Linux 安全宝典

Linux 安全宝典

从各个层面来讲，Linux 的使用中都充斥了各种安全威胁，我们要如何建立一个更加安全的 Linux 环境呢？我们要运用哪些工具来阻挡层出不穷的安全威胁？我们要学习哪些技术来抵抗外界攻击的侵袭？在这个关于 Linux 安全的专题中，我们综合了多个 Linux 专家的意见，针对 Linux 安全这一热门话题，提供技术、工具和操作实践的指导。

Linux 安全漏洞解决方案

在 Linux 环境中，大大小小的安全漏洞隐藏其中，小的造成使用中的不便，大的则危害到隐私信息的泄漏或是造成运用瘫痪。这个老大难的问题，我们究竟要如何解决呢？有没有方法能让我们减少为些而生的烦恼呢？

- 潜伏在你身边的 Linux 安全漏洞
- Linux Web 系统上常见安全漏洞浏览
- 使用 BackTrack 检查 Linux 安全漏洞

SELinux 解析

SELinux 是 Linux 中很重要的工具之一，它对加强 Linux 的安全有着不小的功劳。本专题中，我们将全面解析 SELinux——SELinux 是什么，怎么部署，怎么安装？这将帮助你更加了解 SELinux，这些知识也会让你的 Linux 环境更为安全。

- SELinux：简介安全性能更好的 Linux
- 实施 SELinux 的操作技巧
- 红帽企业 Linux 上的 ModSecurity 防火墙安装指南

Linux 安全问题汇总

运用 Linux 的过程中，总有这样那样的问题出现。我们结合实践经验，总结了一些实践操作中常见并难以解决的问题，希望我们提供的解决方法能够帮助您解决运用中出现的各种问题。

- 如何运行与使用 OpenVAS 客户端?
- 实战：如何安装 OpenVAS?
- 如何使用 OpenSSH 在 Linux 上实现安全网络通道
- 如何安装和配置 Puppet Dashboard?
- 如何将 Puppet 报告导入 Puppet Dashboa?
- 如何运用网络映射器（Nmap）助力 Linux 管理与安全?

潜伏在你身边的 Linux 安全漏洞

在本文中，我将和你们分享一些现实世界中的 Linux 安全漏洞。

通常最简单的漏洞旨在从 Linux 系统中取得没有受保护的 NetBIOS 共享资料。有缺陷的 Samba 配置文件通常很容易泄露。例如，文件共享创造为了方便起见，也可能结束了你的困扰。我曾见过基于 Samba 的 Linux 系统分享那些给所有在网络中的人访问敏感信息的资源，这些敏感信息包括病人健康记录和有详细信息（例如：基础设施系统的密码和源代码等）的网络图。。

一些攻击执行起来非常简单。所有执行这些事情的人都要以正常的 Windows 用户权限登录到网络（即使没有管理员权限），运行一个像 GFI LANguard 一样的网络安全和漏洞扫描工具，然后再运行一个类似 FileLocator 的信息搜索工具。这样一来，任何人想要获得一些不该被访问的机密文件就真得相当简单了，并且这永远不会被人察觉。

相关的攻击只针对不善配置 FTP 服务器的使用者，他们的服务器允许匿名连接或者设置安全级别弱的密码，甚至不设密码。在这里举一个例子来说明：

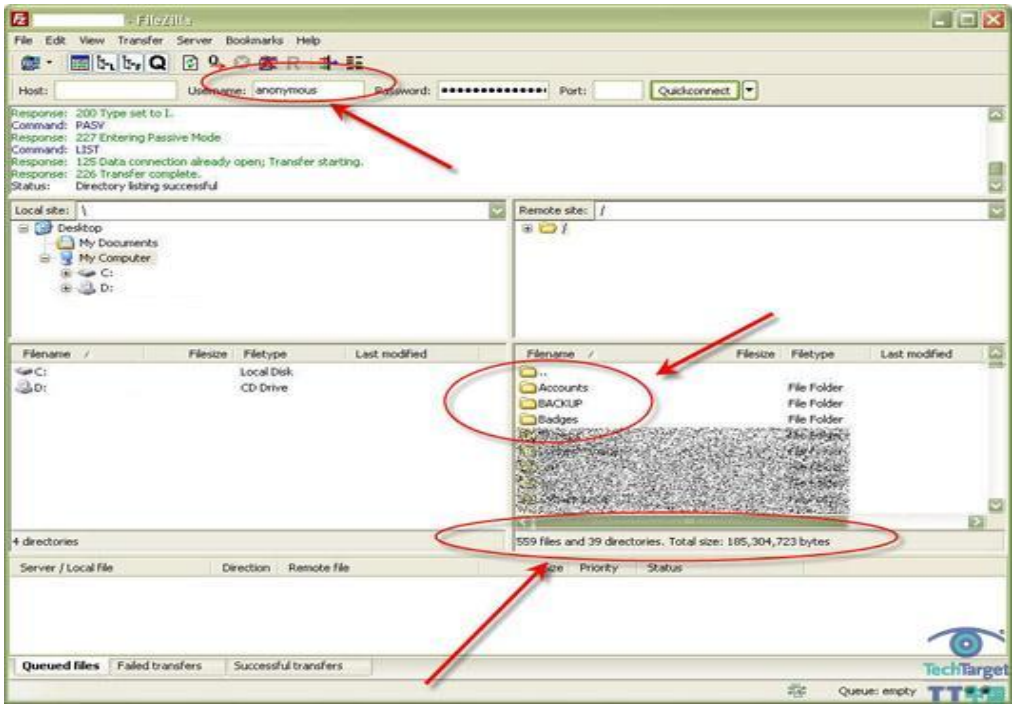


图 1：在 Linux 系统中匿名 FTP 导致数据被访问

在这种情况下，提供匿名 FTP 访问配置文件，以此从财政管理数据库的编码中获得了密码，知道在那里可以获取所要的信息。

另一种 Samba 利用可能导致远程用户的枚举。当一个 Linux 系统的 Samba 配置允许访客访问的时候，像 Nessus 和 QualysGuard 一样的漏洞扫描器能够收集用户名。在大多数情况下，攻击者能够使用这个用户名，在随后的密码破解中对 Linux 的账户进行攻击。在许多情况下，你也能够使用类似 WebInspect 或 Acunetix 的网络漏洞扫描器通过一个安装不完善的 Apache（即没有在 httpd.conf 中禁用 UserDir 指令）来收集 Linux 用户的账户信息。

关于密码的话题，我最近曾经看到过这样的情况，CGI 应用程序运行在基于 Linux 的 Web 服务器时，没有正确的过滤输入信息，并且在 HTTP 查询中允许包含本地文件，如图 2 所示。

图 2：网站输入验证问题可能会导致 Linux 文件被访问

在这种特定的情况下，通过 Web 应用程序返回的 Linux 密码文件中，就会泄露数以百计的用户账户。虽然这个密码屏蔽，但破解系统的密码仍然容易，因为所有的用户账户都是已知的。这种类型的攻击也可能会导致其它的 Linux 操作系统和数据文件易于暴露。

最后，如果我没有提及补丁问题的话，那么我是失职的。论证表明，它是导致最坏结果的最易利用的漏洞之一。这适用于操作系统和第三方软件。例如在这种情况下，攻击者在连接到互联网期间的短短几分钟之内，就可以通过使用 Metasploit 之类的免费工具来获得如图 3 中的操作系统的所有权限。

