MagicBox
中文渗透测试系统

何伊圣

Akast@ngsst.com

About MagicBox

1. Why is Linux
2. Something Different…存在的意义
3. Something HOTO…怎么使用
4. MagicBox - APT 渗透思路
5. Something TODO…一些想法

Why is Linux

- Windows 是微软的。
- Linux才是大家的。
- 让我们把Linux的魅力带给大家！
- 有兴趣作为驱动，Linux不难学。困难才有味道！
- 培训和交流氛围依然是重点！
- 甚至可以把Linux的界面改成和Windows一样来用……

MagicBox 系统概述

英文名称：	MagicBox Penetration Test System
中文名称：	魔方渗透系统
英文开发代号：	Genesis
中文开发代号：	麤 （cu）
开发团队：	NEURON Magicbox小组
第一版本发布时间：	2012年12月5日　　更新周期：3个月发布一个新版本
母板：	ubuntu 10.04；
系统内核：	3.2.6
系统界面：	gnome
体系结构：	32位 ISO　　VMWARE、ARM
ISO大小：	2.85 GB
文件MD5：	30e9dd2a00394585b69911e85ef6825d
主要功能：	各类信息系统的渗透测试，主要是WEB、无线。 OWASP live CD + backtrack + OpenPCD Live RFID Hacking System + 原创工具

MagicBox 存在的意义

- 国外用于信息安全的Linux live CD非常多，西班牙、俄罗斯、美国、欧洲等很多国家都有这样的安全系统，而国内还一个都没有，到目前为止magicbox是唯一一个。
- Backtrack是一个大而全的信息安全专用系统，越来越大，但绝大部分工具是我们平时不需要用的，而且官方说不考虑发布中文版本、英语之外的语言版本。Backtrack 5 R1 KDE中文版是我在蓝盾的时候为一个朋友做的，目前已经停止下载了，1万多的下载量。
- OWASP live CD 项目在6月份已经宣布停止了。
- OpenPCD Live RFID Hacking System是基于Fedora-15-x86_64的“物联网”安全测试系统。 http://www.openpcd.org/Live_RFID_Hacking_System

MagicBox 存在的意义

OWASP live CD project 2012 .6.16日官网已经宣布停止了，2011最后版本的软件列表：

- burpsuite-1.4.01-1
- cal9000-2.0-1
- cloud-1.0-1
- doc-2.0-1
- ende-1.0rc7-1
- fierce-1.0.3-1
- firefox-6.0.2-1
- grendel-scan-1.0-2
- httprint-301-1
- jbrofuzz-2.5-1
- maltego-3.0-1
- metasploit-3.5.1-1
- netcat-0.7.1-1
- nikto-2.1.4-1
- nmap-5.00-1
- paros-3.2.13-2
- ratproxy-1.58-1
- spikeproxy-1.4.8-1
- sqlbrute-1.0-1
- sqlmap-0.8-1
- tcpdump-4.0.0-1
- w3af-4041svn-1
- wapiti-2.2.1-1
- webgoat-5.3-RC1-2
- webscarab-20090122-2
- webslayer-svn-r4-1
- wireshark-1.2.7-1
- wsfuzzer-1.9.5-2
- zap-1.3.4-1

http://appseclive.org/content/possible-upgrade-webgoat-maybe-end-owasp-live-cd-project

MagicBox 存在的意义

- 把三款Linux live CD 的优点集合到一起。
- **中文化**，繁体、简体，开源工具汉化、商业工具合作中文版。
- **自由化**，从Windows平台到Linux平台的转变，让渗透测试更加自由。
- 属于我们的——自主、可控！

Something Different

- Backtrack 是一款大而全的安全专用系统，
- Magicbox 只针对于WEB和无线的渗透测试。

- 如果要用live CD做取证，可以单独做一款700MB以内的就差不多了，国内有厂家应该做的更专业吧，所以我们这个magicbox没有取证的功能，但magicbox live CD 里面还保留着取证的启动模式。

- 另外会有人用单台电脑跑live CD来做压力测试吗？应该没有这样的需求吧，所以不需要压力测试的功能。

- 逆向工程的工作我们觉得也没必要加入到live CD之中。

Something Different

- **RFID**
- libnfc套件
- nfc-tools套件
- proxmark3客户端
- mfcuk
- mfoc
- kdiff
- pcscd

