INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA

SEGURANÇA DE REDES

ATIVIDADE - 1

Nome: _____

Neste exercício prático, o objetivo é compreender e fixar os conceitos básicos de TCP/IP, importantes para a segurança de redes. A ferramenta utilizada para o aprendizado é o *tcpdump*, um analisador de redes que faz parte das distribuições Linux.

1. Abra dois terminais do Linux. Em um terminal (A) você usará o *tcpdump* para monitorar o tráfego, e no outro terminal (B) você irá observar o tráfego gerado pelo outro terminal (A).

2. Teste as opções do *tcpdump*. Verifique as opções existentes de uso via *man pages*. Inicie o *tcpdump* com a sua opção padrão, ou seja, apenas digite: *tcpdump*. O que você está verificando? Que tipo de informação é possível obter?

3. Teste o modo *verbose* do *tcpdum*. Digite "*tcpdump* –v". O que você está verificando? Quais tipos de informações são possíveis se obter? Quais as diferenças que você está observando com relação ao comando anterior?

4. Agora teste o modo *verbose* mais poderoso do *tcpdump*. Digite "*tcpdump* –vv". O que você está verificando? Quais tipos de informação são possíveis se obter? Quais as diferenças que você está observando com relação ao comando anterior?

5. Use o *tcpdump* no terminal (A) para verificar o comportamento dos pacotes. No terminal (B), abra uma conexão Telnet para o equipamento do instrutor. Não digite nem usuário, nem senha. Como é possível verificar que está havendo uma conexão? Quais características devem ser observadas?

6. Agora tente capturar o usuário e a senha que você irá digitar no terminal (A). Foi possível capturar? Você capturou o usuário e a senha dos seus colegas também? A quantidade de informações obtidas pelo *tcpdump* foi elevada? Foi difícil observar alguma coisa?

7. É possível limitar o que o *tcpdump* apresenta na tela. Use, por exemplo, "*tcpdump* host 10.20.30.40", onde 10.20.30.40 é o endereço IP do equipamento do professor. Agora use "*tcpdump dst host* 10.20.30.40". Qual a diferença que você observou?

8. Agora tente utilizar "*tcpdump* | *grep* 10.20.30.40". Qual a diferença em relação ao item anterior?

9. É possível também filtrar os resultados do *tcpdump* para obter somente pacotes relacionados a um determinado serviço. Qual comando você utilizaria para observar, por exemplo, somente o tráfego relacionado ao Telnet?

10. É possível gerar um arquivo com os pacotes capturados para realizar uma análise posterior? Em caso afirmativo, como isso pode ser feito? Teste os comandos.