

Segurança Ofensiva com Raspberry Pi



Lucas Albano

Agenda

- Objetivos
- Segurança Ofensiva
- Raspberry Pi
- WiFi Cracking
- Ataque Man-in-the-Middle (ARP Spoofing)
- Botnets e Ataques DDoS

Objetivos

- Conceitos básicos de Segurança Ofensiva
- Apresentar o Raspberry Pi e casos de uso
- Demonstração de ataques com Raspberry Pi
 - WiFi Cracking
 - Mapeamento de Rede
 - Man-in-the-Middle (MITM)
 - Construção de Botnet e Ataque DDoS
- Conscientizar sobre ameaças cibernéticas atuais

Cibersegurança Ofensiva

“A prática de explorar vulnerabilidades e simular ataques para identificar e corrigir falhas de segurança antes que sejam exploradas por agentes mal-intencionados.”

Áreas de Atuação



Pentest
(Teste de Intrusão)



Red Team

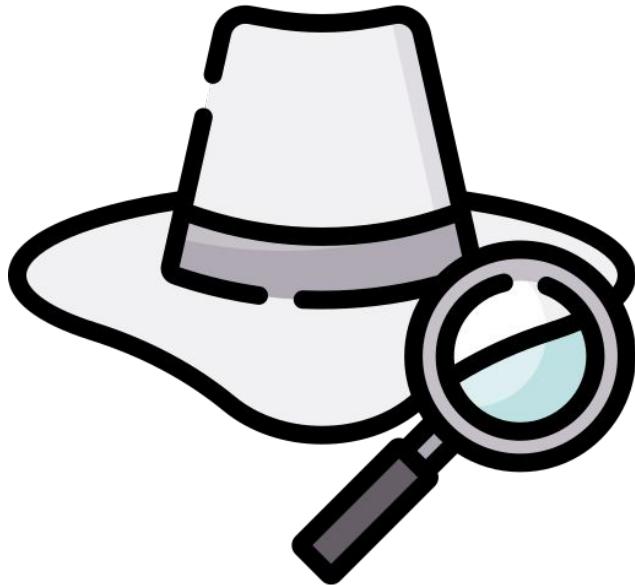


Bug Bounty



Engenharia Social e
Testes de Phishing

Tipos de Hacker



White Hat

Hackers que utilizam suas habilidades para proteger sistemas, realizar testes de penetração e ajudar organizações a melhorar sua segurança

Tipos de Hacker



Black Hat

Hackers mal-intencionados que exploram vulnerabilidades para ganho pessoal, praticando atividades ilegais como roubo de dados e extorsão

Tipos de Hacker



Grey Hat

Hackers que exploram falhas sem permissão, mas não para ganho pessoal. Geralmente expõem vulnerabilidades para conscientizar e, às vezes, para recompensas

Tipos de Hacker



Script Kiddie

Iniciantes que usam ferramentas e scripts prontos, sem profundo conhecimento técnico, para realizar ataques básicos e ganhar notoriedade

Tipos de Hacker



Hacktivista

Hackers que conduzem ataques para promover causas políticas ou sociais, visando influenciar a opinião pública e governos

Raspberry Pi



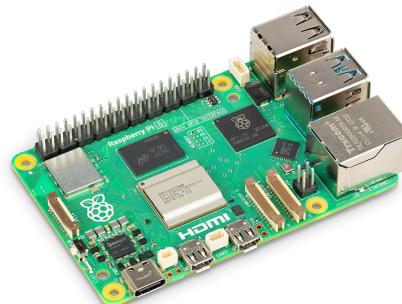


Raspberry Pi

Mini-computador de placa única desenvolvido pela Fundação Raspberry Pi, com sede no Reino Unido

Iniciou seu desenvolvimento (Model A) em 29 de fevereiro de 2012

- Objetivo da fundação:
 - Criar um computador acessível e de baixo custo (A partir de \$35)
 - Promover o ensino de Ciência da Computação básica em escolas
 - Inclusão digital



