Visualize sua rede com o RadialNet

Visão conectada

O RadialNet fornece uma imagem da rede e ajuda administradores a identificarem falhas potenciais de segurança.

por Hagen Höpfner

Existem inúmeros programas para mapeamento de estruturas de rede e identificação de vulnerabilidades. Uma das ferramentas mais populares é o célebre Nmap [1]. Vários administradores valorizam esse software por seus recursos de análise de estrutura e segurança, mas infelizmente ele oferece poucas opções internas para visualização dos resultados da análise.

Uma ferramenta chamada *RadialNet* [2], de autoria do brasileiro João Paulo de Souza Medeiros, é ótima para visualizar estruturas de rede mapeadas pelo Nmap, pois fornece um panorama gráfico dos computadores conectados (**figura 1**).

Instalação

O RadialNet é escrito em *Python*. Para usá-lo, são necessários, além do interpretador Python, os pacotes *PyCairo*, *PyGTK* e *PyGObject* para a interface gráfica. Todos são facilmente instaláveis pelos repositórios das distribuições.

Após baixar o RadialNet em [2], basta descompactá-lo e em seguida iniciá-lo com o comando:

```
python radialnet.pyw
```

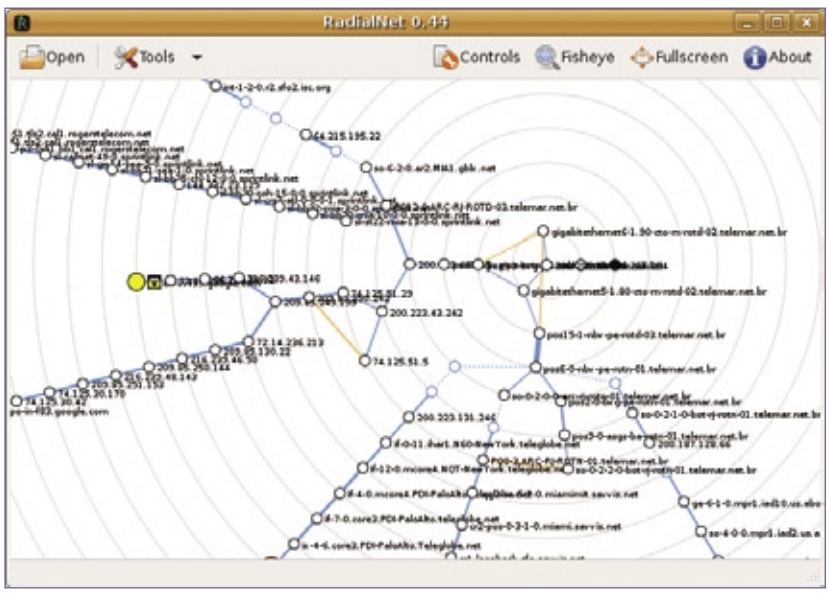

Figura 1 O RadialNet visualiza estruturas complexas de rede e vulnerabilidades potenciais num relatório intuitivo.

O RadialNet utiliza os resultados do Nmap para mostrar uma visualização do seu significado. Os dados precisam estar formatados em XML e podem ser passados para o programa tanto na linha de comando (opção `-f nome_do_arquivo`) quanto interativamente pelo menu *Open*.

Utilização

O RadialNet inclui um arquivo de entrada de exemplo, `nmap_example.xml`. O arquivo se localiza no diretório `share/sample/` após a descompactação do pacote e é suficiente para experimentos iniciais. Por padrão, o localhost fica no centro do mapa, mostrado como um ponto preto. As cores dos nós mostram os dispositivos analisados pelo Nmap e indicam o número de portas abertas. Como portas abertas são riscos potenciais de segurança, computadores com muito poucas portas abertas são mostrados em verde. O amarelo indica risco mediano, enquanto que nós vermelhos estão praticamente "escancarados". Nos nós brancos, não há informações sobre portas. Os quadrados na imagem significam roteadores, switches e pontos de acesso sem fio. O tipo é indicado por um ícone azul claro (**figura 2**). Os círculos

