética que marcou a minha geração.

Caso você tenha baixado essa revista fora do meu site ([juliodellaflora.com](http://juliodellaflora.com)) e gosta desse tipo de conteúdo, da uma passada lá e deixa seu e-mail na newsletter, assim que eu produzir novas edições dessa revista elas serão enviadas para o seu e-mail.



scan or click



# NINTENDO FAMICOM

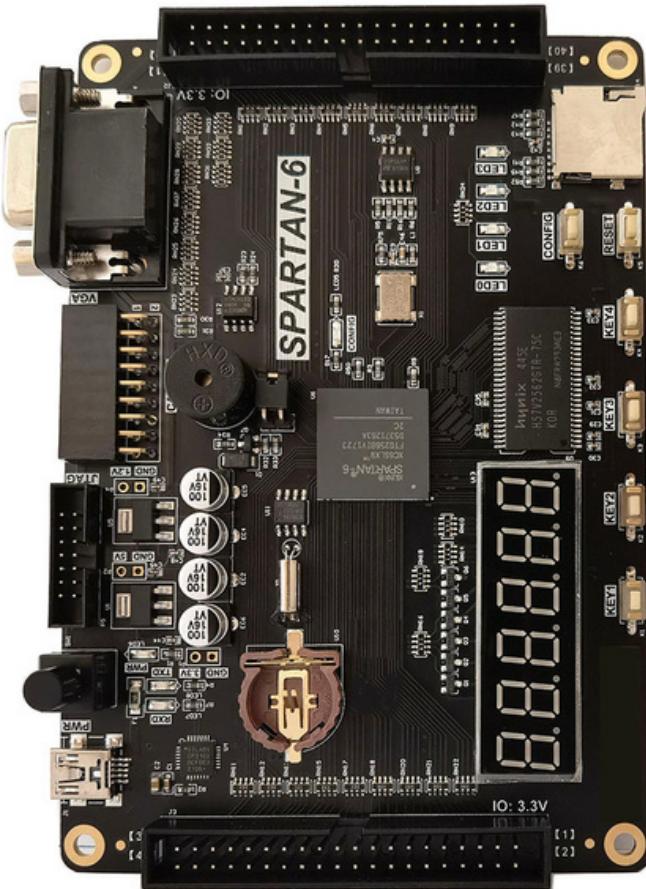


Enquanto o PlayStation 5, o Xbox Series X|S e o Nintendo Switch dominam os lançamentos contemporâneos, o icônico NES, ainda vê novos títulos surgindo. Esses lançamentos provêm tanto da paixão da comunidade quanto de estúdios dedicados que valorizam o charme do console de 8 bits. Um exemplo notável é "Malasombra", um jogo de plataforma retrô desenvolvido pela 4MHz, uma equipe espanhola renomada por seu foco em títulos clássicos, como "Operation Alexandra" e "Profanation 2". Embora estejamos em 2024, e não em 1989, "Malasombra" será disponibilizado não apenas em cartucho tradicional, mas também em formato digital.

@JULIODELLAFLORA

# O QUE É FPGA?

Um FPGA, ou Field-Programmable Gate Array, é um dispositivo integrado capaz de ser reprogramado após sua fabricação, permitindo que os designers criem circuitos digitais sem necessariamente fabricar chips de silício customizados. Muitos engenheiros recorrem aos FPGAs para prototipar, testar e modificar seus designs antes de finalizar um ASIC, que é um circuito dedicado. Além da prototipagem, os FPGAs encontraram utilidade no processamento de sinal digital, em áreas como comunicações e processamento de imagens, na mineração de criptomoedas, em pesquisas e em sistemas embarcados.



@JULIODELLAFLORA

Uma das maiores vantagens do FPGA é sua flexibilidade; ele pode ser reprogramado para atender diferentes necessidades. Eles também são otimizados para executar tarefas específicas rapidamente e podem processar várias tarefas em paralelo, contrapondo-se à natureza sequencial das CPUs.



scan or click



## O PODER DO ABACAXI

### MARK VII

O novo WiFi Pineapple Mark VII oferece um desempenho incrível a partir de uma interface web simples, complementada por um vasto ecossistema de aplicativos, campanhas automatizadas de teste de penetração e o Cloud C2 para acesso remoto de qualquer lugar. Domine o espaço aéreo com um painel de reconhecimento interativo e mantenha-se focado e dentro do escopo usando a principal suíte de pontos de acesso não autorizados para ataques avançados de intermediário (man-in-the-middle).





# TREINAMENTO HARDWARE HACKING

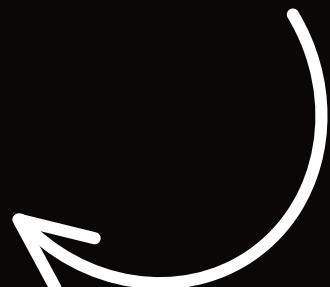
SOLYD.COM.BR



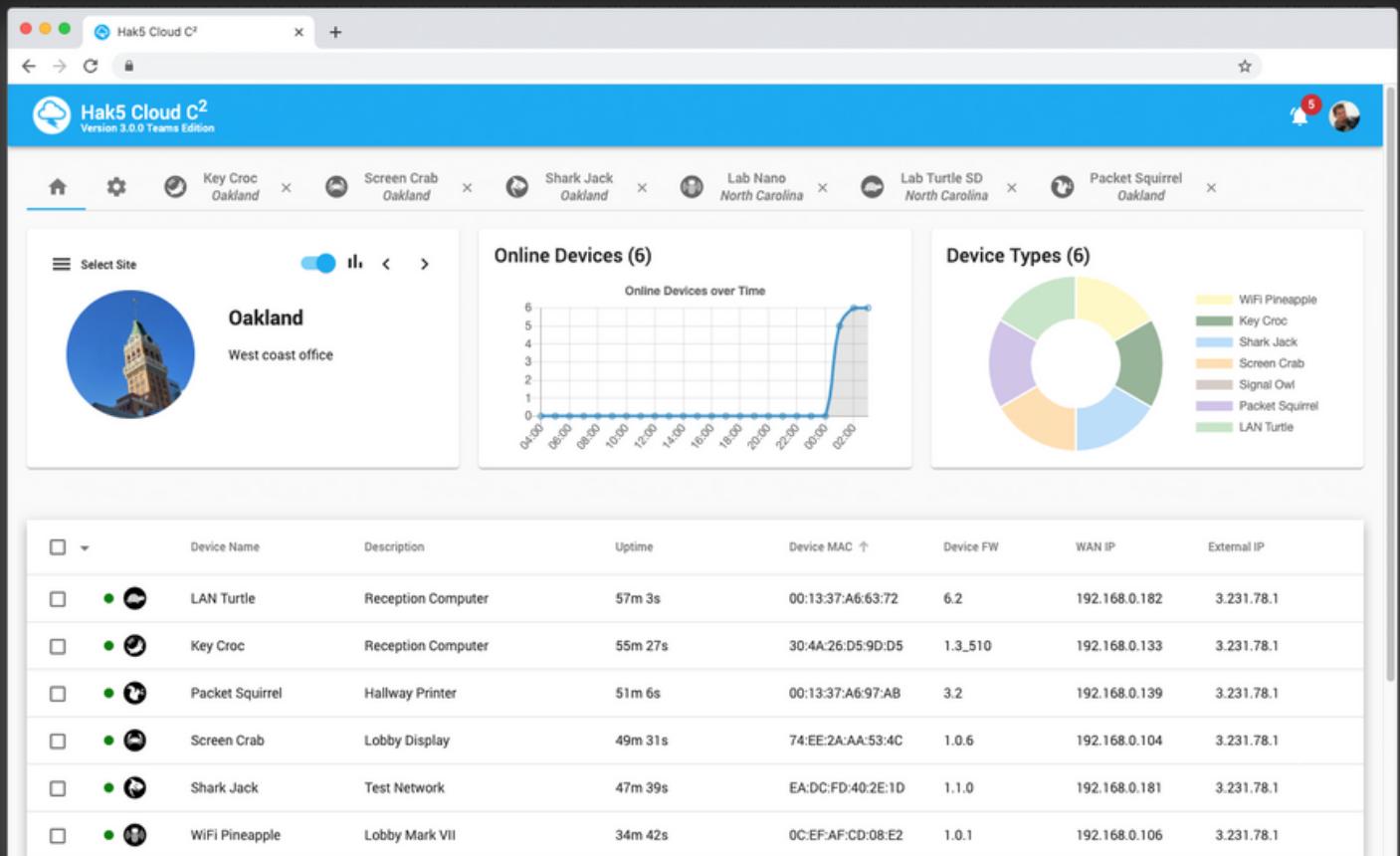
## Quer melhorar suas habilidades?

Em um mundo cada vez mais conectado, a segurança e a manipulação de dispositivos eletrônicos tornaram-se uma habilidade vital. E, neste treinamento, propomos abrir as portas desse universo para você!

**saiba mais em:**  
**solyd.com.br**



# CLOUD C<sup>2</sup>

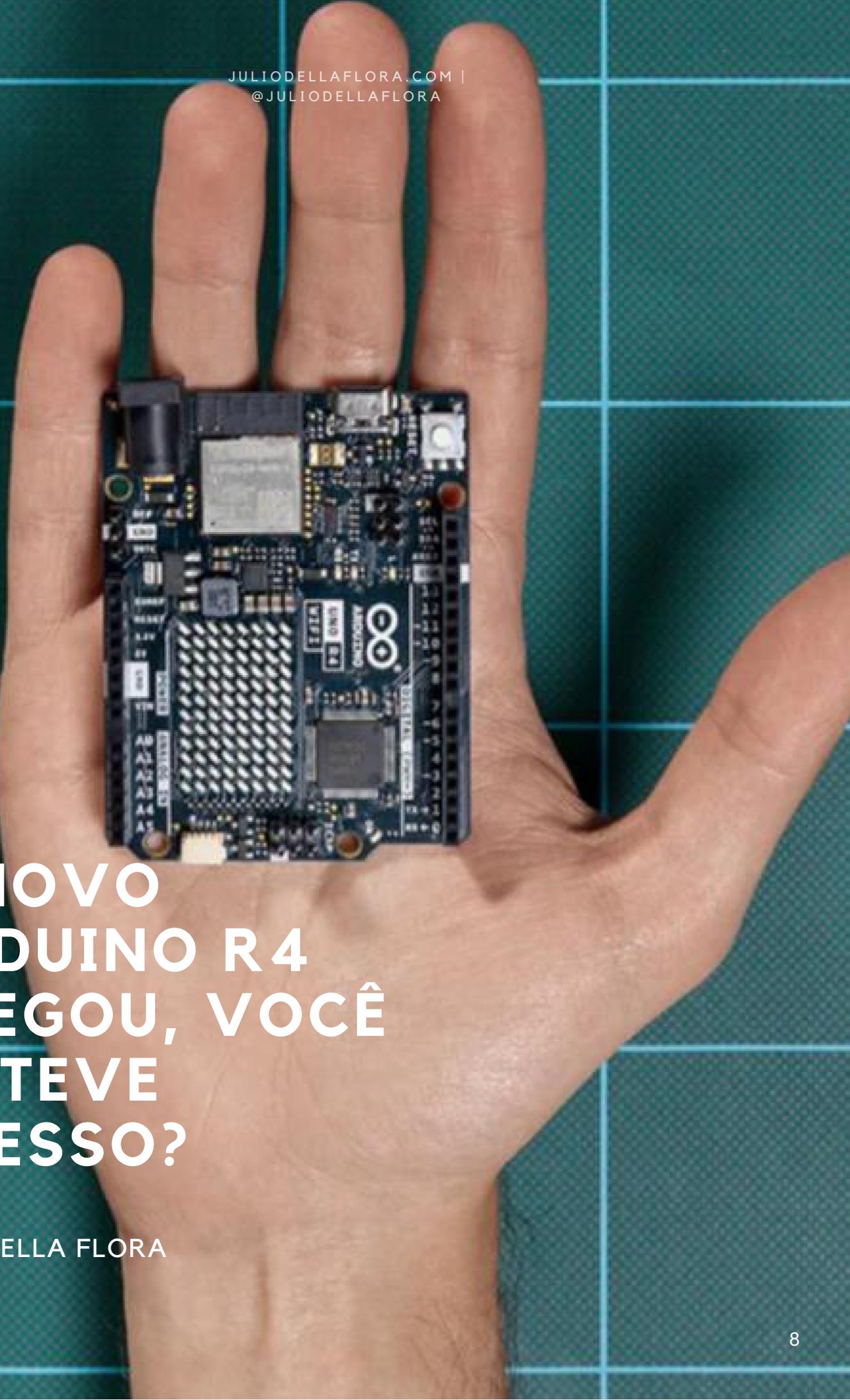


The screenshot shows the Hak5 Cloud C<sup>2</sup> web interface. At the top, there's a navigation bar with tabs for different sites: Key Croc (Oakland), Screen Crab (Oakland), Shark Jack (Oakland), Lab Nano (North Carolina), Lab Turtle SD (North Carolina), and Packet Squirrel (Oakland). Below the navigation is a sidebar titled "Select Site" showing "Oakland" as the active site, described as "West coast office". To the right of the sidebar are two cards: "Online Devices (6)" which includes a line graph titled "Online Devices over Time" showing a sharp increase from 0 to 6 devices between 22:00 and 02:00, and "Device Types (6)" which is a donut chart showing the distribution of device types: WiFi Pineapple, Key Croc, Shark Jack, Screen Crab, Signal Owl, Packet Squirrel, and LAN Turtle. The main area below these cards is a table listing six devices:

Device Name	Description	Uptime	Device MAC ↑	Device FW	WAN IP	External IP
LAN Turtle	Reception Computer	57m 3s	00:13:37:A6:63:72	6.2	192.168.0.182	3.231.78.1
Key Croc	Reception Computer	55m 27s	30:4A:26:D5:9D:D5	1.3_510	192.168.0.133	3.231.78.1
Packet Squirrel	Hallway Printer	51m 6s	00:13:37:A6:97:AB	3.2	192.168.0.139	3.231.78.1
Screen Crab	Lobby Display	49m 31s	74:EE:2A:AA:53:4C	1.0.6	192.168.0.104	3.231.78.1
Shark Jack	Test Network	47m 39s	EA:DC:FD:40:2E:1D	1.1.0	192.168.0.181	3.231.78.1
WiFi Pineapple	Lobby Mark VII	34m 42s	0C:EF:AF:CD:08:E2	1.0.1	192.168.0.106	3.231.78.1

O Cloud C<sup>2</sup> é uma suíte de comando e controle baseada na web e auto-hospedada para equipamentos Hak5 em rede, permitindo que você realize testes de penetração de qualquer lugar. Computadores Linux, Mac e Windows podem hospedar o servidor Cloud C<sup>2</sup>, enquanto equipamentos Hak5, como o WiFi Pineapple, LAN Turtle e Packet Squirrel, podem ser configurados como clientes.

Após configurar o servidor Cloud C<sup>2</sup> em uma máquina de acesso público (como um VPS) e os dispositivos Hak5 estarem provisionados e implantados, você pode acessar a interface web do Cloud C<sup>2</sup> para gerenciar esses dispositivos como se estivesse conectado diretamente a eles. Com vários dispositivos Hak5 implantados em um local cliente, os dados agregados oferecem uma visão geral dos ambientes com e sem fio.

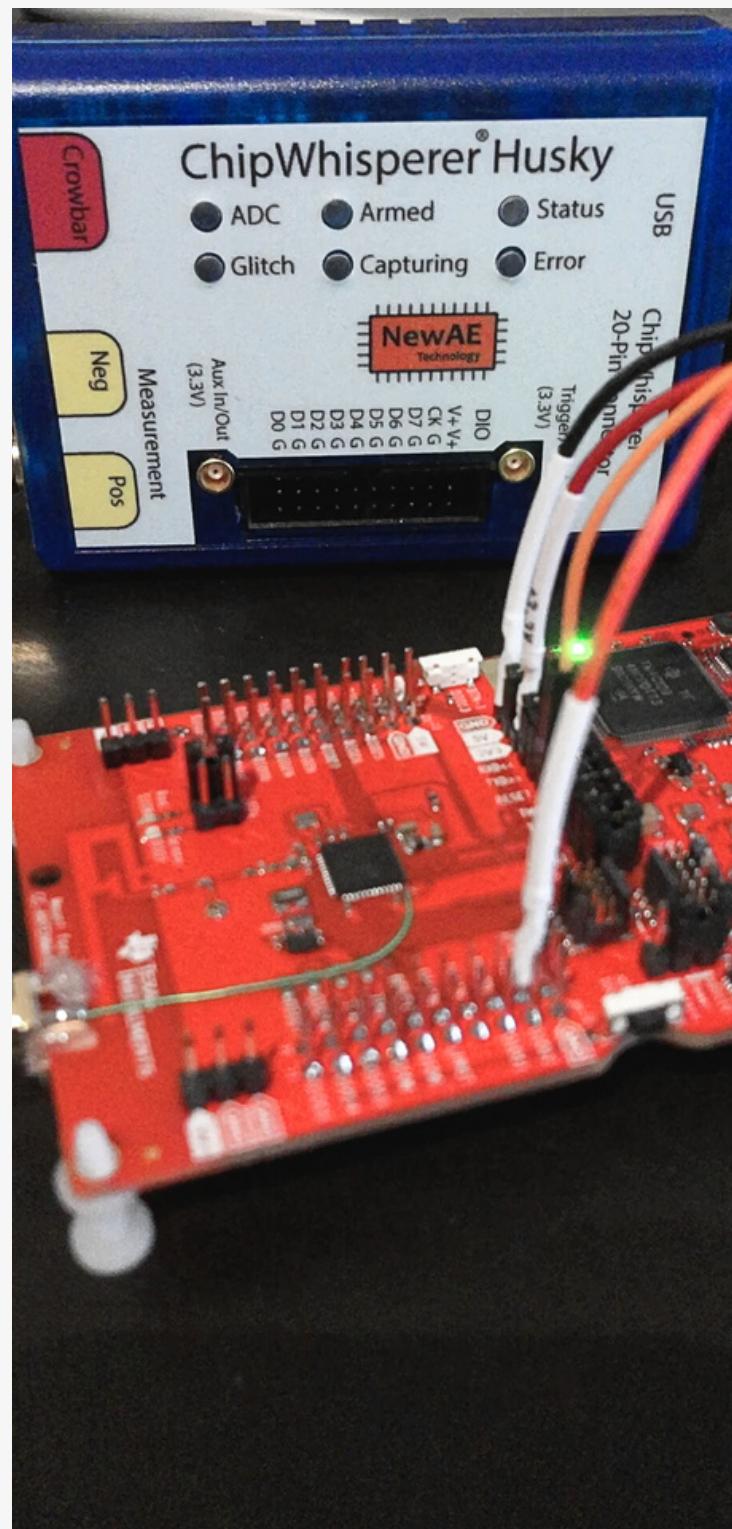


O NOVO  
ARDUINO R4  
CHEGOU, VOCÊ  
JÁ TEVE  
ACESSO?

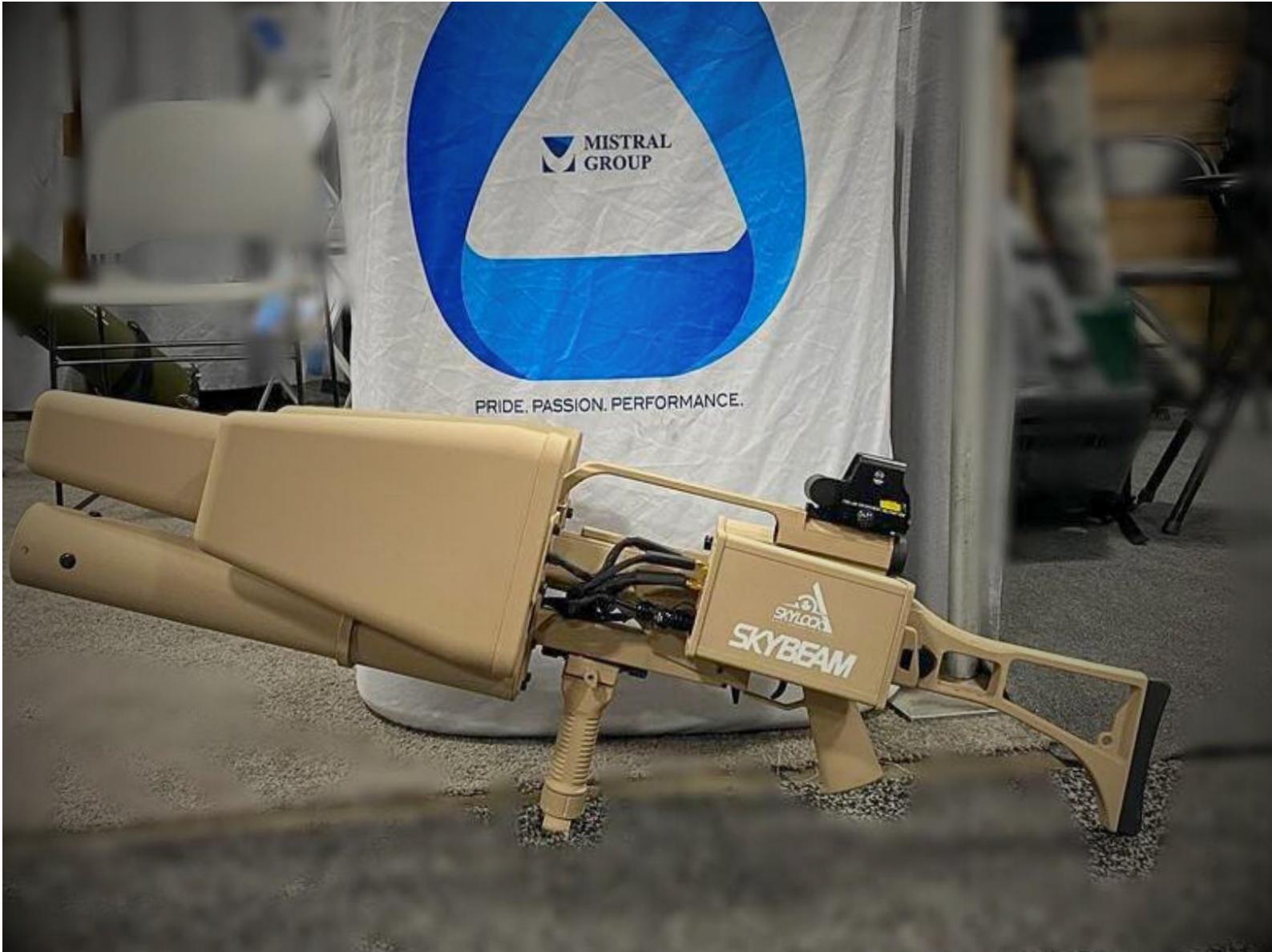
JULIO DELLA FLORA

# HUSKY

O ChipWhisperer-Husky é projetado como um pacote compacto para trabalhar com análise de potência de canal lateral e injeção de falhas. Ele se baseia em nossa experiência com o ChipWhisperer-Lite e o ChipWhisperer-Pro, incorporando novas funcionalidades como analisadores lógicos de alta velocidade (para visualizar falhas), transmissão de dados em tempo real para atacar algoritmos assimétricos, suporte para programação JTAG/SWD com um modo compatível com FTDI e pinos adicionais de expansão de I/O. O ChipWhisperer-Husky foi projetado para ser altamente acessível aos pesquisadores, mantendo nossa capacidade de oferecer suporte a longo prazo. Isso significa que, embora todo o produto não seja certificado como OSHW, o núcleo - incluindo a lógica FPGA, firmware do microcontrolador e código de computador - é de código aberto, permitindo que você faça modificações e adicione recursos.