Modelos



Pi A+



Pi Zero W



Pi 3 B+



Pi 4B



Pi 5



Pi 400

Valores Atuais



Raspberry Pi 5 2GB

R\$ 609,90

3X R\$ 203,30 sem juros

R\$ 579,40 no PIX



Raspberry Pi 5 4GB

R\$ 705,90

3X R\$ 235,30 sem juros

R\$ 670,60 no PIX



Raspberry Pi 5 8GB

R\$ 1.019,00

3X R\$ 339,67 sem juros

R\$ 968,05 no PIX



Raspberry Pi 3 - Model B+
Anatel

R\$ 405,90

3X R\$ 135,30 sem juros

R\$ 385,60 no PIX



Raspberry Pi 4 2GB - Model B
Anatel

R\$ 579,00

3X R\$ 193,00 sem juros

R\$ 550,05 no PIX



Raspberry Pi 4 4GB - Model B
Anatel

R\$ 659,90

3X R\$ 219,97 sem juros

R\$ 626,90 no PIX



Raspberry Pi 4 8GB - Model B
Anatel

R\$ 919,90

3X R\$ 306,63 sem juros

R\$ 873,90 no PIX



Raspberry Pi Pico 2

R\$ 49,40

3X R\$ 16,47 sem juros

R\$ 46,93 no PIX



Raspberry Pi 4 1GB - Model B
Anatel

R\$ 449,90

3X R\$ 149,97 sem juros

R\$ 427,40 no PIX



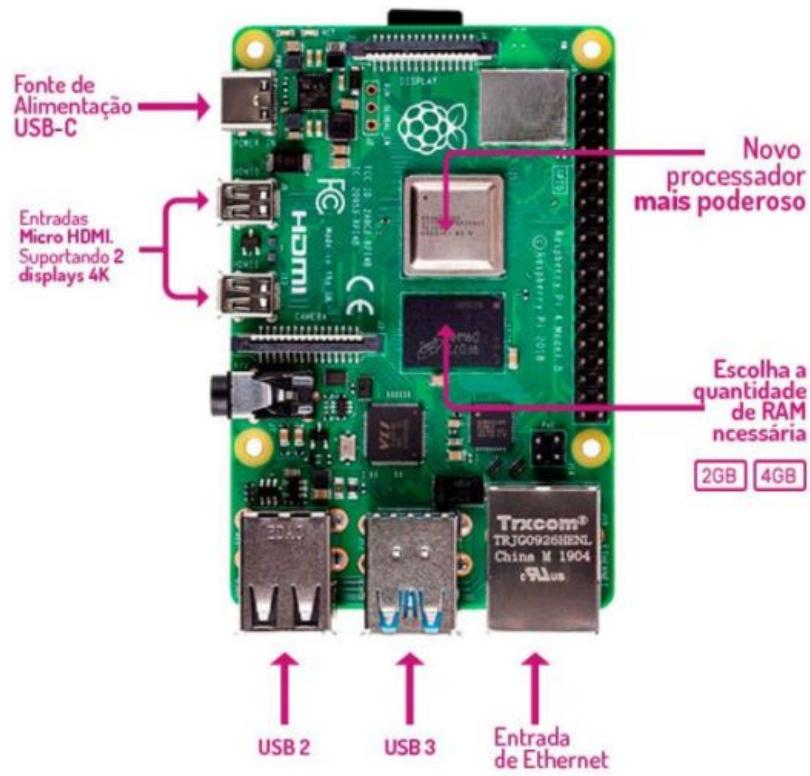
Raspberry Pi 400 PT ANATEL

R\$ 749,90

3X R\$ 249,97 sem juros

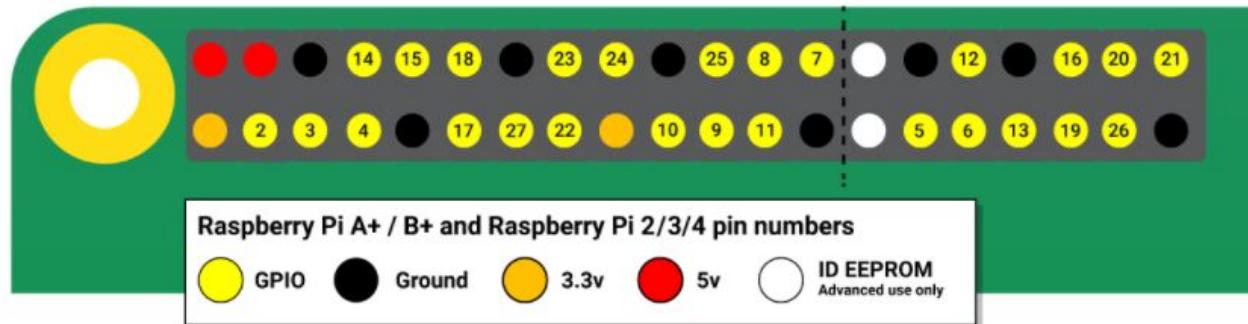
R\$ 712,40 no PIX

- Processador Broadcom 2711 Quad-core **Cortex-A72** 64-bit **1,5 GHz**
- **1GB / 2GB / 4GB / 8GB de memória RAM**
- GPU Broadcom VideoCore IV @ 250 MHz
- WiFi 2,4 GHz / 5,0 GHz IEEE 802.11.b/g/n/ac
- Bluetooth 5.0
- 2 portas USB 2.0
- 2 portas USB 3.0
- True Gigabit Ethernet over USB 3.0
- **GPIO com 40 pinos**
- 2 portas micro HDMI, **vídeo de 4k**
