Visualizing your network with RadialNet

NET VIEW

Saniphoto, Fotolia

RadialNet draws a picture of the network, helping admins identify potential security holes. **BY HAGEN HÖPFNER**

A number of programs let the user map network structures and vulnerabilities. One of the most popular tools is the terminal-based network mapper Nmap [1]. Many admins value Nmap's security and structure analysis functionality. Unfortunately, Nmap only offers a few internal options for visualizing the results of the analysis. A tool called RadialNet [2] visualizes network structures mapped by Nmap to provide a graphical overview of the networked computers (Figure 1).

Installation

RadialNet is written in Python. To use the program, you need a Python interpreter, along with the PyCairo, PyGTK, and PyGObject packages for the graphics. On Ubuntu, you can install these packages by typing *sudo apt-get install python-cairo python-gtk2 python-gobject*. Other distributions also include the packages by default. Launch your favorite distribution's software management tool to complete the installation.

After downloading RadialNet 0.44 [2], you can unpack the tool in a terminal window by typing *tar xfvz radial-net-0.44.tar.gz*. Then, to launch the program, type *python radialnet.pyw*. RadialNet

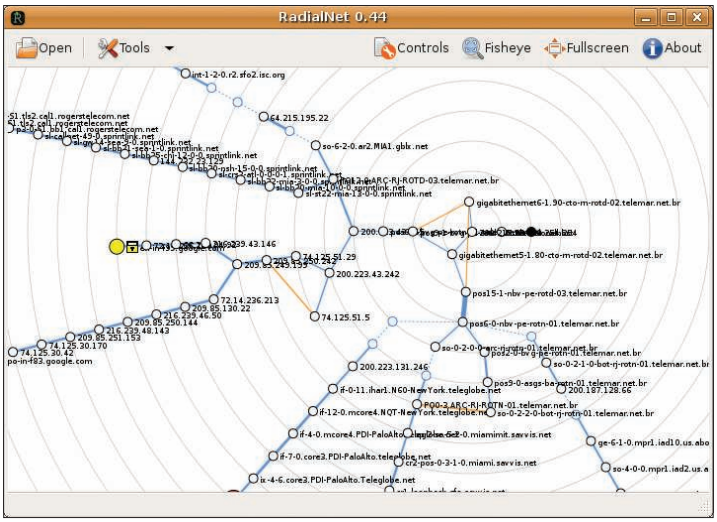

Figure 1: RadialNet visualizes complex network structures and potential vulnerabilities in an intuitive report.

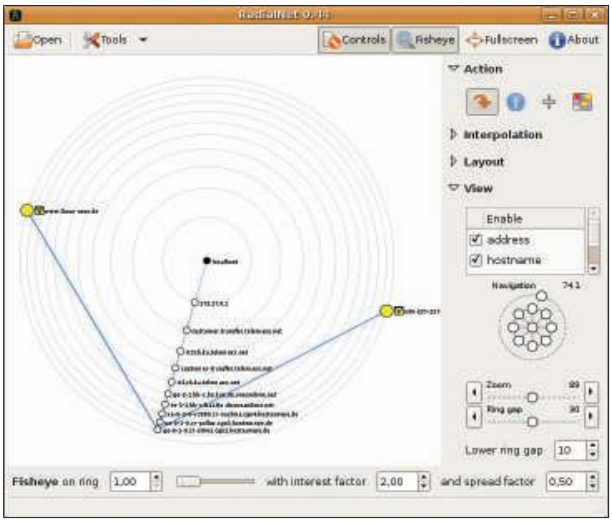

Figure 2: The path from the author's computer to a pair of target websites.

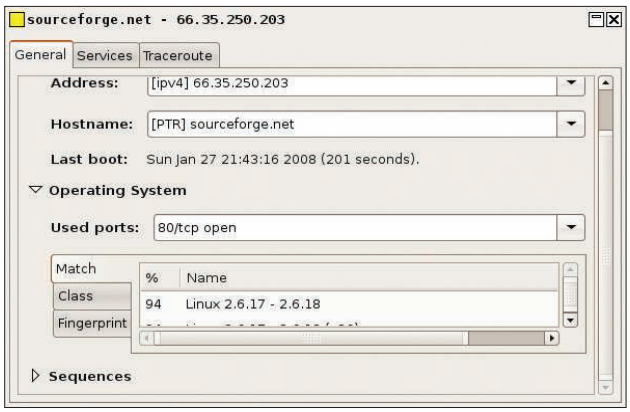

Figure 3: Right-click on a network node for detailed information on the devices.

