Pitch

PROJETO APLICADO

MSIS - Um *software* aplicável a verificação de informações de portas e versões sistêmicas de dispositivos de Internet das coisas (IoT) utilizando redes *Ethernet* e Wi-FI

Sumário

01.

APRESENTAÇÃO

Quem sou eu?

02.

PROBLEMA

Qual é a dor?

03.

SOLUÇÃO

O que eu proponho?

04.

DIFERENCIAL

O que a sua solução tem de especial?

05.

ARQUITETURA

Quais são os impactos da minha solução?

01.

Apresentação

Quem sou eu?

Júnior André Marostega, graduado em Ciência da Computação, Mestre em Computação Aplicada e cursando Pós Graduação em Segurança Cibernética. 13 anos no mercado de trabalho atuando em Tecnologia da Informação. Atualmente sou pesquisador, palestrante e consultor e também Gerente de T.I da RICOHPEL Soluções Corporativas. Um apaixonado por segurança da informação, IoT (Internet das coisas), automação, robótica e negócios.

02.
Problema

Qual é a dor?

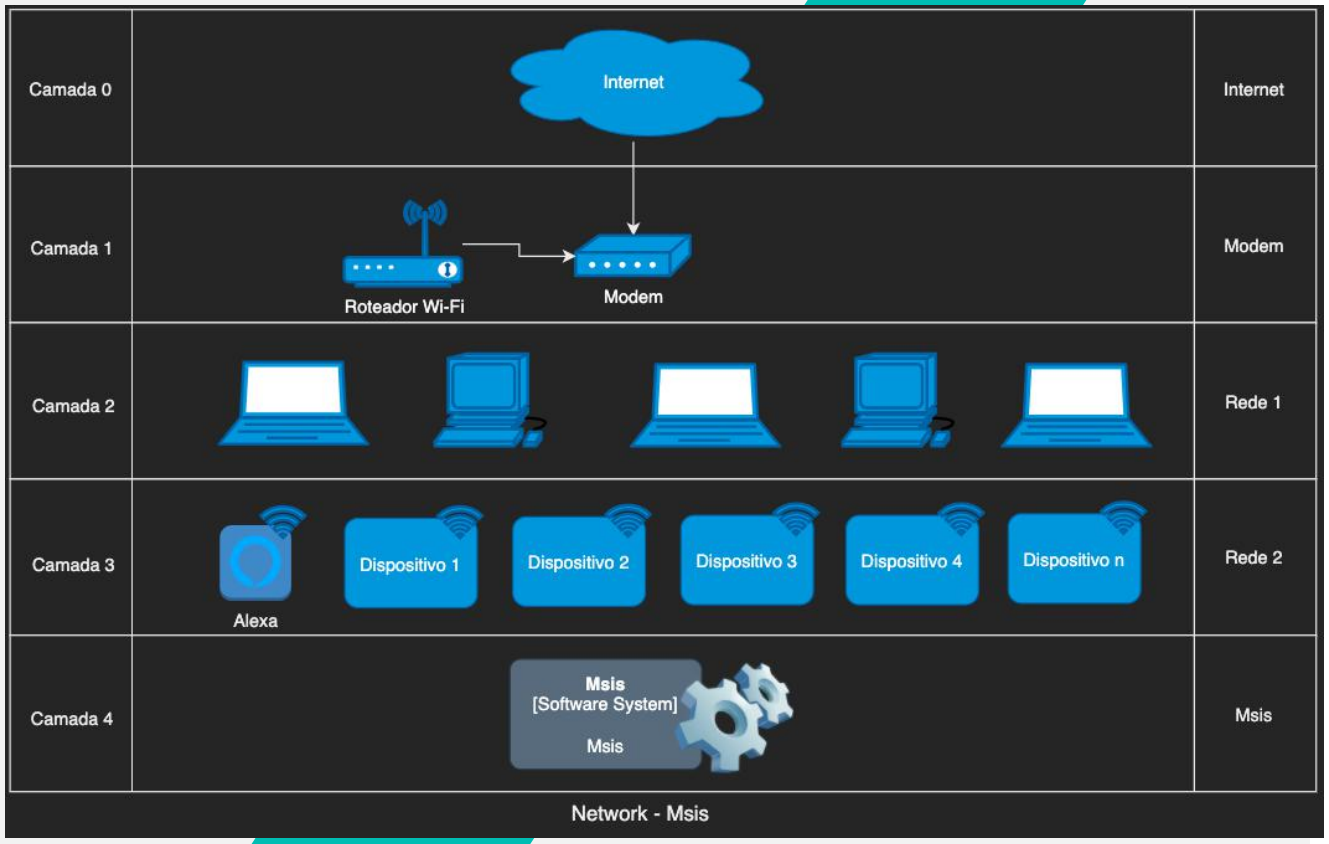
Dispositivos de IoT (internet das coisas) estão a cada dia mais presentes em ambientes educacionais, dómesticos e corporativos. A falta de padronização em arquiteturas, protocolos e tecnologia afeta muitas vezes o conhecimento em manusear / implantar e monitorar estes, como resultado, os dispostivos são portas de entradas para o desenvolvimento de ataques a determinados ambientes.

