



Desafio de Segurança do EnSI 2016

Este ano o desafio de segurança do EnSI foi desenvolvido pelo grupo [LampiãoSec](#).

O desafio é organizado em etapas. Cada uma delas tem a informação que dará acesso a etapa seguinte.

Cada etapa consiste de atividades de diversas categorias e busca manter o teor realístico. Vence o primeiro que completar o desafio, porém apenas competidores inscritos e presentes no EnSI serão premiados. Caso ninguém cumpra todas as etapas, quem chegar mais longe leva o prêmio. A clareza e detalhes na explicação da solução será utilizado como critério de desempate.

Após completar o desafio, o participante deverá enviar e-mail para o endereço **desafio.ensi2016@pop-ba.rnp.br** com a descrição das soluções de todas as etapas. Serão aceitas respostas até às **15h do dia 28/09/2016**.

Início do desafio:

Sempre é citado a importância de se atentar para questões de login, força de senhas, singularidade das senhas, trocá-las com certo período, mas não é só isso que faz com que você esteja menos vulnerável na rede.

É sempre recomendado que se use criptografia nas transações, mas o usuário “fulano” é um pouco cabeça dura e fez login em um sistema web (que ele gerencia coisas importantes) sem nenhum nível de criptografia, apenas com uma autenticação básica. Infelizmente para ele, alguém estava na escuta do tráfego e capturou tudo que aconteceu, jogou o PCAP em alguns fóruns, até que chegou em suas mãos. A empresa do “Fulano” pode sofrer muito com isso e o desafio é chegar o mais fundo possível.

Link do arquivo PCAP:

<https://ensi.pop-ba.rnp.br/2016/files/20ccbf1b438148c601938e9abf694d34/captura.pcap>