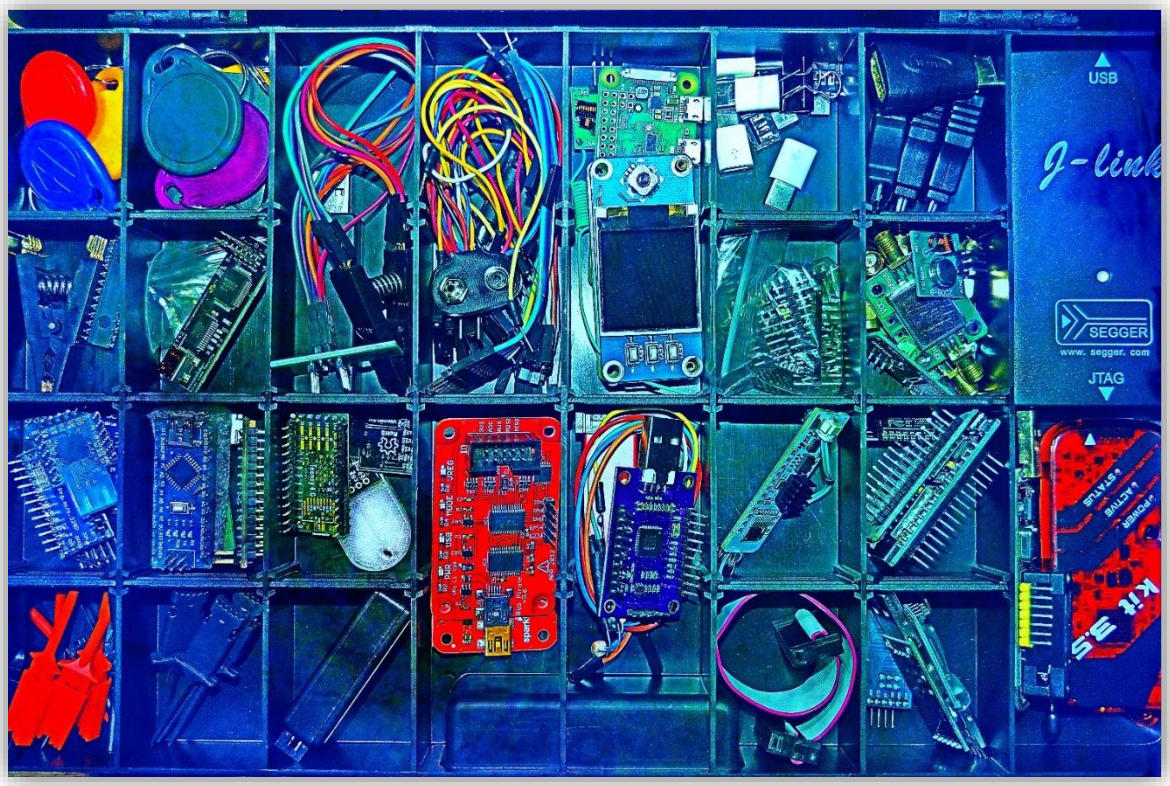
FERRAMENTAS PARA HARDWARE HACKING



Link para o treinamento: https://go.hotmart.com/G35913582B

Prof. Julio Della Flora

https://www.instagram.com/juliodellaflora/

https://www.linkedin.com/in/juliodellaflora/

https://twitter.com/jcldf

Um multímetro ou multiteste (multimeter ou DMM - digital multi meter em inglês) é um aparelho destinado a medir e avaliar grandezas elétricas. Existem modelos com mostrador analógico (de ponteiro) e modelos com mostrador digital.

Utilizado na bancada de trabalho (laboratório) ou em serviços de campo, incorpora diversos instrumentos de medidas elétricas num único aparelho como voltímetro, amperímetro e ohmímetro por padrão e capacímetro, frequencímetro, termômetro entre outros, como opcionais conforme o fabricante do instrumento disponibilizar.