03.

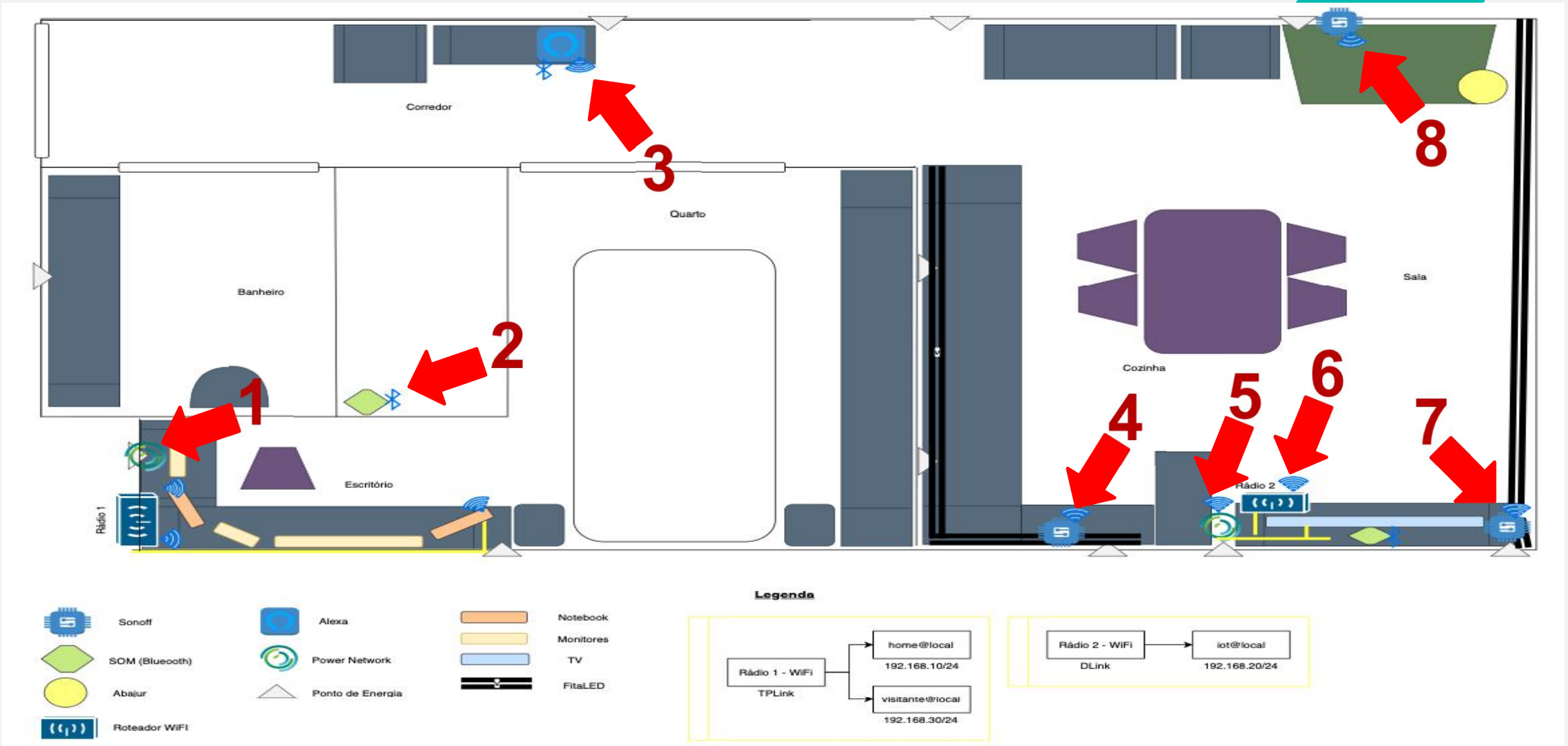
Solução

O que eu proponho?

