# reDuhGUI 帮助手册

诺赛科技

网站：http://www.nosec.org

Email：zwell@sohu.com

# 目录

# 一、 简介

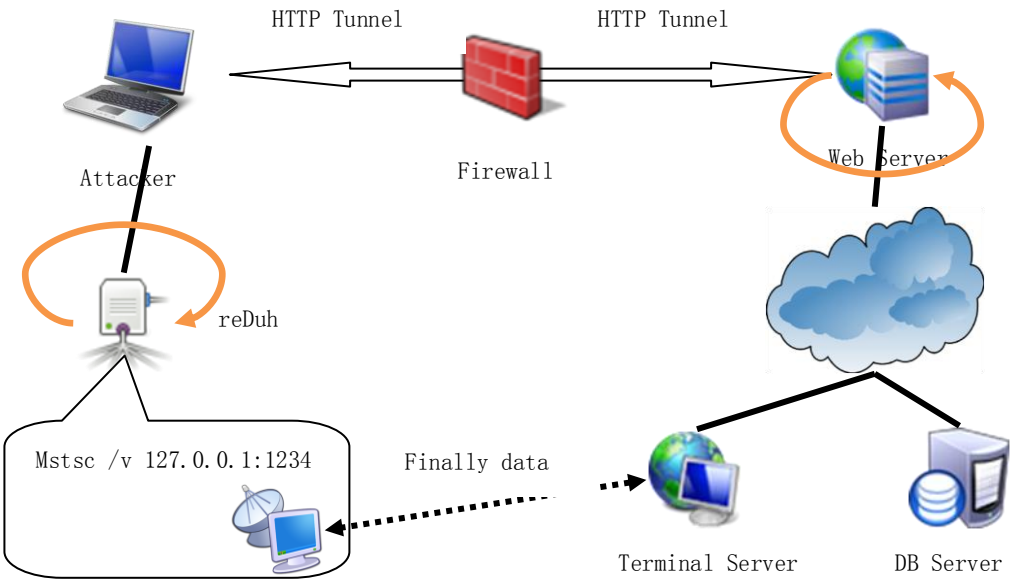
reDuh 最开始是由 SensePost 在 BlackHat USA 2008 会议上发表的一个议题中的一部分。它的出现是针对当前 Web 安全渗透测试经常会面临的一个问题，同时也是 Web 服务器加固方面一个很重要的部分，那就是 Web 服务器对外只开放一个 80 端口。Web 服务器的安全防护可以是操作系统的端口定制或者是网管防火前的端口定制。这时渗透测试人员如果想进一步测试内网的话必须先拿下目标服务器并拥有一定的控制权限。

以前渗透测试人员常用的一些方法是通过上传一些针对操作系统的可执行文件到目标服务器，并且必须要通过进程的方式执行该程序。这就存在两个问题：1、通过渗透测试拿到的权限不一定允许执行进程；2、目标服务器的种类可能很多，比如 Windows、Linux、Solaris 等等，且对于库依赖性比较强，这样就要求渗透测试人员必须维护一个不小的程序库以满足渗透测试的场景。

事实上，我们容易忽略的一点就是，其实脚本代码本身就支持 SOCKET 套接字的操作，它完全可以制作成为一个 SOCKET 中转代理（当然这也是有一定的限制的，就比如在 PHP 中需要启用 SOCKET 模块）。那么这种代理是可以直接绕过防火墙进入到内网的。我们举个现实生活中比较常见的例子说明：A 是一台 web 服务器，B 是与 A 在同一内网一个文件服务器，由于工作需要及简化操作，B 的文件访问是对内网公开的，也就是没有任何的认证要求。同时为了保证 B 服务器的安全性，在网关防火墙上做了端口过滤：只允许外网访问 A 的 80 端口。这时我们如果想要从测试点访问 B，传统的做法是控制 A，上传执行文件，做一个程序级的端口转发器。假设目标服务器根本就不允许从 web 上来的请求执行程序，换句话说是不允许执行进程，那么我们就没有办法拿到 B 的文件了吗？这里，我们就可以想到 reDuh 了。

# 二、 工作原理

我想大部分的测试人员都理解什么叫端口转发，说白了，reDuh 就是一款由脚本（asp; php; jsp）实现的端口转发器。其实这个转发器通过了两次中转，我们下面以远程桌面服务连接做个图例说明：