- Interface para display (DSI)
- Interface para câmera (CSI)
- Conector P2 para saída de áudio e vídeo
- Slot para cartão micro SD
- Alimentação 5V / 3A via **conector USB tipo C**



GPIO - General Purpose Input/Output

- Portas programáveis de entrada e saída de dados
- Utilizadas para prover uma interface entre os periféricos e os microcontroladores/microprocessadores
- PWM (modulação de largura de pulso)
- SPI
- I2C
- Serial



Sistemas Operacionais

01 - **Raspberry Pi OS (oficial)**

02 - Ubuntu

03 - Fedora

04 - Manjaro

05 - **Kali Linux**

06 - DietPi

07 - Kano OS (para crianças)

08 - Firefox OS

09 - Chromium OS

10 - Batocera (retro-gaming)

11 - RecalBox (retro-gaming)

12 - Retropie (retro-gaming)

13 - LibreELEC (Kodi)

14 - OSMC (Open Source Media Center)

15 - OpenMediaVault

16 - Android 12L (ROM customizada)

17 -  Windows 10 IoT

18 - ROKOS (mineração)

Raspberry Pi OS

- Recomendado para uso normal
- Gratuito
- Baseado no **Debian**
- Otimizado para o hardware
- Possui mais de 35.000 pacotes
- Desenvolvimento constante
 - Ênfase em melhorar a estabilidade e o desempenho dos pacotes Debian no Raspberry Pi



Kali Linux

- Distribuição Linux focada em **Cibersegurança**
- Diversas ferramentas de hacking pré-instaladas
- Não recomendado para uso como sistema operacional convencional
- Grande vantagem: **Portabilidade**



