**Team C**

Brad Norman

Jamie Lane

Daniel Ross

**Reflected Denial of Service Tester User’s Guide**

This application, RdosTester, will generate the type of traffic but not the volume of traffic necessary to initiate a reflected denial-of-service attack (RDoS). It is not meant to be an actual hacking tool, but a proof of concept. Without a proof-of-concept exploit application available, many developers will not patch security vulnerabilities. The vulnerability that this application exploits was patched in 2010.

**System Software Requirements**

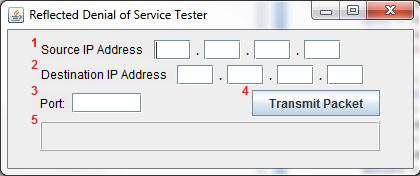
RdosTester is supported on Microsoft Windows XP SP1 and above (32/64-bit). RdosTester may also run on Linux with kernel v2.6.18 and above, FreeBSD 7.1 and above, and Open Solaris 2009 but performance is not guaranteed. Execution additionally requires the system to have the Java Runtime Environment v7 (32-bit) installed, as well as the jNetPcap API v1.3. Administrative privileges may be required to execute the application.

**System Hardware Requirements**

The minimum hardware specifications are determined by the OS hosting the JRE. To execute on a supported Linux distribution, only 64 MB of ram and 58 MB of hard disk space are required. Supported processors include x86, x86-64, x64 and AMD64. Processors such as ARM v6+ and Sparc may also suffice but performance is not guaranteed.

**Graphical User Interface**

When the application is run, the RdosTester GUI will be displayed. Please see below for details regarding the RdosTester GUI.



**RdosTester GUI**

There are 5 main components to the RdosTester GUI:

1) Source IP Address Input Field

2) Destination IP Address Input Field

3) Port Input Field

4) Transmit Packet Button

5) Status Bar

**Operation Instructions**

1) Double-click the RdosTester.jar file to run the application.

2) Enter a valid source IPv4 address. This source IP address will identify the host that will receive the large return packet(s) from the exploited server. This host is considered the victim of the reflected denial-of-service attack.

3) Enter a valid destination IPv4 address for a vulnerable OpenArena server. This destination IP address will identify the server that the RdosTester will attempt to exploit. If successful, the destination server will respond to the “source” host with a packet up to twenty times bigger than the original packet it receives from RdosTester.

4) Enter a valid destination port for the vulnerable OpenArena server.

5) Click the “Transmit Packet” button.

6) In the status bar, the application should now be displaying the size of the packet received from the vulnerable OpenArena server. The size of the received packet is formatted as a percentage of the original packet size. ***If the exploit is successful, the received packet will be much larger than the original packet*** (If any errors have occurred, they will be shown in the status bar area).

7) Repeat steps 1 through 5 as desired. To exit the application, click the X button in the top right corner of the GUI.