由图示上我们也可以看出，从 MSTSC 客户端到目标的 Terminal 服务器中间其实是走了一个这样的流程：

Mstsc 客户端-->reDuh 代理-->HTTP tunne-->Web 服务器-->Terminal 服务器

当然，对于 MSTSC 客户端而言，这些过程都是透明的，我们只需要在 MSTSC 中指定连接的端口为本地 reDuh 监听的端口即可。

# 三、 reDuh GUI

reDuh GUI 是由诺赛科技从原有的 JAVA 语言上移植到 C++语言的一个 Windows GUI 版本，具有如下一些特性：

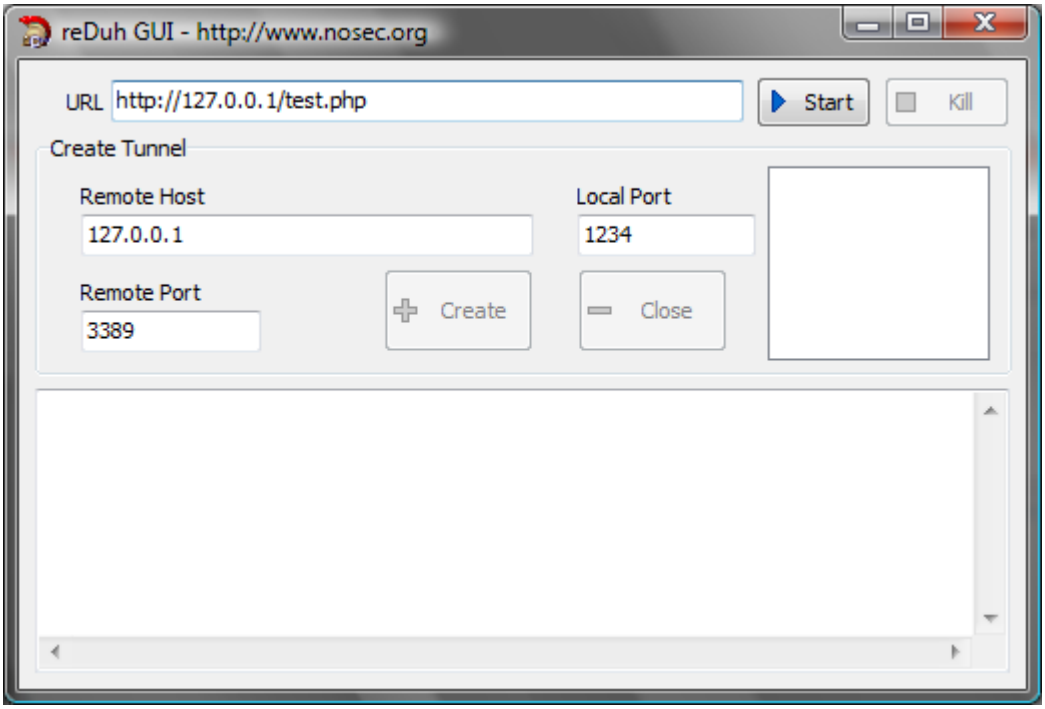
- 不需要 JAVA 运行环境
- 可视化操作
- 支持 HTTP/HTTPS
- 支持二级代理