- **Bluetooth**
- ubertooth-one客户端
- spectools

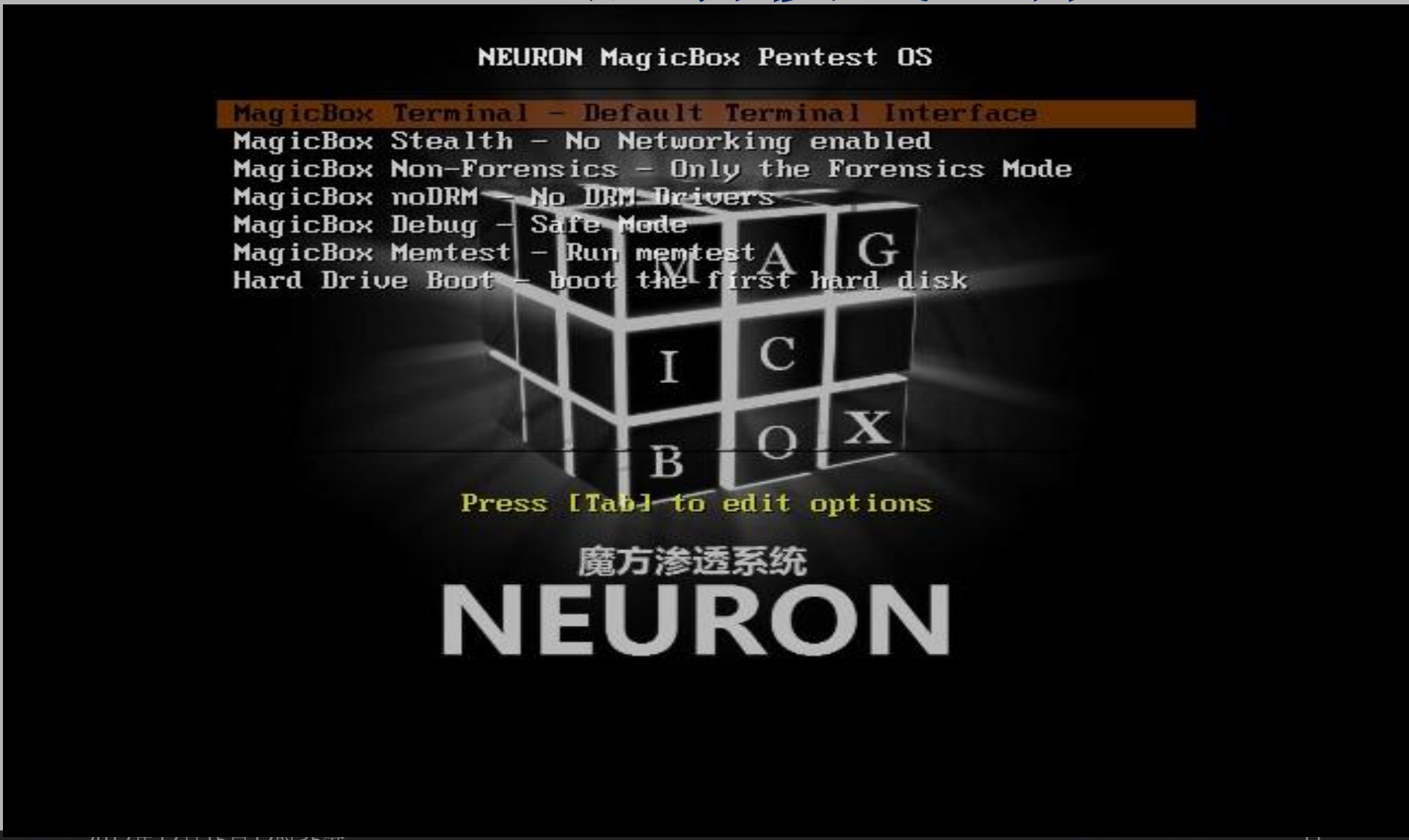
- **GSM**
- OsmocomBB套件

- **WIFI/LAN**
- Airoscript GTK
- ferret
- hamster
- Reaver
- inssider
- kismet
- spectools