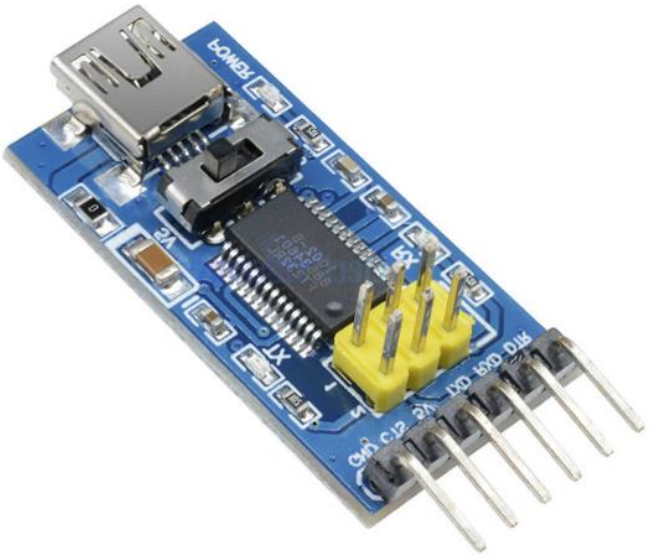
Tem ampla utilização entre os técnicos em eletrônica e eletrotécnica, pois são os instrumentos mais usados na pesquisa de defeitos em aparelhos eletro-eletrônicos devido à sua simplicidade de uso e, normalmente, portabilidade.

Diferentes fabricantes oferecem inúmeras variações de modelos. Oferecem uma grande variedade de precisões (geralmente destaca-se a melhor precisão para medidas em tensão CC), nível de segurança do instrumento, grandezas possíveis de serem medidas, resolução (menor valor capaz de ser mostrado/exibido), conexão ou não com um PC, etc.

Há modelos destinados a uso doméstico (onde o risco de um acidente é menor) e modelos destinados a uso em ambiente industrial (que devido as maiores correntes de curto-circuito apresentam maior risco). A precisão de leitura (exatidão) não é o que diferencia estas duas opções e sim sua construção interna (trilhas do CI mais espaçadas, maior espaçamento entre a placa de CI e a carcaça e maior robustez a transientes nos modelos industriais).

https://pt.wikipedia.org/wiki/Mult%C3%ADmetro

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_d8he3mb



O Módulo FTDI é um módulo conversor exclusivo que possui a capacidade de converter sinais USB em sinais Serial de nível TTL e RS232 para facilitar a comunicação entre computadores e plataformas microcontroladoras.

- Com um circuito integrado FT232R próximo ao conector USB, o Módulo FTDI é capaz de executar com competência e precisão a conversão dos dados recebidos.

- Na extremidade oposta ao terminal USB do Módulo FTDI existe um conector com uma sequência de 6 pinos, os quais possuem uma configuração própria e estão devidamente especificados logo abaixo.

- Muito funcional o Módulo FTDI é ideal programação junto ao Arduino Pro, Pro Mini e LilyPad, executando com qualidade comprovada todas as conversões necessárias.

- Segue a relação dos terminais do Módulo FTDI: GND, CTS, VCC, TX, RX e DTR e um exclusivo sistema que possibilita ao projetista hobista ou profissional do ramo um conversor integrado que pode ter sua tensão de trabalho tanto em 3.3V como em 5V.

- A principal diferença do cabo FTDI para o Módulo FTDI é que este possui o pino DTR no lugar do RTS do cabo. O pino DTR possibilita ao Arduino se auto resetar quando um novo programa é instalado na placa, dispensado dessa forma o botão reset ao fazer um upload.

https://www.usinainfo.com.br/conversores-de-sinal/modulo-conversor-usb-para-ttl-serial-ft232r-33v-5v-2764.html?search_query=rs232&results=24

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_dSIAjWL

O Programador Gravador EPROM FLASH BIOS USB CH341A é um módulo gravador e programador interno para memórias das séries 24xx e 25xx, DIP e SMD.

Aplicações:

Aparelhos de Som / Módulos Automotivos EPROM séries 24xx e 25xx.

Memórias de Receptores de EPROM série 25xx.

Memórias de TVs (CIs séries 24xx e 25xx).

Memórias de Monitores de Vídeo (CIs séries 24xx e 25xx).

Memórias BIOS de placas Mãe PC e Notebook séries 25xx.

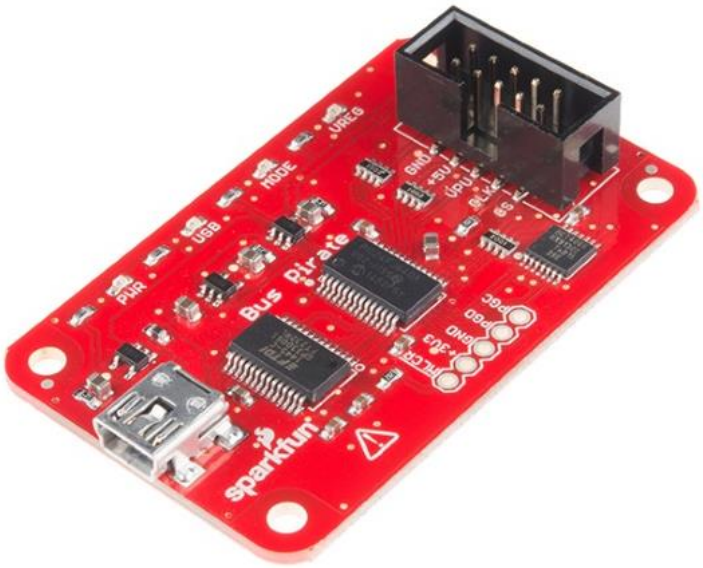
Memórias de DVD players e gravadores de DVD de séries 25xx.