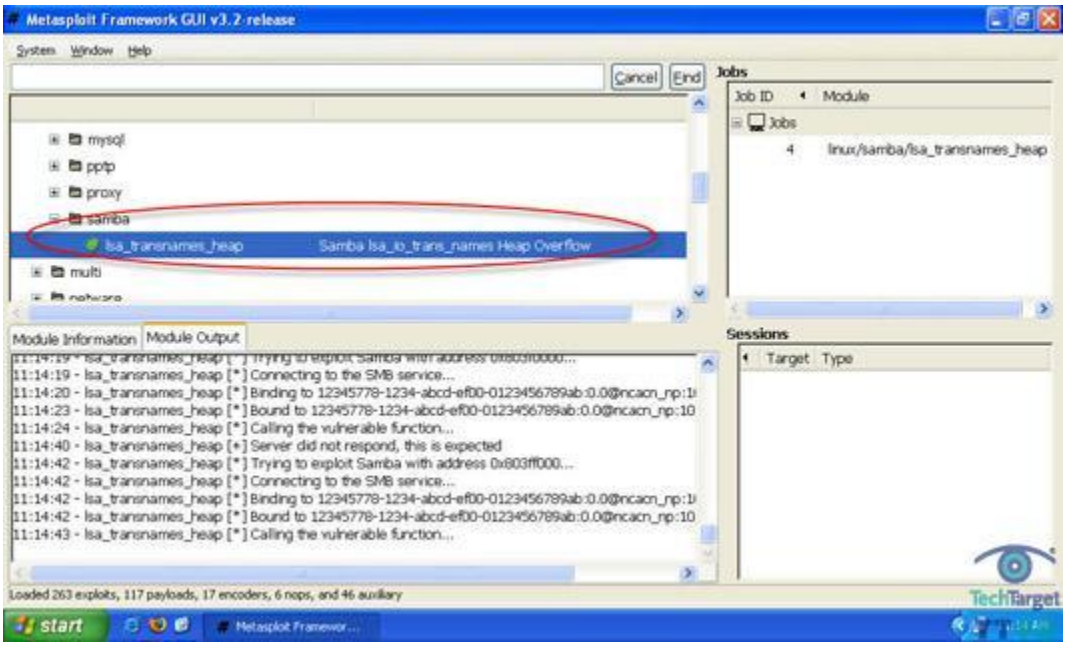


图 3：使用这个 Metasploit 工具来利用过期版本的 Samba

同样，在大多数情况下，直到为时已晚，没有人会知道这样的攻击。

有时你会发现 Linux 内核本身没能识别出有些漏洞，但是它们仍然会被利用，产生更多的 Linux 系统问题。执行 Linux 漏洞检查时，别忘记尽可能从每一个角度查看一下你的 Linux 系统。只是因为一些问题不能从外部利用并不意味着不能被所谓的“值得信赖”的人通过正常的登录方式登录后滥用。此外，因为在风险报告并不能把系统环境中的每个安全隐患都一一列出，你需要有保留地采用自动扫描工具获得一些发现。从剩下的电子干扰讯号中筛选出重要的东西只会让你投入太过，并且给你带来更多的麻烦。

（作者：Kevin Beaver 译者：Mark 来源：TechTarget 中国）

原文标题：潜伏在你身边的 Linux 安全漏洞

原文链接：http://www.searchsv.com.cn/showcontent_39372.htm

Linux Web 系统上常见安全漏洞浏览

在执行漏洞评估和渗透测试时，我们通常纠结于操作系统级别的漏洞，最终忽视了 Layer 7 问题。由于在远程登录和 SSH 的 Linux 系统上存在许多攻击面，因此这是一个非常危险的陷阱。事实上，在我看来，多数基于 Linux 的缺陷位于应用层。可能是 Apache、PHP 或 OpenSSL，或者只是一般的错误配置，如果漏洞可以通过 HTTP 访问，那就更危险了。

常见的漏洞有 SQL 攻击和跨站点脚本，对于 Linux Web 安全来说还有更多。下面列出的是我经常看见的基于 Linux 的系统上的其他 Web 安全漏洞，供你参考，便于降低与 Web 相关的风险：

PHP 代码入侵会允许恶意代码直接执行。我见到过服务器端脚本引擎接受未过滤的 PHP 输入，运行在服务器上，提供系统级别的服务器访问。

使用 HTTP GET 请求而不是 POST 请求通过用户名和密码。这个缺点能造成允许 Web 应用和操作系统级别的特权扩展。

密码弱连同入侵者锁定的缺少。我曾发现使用自动的密码破解者，如 Brutus 和旧有的登录猜测器，通常，当出现弱登录时，获取在 Web 站点或应用的未授权访问非常简单。

弱的文件和目录权限会允许系统列举。我常发现备份或测试文件包含旧有和未经维护的代码，提供了不是每个人都需要看见的信息。

（作者：Kevin Beaver 译者：唐琼瑶 来源：TechTarget 中国）

原文标题：Linux Web 系统上常见安全漏洞浏览

原文链接：http://www.searchsv.com.cn/showcontent_33470.htm

使用 BackTrack 检查 Linux 安全漏洞

无论你是否用过 Bastille UNIX 工具，以便手动加固你的 Linux 系统，或者只是想对目前系统的状态进行快照，你需要使用 BackTrack。这是款基于 Slackware Linux 的版本，通过启动 CD 或虚拟机镜像（VMI）运行。在官方的第三个版本（如果你计算最新发布的就是第四版），BackTrack 含有方便的安全工具，用于检测 Linux 系统里的漏洞。本着“黑客入侵”的精神，BackTrack 集成这种通常的安全测试方法：

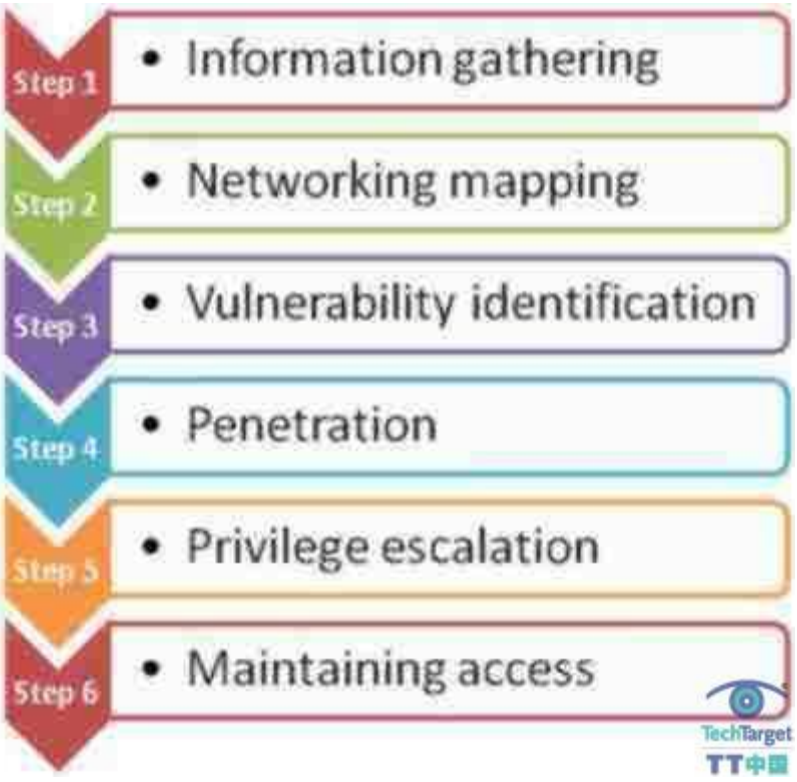


图 1：BackTrack 的安全测试方法

BackTrack 包含利基安全工具，很难下载、编译和安装。无论你是 Linux 技术专家或新手，很难下载完整版本的 Linux 与安全测试工具。BackTrack 的主要接口如下图所示：

