



貴州大學

基于 Asianux 的 “GZU-59” 网络安全 LiveCD

队伍编号: GZU-59

团队成员: 王洁林

: 杨震

: 李阳

指导教师: 王道书



## 目 录

摘 要.....	3
项目规格书.....	4
分析设计说明书.....	6
一、背景和应用领域.....	6
二、作品特点和设计思路.....	6
三、运行硬件环境要求.....	6
四、功能描述.....	7
五、工作原理.....	7
六、体系结构和关键技术点.....	7
七、功能模块设计.....	7
八、相关技术比较和分析.....	17
九、总结.....	17
指导老师意见与评价.....	19
团队成员.....	20
附录：存在问题	



## 摘 要

随着 Internet 的普及，电子商务的应用逐渐增大。人们对网络的依赖也逐渐加深。但是，Internet 的普及也伴随着接踵而来的安全问题。

目前人们对网络安全并不是非常重视，在这种大环境下。使得很多‘脚本小子’四处破坏、病毒肆意横行。使得用户遭受不必要的损失。如：重要文件被窃取或破坏、银行账号被盗、私人信息被提取。

但是，保护网络安全并不是一件容易的事情。我们要知道自己的弱点，可能的威胁以及检测攻击的方法，并在攻击尚未成功之前能有一套方案来处理可能的威胁。

网络安全重要一个目标是保护数据。网络安全是要保护数据的特性，即机密性，完整性，有效性。但是，无论如何，对这些特性的损害可以认为是个威胁。威胁是任何通过可能利用的方式对某些漏洞进行的攻击。伴随着漏洞利用和攻击，数据可能在存储、处理或者传输中而被窃取或者篡改。

因此，我们的 LiveCD 的作用就是对特定用户进行一系列的安全检测。通过这些检测，发现用户存在的安全问题，然后通过这些检测出的安全问题来解决可能存在的威胁。

该 LiveCD 包含如下工具：

1. 信息收集
2. 网络映射工具
3. 渗透工具
4. 提权工具
5. 漏洞检测
6. 其他常用工具

这一系列的工具，能够基本满足我们对特定目标的安全的检测。通过这一系列的测试使我们尽早发现漏洞。然后通过发现的这些漏洞来消除我们面临的威胁从而增强我们的安全性能。

目前，我们的 LiveCD 的功能只能实现基本的漏洞扫描，而且基于的是有线网络。我们下一步目标是添加目前比较主流的蓝牙以及 WIFI 等无线网络工具。针对越来越多的无线攻击。我们希望能够加入这一系列的测试工具来解决这些无线漏洞的发掘问题。



## 项目规格书

### 一、项目背景

随着信息化进程的深入和互联网的迅速发展，人们的工作、学习和生活方式正在发生巨大变化，效率大为提高，信息资源得到最大程度的共享。但是，紧随信息化发展而来的网络安全问题日渐凸出，如果不很好地解决这个问题，必将阻碍信息化发展的进程。如何方便快捷的了解网络安全相关知识，了解常见的网络安全攻防方式，是从攻击角度研究防御的一种最有效方式。

#### 1、网络安全现状

可以从不同角度对网络安全作出不同的解释。一般意义上，网络安全是指信息安全和控制安全两部分。国际标准化组织把信息安全定义为“信息的完整性、可用性、保密性和可靠性”；控制安全则指身份认证、不可否认性、授权和访问控制。

互联网与生俱有的开放性、交互性和分散性特征使人类所憧憬的信息共享、开放、灵活和快速等需求得到满足。网络环境为信息共享、信息交流、信息服务创造了理想空间，网络技术的迅速发展和广泛应用，为人类社会的进步提供了巨大推动力。然而，正是由于互联网的上述特性，产生了许多安全问题。美国前总统克林顿在签发《保护信息系统国家计划》的总统咨文中陈述道：“在不到一代人的时间里，信息革命以及电脑进入了社会的每一领域，这一现象改变了国家的经济运行和安全运作乃至人们的日常生活方式，然而，这种美好的新的代也带有它自身的风险。所有电脑驱动的系统都很容易受到侵犯和破坏。对重要的经济部门或政府机构的计算机进行任何有计划的攻击都可能产生灾难性的后果，这种危险是客观存在的。过去敌对力量和恐怖主义分子毫无例外地使用炸弹和子弹，现在他们可以把手提电脑变成有效武器，造成非常巨大的危害。如果人们想要继续享受信息时代的种种好处，继续使国家安全和经济繁荣得到保障，就必须保护计算机控制系统，使它们免受攻击。”

在各领域的计算机犯罪和网络侵权方面，无论是数量、手段，还是性质、规模，已经到了令人咋舌的地步。据有关方面统计，目前美国每年由于网络安全问题而遭受的经济损失超过 170 亿美元，德国、英国也均在数十亿美元以上，法国为 100 亿法郎，日本、新加坡问题也很严重。在国际刑法界列举的现代社会新型犯罪排行榜上，计算机犯罪已名列榜首。2003 年，CSI/FBI 调查所接触的 524 个组织中，有 56% 遇到电脑安全事件，其中 38% 遇到 1~5 起、16% 以上遇到 11 起以上。因与互联网连接而成为频繁攻击点的组织连续 3 年不断增加；遭受拒绝服务攻击（DoS）则从 2000 年的 27% 上升到 2003 年的 42%。调查显示，521 个接受调查的组织中 96% 有网站，其中 30% 提供电子商务服务，这些网站在 2003 年 1 年中有 20% 发现未经许可入侵或误用网站现象。更令人不安的是，有 33% 的组织说他们不知道自己的网站是否受到损害。据统计，全球平均每 20s 就发生 1 次网上入