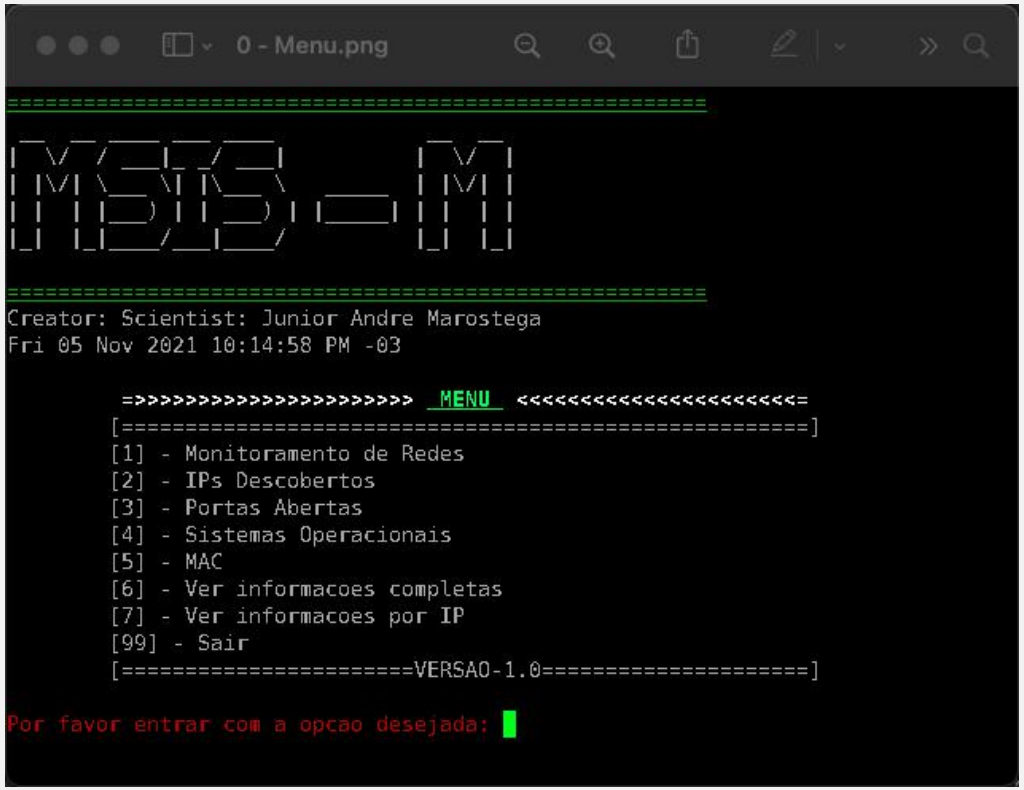
O desenvolvimento de um *software* que vai atuar na varredura de determinada rede para identificar informações básicas de configurações com IPs, Portas e dados de *Firmwares/S.O* dos dispositivos conectados na rede. Informações que dado ambiente pode ser explorada por atacantes.