图 2：BackTrack 桌面和安全工具目录

使用 BackTrack 测试内部 Linux 系统的常用安全评估情景如下：

1. 使用 fping 识别活动主机
2. 使用 nmap 识别操作系统和检测打开的端口
3. 使用 amap 识别正在运行的应用
4. 使用 SAINT 查找操作系统里的漏洞
5. 使用 Metasploit 开发操作系统和应用漏洞

Linux 的集中可能性是无穷的。此外，BackTrack 包括广泛的数据库、Web 和无缝工具的设置，用于查找和挖掘 Linux 宣称之外的系统缺陷。它甚至包含内置的 HTTP、TFTP、SSH 和 VNC 设备，在漏洞验证和

分析期间使用。并且，如果你有这样的需求，BackTrack 也能集成数字取证工具。事实上，使用 Autopsy 和 Sleuthkit 这样的工具对于“倒回”黑客技术，进一步坚强的你安全技能是很好的。

我一直是使用好的商业安全测试工具的支持者，不过你可能不再使用付费工具。实际上，BackTrack 工具不止是够好，她其实非常不错，尤其是精心的报道和正在遭遇漏洞的管理不是你首要考虑的。我将继续在安全评估方面使用商业工具。

（作者：Kevin Beaver 译者：唐琼瑶　来源：TechTarget 中国）

原文标题：使用 BackTrack 检查 Linux 安全漏洞

原文链接：http://www.searchsv.com.cn/showcontent_29142.htm

SELinux：简介安全性能更好的 Linux

可以说，今天 IT 领域的最热门话题之一就是安全。在谈到 Linux 系统的时候，安全加强型 Linux（Security-Enhanced Linux，SELinux）毫无疑问总是人们讨论的话题之一。本文中，我也将讨论一些这方面的问题：什么是 SELinux，它到底能为你做些什么？它有哪些局限性？你该在你支持的 Linux 版本上启动 SELinux 吗？它有什么新的功能，实施 SELinux 的最好办法是什么？

SELinux 是由美国国家安全局开发的， 最初用来提供强制访问控制（通过使用 Linux 安全模型）。这种开发改变了 Linux 内核，实际上加强了安全控制。2000 年，SELinux 首次发布（遵守 GPL 协议），实际上到 2003 年八月它融入了标准 2.6 内核。启用 SELinux 有助于减少应用程序以及其他用户程序受到损害的风险。它有助于防止恶意程序或者写得不好的程序对整个系统带来危害。要理解 SELinux 其实并不是一个 Linux 版本，这个概念很重要。它现在集成在 2.6 内核中---许多 Linux 版本都支持这个功能，但并不是所有 Linux 版本都支持。SELinux 的实质是访问控制、完整性控制、基于角色的访问控制（RBAC）以及强类型的架构。换句话说，它包含了改进的内核、一套核心库、以及功能改进的程序包和一个策略配置。

SELinux 到底是用来做什么的呢？这是一个重要的问题。首先，它的目的是根据你设定的规则加强数据分离。这种配置将有助于防止不必要的进程访问你的数据。通过这种方式，它可以根据系统授权定义的不同安全要求来隔离单个主机系统。

哪些 Linux 版本支持 SELinux 呢？许多版本中集成了 SELinux，人们只需要开启 SELinux 功能就可以使用。有些 Linux 版本可以通过安装可选程序包来集成 SELinux 功能；但如果我的 Linux 版本中不包含 SELinux，我不会使用 SELinux。支持 SELinux 的 Linux 版本包括：Red HAT、Debian 和 Fedora。值得注意的是 SUSE 和 Slackwaredo 并不支持 SELinux。

SELinux 有哪些竞争对手？

它可能的主要竞争对手是 AppArmor（它们两者都遵守 GPL 协议）。AppArmor 最大的分销商是 Novell SUSE。Novell 公司收购 Immunix 之后就把这个产品集成在它的 SUSE 版本中。AppArmor 最重要的功能是什么？一个很简单的功能，但是 SELinux 里面没有。你只需要点击几下鼠标就可以创建一个配置文件，并且 YaST

控制中心还可以管理这个文件。AppArmor 与 SELinux 之间根本的技术区别是：AppArmor 通过路径识别文件系统目标，而不是通过信息节点。

SELinux 中有哪些新东西？下面是 2008 年六月发布的最新版本中的亮点：

- 新增支持用户和角色重置。这主要是为 libsepol 提供的，可以选择使用。
- checkpolicy 中专用的角色控制
- libsepol 和 checkpolicy 中新增支持策略能力
- 通过 libsemanage 和 libsepol 减少内存使用
- libselinux 中新增 avg_opne 界面

下篇文章中，我们将为您提供一些实施 SELinux 操作中的技巧。

（作者：Ken Milberg　译者：Dan 来源：TechTarget 中国）

原文标题：SELinux：简介安全性能更好的 Linux
原文链接：http://www.searchsv.com.cn/showcontent_39191.htm

实施 SELinux 的操作技巧

上篇文章中，我们已经简单介绍了作为性能更好的 Linux 的 SELinux，本文中，将为您提供一些实际操作中解决问题的小技巧。

我需要 SELinux 吗？

我想说的是，我知道许多系统管理员在启用这个产品之后，眼睁睁地看着所有的应用程序迅速死亡。实施 SELinux 是一项工程。如果你想要你的应用程序在这个环境中运行，那么就不要想方设法的减少工作量。如果你想在产品环境中运行，我强烈建议你让一个专职 SELinux 系统管理员在这个错综复杂的系统中进行充分的培训。不要在开启 SELinux 以后还期望所有的事情都像以前那样正常工作，或者认为只需要进行简单的调整就行了。如果你这样做，我向你保证，你很快就会被炒鱿鱼。在现今世界里，安全性变得越来越重要，而可用性则位居次席。SLA（服务等级协议）通常要求系统全天候工作，而且用户不想听到任何安全故障。

实施 SELinux 的最好办法是什么？

我曾成功使用的方法是要确保你有多个环境。其中包括：一个沙盒、一个开发环境和一个 Q/A 或者一个试验性生产环境。在这种情况下，开发团队应该首先让 SELinux 在沙盒环境中正常工作。这个沙盒可能装载了一些基本的应用程序，但是 IT 人员（如系统管理员）可以决定装载哪些应用程序。我认为有这样一个环境非常重要。为什么这么重要呢？因为系统管理员可以尽情地在沙盒中折腾，这意味着他们可以破坏系统，但是不会带来任何影响。当 IT 人员已经了解了足够多的知识，并且已经能让核心应用程序在 SELinux 中工作的时候，你就可以进行环境循环，这类似于人们配置操作系统补丁或者配置应用程序新版本。这个开发环境通常由开发人员掌握。虽然他们可能不会因为你想限制他们的活动而紧张，但是如果实施 SELinux 是公司的一个政策，那么他们在跟你合作这件事上不会有太多选择。