侵事件，黑客一旦找到系统的薄弱环节，所有用户均会遭殃。

目前，我国网络安全问题日益突出的主要标志是：a) 计算机系统遭受病毒感染和破坏的情况相当严重。b) 电脑黑客活动已形成重要威胁 c) 信息基础设施面临网络安全的挑战。 d) 网络政治颠覆活动频繁。

由于种种原因制约了提高我国网络安全防范的能力，比如：缺乏自主的计算机网络和软件核心技术、安全意识淡薄、运行管理机制的缺陷和不足、缺乏制度化的防范机制等等。在此，大力加强网络安全相关理论、工具、技术的研究，是我们目前面对网络安全挑战的重点。

## 2、Linux与网络安全

Linux 操作系统在短短的几年之内得到了非常迅猛的发展，这与 Linux 具有的良好特性是分不开的。Linux 包含了 Unix 的全部功能和特性。并且具有开放性、多用户、多任务、良好的用户界面、设备独立性、丰富的网络功能、可靠的系统安全、良好的可移植性等一系列特性。

同时，由于 Linux 及其相关软件遵循自由软件协议，全面开放源码，大量主流的工具都能够免费使用。而且，linux 的模块化系统使我们能够自行定制，从而精简了系统。因为精简了部分不需要的工具，使 linux 的运行速度有了很大的提升，操作系统的容量也不会太大。对于追求效率的网络安全测试，这一点非常重要。

## 二、创作思路

针对目前安全工具多而杂，缺乏一个统一而方便的管理。我们使用了 Linux 来对安全测试工具进行打包管理。利用 Linux 下强大而众多的安全工具，我们可以搭建一个网络安全工具包，通过光盘启动方式，运行网络安全工具。通过 linux 来集成网络安全工具包，具有如下优点：

- 1、因为安全工具包是由 LiveCD 运行，因此不需要安装大量的网络安全工具包，从而免去了工具安装的时间，提高了效率。
- 2、因为集成了大量的安全工具，使我们能够对目标进行有效的测试。
- 3、Linux 对大部分的硬件环境能提供有效的支持，这样使我们能够不分场合地点来对目标进行安全测试，增大了测试环境的自由度。

## 三、应用领域

我们制作的 “GZU-59” LiveCD，具有启动速度快、包含工具多，容量小，只需一装光盘即可装载等优点。因此比较适合网络管理员对自己的服务器进行安全测试。通过这一系列的安全测试能够尽快发现漏洞而解决隐蔽的安全隐患。



## 分析设计说明书

### 一、背景和应用领域

随着信息化进程的深入和互联网的迅速发展，人们的工作、学习和生活方式正在发生巨大变化，效率大为提高，信息资源得到最大程度的共享。但是，紧随信息化发展而来的网络安全问题日渐凸出，如果不很好地解决这个问题，必将阻碍信息化发展的进程。如何方便快捷的了解网络安全相关知识，了解常见的网络安全攻防方式，是从攻击角度研究防御的一种最有效方式。

针对目前安全工具多而杂，缺乏一个统一而方便的管理。我们使用了 Linux 来对安全测试工具进行打包管理。利用 Linux 下强大而众多的安全工具，我们可以搭建一个网络安全工具包，通过光盘启动方式，运行网络安全工具。

我们制作的“GZU-59” Live CD，具有启动速度快、包含工具多，容量小，只需一装光盘即可装载等优点。因此比较适合网络管理员对自己的服务器进行安全测试。通过这一系列的安全测试能够尽快发现漏洞而解决隐蔽的安全隐患

### 二、作品特点和设计思路

工具多且范围大。除了嗅探、扫描、密码猜解等基本网络安全工具外，还有基于 wine 下运行的逆向工程软件。

我们的设计思路是希望能够构造一个比较全面的安全工具检测包。通过这一系列的安全检测包来检测出目标主机的漏洞。并对针对这些漏洞来对目标主机进行安全优化。针对目前网络上攻击方式多种多样，很难用一种单一的模式来模拟攻击。因此，安全工具检测包能够弥补这种缺陷。它丰富的工具能够最大化的模拟出网络上不同攻击方式。从而使网络管理员有的放矢来对目标主机进行安全配置。

### 三、运行硬件环境要求

系统基本运行环境为：i386

### 四、功能描述

本系统包含以下主要功能：

1. 信息收集
2. 网络映射工具
3. 渗透工具
4. 提权工具
5. 漏洞检测
6. 逆向工程



## 7. 其他常用工具

## 五、工作原理

系统通过光盘引导后进入 isolinux 菜单，根据用户选择进入不同的 Linux 系统，在基本 KDE 系统下，用户可以选择图形工具和命令工具来进行安全工具的运行。

## 六、体系结构和关键技术点

系统通过 isolinux 引导进入 LiveCD。内核版本号为 2.6.26

本系统的与众不同之处在于舍弃了多余的 linux 程序。如多媒体、办公、娱乐、图像处理。使本系统能够尽可能的精简，并且使 LiveCD 运行速度有一定的提升。

关键技术点为工具包加载为模块并且红旗系统的库文件对安全工具能够有很好的支持。

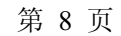
## 七、功能模块设计

系统主要分为引导模块、启动模块、基本系统、桌面环境、安全工具等功能模块

### 1、引导模块设计

引导模块采用 ISOLINUX, ISOLINUX 是 Linux/i386 的一个启动引导器，其核心是 Linux，如果用户配置过 LILO，将发现 ISOLINUX 的配置文件 isolinux.cfg 与 LILO 的配置 lilo.conf 有点相似。ISOLINUX 本身以非模拟方式运行于 ISO 9660/El Torito CD-ROMs，这避开了软盘模拟的磁盘空间容量问题和硬盘模拟会产生的一些兼容性问题。





