

GFI LANguard 的使用

GFI LANguard 网络安全扫描器是一个漏洞扫描工具，主要致力于告知你，在你的电脑环境中，可能会在哪里存有问题。 它的扫描功能和过滤功能都是非常令人惊讶的，并且可以让你从桌面上收集非常多的相关信息。 一旦收集到了信息，你可能需要对它采取行动。 这就是需要工具集出马的地方了。

可以支配哪些工具？

可用的工具如下所示，你可以在浏览器树形视图下，在程序的左侧面板，Tools 的下面找到它们



你将看到的这些工具包括：

- ◆Deploy Microsoft Updates（部署微软更新）：允许实施微软的相关更新
- ◆Deploy Custom Software（部署自定义软件）：允许对其他软件进行部署，比如 Firefox。
- ◆DNS Lookup（DNS 查看）：允许对你的网络上的机器名进行解析。
- ◆Traceroute（追踪路由）：显示到达某台主机所经的路由信息。
- ◆Whois: 互联网 “Whois” 引擎，用于查询。
- ◆Enumerate Computers（枚举电脑）：一个实用工具，用于列出某个域中的所有电脑。

- ◆Enumerate Users（枚举用户）： 一个实用工具，用于列出某个域中的所有用户。
- ◆SNMP Audit（SNMP 审核）： 对于指定的主机，鉴定弱 SNMP 共有字符串。
- ◆SNMP Walk（SNMP 行走）： 探测你的网络以获取 SNMP 信息
- ◆SQL Server Audit（SQL 服务器审核）： 对 SQL 的账户执行基于字典的攻击。

部署微软更新

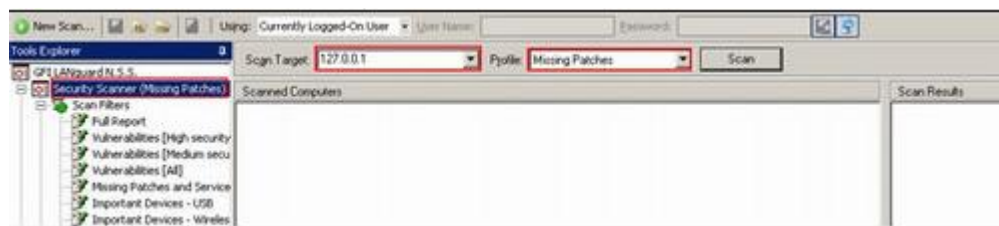
到目前为止，我们所有人看到的 Windows Update，都是一个自动执行来自微软补丁安装的服务。但是，微软其实还有另外一个免费服务，叫做“Windows Server Update Services（Windows 服务器更新服务）”，可以直接帮助完成企业级别的补丁更新工作。

WSUS 是一个很好的工具，但是有时候在服务器架上没有足够的空间来存放，或者预算不足以购买另一台服务器，来专用于监控 Windows 以及 Office 的补丁。这时，LNSS 就可以帮得上忙了。通过进行错漏补丁的扫描，你可以收集整理出所需补丁的项目列表。关于 LNSS 之中的微软更新工具，最棒的事情就是它可以被设定为定期执行，就像使用 WSUS 进行部署一样，只不过当事情发生时，需要有更多一点的控制罢了。

作为一个示例，我们会扫描一台单独 PC，扫描一下错漏的补丁，看看是否需要更新什么。你应当执行下述步骤：

1. 在 LNSS 左侧面板上点击“Security Scanner（安全扫描器）”节点。
2. 选择一个扫描目标。（就本例而言，我输入了 127.0.0.1，这样我们扫描的就是我的本地电脑）。
3. 选择“Missing Patches”类型文件。

你的屏幕看起来应当是类似图这样，所有的项目都设置好了。



一旦扫描所需的设定都配置完毕，点击“Scan（扫描）”按钮，开始分析指定系统。当扫描完成后，你会在已经扫描过的电脑面板上，看到类似图这样的情况。



在你选择漏洞列表项目时，项目的扫描结果将显现在中间面板的右半侧，显示在被扫描电脑上找到了哪些错漏调的更新。扫描结果如图所示。



要为这些错漏的补丁，执行相应部署的话，右键点击屏幕左侧的漏洞列表项目，或者右键点击任何一个被发现错漏调的补丁。选择“Deploy Microsoft Updates（部署微软更新）”，然后选择“On Selected Computers（在被选中的电脑上）”。

一旦你已选择了打算如何部署更新，控制台屏幕会改变为显示部署选项，如下面的图 E 所示。当部署微软更新的时候，LNSS 会分别处理补丁和 Service Pack

包。 基于这个理由，任何要被部署的 Service Pack，都将需要被安排从补丁中单独分离出来。



当这个屏幕打开时，被选中更新的状态会显示出来。 如果更新文件尚未被下载，右键点击它们，然后选择“download（下载）”，即可从互联网上下载相应的更新文件。 当文件下载时，你就可以为这次部署设定其他选项了。 如屏幕底部所显示的，是计划立刻实施此次部署，或是在指定的日期和时间下再进行部署的相关选项。

仅在你非常确定要进行的更新肯定不需要重新启动的情况下，你才可以使用“deploy immediately（立刻部署）”。

你可以使用“Deploy on”框（如图 F 所示），以指定在业余时间，或者是在周末才进行更新。 LNSS 将安装和开启一个服务，以便处理在选中的客户机上的相关更新，并在任务完成后，将其自身再从客户机上移除。



在按下 “Start（开始）” 按钮之前，还有另外一个选项面板可以进行设置，但这不是必需的。在部署屏幕上，LNSS 控制台的最右侧，是选项板。其 General 页面如下文的图所示。



这里你可以告知 LNSS，是否应当在部署之前对用户提出警告。一般情况下，我会去掉这个选择，以免去不必要的询问，或者是为了在工作以外的时间才进行相应更新。

你也可以在部署之前停止被选中的服务。举例来说，如果你是在部署一个 SQL 服务器补丁，需要先停止 MSSQLSERVER 服务的话，那么这个功能就能助你一臂之力。

你能做的另一件事情是强制重启，并选择一台满足指定过滤要求的电脑。也许，你只是不想那些更新被发送到运行 Windows 95 的电脑上罢了。所有这些可选的项目都可以在 Options（选项）面板中进行配置。

Advanced（高级）标签允许你修改某个部署的超时期限，并可以指定备用的信用凭据，以防在需要你是系统管理员时，你使用的却是某个普通权限的帐号。

你也可以为 LNSS 设定，一次部署中的线程数量是多少。GFI 推荐最多不要超过 5 个线程，5 个是默认的。

在 Download Directory（下载目录）标签上，你可以指定一个目录以存放下载的补丁，或者你可以设定 LNSS 和一台 WSUS 服务器协同工作。

一旦你的部署所有配置都做完了，就可以点击“Start（开始）”按钮了。如果该部署是被安排立刻执行，那你就可以看到控制台窗口开始活动了。如果它被安排过些时候再执行，那么到时候定期程序会出现，并由 LNSS 监控器执行。