Something HOTO…怎么使用

- 1、 刻录DVD光盘使用，ISO刻录；
- 2、 安装到U盘使用，ISO安装；
- 3、 安装到物理硬盘使用，U盘、光盘安装；
- 4、 安装到虚拟机使用，虚拟机版本；
- 5、平板电脑、安卓手机上使用ARM版本（测试中……）。

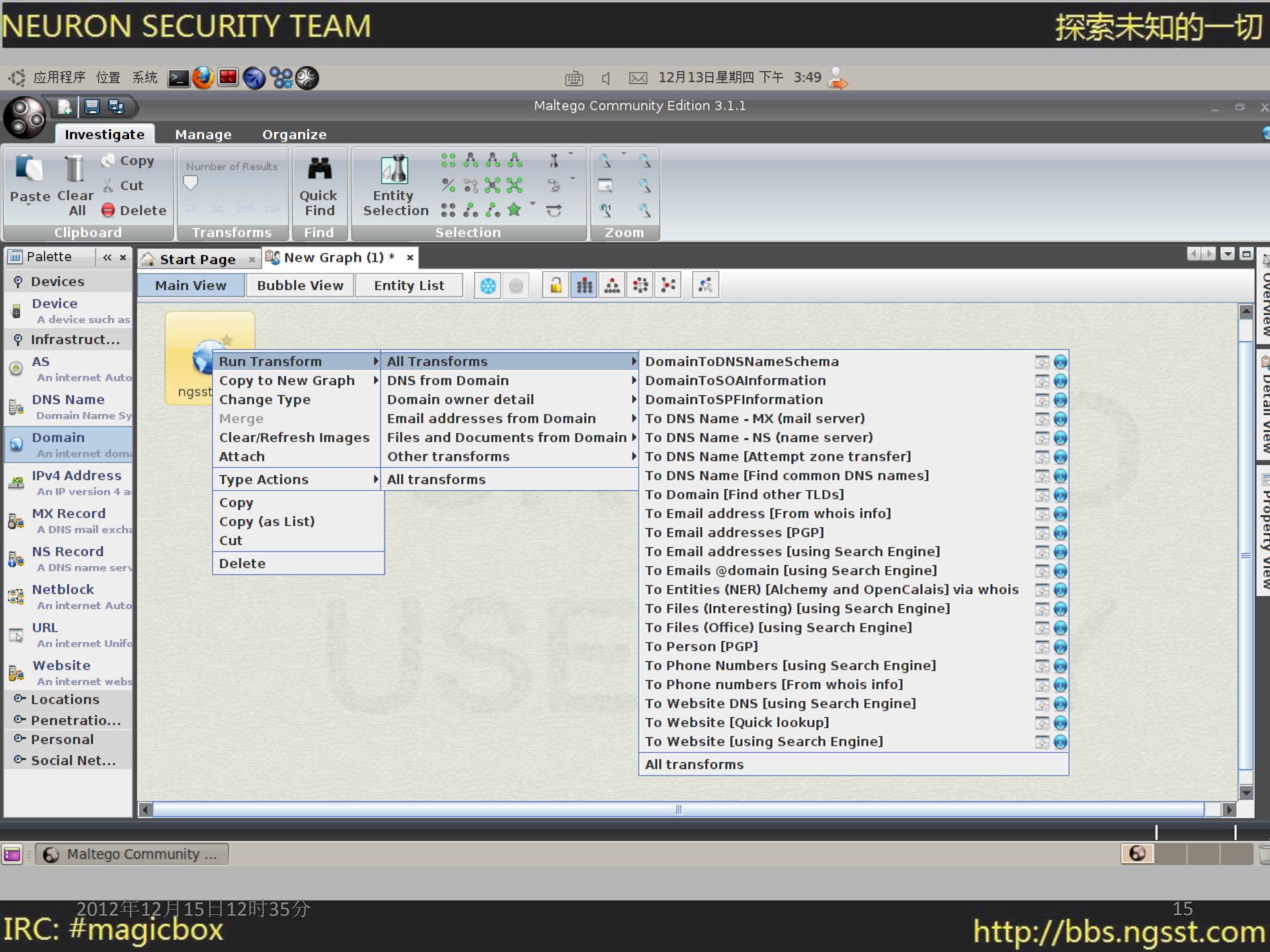
Live CD 启动模式选择

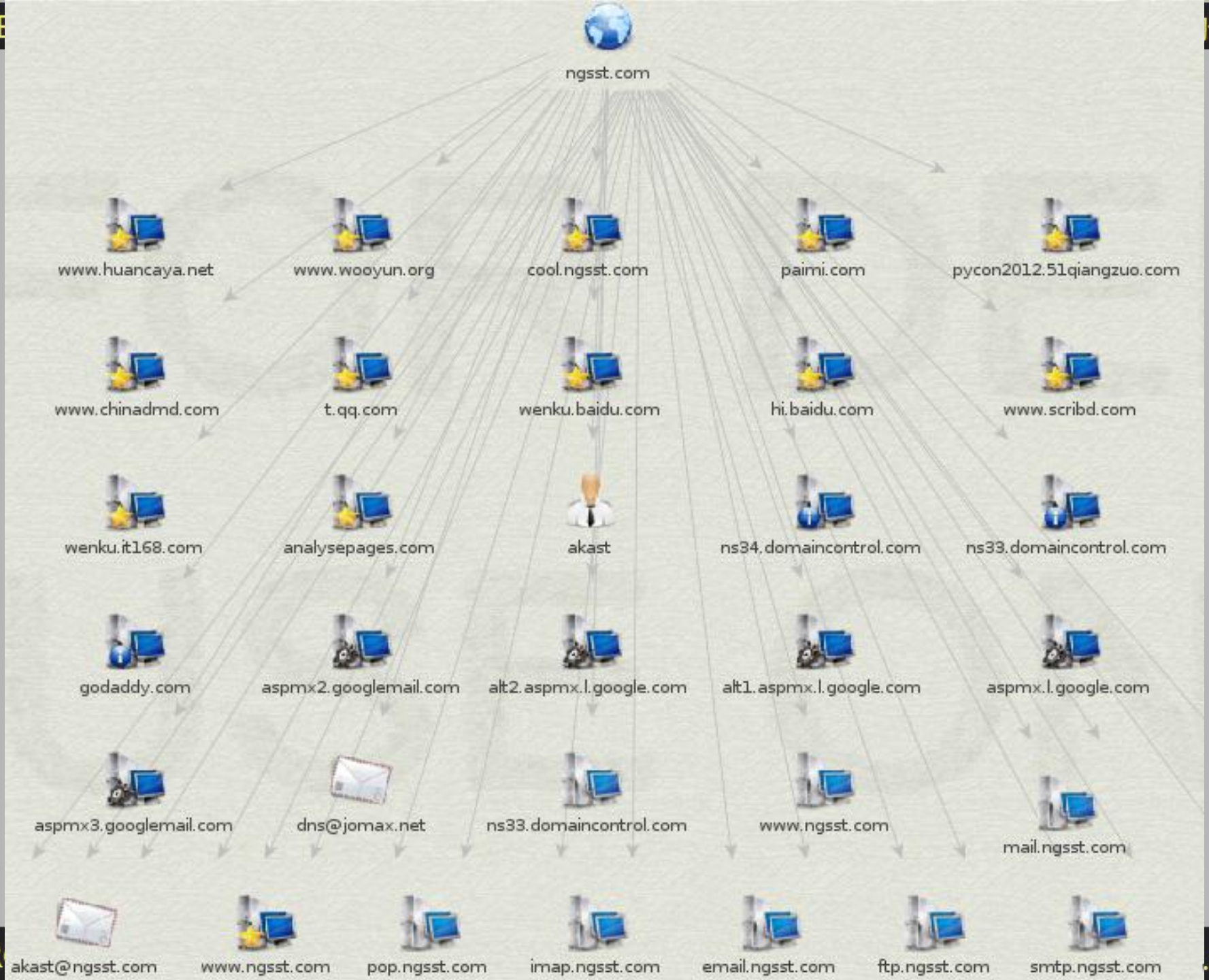


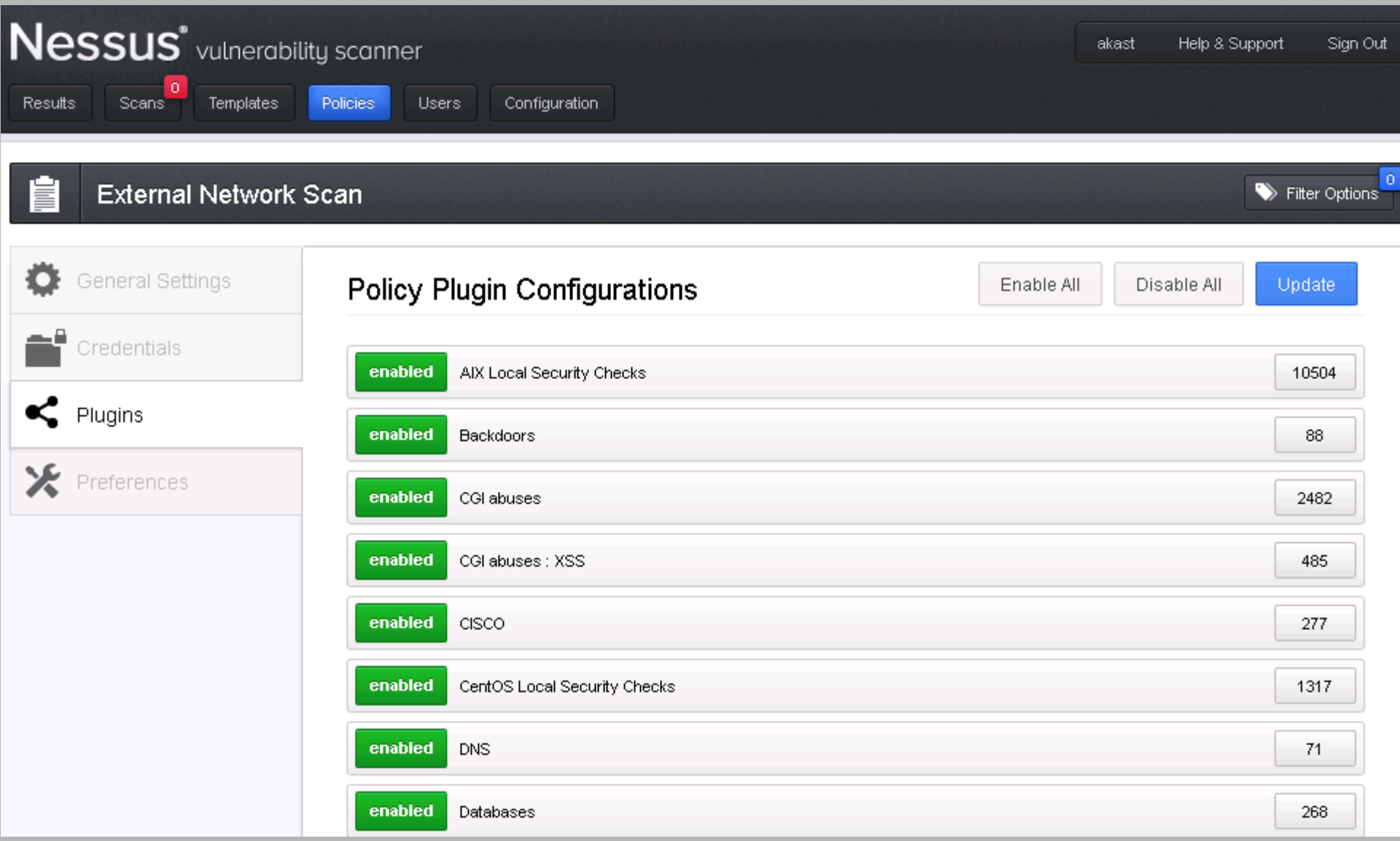
```
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       .................ccccccccc
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ..........................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffff..................
       ffffffff..................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing



       =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 974 exploits - 518 auxiliary - 158 post
+ -- --=[ 261 payloads - 28 encoders - 8 nops

msf > exit
root@magicbox:~/Desktop# _
```