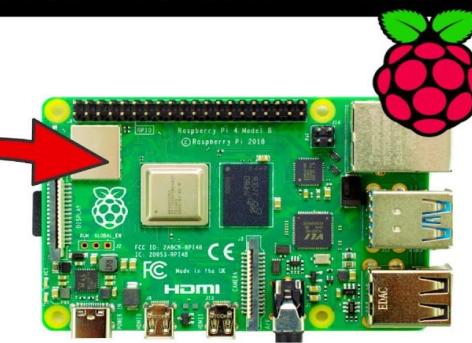
Aplicações do Raspberry Pi

- Servidor Web

LAMP Web Server



WordPress



Aplicações do Raspberry Pi

- Servidor Web
- Streaming Doméstico



Aplicações do Raspberry Pi

- Servidor Web
- Streaming Doméstico
- Emulação de Games



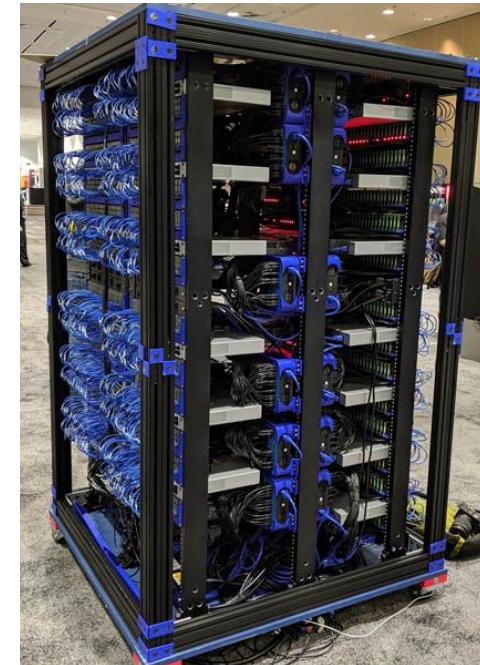
Aplicações do Raspberry Pi

- Servidor Web
- Streaming Doméstico
- Emulação de Games
- Mineração de Criptomoedas



Aplicações do Raspberry Pi

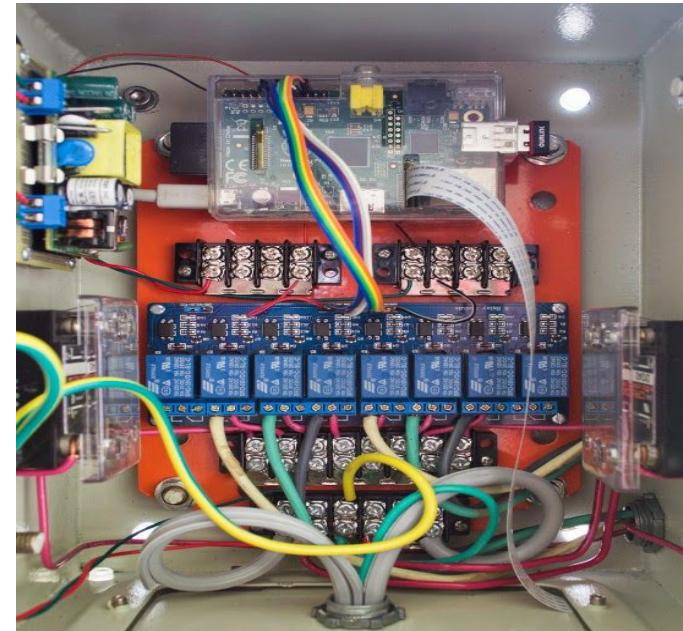
- Servidor Web
- Streaming Doméstico
- Emulação de Games
- Mineração de Criptomoedas
- Supercomputação



Cluster da Oracle com 1.060 Raspberry Pi 3B+ e 4240 núcleos

Aplicações do Raspberry Pi

- Servidor Web
- Streaming Doméstico
- Emulação de Games
- Mineração de Criptomoedas
- Supercomputação
- Automação

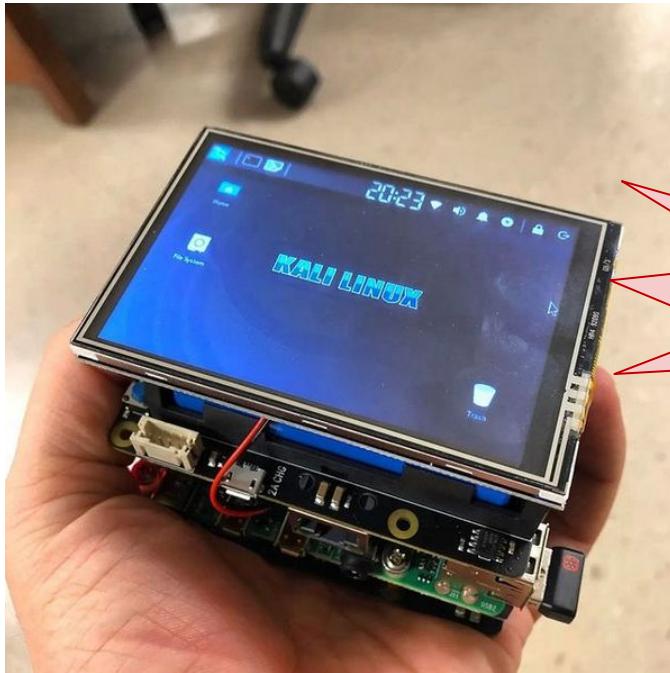


Aplicações do Raspberry Pi

- Servidor Web
- Streaming Doméstico
- Emulação de Games
- Mineração de Criptomoedas
- Supercomputação
- Automação
- Bloqueador de Anúncios