未来的一些特性准备

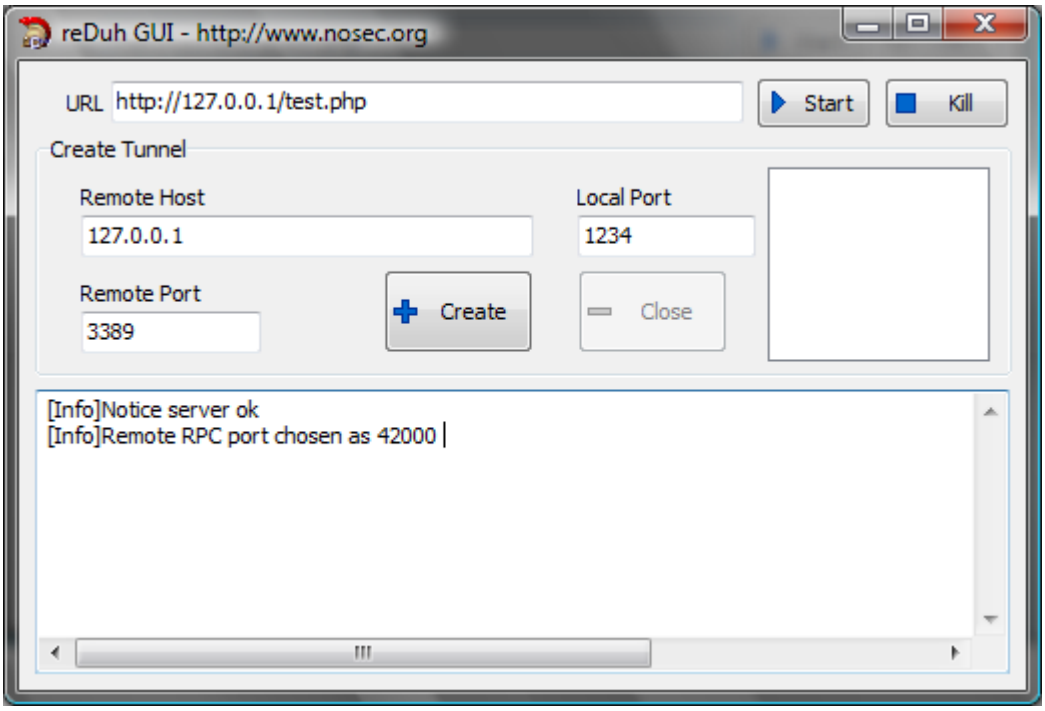
- 优化速度，在原有基础上加速 50%
- 加入连接认证功能

# 四、 软件使用

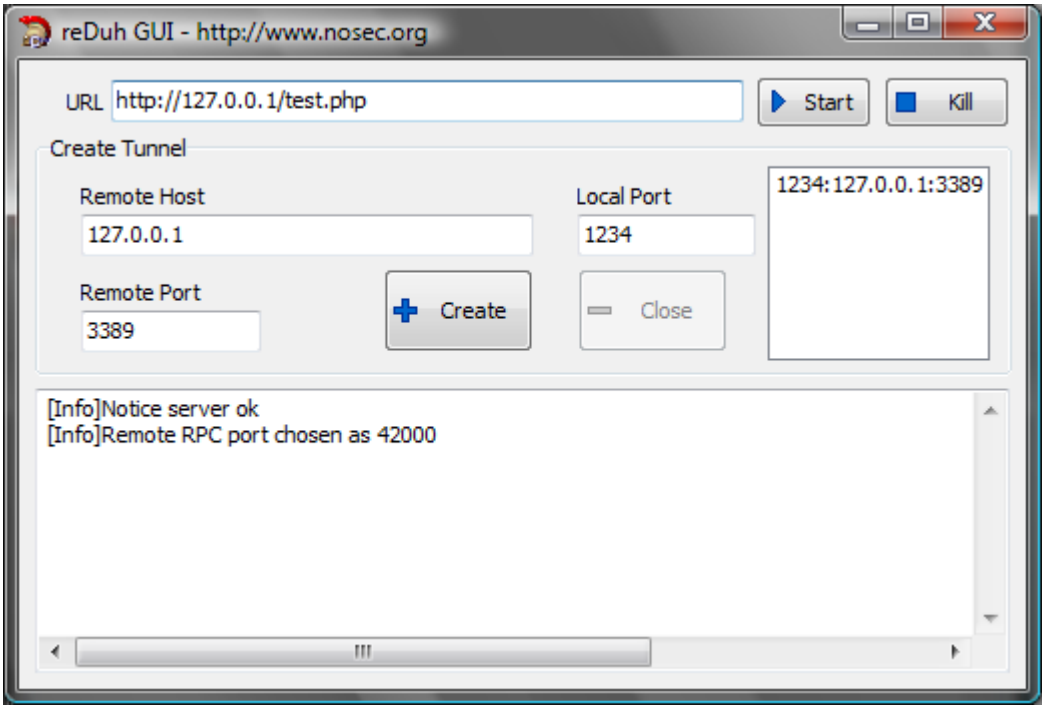
1) 运行 reDuhGUI 程序，出现如下界面。在 URL 输入框中输入 reDuh 的地址，点击 Start 按钮：