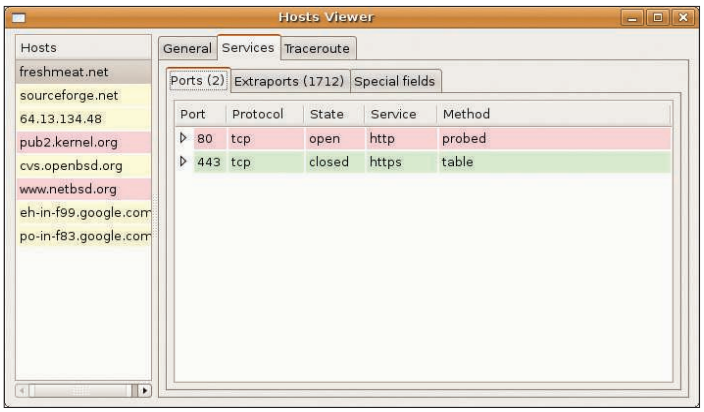

Figure 4: The Host Viewer shows detailed information for analyzed nodes.

helps you visualize Nmap analysis results (see the "Exploring the Network with Nmap" box). The data must be formatted in XML and can be passed in to the program either at launch time, by adding a *-f FILENAME* flag, or interactively by selecting *Open*.

Getting Started

RadialNet includes a sample input file, *nmap_example.xml*. The file is located in the *share/sample/* subdirectory and will suffice for initial experiments. By default, your computer (localhost) will be at the center of the map, shown as a black dot. The colored nodes show the devices analyzed by Nmap. The color indicates the number of open ports. Because open ports are potential security risks, computers with very few open ports are shown in green. Yellow indicates a medium-scale risk, and red nodes are open as wide as a barn door. No port information is available for white nodes. Squares depict routers, switches, or WLAN access points. The type is indicated by a light blue icon [2]. Circles are "real" computers. Other icons might also appear. A yellow padlock stands for a computer with filtered ports, and a red wall is a firewall.

Left-clicking a circle or a square moves it to the center of the map. Right-clicking opens a pop-up dialog with detailed information on the selected network node (Figure 3). The *General* tab takes you to general operating system information and the active network interface. *Services* lists the open ports, and *Traceroute* tells you the route from the localhost to the node you clicked. Unfortunately, you cannot scale the pop-up window, which means you will probably need to scroll no matter how big your screen is.

The *Tools | Host Viewer* menu item takes you to a scalable overview (Figure 4) of the detailed information. The left-hand side of the window shows the nodes analyzed, with the information from the pop-up window on the right.

The map shows connections between individual nodes on the map, indicating the routes that data will take from localhost to the border nodes. If traceroute information is missing, the path is shown as a dotted line.

Visualization Options

Besides the buttons referred to already, RadialNet has four more in the top right of the window. *About* takes you to an About RadialNet dialog with licensing information (GPL 2) for the program. *Fullscreen* toggles the full-screen view on or off. The *Fisheye* button lets you toggle between a flat display and a fisheye view. The fisheye view assigns more space to the center of the map than to the border areas, thus making the information at the center easier to read. A slider appears at the bottom of the window, which you can use to change the fisheye view aspect. The flat view allocates the same amount of space to all the nodes on the map.

Clicking *Controls* displays a navigation aid on the right side of the window. With this tool, you can zoom in or out of the map or toggle between address and hostname views. Strangely, when you disable the *address* checkbox, the hostnames disappear too. Also, you might want to try a few of the parameters I looked at on the sample file to discover a perfect view mode for your own needs.

Conclusions

Thanks to RadialNet, vulnerability analysis and network mapping are no longer restricted to text-based output. In combination with Nmap, RadialNet gives administrators a tool for visualizing the network that clearly identifies potential risks. The only drawback is that you still need to run Nmap separately because RadialNet does not integrate seamlessly with the mapper. ■

Exploring the Network with Nmap

Before you can start exploring your own network with Nmap, you need to be certain that Nmap is installed on your system. On Ubuntu, you can type *sudo apt-get install nmap*. For other distributions, it makes sense to launch a software management tool. RadialNet expects an XML input file, and Nmap will create XML if you specify *-oX FILENAME* when you launch. The following command

```
sudo nmap --traceroute -oX ➥
nmap-xml-output.xml ➥
www.linuxuser.de ➥
www.linux-magazine.com
```

analyzes the open ports on the *www.linuxuser.de* and *www.linux-magazine.com* web servers. The *--traceroute* parameter ensures that routing information is stored in the XML-formatted (*-oX*) file (*nmap-xml-output.xml*). You can then open and visualize the results in RadialNet (Figure 2).

INFO

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

[2] RadialNet homepage: *http://www.dca.ufrn.br/~joaomedeiros/radialnet/*