Raspberry Pi em Hacking



HACKING

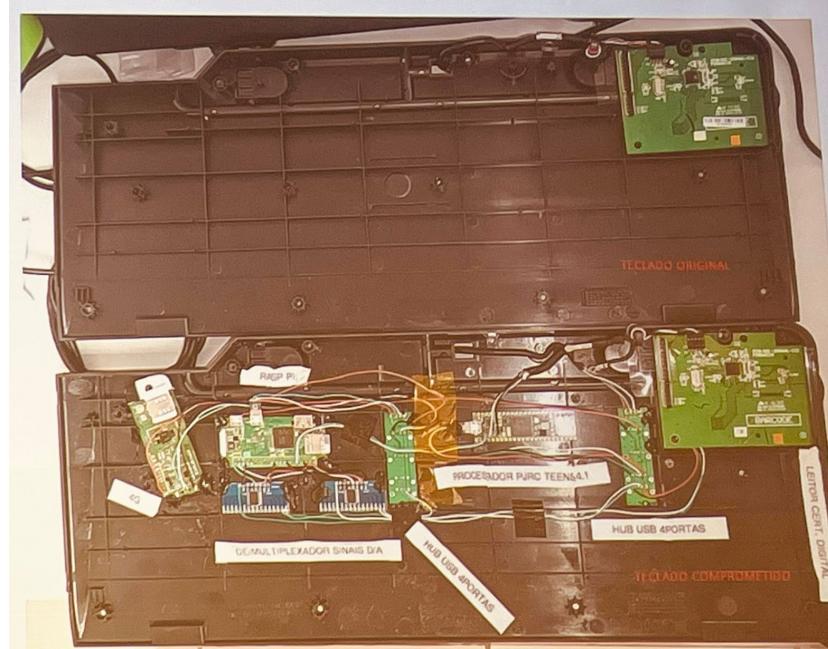


Ocorrências Recentes

Teclado implantado em uma unidade da CAIXA por um terceirizado. O responsável foi preso em operação da PF

Na imagem, um teclado comum (acima) e o teclado modificado (abaixo). Externamente, não há diferença, mas internamente:

- **Raspberry Pi**: mini-computador programado para registrar tudo o que era digitado
- Modem 4G: enviava as informações capturadas para o atacante pela internet
- Unidade de Armazenamento: guarda os dados para serem acessados depois
- Leitor de Certificado Digital: acessa informações de certificados digitais



Ocorrências Recentes

Home > Ataque hacker

Grupo usava Raspberry Pi para hackear caixas eletrônicos e roubar dinheiro

07/09/2023 às 13:30 • 1 min de leitura



Imagem: Getty Images/Reprodução

Ocorrências Recentes

Nasa foi hackeada por computador de US\$ 35 normalmente usado por crianças

Ataque durou quase um ano e agência foi obrigada a desligar sistemas de controle de voos espaciais do centro afetado pelo invasor de sistema



Hackers: invadiram sistema da Nasa (Pixabay/Reprodução)