你让应用程序在沙盒中正常运行之后，你可以继续进入 Q/A 或者试验性生产环境。我认为，在这个组合测试中要包括单元/系统测试以及 UAT 测试，而在经过严格的测试之后，你就可以进入生产环境了。单元/系统测试是指基本系统功能测试，而用户接受测试（UAT）包括用户实际使用系统，确保系统的核心功能可以正常工作。正如你看到的，这需要很大的努力，但是这些的确是实施 SELinux 系统时必须要做的工作。

总之，虽然我肯定会建议你要制定强大的安全政策，但是我建议你在使用SELinux 这种产品之前需要多加小心。虽然成功部署可以实现，但你需要像对待真正的工程一样对待 SELinux 的实施过程。你在实施中花费适当时间会改进应用程序的可用性、带来用户认可的系统安全性，这些好处会给你带来十倍的回报。

（作者：Ken Milberg 译者：Dan 来源：TechTarget 中国）

原文标题：实施 SELinux 的操作技巧

原文链接：http://www.searchsv.com.cn/showcontent_39192.htm

红帽企业 Linux 上的 ModSecurity 防火墙安装指南

ModSecurity 是一个开源的 Web 应用防火墙（WAF）解决方案。它基于当前流行的 Apache 服务器，能轻易地部署在大部分基于 Linux 的 Web 应用上。WAF 是应用层的防火墙，用来监控 Web 服务器的访问，以验证访问请求有效且没有非法入侵 Web 服务器的意图。这种用于检测的技术叫做“深层检测“，因为防火墙将在数据包中检测得更深。

典型的防火墙检测方式是基于 IP 地址的，通过协议(TCP 或者 UDP)和端口来判断流量是否为合法的。WAF 通过传统的 IP 和 TCP/UDP，并结合检测流量大小来判断该数据流是否为非法的。深层检测可以通过两种方式来发现异常数据：协议发现和签名。用协议发现，深层检测可以查看协议版本、协议的一致性、无效请求、域名解析检查及其它容易被判断为反常的方法。通过签名，检测某种数据包（比如 HTTP）应该有的负载范围，可以判断黑客攻击具有的特征。例如，对某个特定版本 CGI 程序的请求可能会以 http://www.domain.com/cgi/hacked.cgi?a=4 这样的形式出现，这样就会以它的签名为由被屏蔽。

为什么要用 WAF?

应用防火墙除了能增强安全性外，有些组织还需要它来支持支付卡行业项目，以使其满足 VISA 卡和 MASTER 卡要求的支付卡行业数据安全标准（PCI DSS）。PCI DSS 要求部署应用防火墙和操作规程来保证安全性。

开源的 WAF 解决方案

目前有两个有名的开源 WAF：Aqtronoxa 和 ModSecurity。Aqtronoxa 可以用 IIS 环境中部署和发布，ModSecurity 则用 Apache 环境。升级转换版的 ModSecurity 可以部署在任何 WEB 服务器上（不要求 Apache）。

ModSecurity 的要求

我建议用 Apache2.2.X 或者更高版本来做 Web 服务器。以下的步骤是假设 Apache 未安装的情况下，将使用最新增的功能来简化安装过程。

DNS 是网页流量和使用 WEB 应用防火墙的基础条件。所以，请确认 DNS 在运行 WAF 的红帽系统中能正常工作。本文档中使用红帽 5.4 版本做为例子，但是实际在 5.3 版本中会运行的更好。

ModSecurity 的安装

在本文档中，我们将在开放了 80 到 8080 端口的服务器上来安装 ModSecurity。WEB 服务器的地址为 192.168.1.5 。

ModSecurity 可以用源代码来安装，它附有详细的安装说明。但是，我还是选择用模块包的方式通过包管理来安装 ModSecurity。

要用包管理的方式，就要选择一个合适的库来安装。这里我选择 Jason Litka 的库。添加一个库到 Yum 让它能够认到 Jason 的库。例如，编辑 /etc/yum.repos.d/utter.repo，并添加以下内容：

```
[utter] name=Jason's Utter Ramblings
Repo                                baseurl=http://www.jasonlitka.com/media
/EL$releasever/$basearch/ enabled=1 gpgcheck=1
gpgkey=http://www.jasonlitka.com/media/RPM-GPG-KEY-jlitka
```

这样 Yum 就可以认到 APACHE 所能安装到的库了：

```
yum install httpd
yum install httpd-devel
```

然后 ModSecurity 就可以用以下命令来安装：

```
yum install mod_security
```

不幸的是用这个办法 ModSecurity 还是需要手动指定一些 ModProxy 的汇编，所以这里要安装一个 gcc 编译器（稍后可以卸载）：

```
Cd /root
wget
http://www.manticmoo.com/articles/jeff/programming/proxy/mod_proxy_html.
c
yum install libxml2-devel     yum install gcc apxs -c -I
/usr/include/libxml2/ -i mod_proxy_html.c
```

其余的可以用以下命令删除：

```
yum erase kernel-headers yum erase cpp yum erase libgomp
```

ModSecurity 需要 libxml 模块，将以下命令添加到 httd.conf 中去：

```
LoadFile /usr/lib/libxml2.so LoadModule proxy_html_module
modules/mod_proxy_html.so
```

添加如下行：

```
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
```

现在可用用 httd.conf 中的以下命令来激活 proxy：

```
<Proxy *>
        Order deny,allow
        Allow from all
</Proxy>
SSLProxyEngine On ProxyPass / http://192.168.1.5:8080/
ProxyPassReverse / http://website.domain.com/
<Location>
ProxyHTMLExtended On </Location>
```

参数 ProxyPass 和 ProxyPass reverse 定义了发送实际数据的位置。默认情况这里会要求填入 Web 服务器负载均衡地址的完全域名。

(作者：Laura E. Hunter 译者：刘波 来源：TechTarget 中国)

原文标题：R2 里的活动目录网络服务新特色

原文链接：http://www.searchsv.com.cn/showcontent_32592.htm

如何运行与使用 OpenVAS 客户端？

与旧版本一样，为了在底层域中引入域控制器（Domain Controller，DC），Windows Server 2008 及 R2 版本需要先利用 Adprep.exe 工具来更新活动目录架构（Active Directory schema）。林准备和域准备两者都必须运行，而每个域都必须运行一次域准备。

Windows Server 所有版本的 DVD 光盘都能找到域控制准备工具。如果你有一个 Windows Server 2003 林和 Windows 2003 域，那么你必须先运行 Windows Server 2008 DVD 光盘中的域控制准备工具，为林中的所有域建立域控制器。如果不这样做，系统会产生错误信息，提示你应先运行域控制准备工具。

但如果域控制准备工具程序本身出错了呢？本文将介绍一个已知的域控制准备工具错误以及相应的解决办法。

域控制准备工具链接标识符错误

运行域控制准备工具期间可能出现的错误会被记录到%windir%\debug\adprep\logs 目录下的日志文件中。在域控制准备工具出错退出之前，错误消息显示为：