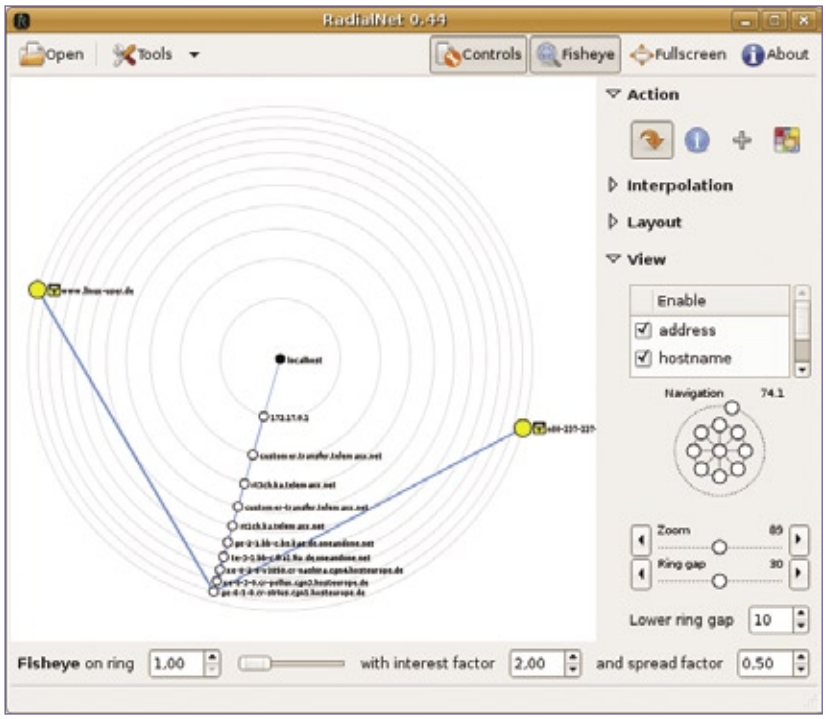

Figura 2 O caminho do computador do autor até dois sites distintos.

são computadores "reais". Também podem aparecer outros ícones. Um cadeado amarelo significa um computador com portas filtradas, ao passo que um muro vermelho sinaliza, obviamente, um firewall.

Um clique esquerdo sobre um círculo ou quadrado o move para o centro do mapa. Um clique direito abre um diálogo com informações mais detalhadas sobre o nó de rede selecionado (**figura 3**). A aba *General* mostra informações gerais sobre o sistema operacional e a interface de rede ativa. A aba *Services* lista as portas abertas, e *Traceroute* informa a rota do *localhost* até o nó clicado. Infelizmente, não é possível aumentar ou diminuir a janela, o que significa que provavelmente será preciso usar as barras de rolagem independentemente do tamanho do seu monitor.

O item de menu *Tools* | *Host Viewer* exibe um panorama das informações detalhadas que pode ser aproximado e afastado. O lado esquerdo da janela mostra os nós analisados, com as informações retiradas da janela à esquerda.

O mapa exibe as conexões entre os nós individuais do mapa, indicando rotas que os dados tomarão do localhost até os nós da borda. Se estiverem faltando informações do traceroute, o caminho será mostrado como uma linha pontilhada.

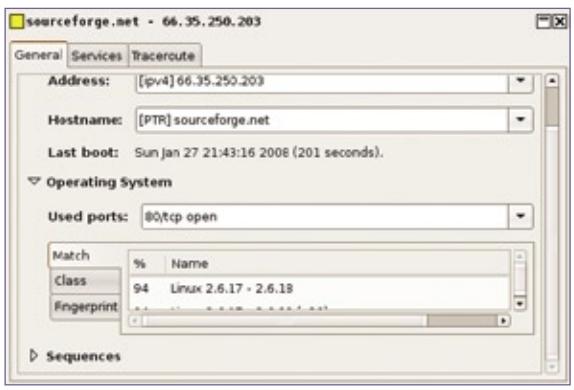

Figura 3 Um clique duplo num nó de rede mostra informações detalhadas sobre ele.

Opções de visualização

Além dos botões já citados, o RadialNet possui outros quatro no canto superior direito da janela. O item *About* mostra as informações sobre o programa, enquanto *Fullscreen* ativa e desativa a visualização em tela cheia. O botão Fisheye permite alternar para uma visão no estilo "olho de peixe", que dá mais espaço ao centro do mapa do que às bordas, facilitando a leitura das informações no centro da tela. Uma barra aparece na parte de baixo da janela e pode ser usada para alterar o aspecto de olho de peixe. A visão plana aloca o mesmo espaço a todos os nós do mapa.

Clicar em *Controls* mostra um auxiliar de navegação no lado direito da janela. Com essa ferramenta, pode-se aproximar e afastar o mapa ou alternar entre as visões de nomes de máquinas e endereços. Estranhamente, quando a opção *address* é desativada, os nomes de máquinas também desaparece. Com isso, o objetivo é fornecer sempre a melhor forma de visualizar os dados, de acordo com a vontade do usuário.

Conclusões

Graças ao RadialNet, a análise de vulnerabilidades e o mapeamento de redes não estão mais restritos ao modo texto. Junto com o Nmap, o RadialNet oferece aos administradores uma boa ferramenta para visualizar a rede que identifica claramente riscos potenciais. A única desvantagem é que ainda é preciso rodar o Nmap separadamente, pois o RadialNet não se integra a ele. ■

Mais informações

[1] Nmap: http://nmap.org

[2] RadialNet: http://www.dca.ufrj.br/~joaomedeiros/radialnet