



# Learn Git and GitHub without any code!

Using the Hello World guide, you'll start a branch, write comments, and open a pull request.

Read the guide

grayddq / GScan

本程序旨在为安全应急响应人员对Linux主机排查时提供便利，实现主机侧Checklist的自动全面化检测，根据检测结果自动数据聚合，进行黑客攻击路径溯源。

#security #security-scanning #security-tools #vulnerability-scanning #auditing #security-audit

182 commits

1 branch

0 packages

10 releases

1 contributor

Branch: master

New pull request

Create new file

Upload files

Find file

Clone or download

grayddq	Update User_Analysis.py	...	Latest commit e0caf5f on 30 Dec 2019
db	.		7 months ago
lib	Update User_Analysis.py		6 months ago
pic	code_update		13 months ago
.gitattributes	malwre_delsuc_info		14 months ago
.gitignore	.		7 months ago
GScan.py	code_update		13 months ago
README.md	code_update		13 months ago

README.md

## GScan v0.1

本程序旨在为安全应急响应人员对Linux主机排查时提供便利，实现主机侧Checklist的自动全面化检测，根据检测结果自动数据聚合，进行黑客攻击路径溯源。

### 作者

咚咚呛

如有其他建议，可联系微信280495355

### CheckList检测项

自动化程序的CheckList项如下：

- 1、主机信息获取
- 2、系统初始化alias检查
- 3、文件类安全扫描
  - 3.1、系统重要文件完整性扫描
  - 3.2、系统可执行文件安全扫描

- 3.3、临时目录文件安全扫描
- 3.4、用户目录文件扫描
- 3.5、可疑隐藏文件扫描
- 4、各用户历史操作类
  - 4.1、境外ip操作类
  - 4.2、反弹shell类
- 5、进程类安全检测
  - 5.1、CUP和内存使用异常进程排查
  - 5.2、隐藏进程安全扫描
  - 5.3、反弹shell类进程扫描
  - 5.4、恶意进程信息安全扫描
  - 5.5、进程对应可执行文件安全扫描
- 6、网络类安全检测
  - 6.1、境外IP链接扫描
  - 6.3、恶意特征链接扫描
  - 6.4、网卡混杂模式检测
- 7、后门类检测
  - 7.1、LD\_PRELOAD后门检测
  - 7.2、LD\_AOUT\_PRELOAD后门检测
  - 7.3、LD\_ELF\_PRELOAD后门检测
  - 7.4、LD\_LIBRARY\_PATH后门检测
  - 7.5、ld.so.preload后门检测
  - 7.6、PROMPT\_COMMAND后门检测
  - 7.7、Cron后门检测
  - 7.8、Alias后门
  - 7.9、SSH 后门检测
  - 7.10、SSH wrapper 后门检测
  - 7.11、inetd.conf 后门检测
  - 7.12、xinetd.conf 后门检测
  - 7.13、setUID 后门检测
  - 7.14、8种系统启动项后门检测
- 8、账户类安全排查
  - 8.1、root权限账户检测
  - 8.2、空口令账户检测
  - 8.3、sudoers文件用户权限检测
  - 8.4、查看各账户下登录公钥
  - 8.5、账户密码文件权限检测
- 9、日志类安全分析
  - 9.1、secure登陆日志
  - 9.2、wtmp登陆日志
  - 9.3、utmp登陆日志
  - 9.4、lastlog登陆日志
- 10、安全配置类分析
  - 10.1、DNS配置检测
  - 10.2、Iptables防火墙配置检测
  - 10.3、hosts配置检测
- 11、Rootkit分析
  - 11.1、检查已知rootkit文件类特征
  - 11.2、检查已知rootkit LKM类特征
  - 11.3、检查已知恶意软件类特征检测
- 12.WebShell类文件扫描
  - 12.1、WebShell类文件扫描