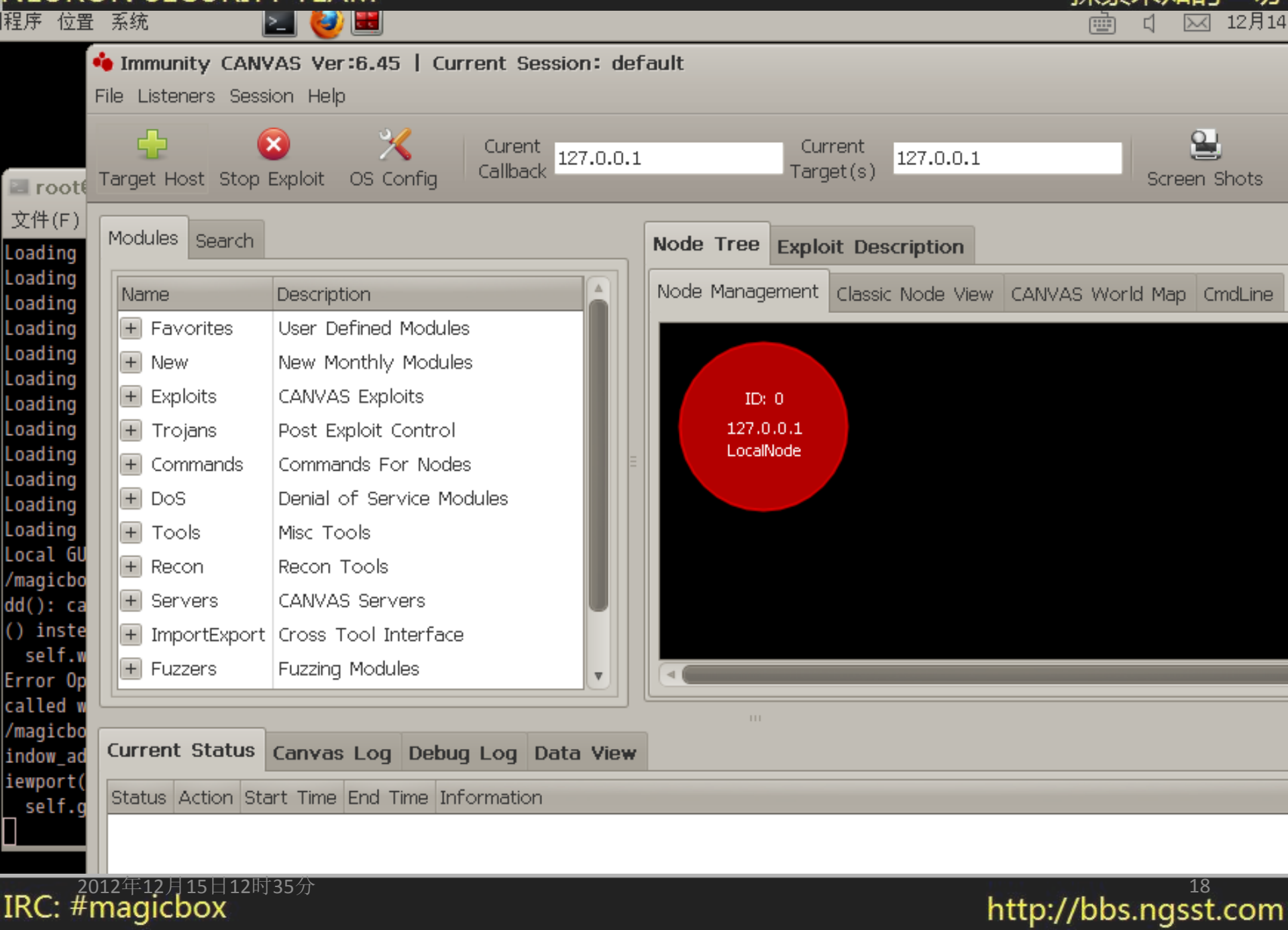
桌面环境/窗口管理器	RAM used	% CPU used	类型
KDE 4.6	363 MB	4 %	桌面环境
*** Unity	271 MB	14%	桌面环境(shell)
*** GNOME 3	193 MB	10%	桌面环境
GNOME 2.x	**191 MB**	**1 %**	**桌面环境**
XFCE 4.8	144 MB	10 %	桌面环境
LXDE	85 MB	10 %	桌面环境
IceWM	85 MB	2 %	窗口管理器
Enlightenment (E17 Standard)	72 MB	1 %	窗口管理器
Fluxbox	69 MB	1 %	窗口管理器
OpenBox	60 MB	1 %	窗口管理器
JWM	58 MB	1 %	窗口管理器