scan or click



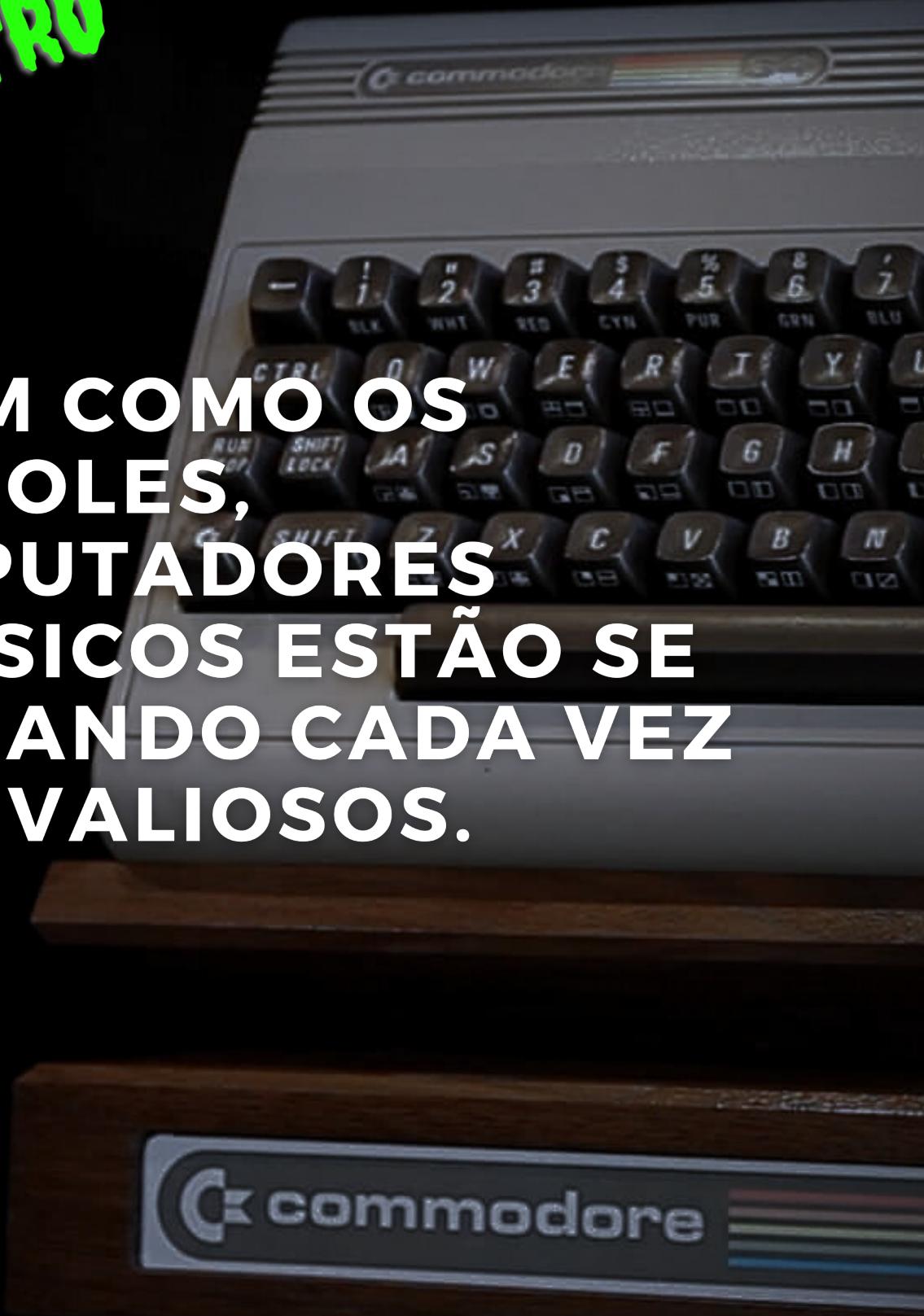
O dispositivo foi apresentado pela primeira vez pela empresa NT Service, sediada em Kaunas, Lituânia, na Exposição de Segurança e Contra-Terrorismo de 2019 em Londres. Em parceria com a empresa israelense Skylock, a NT Service também produz o sistema sob o nome "Skybeam".

## ANTI DRONE GUN

...pode ter 4 ou 6 antenas. Por padrão, há duas antenas para as bandas de frequência de 2,4 GHz e 5,8 GHz, com uma potência de 10 W cada, uma antena para a banda GPS de 1,5 GHz com uma potência de 10 W, e uma antena para a banda GLONASS de 1,5 GHz com uma potência de 10 W.

**COMPUTADOR  
RETRO**

**ASSIM COMO OS  
CONSOLES,  
COMPUTADORES  
CLÁSSICOS ESTÃO SE  
TORNANDO CADA VEZ  
MAIS VALIOSOS.**



# WIFI NUGGET DA HAK5

@juliodellaflora  
<https://juliodellaflora.com>

O WiFi Nugget é uma ferramenta open-source criada por Kody Kinzie e Alex Lynd do Hak5, projetada para tornar o aprendizado de hacking em Wi-Fi divertido e acessível. Este dispositivo tem uma pequena tela OLED, botões e a imagem de um gato, e foi criado em homenagem a um gato chamado Nugget. Embora a HakCat venda o produto pré-montado em sua loja online, entusiastas podem construir o próprio dispositivo utilizando arquivos do GitHub e comprando peças online.

A principal função do WiFi Nugget é interferir em redes Wi-Fi, emitindo comandos que afetam como as redes e dispositivos se autenticam. Além disso, pode executar versões do Deauther tool e outros ataques como o probe e beacon. A HakCat também tem outros produtos, como o USB Nugget, que realiza funções similares porém em USBs.

O WiFi Nugget é baseado no microcontrolador ESP8266, tornando-o uma ferramenta acessível para aprender sobre hacking de Wi-Fi. Apesar de não ser extremamente poderoso, pode causar interrupções, principalmente em redes e dispositivos mais antigos.



**saiba mais em:**  
[juliodellaflora.com](https://juliodellaflora.com)

# TIGARD

@juliodellaflora  
<https://juliodellaflora.com>

Tigard é baseado na plataforma FT2232H.

Sua principal força reside na sua simplicidade e ampla compatibilidade.

Incorporando pin-outs comumente usados, um chicote de fiação rotulado,

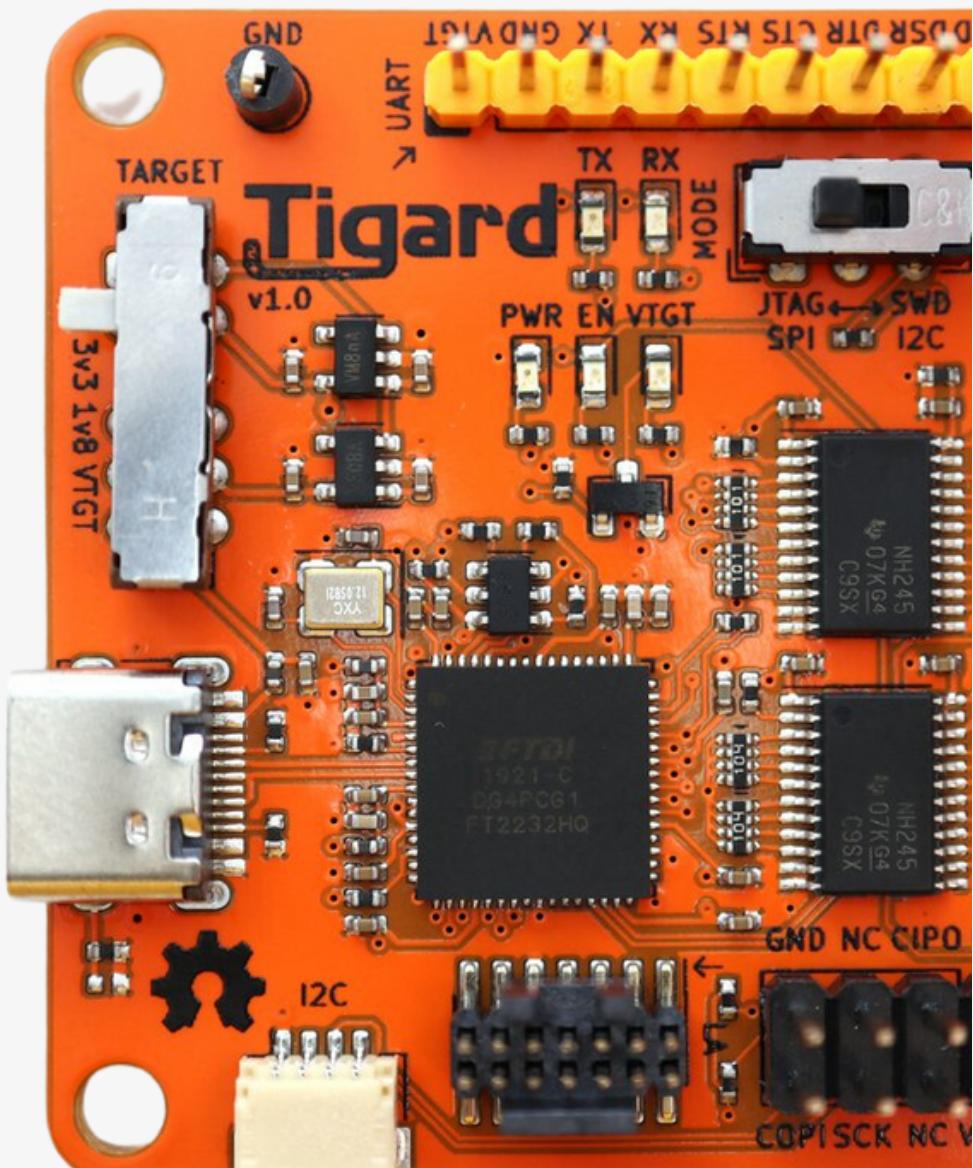
conversão de nível a bordo e uma conexão de analisador lógico, Tigard

elimina a necessidade de várias ferramentas. Como uma solução "tudo em um", serve como um excelente complemento ou até mesmo uma substituição para dezenas de outras ferramentas baseadas em chips FTDI.

Seja você um novato no hacking de hardware ou simplesmente procurando uma solução rápida e simples, Tigard é projetado para ser o seu primeiro passo ideal.

Além disso, graças à sua compatibilidade nativa com ferramentas populares como

OpenOCD e FlashROM, não há necessidade de ferramentas específicas para Tigard para interface com seus alvos. E se a personalização for necessária, a interface FT2232H garante flexibilidade e adaptabilidade.



# BIT MAGIC

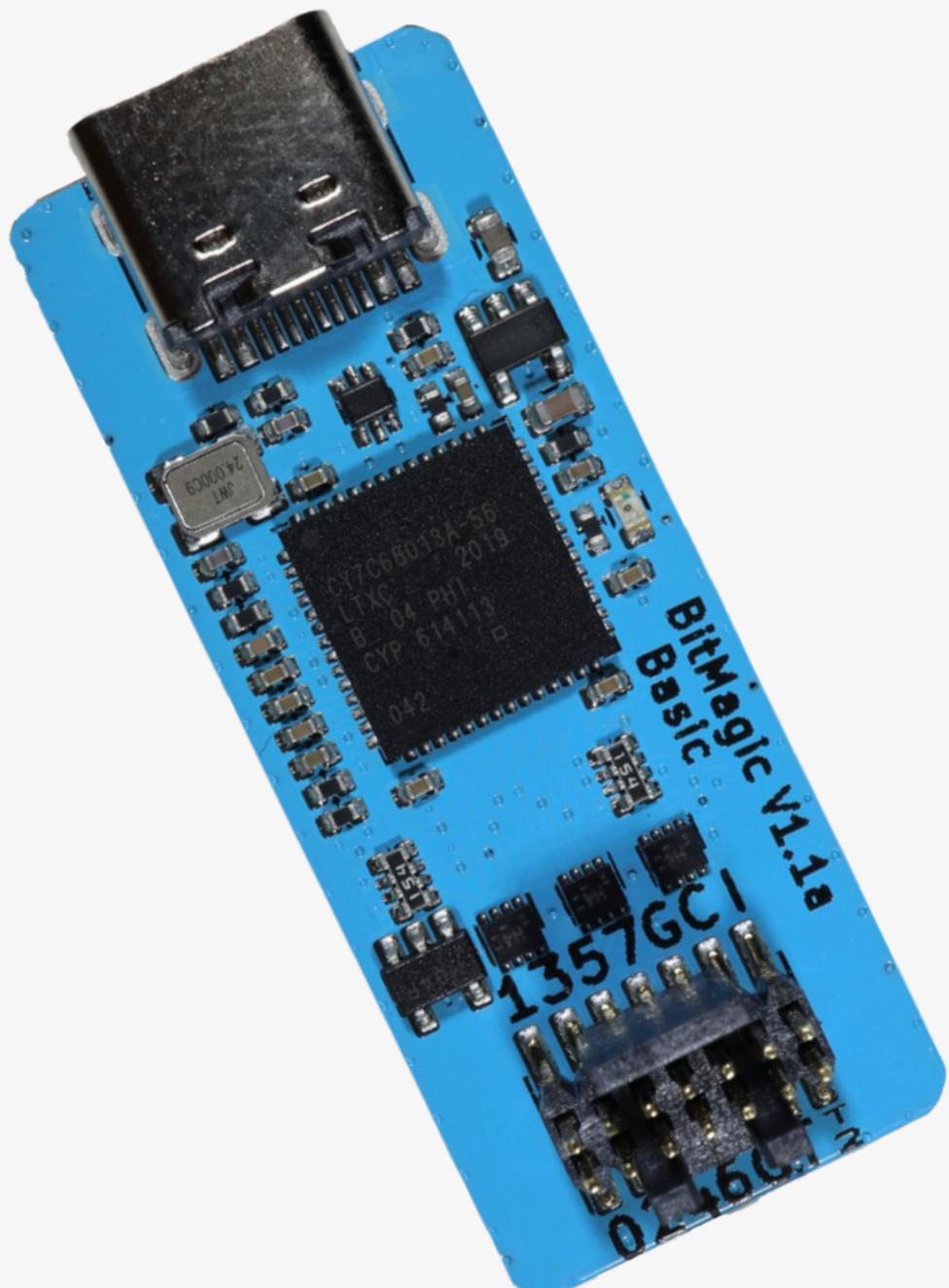
@juliodellaflora  
<https://juliodellaflora.com>

O BitMagic Basic é um analisador lógico baseado na plataforma de hardware aberto FX2. Ele foi especificamente projetado para funcionar com o firmware de código aberto fx2lafw e o conjunto de analisadores lógicos de código aberto Sigrok, incluindo a interface gráfica Pulseview.

Com a capacidade de suportar oito canais amostrados em até 24 Msps, o BitMagic Basic opera como qualquer outro analisador lógico. Ele inclui um chicote de fiação rotulado, permitindo sua utilização com qualquer cabeçalho de pinos de 2,54 mm ou seus clipes de sonda favoritos.

Um destaque é o cabo de 14 pinos que permite conexão direta com o Tigard.

Quando tudo está conectado, o Pulseview pode ser usado para monitorar todas as comunicações entre o Tigard e o sistema alvo. Isso é particularmente útil para depurar questões elétricas, de protocolo e de integridade de sinal.



**saiba mais em:**  
[juliodellaflora.com](https://juliodellaflora.com)

# Y U B I K E Y   5 C

## N F C

@juliodellaflora  
<https://juliodellaflora.com>

A era da autenticação digital evolui constantemente, e a Yubico está à frente dessa transformação. Apresentando o YubiKey 5C NFC, uma chave de segurança física inovadora que promete revolucionar a maneira como vemos a autenticação em dois fatores. Esta chave não apenas adota o padrão USB-C, tornando-a compatível com a maioria dos dispositivos modernos, como também incorpora a tecnologia NFC para uma autenticação por aproximação segura, distanciando-se de vulnerabilidades conhecidas em métodos Bluetooth. Desenvolvido para funcionar em uma ampla variedade de plataformas - desde computadores Windows, macOS e Linux até smartphones Android e iOS - o YubiKey 5C NFC é mais do que apenas um dispositivo de segurança. Ele é uma promessa de proteção robusta contra ameaças como ataques de phishing e man-in-the-middle. Graças à sua capacidade de armazenar chaves únicas e fortes fisicamente, torna-se uma ferramenta essencial para aqueles que buscam uma camada extra de segurança. E, com suporte a uma variedade de protocolos de autenticação, os usuários podem contar com uma solução versátil para suas necessidades digitais.



# ENTREVISTA COM O TESKE

Em um mundo cada vez mais interconectado, a segurança de sistemas é de suma importância. Enquanto muitos focam apenas na segurança de software, uma área que muitas vezes é negligenciada, mas é igualmente crucial, é a segurança de hardware. Neste contexto, destaca-se Lucas Teske, especialista em hardware hacking e uma mente brilhante no panorama atual da segurança cibernética. Lucas carrega uma perspectiva única que combina um entendimento profundo das leis naturais com o complexo mundo da tecnologia.

Este artigo explora a jornada, insights e sabedoria de Lucas Teske, oferecendo um olhar profundo sobre o fascinante mundo do pentest de hardware e as nuances de manter sistemas seguros em uma era digital. Através de uma série de perguntas, mergulhamos no coração de seus desafios, conquistas e visão para o futuro da segurança de hardware. Se você é um profissional iniciando na área ou simplesmente alguém curioso sobre como o hardware que usamos todos os dias é mantido seguro, esta entrevista com Lucas é uma leitura obrigatória.

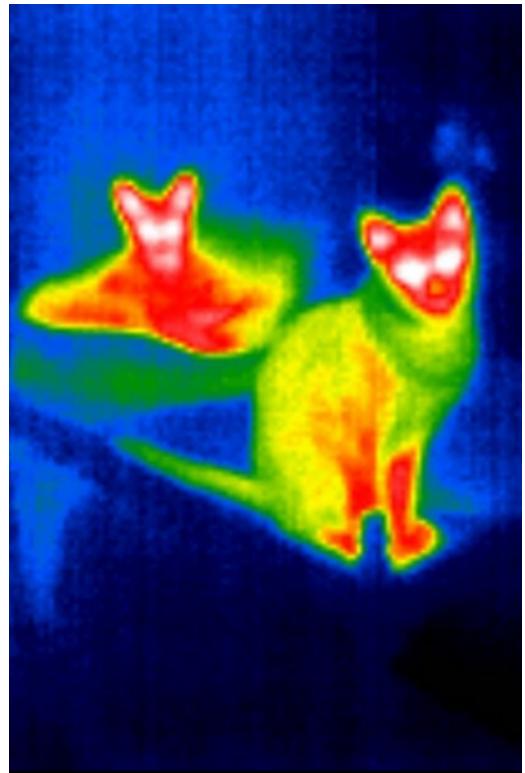


Lucas é analista de segurança em hardware e exímio apreciador de gatos...

# VAMOS PARA AS PERGUNTAS!

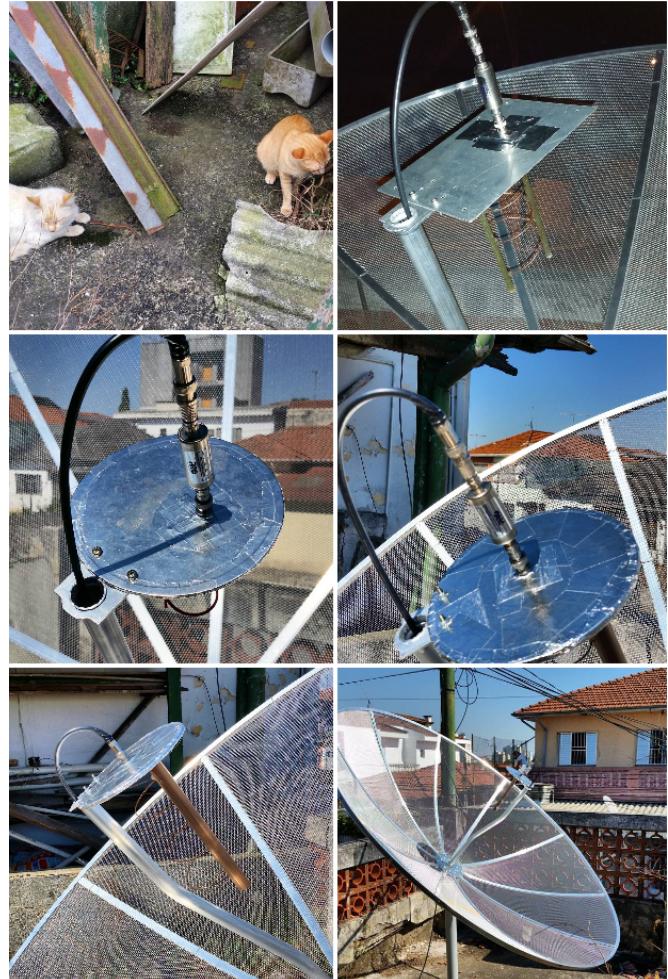
# COMO VOCÊ COMEÇOU NA ÁREA DE PENTEST EM HARDWARE E QUAL FOI O PAPEL DA SUA FORMAÇÃO EM FÍSICA NESSE PROCESSO?

Comecei de maneira meio aleatória. Eu já fazia engenharia reversa e hardware hacking a bastante tempo, mas uma amiga minha me chamou para ir trabalhar na PRIDE Security e eu topei ir. No começo estava meio inseguro (especialmente por que não é só hardware hacking) por que nunca tinha trabalhado mesmo na área, mas no fim deu tudo certo. O técnico em eletrônica foi o que me ajudou a ter a base para ataques de hardware, mas os conhecimentos em física ajudam para planejar ataques mais complexos geralmente na área de Fault Injection (Injeção de Falhas) e extração de informação via Side-Channel.