Dispositivos Raspberry Pi com senha 'padrão' são alvos de ataque

18/03/2022 às 16:00 • 1 min de leitura



 Adriano Camacho
via nexperts

Utilizando um Raspberry Pi na Prática

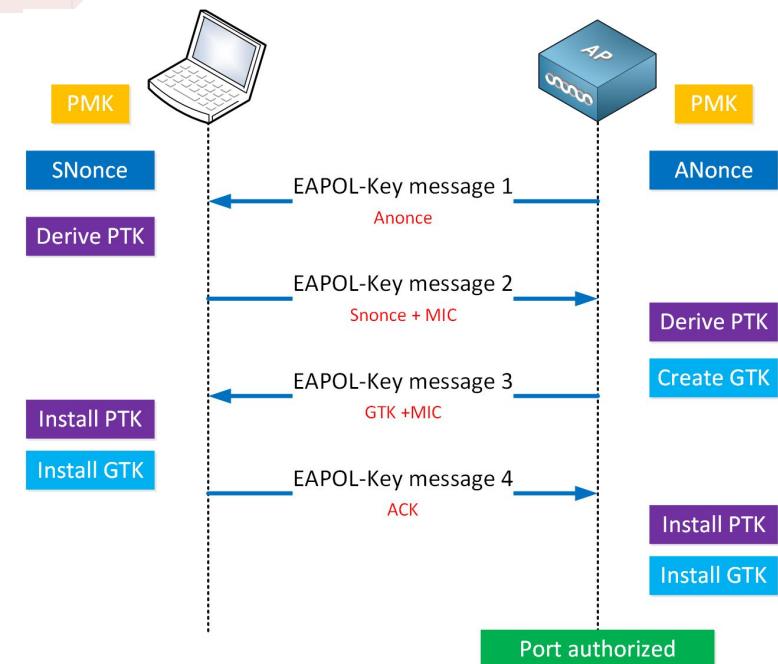


WiFi WPA2 Cracking

- **Wi-Fi Protected Access 2 (WPA2)** é um protocolo de segurança para redes WiFi desenvolvido para corrigir falhas do WPA
- Criptografia AES (Advanced Encryption Standard) para proteger os dados transmitidos pela rede e autenticar os dispositivos conectados
- No entanto, o WPA2, embora seguro, não é totalmente imune a ataques, especialmente quando são usadas senhas fracas

WPA2 4-way Handshake

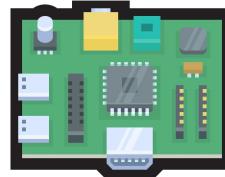
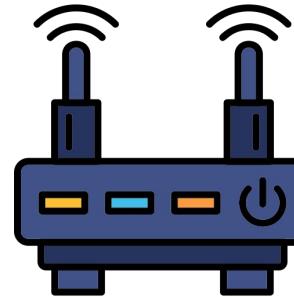
- Para se conectar a uma rede WiFi WPA2, é necessário realizar uma autenticação de handshake de 4 vias
- Esse handshake é uma troca de pacotes entre o dispositivo (cliente) e o roteador para confirmar a identidade e estabelecer uma conexão segura
- O roteador e o cliente trocam informações criptografadas, incluindo dados que comprovam o conhecimento da chave (senha) da rede.

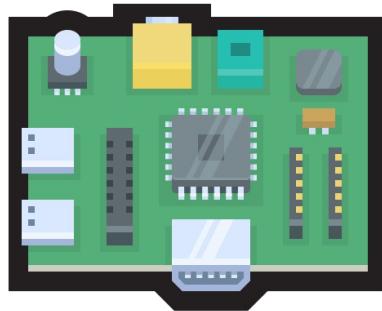


Brute Force

- Testa todas as combinações possíveis de caracteres para descobrir a senha
 - Lento e computacionalmente caro, especialmente se a senha for longa e complexa
- **Dictionary Attack:** utiliza uma lista predefinida de senhas para tentar quebrar a segurança da rede.
 - Mais rápido, porém depende de o atacante possuir uma lista que contenha a senha ou uma senha similar