选择 nvi 显卡模式:





```
* -> base/01-bin.lzm
* -> base/02-etc.lzm
* -> base/03-home.lzm
* -> base/04-lib.lzm
* -> base/05-opt.lzm
* -> base/06-root.lzm
* -> base/07-sbin.lzm
* -> base/08-srv.lzm
* -> base/09-usr.lzm
* -> base/10-var.lzm
* -> base/java-path.lzm
* -> base/pentest.lzm
* -> base/qt.lzm
* -> base/wine.lzm
* -> base/xhalt.lzm
* -> optional/nvidia.lzm
```

\*\*\*\*最后一个模块是 nvidia.lzm\*\*\*\*

选择 ati 显卡进入:

```
* -> base/01-bin.lzm
* -> base/02-etc.lzm
* -> base/03-home.lzm
* -> base/04-lib.lzm
* -> base/05-opt.lzm
* -> base/06-root.lzm
* -> base/07-sbin.lzm
* -> base/08-srv.lzm
* -> base/09-usr.lzm
* -> base/10-var.lzm
* -> base/java-path.lzm
* -> base/pentest.lzm
* -> base/qt.lzm
* -> base/wine.lzm
* -> base/xhalt.lzm
* -> optional/ati.lzm
```

\*\*\*\*\*最后一个模块是 ati.lzm\*\*\*\*\*

### 3. 基本系统

我们首先装了 Asianux 3 workstation 最精简版大约 1.6G, 即: 去掉所有我们这个 LiveCD 用不到的软件, 譬如 openoffice, printf 以及一些用不到的工具, 我们的内核基于内核版本号为 2.6.26 的 linux 内核。内核模块配置参照了 slax。工具包参照 Backtrack 3。

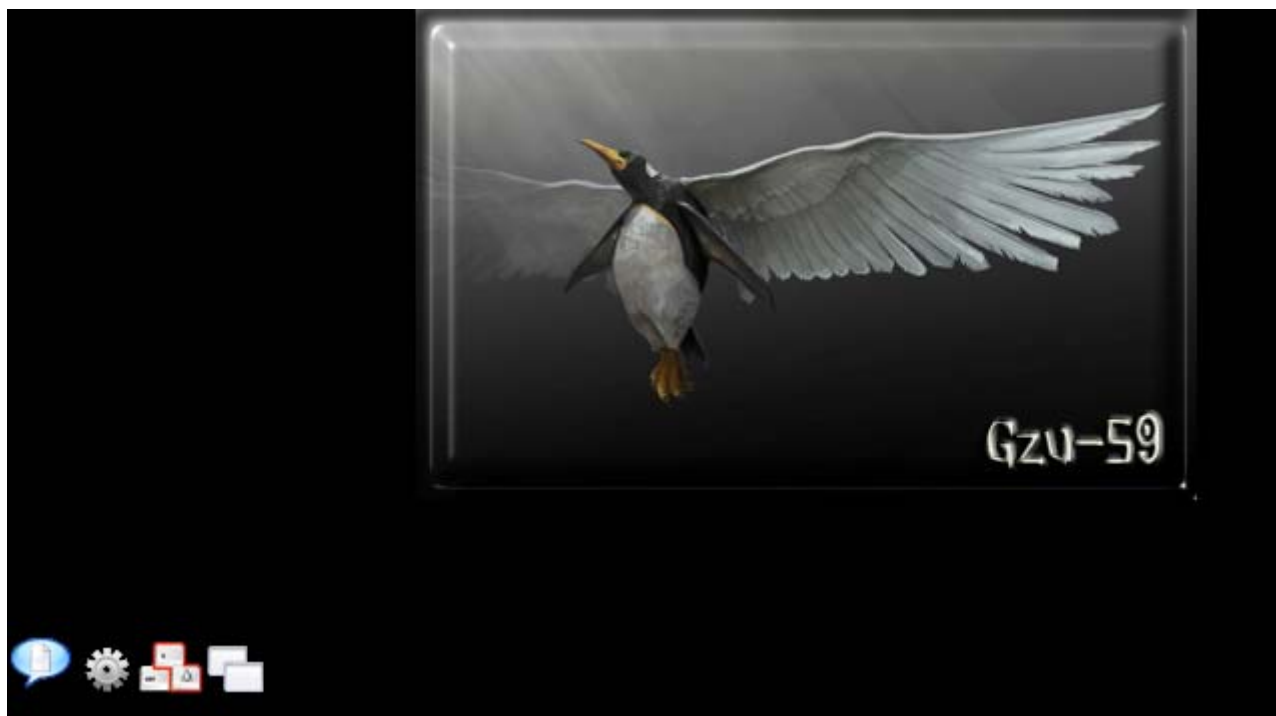
### 4、桌面环境

桌面环境为 kde3.5.5, 图标:

在 /usr/share/apps/kdm/themes 中的登陆界面面包用我们自己做的替换了, 效果:



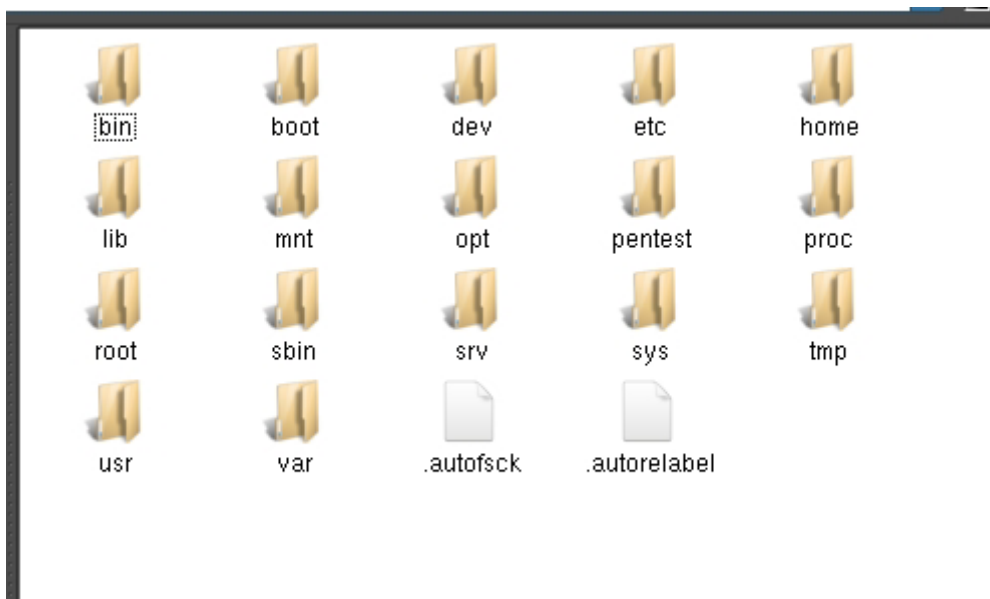
Splash 更改为:



在 `/usr/share/wallpapers` 中加入我们自己的以我们队名 “GZU-59” 为底的黑色基调图片同时删除多余的图片



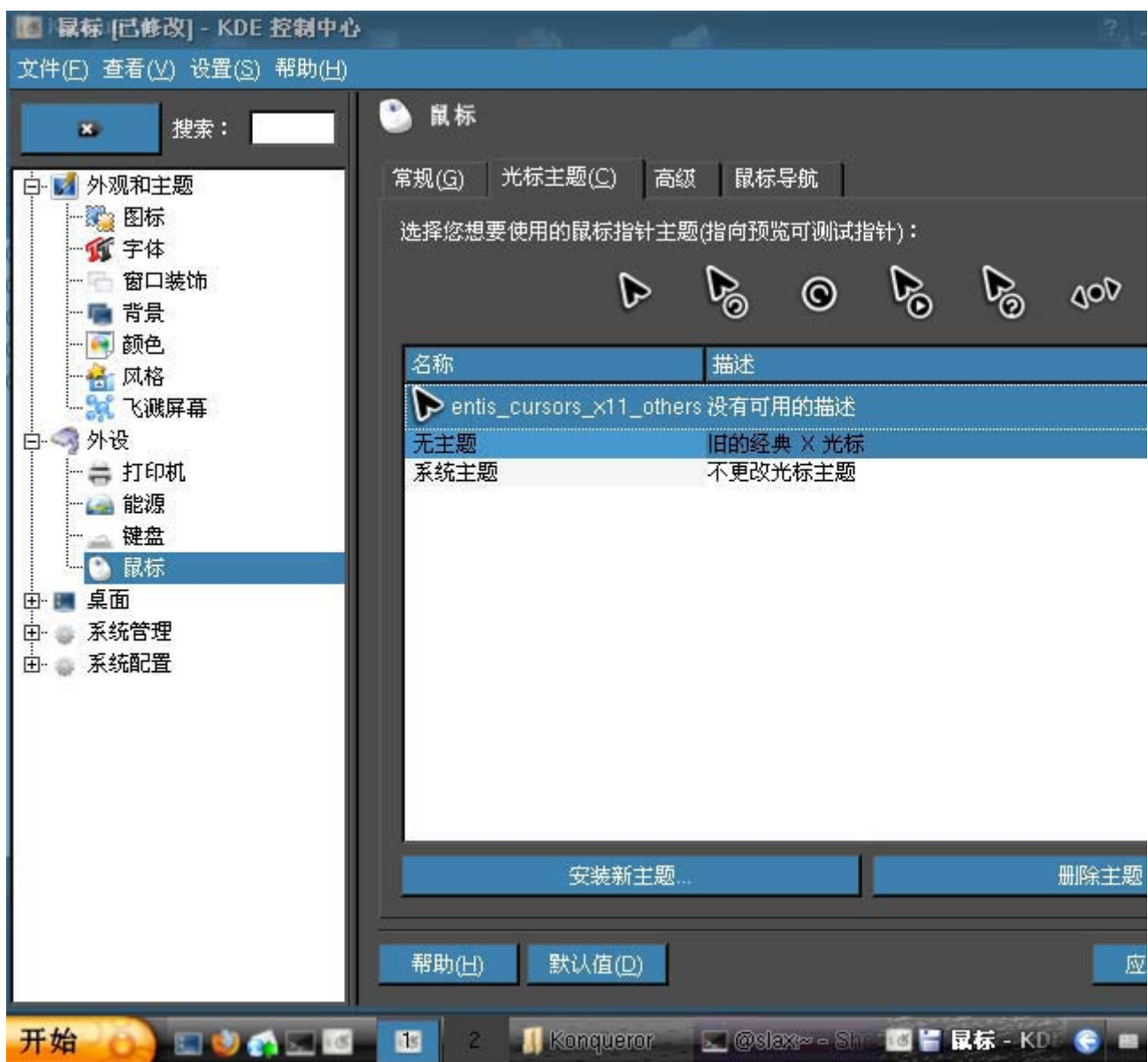
图标更改为:



颜色更改为 DarKFD0

风格改为:CDE, 同时删除多余的风格

从[www.kde-look.org](http://www.kde-look.org)上下载鼠标主题:, 如下:



右击任务栏, 选择“配置桌面”->“外观”, 在该选项下“常规”中选择“启用图标鼠标悬停特效”。



在/root/.config/menus 中更改 applications-kmenuedit.menu (修改开始菜单, 添加工具)



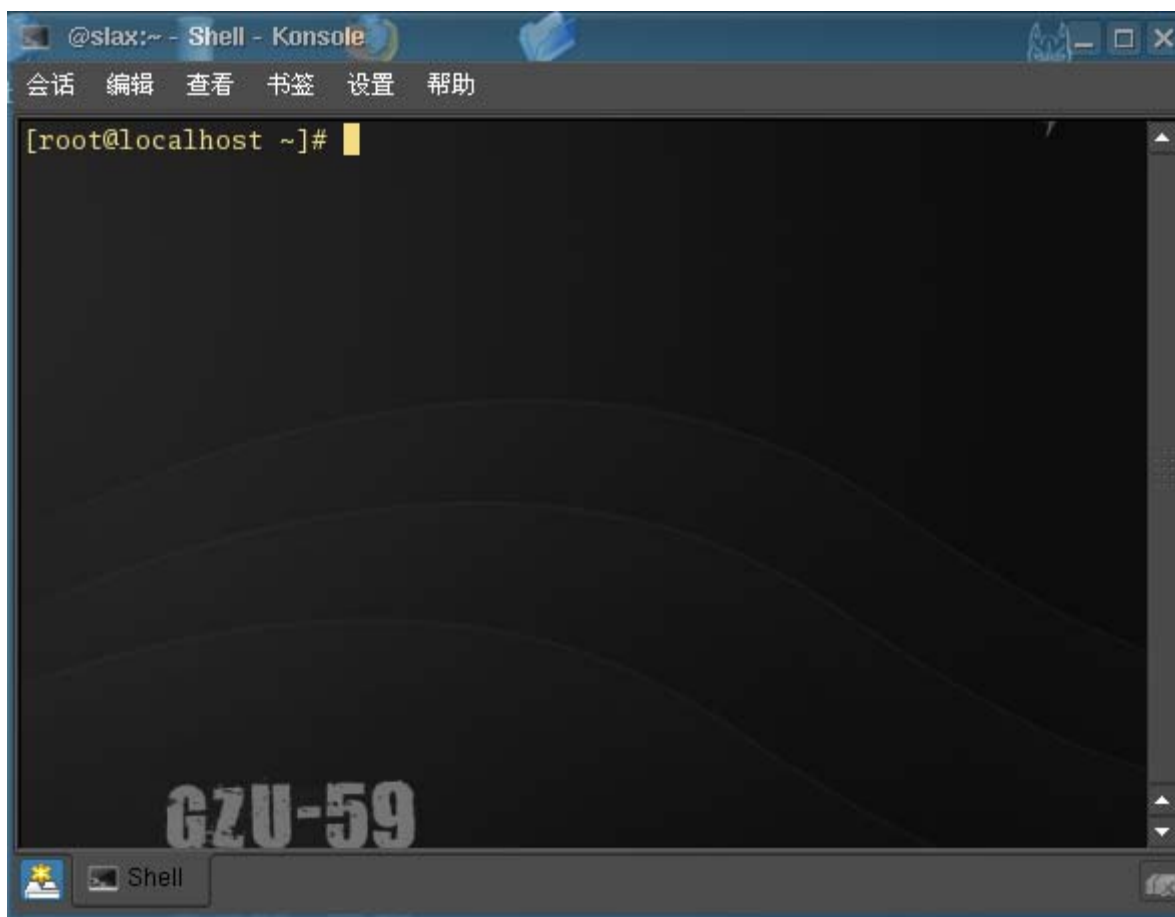
配置终端: 打开终端, “设置” -> “方案” -> MC 透明 (配置终端背景)

“设置” -> “配置 konsole” -> “方案” -> “konsole 颜色” 选择颜色.

“设置” -> “保存为默认值”。

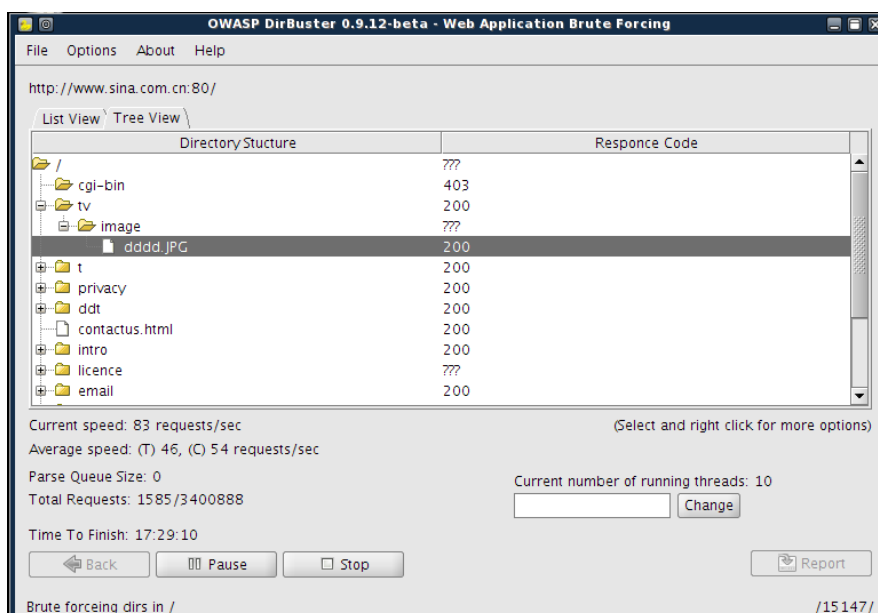
这样终端就配置好了.