...IMAGEM TERMICA DOS GATOS DO LUCAS





## QUAIS SÃO OS DESAFIOS MAIS COMUNS QUE VOCÊ ENFRENTA AO CONDUZIR TESTES DE INVASÃO EM SISTEMAS EMBARCADOS, E COMO VOCÊ OS SUPERA?

O desafio mais comum é analisar firmware baremetal (aquele quando você não tem um sistema operacional). Em geral a maior dificuldade é que essas análises, levam muito mais tempo pois nem sempre há identificadores de versões de biblioteca e vulnerabilidades conhecidas logo de cara, o que geralmente é comum para outros tipos de pentest. Em geral eu tento procurar por padrões conhecidos de bibliotecas que eu já encontrei anteriormente, e fazer comparação de firmware de dispositivos similares.



2.832 publicações      4.496 seguidores

**Lucas Teske**

Cientista

💻 #Programming 🦷 #Hacking

📡 #SDR 🛸 #Satellites

⚡ #Tesla Coils ✈️ #Drones

BR / US

📡 PU2NVX

'Prefiro um #ódio sincero, do que um #amor falso'

🔗 [lucasteske.dev](https://lucasteske.dev)



ENCONTRO HISTÓRICO COM O SERJÃO DOS  
FOGUETE!

## COMO A SEGURANÇA DO HARDWARE DIFERE DA SEGURANÇA DO SOFTWARE, E QUAIS SÃO AS PRINCIPAIS VULNERABILIDADES QUE VOCÊ FREQUENTEMENTE ENCONTRA EM SISTEMAS DE EMBARCADOS?

Eu geralmente gosto de falar que teste de hardware se resume basicamente em tornar o teste de hardware em um de software. O objetivo principal costuma tentar enumerar os meios (de hardware) que você pode usar para extrair a firmware, alterar seu comportamento e talvez induzir a fraudes. As vulnerabilidades mais comuns é falta de verificação de integridade (o que permite alteração do software embarcado) e ausência de criptografia de conteúdo (que permite inspecionar o conteúdo e programa).



Instagram do Lucas

## QUAIS SÃO AS MELHORES PRÁTICAS OU FERRAMENTAS QUE VOCÊ RECOMENDARIA PARA ALGUÉM QUE ESTÁ COMEÇANDO NA ÁREA DE PENTEST EM HARDWARE?

A melhor prática é não subestimar o quanto simples pode ser a segurança do dispositivo. As vezes até mesmo os hardwares considerados mais seguros tem interfaces expostas que permitem execução livre de comandos ou código, e estão protegidas apenas pela falta de um indicativo na PCB falando que aquilo é uma interface de acesso. Hoje em dia eu recomendo fortemente pra alguém que está começando se familiarizar em escrever código para microcontroladores (Arduino, Raspberry Pi Pico, etc...) e tentar "brincar" com hardwares de prateleira existentes (tipo câmeras IP chinesas, roteadores, etc...). Esses alvos costumam ser bem vulneráveis devido a seu baixo custo, e é um excelente meio de começar a aprender.



Instagram do Lucas



## QUE CONSELHO VOCÊ DARIA PARA PROFISSIONAIS QUE ESTÃO INICIANDO NA ÁREA DE HARDWARE HACKING E PENTEST, E O QUE VOCÊ GOSTARIA DE TER SABIDO QUANDO COMEÇOU SUA CARREIRA?



H2HC 2022, O BOBÃO DA ESQUERDA FOI QUEM ESCREVEU ESSA REVISTA.

O melhor conselho é: Não tenha medo de perguntar e estude eletrônica. Um bom conhecimento de eletrônica é metade do caminho e é indispensável no dia a dia.

Não precisa nem ser uma faculdade de engenharia (embora seja mais interessante), o conhecimento de nível técnico é suficiente para começar na área e poder aprender as coisas na prática. A segurança de hardware ainda está na "época de ouro" onde existem muitas coisas com vulnerabilidades muito simples, então é o momento ideal para se começar na área e aprender.



Instagram do Lucas



## NFC/RFID BIOCHIP IMPLANTS



Existem dois tipos de implantes de biohacking nos quais estamos focando no momento: o implante passivo de transponder RFID (também conhecido como "implantes de chip") e os implantes magnéticos (implantes de ímã biosseguros). Nossos implantes de chip são populares para aplicações de controle de identidade e acesso, enquanto nossos implantes magnéticos são comumente usados para detecção de campo magnético e aplicações de interação magnética.

(dangerousthings.com)

@JULIODELLAFLORA

# CYBERDECK CAFE

Um cyberdeck é um computador pessoal móvel encontrado em muitos romances e jogos de vídeo cyberpunk que é usado por hackers ou "Deckers" para se conectar temporariamente à ciberespaço, ou seja, "plug in". Algumas das primeiras aparições de cyberdecks foram na Trilogia do Sprawl de William Gibson no início dos anos 80..

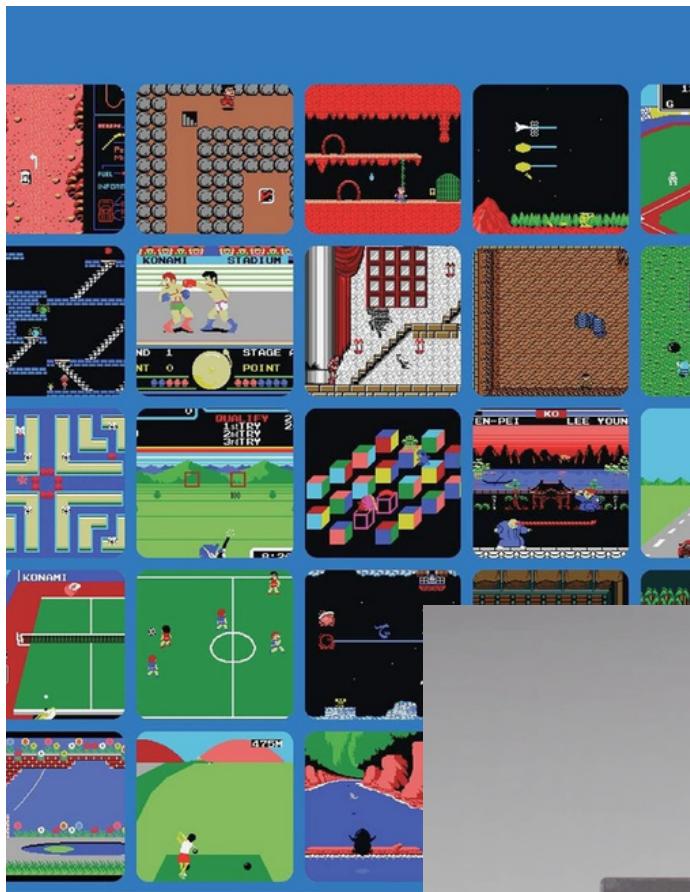


No mundo real, os cyberdecks são "computadores artesanais" frequentemente alimentados por placas-mãe de computadores únicos com algum tipo de display e teclado feito no estilo cyberpunk

Você pode encontrar mais informações sobre o projeto em [cyberdeck.cafe](http://cyberdeck.cafe) não é necessário ter noções de programação, é possível construir ou comprar um cyberdeck



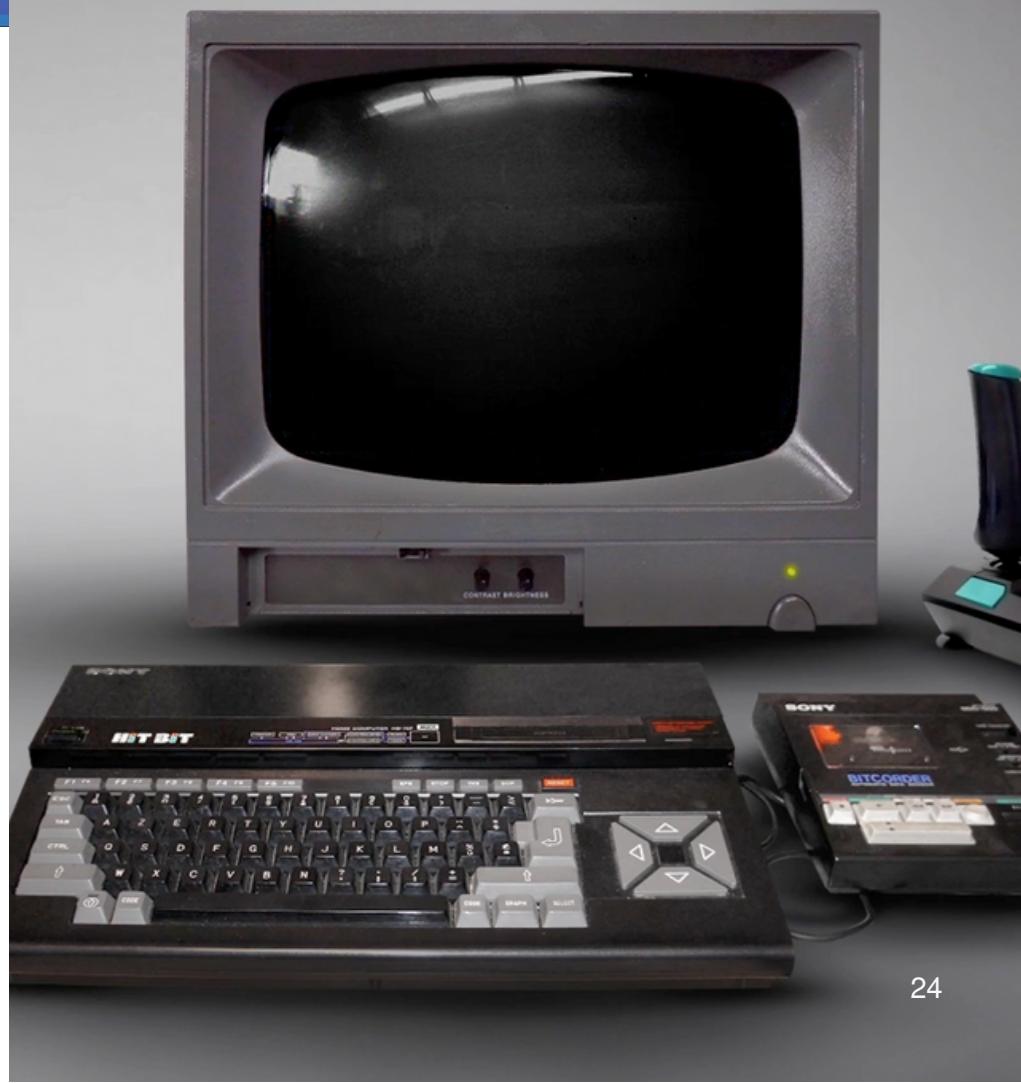
@JULIODELLAFLORA



VOCÊ JÁ USOU  
UM MSX? QUAL  
ERA O MODELO?

## PADRÃO MSX

O MSX foi uma arquitetura de microcomputadores pessoais criada no Japão em 1983 e apresentada em 27 de junho do mesmo ano, que estabeleceu um padrão para desenvolvedores de hardware. Foi desenvolvido por Kazuhiko Nishi, vice-presidente da ASCII Corporation, que na época representava a Microsoft no Japão. O objetivo era permitir que várias empresas de eletrônicos produzissem seus próprios computadores, mantendo um mínimo de compatibilidade entre eles, mas ainda assim diferenciando-os com recursos adicionais. No entanto, a compatibilidade com outros micros do padrão MSX seria mantida.



# A HISTÓRIA DO HACKING

A função de um hacker é explorar e experimentar sistemas e redes de computadores para descobrir vulnerabilidades de segurança e melhorar a proteção dos sistemas.

**A**história do hacking remonta às primeiras décadas da computação moderna. Nos anos 60, as primeiras redes de computadores foram criadas para fins militares e de pesquisa acadêmica. Essas redes eram pequenas e isoladas, e o acesso era estritamente controlado. Na década de 70, a popularidade dos computadores pessoais começou a crescer, e surgiram as primeiras comunidades de usuários de computador. Foi nessa época que o termo "hacker" começou a ser usado para descrever pessoas que tinham um conhecimento profundo de computadores e redes, e que usavam esse conhecimento para explorar e experimentar com sistemas de computador.

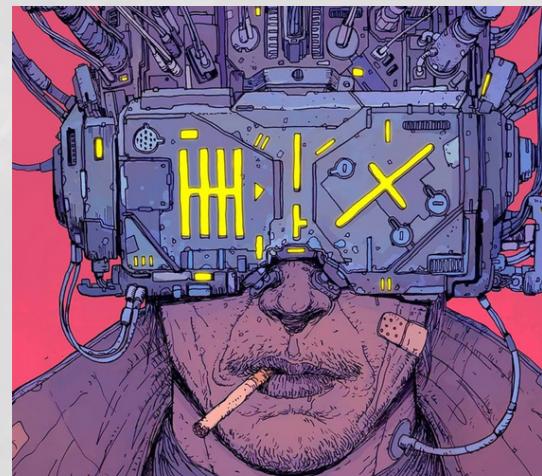
A maioria desses hackers eram jovens entusiastas que queriam explorar os limites da tecnologia. Eles compartilhavam suas descobertas com outros hackers em redes locais e, eventualmente, em BBSs (Bulletin Board Systems), que eram as primeiras formas de comunicação online.

Nos anos 80, a internet começou a se tornar popular, e o número de hackers aumentou exponencialmente. Foi nessa época que surgiram os primeiros grupos de hackers, como o Chaos Computer Club na Alemanha e o Legion of Doom nos Estados Unidos.

Esses grupos de hackers eram frequentemente motivados pela curiosidade e pelo desafio de invadir sistemas de computador. Eles exploravam falhas de segurança e desenvolviam técnicas para contornar as proteções que os administradores de sistema haviam implementado.

Na década de 90, o termo "hacker" começou a ser associado cada vez mais com os crackers e com a atividade criminosa. O governo e as empresas começaram a investir em segurança de computadores para proteger seus sistemas contra ataques de hackers.

Hoje, o hacking é uma atividade amplamente reconhecida e muitos hackers trabalham legalmente como consultores de segurança de computadores ou em empresas de tecnologia.



"Hacker" é um indivíduo com habilidades avançadas em computação que usa sua experiência para explorar e testar sistemas de computador.

# HARDWARE HACKING

O hardware hacking tem sido uma técnica popular entre os hackers desde o surgimento dos primeiros computadores pessoais nos anos 70. O hardware hacking envolve a manipulação de dispositivos eletrônicos, como placas de circuito impresso, chips e outros componentes, para modificar ou explorar as funções do dispositivo.

Nos primeiros dias da computação, os computadores eram caros e de acesso limitado, tornando o hardware hacking uma atividade restrita a entusiastas e profissionais. Os primeiros hackers que se envolveram em hardware hacking eram engenheiros eletrônicos que trabalhavam em laboratórios de pesquisa, e que estavam interessados em explorar os limites da tecnologia.

No entanto, com o tempo, a popularidade dos computadores pessoais cresceu, e o hardware hacking se tornou uma técnica mais acessível. Os primeiros hackers de hardware começaram a experimentar com a modificação de placas de circuito impresso e chips, desenvolvendo técnicas para ajustar o desempenho e expandir as funcionalidades dos dispositivos.

Com o tempo, o hardware hacking evoluiu e se expandiu para incluir a exploração de dispositivos eletrônicos em geral, incluindo telefones, dispositivos de armazenamento e sistemas de segurança. Os hackers de hardware também começaram a trabalhar em conjunto com hackers de software para desenvolver soluções mais avançadas e integradas.

Hoje, o hardware hacking é uma técnica amplamente reconhecida e usada em uma variedade de contextos. Muitos hackers trabalham legalmente como engenheiros de hardware ou consultores de segurança de dispositivos eletrônicos. No entanto, o hardware hacking ilegal também é uma ameaça real e pode ser usado para fins maliciosos, como roubo de informações ou sabotagem de dispositivos.

A história do hardware hacking é uma história de inovação e experimentação, em que os hackers têm usado suas habilidades e conhecimentos para explorar e modificar dispositivos eletrônicos e expandir as possibilidades da tecnologia. A técnica tem evoluído ao longo do tempo e continua sendo uma técnica importante para hackers e profissionais de segurança de dispositivos eletrônicos.

# LOPHT

A origem do L0pht remonta a Brian Oblivion e Count Zero, dois de seus fundadores, que compartilhavam um loft em South Boston com suas esposas que administravam um negócio de chapéus na metade do espaço. Foi lá que eles começaram a experimentar com seus próprios computadores pessoais, equipamentos adquiridos no Flea no MIT e itens encontrados por meio de "dumpster diving" em locais locais de interesse.

Fundado em 1992, o L0pht rapidamente se tornou um local para seus membros armazenarem seus equipamentos de computador e trabalharem em vários projetos. Com o tempo, eles abandonaram seus empregos diurnos para iniciar um empreendimento comercial chamado L0pht Heavy Industries, um think tank de hackers que lançou inúmeras recomendações de segurança e produziu ferramentas de software amplamente utilizadas.

Em 1997, alguns membros do L0pht discutiram projetos e conquistas recentes, Windows NT, novos projetos, tendências emergentes e deficiências em tecnologias em uma sessão de perguntas e respostas no Beyond HOPE no Puck Building em Nova York.

Em outubro de 1999, o L0pht foi apresentado em um extenso artigo na revista New York Times Sunday Magazine. Jeffrey Hunker, Diretor de Proteção da Informação do NSC, comentou sobre o L0pht, afirmando que seu objetivo era ajudar a melhorar o estado da arte em segurança e ser uma voz crítica para a indústria.

Em janeiro de 2000, a L0pht Heavy Industries fundiu-se com a startup @stake, completando a transição do L0pht de uma organização subterrânea para uma empresa de segurança de computadores "whitehat". Posteriormente, a Symantec adquiriu a @stake em 2004 e a Veracode foi fundada em 2006 como uma spin-out da Symantec, baseada em protótipos e ideias incubadas no L0pht.

Em 2008, vários membros do L0pht participaram de um painel em um grupo de profissionais de segurança da informação na SOURCE: Boston. O painel incluiu membros como Weld Pond, John Tan, Mudge, Space Rogue, Silicose e Dildog.



ORIGINAL MOTION PICTURE SOUNDTRACK

DICA DE  
FILME

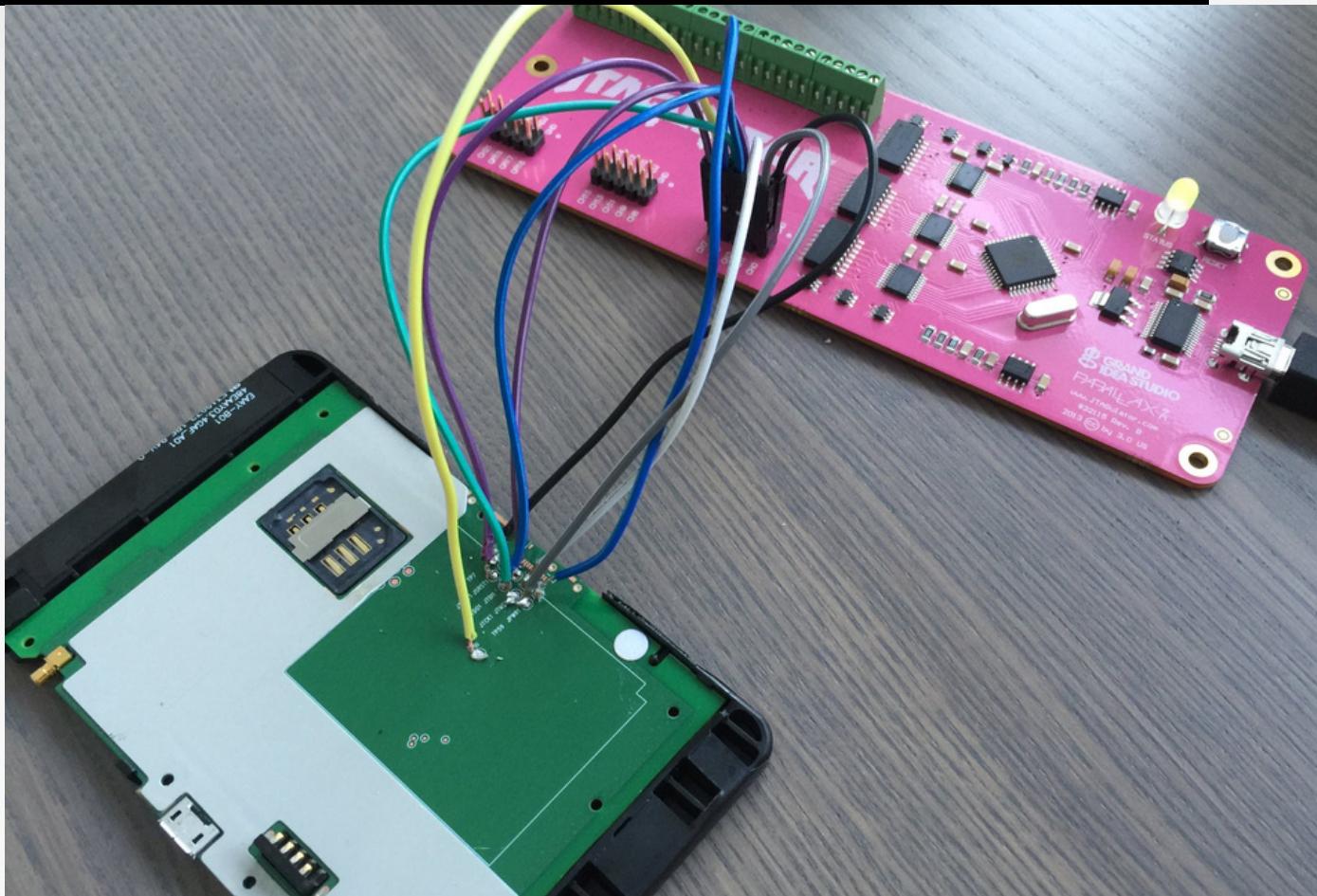
# O FILME "PASTELÃO" QUE SE TRANSFORMOU EM ÍCONE CULT DA COMUNIDADE HACKER

ASSISTA "HACKERS" DE 1995

AN IAIN SOFTLEY FILM

**HACKERS**

# JTAGULATOR



As interfaces de depuração on-chip (OCD) podem fornecer controle de nível de chip de um dispositivo alvo e são um vetor primário usado por engenheiros, pesquisadores e hackers para extrair o código ou dados do programa, modificar o conteúdo da memória ou afetar a operação do dispositivo em tempo real. Dependendo da complexidade do dispositivo alvo, localizar manualmente as conexões OCD disponíveis pode ser uma tarefa difícil e demorada, exigindo às vezes destruição ou modificação física do dispositivo.