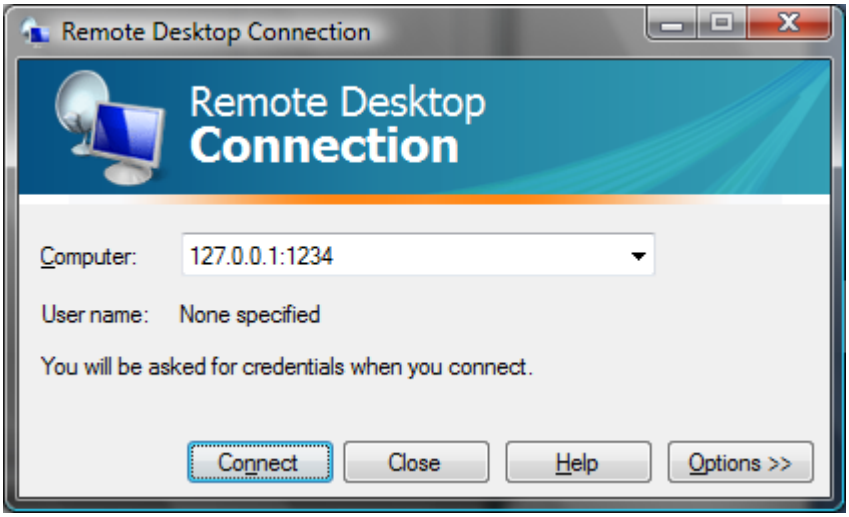

2) 如果目标 URL 存在且工作正常，那么界面上会变成如下的样式，我们可以看到，Create 按钮的状态变为可用，这是，我们在 Create Tunnel 中输入目标服务器需要连接的地址和端口，以及本地监听的端口号，点击 Create 按钮。这里需要注意的是 Remote Host 的地址不是目标服务器的 IP 地址，而是目标服务器可以访问的任意地址，假设目标服务器的地址为 10.10.10.10，那么如果 Remote Host 为 127.0.0.1，其实就相当于连接服务器上的地址；如果 Remote Host 为 10.10.10.11，那么相当于让服务器去连接内网的另一台服务器：