效果如下:



## 5、安全工具

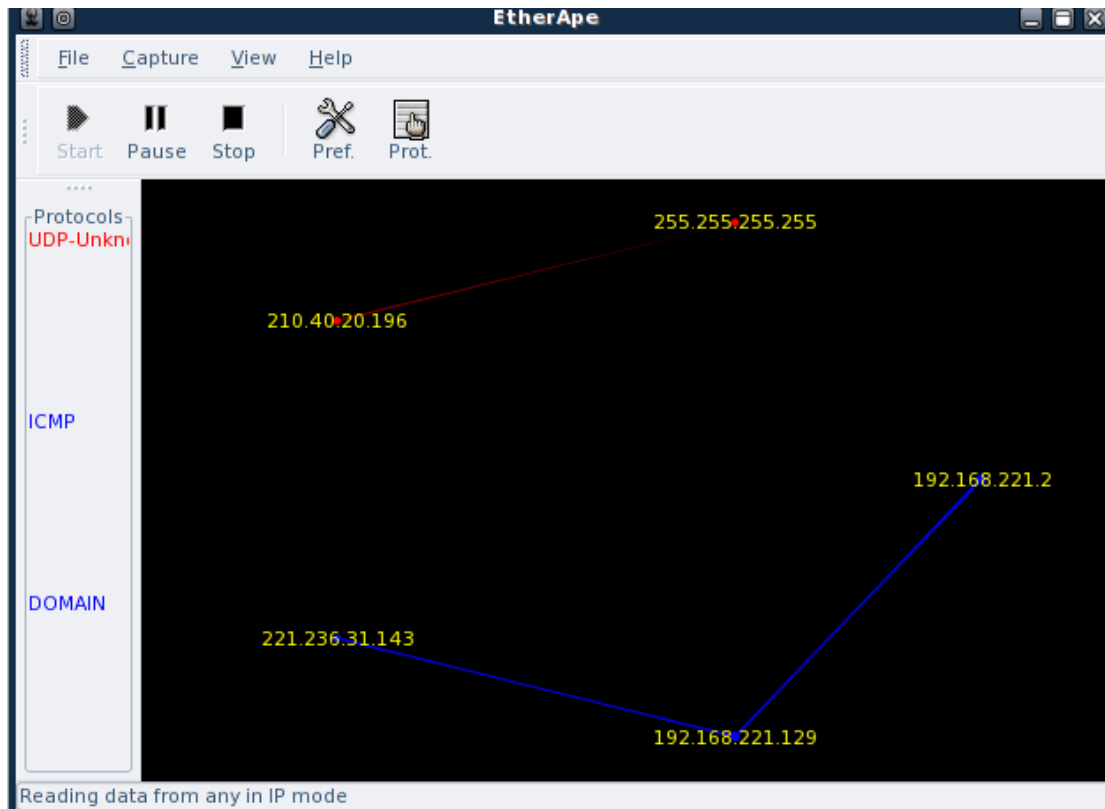
安全工具内容较多，主要分为以下几个方面：信息收集、网络映射工具、渗透工具、提权工具、漏洞检测、逆向工程以及其他常用工具. 这是一个网站后台文件扫描工具 DirBuster :







这是网络流量以及路由跳转的分析工具，Etherape



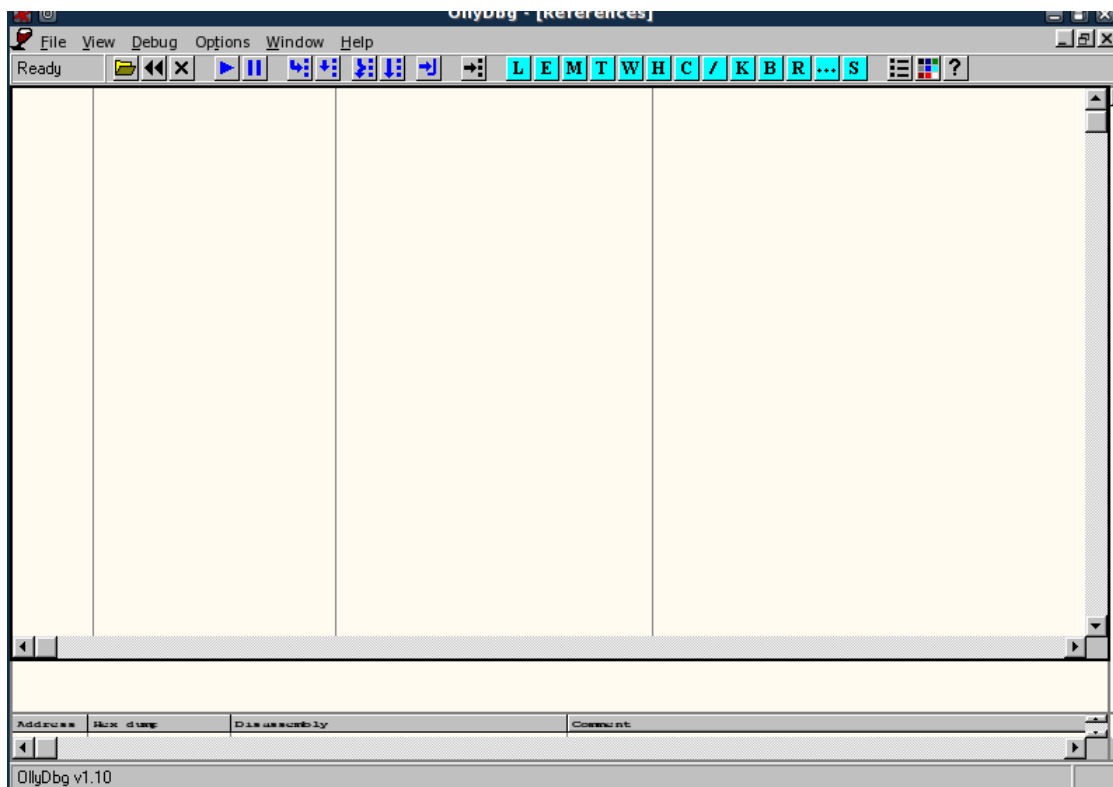
这是一个网段存活主机分析工具：路径位于/pentest/scanner/ipscan