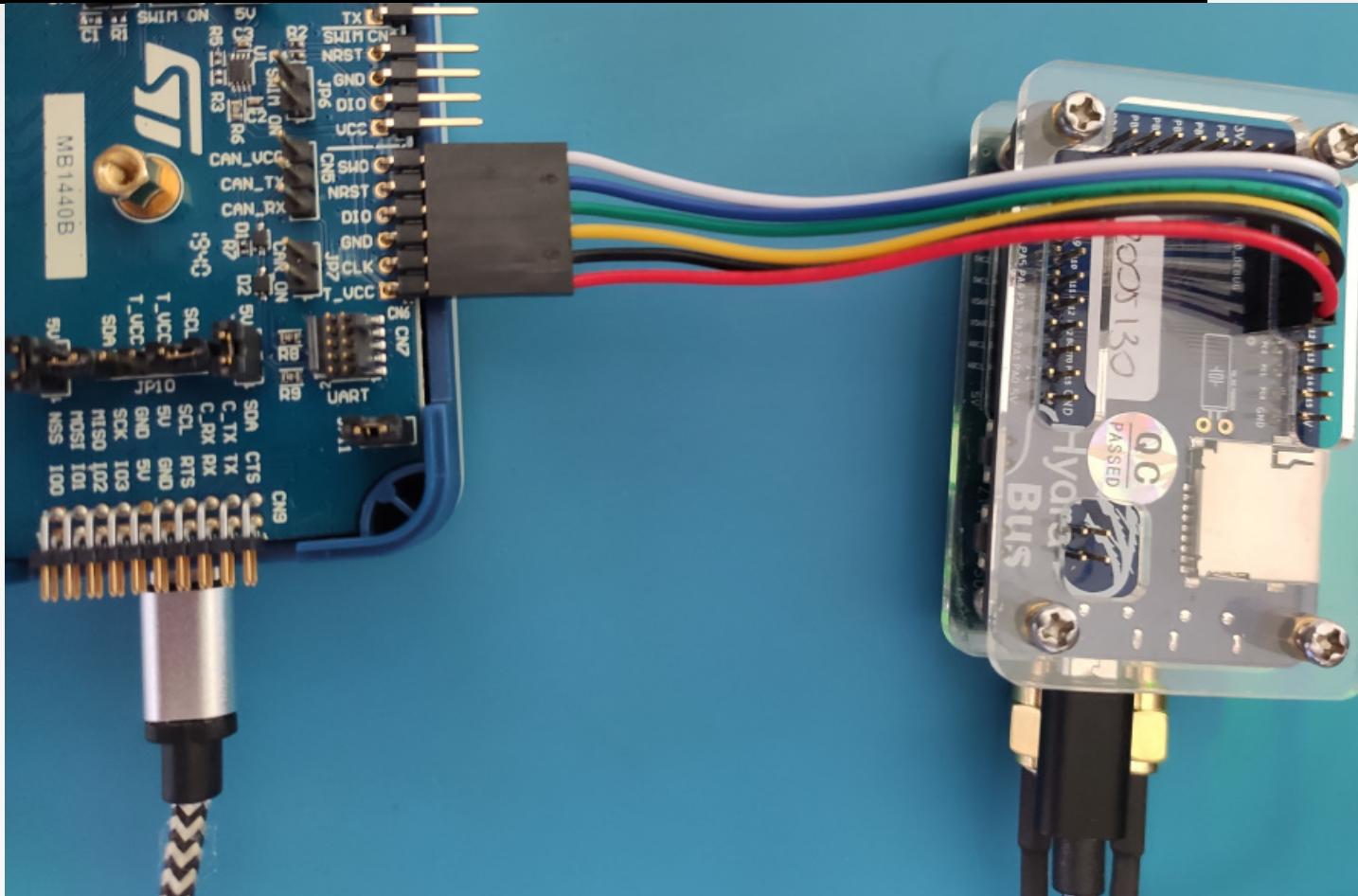
O JTAGulator é uma ferramenta de hardware de código aberto que ajuda a identificar as conexões OCD a partir de pontos de teste, vias ou pads de componente em um dispositivo alvo.

# NFCKill



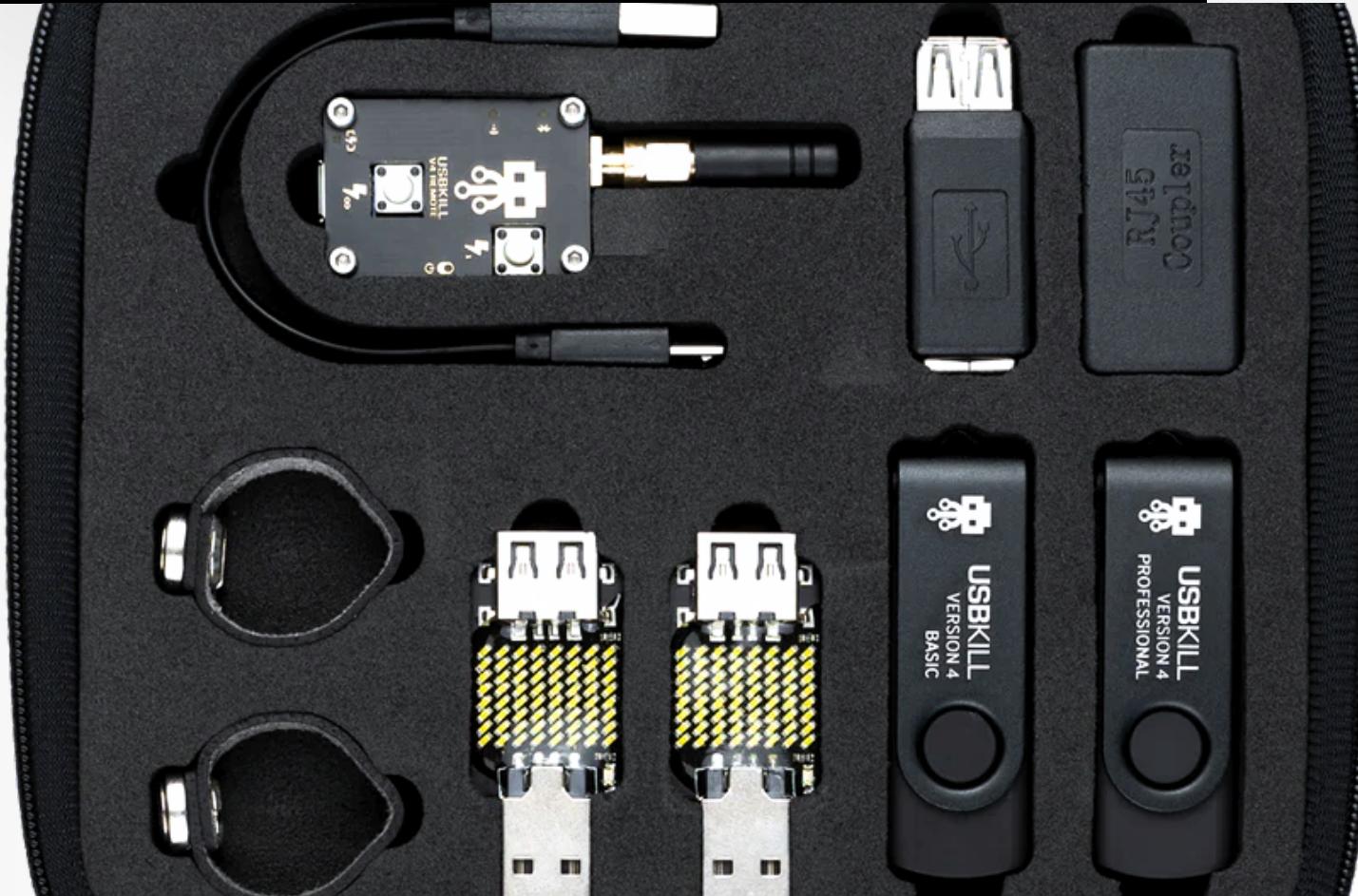
O NFC Kill é a única ferramenta de fuzzing RFID no mundo. É utilizada para desativar com segurança crachás RFID, testar hardware RFID, auditar modos de falha de controle de acesso e investigar/explorar superfícies de ataque RFID durante testes de penetração. É a única ferramenta disponível para desativar de forma segura e permanente cartões RFID em conformidade com o GDPR. Clientes em ambientes de alta segurança (aplicação da Lei, Governo, Empresas e Indústria) utilizam o NFC Kill como parte de sua Política de Destrução de Dados.

# HydraBus



O HydraBus v1.0 é um hardware multi-ferramenta de código aberto para qualquer pessoa interessada em aprender/desenvolver/depurar/hackear hardware embarcado seja ele básico ou avançado. O MCU é um dos Cortex M4F mais rápidos do mercado e é mais de 40X mais rápido que um Arduino. O HydraBus também pode ser usado como bancada de testes para validação de hardware com a ajuda de script python incorporado ou firmware nativo C/C++, e é uma ferramenta perfeita para testes de invasão de hardware usando para 1-wire, 2-wire e 3-wire, SWD & JTAG, SMARTCARD, NAND flash, Wiegand, LIN, CAN, analisador lógico, SPI, I2C, UART, ADC (0 a 3,3V), DAC (0 a 3,3V, triângulo, ruído), PWM (1Hz a 42MHz, ciclo de trabalho 0 a 100%), GPIO (Entrada/Saída/Open-Drain). O HydraBus é evolutivo com a ajuda de extensões de hardware "Shield" (o primeiro Shield é o HydraNFC).

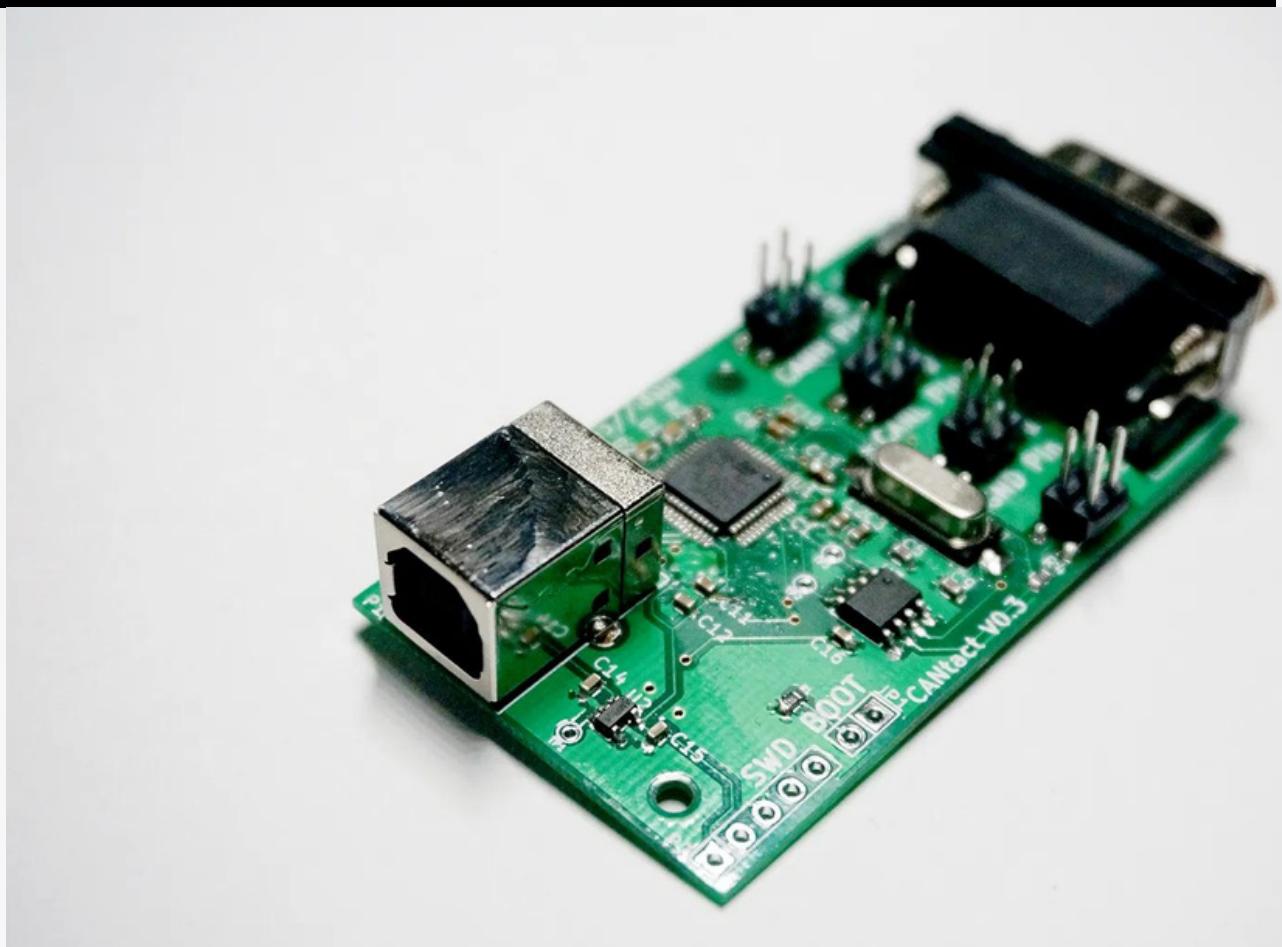
# USB KILL



O USB Killer é um dispositivo de teste aprovado pela CE e FCC, projetado para avaliar a eficácia do circuito de proteção contra surtos de eletrônicos. Quando conectado a um dispositivo, o USB Killer rapidamente carrega seus capacitores usando as linhas de energia USB e, em seguida, descarrega -200VDC nas linhas de dados do dispositivo hospedeiro. Esse processo é repetido várias vezes por segundo até que o USB Killer seja removido. Em outras palavras, quando usado em equipamentos desprotegidos, o USB Killer desativa instantaneamente e permanentemente o hardware-alvo.

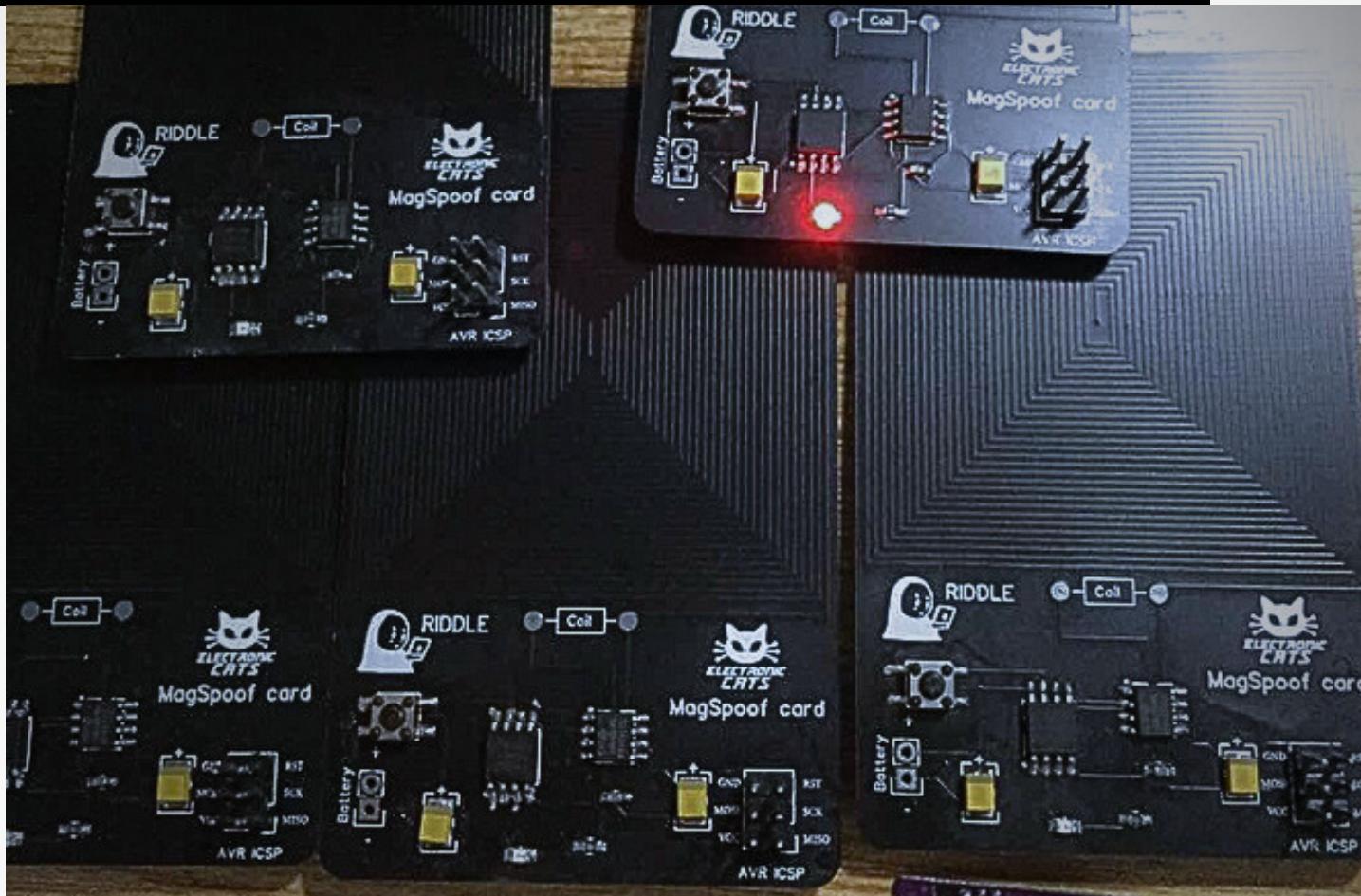
O USB Killer não requer baterias e pode ser usado um número ilimitado de vezes. Seu tamanho compacto e caixa em forma de pen-drive o tornam um dispositivo valioso para testes de penetração e segurança de hardware. O USB Kill V3.0 também vem em uma edição anônima, sem nenhum logotipo ou marca, em uma caixa genérica de pendrive USB.

# CANTact



O CANtact é uma interface USB de código aberto do Controller Area Network (CAN) para o seu computador, permitindo conectar-se a sistemas CAN bus, incluindo carros, veículos pesados e sistemas de automação industrial. Com um design de canal único, é suportado pelo SocketCAN, Cantact App e pyvit, e pode ser usado em sistemas operacionais Linux, OS X e Windows. O hardware e firmware são de código aberto e estão disponíveis no Github, projetados no KiCad, uma ferramenta gratuita e de código aberto para design de hardware. Com o uso de um cabo OBD-II para DE9, é fácil acessar o barramento CAN OBD-II de qualquer veículo com suporte para CAN. Este é um projeto verdadeiramente de código aberto, com todos os arquivos de design disponíveis sob uma licença permissiva. Ele funciona em Mac, Linux e Windows, e pode ser facilmente programado usando uma biblioteca Python de código aberto especialmente projetada para hackers.

# MagSpoof



O Magspoof, criado originalmente por Samy Kamkar, é um emulador sem fio de tarja magnética. Este pequeno dispositivo incrível pode emular todas as três trilhas de um cartão de faixa magnética sem precisar ser deslizado em uma leitora. A Rysc Corp revisou o design original para incluir uma antena integrada, um interruptor liga/desliga e um conveniente suporte para bateria de célula de moeda. O MagSpoof é entregue totalmente montado, programado e testado (incluindo as baterias).

# HACKING

A HISTÓRIA ATRAVÉS DOS ANOS



5

PESQUISADORES  
DA ÁREA



@juliodellaflora



Quais perfis você  
precisa seguir  
para se manter  
atualizado?



**JOE GRAND**

**JULIO DELLA FLORA**

# JOE GRAND

Joe Grand é um hacker e engenheiro de hardware altamente respeitado e conhecido por suas habilidades em desmontar e explorar dispositivos eletrônicos. Ele é formado em engenharia elétrica e tem mais de 20 anos de experiência em hardware hacking e segurança cibernética. Grand é o fundador da Grand Idea Studio, uma empresa que desenvolve produtos de hardware personalizados e oferece serviços de consultoria em segurança cibernética.

Ele também é conhecido por suas aparições em programas de TV, incluindo a série "Prototype This!" do Discovery Channel, onde ele liderou uma equipe que construiu protótipos de dispositivos eletrônicos inovadores. Grand é um defensor da comunidade de hackers e já palestrou em diversas conferências de segurança cibernética ao redor do mundo. Ele também é o autor de vários livros sobre hardware hacking e segurança cibernética, que são referência na área.





# COLIN O'FLYNN

Colin O'Flynn é um renomado pesquisador e especialista em hardware hacking. Ele é conhecido por suas habilidades em invadir diversos dispositivos eletrônicos, incluindo medidores inteligentes, câmeras digitais e dispositivos médicos.

O'Flynn é formado em engenharia elétrica e tem um doutorado na área, onde se concentrou em circuitos integrados para sistemas de comunicação sem fio. Além de suas realizações técnicas, ele também é reconhecido por seu compromisso com a educação e a conscientização na área de segurança cibernética.

O'Flynn é o criador do ChipWhisperer, uma ferramenta de código aberto para análise e manipulação de microcontroladores que se tornou amplamente utilizada na comunidade de hardware hacking. Ele é frequentemente convidado para palestrar em conferências de segurança cibernética em todo o mundo e é considerado uma figura altamente qualificada e respeitada no campo.





# TRAVIS GOODSPEED

Travis Goodspeed é um experiente hacker de hardware e especialista em segurança cibernética. Ele é conhecido por suas contribuições no campo de análise de dispositivos eletrônicos, incluindo o desenvolvimento de ferramentas para analisar e manipular microcontroladores. Goodspeed é um membro ativo da comunidade de hackers e é comprometido com a ética hacker e a educação em segurança cibernética.

Ele também já palestrou em diversas conferências de segurança cibernética e hardware hacking em todo o mundo, e é reconhecido como uma figura altamente qualificada e respeitada no campo.