Memórias de diversos equipamentos eletrônicos com chips 24xx e 25xx.

Especificações Técnicas:

Programador Gravador EPROM FLASH BIOS USB CH341A
Marca: OEM
Alimentação de 5V via USB
Interface USB 1.1 de alta velocidade compatível
Conector ZIF
Suporte 24EEPROM e 25 SPI flash de 8 pinos / 16 pinos
Chip CH341A
Suporta a familia 24xx e 25xx
LED indicador de funcionamento
Material: Termoplásticos / Metal / Placa de Fenolite
Origem: China
Tamanho: 57mm Largura x 20mm Profundidade x 12mm Altura
Peso: 12g
https://www.saravati.com.br/programador-gravador-eprom-flash-bios-usb-ch341a

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_d62fRI3



A placa Sparkfun Bus Pirate V3.6A é uma placa que você conecta no computador e com ela consegue efetuar a comunicação com dispositivos embarcados que usam o protocolo I2C, 1-wire, 2-wire, 3-wire, UART, SPI e também o controlador de LCD HD44780, com tensões entre 0 e 5.5VDC.

Utilizar a Bus Pirate é relativamente simples: digite os comandos em uma janela de terminal no computador, e estes comandos serão interpretados pelo Bus Pirate e enviados para o dispositivo utilizando o protocolo correto. A mesma coisa acontece com o sentido inverso: dados enviados pelo dispositivo são interpretados pelo Bus Pirate e retornam ao computador.

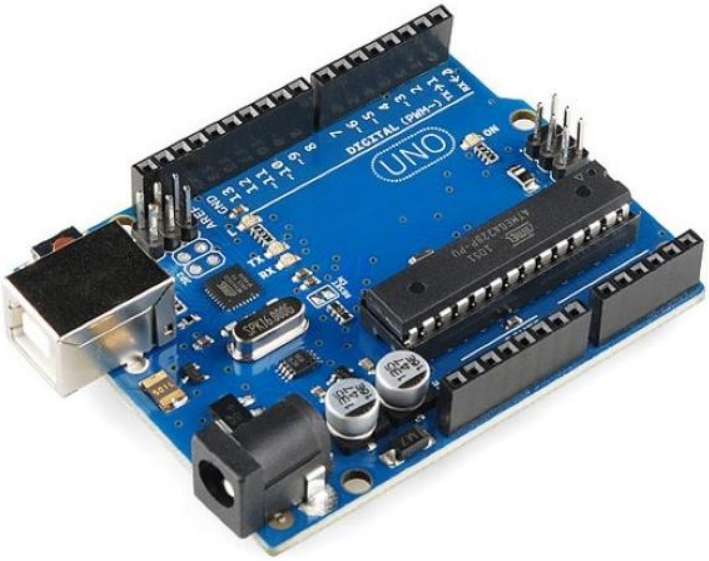
O componente principal do Bus Pirate é um microcontrolador PIC24FJ64, e para comunicação com o computador temos o já conhecido chip FTDI FT232RL. O microcontrolador contém um bootloader que permite que o CI seja atualizado e customizado.

Especificações:

– Microcontrolador PIC24FJ64 (datasheet)
– Protocolos suportados: 1-wire, I2C, SPI, JTAG, Serial assíncrona, MIDI, teclado PC, HD44780, 2 e 3-wire com pino de controle bitwise, UART
– Pinos tolerantes à 5V
– Frequência de medição 1Hz à 40MHz
– Gerador de frequência de 1KHz à 4MHz
– Resistore pull-up embutidos
– Pinos de alimentação 3.3 e 5VDC com software reset
– Bus Traffic Sniffers (SPI, I2C)
– Bootloader para updates de firmware
– Interface Serial -> USB FTDI
– Analizador lógico 10Hz _a 1MHz de baixa velocidade
– Programável com Python, Perl, etc
– Acesso à porta de programação ICSP do PIC24FJ64
– Leds indicadores de operação
– Dimensões: 60 x 37 x 11mm

https://www.filipeflop.com/produto/bus-pirate-v3-6a-sparkfun/

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_dUPIrJ9



Arduino é uma plataforma de prototipagem eletrônica de hardware livre e de placa única, projetada com um microcontrolador Atmel AVR com suporte de entrada/saída embutido, uma linguagem de programação padrão, a qual tem origem em Wiring, e é essencialmente C/C++. O objetivo do projeto é criar ferramentas que são acessíveis, com baixo custo, flexíveis e fáceis de se usar por principiantes e profissionais. Principalmente para aqueles que não teriam alcance aos controladores mais sofisticados e ferramentas mais complicadas.