- 用户名：root 密码：magicbox
- 启动图形界面：startx


应用程序 位置 系统
12月13日星期四 下午 3:49
Maltego Community Edition 3.1.1
Investigate
Manage
Organize
Paste
Clear All
Copy
Cut
Delete
Clipboard
Number of Results
Transforms
Quick Find
Find
Entity Selection
Selection
Zoom
Palette
Devices
Device
A device such as
Infrastruct...
AS
An internet Auto
DNS Name
Domain Name Sy
Domain
An internet dom
IPv4 Address
An IP version 4 a
MX Record
A DNS mail excha
NS Record
A DNS name serv
Netblock
An internet Auto
URL
An internet Unifo
Website
An internet webs
Locations
Penetratio...
Personal
Social Net...
Start Page
New Graph (1) *
Main View
Bubble View
Entity List
ngsst
Run Transform
Copy to New Graph
Change Type
Merge
Clear/Refresh Images
Attach
Type Actions
Copy
Copy (as List)
Cut
Delete
All Transforms
DNS from Domain
Domain owner detail
Email addresses from Domain
Files and Documents from Domain
Other transforms
All transforms
DomainToDNSNameSchema
DomainToSOAInformation
DomainToSPFInformation
To DNS Name - MX (mail server)
To DNS Name - NS (name server)
To DNS Name [Attempt zone transfer]
To DNS Name [Find common DNS names]
To Domain [Find other TLDs]
To Email address [From whois info]
To Email addresses [PGP]
To Email addresses [using Search Engine]
To Emails @domain [using Search Engine]
To Entities (NER) [Alchemy and OpenCalais] via whois
To Files (Interesting) [using Search Engine]
To Files (Office) [using Search Engine]
To Person [PGP]
To Phone Numbers [using Search Engine]
To Phone numbers [From whois info]
To Website DNS [using Search Engine]
To Website [Quick lookup]
To Website [using Search Engine]
All transforms
Overview
Detail View
Property View
Maltego Community ...


ngsst.com
www.huancaya.net
www.wooyun.org
cool.ngsst.com
paimi.com
pycon2012.51qiangzuo.com
www.chinadmd.com
t.qq.com
wenku.baidu.com
hi.baidu.com
www.scribd.com
wenku.it168.com
analysepages.com
akast
ns34.domaincontrol.com
ns33.domaincontrol.com
godaddy.com
aspmx2.googlemail.com
alt2.aspmx.l.google.com
alt1.aspmx.l.google.com
aspmx.l.google.com
aspmx3.googlemail.com
dns@jomax.net
ns33.domaincontrol.com
www.ngsst.com
mail.ngsst.com
akast@ngsst.com
www.ngsst.com
pop.ngsst.com
imap.ngsst.com
email.ngsst.com
ftp.ngsst.com
smtp.ngsst.com


Nessus vulnerability scanner
akast
Help & Support
Sign Out
Results
Scans
0
Templates
Policies
Users
Configuration
External Network Scan
Filter Options
0
General Settings
Credentials
Plugins
Preferences
Policy Plugin Configurations
Enable All
Disable All
Update
enabled AIX Local Security Checks 10504
enabled Backdoors 88
enabled CGI abuses 2482
enabled CGI abuses : XSS 485
enabled CISCO 277
enabled CentOS Local Security Checks 1317
enabled DNS 71
enabled Databases 268


程序 位置 系统
12月14
Immunity CANVAS Ver:6.45 | Current Session: default
File Listeners Session Help
Target Host
Stop Exploit
OS Config
Curent Callback
127.0.0.1
Current Target(s)
127.0.0.1
Screen Shots
root
文件(F)
Loading
Loading
Loading
Loading
Loading
Loading
Loading
Loading
Loading
Loading
Loading
Loading
Local GU
/magicbo
dd(): ca
() inste
self.w
Error Op
called w
/magicbo
indow_ad
iewport(
self.g
Modules
Search
Name
Description
Favorites
User Defined Modules
New
New Monthly Modules
Exploits
CANVAS Exploits
Trojans
Post Exploit Control
Commands
Commands For Nodes
DoS
Denial of Service Modules
Tools
Misc Tools
Recon
Recon Tools
Servers
CANVAS Servers
ImportExport
Cross Tool Interface
Fuzzers
Fuzzing Modules
Node Tree
Exploit Description
Node Management
Classic Node View
CANVAS World Map
CmdLine
ID: 0
127.0.0.1
LocalNode
Current Status
Canvas Log
Debug Log
Data View
Status
Action
Start Time
End Time
Information