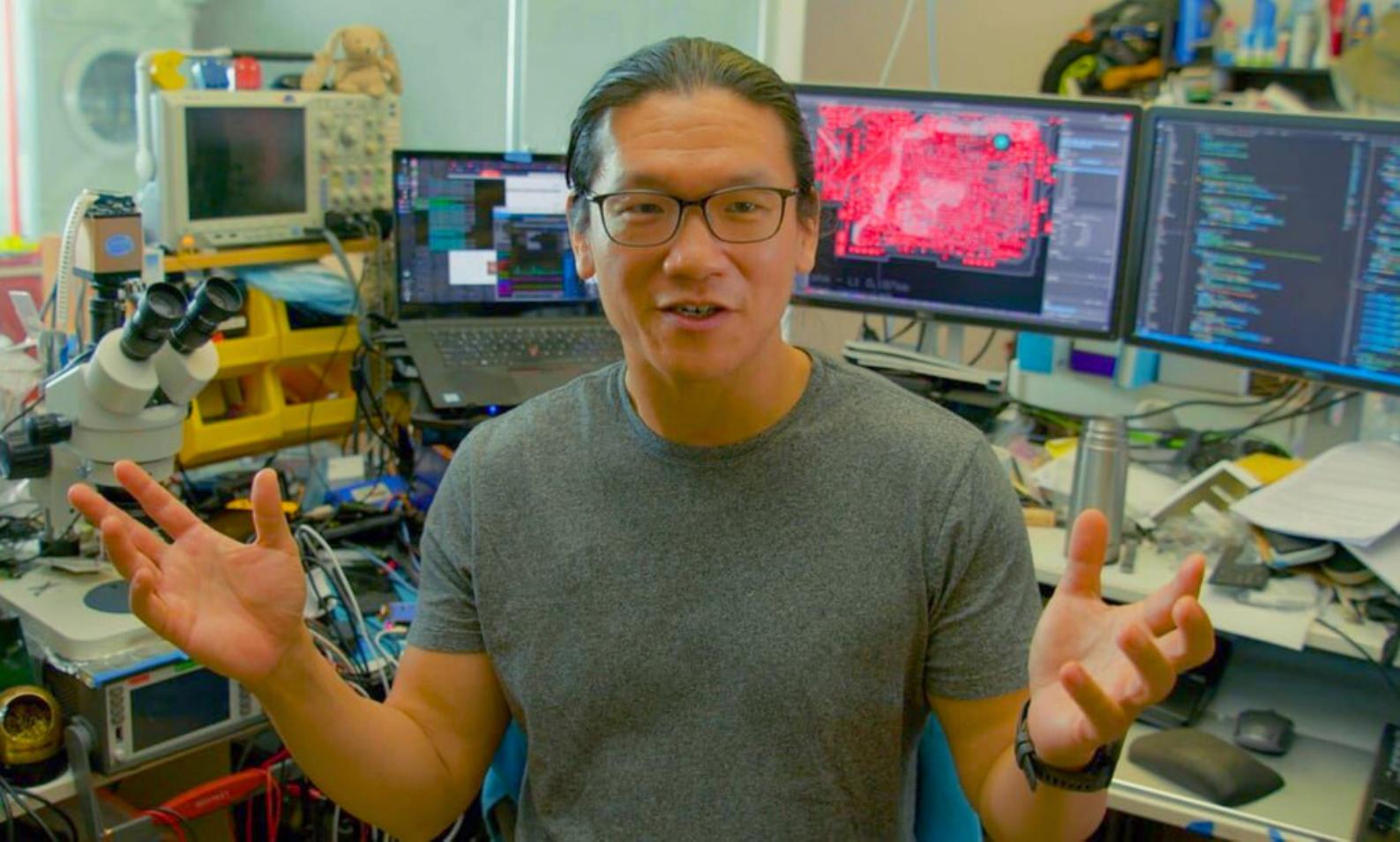


# MICHAEL OSSMANN

Michael Ossmann é um respeitado especialista em segurança cibernética e hardware hacking, conhecido por suas contribuições no campo de análise de dispositivos de comunicação sem fio. Ele é o criador do HackRF, uma ferramenta de código aberto usada para explorar e manipular sinais de rádio. Ossmann é comprometido com a ética hacker e a educação em segurança cibernética, e seu trabalho tem tido um impacto significativo na indústria.

Ele é frequentemente convidado a palestrar em conferências de segurança cibernética e hardware hacking em todo o mundo, e é reconhecido como uma figura altamente qualificada e respeitada no campo.

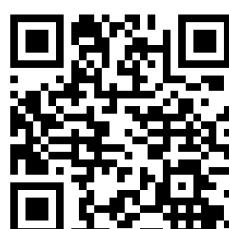




# ANDREW HUANG

Andrew "Bunnie" Huang é um engenheiro de hardware, hacker e autor americano. Ele é conhecido por suas contribuições para o campo de hardware hacking, incluindo o desbloqueio do Xbox, que permitiu a execução de software caseiro no console.

Huang também é um defensor da liberdade do hardware, promovendo a ideia de que as pessoas deveriam ter o direito de modificar e controlar os dispositivos eletrônicos que possuem. Ele é o fundador da empresa Chumby Industries e autor do livro "Hacking the Xbox", que detalha sua experiência em desbloquear o console. Huang também palestra regularmente em conferências de segurança cibernética e é um membro ativo da comunidade de hackers.



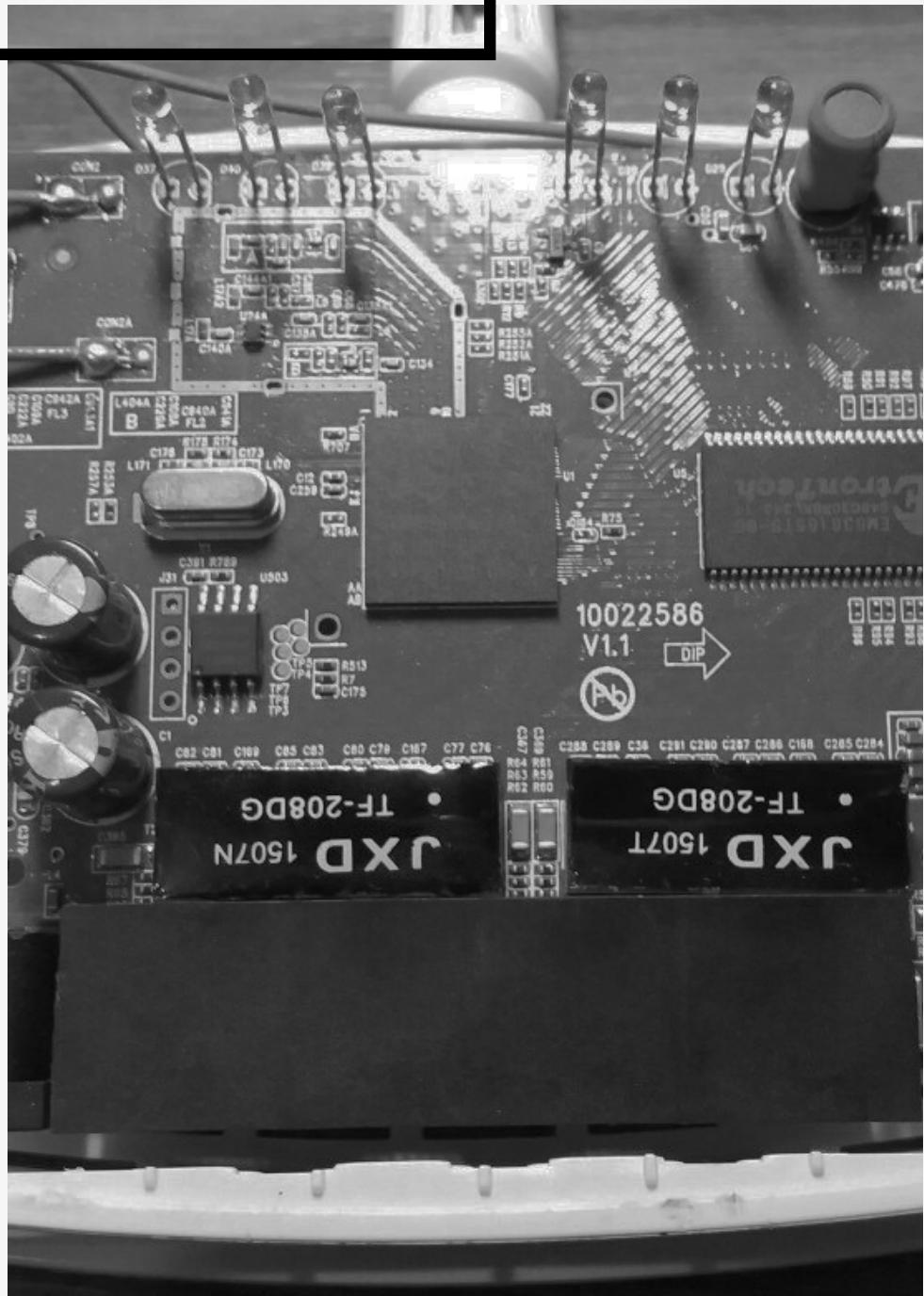
# O COMEÇO DA JORNADA . . .

@juliodellaflora  
<https://juliodellaflora.com>

Com o rápido avanço da tecnologia, o estudo de hardware hacking tem se tornado cada vez mais importante e necessário. Porém, apesar do crescente interesse nessa área, muitas informações ainda não estão disponíveis em português, o que pode dificultar o aprendizado para aqueles que não possuem conhecimento em língua estrangeira.

O objetivo deste documento é oferecer um caminho para iniciar seus estudos em hardware hacking e fornecer informações úteis sobre a prática do pentest em dispositivos embarcados e ferramentas para red team. Esperamos que este material possa ajudar a preencher a lacuna de informações em português nessa área, oferecendo aos interessados um ponto de partida para o aprendizado e aprimoramento de suas habilidades.

Por fim, gostaríamos de enfatizar que o estudo de hardware hacking exige dedicação e comprometimento, mas também pode ser extremamente gratificante. Esperamos que este documento possa servir como um guia útil para aqueles que desejam iniciar sua jornada nessa área fascinante.



# 1º PASSO

*Se você está interessado em começar a aprender hardware hacking, o primeiro passo é construir um conhecimento básico em eletrônica. Assim como em outras áreas do hacking, como sistemas operacionais, web ou dispositivos móveis, entender os fundamentos é crucial.*

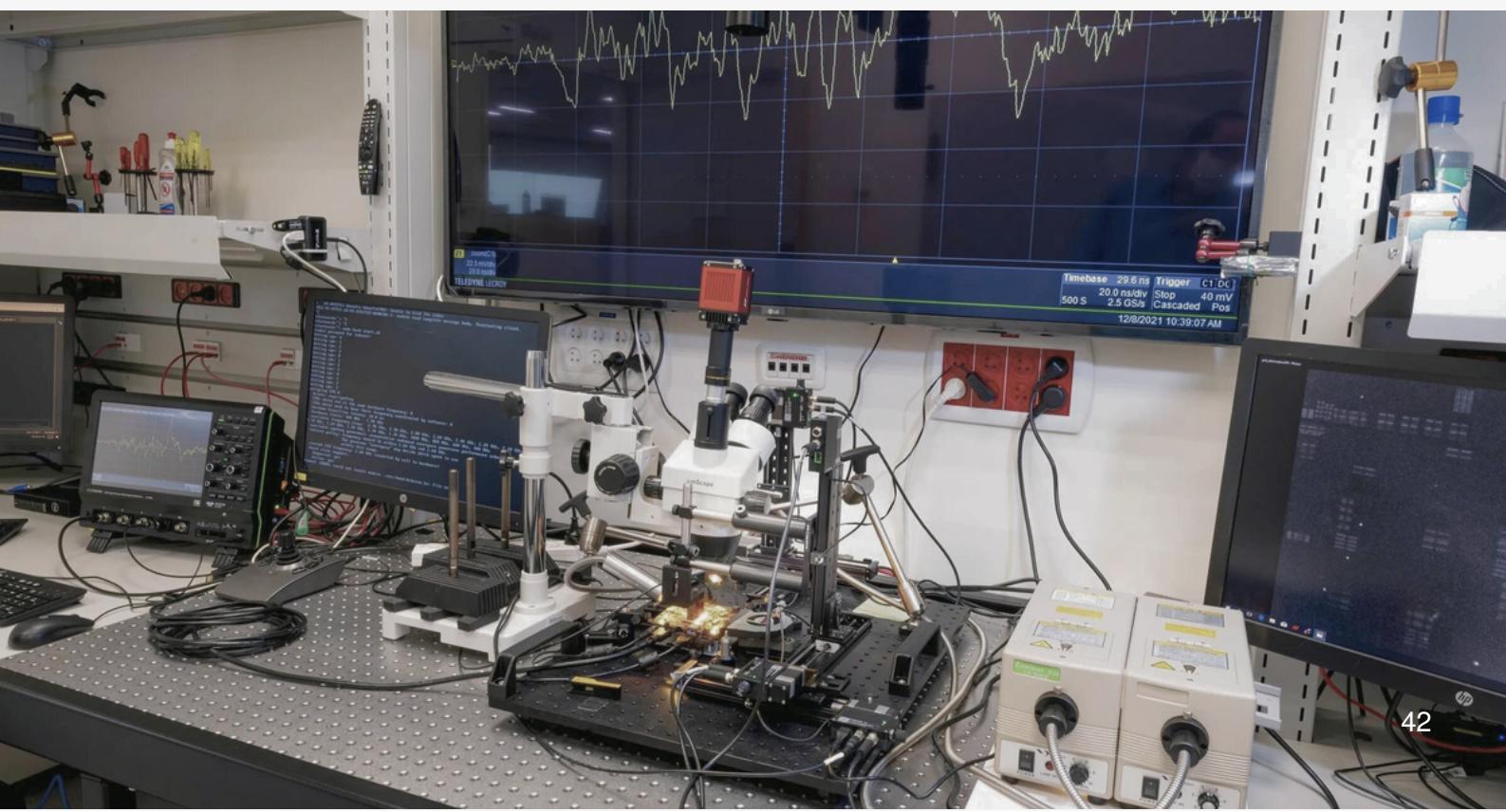
*A eletrônica é a base para o hardware hacking, pois é a partir dela que é possível entender como os dispositivos funcionam e como eles podem ser explorados. Para isso, é importante estudar conceitos básicos, como circuitos elétricos, leis de Ohm, capacidade e resistência.*

*Além disso, é importante se familiarizar com as ferramentas e equipamentos utilizados no hardware hacking, como multímetros, osciloscópios, programadores de microcontroladores e soldadores. Essas ferramentas são essenciais para entender como os dispositivos funcionam e como é possível explorá-los.*

*Outro ponto importante é estudar o funcionamento dos dispositivos e seus componentes. É necessário entender como cada componente interage com o outro e como o dispositivo como um todo funciona. Isso inclui o estudo de diagramas de circuitos, datasheets de componentes e manuais de dispositivos.*

*Com um conhecimento básico em eletrônica, é possível começar a explorar a segurança de dispositivos eletrônicos e desenvolver habilidades em hardware hacking. A partir daí, é importante continuar estudando e aprimorando suas habilidades, sempre mantendo-se atualizado sobre as novas tecnologias e técnicas utilizadas nessa área.*

*Lembre-se que o hacking ético é fundamental, e é importante sempre respeitar a privacidade e a segurança de outras pessoas e empresas. Com dedicação e estudo constante, é possível se tornar um especialista em hardware hacking e contribuir para a segurança da informação.*



# ...eletrônica analógica

A eletrônica analógica é um ramo da eletrônica que se dedica ao estudo dos circuitos elétricos que processam sinais analógicos. Ao contrário da eletrônica digital, que trabalha com sinais digitais (0 e 1), a eletrônica analógica lida com sinais que variam de forma contínua no tempo.

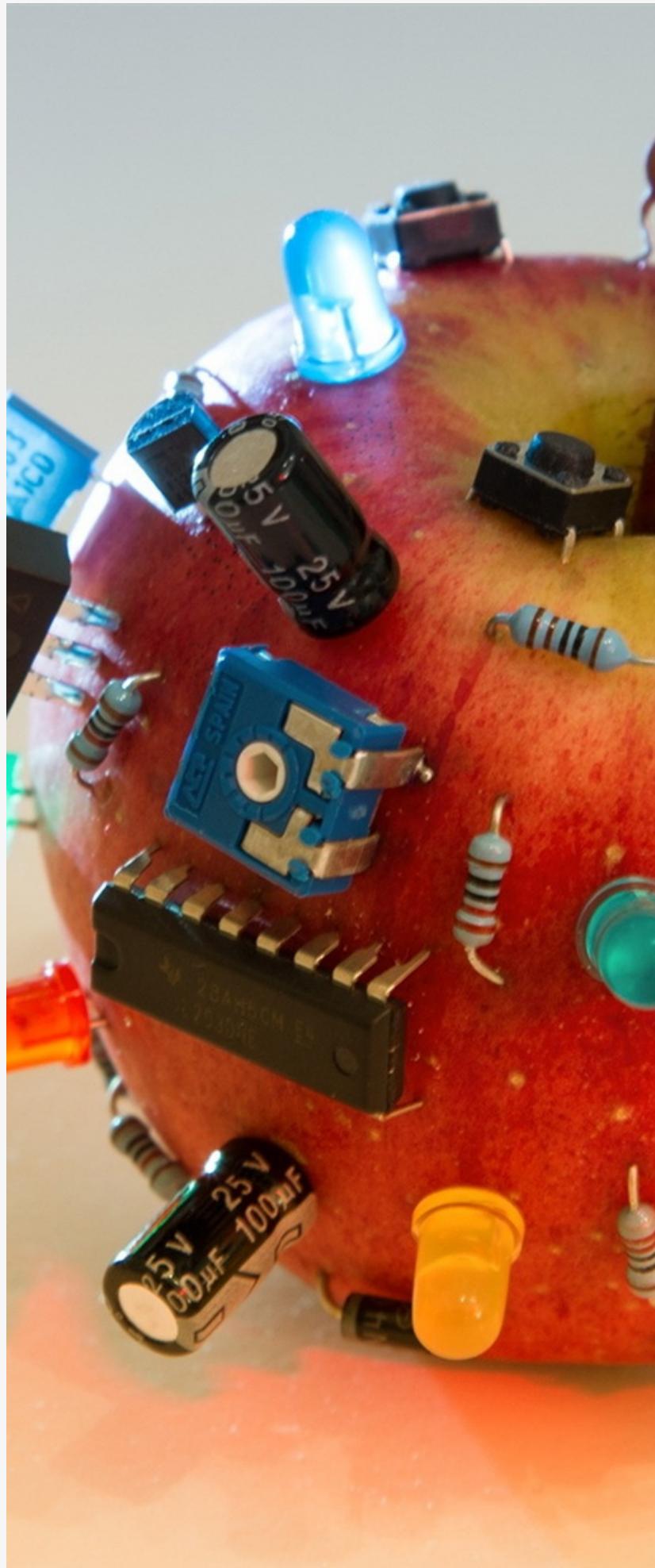
Aprender eletrônica analógica é importante por vários motivos. Em primeiro lugar, a eletrônica analógica é a base para a compreensão de muitos dispositivos eletrônicos. Ao entender os circuitos analógicos que estão por trás desses dispositivos, é possível compreender melhor como eles funcionam e como podem ser explorados.

Além disso, a eletrônica analógica é fundamental para o estudo de outras áreas da eletrônica, como a eletrônica digital e a eletrônica de potência. Isso ocorre porque muitos dispositivos eletrônicos utilizam circuitos analógicos em conjunto com circuitos digitais e de potência.

Outra razão para aprender eletrônica analógica é que ela é uma habilidade valiosa para profissionais de diversas áreas, como engenharia, eletrônica, telecomunicações e automação. Com um conhecimento sólido em eletrônica analógica, é possível trabalhar em projetos que envolvam o desenvolvimento de circuitos eletrônicos, sistemas de controle, equipamentos de telecomunicações e muito mais.

Por fim, aprender eletrônica analógica é importante porque permite entender a relação entre o mundo físico e o mundo digital. Ao compreender como os sinais analógicos são processados e transformados em sinais digitais, é possível entender melhor como a tecnologia funciona e como ela pode ser aplicada para resolver problemas reais.

Em resumo, aprender eletrônica analógica é fundamental para quem deseja compreender o funcionamento dos dispositivos eletrônicos, trabalhar em áreas relacionadas à eletrônica e tecnologia, e desenvolver habilidades valiosas para o mercado de trabalho.





E O PRÓXIMO PASSO?

# ELETRO NICA DIGITAL

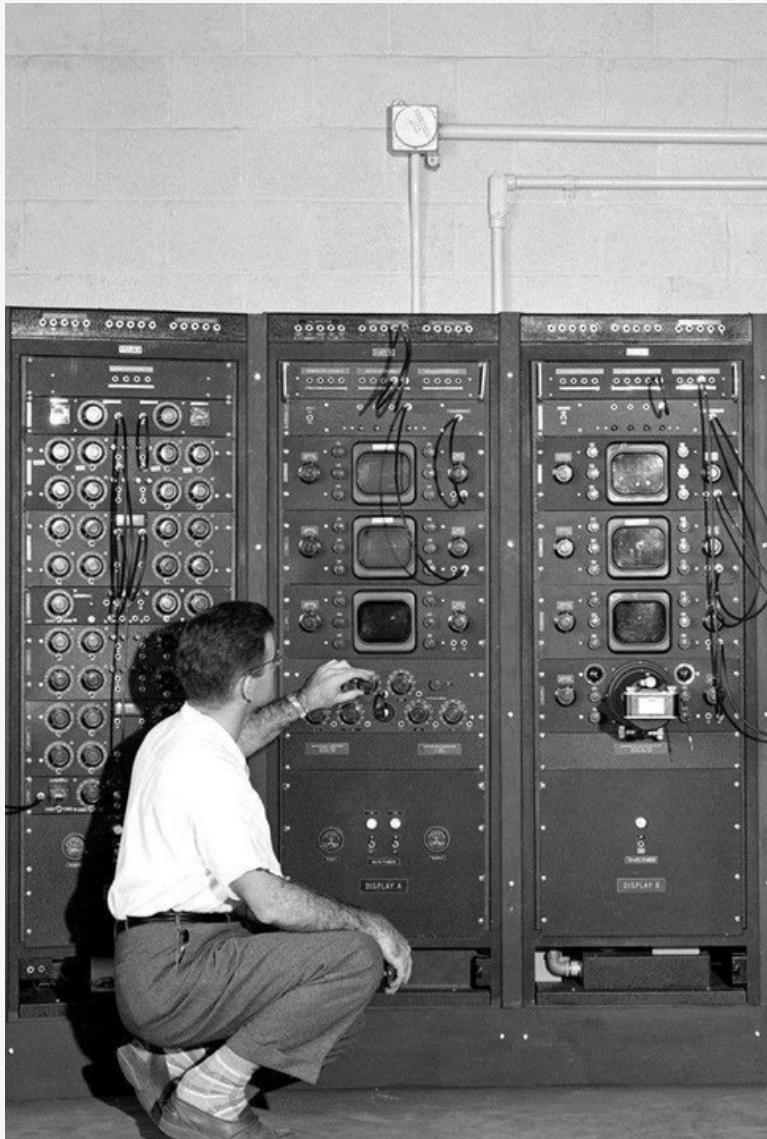
...imagine construir um computador  
inteiro do zero...