Pode ser usado para o desenvolvimento de objetos interativos independentes, ou ainda para ser conectado a um computador hospedeiro. Uma típica placa Arduino é composta por um controlador, algumas linhas de E/S digital e analógica, além de uma interface serial ou USB, para interligar-se ao hospedeiro, que é usado para programá-la e interagi-la em tempo real. A placa em si não possui qualquer recurso de rede, porém é comum combinar um ou mais Arduinos deste modo, usando extensões apropriadas chamadas de shields. A interface do hospedeiro é simples, podendo ser escrita em várias linguagens. A mais popular é a Processing, mas outras que podem comunicar-se com a conexão serial são: Max/MSP, Pure Data, SuperCollider, ActionScript e Java. Em 2010 foi realizado um documentário sobre a plataforma chamado Arduino: The Documentary.

https://pt.wikipedia.org/wiki/Arduino

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_dW85MoT

O osciloscópio é um instrumento de medida de sinais elétricos/eletrônicos que apresenta gráficos a duas dimensões de um ou mais sinais elétricos (de acordo com a quantidade de canais de entrada). O eixo vertical (y) do ecrã (monitor) representa a intensidade do sinal (tensão) e o eixo horizontal (x) representa o tempo, tornando o instrumento útil para mostrar sinais periódicos. O monitor é constituído por um "ponto" que periodicamente "varre" a tela da esquerda para a direita.

Apesar de a maioria das pessoas pensarem no osciloscópio como um instrumento dentro de uma caixa, um novo tipo de "osciloscópio" está surgindo, o qual consiste de um conversor analógico-digital externo (algumas vezes com sua própria memória ou com habilidade de processamento de dados) conectado a um PC que provê o display, interface de controle, armazenamento em disco, rede e muitas vezes a alimentação elétrica. A viabilidade destes Osciloscópio baseados em PC esta no seu uso comum e no baixo custo dos PCs padrão. Isto torna o instrumento particularmente prático para o mercado educacional, onde os PCs são comuns porém os investimentos em equipamentos são comumente baixos.

As vantagens dos osciloscópios baseados em PC incluem:

Custo reduzido (considerando que o usuário já possua um PC).

Fácil exportação de dados para softwares comuns do PC como processadores de texto e planilhas.

Habilidade de controlar o instrumento através de um programa no PC.

Uso das funções de rede e armazenamento do computador, que aumentam o custo em um osciloscópio comum.

Portabilidade mais fácil quando utilizado em uma laptop.

Este tipo de instrumento também possui desvantagens, entre elas:

Necessidade de instalar o software no PC.

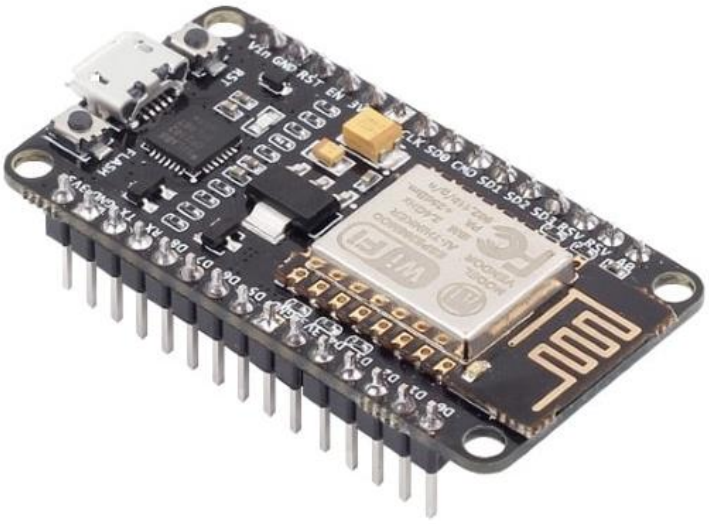
Tempo levado pelo boot do PC, quando comparado ao tempo praticamente instantâneo de início de atividades de um osciloscópio padrão (apesar de alguns osciloscópios modernos serem PCs ou máquinas similares).