The screenshot shows the Angry IP Scanner application window. The title bar is "100% - IP Range - Angry IP Scanner". The main window has a menu bar (File, Go to, Commands, Favorites, Tools, Help) and a toolbar. The IP Range is set to 192.168.221.1 to 192.168.221.200. The Hostname is set to Gzu-59. The Netmask is set to 255.255.255.0. The Stop button is highlighted. The main display area shows a table of IP addresses and their ping status.

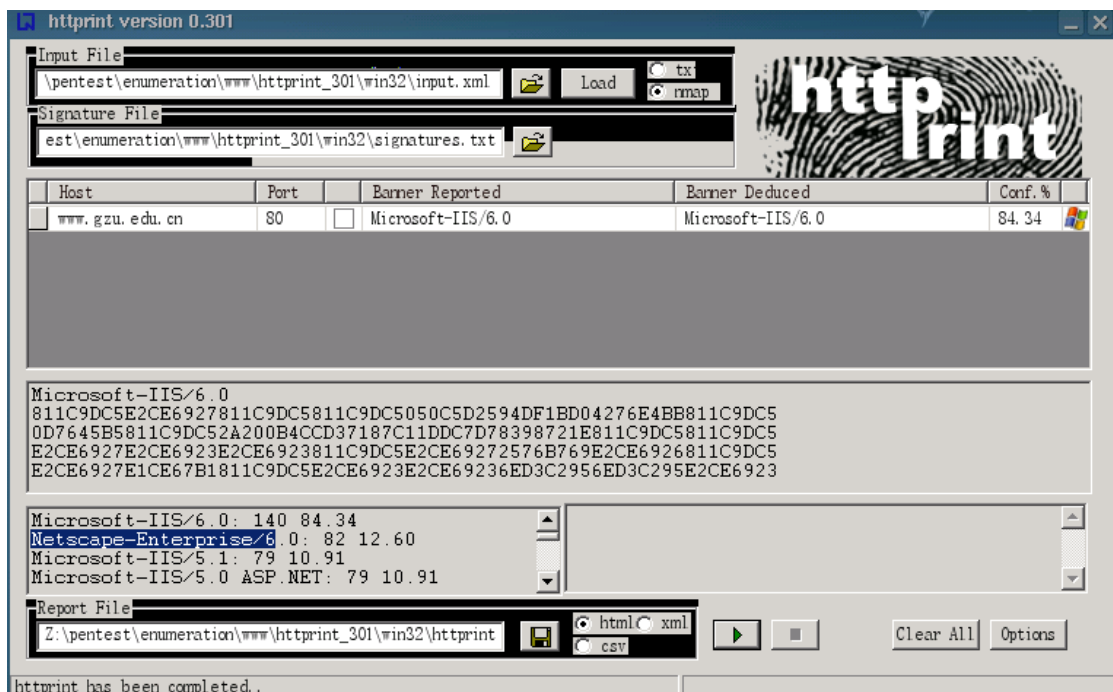
IP	Ping	Hostname	Ports [0+]
192.168.221.1	[n/a]	[n/s]	[n/s]
192.168.221.2	0 ms	[n/a]	[n/s]
192.168.221.3	[n/a]	[n/s]	[n/s]
192.168.221.4	[n/a]	[n/s]	[n/s]
192.168.221.5	[n/a]	[n/s]	[n/s]
192.168.221.6	[n/a]	[n/s]	[n/s]
192.168.221.7	[n/a]	[n/s]	[n/s]
192.168.221.8	[n/a]	[n/s]	[n/s]
192.168.221.9	[n/a]	[n/s]	[n/s]
192.168.221.10	[n/a]	[n/s]	[n/s]
192.168.221.11	[n/a]	[n/s]	[n/s]
192.168.221.12	[n/a]	[n/s]	[n/s]
192.168.221.13	[n/a]	[n/s]	[n/s]
192.168.221.14	[n/a]	[n/s]	[n/s]

At the bottom, there are buttons for "Wait for all threads to terminate...", "Display: All", and "Threads: 52".