JULIODELLAFLORA.COM

A eletrônica digital é uma parte essencial de nossas vidas e é usada em uma variedade de dispositivos e sistemas que dependemos diariamente. Ela permite a criação de sistemas mais rápidos, precisos e eficientes, além de possibilitar o desenvolvimento de tecnologias como a Internet, a computação em nuvem, a inteligência artificial e a robótica. A eletrônica digital também é fundamental para a segurança e privacidade de informações e é uma habilidade valiosa para quem trabalha em áreas relacionadas à tecnologia.

Para começar a aprender eletrônica digital, é recomendável ter conhecimentos básicos de eletrônica analógica e matemática. Em seguida, é importante estudar os conceitos de álgebra booleana, portas lógicas, flip-flops e circuitos combinacionais e sequenciais. Uma boa opção é realizar cursos online, livros e práticas de projetos para aprimorar o aprendizado. É importante ter em mente que a eletrônica digital é uma área que exige prática constante para se tornar proficiente.

# ATENÇÃO



*quer aprender mais sobre hacking?*

A eletrônica digital é uma área essencial para o desenvolvimento de sistemas de hardware modernos, e é fundamental para quem busca aprimorar suas habilidades em hacking de hardware, pentest e segurança de sistemas embarcados. Antes de mergulhar na eletrônica digital, é necessário ter uma base sólida em eletrônica analógica e em matemática básica, pois esses conhecimentos são a base para a compreensão de conceitos mais avançados.

Ao estudar eletrônica digital, é possível compreender os princípios de álgebra booleana, portas lógicas, flip-flops e circuitos combinacionais e sequenciais, que são fundamentais para o desenvolvimento de tecnologias como a Internet das Coisas (IoT), inteligência artificial e robótica. É importante lembrar que a eletrônica digital utiliza componentes que trabalham em dois estados distintos, geralmente representados como 0 e 1.

A compreensão da eletrônica digital é fundamental para entender como os dispositivos funcionam e quais são as vulnerabilidades potenciais, o que é crucial para quem quer se aprofundar em hacking de hardware e pentest. Além disso, é essencial para a segurança e privacidade de informações em sistemas embarcados e dispositivos conectados à Internet.

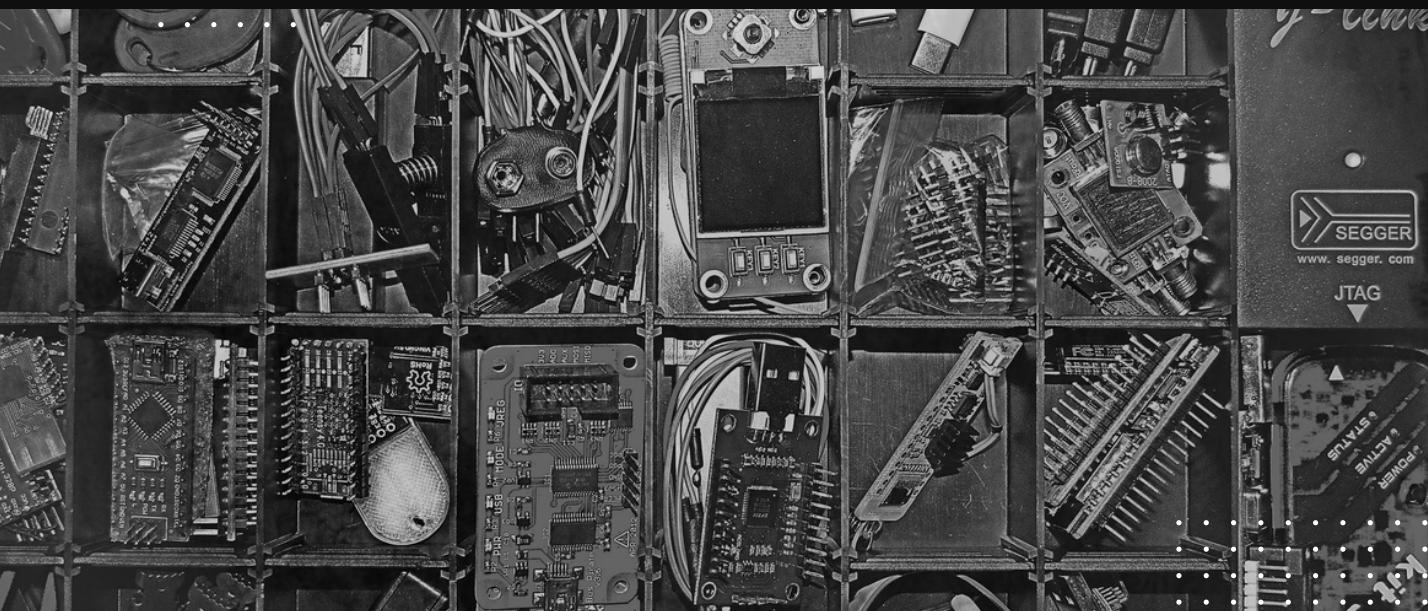


técnicas de

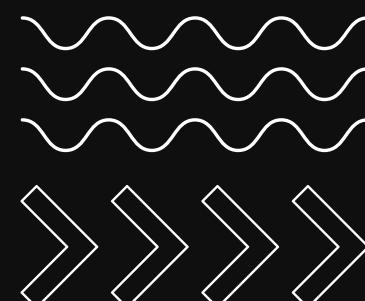
# INVASÃO

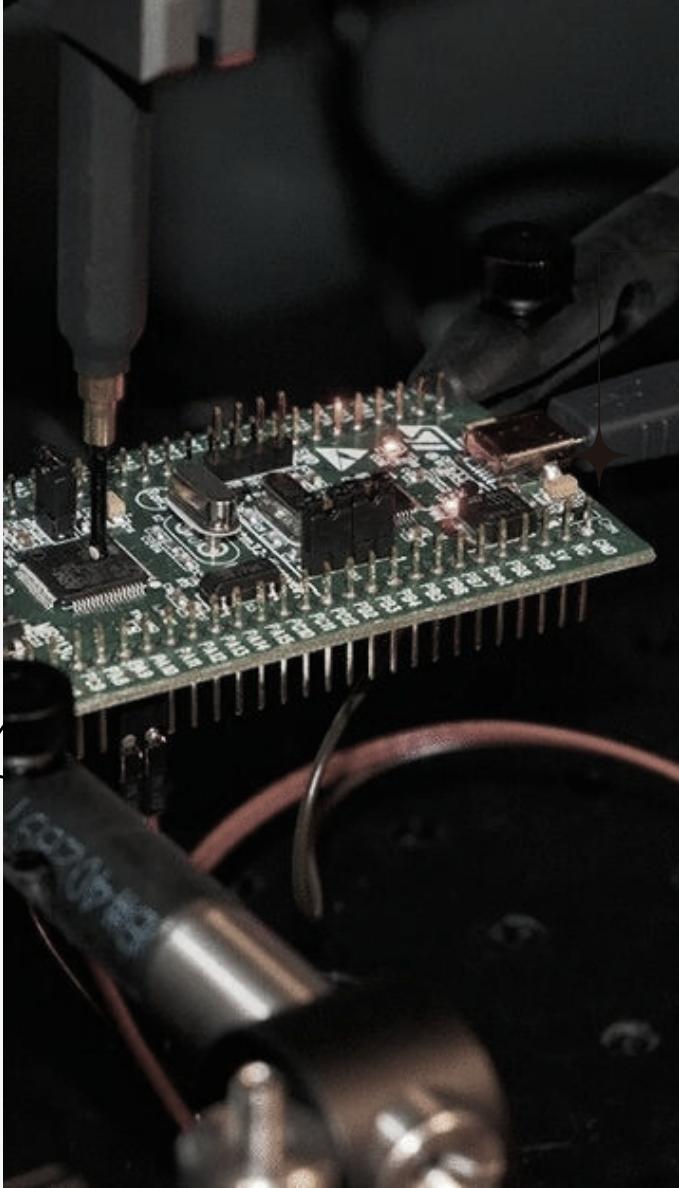
# EM

# HARDWARE



Para quem busca aprimorar suas habilidades em hacking de hardware, pentest e segurança de sistemas embarcados, é importante ter um conhecimento básico das principais técnicas de invasão, que são genéricas o suficiente para serem aplicadas em diferentes cenários. Um exemplo disso é o ataque de Man in The Middle, que além de seu uso tradicional em redes de computadores, também pode ser utilizado para verificar a comunicação em barramentos de hardware.





# conheça...

...as ferramentas e extraia todo o potencial delas. Quando você compra uma ferramenta (ex: bus pirate) procure se aprofundar em todas as possibilidades que aquele dispositivo lhe traz. Se você ainda não conhece esses dispositivos, eu vou deixar uma palestra que ministrei na última RoadSec, ela vai te ajudar a ter uma ideia inicial dos dispositivos mais utilizados.

conheça  
o ts100

@juliodellaflora



...assista esse vídeo



# ataques

---

Para quem deseja se aprofundar na área de segurança de sistemas e hacking de hardware, é importante buscar conhecimento sobre ataques "exotéricos" e técnicas novas e não convencionais. Essas técnicas são geralmente pouco conhecidas e podem ser uma surpresa para muitos profissionais da área de segurança.

Uma forma de adquirir esse tipo de conhecimento é explorar as palestras apresentadas nas diversas conferências de segurança realizadas no Brasil e em todo o mundo. No entanto, é preciso estar preparado para o fato de que muitas dessas palestras estarão em inglês.

É possível encontrar palestras de diversos especialistas no assunto, incluindo ataques em sistemas e dispositivos embarcados. Uma dessas palestras é a do autor deste texto, que pode fornecer uma visão sobre os tipos de ataques exotéricos que estão sendo desenvolvidos atualmente.

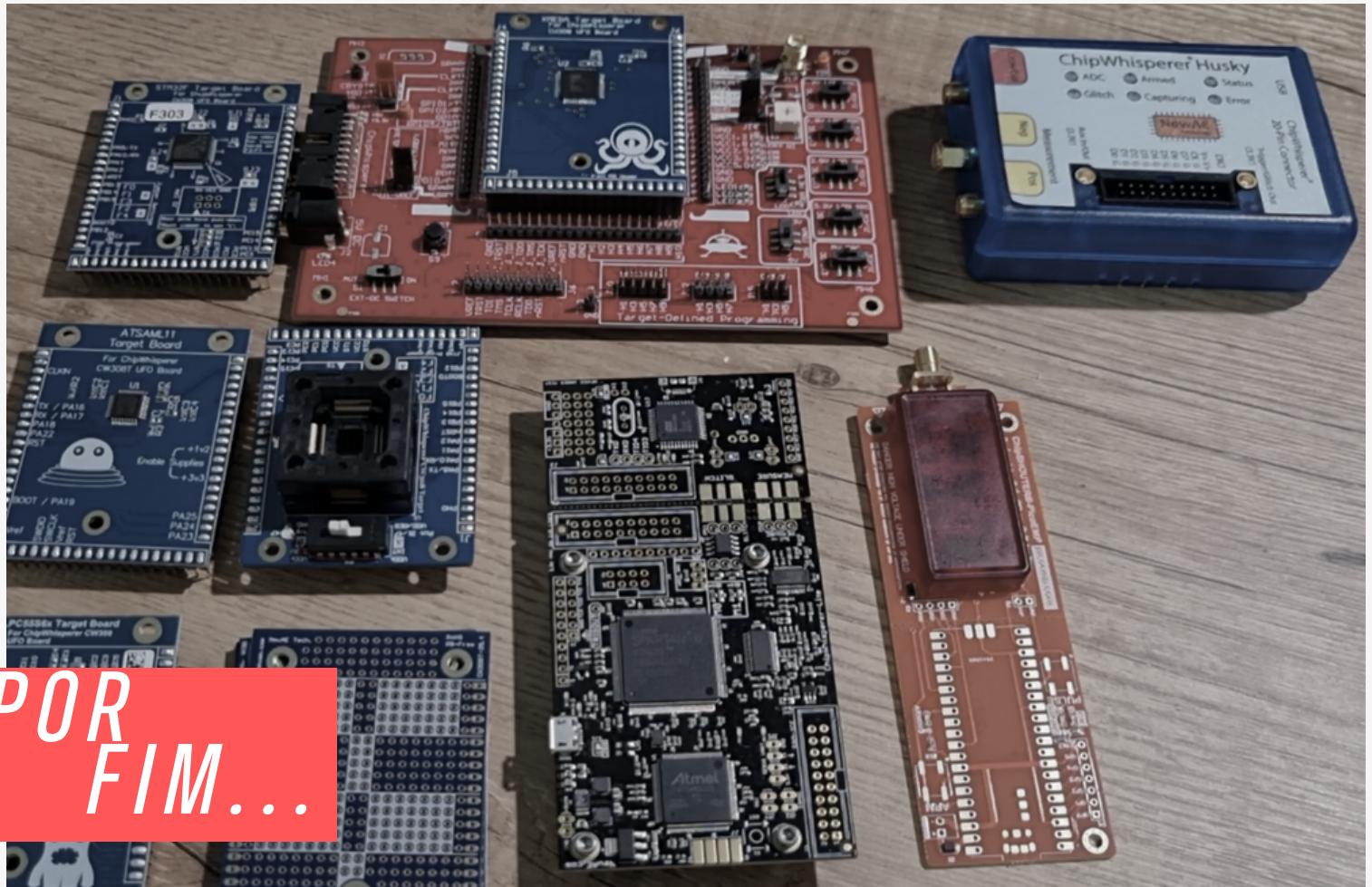




# NÃO BASTA SOMENTE...



...assistir tutoriais e palestras, você terá que pôr a mão na massa, quando se estuda dispositivos embarcados você constantemente precisa soldar, medir, furar e prototipar coisas. Para isso você vai precisar de ferramentas, e vale a pena organizar essas ferramentas de forma que você consiga transportá-las para onde precisar. Nesse vídeo em parceria com o Gabriel Pato eu mostro algumas ferramentas da minha maleta.



POR  
FIM...

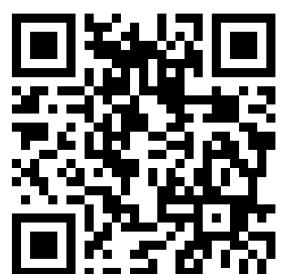
## (MAS NÃO MENOS IMPORTANTE)

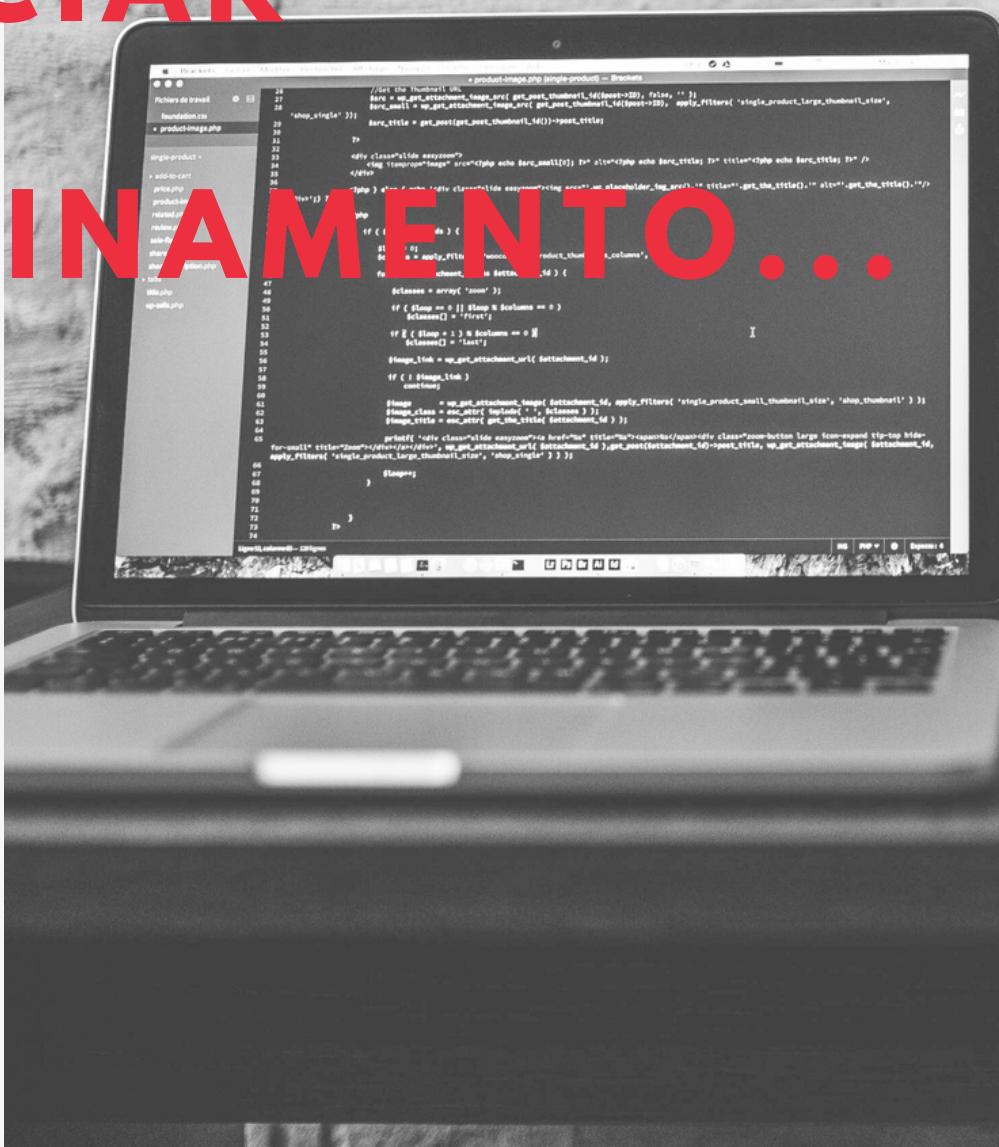
@juliodellaflora

...comece a se aprofundar em alguma técnica ou tipo de exploração, eu por exemplo (nos últimos anos) pesquisei sobre ataques de injeção de falhas em hardware. Não quer dizer que você precisa estudar o mesmo que eu, mas é importante além do panorama geral, ter um ponto específico de estudo (que vai mudar de tempos em tempos).

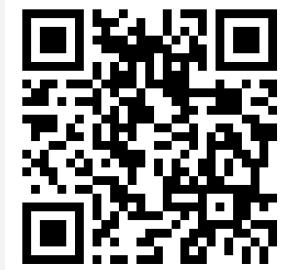
Se comunicar com outros profissionais da área é extremamente importante quando você precisa desenvolver suas habilidades em um campo específico. Mesmo que você seja estudioso e procure dia após dia sobre o tema desejado no google, mesmo que leia artigos e participe de palestras, você precisará fazer as perguntas certas para ter as respostas certas e nesse quesito, conversar com outros profissionais ajuda a fomentar dúvidas e procurar respostas.

**"PARA TER  
DÚVIDAS É  
PRECISO AO  
MENOS  
PRESTAR  
ATENÇÃO NA  
MATERIAL."**





...o professor tenta trazer o know-how de anos de pesquisa, meses de estudo e tentativas infundáveis para resolver problemas e acelerar o seu aprendizado. Você obviamente conseguiria todo esse conhecimento sozinho, pesquisando por alguns anos os termos corretos, investindo em ferramentas e passando noites tentando, falhando, tentando novamente e finalmente obtendo sucesso. Todavia, os treinamentos buscam acelerar o seu domínio em certas práticas através do conhecimento de outra pessoa com maior domínio.



## RUBBERDUCKY

O Rubber Ducky da Hak5 é um dispositivo USB utilizado para testes de intrusão que imita o funcionamento de um teclado. Quando conectado a um dispositivo eletrônico, ele pode executar uma sequência de ações automaticamente, simulando a entrada de dados através de um teclado USB.



O funcionamento do Rubber Ducky é baseado em uma linguagem de script própria, que permite que o usuário execute uma série de tarefas de forma automática. Essa linguagem, chamada de Ducky Script, é fácil de aprender e permite que o usuário personalize as sequências de ações de acordo com suas necessidades.

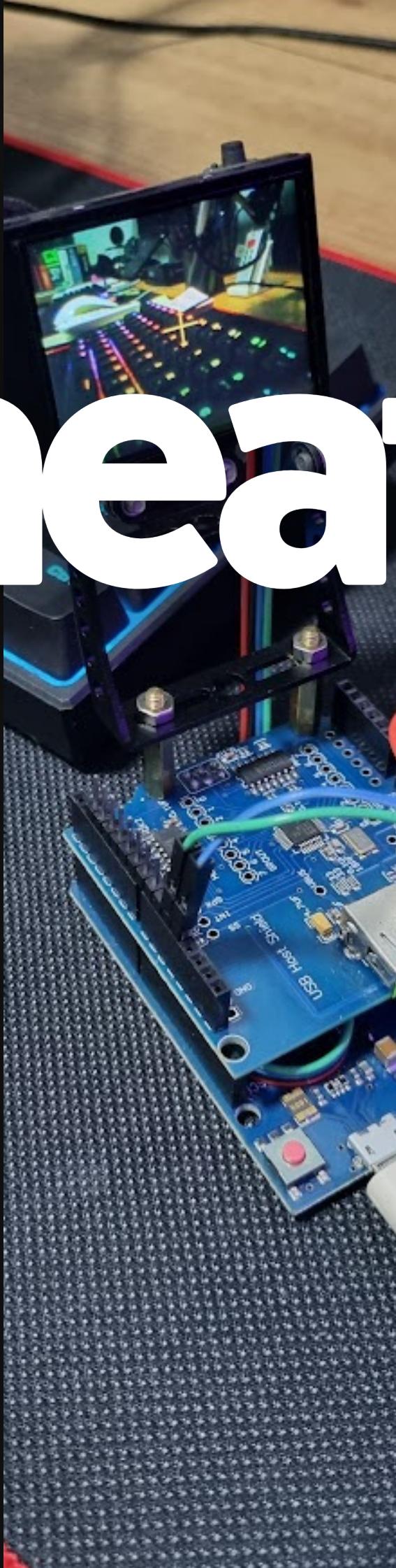
O dispositivo pode ser utilizado em uma ampla variedade de dispositivos eletrônicos, incluindo computadores e dispositivos móveis que tenham suporte para um teclado físico. Ele funciona em qualquer sistema operacional que suporte um teclado USB, o que o torna uma ferramenta versátil para testes de intrusão.

Ao contrário de outros dispositivos de hacking, o Rubber Ducky da Hak5 é projetado para parecer um dispositivo USB comum, o que o torna mais discreto e fácil de transportar. Isso permite que os usuários realizem testes de intrusão sem levantar suspeitas e sem serem detectados.

