Engenharia de Segurança (SSC -0747)

São Carlos, 6 de Abril de 2010

Prática 2 – Scanning & Mapping

1. Introdução

Mapping é um procedimento para identificação de hosts e de seus sistemas operacionais dentro de uma rede. *Scanning* de redes é um procedimento para identificação dos serviços disponíveis. Este procedimento pode ser utilizado para levantar a infra-estrutura da rede e detectar vulnerabilidades. Hackers, tipicamente, fazem o *scanning* da rede para detectar quais hosts são mais sucetíveis a ataques. Nesta prática mapearemos a rede do campus II e descobriremos os servidores que estão executando em cada um dos computadores.
Utilizaremos a infra-estrutura controlada do campus II para este experimento. Vale ressaltar que um *scanning* de uma rede pode gerar alertas para o administrador e causar, eventualmente, punições de acordo com o regulamento vigente.

2. Materiais

Utilizaremos os seguintes materiais:

- Notebook com interface Ethernet
- Linux BT4 (Live CD)
- Autoscan
- Nmap

3. Descrição da Prática

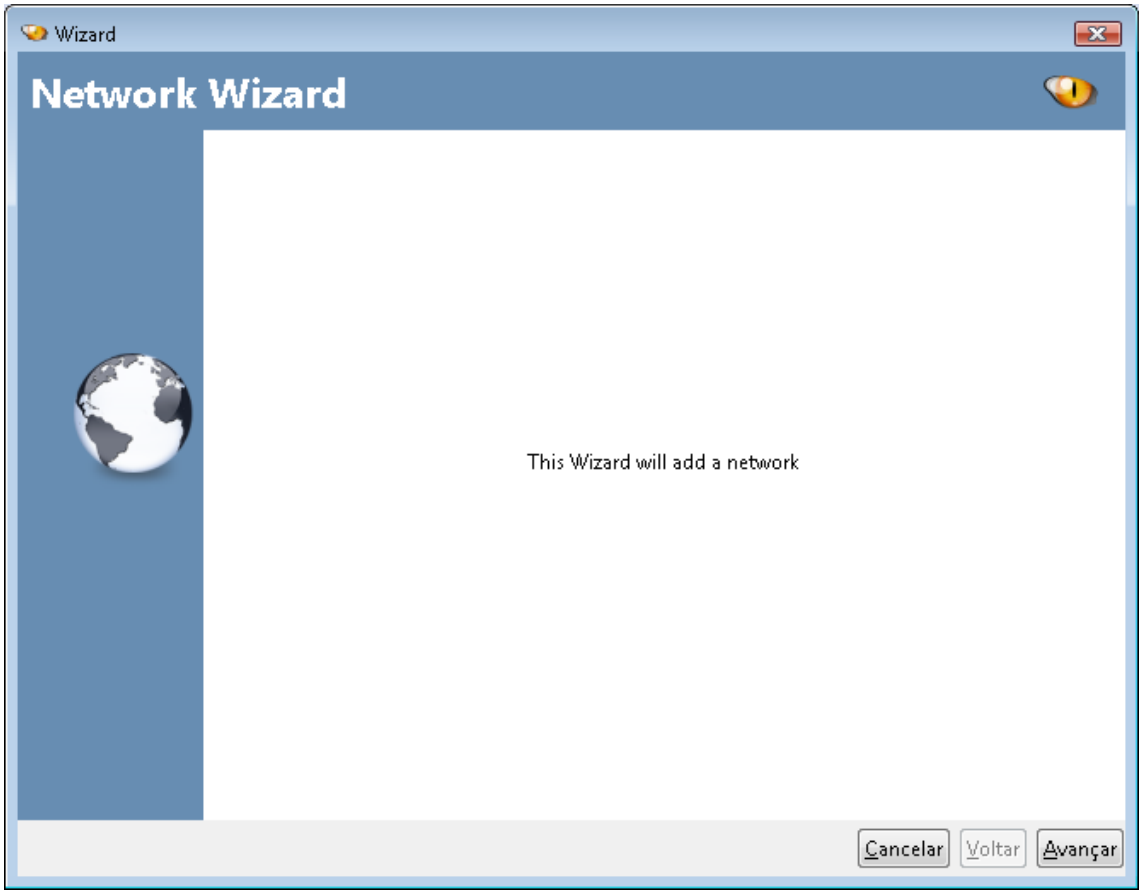
Os alunos se dividirão em grupos de 4 pessoas, e cada grupo receberá um notebook. Em seguida anote o número do notebook na folha de presença na frente do nome.

