HARDWARE HACKING TOOLS

TODOS OS CRÉDITOS E FONTES SE ENCONTRAM AO FINAL.

ESTE CONTEÚDO FOI REUNIDO E TRADUZIDO (Tradução livre Inglês-Português) PELO PESQUISADOR DE SEGURANÇA FELIPE HIFRAM, ATUANTE NO CENTRO DE TREINAMENTO TECNOLÓGICO EXPERSEC.

INTRODUÇÃO

Embora você possa pensar que as ferramentas que os hackers usam são completamente ilegais, a maioria são ferramentas cotidianas de profissionais de segurança legítimos - apenas, você sabe, não sendo utilizados para o uso pretendido. Se você acha que os fabricantes desses produtos estavam piscando quando disseram que "uso pretendido" é inteiramente sua escolha.

O que isso significa é que existem vários dispositivos e dispositivos de hackers intrigantes disponíveis para sua leitura. Embora esteja avisado: não é fácil se tornar um hacker barato.

TOOLS

1. Keyllama 4MB USB Value Keylogger

O keylogger faz exatamente o que o nome sugere: registre todas as últimas atividades do teclado que está monitorando. Este é instalado de forma totalmente secreta - nenhum software pode detectá-lo - e pode gravar até um ano de digitação. Um alegado favorito de certos ex-estudantes empreendedores da Universidade de Iowa. (US $ 55,50, Amazon)

2. HackRF One

Um transmissor e receptor de rádio incrivelmente poderoso, é capaz de todos os tipos de manipulações descoladas. Pode até ser usado para destrancar portas de carros ... ou é o que nos dizem. ($ 317,95, Amazon)

3. Tomssmartcam Mini Câmera escondida USB

As câmeras secretas de espionagem estão na moda, e essa talvez seja a mais naturalmente compatível com hackers, pois parece - e é - um pen drive USB comum. Ele pode gravar em qualquer lugar por até duas horas e, em seguida, encaixar imediatamente no computador, vídeos prontos para serem vistos. Também funciona como um USB normal, caso alguém também precise que você transfira algumas planilhas ou algo assim. (US $ 39,99, Amazon)

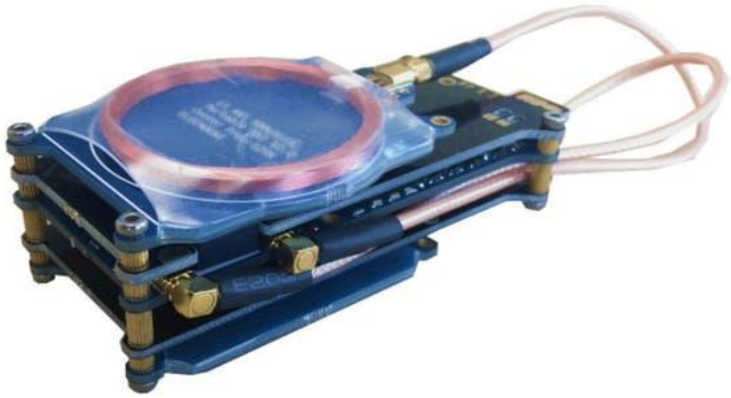
4. Gravador de espião digital EyeSpy

Ele literalmente se chama um bug. A coisa pode gravar por 140 horas com apenas o toque de um botão, apenas gravando quando as pessoas estão realmente falando. ($ 119, Amazon)

5. Adaptador de Rede Alfa

Se você já desejou invadir uma rede wifi, esse é um dos poucos adaptadores configurados com o objetivo de monitorar outras redes e enviar dados passivamente. Não que você queira invadir uma rede wifi. Você não deve fazer nada do que está nesta lista. Só para esclarecer. (US $ 32,99, Amazon)

6. Kit Proxmark 3



Este dispositivo pode ler e copiar tags RFID, que são usadas em todo o lugar como uma maneira de rastrear itens usando a frequência eletromagnética específica das tags. Copie essa assinatura e você poderá obter acesso a tudo o que essa tag tiver acesso. (US $ 325, Amazon)

7. Ubertooth One

Isso é capaz de monitorar e rastrear qualquer dispositivo bluetooth próximo. Isso teria sido ainda mais útil alguns anos atrás, quando os bluetooths pareciam ser o domínio exclusivo dos idiotas de negócios barulhentos que precisavam ficar de olho, mas ainda assim muito legais. ($ 127,95, Amazon)

