NIGHTSHADE USER'S MANUAL

Last Updated: 1 November 2007

1 DESCRIPTION

This document describes installation and operation of Nightshade, a collection of tools intended to exploit vulnerabilities in network devices, including but not limited to wireless access points and routers.

2 GENERAL REQUIREMENTS

Nightshade requires:

- **Hardware:** laptop with 802.11 wireless card (internal or external)
- **OS:** Windows XP or Linux
- **Software:** Java JDK 1.5 (5.0) or newer (latest java download available from: http://www.java.com/getjava)

3 INSTALLATION

To install Nightshade, unzip Nightshade.zip to a directory of your choosing.

- **Windows:** use Winzip, WinRAR, or a similar unzip tool.

- **Linux:** from a terminal, execute: `unzip Nightshade.zip`

After unzipping the file, you should see a "Nightshade" directory. Each subdirectory under Nightshade is a different Tool (e.g., Nightshade/Tomato/ contains all relevant software for the Tomato tool).

4 OPERATION

This section describes the operation of each Nightshade tool.

4.1 TOMATO

Tomato is a tool that fetches the administrator password from various Broadcom-based wireless access points and routers.

4.1.1 General Operation

Tomato is generally operated as follows:

- Tomato user wirelessly connects to the network device.
- Tomato user runs the Tomato program which returns the network device's administrator password (and performs any other actions), or indicates an error.

4.1.2 Linux Operation

To run Tomato on a Linux laptop:

- Wirelessly connect to the network device. This procedure can vary per linux distribution, but typically one can use linux wireless tools (iwconfig) and wpa_supplicant (pre-installed on most recent linux distributions). Consult the man pages if necessary. Also, the wpa_supplicant GUI, is a particularly useful tool (see **http://hostap.epitest.fi/wpa_supplicant/wpa_gui.html**).
- Change to the Tomato Release directory. For example, if you unzipped Nightshade in the "/home/myuser/foobar" directory, at a terminal prompt, type:

```
cd /home/myuser/foobar/Nightshade/Tomato/Release
```

- Run Tomato.sh with the appropriate action argument (see section 4.1.4 for a discussion of which action may be appropriate)::
  - **`./Tomato.sh pass`** fetches the password
  - **`./Tomato.sh passr`** fetches the password and reboots the device
  - **`./Tomato.sh shell`** fetches the password and opens a telnet-like interactive shell to the device
  - **`./Tomato.sh help`** prints help for Tomato, including device coverage

4.1.3 Windows XP Operation

To run Tomato on a Windows XP laptop:

- Wirelessly connect to the network device. Start -> Control Panel -> Network Connections -> Wireless Network Connection (or similar). Then select the wireless network of interest and click the Connect button. If this network is encrypted, Windows will prompt for the WPA or WEP key.

- Once connected to the wireless network of interest, open an explorer window and navigate to the Tomato Release directory. For example, if you unzipped Nightshade in the “C:\foobar” directory, in the address bar type:

```
C:\foobar\Nightshade\Tomato\Release
```

- To run Tomato, double-click the appropriate batch (.bat) file (see section 4.1.4 for a discussion of which batch file may be appropriate):

    - **TomatoGetPassword.bat** fetches the password

    - **TomatoGetPasswordAndReboot.bat** fetches the password and reboots the device

    - **TomatoGetPasswordAndOpenShell.bat** fetches the password and opens a telnet-like interactive shell to the device

    - **TomatoHelp.bat** prints help for Tomato, including device coverage

    The batch files are simply for convenience. Alternatively, you can open a command prompt (Start->Run, type “cmd”, and click “OK”), change to the Tomato Release directory (cd C:\foobar\Nightshade\Tomato\Release), and type “Tomato.bat help” for more Tomato information, including device coverage.

4.1.4 USAGE CONSIDERATIONS

This section discusses usage considerations when using the Tomato tool – i.e., what are the consequences of each Tomato action (get password, get password and reboot, get password and open shell), and under what circumstances might that action be appropriate.

As Tomato finishes its last operation, the UPnP service on the network device will terminate. So, running:

Windows: “TomatoGetPassword.bat”
Linux “Tomato.sh pass”

will fetch the password, and in doing so terminate the UPnP service.
Running:

Windows: “TomatoGetPasswordAndReboot.bat”
Linux: “Tomato.sh passr”

will fetch the password and reboot the device. Once rebooted, the device will again be running the UPnP service.

Thus, the user must consider which will be more detectable: a missing UPnP service, or a temporary interruption in network service while the device reboots. In general, UPnP is not a particularly oft-used service, and a network administrator may not be too suspicious if the service fails. All of the Tomato-covered network devices reboot in less than 10 seconds, although a system administrator may be more suspicious about a temporary drop in network service.

Running:

Windows: “TomatoGetPasswordAndOpenShell.bat”

Linux: “Tomato.sh shell”

should be used in advanced situations where an interactive shell is appropriate. Note that all Tomato-covered devices have a reboot utility, typically run as “/sbin/reboot” through the interactive shell.