## 测试环境

- 系统：CentOS (6、7) + python (2.x、3.x)
- 权限：root权限启动
- 执行时间：默认安全扫描大概执行时间为4~6分钟，完全扫描在1~2小时之间，程序执行时间的长度由检测文件的多少决定，有可能会存在较长的时间，请耐心等待
- 兼容性：目前程序只针对Centos进行开发测试，其他系统并未做兼容性，检测结果未知

## 部署和执行

### 程序下载

```
root# git clone https://github.com/grayddq/GScan.git
root# cd GScan
```

### 参数参考

```
sh-3.2# python GScan.py -h
```

```
{version:v0.1}
{author:咚咚咚}
http://grayddq.top
```

Usage: GScan.py [options]

Options:

```
-h, --help      show this help message and exit
--version       当前程序版本
```

Mode:

## GScan running mode options

--overseas	境外模式，此参数将不进行境外ip的匹配
--full	完全模式，此参数将启用完全扫描
--debug	调试模式，进行程序的调试数据输出
--dif	差异模式，对比上一次的结果，输出差异结果信息。
--sug	排查建议，用于对异常点的手工排查建议
--pro	处理方案，根据异常风险生成初步的处理方案

Optimization:

## Optimization options

```
--time=TIME 搜索指定时间内主机改动过的所有文件, demo: --time='2019-05-07
00:00:00~2019-05-07 23:00:00'
--job 添加定时任务, 用于定时执行程序
--log 打包当前系统的所有安全日志 (暂不支持)
```

执行命令参考：

```
root# python GScan.py
```

```
root# python GScan.py --sug --pro
```

进行定时任务设置，异常日志将按行输出到./GScan/log/log.log，可通过syslog等服务同步日志信息。

```
root# python GScan.py --job #每天零点执行一次
```

```
root# python GScan.py --job --hour=2 #每2小时执行一次
```

## 程序脚本说明

```
GScan
----GScan.py                #主程序
----log                    #日志和结果记录
----lib                    #模块库文件
-----core                #调用库文件
-----common.py          #公共库模块
-----globalvar.py       #全局参数管理模块
-----option.py          #参数管理模块
-----ip                 ##ip地址定位库
-----egg                #yara打包动态库
-----malware            #恶意特征库
-----plugins            #检测插件模块库
-----Host_Info.py       #主机信息获取
-----File_Analysis.py   #文件类安全检测
-----History_Analysis.py #用户历史操作类
-----Proc_Analysis.py   #进程类安全检测
-----Network_Analysis.py #网络类安全检测
-----Backdoor_Analysis.py #后门类检测
-----User_Analysis.py   #账户类安全排查
-----Log_Analysis.py    #日志类安全分析
-----Config_Analysis.py #安全配置类分析
-----Rootkit_Analysis.py #Rootkit分析
-----SSHAnalysis.py      #secure日志分析
-----Webserver.py       #获取当前web服务的web根目录
```

```
-----Webshell_Analysis.py #webshell检测
-----webshell_rule          #webshell检测的规则
```

## 程序特点

- 1、程序检测的逻辑和方法，均是由一线安全应急人员根据多年实战经验总结出来的。
- 2、程序包括10W+的恶意特征信息，用于恶意文件的比对和查杀。
- 3、结果自动化分析，进行黑客攻击溯源

## 程序对标

入侵痕迹的检测按照经验归纳为如下子项，省去了一些安全配置和基线类等无关项。

注：对比内容为程序的实际检测输出结果，其仅代表个人的观点，不代表产品说明。

GScan	程序定位为安全人员提供的一项入侵检测工具，旨在尽可能的发现入侵痕迹，溯源出黑客攻击的整个路径。
chkrootkit	程序定位为安全人员提供的一项入侵检测工具，旨在发现被植入的后门或者rootkit。
rkhunter	程序定位为安全人员提供的一项入侵检测工具，旨在发现被植入的后门或者rootkit。
lynis	程序定位为安全人员日常使用的一款用于主机基线和审计的工具，可辅助漏洞扫描和配置管理，也可部分用于入侵检测。