Portabilidade reduzida em um desktop.

O inconveniente de usar parte da tela do PC como display do osciloscópio.

https://pt.wikipedia.org/wiki/Oscilosc%C3%B3pio

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_d8oYjJl



NodeMCU é uma plataforma open source da Internet das Coisas. Ela usa a linguagem de script Lua. Baseado no projeto eLua, foi construído sobre o SDK ESP8266 0.9.5. Existem muitos projetos de código aberto para o seu uso como a lua-cjson e spiffs.

NodeMCU foi criado logo após o lançamento do ESP8266. Em 30 de dezembro de 2013, a empresa Espressif começou a produzir o ESP8266. A produção do NodeMCU começou em 13 outubro de 2014, quando Hong postou o primeiro arquivo do nodemcu-firmware no GitHub.[4] Dois meses depois, o projeto se expandiu para incluir uma plataforma de open hardware quando o desenvolvedor Huang R publicou o arquivo gerber de uma placa ESP8266, chamando de devkit 1.0.

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_dVzK5qj

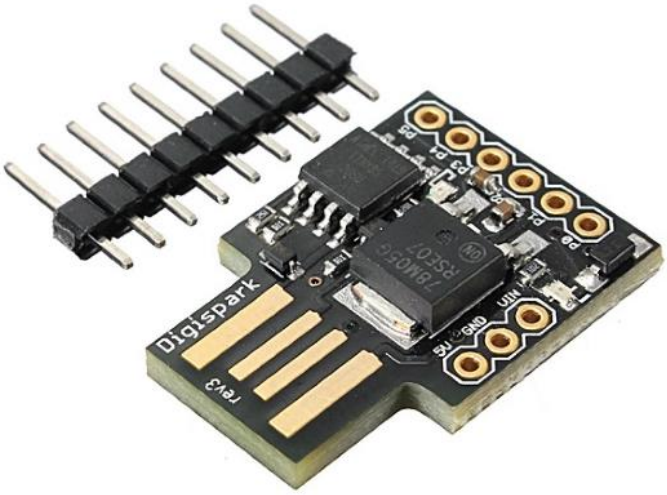
O módulo ESP32 é um módulo de alta performance para aplicações envolvendo wifi, contando com um baixíssimo consumo de energia. É uma evolução do já conhecido ESP8266, com maior poder de processamento e bluetooth BLE 4.2 embutidos.

Na placa temos o chip ESP32 com antena embutida, uma interface usb-serial e regulador de tensão 3.3V. A programação pode ser feita em LUA ou usando a IDE do Arduino através de um cabo micro-usb. Com 4 MB de memória flash, o ESP32 permite criar variadas aplicações para projetos de IoT, acesso remoto, webservers e dataloggers, entre outros.

Sem dúvidas este módulo é um grande aliado do maker IoT! Ao comparar seu preço com todas as possibilidades que ele proporciona, é possível concluir que seu custo benefício é excelente.

https://www.filipeflop.com/produto/modulo-wifi-esp32-bluetooth/

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_d7orFfH



A Placa de Desenvolvimento ATTINY85 Digispark é uma placa com o microcontrolador ATMEL AVR ATTINY85. Pode ser encaixada diretamente na USB do computador e programada utilizando a IDE do Arduino, ótima opção para projetos wearables ou se você tem pouco espaço disponível.

Tem 6 pinos de I/O, dos quais 3 podem ser usados como PWM, 8K de memória flash e suporta alimentação externa. O mais legal é que não precisa de cabo para programação, basta plugar e descarregar o programa!

https://www.filipeflop.com/produto/placa-de-desenvolvimento-attiny85-digispark/

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_dZfgtbl

O Proxmark é um canivete suíço de RFID, permitindo interações de alto e baixo nível com a grande maioria das etiquetas e sistemas de RFID em todo o mundo. Originalmente construído por Jonathan Westhues há mais de 10 anos, o dispositivo evoluiu progressivamente para a ferramenta padrão da indústria para análise de RFID.

Sua versatilidade o adaptou a muitos setores e usos: entusiastas da RFID, pesquisa acadêmica, desenvolvimento de produtos, aplicação da lei e testes de penetração.