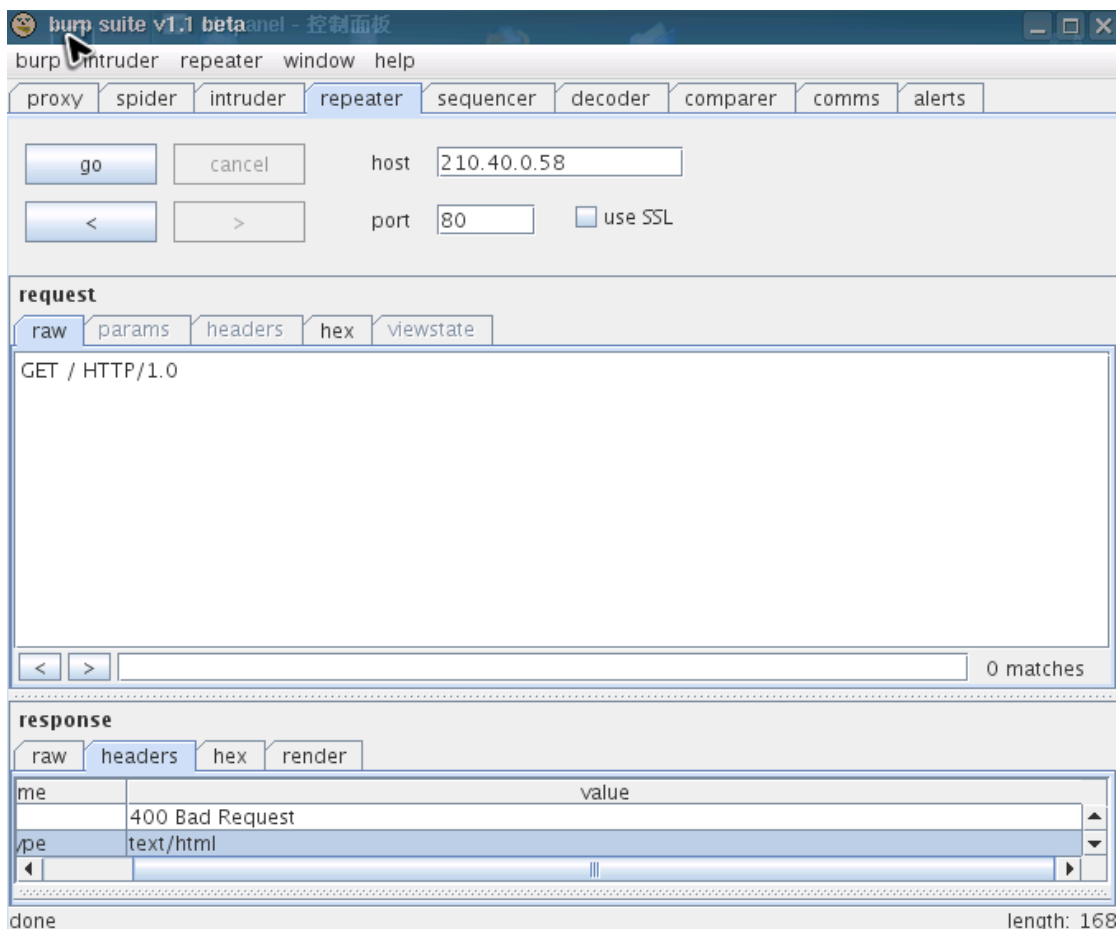
大名鼎鼎的逆向工程软件 01lyDBG 通过自带的 wine 模拟：



对远程服务器扫描的工具：httpprint\_GUI，该软件也是基于 wine 运行



网站攻击器 Burp Suite



该工具需要 java 工具来运行  
还有许多基于命令行的网络工具，这些不再举例。

## 八、相关技术比较和分析

本系统引导速度快、内存消耗小，进入系统时间短，工具多，覆盖的安全检测范围广。

## 九、总结

通过这次 LiveCD 的制作，使我们能够加深对 LINUX 内核的理解，大量安全工具的使用，使我们明白了对于网络安全，仅仅是一方面的安全优化是不够的。需要由局部到整体的考虑。任何一个疏忽，都可能造成自己管理的系统让‘脚本小子’有机可乘。导致整个系统的瘫痪，蒙受不必要的损失。

该 LiveCD 或许不是成功的网络安全测试 LiveCD，但是经过一次次内核配置失败，工具加载库文件出错，等等。我们自己也在这些失败中学到了很多东西。曾经碰都不敢碰的东西到现在我们能够亲手制作并精简。由仅仅使用单一的工具到现在我们能够整合不同安全工具的长处来进行有目的测试，都是非常有价值的经验。

同时，我们 Gzu-59 团队成员由不同分工到把自己的经验整合也是让这次



LiveCD 能够打包成功的重要因素，对于一个三人团队，要做到分工的合理以及沟通的协调，是非常不容易的。这对我们以后在自己的工作中提高团队意识有大的帮助。

## 十、相关版权与许可

在本次系统制作过程中，除了使用 asianux 相关软件外, 在制作过程中主要参照了 backtrack3, operator 和 slax LiveCD

内核源代码来自[www.linux-live.org](http://www.linux-live.org)

主题来自[www.kde-look.org](http://www.kde-look.org)



### 指导老师意见与评价

在这次竞赛活动中，该小组同学从刚始信息的收集、资料的收集，到资料的学习，到整合等投入了极高的热忱。在整个 LiveCD 制作过程中，充分展示了一个团队的分工、互助的协作精神。



### 团队成员

姓 名	联系方式	主要分工
王洁林	13765823409	LiveCD 方向确定、工具和资料搜集，工具包测试。
杨震	13885130130	内核以及模块的修改配置。K D E 环境的修改与美化
李阳	13765819101	内核以及模块的修改配置。K D E 环境的修改与美化





## 附录：存在的问题

1. ntfs 挂载问题：现在挂载失败。编译安装 fuse & ntfs-3g 即可解决挂载问题。因为涉及版权问题。
2. NVI 显卡进入模式：根据硬件要求有时需要用户手动配置 xorg.Conf，在终端下输入“setup”设置 xwindow，点击 ok，保存设置就可以进入。或者输入 xconf && startx（后面这个命令不一定成功有待完善）

用户名：**root**

密码：空