Trabalho de Segurança de Redes – válido como AV3

Este trabalho poderá ser feito individualmente ou em grupos de, no máximo 3 alunos. Deve ser enviado por email ATÉ o dia **08 de julho** para o email contato@fredsauer.com.br.

Regras básicas:

1. As respostas não devem ser copiadas da Internet, livros ou manuais;
2. Capturas devem ser colocadas em todas as experiência E devem estar comentadas; e
3. As respostas não podem ser copiadas de trabalhos dos outros grupos. Se isso for identificado, ambos trabalhos ficarão com zero;

A transgressão de qualquer uma destas regras provocará o lançamento de nota ZERO para o trabalho.

Enunciado: O trabalho consiste na avaliação de algumas ferramentas disponíveis no BackTrack Linux (atual Kali Linux). Sugiro usá-lo, para tornar a tarefa mais rápida, mas isso não é obrigatório. As ferramentas também podem ser instaladas isoladamente. O BackTrack (Kali) pode ser usado em modo Live, sem instalá-lo na máquina, ou instalado em uma nova partição. Apenas faça isso se tencionar mantê-lo para usá-lo regularmente. As dificuldades para o uso e ativação das interfaces de captura podem ser facilmente resolvidas através de pesquisa na Internet, então isso faz parte do trabalho. Nem adianta me pedir ajuda...

Primeira Tarefa: Uso do Wireshark.

a) Identificar a utilidade prática do Wireshark. Como ele pode ser útil para um administrador de segurança identificar ataques à rede;
b) Que tipos de ataques ele pode identificar ?
c) Faça uma captura da rede onde você está fazendo o trabalho. Identifique pacotes que permitam a identificação dos IP de:
    i. do servidor DNS; e
    ii. do Gateway da rede, potenciais vítimas de ataques.

Segunda Tarefa: Uso do NMAP.

a) Identificar a utilidade prática do NMAP. Como ele pode ser útil para um administrador de segurança identificar vulnerabilidades na rede;
b) Quais informações o NMAP captura que podem ser usadas para reduzir vulnerabilidades ? Exemplifique isso em uma captura na sua rede;
c) Execute os comandos abaixo e capture as saídas; para cada um, explique o que o comando fez, vantagens e desvantagens de usá-lo:
    i. nmap -sS <IP do alvo>
    ii. nmap -sS -v <IP do alvo>
    iii. nmap -sS -n <IP do alvo>
    iv. nmap -sT <IP do alvo>
    v. nmap -sA <IP do alvo>
    vi. nmap -sO <IP do alvo>

Terceira Tarefa: Uso do Nessus.

a) Identificar a utilidade prática do Nessus. Como ele pode ser útil para um administrador de segurança identificar vulnerabilidades na rede;
b) Identifique os elementos funcionais do Nessus e os cuidados que devem ser tomados para que a busca por assinaturas seja eficaz;
c) Quais informações o Nessus captura que podem ser usadas para reduzir vulnerabilidades ? Exemplifique isso em uma captura na sua rede;

Quarta Tarefa: Uso do Snort.

a) Identificar a utilidade prática do Snort. Como ele pode ser útil para um administrador de segurança identificar ataques na rede;
b) Execute o Snort em modo IDS. Capture a tela e analise o que a operação neste modo pode proporcionar para aumentar a segurança de sua rede