检测项	GScan	chkrootkit	rkhunter	lynis
对比版本	v0.1	v0.53	v1.4.6	v2.7.1
【检测前检查项】文件alias检查	√	√		
【检测前检查项】系统重要文件完整性检测	√	√		
【主机文件检测】系统重要文件权限检测		√	√	
【主机文件检测】文件恶意特征扫描	√			
【主机文件检测】文件境外IP特征扫描	√			
【主机文件检测】敏感目录mount隐藏检测			√	√
【主机操作检测】境外IP操作记录检测	√			
【主机操作检测】可疑操作或异常检测	√	√		
【主机进程检测】CPU&内存使用异常检测	√			√
【主机进程检测】I/O异常检测				√
【主机进程检测】隐藏进程检测	√		√	
【主机进程检测】反弹shell进程检测	√			
【主机进程检测】可疑进程名称检测	√			
【主机进程检测】进程exe恶意特征检测	√			
【主机进程检测】僵尸进程检测				√
【主机进程检测】可疑的较大共享内存检测			√	
【主机进程检测】内存恶意特征检测				
【网络链接检测】境外IP链接检测	√			
【网络链接检测】恶意特征链接检测	√	√	√	
【网络链接检测】网卡混杂模式检测	√	√	√	√
【常规后门检测】LD_PRELOAD后门检测	√		√	
【常规后门检测】LD_AOUT_PRELOAD后门检测	√		√	
【常规后门检测】LD_ELF_PRELOAD后门检测	√		√	

检测项	GScan	chkrootkit	rkhunter	lynis
【常规后门检测】LD_LIBRARY_PATH后门检测	√		√	
【常规后门检测】ld.so.preload后门检测	√		√	
【常规后门检测】PROMPT_COMMAND后门检测	√			
【常规后门检测】Cron后门检测(/var/spool/cron/)	√			
【常规后门检测】Cron后门检测(/etc/cron.d/)	√			
【常规后门检测】Cron后门检测(/etc/cron.daily/)	√			
【常规后门检测】Cron后门检测(/etc/cron.weekly/)	√			
【常规后门检测】Cron后门检测(/etc/cron.hourly/)	√			
【常规后门检测】Cron后门检测(/etc/cron.monthly/)	√			
【常规后门检测】alias后门检测	√		√	
【常规后门检测】其他环境变量未知后门检测	√			
【常规后门检测】SSH后门检测	√			
【常规后门检测】SSH Wrapper后门检测	√			
【常规后门检测】inetd.conf后门检测	√		√	
【常规后门检测】xinetd.conf后门检测	√		√	
【常规后门检测】setUID后门检测	√			
【常规后门检测】setGID后门检测				
【常规后门检测】fstab后门检测				
【常规后门检测】系统启动项(/etc/init.d/)后门检测	√		√	
【常规后门检测】系统启动项(/etc/rc.d/)后门检测	√		√	
【常规后门检测】系统启动项(/etc/rc.local)后门检测	√		√	
【常规后门检测】系统启动项(/usr/local/etc/rc.d)后门检测	√		√	
【常规后门检测】系统启动项(/usr/local/etc/rc.local)后门检测	√		√	
【常规后门检测】系统启动项(/etc/conf.d/local.start)后门检测	√		√	
【常规后门检测】系统启动项(/etc/inittab)后门检测	√		√	
【常规后门检测】系统启动项(/etc/systemd/system)后门检测	√		√	
【账户安全检测】root权限账户检测	√		√	√
【账户安全检测】空口令账户检测	√		√	√
【账户安全检测】sudoers文件检测	√			√
【账户安全检测】用户组文件检测			√	√
【账户安全检测】密码文件检测	√		√	√
【账户安全检测】用户免密登录公钥检测	√		√	
【日志安全检测】secure日志安全检测	√			
【日志安全检测】wtmp日志安全检测	√	√		
【日志安全检测】utmp日志安全检测	√	√		
【日志安全检测】lastlog日志安全检测	√	√		
【日志安全检测】web日志安全检测				
【日志安全检测】其他服务日志安全检测				

