Insper

Tecnologias Hacker
Prof. Rodolfo Avelino
Laboratório aula 4 – Análise de Tráfego de rede

Considere o host alvo com o IP 10.0.0.102, utilize os comandos e ferramentas apresentadas em aula e responda as seguintes perguntas:

1. Qual o endereço Mac Address do alvo?
2. Quantas máquinas estão ativas na rede? Quais seus respectivos endereços ips?
3. Qual o Sistema Operacional do alvo?
4. Quantos datagramas IP, mensagens ICMP, datagramas UDP, segmentos TCP o seu host transmitiu e recebeu desde a última iniciação.
5. Liste todas as conexões TCP ativas de seu host.
6. Faça um ou mais pings para algum(ns) sites e, com o uso de parâmetros apropriados, faça com que o tcpdump:
   a. Capture todos os pacotes da rede.
   b. Capture somente os pacotes gerados por sua máquina.
   c. Capture somente pacotes destinados à sua máquina.
   d. Capture pacotes para ou da máquina 10.0.0.102.
   e. Capture pacotes FTP (lembre-se da porta de cada serviço).

7. Faça com que os pacotes capturados anteriormente sejam salvos num arquivo, chamado "capturados_SEUNOME.pcap", e coloque em seu diretório no Dropbox.

Observação: As perguntas deverão estar respondidas com os comandos executados e um print de suas respectivas saídas.