...já ouviu falar em  
trapaças utilizando  
hardware?



# cheats.



*quer saber como isso  
funciona? então  
assista ao vídeo  
abaixo!*

be nice ;)



# BUS PIRATE

O Bus Pirate é uma ferramenta versátil e multiuso que serve como uma espécie de "canivete suíço" para sistemas embarcados.

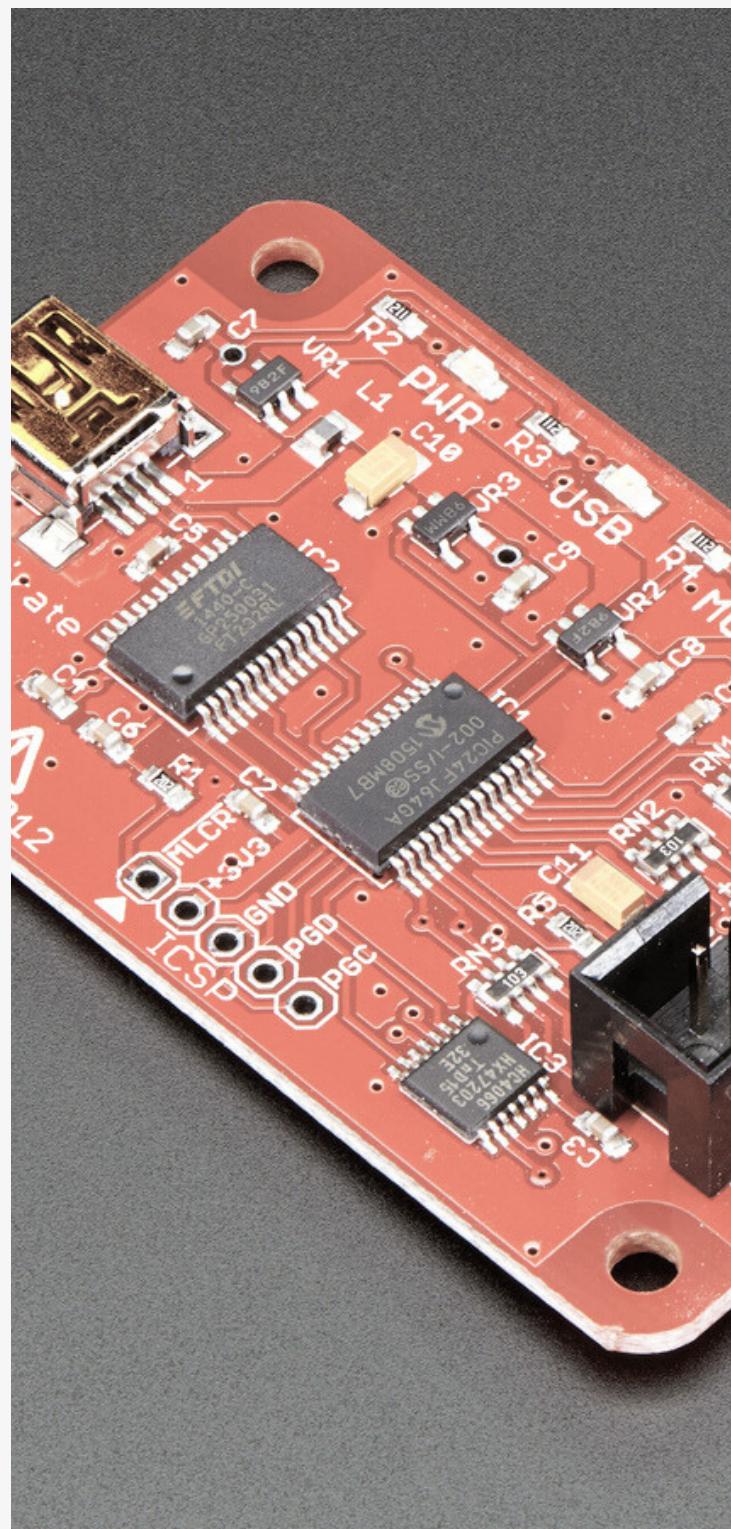
Assim como o famoso objeto suíço, que tem várias funcionalidades em um só lugar, o Bus Pirate é capaz de realizar várias tarefas em um único dispositivo.

Entre suas funções, o Bus Pirate pode analisar protocolos de comunicação, gerar formas de onda, captar sinais analógicos e servir de ponte USB-Serial, além de atuar como gravador de microcontroladores. Ele

é uma placa pequena, mas com grande capacidade, que pode assustar à primeira vista, pois possui apenas alguns pinos de interface.

A versão disponível no MakerHero é a v3.6, uma das mais consagradas atualmente no mercado. A vista superior da Bus Pirate mostra todas as informações e elementos úteis para o posterior manuseio já expostos. À esquerda, há um conector mini-USB, e à direita, os sinais de interface usados nos recursos do Bus Pirate. Apesar de parecerem poucos, são multifuncionais.

Com suas várias funcionalidades, o Bus Pirate é uma ferramenta indispensável para quem trabalha com sistemas embarcados. Ele permite a realização de diversas tarefas em um único dispositivo, o que pode reduzir consideravelmente o tempo gasto em testes e análises. É uma ferramenta extremamente útil para engenheiros, técnicos e entusiastas da eletrônica.



# FLIPPER ZERO





## CONHECENDO O FLIPPER ZERO

O Flipper Zero é um equipamento portátil e compacto que tem sido o objeto de desejo de pentesters e geeks. Sua aparência lúdica e divertida esconde um verdadeiro canivete suíço para hacking digital, capaz de invadir sistemas de acesso, redes e protocolos de rádio com facilidade.

Totalmente aberto e personalizável, o Flipper Zero oferece a flexibilidade e a liberdade que os profissionais de segurança precisam para realizar seus testes e ataques com eficácia. Além disso, o equipamento é extremamente fácil de usar e transportar, graças à sua tela OLED de alta resolução e seus poucos botões.

Uma das grandes vantagens do Flipper Zero é sua capacidade de executar várias funções de hacking em um único dispositivo. Com a possibilidade de capturar pacotes, gerar sinais e analisar protocolos, o equipamento se destaca pela versatilidade e pela possibilidade de customização, podendo ser ajustado para as necessidades específicas do usuário.

O Flipper Zero também conta com uma arquitetura de hardware aberta, o que permite que os usuários programem e desenvolvam novas funcionalidades para o equipamento. Isso significa que a ferramenta pode ser adaptada a diferentes contextos e projetos, o que faz do Flipper Zero uma das ferramentas mais valiosas para quem trabalha com segurança digital.



# CALMA, EXISTEM ALTERNAТИVAS AOS FLIPPER ZERO!

JULIO DELLA FLORA

Nicacee

wow

omg!





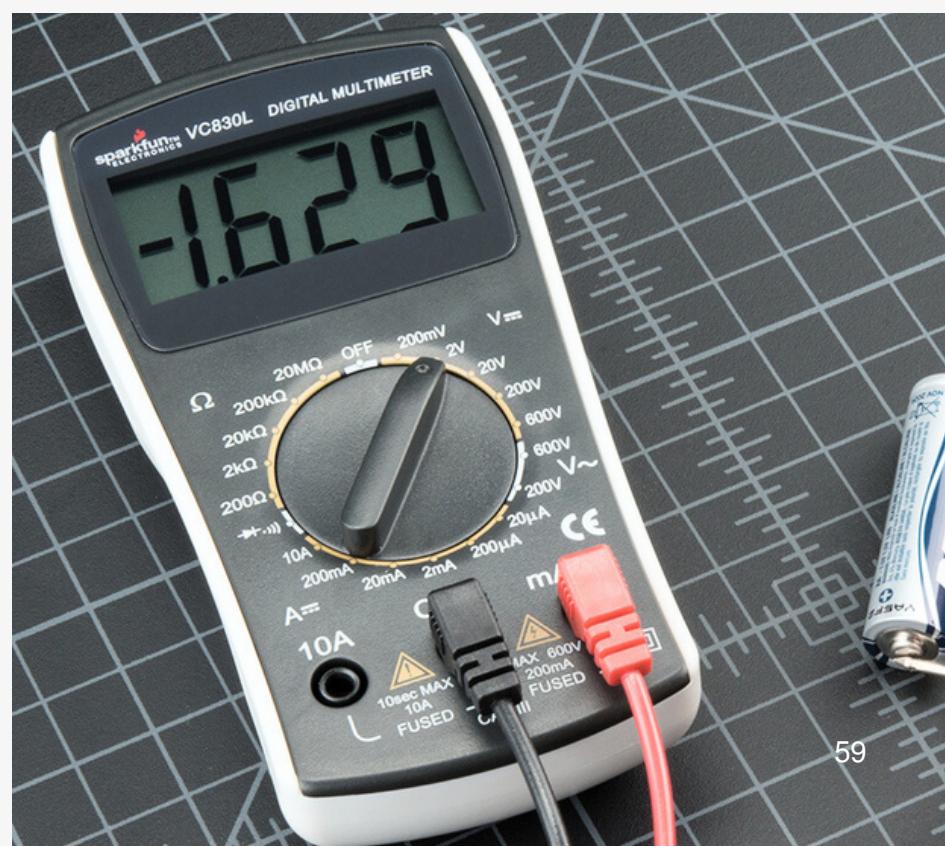
Um multímetro é um instrumento eletrônico usado para medir grandezas elétricas como tensão, corrente e resistência. Ele é útil para solucionar problemas elétricos em circuitos, testar a integridade de componentes eletrônicos e avaliar o desempenho de sistemas elétricos em geral.

## "MEDIR GRANDEZAS ELÉTRICAS EM CIRCUITOS"

JULIO DELLA FLORA

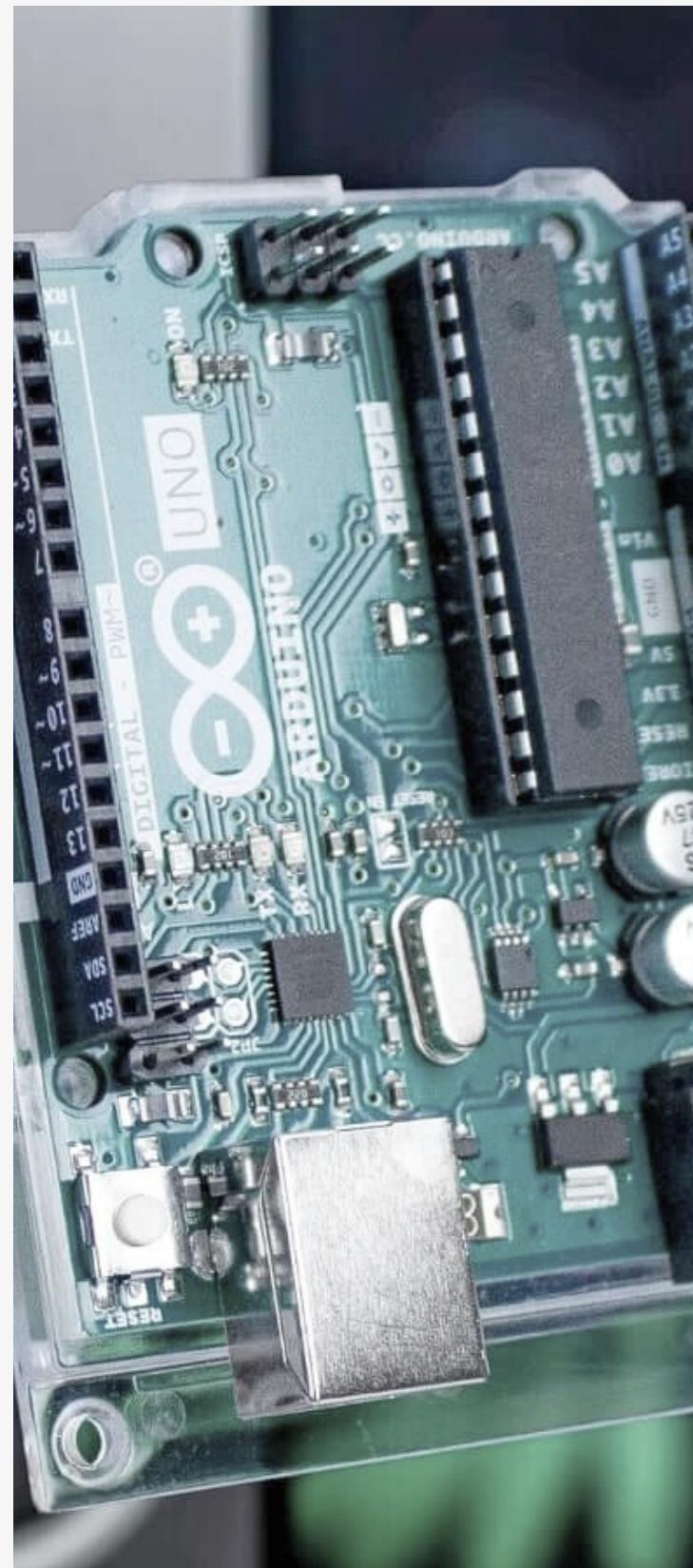
Se o hacker estiver envolvido em atividades relacionadas à segurança da informação, o multímetro pode ser usado para testar a integridade física de dispositivos de segurança, como fechaduras eletrônicas ou sistemas de alarme. O multímetro pode ser usado para verificar a presença de corrente elétrica em um sistema de alarme, por exemplo, para determinar se ele está ativado ou desativado.

Já se o hacker estiver envolvido em atividades relacionadas a hardware em geral, o multímetro pode ser usado para testar o desempenho de componentes eletrônicos individuais, medir a tensão em diferentes pontos de um circuito ou verificar a continuidade de uma trilha de cobre em uma placa de circuito impresso. Essas medições são fundamentais para entender o funcionamento de um circuito, identificar problemas de funcionamento e desenvolver soluções para corrigi-los.



# ARDUINO

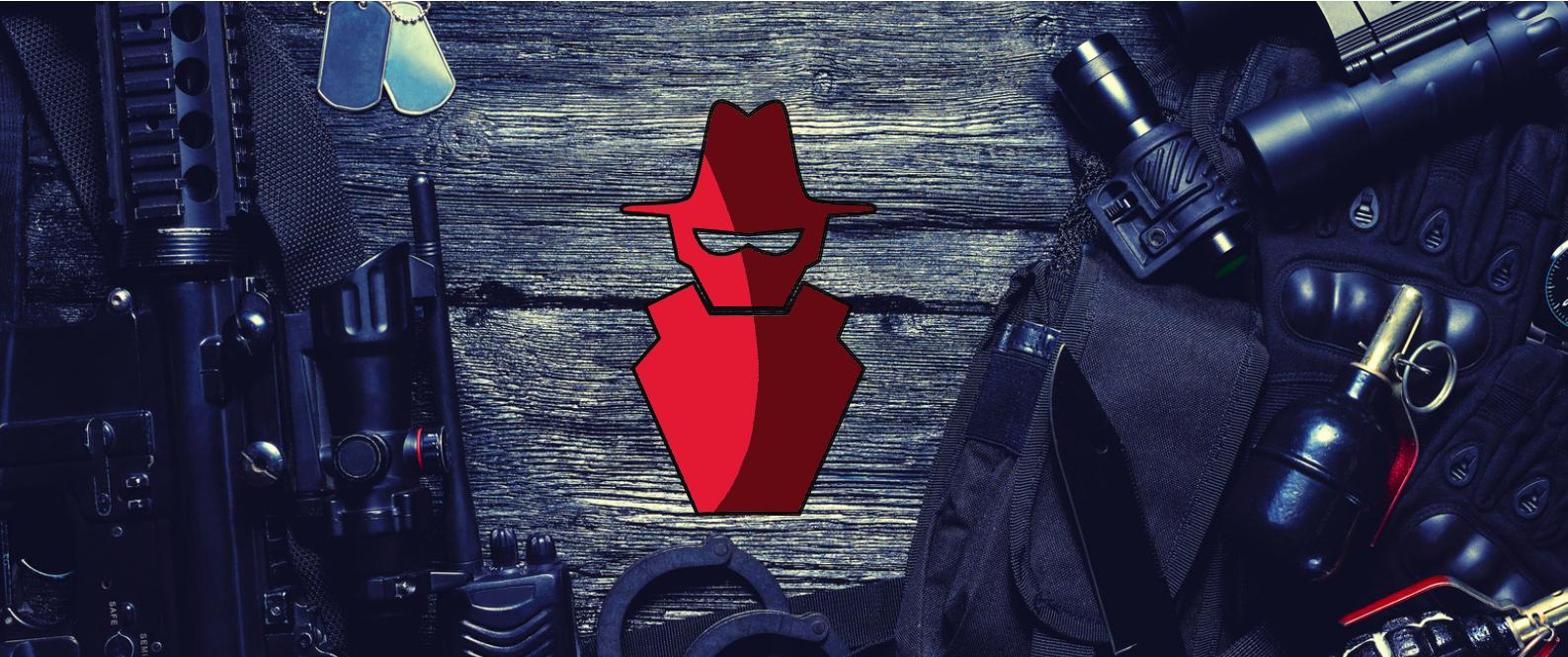
Arduino é uma plataforma eletrônica de código aberto que permite a criação e prototipagem de projetos eletrônicos interativos de forma relativamente fácil e acessível. O coração da plataforma é uma placa de circuito impresso que contém um microcontrolador programável, que pode ser conectada a uma série de componentes eletrônicos, como sensores, atuadores, displays, entre outros. O Arduino pode ser programado em uma linguagem de programação própria, baseada em C++, que permite aos usuários criar projetos que reagem a diferentes entradas do ambiente (como sensores) e controlam diferentes saídas (como motores ou LEDs). A plataforma é amplamente utilizada por entusiastas, artistas, designers, estudantes e profissionais em uma variedade de áreas, desde robótica e automação até arte interativa e ciência cidadã.



# PLATAFORMA DE PROTOTIPAGEM ELETRÔNICA INTERATIVA E ACESSÍVEL

JULIO DELLA FLORA





No âmbito da segurança da informação, um "red team" é um grupo de profissionais de segurança que atua como um adversário simulado, com o objetivo de avaliar e testar a segurança de uma organização. O red team é responsável por encontrar falhas e vulnerabilidades nos sistemas, processos e políticas de segurança da organização, utilizando técnicas e métodos semelhantes aos utilizados por hackers e outros criminosos cibernéticos.

O trabalho do red team envolve simular ataques cibernéticos e outras ameaças, como engenharia social, para identificar falhas e fraquezas nos controles de segurança da organização. Esses testes podem incluir ataques de phishing, tentativas de invasão de sistemas, exploração de vulnerabilidades de software e tentativas de obter acesso físico às instalações da organização. Ao realizar esses testes, o red team pode fornecer informações valiosas sobre as deficiências na segurança da organização e ajudar a identificar áreas onde são necessárias melhorias. Os resultados desses testes podem ser usados para aprimorar as políticas de segurança, treinamentos para os colaboradores e outras iniciativas de segurança da informação.

O red team pode colaborar para o incremento de segurança da informação de uma empresa de diversas maneiras, incluindo:

1. Identificação de vulnerabilidades: o red team pode ajudar a empresa a identificar vulnerabilidades em seus sistemas e processos de segurança. Ao simular ataques cibernéticos, o red team pode detectar falhas na rede, brechas de segurança e outras vulnerabilidades que possam ser exploradas por atacantes reais.
2. Teste de eficácia de políticas de segurança: o red team pode ajudar a empresa a avaliar a eficácia de suas políticas de segurança. Ao tentar superar essas políticas, o red team pode identificar áreas em que as políticas precisam ser aprimoradas ou em que os colaboradores precisam ser treinados para garantir que a empresa esteja em conformidade com as melhores práticas de segurança.
3. Desenvolvimento de soluções de segurança: o red team pode ajudar a empresa a desenvolver soluções de segurança personalizadas. Ao avaliar as necessidades de segurança específicas da empresa, o red team pode recomendar soluções que sejam adequadas para suas necessidades exclusivas.
4. Treinamento de colaboradores: o red team pode ajudar a empresa a treinar seus colaboradores em práticas de segurança eficazes. Por meio de programas de treinamento personalizados, o red team pode ajudar a educar os colaboradores sobre as melhores práticas de segurança, como identificar e evitar ameaças de segurança e como proteger informações confidenciais.



As ferramentas da Hak5 são uma série de dispositivos e softwares desenvolvidos especificamente para testes de penetração e avaliação de segurança em redes e sistemas de computadores. Essas ferramentas são altamente portáteis e flexíveis, o que as torna ideais para uso por membros de um red team em simulações de ataque cibernético em uma empresa.

Algumas das principais ferramentas da Hak5 incluem:

1. Pineapple: um dispositivo que pode ser usado para criar pontos de acesso sem fio falsos e realizar ataques de phishing em redes Wi-Fi.
2. Bash Bunny: um dispositivo USB que pode ser programado para executar várias tarefas automatizadas, como coletar informações do sistema ou injetar malware.
3. LAN Turtle: um dispositivo que pode ser conectado a uma porta Ethernet e usado para obter acesso remoto a um sistema, mesmo em redes protegidas por firewalls.
4. Rubber Ducky: um dispositivo USB que pode ser programado para emular teclas do teclado e realizar uma série de ações, como inserir senhas ou executar comandos.