有同一链接标识符的属性已经存在。

为了解决这个问题，我们需要了解链接标识符或者说链接 ID（Link ID）是什么。在活动目录架构中，一些对象属性的值是向前或向后链接的。这些存储在“Link ID”中的值，本质上是互相指向对方的两个属性。

“Member”和“MemberOf”两个属性就是最简单的例子。一个组的“Member”属性是一个前向链接，指明了哪些对象是该组的成员。该属性能够被管理员修改，还可以直接复制到其他域控制器中。“MemberOf”属性则是一个后向链接，当前向链接被设置时，该属性的值会被自动计算出来。前向链接的值最终会是一个正的非零偶数，而后向链接则是前向链接数加 1。这些属性的值具体是多少并不重要，重要的是在目录中它们是唯一的。如果不唯一，域控制准备工具运行时就会出现上述错误。任何目录激活（directory-enabled）程序都可以为它们的对象提供链接 ID，但这些 ID 必须是唯一的。微软以前采用的做法是建立一个分配唯一链接 ID 值的机制——类似于对象标识符（object identifiers，OID）——但现在的链接 ID

都是自动产生，并保证是唯一的。（对于开发者来说，还可以选择使用 13800 或以上的值。）

错误信息清晰地指明了域控制准备工具的问题所在。因为我们要安装一个新版的 Windows 系统，它有一些和链接 ID 相关的新对象，所以这些 ID 必须是独一无二的。

下篇文章中，我们将讨论如何解决 Windows Server 2008 中域控制准备工具复制链接 ID 的冲突错误。

（作者：Ronald McCarty　译者：鬼谷　来源：TechTarget 中国）

原文标题：红帽企业 Linux 上的 ModSecurity 防火墙安装指南

原文链接：http://www.searchsv.com.cn/showcontent_39308.htm

实战：如何安装 OpenVAS？

确保您主机的基线安全是很重要的，而其中一个很有用的工具就是网络安全扫描器。网络安全扫描器虽然不如集中的渗透测试，但对于识别简单的漏洞、缺少的补丁、开放的端口以及其它的问题都是很有用的。

Tenable 的开源或商业混合的工具 Nessus，是一款您可能会比较熟悉的网络安全扫描工具。这个工具已经有超过 10 年的历史了，并且从 2005 年开始有了双重发行，并仅对非商业目的的使用是免费的。但工具已经不再是免费的了，并且从 3.0 版开始，不再开源。

自由而开放的网络安全扫描

为了适应 Nessus 的商业化和开源代码的不开源化，开发了开放式漏洞评估系统(Open Vulnerability Assessment System OpenVAS)。最开始，其只是 Nessus 的一个纯 GPL 性质的克隆产物。但现在已经开始了进一步的开发，并扩展了 Nessus 项目所没有的能力和功能。在这里，我们将向您展示，如何去安装 OpenVAS 并进行初步的使用。这是一个很简单的过程。我们将很快让您可以在自己的主机上运行安全扫描。

最新版本的 OpenVAS 3.0.0 是从 Nessus 2.2 克隆出来（Nessus 从 3.0 开始发行自己专有的许可证）。它将一个客户端—服务端的扫描架构和一个图形化的前端结合起来，并可以在多种 Linux、Windows 以及其它操作系统上运行。它可以利用网络漏洞测试或者使用 Nessus 攻击脚本语言(Nessus Attack Scripting Language NASL)编写的网络漏洞测试，其中 NASL 是 Nessus 项目中用于编写测试的语言。

截止到 2009 年 12 月，OpenVAS 项目已经发布了 15，500 个带签名的网络漏洞测试，而这些测试都由一个 GPL 许可进行授权。从 3.0.0 版本起，OpenVAS 从原来的一个漏洞扫描器扩充为了一个完整的漏洞管理解决方案。OpenVAS 现在有了一个模块化的架构并支持一个中心管理扫描服务器和控制台。

安装 OpenVAS

让我们从安装各种 OpenVAS 模块开始。对于 3.0.0 版本来说，有三个核心模块：openvas-libraries、openvas-scanner 以及 openvas-client，以及两个可选

的模块：openvas-manager 和 openvas-administrator。我们将对三个核心模块进行安装。在写这篇文章时，OpenVAS 3.0.0 还没有被打包用于发布。如果您想要一个打包后的版本，那么您只能使用 2.x 分支的发布版本。因此，由于我们没有包，我们将通过源码进行安装。
在编译 OpenVAS 之前，需要先安装一些先决条件。比如说，在 Red Hat 上，我们将需要通过 yum，安装一个编译器，以及下面的一些包：

```
$ sudo yum install gcc glib glib2 glib-dev glib2-dev gpgme gpgme-devel
make bison
     gnutls gnutls-devel libpcap libpcap-devel cmake gtk+ gtk+-devel
```

在 Ubuntu 上，我们需要通过 apt-get 去安装相同的包。这可以通过下载所需的源 tarball，并进行解包来完成：

```
$ wget http://wald.intevation.org/frs/download.php/683/openvas-
libraries-3.0.0.tar.gz
$ tar -zxf openvas-libraries-3.0.0.tar.gz
$ cd openvas-libraries-3.0.0
$ ./configure
$ make
$ sudo make install
$ sudo ldconfig
```

然后，对下面的文件重复这些步骤：

http://wald.intevation.org/frs/download.php/684/openvas-scanner-3.0.0.tar.gz
http://wald.intevation.org/frs/download.php/685/openvas-client-3.0.0.tar.gz

下来，我们需要为 OpenVAS 创建一个服务器证书。

```
$ sudo openvas-mkcert
```

按照屏幕上的指示，去创建您的证书。

现在，我们需要使用 openvas-adduser 命令去为 OpenVAS 的运行创建一个用户。

```
$ sudo openvas-adduser
```

同样地，按照屏幕上的指示，为 OpenVAS 用户提供一个用户名字和用户密码。最后，我们需要安装我们用来扫描的网络漏洞测试（NVTs）。OpenVAS 的命令为：

```
$ sudo openvas-nvt-sync
```