8. Magspoof

Com este dispositivo, você pode copiar e armazenar todos os seus cartões de crédito e qualquer outra coisa com uma tarja magnética em um dispositivo, depois transmitir os dados desejados do cartão sem fio, sem precisar ter o plástico real com você. O site da Magspoof enfatiza que também não seria possível fazer isso com os cartões de crédito de outra pessoa, apenas para constar, mas provavelmente é melhor não apostar na empresa das pessoas. (US $ 75, Amazon)

9. Saco de Faraday das Trevas da Missão

Se apenas o simples ato de ler esta lista o deixou paranóico, agora você está em alguma outra lista em algum lugar, bem 1) como você acha que se sente depois de escrevê-la e 2) você pode considerar uma bolsa Faraday, cuja O revestimento foi projetado para impedir que todos os sinais cheguem a dispositivos eletrônicos dentro dele. Este é grande o suficiente para um laptop, embora modelos mais baratos sejam projetados apenas para telefones. (US $ 95, Amazon)

10. Raspberry Pi

É fácil ver o uso não nefasto do Raspberry Pi. É apenas um computador em miniatura e despojado - ele nem se importa com um gabinete, e muito menos com uma tela embutida! - destinado a ensinar às pessoas o básico da programação. Também é um bom centro de comando de computação portátil para todos os fins, não importa o que você esteja fazendo. Lá, isso é quase saudável! (US $ 69,99, Amazon)

11.USB Armory Bundle

O USB Armory Bundle é um computador discreto, do tamanho de uma unidade flash, seguro, de código aberto e ideal para desenvolver e executar uma variedade de aplicativos. Desenvolvedores e usuários comuns se beneficiam do rápido processador NXP i.MX53 deste dispositivo, recursos avançados de segurança como inicialização segura e integração com ARM® TrustZone®, ambiente operacional totalmente personalizável, suporte nativo excepcional e muito mais.

Com os recursos de sistema seguro em um chip (SoC) do arsenal USB e design aberto, este dispositivo fornece aos desenvolvedores e usuários uma plataforma confiável para criar e executar aplicativos de segurança pessoal, armazenar e criptografar dados automaticamente, gerenciar chaves e senhas digitais e executar uma variedade de outras tarefas orientadas à segurança. O arsenal USB pode até ser usado para acessar com segurança computadores remotos (através de uma VPN ou SSH), atuar como uma carteira eletrônica (para Bitcoin) ou servir como ponte para o Tor. (hackerwarehouse.com - $155)

12.CANtact Bundle

CANtact é uma interface de rede de área de controlador (CAN) de fonte aberta para USB do seu computador.

Ele pode ser usado para conectar-se a sistemas de barramento CAN, incluindo carros, veículos pesados e sistemas de automação industrial. O CANtact funciona no Linux, OS X e Windows.

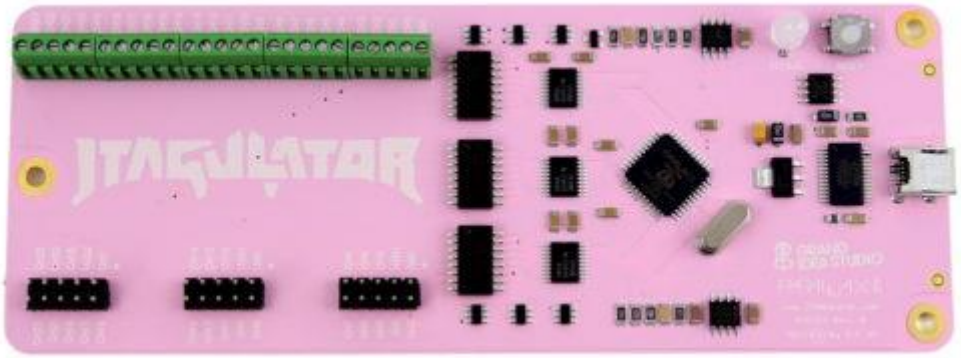
Wiki do CANtact

CANtactar arquivos de design de código aberto

CANtact firmware de código aberto

(hackerwarehouse.com - $76)

13.JTAGulator



O JTAGulator é uma ferramenta de hardware de código aberto que auxilia na identificação de conexões de depuração no chip (OCD) de pontos de teste, vias ou blocos de componentes em um dispositivo de destino.