Houve uma rápida evolução do hardware e software nos últimos anos, resultando em versões maduras e minaturizadas do hardware. Há revisões otimizadas para uso em campo, com equipes de red team ou testes de invasão, e versões de desktop aprimoradas para uso em pesquisa no corporativa ou acadêmica.

https://proxmark.com/

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_dUTFHmL

O Analisador Lógico 24Mhz 8CH tem como funcionalidade duas operações básicas, uma delas é registrar o estado de sinais digitais em uma memória interna durante determinado tempo e a outra é apresentar os resultados obtidos em um visor para que os dados possam ser analisados, de modo a identificar qualquer mudança de estado.

Para monitorar ou testar o comportamento dos pinos digitais usamos o Analisador Lógico e estabelecemos a correlação entre a mudança de estado de um sinal para o outro.

Relativamente econômico e simples, o Analisador Lógico possui a capacidade de implementar outras funções e consecutivamente ampliar sua capacidade conforme seus recursos e imaginação.

O Analisador Lógico possui a capacidade de captar 8 sinais digitais em uma memória RAM estática de 32 kB. Para análise e estudo da funcionalidade do equipamento em teste, o Analisador Lógico compartilha seus dados com um computador que fica responsável pela apresentação do diagrama de tempo em formato de gráfico.

Perfeito para experimento com microcontroladores o Analisador Lógico é o equipamento responsável por monitorar a execução e a programação, realizando a análise de diversos protocolos como, por exemplo, I2C, SPI, dentre outros.

https://www.usinainfo.com.br/testadores-e-medidores-diversos/analisador-logico-24mhz-8ch-al24-2691.html

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_d9e9PDD

A Raspberry Pi Zero W Anatel é uma placa de baixo custo com um tamanho reduzido (apenas 6,5 x 3cm), permitindo que você crie projetos compactos sem perder a flexibilidade que as placas da linha Raspberry proporcionam.

A placa conta com WiFi e Bluetooth integrados, eliminando assim, a necessidade de usar adaptadores na porta USB. O seu processador é o Broadcom BCM2835 single-core de 1GHz que, aliado à memória de 512MB, permite que você crie aplicações controlando a GPIO de 40 pinos, desenvolva projetos de IoT ou simplesmente se divirta rodando um emulador de videogames (confira na seção blog abaixo como você pode fazer isso usando Lakka).

A Raspberry Pi Zero W Anatel tem slot para cartão micro SD, conector de vídeo mini HDMI, 2 portas USB (1 para dados e outra para alimentação 5V) e roda diversas distribuições Linux como o Raspbian e Ubuntu, e aplicações como Scratch, Minecraft e Sonic Pi.

A certificação por parte da Anatel (Agência Nacional de Telecomunicações) garante que o equipamento está dentro das especificações definidas pela agência, e em conformidade com a regulamentação brasileira de telecomunicações, o que significa que você pode desenvolver e comercializar produtos utilizando esta placa.

https://www.filipeflop.com/produto/raspberry-pi-zero-w/

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_Bf7UqZxN

O Pickit 3 é um gravador de baixo custo, mais rápido se comparado com versões anteriores e que realiza a gravação dos microcontroladores PIC por meio de conexão ICSP (In Circuit Serial Programming). Suporta os microcontroladores PIC das linhas PIC16F, PIC18F, dsPIC33f, PIC24 e PIC 32. Ele também tem a função de debug (depurador), onde você pode conectar o Pickit 3 diretamente no circuito e verificar em tempo real as condições e configurações do equipamento.

https://www.filipeflop.com/blog/como-utilizar-gravador-pic-pickit-3/

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_dYwoTqL

O que o chip FT232H pode fazer? Este chip da FTDI é semelhante ao seu conversor de USB para serial, mas adiciona um 'mecanismo serial síncrono multiprotocolo' que permite falar muitos protocolos comuns como SPI, I2C, UART serial, JTAG e muito mais! Há até um punhado de pinos GPIO digitais que você pode ler e escrever para fazer coisas como LEDs piscarem, interruptores ou botões de leitura e muito mais. O FT232H é como adicionar um pequeno canivete suíço para protocolos seriais no seu computador!

https://learn.adafruit.com/adafruit-ft232h-breakout

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_dUpL9XN

O M5StickC é um mini M5Stack, equipado com um ESP32, que é um único chip combinado de Wi-Fi e Bluetooth de 2,4 GHz e integra um flash SPI de 4 MB. É uma placa de desenvolvimento de IoT portátil, fácil de usar e de código aberto. O que isso pode fazer? Esse pequeno bloco é capaz de realizar sua ideia, iluminar sua criatividade e ajudar com a prototipagem da IoT em um tempo muito curto. O M5stickC é um dos principais dispositivos da série de produtos M5Stack.