Essas ferramentas da Hak5 podem ser usadas para realizar uma ampla variedade de testes de segurança em redes e sistemas de computadores, incluindo:

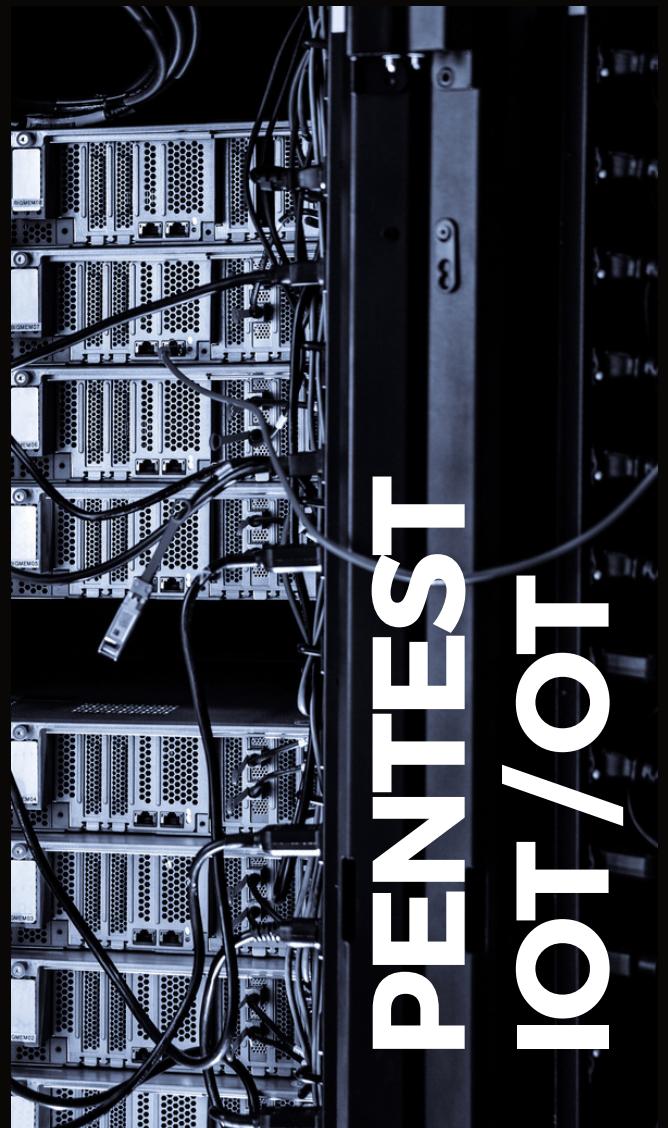
- Engenharia social: os dispositivos Pineapple e Rubber Ducky podem ser usados para realizar ataques de phishing e obter informações sensíveis dos colaboradores da empresa.
- Teste de vulnerabilidade de rede: os dispositivos Pineapple e LAN Turtle podem ser usados para testar a segurança da rede da empresa e identificar possíveis vulnerabilidades.
- Teste de segurança do sistema: o dispositivo Bash Bunny pode ser programado para executar vários testes de segurança automatizados em sistemas de computadores.
- Avaliação da segurança física: os dispositivos Pineapple e LAN Turtle podem ser usados para testar a segurança física da empresa, obtendo acesso não autorizado às instalações.



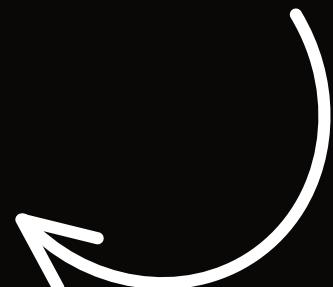
**precisa  
testar seu  
ambiente?**

A p1 Infosec é uma empresa que oferece serviços de segurança ofensiva para aplicações, empresas e indústrias. Seu portfólio inclui serviços de pentest, operações de red team e diversas outras soluções com o objetivo de fortificar as barreiras de segurança da organização contratante. O principal objetivo é garantir que as vulnerabilidades sejam identificadas e corrigidas antes que possam ser exploradas por atacantes mal-intencionados.

**p1**  
**Infosec**  
segurança ofensiva



**saiba mais em:**  
**[plinfosec.com](http://plinfosec.com)**





O Key Croc da Hak5 é um dispositivo de keylogging armado com ferramentas de testes de penetração, acesso remoto e payloads que disparam ataques de vários vetores quando palavras-chave escolhidas são digitadas. É o implante definitivo de keylogging pentest.

Mais do que apenas registrar e transmitir keystrokes online, ele explora o alvo com payloads que disparam quando palavras-chave de interesse são digitadas.

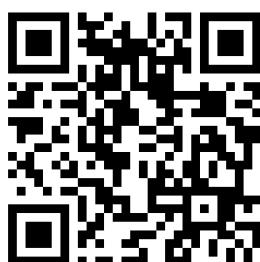
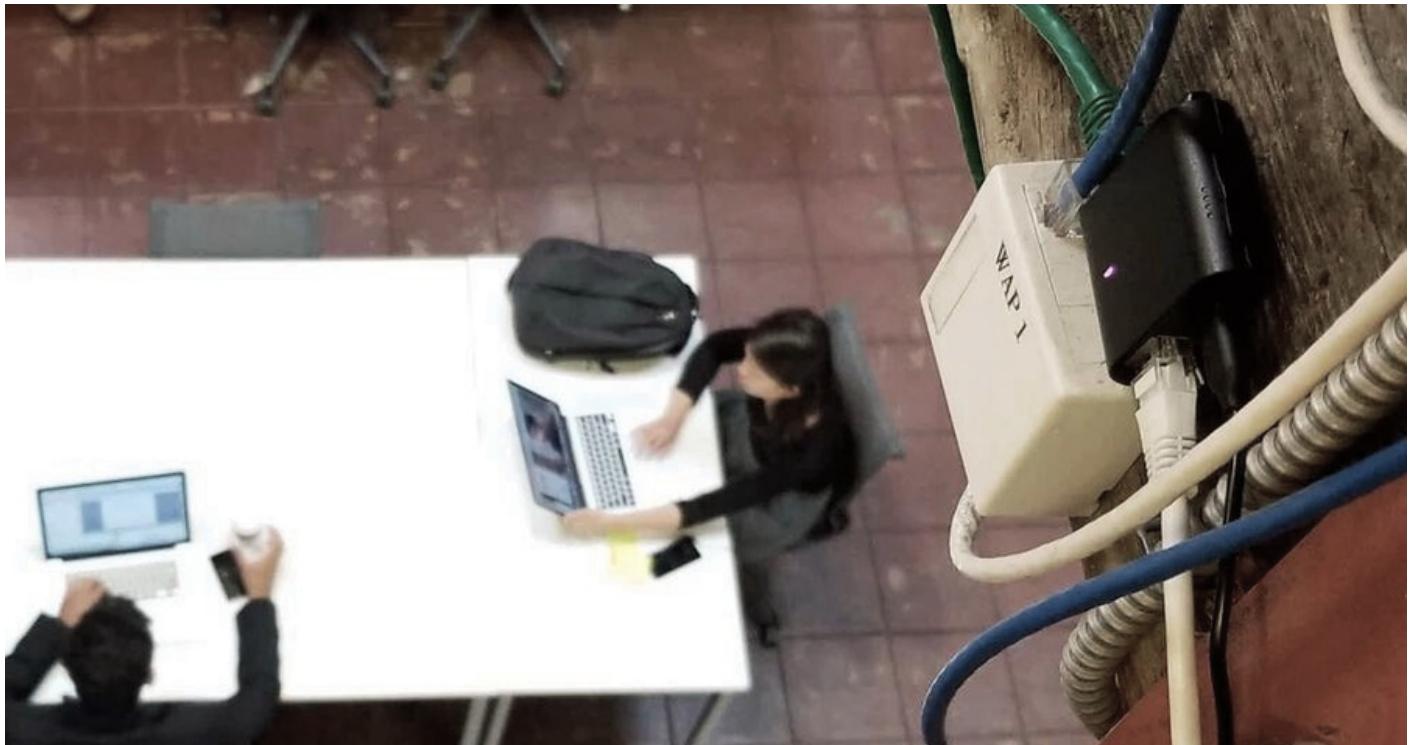
Ao emular dispositivos confiáveis como serial, armazenamento, HID e Ethernet, ele abre múltiplos vetores de ataque - desde injeção de keystroke até sequestro de rede.

Imagine capturar credenciais e usá-las sistematicamente para exfiltrar dados.

O teste de penetração de qualquer lugar, ao vivo em um navegador da web com Cloud C2.

É simples também. Um botão oculto o transforma em uma unidade flash, onde a alteração de configurações é apenas a edição de um arquivo de texto. E com um shell raiz, suas ferramentas de teste de penetração favoritas como nmap, responder, impacket e metasploit estão prontas para uso.

# PACKET SQUIRREL



A ferramenta Packet Squirrel da Hak5 é um mini-computador Linux de alta performance, otimizado para operações em rede. Ele foi projetado para oferecer uma ampla gama de funcionalidades de segurança de rede, incluindo packet sniffing, DNS spoofing, reverse shell/VPN e acesso root shell.

O Packet Squirrel é centrado em torno do seu interruptor de 4 vias: cada posição do interruptor representa um modo de operação configurável. Ao mudar a posição do interruptor, é possível acionar um payload específico. Além disso, ele possui um botão configurável e um LED RGB para fornecer implantação instantânea e feedback dos payloads.

Totalmente programável e com suporte da biblioteca de payloads da Hak5, o Packet Squirrel é a ferramenta perfeita para testadores de penetração, administradores de sistemas ou usuários avançados. Ele é discreto e compacto, projetado para se misturar ao ambiente quando conectado a uma rede alvo. Com sua capacidade de executar payloads configuráveis e acessar remotamente uma rede, o Packet Squirrel é uma ferramenta poderosa para testes de segurança em redes. Ele permite que os testadores de penetração avaliem a segurança da rede, identifiquem vulnerabilidades e explorem falhas, tudo de forma eficiente e discreta.

# SCREEN CRAB

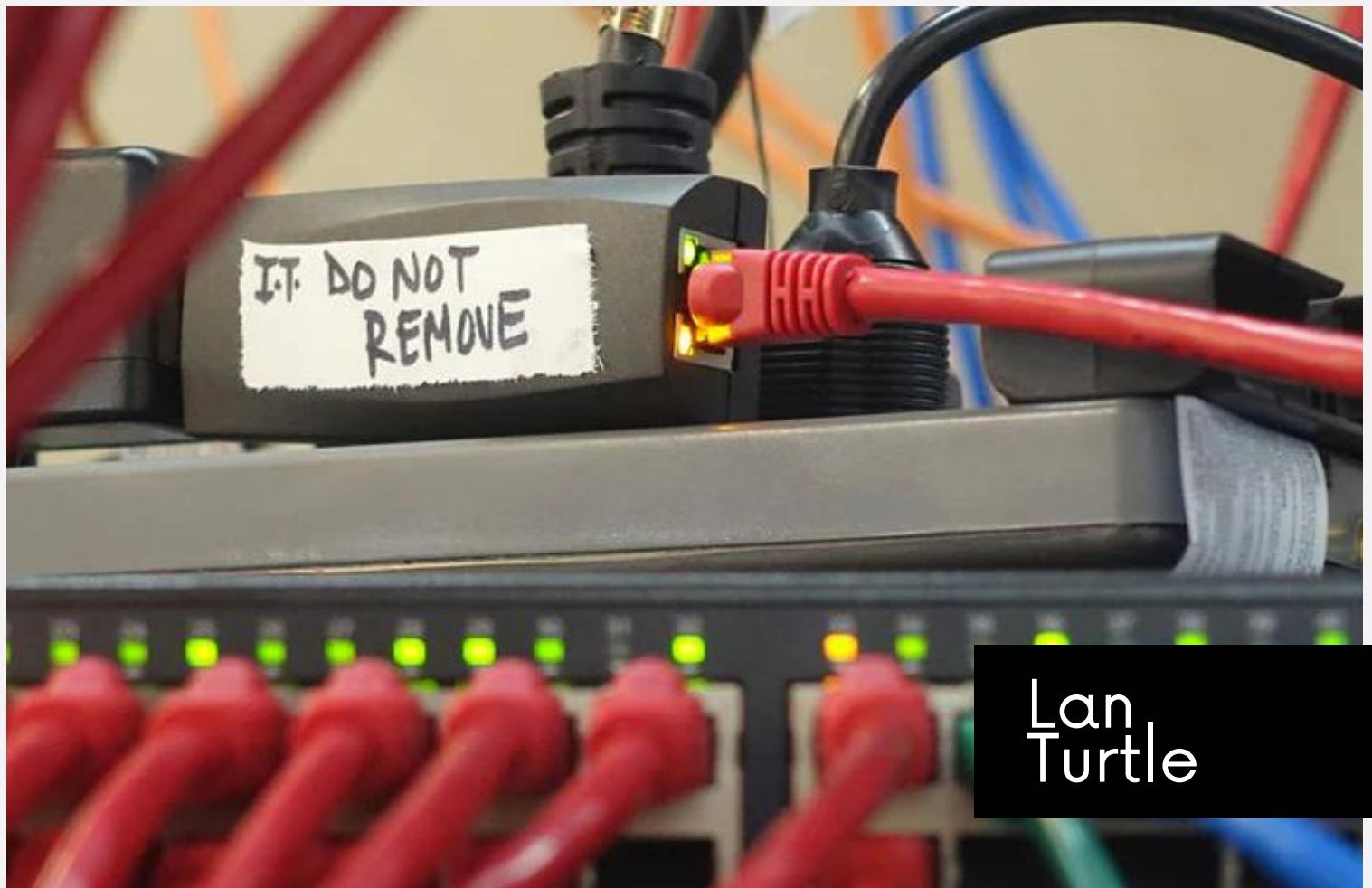
DO NOT REMOVE  
Conference Room 3

A ferramenta Screen Crab da Hak5 é um implante de vídeo stealth man-in-the-middle. Esse discreto capturador de tela em linha fica entre dispositivos HDMI - como um computador e um monitor, ou um console e uma televisão - para capturar silenciosamente capturas de tela. É perfeito para administradores de sistemas, pentesters e qualquer pessoa que queira registrar o que está em uma tela.

Com o Screen Crab, é possível capturar as telas dos dispositivos HDMI conectados a ele, sem que o usuário perceba. Isso permite que os pentesters avaliem a segurança de um sistema, observem o que um usuário está fazendo em um dispositivo ou registrem as atividades de um sistema para fins de monitoramento.



scan or click



## IMPLANTES DE HARDWARE

Julio Della Flora

A ferramenta Lan Turtle da Hak5 é um dispositivo de hacking em rede que pode ser conectado a uma porta LAN para permitir o acesso remoto e furtivo a redes de computadores. Ele possui vários recursos, como a captura de senhas, a instalação de backdoors e a execução de comandos remotos. O Lan Turtle é um dispositivo pequeno, discreto e fácil de usar, sendo uma ferramenta poderosa para testes de penetração em redes corporativas ou domésticas.

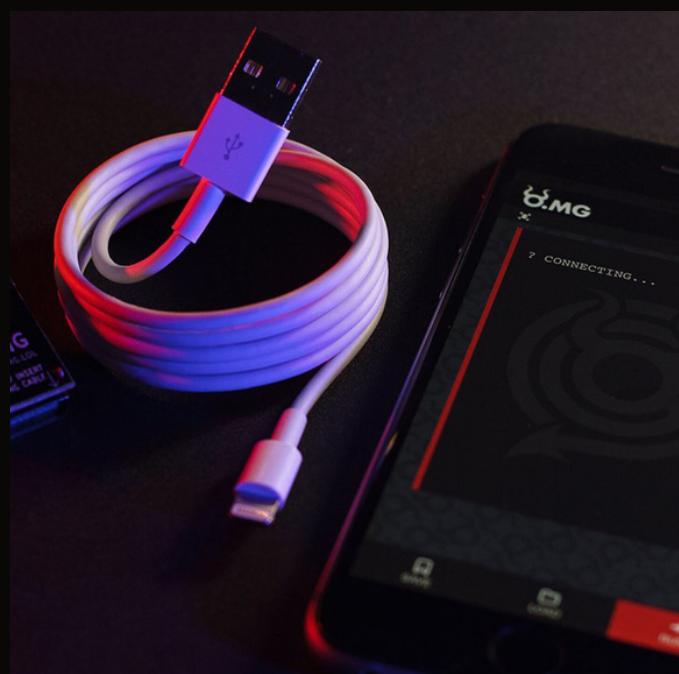
*"...o implante acima se chama lan turtle"*

Um membro do red team poderia utilizar a ferramenta Lan Turtle para comprometer a segurança de uma empresa conectando-a a uma porta LAN disponível e, em seguida, utilizando-a para executar uma série de ataques de rede furtivos. Por exemplo, a ferramenta poderia ser usada para capturar senhas ou credenciais de rede, ou para instalar um backdoor em um sistema para acesso remoto posterior.

— julio della flora

# O.MG Cable

O O.MG Cable é um cabo USB artesanal com um implante avançado escondido em seu interior, projetado para permitir que o Red Team emule cenários de ataque de adversários sofisticados. Esses cabos permitem testar novas oportunidades de detecção para as equipes de defesa e são ferramentas extremamente impactantes para ensino e treinamento. O tamanho físico do implante é projetado com atenção para ser discreto e fácil de usar, e o firmware é atualizado continuamente para melhorar a potência, flexibilidade e facilidade de uso.





# ANALISADOR LÓGICO

Um analisador lógico é um dispositivo eletrônico usado para capturar e analisar sinais digitais em um sistema. Ele é usado para visualizar e depurar a comunicação entre dispositivos digitais, tais como microcontroladores, memórias, interfaces, dentre outros.

Os analisadores lógicos possuem vários canais de entrada, permitindo capturar simultaneamente múltiplos sinais digitais. Eles são capazes de registrar e exibir dados em tempo real ou em uma taxa pré-definida, permitindo que os usuários visualizem as formas de onda dos sinais digitais e identifiquem problemas de temporização, ruído e outras anomalias que podem afetar o desempenho do sistema.

*"Ferramenta de hacking  
RFID de código aberto"*

## RFID (Radio-Frequency IDentification)

O Proxmark3 é uma ferramenta de hardware de código aberto usada para análise, clonagem e emulação de dispositivos RFID (Radio-Frequency IDentification). Ele permite a leitura e escrita em tags RFID, bem como a simulação de tags para emulação de dispositivos. O Proxmark3 é amplamente utilizado para fins de pesquisa em segurança, bem como para testes de penetração em sistemas de controle de acesso e identificação. Ele também é altamente personalizável e pode ser estendido com vários módulos e scripts para suportar diferentes tipos de RFID e outras funcionalidades.





## HackRF One

# Rádio Definido por Software

O HackRF One é uma ferramenta de hardware de código aberto que pode ser usada para testes de segurança, pesquisa em comunicações sem fio e experimentação em radiofrequência (RF). Ele permite que os usuários transmitam e recebam sinais de rádio em uma ampla faixa de frequências, desde baixa frequência (LF) até frequência muito alta (VHF) e ultra alta frequência (UHF), tornando-o uma ferramenta versátil para vários fins.

A principal funcionalidade do HackRF One é permitir que os usuários explorem as vulnerabilidades em dispositivos que usam comunicação sem fio, como dispositivos IoT, sistemas de controle de acesso sem fio e até mesmo drones. O HackRF One também é amplamente utilizado em pesquisa acadêmica e para desenvolvimento de protótipos em áreas como comunicações sem fio, redes móveis e segurança cibernética.



# RASPBERRY PI

O Raspberry Pi é um computador de placa única (SBC) desenvolvido pela Fundação Raspberry Pi, com o objetivo de promover a educação em ciência da computação e a programação para crianças e jovens. No entanto, o Raspberry Pi rapidamente ganhou popularidade como uma plataforma acessível e versátil para vários fins, desde projetos de IoT até servidores de mídia e centros de jogos.

---

O Raspberry Pi é baseado em um processador ARM de baixo consumo de energia e é executado em uma distribuição do Linux chamada Raspbian, que é otimizada para o hardware do Raspberry Pi. O Raspberry Pi também possui várias portas de entrada e saída (I/O) para se conectar a outros dispositivos, incluindo USB, HDMI, Ethernet, Wi-Fi e Bluetooth.

# M5STACK

... E TODA A FAMÍLIA M5



ARE YOU  
READY?

ESP32  
MCU

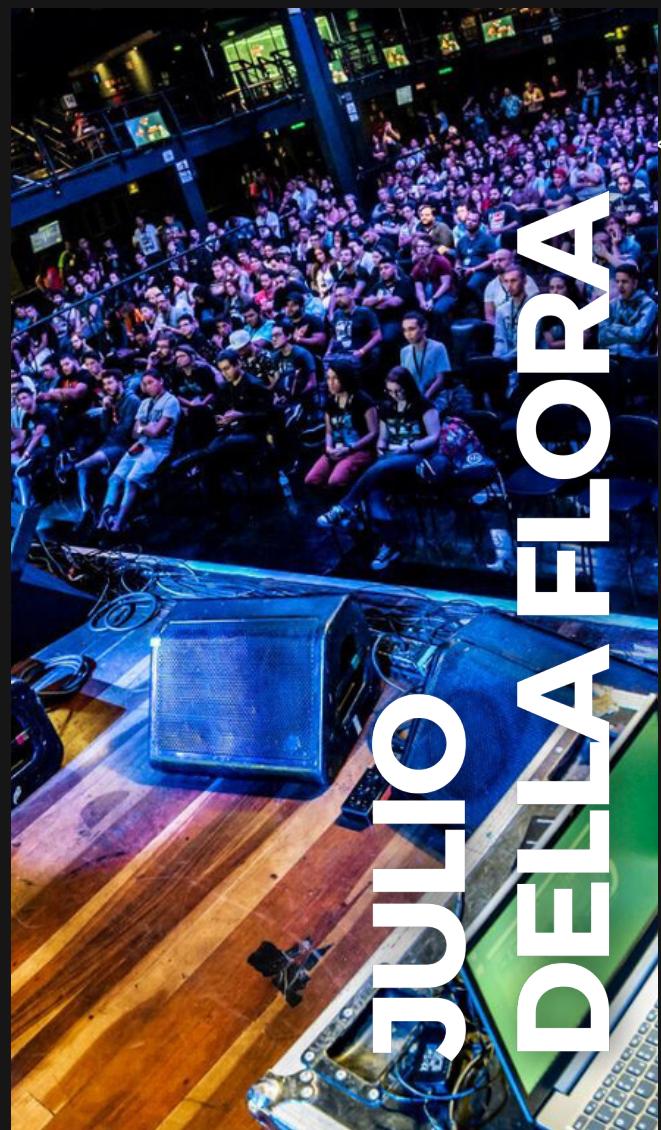
O M5Stack é uma plataforma de desenvolvimento de IoT modular e portátil. É composto por uma placa base com uma tela a cores, vários módulos de sensores e atuadores, bem como uma bateria recarregável. A plataforma é baseada em um microcontrolador ESP32, que possui conectividade Wi-Fi e Bluetooth, permitindo que os usuários criem e interajam com dispositivos IoT de maneira rápida e fácil.

O M5Stack é uma ferramenta acessível e versátil para projetos de IoT, permitindo que os usuários criem protótipos rapidamente e testem ideias com facilidade. Com sua ampla variedade de módulos e recursos, o M5Stack pode ser usado em várias aplicações, incluindo medição de temperatura e umidade, controle de motores, monitoramento de energia e muito mais.



E Agora?

qual o próximo  
passo?



# treinamento em hardware hacking

Você já imaginou ser capaz de hackear dispositivos eletrônicos e explorar vulnerabilidades em sistemas de segurança para proteger sua empresa ou instituição? Agora, você pode! Estamos oferecendo um treinamento em hardware hacking, ministrado pelo professor Julio Della Flora, especialista em segurança de sistemas e hardware.

Com o treinamento, você terá acesso a um conhecimento exclusivo que irá ajudá-lo a se destacar no mercado e garantir a segurança de sua empresa ou instituição.

SAIBA MAIS PELO QR CODE ABAIXO



scan or click