第一次运行会持续一段时间，而且您需要定期地运行它以便收到更新和新的测试。我一般通过 cron，一天运行它一次。

运行 OpenVAS 扫描器

当安装完以后，您就可以运行 OpenVAS 扫描器守护进程：

```
$ sudo openvassd
```

由于守护进程会将所有的网络漏洞测试都加载到扫描器中，所以根据你扫描用的主机的性能，会花一点时间。

（作者：Gary Olsen 译者：Dan 来源：TechTarget 中国）

原文标题：实战：如何安装 OpenVAS？

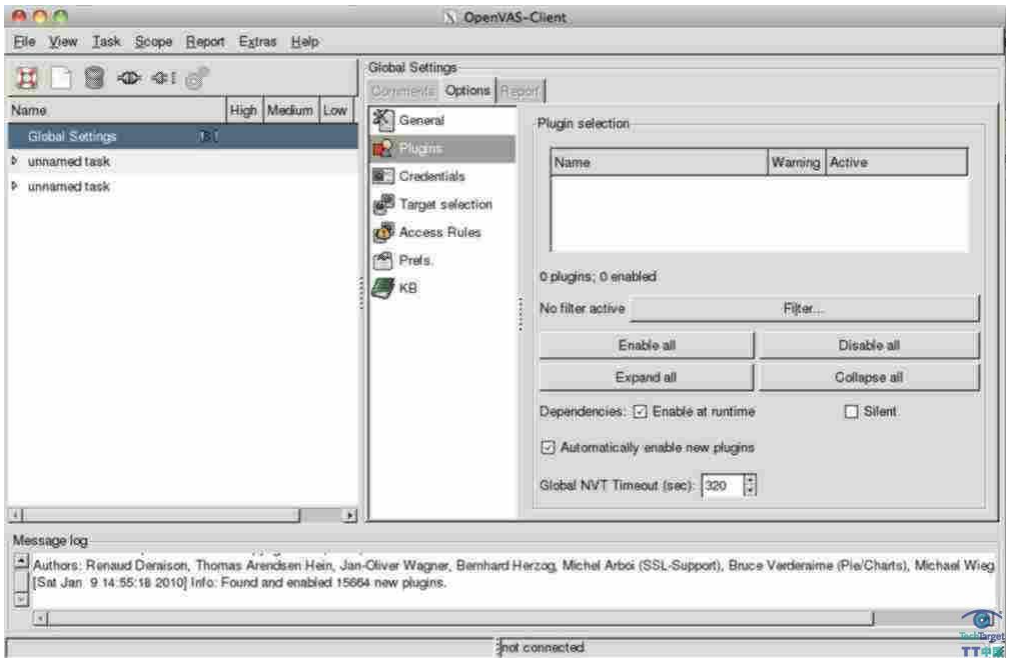
原文链接：http://www.searchsv.com.cn/showcontent_31729.htm

如何使用 OpenSSH 在 Linux 上实现安全网络通道

一旦扫描器守护进程开始运行，您就可以启动一个客户端并连接到该扫描器。我们已经在作为扫描器的同一个主机上安装了客户端，但其实您也可以在任何想要的主机上安装客户端，并远程连接到扫描器。现在，我们运行该客户端：

```
$ OpenVAS-Client
```

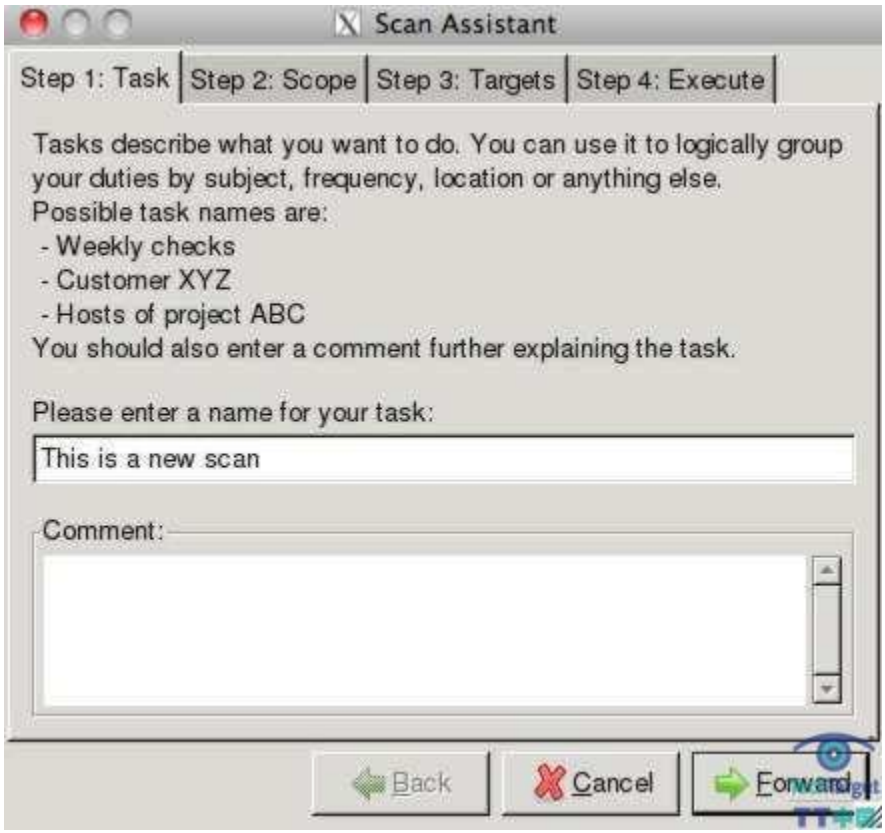
这样就会启动客户端，并显示出来：



这时，您可以选择 File=>Connect 去连接到 OpenVAS 的扫描器守护进程：

系统会提示您指定运行该扫描器守护进程的主机 IP 地址（守护进程在 TCP 端口 9390 上运行，所以您需要确保该端口在任何会造成影响的防火墙上都是打开的）。在我们的例子里，将连接到本机，所以不需要担心这一点。您也需要提供之前创建的用户名和密码。

当已经连接到 OpenVAS 扫描器守护进程之后，您就可以启动扫描。最简单的启动方式是使用扫描器助理，您可以通过客户端的文件菜单对其进行访问，在启动扫描器助理的同时，指定您的目标扫描主机。



这样，您就可以执行扫描，并在 OpenVAS 客户端中查看结果报告。

OpenVAS 资源

我们已经对 OpenVAS 进行了一个很快速的介绍。您还可以探索许多其他的功能，包括编写您自己的网络漏洞测试，以及通过使用新的管理器和管理员模块扩展 OpenVAS 的能力。

如果您有 OpenVAS 的相关问题，可以参考 OpenVAS Compendium 去获取更多的信息（尽管一些文档仍然是针对 2.0.0 版本的，并没有依据 3.0.0 版本进行相应的升级）。您也可以在 OpenVAS mailing list 上获得帮助。如果您不能为问题找到答案，可以使用 OpenVAS bug tracker 对其进行记录。

OpenVAS 同样处于积极的开发过程中。您可以通过阅读 Roadmap 学到 OpenVAS 新的功能和方向，并且您也应该订阅 OpenVAS-Announcement mailing list 进行更多的学习。

（作者：James Turnbull 译者：刘波 来源：TechTarget 中国）

原文标题：如何运行与使用 OpenVAS 客户端？

原文链接：http://www.searchsv.com.cn/showcontent_31730.htm

如何安装和配置 Puppet Dashboard?

在以前的文章中，我讨论过怎样使用 Puppet 来管理你的配置。而现在你可以用 Puppet Dashboard 为你的 Puppet 环境添加一个图形用户界面（GUI）。Puppet Dashboard 可以显示主机上 Puppet 的运行结果，并且可以提供一个节点分类工具来配置你的主机。在本文中，我将向你们介绍如何安装和配置 Puppet Dashboard。

该 Dashboard 是一种运行在 Rails 上的 Ruby 应用程序，它还不是可以添加到系统版本中的程序包，但是我们可以从 Puppet Labs 以 RPM 或者 DEB 包的形式获得该软件。我们也可以选择从资源进行安装。

作为前提条件，Dashboard 需要 Puppet 已经安装，并且使用存储的配置运行。Dashboard 可以在最近出现的大多数 Puppet 版本上工作，0.24.8 版及更高版本都可以。它还需要 Ruby、Rake 工具以及一个 MySQL 数据库（以后的版本会支持更多的数据库）。

添加 Yum 或者 Apt 仓库

首先，我们需要添加 Puppet Labs Yum，或者添加 Apt 仓库。对于 Yum 来说，我们需要为 Puppet Labs 创建一个 Yum 报告条目：

```
$ vi /etc/yum.repos.d/puppetlabs.repo
```