Ele é construído em um ecossistema de hardware e software em crescimento contínuo. Possui muitos módulos e unidades compatíveis, bem como o código-fonte aberto e as comunidades de engenharia que ajudarão você a maximizar seus benefícios em todas as etapas do processo de desenvolvimento.

https://m5stack.com/products/stick-c

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_dVbh4T1

Monte um prático testador de componentes para sua bancada com este Kit Testador de Componentes DIY, que realiza medições de resistores, transistores, capacitores, diodos, leds e outros componentes de forma simples e prática.

O testador é capaz de identificar o tipo de componente que foi conectado nos pinos de teste, e exibe a pinagem e os valores no display gráfico LCD, funcionando também com componentes SMD.

Antes de usar, consulte o manual do usuário na seção de downloads abaixo para verificar o tipo de componente aceito pelo medidor, assim como as respectivas tolerâncias.

Atenção: A montagem deste kit exige conhecimentos básicos de eletrônica e soldagem de componentes eletrônicos.

https://www.filipeflop.com/produto/kit-testador-de-componentes-diy/

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_d6tbMnv

O microscópio é um instrumento óptico com capacidade de ampliar imagens de objetos muito pequenos graças ao seu poder de resolução. Este pode ser composto ou simples: microscópio composto tem duas ou mais lentes associadas; microscópio simples é constituído por apenas uma lente células.

Acredita-se que o microscópio tenha sido inventado no final do século XVI por Hans Janssen e seu filho Zacharias, dois holandeses fabricantes de óculos. Tudo indica, porém, que o primeiro a fazer observações microscópicas de materiais biológicos foi o neerlandês Antonie van Leeuwenhoek (1632 - 1723). Serve-se especialmente para os cientistas, que utilizam este instrumento para estudar e compreender os micro-organismos.

Os microscópios de Leeuwenhoek eram dotados de uma única lente, pequena e quase esférica. Nesses aparelhos ele observou detalhadamente diversos tipos de material biológico, como embriões de plantas, os glóbulos vermelhos do sangue e os espermatozoides presentes no sêmen dos animais. Foi também Leeuwenhoek quem descobriu a existência dos micróbios, como eram antigamente chamados os seres microscópicos, hoje conhecidos como micro-organismos.

https://pt.wikipedia.org/wiki/Microsc%C3%B3pio

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_dZQ8RIj

O ferro de solda é utilizado para unir duas partes metálicas, como fios condutores, placas de circuito e demais componentes, por meio da solda. O ferro de solda mais utilizado é o do tipo lápis, pois são pequenos e de fácil manuseio, recomendado para aqueles que gostam de fazer pequenos reparos em casa. Porém, existem ferros de soldas de diferentes potências e com diferentes pontas. Escolha o que melhor se adapta as suas necessidades e bom trabalho.

https://www.lojadomecanico.com.br/setor/19/193/795/ferro-de-solda-estacao-de-solda

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_d82rnhh

O RTL-SDR é um dongle USB muito barato, que pode ser usado como um scanner de rádio baseado em computador para receber sinais de rádio ao vivo em sua área (sem necessidade de internet). Dependendo do modelo específico, ele pode receber frequências de 500 kHz a 1,75 GHz. A maioria dos softwares para o RTL-SDR também é desenvolvida pela comunidade e fornecida gratuitamente.

As origens do RTL-SDR decorrem de dongles de sintonizadores de TV DVB-T produzidos em massa, baseados no chipset RTL2832U. Com os esforços combinados de Antti Palosaari, Eric Fry e Osmocom (em particular Steve Markgraf), verificou-se que os dados brutos de I / Q no chipset RTL2832U podiam ser acessados diretamente, o que permitiu que o sintonizador de TV DVB-T fosse convertido em um rádio definido por software de banda larga por meio de um driver de software personalizado desenvolvido por Steve Markgraf. Se você já gostou do projeto RTL-SDR, considere doar para a Osmocom via Open Collective, pois foram eles que desenvolveram os drivers e deram vida ao RTL-SDR.

Ao longo dos anos desde sua descoberta, o RTL-SDR se tornou extremamente popular e democratizou o acesso ao espectro de rádio. Agora qualquer pessoa, incluindo hobistas com orçamento limitado, podem acessar o espectro de rádio. Vale a pena notar que esse tipo de capacidade SDR custaria centenas ou mesmo milhares de dólares apenas alguns anos atrás. Às vezes, o RTL-SDR também é conhecido como RTL2832U, DVB-T SDR, dongle DVB-T, dongle RTL ou o "rádio definido por software barato".

https://www.rtl-sdr.com/about-rtl-sdr/

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_dUIwoll

O HackRF One da Great Scott Gadgets é um periférico de rádio definido por software capaz de transmitir ou receber sinais de rádio de 1 MHz a 6 GHz. Projetado para permitir teste e desenvolvimento de tecnologias de rádio modernas e de próxima geração, o HackRF One é uma plataforma de hardware de código aberto que pode ser usada como periférico USB ou programada para operação independente.