Características principais:

24 canais de E / S com circuito de proteção de entrada

Tensão alvo ajustável: 1,2 V a 3,3 V

Interfaces de destino suportadas (a partir do firmware v1.1): JTAG / IEEE 1149.1, UART / serial assíncrona

*Interface USB para conexão direta ao computador host (PC, Macintosh ou * nix)*

Ideias de aplicação:

Descubra interfaces de depuração no chip

Analisador lógico simples

Placa de desenvolvimento da hélice

(hackerwarehouse.com - $170)

14. Bus Pirate

O Bus Pirate é uma ferramenta eletrônica universal de hardware aberto para programar e interagir com barramentos de comunicação e programar vários chips, como AVRs da Atmel e PICs da Microchip Technology. Um caso de uso primário para este dispositivo, conforme planejado pelos projetistas, é "Eliminar uma tonelada de esforços iniciais de prototipagem com chips novos ou desconhecidos". Usando um Bus Pirate, os desenvolvedores podem usar um terminal serial para fazer interface com dispositivos em uma variedade de protocolos de hardware , como SPI e 1-Wire.

Suporte para muitos protocolos seriais com níveis de linha de 0 a 5,5 volts:

1 fio

I^2C

JTAG

Serial assíncrono

MIDI

Teclado PC

HD44780 LCD

Bibliotecas de 2 e 3 fios com controle de pinos bit a bit

Modos de bitbang binário gravável, 1 fio, I2C, SPI e UART

Outros recursos:

Sonda de medição de 0 - 6 volts

Medição de frequência de 1 Hz - 40 MHz

Modulador de largura de pulso de 1 kHz - 4 MHz, gerador de frequência

Resistores de pull-up multivoltagem a bordo

Fontes de alimentação integradas de 3,3 volts e 5 volts com redefinição de software

Macros para operações comuns

Farejadores de tráfego de ônibus (SPI, I²C)

Um gerenciador de inicialização para atualizações fáceis de firmware

USB transparente -> modo serial

Analisador lógico de baixa velocidade compatível com SUMP de 10 Hz - 1 MHz

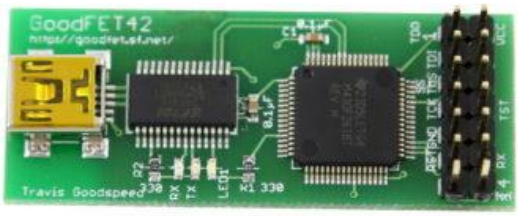
Clone do programador AVR STK500 v2

Suportado no programador AVRDude

Scriptable de Perl, Python, etc.

(hackerwarehouse - $50)

15.GoodFET42



O GoodFET é um adaptador JTAG de código aberto e um adaptador de barramento serial universal.

Ele suporta a comunicação com dispositivos embarcados e circuitos integrados através de vários protocolos diferentes, incluindo várias versões padrão e de propriedade do fornecedor do SPI e JTAG. A comunicação do lado do cliente é feita usando uma biblioteca Python, e os clientes pré-gravados para funções comuns (dumping flash, etc.) já estão gravados. Além disso, os usuários podem estender a base de código para oferecer suporte a protocolos adicionais. (hackerwarehouse.com - $50)

16.Facedancer21

O Facedancer é um emulador e fuzzer USB de código aberto.

Diferentemente das placas GoodFET de uso geral, o único objetivo desta placa é permitir que os dispositivos USB sejam gravados no Python do host, para que uma estação de trabalho possa testar os drivers de dispositivo USB de outro host. ($100)

17.Black Magic Probe v2.1

O Black Magic Probe foi projetado pelo 1BitSquared em colaboração com a Black Sphere Technologies e é um adaptador JTAG e SWD usado para programar e depurar MCUs ARM Cortex.