检测项	GScan	chkrootkit	rkhunter	lynis
【安全配置检测】DNS设置检测	√			√
【安全配置检测】防火墙设置检测	√			√
【安全配置检测】hosts安全检测	√			√
【Rootkit检测】已知Rootkit文件特征检测	√	√	√	
【Rootkit检测】已知Rootkit LKM类特征检测	√	√	√	
【Rootkit检测】恶意软件类特征检测	√		√	
【WEBShell检测】Nginx服务WebShell检测	√			
【WEBShell检测】Apache服务WebShell检测	√			
【WEBShell检测】Tomcat服务WebShell检测	√			
【WEBShell检测】Jetty服务WebShell检测	√			
【WEBShell检测】Resin服务WebShell检测	√			
【WEBShell检测】Jenkins服务WebShell检测	√			
【WEBShell检测】其他默认web目录WebShell检测	√			
【漏洞类检查】服务漏洞或配置错误检查				√
【自动攻击路径追溯】攻击路径追溯	√			

## 检测结果

日志及结果目录默认：./GScan/log/gscan.log

## 运行截图

```
sh-3.2# python GScan.py -h
```

```

  _____      _____      _____      _____      .--  --.
 /  _____  /  _____  /  _____  /  _____  |  \  |  |  {version:v0.1}
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
 \  _____  \  _____  \  _____  \  _____  \  _____  {author:咚咚呛}
  _____      _____      _____      _____      .--  --.
  http://grayddq.top
```

Usage: GScan.py [options]

Options:

-h, --help show this help message and exit  
--version 当前程序版本

Mode:

GScan running mode options

--overseas 境外模式，此参数将不进行境外ip的匹配  
--full 完全模式，此参数将启用完全扫描  
--debug 调试模式，进行程序的调试数据输出  
--dif 差异模式，比对上一次的结果，输出差异结果信息。  
--sug 排查建议，用于对异常点的手工排查建议  
--pro 处理方案，根据异常风险生成初步的处理方案

Optimization:

