**ISG012-02 - Análise conteúdo tráfego – Sniffer - Teoria – Atividades**

Nome: Gabriel Henrique Alves da Silva RA: 1689721211

**Questionário**

1. Qual é o objetivo e a quem se destinam os sniffers?

**Resp:** Fazer a captura de tráfego na rede local para análise. Se destinam tanto para atacantes quanto para os administradores da rede.

1. Defina a aplicação do sniffer em função usuário.

**Resp:**  Os administradores usam a aplicação sniffer para detectar e resolver problemas, já os atacantes leem os dados que passam por determinada máquina em real time ou guardar esses dados para caso seja útil futuramente.

1. Que tipo de dados podem ser capturados com o sniffer?

Podemos capturar qualquer dado que seja enviado na rede desde que não esteja encriptada. Alguns tipos de dados capturados são:

\*nomes de usuários e senhas para sessões de telnet;

\*consultas e respostas a servidores de nomes (DNS);

\*mensagens de correio eletrônico;

\*senhas de FTP;

\*arquivos acessados através de NFS ou

\*compartilhamentos do Windows;

\*etc..

1. O quer é o modo promíscuo e o modo não-promíscuo de uma interface de rede?

**Resp:** O modo promíscuo funciona quando a interface de rede captura todo o tráfego independe do endereço MAC (Media Access Control) de destino e pode ser utilizado em capturas de sniffing. Já o modo normal ou conhecido por modo não-promíscuo se refere a interface de rede que captura apenas o tráfego destinado a ela.

1. O que é preciso para que possamos utilizar um sniffer? É suficiente ter acesso à máquina? Por quê?

**Resp:** Para que possamos fazer a utilização do sniffer precisamos obter uma conta de acesso á máquina onde o sniffer está ou pode ser instalado. Sendo assim os empregados, fornecedores ou contratados podem se tornarem atacantes sendo que eles possuem acesso a essas máquinas.

Outras maneiras de se ter acesso é por meio da exploração de vulnerabilidades através de ataques de aplicação e ao SO como por exemplo o ataque de “buffer overflow” (transbordamento de dados).

1. O que é sniffing passivo e quais são as suas principais ferramentas?
2. O que é sniffing ativo e quais são as suas principais ferramentas?