root@magicbox: /pentest/exploits/websploit

文件(F) 编辑(E) 查看(V) 终端(T) 帮助(H)

```
root@magicbox:/pentest/exploits/websploit# ./websploit

       (  (              )            (            )
       )\))(   '   (   ( /(           )\    (   ( /(
      ((_)()\ )   ))\  )\()) (   `  ) ((_) (  )\  )\())
      _(())\_)() /((_)((_)\  )\  /(/(   _   )\((_)(_))/
      \ \((_)/ /(_))  | |(_)((_)((_)_\ | | ((_)(_)| |_
       \ \/\/ / / -_) | '_ \(_-<| '_ \)| |/ _ \| ||  _|
        \_/\_/  \___| |_.__//__/| .__/ |_|\___/|_| \__|
                                |_|

                --=[WebSploit FrameWork
        +---**---==[Version :2.0.3
        +---**---==[Codename :CyberTron
        +---**---==[Available Modules : 17
                --=[Update Date : [r2.0.3-119 15.10.2012]


wsf > show modules

Web Modules                     Description
-------------------             ---------------------
web/apache_users                Scan Directory Of Apache Users
web/dir_scanner                 Directory Scanner
web/wmap                        Information Gathering From Victim Web Using (Met
asploit Wmap)
web/pma                         PHPMyAdmin Login Page Scanner


Network Modules                 Description
-------------------             ---------------------
network/arp_dos                 ARP Cache Denial Of Service Attack
network/mfod                    Middle Finger Of Doom Attack
network/mitm                    Man In The Middle Attack
network/mlitm                   Man Left In The Middle Attack
network/webkiller               TCP Kill Attack
network/fakeupdate              Fake Update Attack Using DNS Spoof
network/fakeap                  Fake Access Point
```

魔方渗透系统

NEURON

工具分类

- 信息搜集
- 端口扫描
- 漏洞扫描
- 漏洞利用
- 权限提升
- 权限维持
- ……

Hacking anything…

- 各类信息自动收集
- 社会工程利用
- 在线、离线密码破解
- 无线网络密码破解
- RFID射频卡破解
- 蓝牙、Wi-Fi、GSM、NFC各类无线安全测试
- 网站漏洞扫描、利用
- 数据库漏洞扫描、利用
- 服务器漏洞扫描、利用
- 网络设备漏洞扫描、利用
- Anything you want……一切为渗透而准备！

MagicBox - APT 渗透思想

- 高级持续性攻击 (Advanced Persistent Threat，简称 APT)
- 安全公司忽悠的新点子？
- 我们为什么会被APT？这不是一般企业、单位能够享受到的攻击“待遇”。除非是涉及到某种重大的利益关系。
- 一次像样的APT，需要雇用多个黑客团队，甚至是动用国家的黑客部队。
- 但我们做渗透测试可以采用APT这种攻击思想！

MagicBox - APT 渗透思想

1. **同服务器渗透**，最常见的旁注方法之一。
2. **同C段渗透**，最常见的旁注方法之一。
3. **同域名渗透**，二级、三级域名，DNS查询……
4. **同组织渗透**，同公司，同单位下属的目标，注册信息、备案信息查询。
5. **类域渗透**，ngsst.com、ngsst.org、ngsst.gov、ngsst.net，域名注册查询……
6. **同程序渗透**，不开源的源代码

Something TODO…一些想法

- 下载服务器
- 更新源服务器
- Java版本的一句话木马管理和控制端
- 团队渗透信息共享平台
- ARM版本

关注 Magicbox

- 1. IRC交流频道：#MagicBox，服务器：irc.freenode.net。
- 2. 官方微博：http://weibo.com/m4gicbox
- 3. 官方网站：http://www.ngsst.com；http://bbs.ngsst.com
- 4. 官方QQ 2群：**28265834**
- 5. 反馈邮箱：magicbox@ngsst.com

MagicBox 团队吸纳新人

- 1、系统开发组
- 2、软件开发组
- 3、软件汉化组
- 4、动态、静态美工组
- 5、debug测试组

THE END

谢谢！