Prática – Monitorando a rede

Ferramenta: comando **Netstat** (*Prompt do MS-DOS*)

1. Entender o uso do comando pela análise do Help disponível no SO
2. Emitir comando abaixo e analisar resultados.

netstat –aob

   a. Checar portas utilizadas no lado cliente e no lado servidor
   b. O que significa os estados apresentados? (RFC TCP/UDP)
   c. Pesquisar e conhecer as *well know ports* com seus serviços associados
      i. Que conexões (IP envolvidos) estão estabelecidas?
         1. Qual o serviço associado?
         2. "Quem é" o endereço externo conectado?
            a. Está na rede local ou fora dela?
      ii. Que portas estão escutando?
         1. Qual o serviço associado?
      iii. Quais processos na máquina local estão envolvidos?
         1. Explique porque.
      iv. Analise as portas abertas pelo micro em relação à função que executa.

Teoria: **Switchs x Hubs**

1. Explique a diferença de operação entre um *hub* e um *switch*?
2. Como se intercepta dados de outra estação da rede em um *hub*?
3. Como se intercepta dados de outra estação da rede em um *switch*?

Ferramenta: programa **Wireshark**

1. Acessar site web e analisar os dados capturados
   a. Camadas de protocolos
      i. Quais protocolos estão sendo trafegados?
      ii. Que portas locais e remotas demandadas (amostra)?
   b. Cheque os dados trafegados através das opções:
      i. Analyze → Follow → TCP Stream
      ii. Statistics → Flow Graph
      iii. Statistics → HTTP → Requests
      iv. Analyze → Expert information
   c. Verifique dentre os dados capturados se há trafego de dados em texto aberto
2. Copiar arquivos no compartilhamento informado pelo professor
   a. Camadas de protocolos

i. Quais protocolos estão sendo trafegados?
ii. Que portas locais e remotas demandadas (amostra)?

b. Cheque os dados trafegados através das opções
i. Analyze → Follow → TCP Stream
ii. Statistics → Flow Graph
iii. Statistics → HTTP → Requests
iv. Analyze → Expert information

c. Verifique dentre os dados capturados se há trafego de dados em texto aberto.

Ferramenta: programa **Nmap**

1. Fazer varredura e coletar informações do IP informado pelo professor
2. Use : *Intense scan plus UDP*
   a. Qual o *MAC Address* da máquina alvo?
      i. O que é o *MAC Address*?
   b. Quantas portas foram descobertas abertas?
   c. Quais portas abertas?
      i. Quais serviços estão associados?
   d. Qual sistema operacional em execução na máquina alvo?
   e. Qual o nome do computador?
   f. Há que grupo/domínio o computador pertence?
   g. Qual a conta de usuário em uso?
   h. Qual o horário registrado no sistema
3. Alguma informação foi coletada que permita acessar a máquina mesmo sem a "permissão" do usuário?
   a. Há serviços oferecidos sem proteção?
      i. Se sim, qual e qual a forma de acesso?
   b. Há dados expostos?
4. Faça uma análise geral e descreva o recurso bem como os aspectos de serviço e segurança envolvidos.
5. Acesse o link abaixo:
   Site
   a. Para onde você foi direcionado?
   b. Do que se trata?
   c. Que recomendações você faria aos usuários a respeito do assunto?

Ferramenta: programa **Angry IP Scanner** (W)**, WiFi Analyzer** (A) e **LAN Scanner** (A)

1. Manuseie os programas citados fazendo a varredura em rede local
2. Analise os resultados obtidos