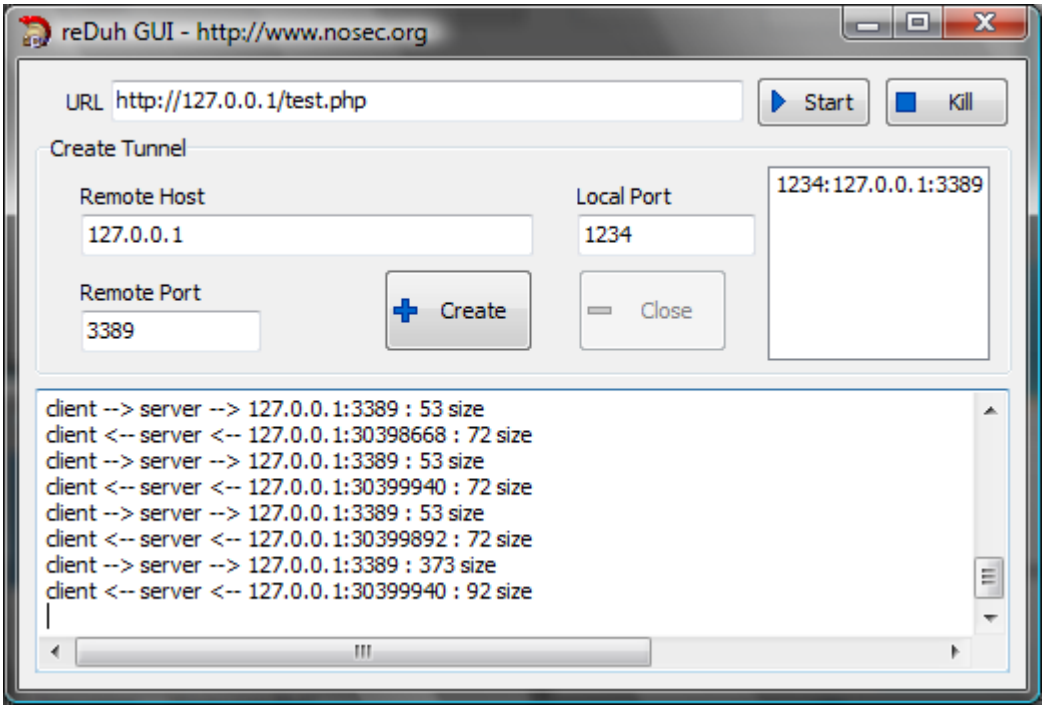

3) 这时界面上会加入一条数据到列表框，说明本地监听到端口 1234，对应于目标服务器连接的 127.0.0.1:3389 端点：



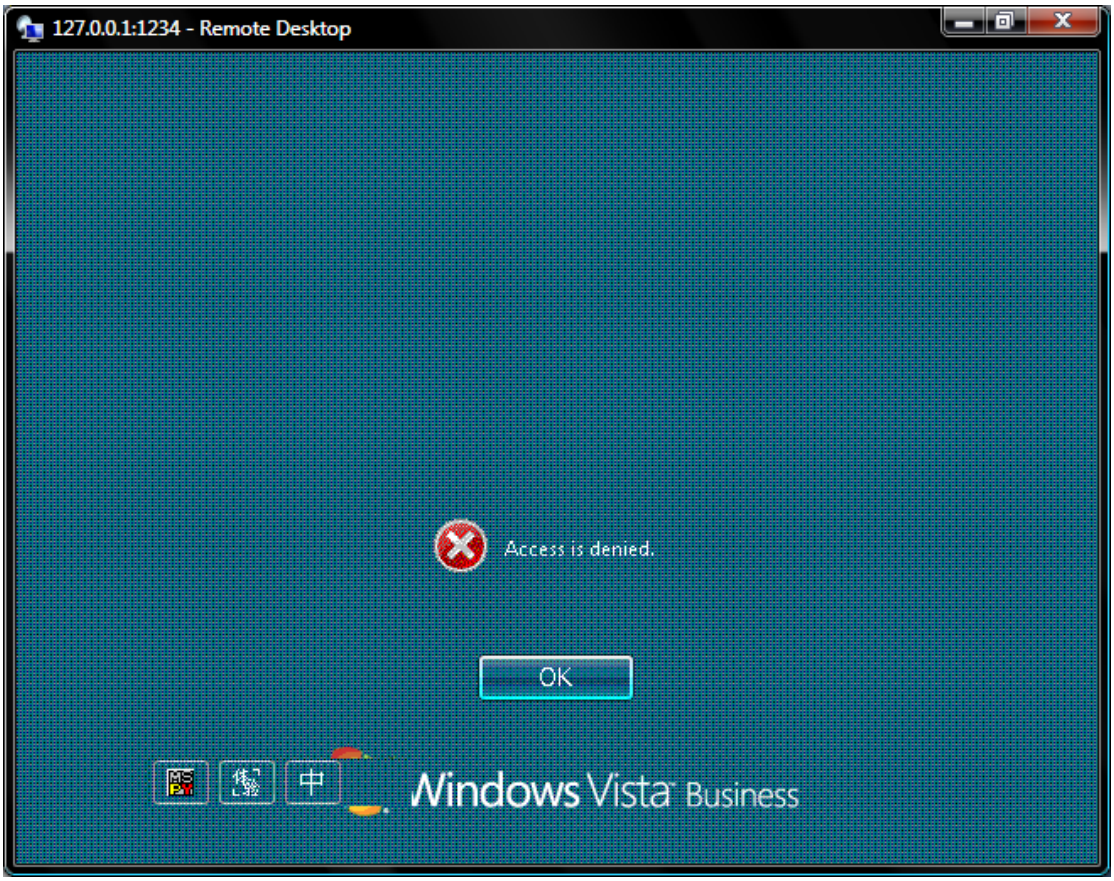

创建 HTTP 隧道成功后，我们可以使用 MSTSC 来进行连接测试，在 Computer 中输入对应的本地监听地址，选择连接：



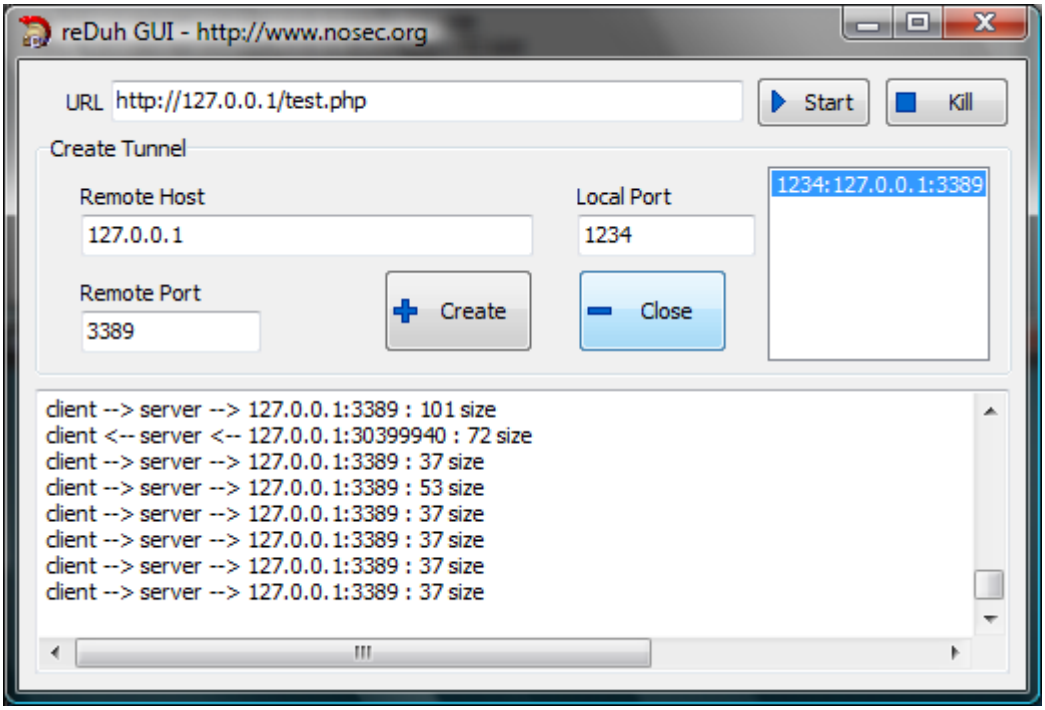

4) 这时我们可以从程序的日志框中查看到大量的数据传输：




5) 在 MSTSC 中能够正常的连接远程桌面：




6） 如果我们完成了操作需要断开时，可以在右边的列表框中选择一项，然后点击 Close 按钮完成某条链路的销毁； 如果想完全断开当前的连接，可以点击 Kill 按钮：



# 五、 参考资料

- reDuh GUI 的官方网站地址：http://www.nosec.org/reDuh
- 官方网站地址：http://www.sensepost.com/research/reDuh/