WiFi WPA2 Cracking





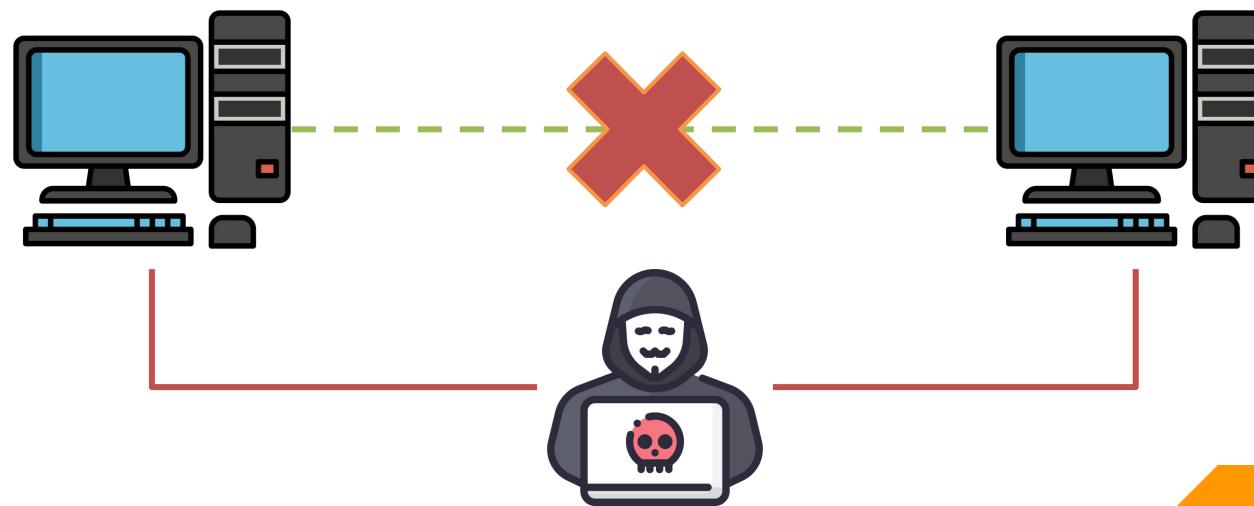
Handshake Capturado



Brute Force

Man-in-the-Middle (MITM)

Um ataque em que o invasor se posiciona entre duas partes em comunicação, interceptando e possivelmente alterando as mensagens entre elas sem que saibam



ARP Spoofing

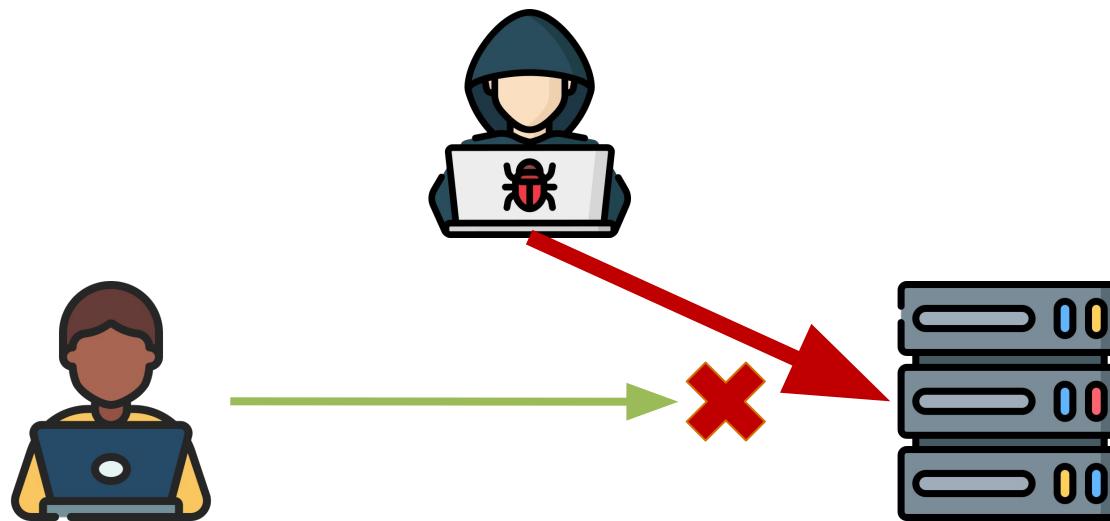
- **Protocolo ARP (Address Resolution Protocol):** Protocolo que mapeia endereços IP para endereços MAC em redes locais, permitindo que dispositivos se comuniquem
- **ARP Spoofing:** Técnica de ataque que envia mensagens ARP falsificadas na rede, associando o endereço IP de um alvo ao endereço MAC do atacante, permitindo interceptar o tráfego