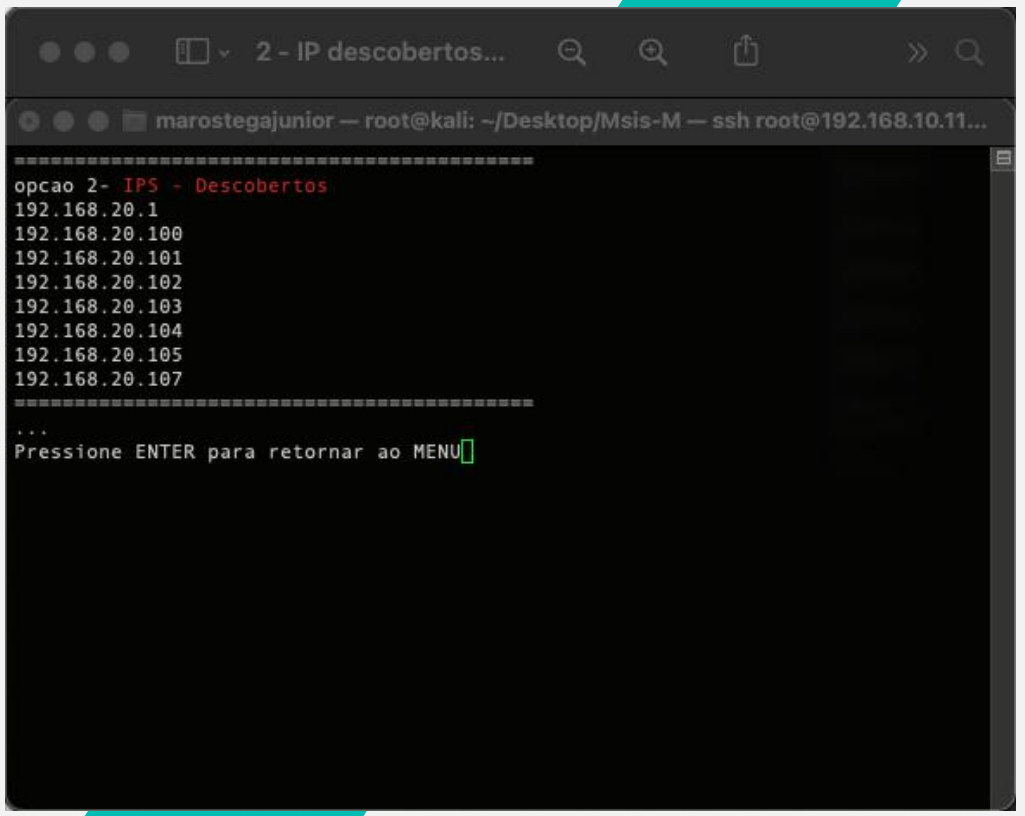


Ambiente de Testes



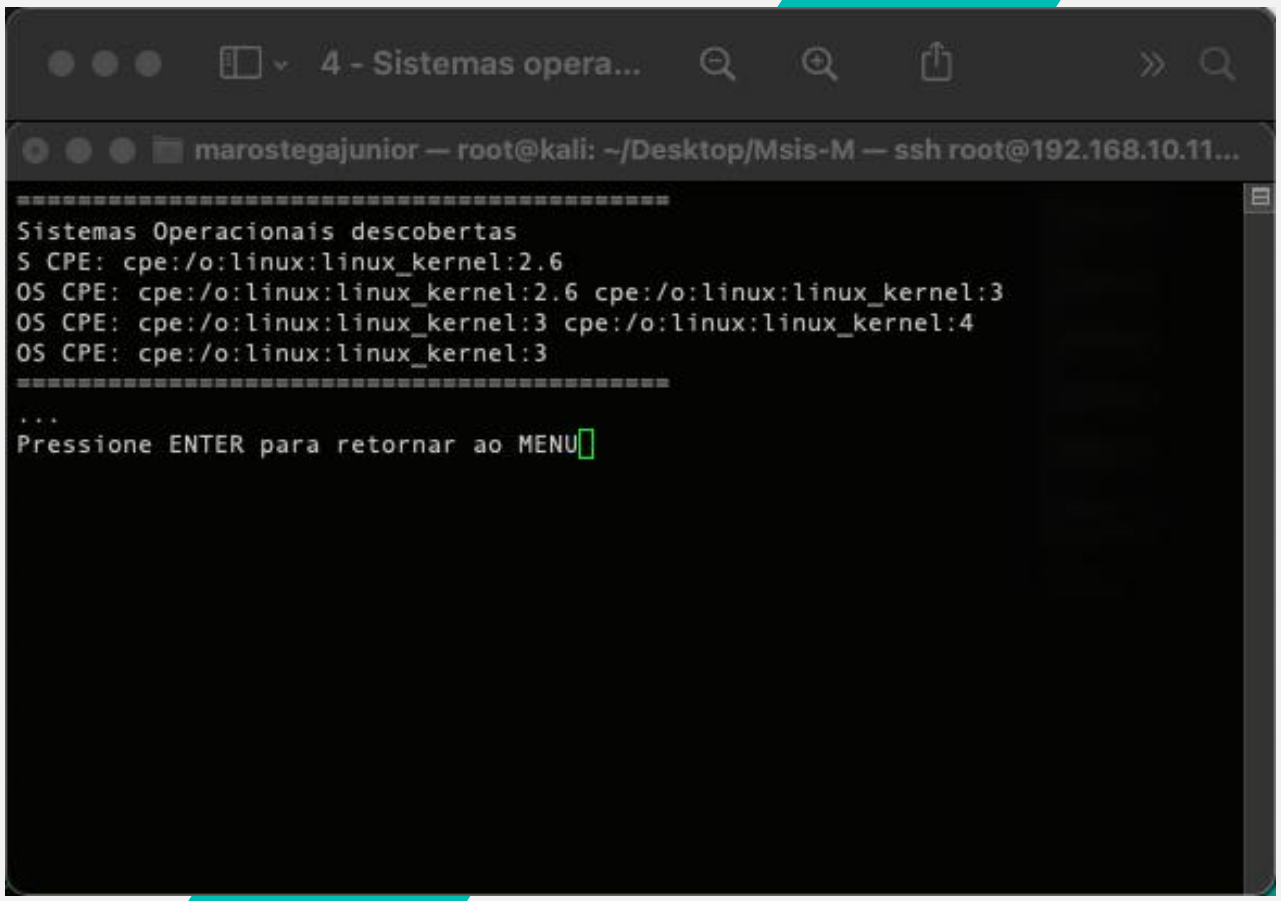
Modelo


0 - Menu.png
Creator: Scientist: Junior Andre Marostega
Fri 05 Nov 2021 10:14:58 PM -03
MENU
[1] - Monitoramento de Redes
[2] - IPs Descobertos
[3] - Portas Abertas
[4] - Sistemas Operacionais
[5] - MAC
[6] - Ver informacoes completas
[7] - Ver informacoes por IP
[99] - Sair
VERSAO-1.0
Por favor entrar com a opcao desejada:

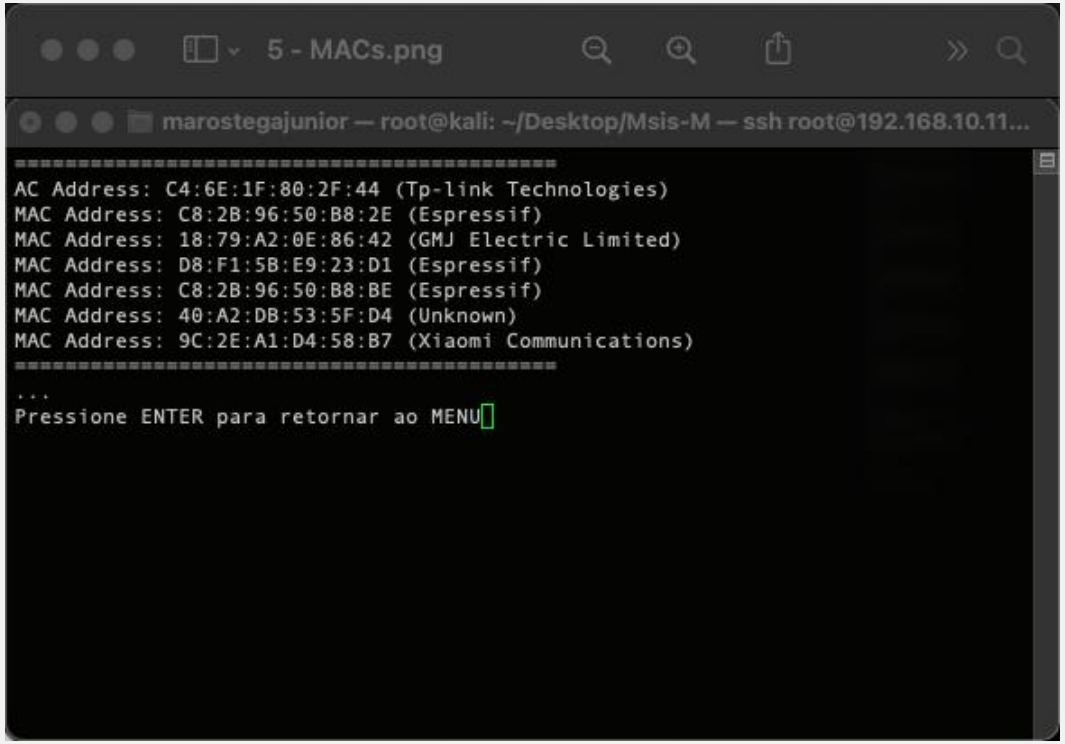

2 - IP descobertos...
marostegajunior — root@kali: ~/Desktop/Msis-M — ssh root@192.168.10.11...
opcao 2- IPS - Descobertos
192.168.20.1
192.168.20.100
192.168.20.101
192.168.20.102
192.168.20.103
192.168.20.104
192.168.20.105
192.168.20.107
...
Pressione ENTER para retornar ao MENU

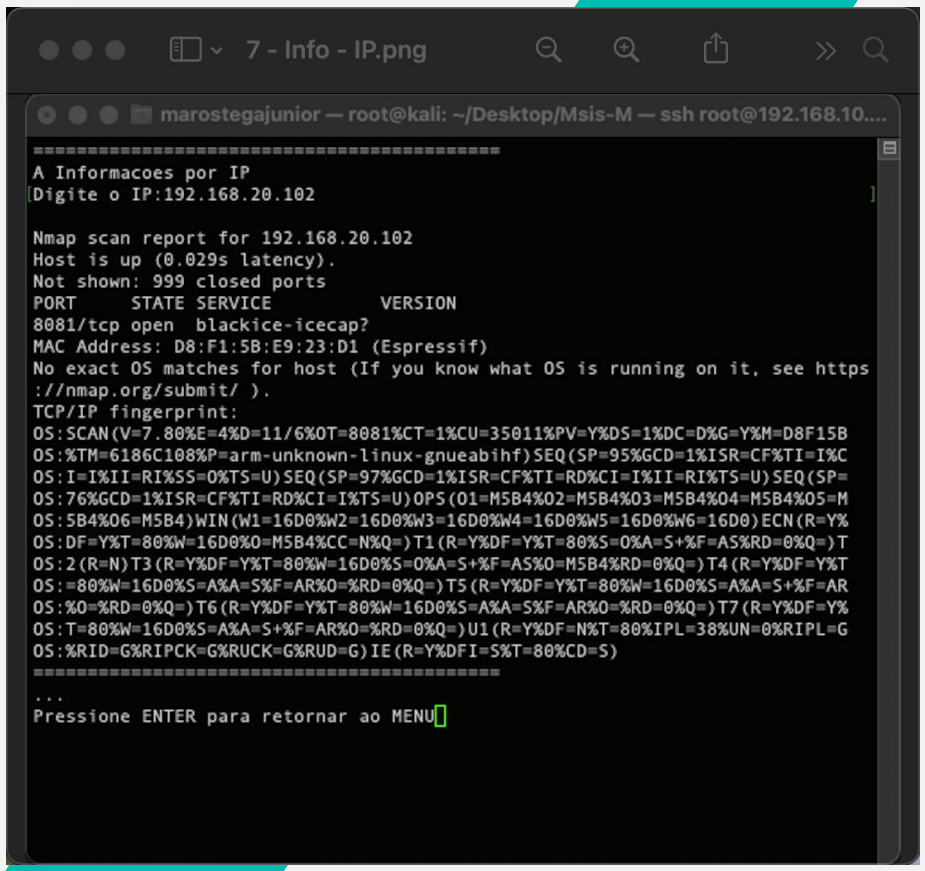
Modelo

```
0/tcp   open  http    TP-LINK WR741ND WAP http config
1900/tcp open  upnp    ipOS upnpd (TP-LINK TL-WR741ND WAP 4.0; UPnP 1.0)
8081/tcp open  blackice-icecap?
6112/tcp open  dtspc?
8089/tcp open  unknown
8081/tcp open  blackice-icecap?
8081/tcp open  blackice-icecap?
1080/tcp open  socks5     (No authentication; connection failed)
8888/tcp open  tcpwrapped
22/tcp open  ssh     OpenSSH 8.1p1 Debian 1 (protocol 2.0)
==============================================
```