# 六、 关于诺赛科技

诺赛科技是全球领先的Web 业务安全技术产品和服务提供商，专注于与各安全公司、企业建立长期合作伙伴关系。

我们拥有富有激情的专家团队和强大的研发能力，快速响应客户需求，提供具有竞争优势的产品和专业的服务，助力客户商业成功。诺赛科技为信息安全专家提供专业的安全测试技术及工具，帮助客户发现网络中存在的各种安全隐患，从而最终保障信息数据的安全性。

目前，我们的客户已经遍布世界各地，包括：中国大陆，中国台湾，美国，英国，西班牙，澳大利亚，新加坡，德国，以色列，巴西，印度等。行业覆盖：金融、电信、服务业、政府等。

愿景

为中小企业的业务与网络安全保驾护航

使命

聚焦客户关注的挑战和压力，提供有竞争力的安全评估方案和服务，持续为客户提高投资回报率。

以客户为中心的战略

为客户服务是诺赛存在的唯一理由；客户需求是诺赛发展的原动力。

产品专业、服务专业、购买成本低，优先满足客户需求，提升客户竞争力和赢利能力。

与友商共同发展，既是竞争对手，也是合作伙伴，共同创造良好的生存空间，共享价值链的利益。

更多信息请联系我们：

邮件：sales@nosec.org

MSN：zwell@yeah.net

QQ：27592430