3.1 Autoscan

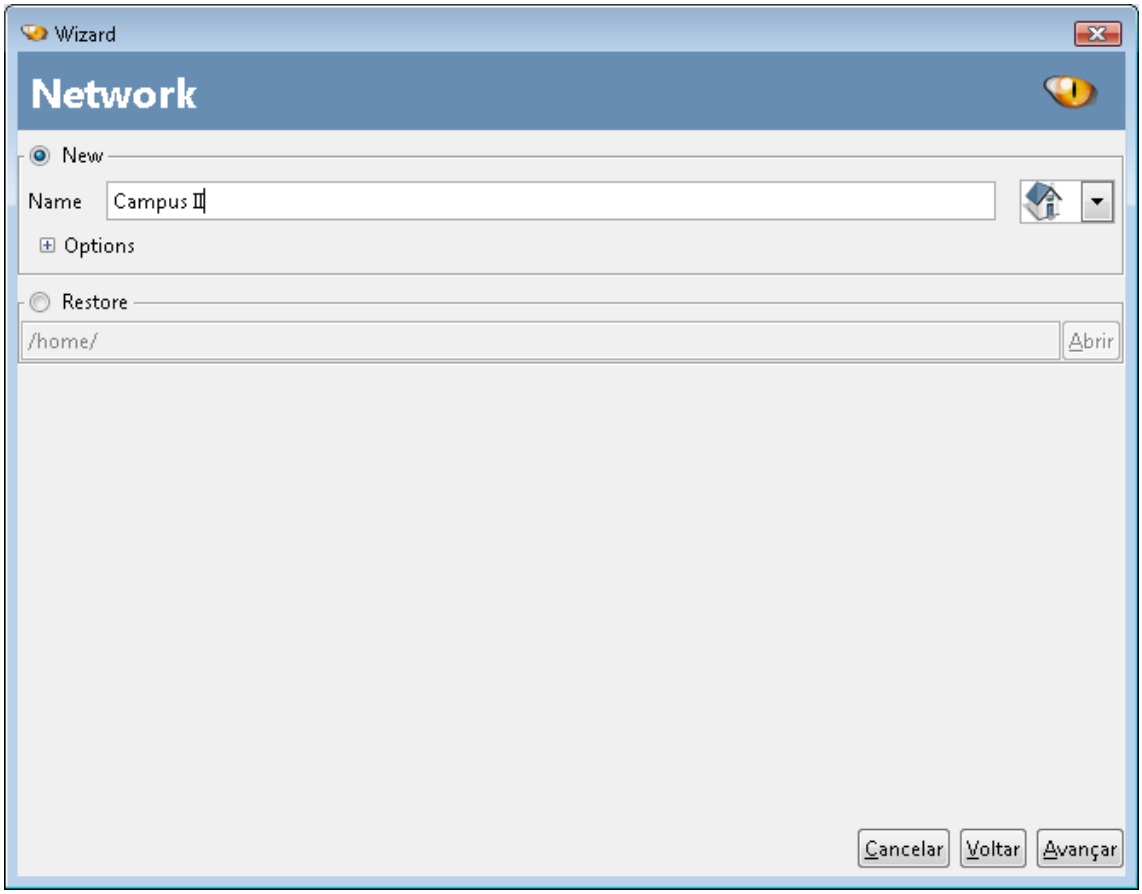
Para mapearmos os computadores da rede utilizaremos a ferramenta **autoscan** pré-instalada no BT4
Digite no terminal:

- autoscan

A seguinte tela será exibida:

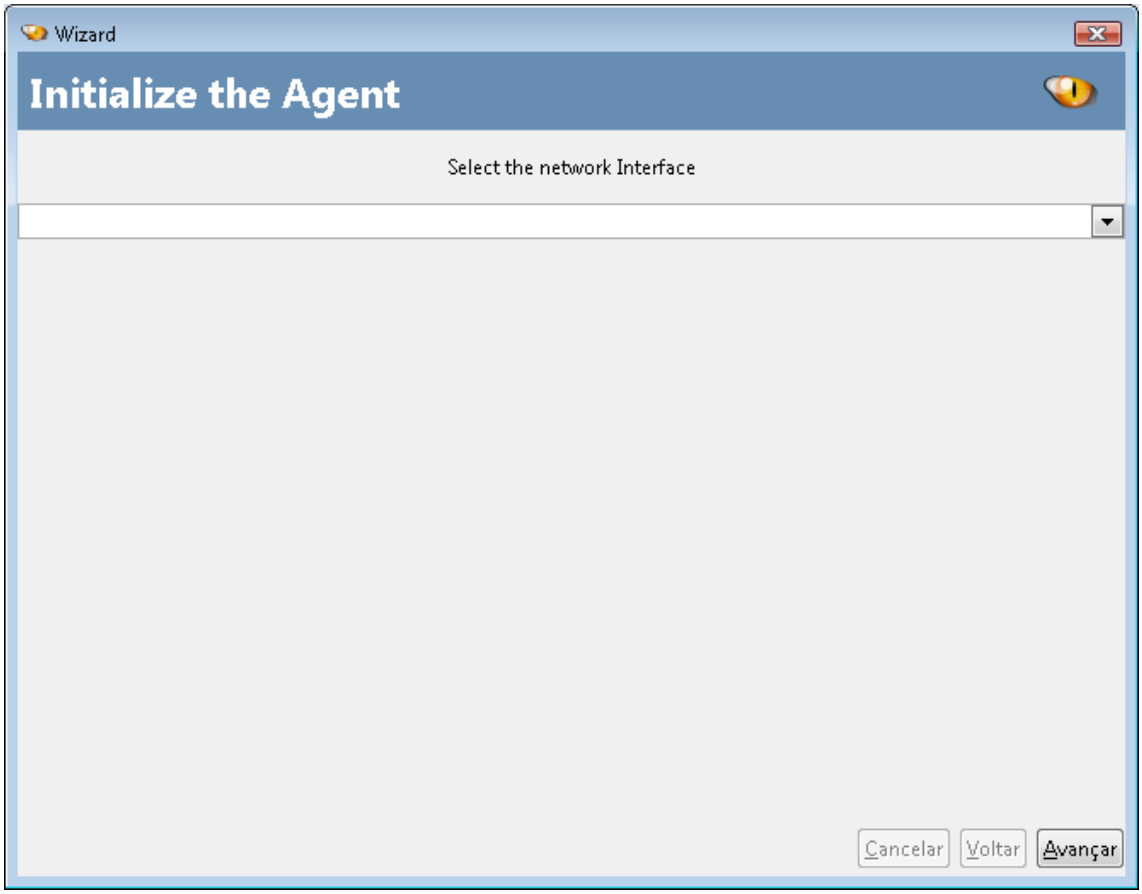


Aperte o botão “Avançar”, e configure os itens da seguinte tela



Note que é possível restringir a varredura de hosts escolhendo o range de IPs em “Options”.

Selecione a interface de rede que será utilizada para o processo de *scanning*



Após o *scanning* responda às seguintes perguntas:

1. Qual os serviços (portas) mais utilizados?
2. Qual o endereço do servidor de impressão? Qual o seu sistema operacional?
3. Qual o IP da impressora? Esta impressora suporta gerenciamento remoto (WEB)?
4. Qual o IP dos Access Points?
5. Qual o SO do computador “Alex-PC”?
6. Quais serviços estão sendo executados no firewall (192.168.181.1)?

3.2 Nmap

Com o comando nmap é possível fornecer um relatório mais detalhado dos serviços de determinado host. Para mapearmos as portas abertas de determinado host utilizaremos o comando:

- nmap -v -A ENDERECO_IP

O último passo é descobrir qual a versão dos serviços descobertos. Utilize o nmap para obter estas informações de algum servidor do campus II com o comando:

- nmap -sV ENDERECO_IP

1. Anote no relatório os serviços abertos no host escolhido e suas respectivas versões.