为该条目添加以下内容：

```
[puppetlabs]
name=Puppet Labs Packages
baseurl=http://yum.puppetlabs.com/base/
enabled=1
gpgcheck=1
gpgkey=http://yum.puppetlabs.com/RPM-GPG-KEY-puppetlabs
```

然后通过 Yum 安装。

```
$ sudo yum install puppet-dashboard
```

安装过程会提示你安装 Puppet Labs 释放键（release key），这是安装过程的一部分。

对于 Apt，我们需要给/etc/apt/sources.list 文件添加条目：

```
deb http://apt.puppetlabs.com/ubuntulucid main
deb-src http://apt.puppetlabs.com/ubuntulucid main
```

然后再给 Apt 添加 Puppet Labs GPG 键。

```
$ gpg --recv-key 4BD6EC30
$ gpg -a --export 4BD6EC30 | sudo apt-key add -
```

接下来，我们运行更新：

```
$ sudo apt-get update
```

然后安装软件包：

```
$ sudo apt-get install puppet-dashboard
```

在装有红帽和 Ubuntu 系统的主机上，Puppet Dashboard 的安装目录为/usr/share/puppet-dashboard。

配置 Rails 应用程序

下一步，我们需要配置 Rails 应用程序，首先从数据库开始。目前 Dashboard 只支持 MySQL 数据库，那么我们就创建一个：

```
$ mysql --u root p
mysql> CREATE DATABASE dashboard CHARACTER SET utf8;
mysql> CREATE USER 'dashboard'@'localhost' IDENTIFIED BY 'password';
mysql> GRANT ALL PRIVILEGES ON dashboard.* TO 'dashboard'@'localhost';
```

在此我们已经创建了一个名为 dashboard 的数据库，添加了一名叫做 dashboard 的用户，并让该用户对这个数据库拥有某些特权。你应该用适当的密码代替代码中的“密码”字符。

接下来，我们需要告诉 Dashboard 有关数据库的信息。为了做到这一点，我们需要对/usr/share/puppet-dashboard/config 目录下的 database.yml 文件进行配置。

该软件包含有一个示例文件，名字为 database.yml.example，我们可以对它进行复制和编辑：

```
$ cp database.yml.example database.yml
$ vi database.yml
```

在该文件中更新生产节（用你自己的密码代替 password 字符），代码如下：

```
production:
adapter: mysql
database: dashboard
username: dashboard
password: password
encoding: utf8
```

这个节需要 YAML 格式验证，所以请确保你保留了现有的缩进。

最后，我们需要用表格和基础数据来填充我们的新数据库。我们用 Rake 任务来完成这个工作。在/usr/share/puppet-dashboard 目录下，运行以下命令：

```
$ rake RAILS_ENV=production db:migrate
```

现在 Dashboard 全部配置完成，我们可以运行该 Rails 应用程序了。运行 Rails 应用程序有很多方法。一种方法是使用内部 Webrick 服务器（这对于生产不是很好，因为它并不能很好的扩展）。

在/usr/share/puppet-dashboard 目录下，运行：

```
$ sudo ./script/server -e production
```

这个命令会在端口 3000 上运行 Dashboard，你可以通过一个网页浏览器进行访问：

http://your.host.name:3000

你还可以配置带有 Passenger 的 Apache 或者 Nginx 来运行 Dashboard，这种做法是一种更稳定、扩展性更好的生产选择。在这里你可以找到一个 Apache Passenger 配置文件示例。

下篇文章中，我们将介绍如何把 Puppet 报告导入 Puppet Dashboard。

（作者：James Turnbull 译者：Dan 来源：TechTarget 中国）
原文标题：如何安装和配置 Puppet Dashboard?
原文链接：http://www.searchsv.com.cn/showcontent_39366.htm

如何将 Puppet 报告导入 Puppet Dashboa?

在以前的文章中，我向你们介绍了如何安装和配置 Puppet Dashboard，本文中，我们将介绍如何将 Puppet 报告导入 Puppet Dashboard。

把 Puppet 报告导入 Puppet Dashboard

现在 Dashboard 正在运行，而我们需要确保它能够获取 Puppet 报告。完成这项工作有几种方法，开始的时候都是用 Rake 任务导入旧报告。在/usr/share/puppet-dashboard 目录下，运行：

```
$ rake RAILS_ENV=production reports:import
```

这个命令假设你的 Puppet 管理器在本地主机上，并将导入 Puppet vardir 目录里面的全部文件（目录通常是/var/lib/puppet/reports，但是你也可以用 REPORT_DIR 选项指定一个其他的目录）。你可以多次运行这个命令，或者用计划任务对其进行设置——它会识别以前导入的报告，并且只会添加新的报告。

你还可以配置 Puppet，让它自动给 Dashboard 传送报告。完成这项工作有两种方法，第一种方法是针对 Puppet 0.25.x 版本以及更低版本，第二种方法则是针对 Puppet 0.26.x 版本以及更高版本。对于 Puppet 0.25.x 版本以及更低版本来说，请确保你在每个想要报告的客户端上开启报告功能，做法是在 puppet.conf 配置文件的[puppet]节中添加 report = true。然后在 Puppet 管理器上的 puppet.conf 文件中添加 /usr/share/puppet-dashboard/lib/puppet 到 Puppet 的 libdir 目录，命令如下：

```
[main]
libdir = /usr/share//puppet-dashboard/lib/puppet:/var/puppet/lib
```

开启 Puppet Dashboard 报告：

```
[puppetmasterd]
reports = puppet_dashboard, any-other-reports
```

这个报告假设你的 Puppet Dashboard 运行在本地主机端口 3000 上。你可以调整这个位置通过编辑文件 /usr/share/puppet-dashboard/lib/puppet/puppet_dashboard.rb，并升级 HOST 和 PORT 选项在文件的顶部。

在 Puppet 2.6.x 以及更高的版本中，你需要在你的客户端开启报告：

```
[agent]
report = true
```

然后指定 http 报告类型，并用新的 reporturl 选项来指定目标主机和 URL，代码如下：

```
[master]
reporturl=http://localhost:80/reports
reports=http
```

更新主机和端口，以便跟你的环境相符（你应该保持 URL 上的报告后缀）。

现在 Puppet Dashboard 应该能够接收你的 Puppet 报告了，大功告成！如果你按照本文的方法一直做到现在，那么你就应该可以看到 Puppet Dashboard 的主屏幕了。

从这个屏幕上你可以看到目前所有的 Puppet 节点，以及 Puppet 运行的成功和失败状况（而且你还可深入研究显示的结果，以便查看哪些资源失败以及产生的错误等）。它为你的 Puppet 环境提供了一个强大的中心界面，环境状况一目了然。

它还是一个相对较新的产品，所以人们每天都会为其添加新的功能（也可能是 bug）。如果你有困难、问题、特别是想法和反馈意见，请登录 Puppet Labs，从#puppet IRC 通道获得帮助，或者通过 Puppet 邮件列表获得帮助。请开始使用吧，并让我们知道您的使用情况！

（作者：James Turnbull 译者：Dan 来源：TechTarget 中国）

原文标题：如何将 Puppet 报告导入 Puppet Dashboard?