Modelo


5 - MACs.png
marostegajunior — root@kali: ~/Desktop/Msis-M — ssh root@192.168.10.11...
==========
AC Address: C4:6E:1F:80:2F:44 (Tp-link Technologies)
MAC Address: C8:2B:96:50:B8:2E (Espressif)
MAC Address: 18:79:A2:0E:86:42 (GMJ Electric Limited)
MAC Address: D8:F1:5B:E9:23:D1 (Espressif)
MAC Address: C8:2B:96:50:B8:BE (Espressif)
MAC Address: 40:A2:DB:53:5F:D4 (Unknown)
MAC Address: 9C:2E:A1:D4:58:B7 (Xiaomi Communications)
==========
...
Pressione ENTER para retornar ao MENU


7 - Info - IP.png
marostegajunior — root@kali: ~/Desktop/Msis-M — ssh root@192.168.10....
==========
A Informacoes por IP
[Digite o IP:192.168.20.102]
Nmap scan report for 192.168.20.102
Host is up (0.029s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
8081/tcp open blackice-icecap?
MAC Address: D8:F1:5B:E9:23:D1 (Espressif)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=11/6%OT=8081%CT=1%CU=35011%PV=Y%DS=1%DC=D%G=Y%M=D8F15B
OS:%TM=6186C108%P=arm-unknown-linux-gnueabihf)SEQ(SP=95%GCD=1%ISR=CF%TI=I%C
OS:I=I%II=RI%SS=O%TS=U)SEQ(SP=97%GCD=1%ISR=CF%TI=RD%CI=I%II=RI%TS=U)SEQ(SP=
OS:76%GCD=1%ISR=CF%TI=RD%CI=I%TS=U)OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M
OS:5B4%O6=M5B4)WIN(W1=16D0%W2=16D0%W3=16D0%W4=16D0%W5=16D0%W6=16D0)ECN(R=Y%
OS:DF=Y%T=80%W=16D0%O=M5B4%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T
OS:2(R=N)T3(R=Y%DF=Y%T=80%W=16D0%S=O%A=S+%F=AS%O=M5B4%RD=0%Q=)T4(R=Y%DF=Y%T
OS:=80%W=16D0%S=A%A=S%F=AR%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=16D0%S=A%A=S+%F=AR
OS:%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=16D0%S=A%A=S%F=AR%O=%RD=0%Q=)T7(R=Y%DF=Y%
OS:T=80%W=16D0%S=A%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=38%UN=0%RIPL=G
OS:%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=80%CD=S)
==========
...
Pressione ENTER para retornar ao MENU

Resultado

```
0/tcp   open  http    TP-LINK WR741ND WAP http config
1900/tcp open  upnp    ipOS upnpd (TP-LINK TL-WR741ND WAP 4.0; UPnP 1.0)
8081/tcp open  blackice-icecap?
6112/tcp open  dtspc?
8089/tcp open  unknown
8081/tcp open  blackice-icecap?
8081/tcp open  blackice-icecap?
1080/tcp open  socks5     (No authentication; connection failed)
8888/tcp open  tcpwrapped
22/tcp open  ssh     OpenSSH 8.1p1 Debian 1 (protocol 2.0)
```