É o melhor amigo de qualquer desenvolvedor de microcontrolador ARM, pois se livra de programas intermediários como o OpenOCD ou o servidor STLink. Isso torna a operação mais rápida e confiável. Você acabou de abrir seu GNU Debugger (GDB) e selecionar a porta virtual oferecida pelo BMP como seu destino remoto estendido. ($75)

Recursos:

Porta do servidor GDB sem a necessidade de software especial do lado do PC.

Interface serial de nível TTL - Suporte SWD e JTAG

Suporta alvos de 1,7V até 5V - Pode fornecer 3.3V para o alvo (até 100mA)

Suporte de semi-hospedagem - Funciona em Linux, Mac e Windows

Funciona com o Eclipse e outros ambientes de desenvolvimento integrado - Suporta STM32, LPC11, LM3S

Compatível com DroneCode - Vem / w Cabo de interface serial, placa de expansão de adaptador JTAG de 7 pinos (não montada)

18.USB Killer Pro Kit v3

O dispositivo USB Killer é um dispositivo USB ESD Testing aprovado pela CE e pela FCC, projetado para testar o circuito de proteção contra sobretensão dos eletrônicos até seus limites - e além.

Ame ou odeie, o USB Killer estabeleceu-se firmemente como uma realidade que os projetistas de hardware não têm escolha a não ser reconhecer. Para testadores de caneta, ele abre um novo vetor de ataques. Para LEA, um novo meio de manipulação de alvo. Para engenheiros de hardware e indústria, uma ferramenta com a qual eles podem proteger seus produtos.

O V3 foi reconstruído do zero para ser mais capaz, portátil e estável. Em conjunto com o kit testador e adaptador, o USB Killer é indispensável para os pentesters de hardware.

Inclui: USB Killer, Shield de teste para realizar testes com segurança, kit adaptador (USB-C, Lightning, Micro USB).

(hackerwerahouse.com - $90)

19.GreatFET One

O GreatFET One é o melhor amigo de um hacker de hardware. Com um design extensível de código aberto, duas portas USB e 100 pinos de expansão, o GreatFET One é o seu gadget essencial para hackers, fabricação e engenharia reversa. Ao adicionar placas de expansão chamadas vizinhas, você pode transformar o GreatFET One em um periférico USB que faz quase tudo.

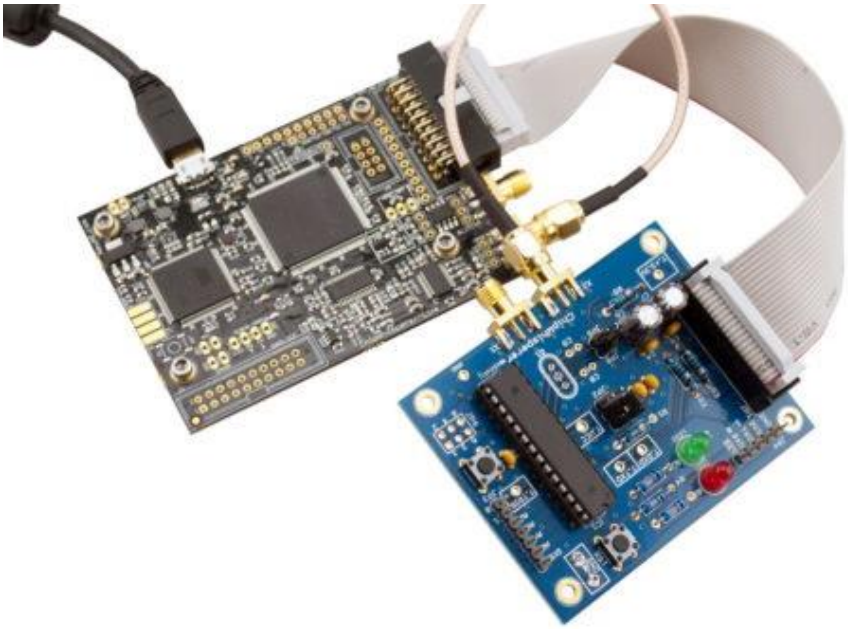
Se você precisa de uma interface para um chip externo, um analisador lógico, um depurador ou apenas um monte de pinos para conectar, o versátil GreatFET One é a ferramenta para você. O USB de alta velocidade e uma API Python permitem que o GreatFET One se torne sua interface USB personalizada para o mundo físico.

