Achilles 0.27

Description

Achilles is a tool designed for testing the security of web applications. Achilles is a proxy server, which acts as a man-in-the-middle during an HTTP session. A typical HTTP proxy will relay packets to and from a client browser and a web server. Achilles will intercept an HTTP session's data in either direction and give the user the ability to alter the data before transmission. For example, during a normal HTTP SSL connection a typical proxy will relay the session between the server and the client and allow the two end nodes to negotiate SSL. In contrast, when in intercept mode, Achilles will pretend to be the server and negotiate two SSL sessions, one with the client browser and another with the web server. As data is transmitted between the two nodes, Achilles decrypts the data and gives the user the ability to alter and/or log the data in clear text before transmission.

Note 1: Achilles does not verify any web servers' certificates. Serving as a man-in-the-middle, Achilles is vulnerable to man-in-the-middle attacks.

Note 2: The current version of Achilles doesn't support host restrictions, so any user with access to the port Achilles is running on can use it as a proxy.

Note 3: Even though Achilles can function as a proxy server, it is HIGHLY discouraged to be used as such when not testing web applications.

System Requirements

OS: Windows 2000, Windows NT, Windows 98, Windows 95 with Winsock2
Web Browser: Tested with Netscape 4.75 and MSIE 5

Features

Proxy Server
Intercept HTTP and SSL traffic in either direction
Log HTTP and SSL sessions in plain text
Inserts data in an edit box to allow alteration
Configurable Port to Listen on
Configurable Timeout Values
Recalculates Content-Length Fields after data is modified
Additional buffer space to allow buffer overflow testing, up to a maximum of 10,000 bytes

Installation

Unzip the download file to any directory (c:\any-directory).

Starting Achilles

From windows explorer, navigate to "c:\any-directory" and double click Achilles.exe. Select intercept mode and intercept client data, and then press the start button to begin.

Configuring the Web Browser

The browser must be configured to use a proxy server.

Microsoft Internet Explorer Setup

Click Tools --> Internet Options --> Connections -->

If using a dial-up connection, in dialup settings click 'settings'
If using a local area network click 'LAN Settings'

Then select Proxy Server, Use Proxy Server—> Advanced and type in 127.0.0.1 for proxy address and 5000 or other configured port (in Achilles port field) for port in the HTTP and Secure boxes only.

Netscape Navigator Setup

Click Ed--> Preference--> Advance--> Proxy--> Manual Proxy Configuration --> View and type in 127.0.0.1 for proxy address and 5000 or other configured port (in Achilles port field) for port in the HTTP and Secure boxes only.

Using Achilles

Achilles operates in two modes; non-intercept mode and intercept mode. In non-intercept mode Achilles operates like a standard proxy. In intercept mode Achilles will act as a man-in-the-middle. Intercept mode must be set in order to capture, alter, and log any data during an SSL session. In order to switch between intercept and non-intercept mode, the proxy must be stopped and restarted.

Intercept Mode

Note that a considerable performance hit will be suffered while in intercept mode. While in this mode the server and client timeouts are used. In the event of a web page not fully loading or an error is received, it is very possible that the **server timeout is too low**. This is common when visiting a web page and submitting a form that requires heavy processing at the server's end, resulting in a lengthy wait. In the event of a timeout, just set the timeout to a higher value, reload the page and change the timeout back to a more efficient value. Only text and html content will be brought up to the edit window for modification.

Note: While in intercept mode, the client browser will pop-up security alerts concerning the servers certificate. Click OK/Continue to continue with the session (NOTE: The web server's certificate is not being authenticated, making the client web browser vulnerable to man-in-the-middle attacks, so proceed with caution).

Non-Intercept Mode

While in non-intercept mode, Achilles will act as a normal proxy. Only a slight performance hit should be noticed. While Achilles is in non-intercept mode timeouts are ignored. At any time during a session, the proxy can be stopped, and switched over to intercept mode and then restarted.

Listening Port

The listening port is the port that the proxy server is listening on. This is the port that the web browser must be instructed to use.

Cert File

The certificate is required for the client SSL connection to the proxy during intercept mode. A dummy certificate (sample.pem) has been provided. To create a new certificate, download OPENSSL (www.openssl.org) and follow their instructions for installation. Modify the configuration file openssl.cnf and execute (in windows):
'openssl req -new -x509 -nodes -out certfile.pem -keyout certfile.pem -days 999 -config openssl.cnf'.