Portas abertas

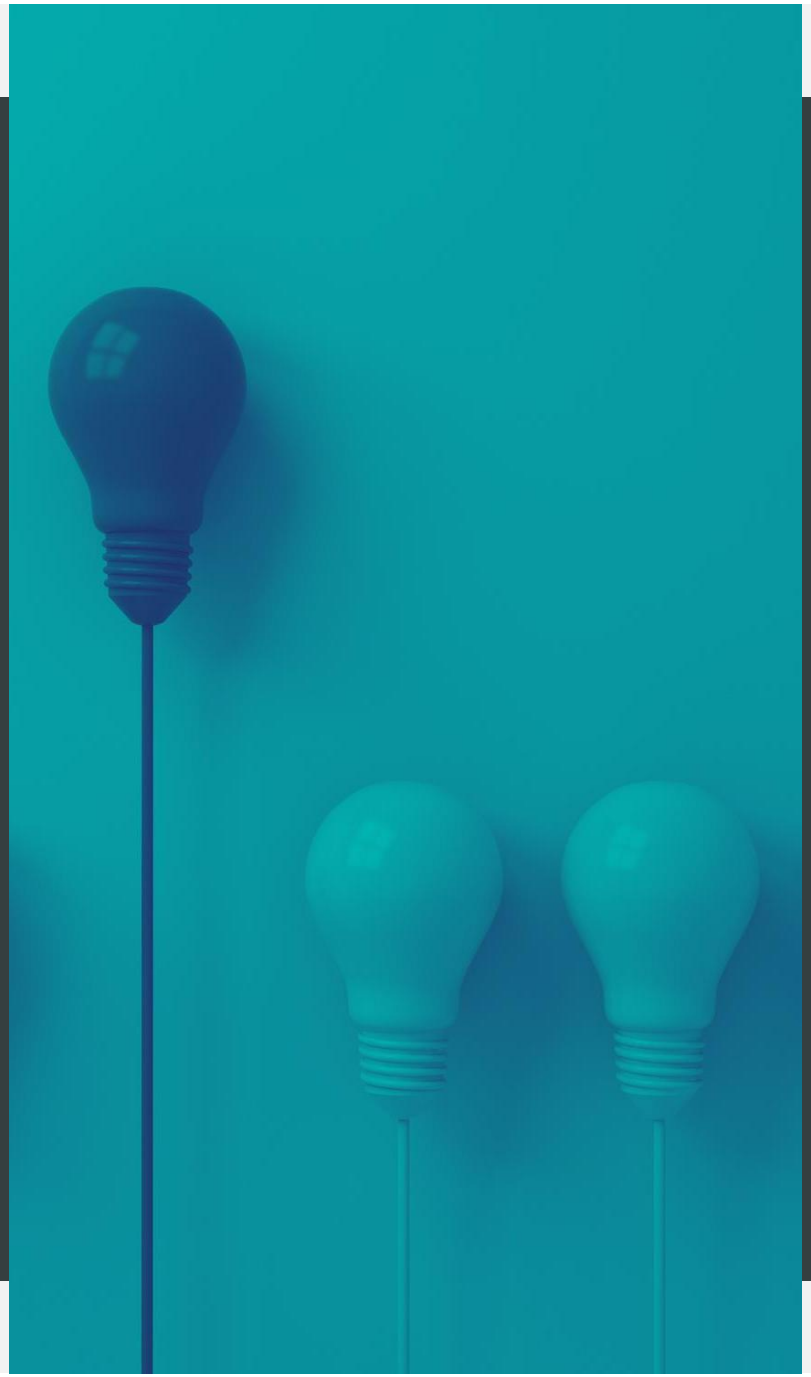
```
opcao 2- IPS - Descobertos
192.168.20.1
192.168.20.100
192.168.20.101
192.168.20.102
192.168.20.103
192.168.20.104
192.168.20.105
192.168.20.107
```

8 Dispositivos

IPs

```
Sistemas Operacionais descobertas
S CPE: cpe:/o:linux:linux_kernel:2.6
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS CPE: cpe:/o:linux:linux_kernel:3
```

SO e outros



04.
Diferencial

O que a sua solução tem de especial?

A **otimização**, **objetividade** de atuar em cenários variaveis como, **educacional**, **doméstico** e **corporativo** focado em trazer uma informação objetiva e limpa para que o usuário possa identificar e tomar conhecimento sobre como seus dispositivos estão configurados em sua rede.

05.
Arquitetura

Como funciona o seu produto?

1

Execução

O *software* atua em qualquer rede de computador. Respeitando sempre o mesmo range de comunicação. O protótipo será construído para ser executada em ambiente Linux e de forma direta via console (terminal).

2

Linguagem de Programação e Ferramentas

O *software* usado no mesmo está sendo desenvolvido usando ***Shell Script*** e ***Python 3***. Também usando ferramentas como netcat e nmap.

3

Resultado

O tratamento dos dados coletados será tratado para uma exibição limpa e intuítiva entre todos os dispostivos encontrados na rede de computadores qual está sendo executado o *software*.

Obrigado!