Frequência de operação de 1 MHz a 6 GHz

transceptor half-duplex

até 20 milhões de amostras por segundo

Amostras de quadratura de 8 bits (I de 8 bits e Q de 8 bits)

compatível com GNU Radio, SDR # e mais

filtro de ganho e banda de base RX e TX configurável por software

potência da porta da antena controlada por software (50 mA a 3,3 V)

Conector de antena fêmea SMA

Entrada e saída de relógio fêmea SMA para sincronização, botões convenientes para programação, cabeçalhos de pinos internos para expansão USB 2.0 de alta velocidade

Alimentado por USB hardware de código aberto

O HackRF One possui um gabinete de plástico moldado por injeção e é fornecido com um cabo micro USB. Uma antena não está incluída. O ANT500 é recomendado como antena inicial para o HackRF One.

O HackRF One é um equipamento de teste para sistemas de RF. Não foi testado quanto à conformidade com os regulamentos que regem a transmissão de sinais de rádio. Você é responsável por usar seu HackRF One legalmente.

https://greatscottgadgets.com/hackrf/one/

LINK PARA COMPRA: http://s.click.aliexpress.com/e/_dSoV9kf

Quero trazer para vocês através desse documento um caminho para iniciar seus estudos em hardware hacking, todos nós sabemos que essa área apesar de estar em crescente desenvolvimento ainda não possui informações abundantes em português. Não é fácil encontrar dicas e tutoriais sobre a prática do hardware hacking, pentest em dispositivos embarcados e ferramentas para red team.

O primeiro passo é construir um conhecimento básico em eletrônica. Da mesma forma que o hacking em sistemas operacionais, web ou para dispositivos móveis, o segredo está em conhecer os fundamentos.

2. Estude então fundamentos de eletrônica analógica e digital, a eletrônica digital está completamente atrelada à computação. Estudando eletrônica você terá um panorama geral dos dispositivos que quer alterar ou invadir.

3. Tenha um conhecimento básico das principais técnicas de invasão, essas técnicas geralmente são genéricas a ponto de poderem ser aplicadas em diversos cenários. Como exemplo, um ataque de Man In The Middle além de seu uso tradicional aplicado às redes de computadores, também pode ser utilizado para verificar a comunicação em barramentos de hardware.

4. 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.

https://youtu.be/DE-FNN5Ps6w

5. Procure conhecer ataques “exotéricos”, técnicas novas e não convencionais. Esse tipo de conhecimento é algo que você vai obter explorando palestras das diversas conferências de segurança no Brasil e no resto do mundo. Tenha em mente que grande parte dessas palestras estarão em inglês.

Para que você tenha noção dos tipos de ataque aos quais me refiro, vou deixar outra palestra ministrada por mim.

https://www.youtube.com/watch?v=aDQq7xITXKs

6. Não basta só 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.

https://www.youtube.com/watch?v=aBYOedssgpY

7. Por fim, 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).

https://www.youtube.com/watch?v=A3neX6KX6xM

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.

Meus professores sempre diziam que para ter dúvidas é preciso ao menos prestar atenção na matéria.

Outra coisa que vai alavancar a sua curva de aprendizado é fazer cursos e treinamentos específicos, e é aqui que deixo o meu jabá ;)

https://go.hotmart.com/Q34601203W?dp=1

Quando você inicia um treinamento, o professor (falo por mim) tenta te trazer o know-how de anos de pesquisa, meses de estudo e tentativas infindáveis 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.

Aqui cabe muito bem a celebre frase de Isaac Newton:

Se enxerguei mais longe, foi porque me apoiei em ombros de gigantes

E finalmente, concluo esse artigo deixando o meu novo treinamento sobre hardware hacking que compila meus últimos 9 anos pesquisando segurança, onde passei cerca de 2 anos testando, gravando e editando mais de 50 aulas. Um total de 14 horas de treinamento e uma quantidade obscena de dólares gastos em plaquinhas (quantidade essa que nunca será revelada à minha digníssima esposa).

Gostou do conteúdo? Quer se aprofundar mais nos estudos? Que tal conhecer o meu treinamento em Hardware Hacking, Iot Pentest e Red Team Gadgets?

https://go.hotmart.com/G35913582B