Atividades – Sniffer

Questionário

1. Qual é o objetivo e a quem se destinam os sniffers?
2. Defina a aplicação do sniffer em função usuário.
3. Que tipo de dados podem ser capturados com o sniffer?
4. O quer é o modo promíscuo e o modo não-promíscuo de uma interface de rede?
5. O que é preciso para que possamos utilizar um sniffer? É suficiente ter acesso à máquina? Por quê?
6. O que é sniffing passivo e quais são as suas principais ferramentas?
7. O que é sniffing ativo e quais são as suas principais ferramentas?

Atividade prática

1. Instalar as VMs de LinuxMint e Windows 7 em modo "bridged". Inicie a captura dos dados, abra o browser e entre em m website (por exemplo da FATECSCS) em uma das VMs e em outro website na outra VM. Após o término do carregamento da página, interrompa a captura, salvando-a em um arquivo. A partir dos dados capturados identifique:
a) O ARP foi usado?
b) Quais são os endereços de camada 2 (cliente e gateway)?
c) Quais são os endereços de camada 3 (cliente e gateway)?
d) Qual é o IP do DNS ?
e) Quais são os endereços IP devolvidos pelo DNS?

2. Refaça a conexão de rede das duas VMs como rede interna (consulte o guia da aula de nmap). Faça as varreduras padrão de vários tipos (tcp, syn, etc..) de uma VM para a outra capturando e salvando cada uma das capturas. Identifique e observe o conteúdo dos "packets".

3. Faça um relatório descrevendo a experiência.