Botnets

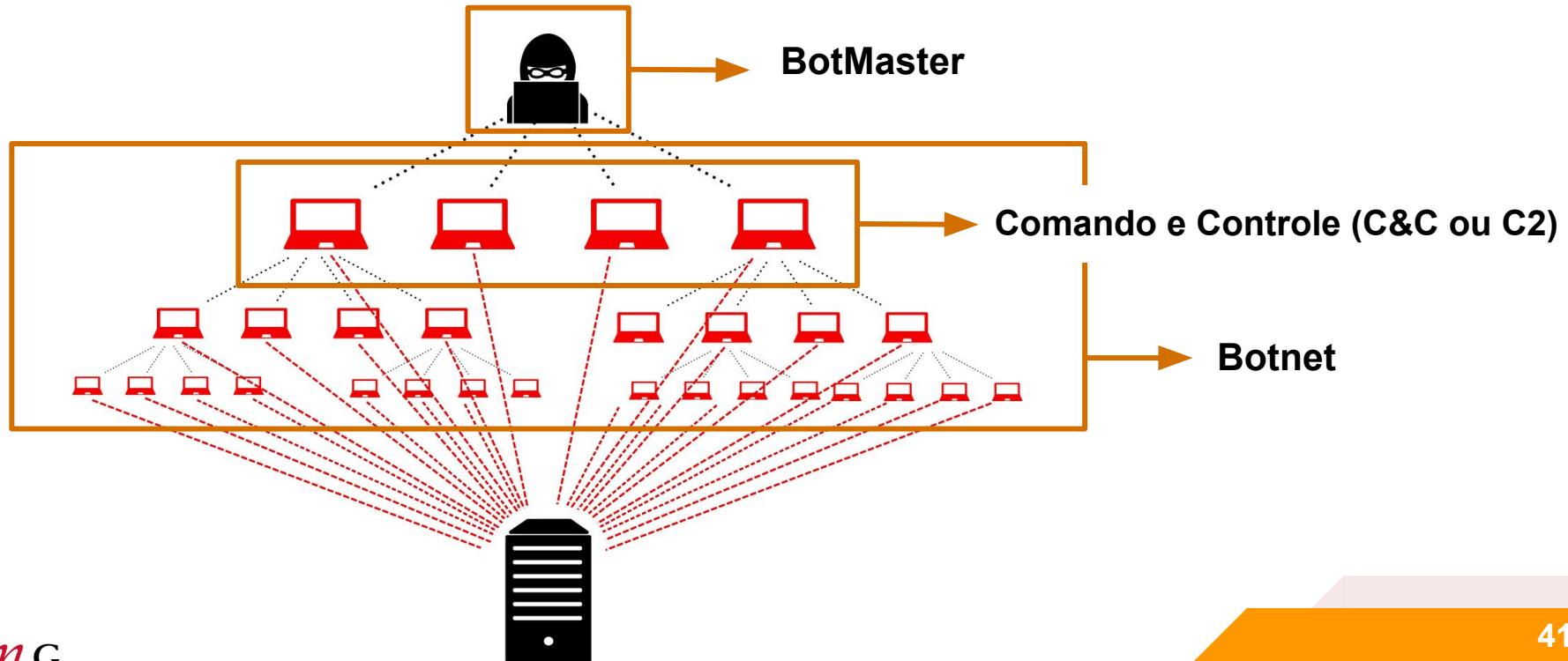
- **Botnets** são redes de dispositivos comprometidos, chamados de "bots" ou "zumbis", que foram infectados com malware e estão sob o controle de um invasor (também chamado de "botmaster")
- Esses dispositivos podem incluir computadores, smartphones, roteadores e outros dispositivos IoT conectados à internet
- O botmaster pode coordenar esses dispositivos para realizar atividades maliciosas em grande escala

O que é Negação de Serviço (DoS)

Definição: Impedir o acesso de um usuário a um recurso ou serviço



Negação de Serviço Distribuído (DDoS)



Dispositivos Infectados pela Mirai

Inside the infamous Mirai IoT Botnet: A Retrospective Analysis

2017-12-14

What's remarkable about these record-breaking attacks is they were carried out via small, innocuous Internet-of-Things (IoT) devices like home routers, air-quality monitors, and personal surveillance cameras. At its peak, Mirai infected over 600,000 vulnerable IoT devices, according to our measurements.

```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10); // root xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9); // root vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8); // root admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7); // admin admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6); // root 888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5); // root xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5); // root default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5); // root juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5); // root 123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5); // root 54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5); // support support
add_auth_entry("\x50\x4D\x4D\x56", "", 4); // root (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4); // admin password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4); // root root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4); // root 12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3); // user user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3); // admin (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3); // root pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3); // admin admin1234
```



lucasalbano@dcc.ufmg.br



Lucas Albano

Sistemas de Informação |
Cibersegurança | ML | Python | C...



LinkedIn

Obrigado!