E / S digital programável - protocolos seriais, incluindo SPI, I2C, UART e JTAG - análise lógica - E / S analógica (ADC / DAC)

aquisição de dados – depuração

- funções USB versáteis, incluindo FaceDancer - mecanismo serial de streaming assistido por hardware de alto rendimento - quatro fabulosos LEDs! (hackerwarehouse.com - $90)

20. Chipwhisperer



Ferramenta de pesquisa de segurança de hardware incorporado

Análise de potência de canal lateral e recursos de falha

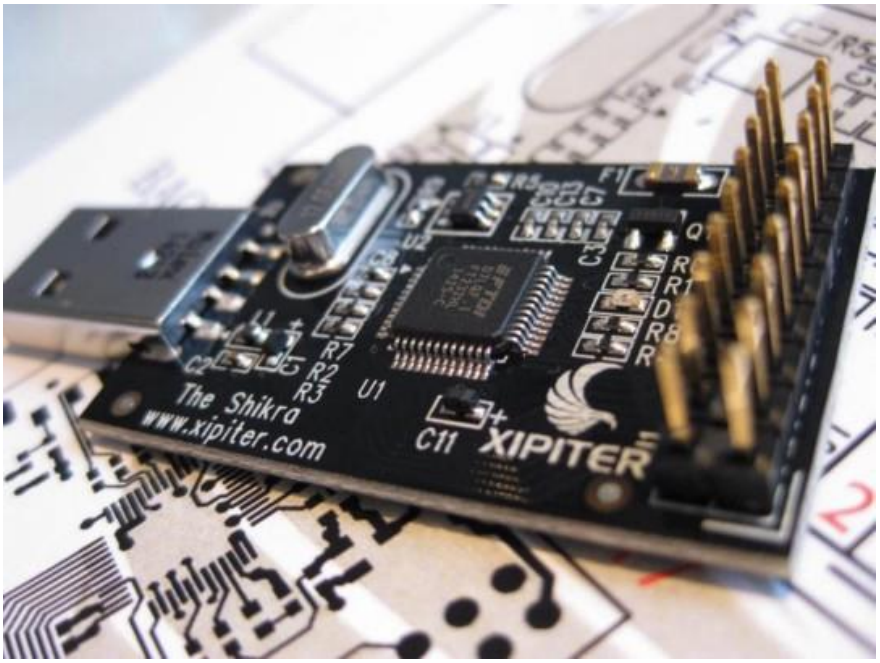
Cadeia de ferramentas de código aberto (licenciada GPL)

Breaker Addon + NOTDuino Target Board:

Inclui os cabos extras necessários ao desmontar o seu ChipWhisperer-Lite.

NOTDuino é um alvo de falha e análise de canal lateral baseado no Atmel AVR.

21.Sikra



Este dispositivo é apresentado como uma ferramenta mais estável em comparação com o Bus Pirate. O hardware é muito confiável e estável para conectar-se ao UART, JTAG e SPI. Muitas pessoas na comunidade de Exploração de software por meio de exploração de hardware gostam muito de usar esse dispositivo um pouco menos conhecido e são usadas no treinamento do SEXviaHEX.

Se você deseja extrair a imagem do firmware de um dispositivo IoT de destino para exploração de software, o Shikra é uma ótima ferramenta para o trabalho. Basta conectar o Shikra ao chip SPI do dispositivo de destino. Pode ser necessário um clipe SOIC de 8 pinos para conectar o Shikra à interface SPI.

Bus Pirate levou 30 minutos para despejar uma imagem de firmware de 4 MB de um dispositivo, em comparação com pouco menos de um minuto para o Shikra fazer o mesmo trabalho. O Shikra pode ser algo com o qual menos pessoas estão familiarizadas, mas fornece desempenho consistente, poderoso e rápido para determinados trabalhos.

CRÉDITOS/FONTES:

FONTE 1: https://www.hackerwarehouse.com

MINHAS REDES SOCIAIS:

Facebook: https://www.facebook.com/hiframfelipe

LinkedIn: https://www.linkedin.com/in/felipe-hifram-946349168

Email: lipehifram@expersec.com

SERVIÇOS

(Centro de Treinamento Tecnológico Expersec)

Facebook: https://www.facebook.com/cttexpersec

LinkedIn: https://www.linkedin.com/company/experience-security/