原文链接：http://www.searchsv.com.cn/showcontent_39367.htm

如何运用网络映射器（Nmap）助力 Linux 管理与安全？

我们将要与您分享的这条技巧关于网络映射器（Nmap），它是一种开源网络浏览器，它在网络故障诊断、浏览和审计方面都非常理想。这项工具可用来识别网络中的设备，也可以识别在特定设备上运行的服务。另外，先进的信息，如正在使用的操作系统、特定服务（名字和版本）和网络滤波器和防火墙也都能识别出来。

用 Nmap 的服务识别通过现含指纹五千以上的指纹数据库实现。这个数据库通过社区允许提交已知指纹来支持。

作为盘点工具的网络映射器

网络映射器的常规应用之一是生成基本库存报告。这对网络地图、维护网络设备和节点一致的更新、还有识别流氓、未授权或遗忘设备都很实用。

盘点的基本扫描利用 ping 扫描。例如，接下来的扫描显示了在 192.168.1.0/24 网络中可用的主机。-sP 指示 Nmap 进行一次 ping 扫描，而-n 则指示不要进行名称解析。

```
nmap -sP -n 192.168.1.0/24
Starting Nmap 4.76 (http://nmap.org) at 2009-05-14 10:18 CDT
Host 192.168.1.1 appears to be up.
MAC Address: 00:18:3A:A4:43:BA (Westell Technologies)
Host 192.168.1.2 appears to be up.
Host 192.168.1.3 appears to be up.
MAC Address: 00:17:EE:01:95:19 (Motorola CHS)
Host 192.168.1.4 appears to be up.
MAC Address: 00:16:CB:A3:27:E4 (Apple Computer)
Host 192.168.1.5 appears to be up.
MAC Address: 00:1E:52:7D:84:7E (Apple)
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.17 seconds
```

这次 ping 扫描对于快速建立库存清单非常实用。它也可以是更复杂脚本和程序验证网络地址和变化的结构单元。举例来说，下面的命令报告了从两个日常扫描输出到文本文件的网络中的新主机（192.168.1.5）：

```
diff monday.scan tuesday.scan | grep "> Host"
> Host 192.168.1.5 appears to be up.
```

指定主机型盘点

看一看决定服务运行的特定主机，你可以使用 Nmap。例如，让我们更近地看看 192.168.1.5，它看上去是周一扫描后周二扫描前某个时候被发现的：

```
nmap -n 192.168.1.5
Starting Nmap 4.76 ( http://nmap.org ) at 2009-05-14 12:44 CDT
Interesting ports on 192.168.1.5:
Not shown: 984 closed ports
PORT STATE SERVICE
22/tcp open ssh
88/tcp open kerberos-sec
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
515/tcp open printer
548/tcp open afp
631/tcp open ipp
1021/tcp open unknown
1022/tcp open unknown
1023/tcp open netvenuechat
2049/tcp open nfs
3300/tcp open unknown
5900/tcp open vnc
20221/tcp open unknown
20222/tcp open unknown
MAC Address: 00:16:CB:A3:27:E4 (Apple Computer)
Nmap done: 1 IP address (1 host up) scanned in 10.46 seconds
```

它看上去是以 ssh 为基础的基于 Unix 系统，但是 MAC 地址识别让这个系统非常像一台 Apple MAC 电脑。但是，近看运用 Nmap 的服务和版本检测，可以收集更多信息。-sV 参数用在这里：

```
mb3:~ root# nmap -n -sV 192.168.1.5
Starting Nmap 4.76 ( http://nmap.org ) at 2009-05-14 12:47 CDT
Interesting ports on 192.168.1.5:
```

```
Not shown: 984 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.1 (protocol 1.99)
88/tcp open kerberos-sec Mac OS X kerberos-sec
111/tcp open rpcbind
139/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
515/tcp open printer
548/tcp open afp?
631/tcp open ipp CUPS 1.3
1021/tcp open rpcbind
1022/tcp open rpcbind
1023/tcp open rpcbind
2049/tcp open rpcbind
3300/tcp open unknown?
5900/tcp open vnc VNC (protocol 3.8)
20221/tcp open unknown?
20222/tcp open unknown?
```

尽管会返回数据，我还是为未识别的数据服务。

如果你知道这个服务/版本，请提交以下指纹到 http://www.insecure.org/cgi-bin/servicefp-submit.cgi ：

```
SF-Port548-TCP:V=4.76%I=7%D=5/14%Time=4A0C5929%P=i386-apple-
darwin9.4.0%r(
SF:SSLSessionReq,172,"\x01\x03\0\0Q\xec\xff\xff\0\0\x01b\0\0\0\0\0\x18\0
\"
AD9
SF:6FA5112ED039C\0\x04mini");
MAC Address: 00:16:CB:A3:27:E4 (Apple Computer)
Service Info: OS: Mac OS X
Host script results:
| Discover OS Version over NetBIOS and SMB: Unix
|_ Discover system time over SMB: 2009-05-14 12:49:02 UTC-5
Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 119.68 seconds
```

现在管理员知道它是 MAC 操作系统 X，并且它用于使用 Samba 的 Windows 文件分享，它最可能通过 CUPS 分享打印机，并且这个系统是针对远程管理用虚拟网络计算配置。

安全的 Nmap 运用

正如上文所说的，Nmap 对管理员来说很实用，它在安全审计方面的能力也很强大。例如，很多公司不允许网络服务器在用户网络中运行（如连接了用户电脑和笔记本的网络）。Nmap 可以通过运行在知名端口 80 和 443 的网络服务很容易地用于识别所有系统：

```
nmap -n -p 80,443 192.168.1.0/24 | egrep "ports|open"
Interesting ports on 192.168.1.1:
80/tcp open http
443/tcp open https
Interesting ports on 192.168.1.2:
Interesting ports on 192.168.1.3:
Interesting ports on 192.168.1.4:
Interesting ports on 192.168.1.5:
```

另一个有用的特征是识别特定版本来决定系统是否易受某一预报弱点的攻击。例如，让我们假设 Samba 团队已经预报一项某特定版本 Samba 的安全事故，你需要辨认所有的 Samba 版本。下文报告这些 Samba 版本：

```
nmap -n -sV -p 139 192.168.1.0/24 | egrep "ports|139"
Interesting ports on 192.168.1.1:
139/tcp closed netbios-ssn
Interesting ports on 192.168.1.2:
139/tcp closed netbios-ssn
Interesting ports on 192.168.1.3:
139/tcp filtered netbios-ssn
Interesting ports on 192.168.1.4:
139/tcp open netbios-ssn Samba smbd 3.2 (workgroup: HQ)
Interesting ports on 192.168.1.5:
139/tcp open netbios-ssn Samba smbd 2.1 (workgroup: REMOTE)
Interesting ports on 192.168.1.15:
139/tcp open netbios-ssn Samba smbd 3.2 (workgroup: WORKGROUP)
```

该技巧已经展示了 Nmap 如何用于网络盘点扫描、更彻底的盘点和审计、识别未授权服务并协助安全攻击评估。Nmap 是随时可用的好工具…把它和检索目标行命令或搜索文件中的特定字符串连结在一起，它会变成有力的报告工具。

（作者：Ronald McCarty　译者：徐艳 来源：TechTarget 中国）

原文标题：运用网络映射器（Nmap）助力 Linux 管理与安全

原文链接 http://www.searchsv.com.cn/showcontent_39248.htm