Optimization options

--time=TIME 搜索指定时间内主机改动过的所有文件，demo: --time='2019-05-07  
00:00:00~2019-05-07 23:00:00'  
--job 添加定时任务，用于定时执行程序（默认每天零点执行一次）  
--hour=HOUR 定时任务，每N小时执行一次  
--log 打包当前系统的所有安全日志（暂不支持）

```
sh-3.2#
```

```
[root@iZ8vb55ijtquxpi4injvy2Z GScan]# python GScan.py --pro

GSCAN {version:v0.1}
      {author:咚咚哈}
      http://grayddq.top

开始扫描当前系统安全状态...

主机信息获取
主机名: iZ8vb55ijtquxpi4injvy2Z
主机IP: 172.26.77.30
系统版本: Linux-2.6.32-696.16.1.el6.x86_64-x86_64-with-centos-6.9-Final
主机时间: 2019-05-11 23:56:24

检测系统初始化扫描
[1]alias检查 [ OK ]

开始文件类安全扫描
[1]系统可执行文件安全扫描 [ OK ]
[2]系统临时目录安全扫描 [ OK ]
[3]各用户目录安全扫描 [ 存在风险 ]
[4]可疑隐藏文件扫描 [ 警告 ]

开始主机历史操作类安全扫描
[1]所有历史操作的可疑记录 [ 存在风险 ]

开始进程类安全扫描
[1]CUP和内存类异常进程排查 [ OK ]
[2]隐藏进程安全扫描 [ OK ]
[3]反弹shell类进程扫描 [ OK ]
[4]恶意进程信息安全扫描 [ OK ]
[5]exe程序安全扫描 [ OK ]

开始网络链接类安全扫描
[1]当前网络对外连接扫描 [ OK ]
[2]恶意特征类链接扫描 [ OK ]
[3]网卡混杂模式扫描 [ OK ]

开始恶意后门类安全扫描
[1]LD_PRELOAD 后门检测 [ OK ]
[2]LD_AOUT_PRELOAD 后门检测 [ OK ]
[3]LD_ELF_PRELOAD 后门检测 [ OK ]
[4]LD_LIBRARY_PATH 后门检测 [ OK ]
[5]ld.so.preload 后门检测 [ OK ]
[6]PROMPT_COMMAND 后门检测 [ OK ]
[7]cron定时任务后门检测 [ 存在风险 ]
[8]未知环境变量 后门检测 [ OK ]
[9]ssh 后门检测 [ OK ]
```



```
[9]ssh 后门检测 [ OK ]
[10]SSH wrapper 后门检测 [ OK ]
[11]inetd.conf 后门检测 [ OK ]
[12]xinetd.conf 后门检测 [ OK ]
[13]setuid 后门检测 [ OK ]
[14]系统启动项后门检测 [ OK ]

开始账户类安全扫描
[1]root权限账户安全扫描 [ OK ]
[2]空口令账户安全扫描 [ OK ]
[3]sudoers权限安全扫描 [ 警告 ]
[4]账户免密码证书安全扫描 [ 警告 ]
[5]账户密码文件扫描 [ OK ]

开始日志类安全扫描
[1]secure日志安全扫描 [ OK ]
[2]wtmp日志安全扫描 [ 警告 ]
[3]utmp日志安全扫描 [ OK ]
[4]lastlog日志安全扫描 [ OK ]

开始配置类安全扫描
[1]DNS设置扫描 [ OK ]
[2]防火墙设置扫描 [ OK ]
[3]hosts设置扫描 [ 警告 ]

开始Rootkit类安全扫描
[1]5S808 Variant A [ OK ]
[2]Adore Rootkit [ 存在风险 ]
[3]AjaKit Rootkit [ OK ]
[4]aPa Kit Rootkit [ OK ]
[5]Apache Worm [ OK ]
[6]Ambient Rootkit [ OK ]
[7]Balaor Rootkit [ OK ]
[8]Beastkit Rootkit [ OK ]
[9]beX2 Rootkit [ OK ]
[10]B0Bkit Rootkit [ OK ]
[11]OSX Boonana-A Trojan [ OK ]
[12]cb Rootkit [ OK ]
[13]CiNIK Worm [ OK ]
[14]CX Rootkit [ OK ]
[15]Abuse Kit [ OK ]
[16]Devil Rootkit [ OK ]
[17]Diamorphine LKM [ OK ]
[18]Dica-Kit Rootkit [ OK ]
[19]Dreams Rootkit [ OK ]
[20]Duarawkz Rootkit [ OK ]
[21]Ebury sshd backdoor [ OK ]
[22]ENYE LKM [ OK ]
[23]Flea Rootkit [ OK ]
[24]FreeBSD Rootkit [ OK ]
[25]Fu Rootkit [ OK ]
[26]Fuckit Rootkit [ OK ]
[27]GasKit Rootkit [ OK ]
[28]Heroin LKM [ OK ]
```

```
[85]VcKit Rootkit [ OK ]
[86]Vampire Rootkit [ OK ]
[87]Vole Rootkit [ OK ]
[88]WeaponX [ OK ]
[89]Xzikit Rootkit [ OK ]
[90]X-Org SunOS Rootkit [ OK ]
[91]zaRt-Kit Rootkit [ OK ]
[92]ZK Rootkit [ OK ]
[93]Miscellaneous login backdoors [ OK ]
[94]Sniffer log [ OK ]
[95]Suspicious dir [ OK ]
[96]Apache backdoor [ OK ]
[97]检测LKM内核模块 [ OK ]

开始Webshell安全扫描
[1]Webshell安全扫描 [ 存在风险 ]

-----
根据系统分析的情况，溯源后的攻击行动轨迹为：
[1][风险] 黑客在未知时间，输入了恶意指令/root/setuptools-19.6/README.txt，反弹shell类：> wget https://bootstrap.pypa.io/ez_setup.py -O - | python --user
[2][可疑] 黑客在2017-03-23 08:15:00时间，输入了恶意指令/usr/share/man/man1/.1.gz，文件 /usr/share/man/man1/.1.gz 属于可疑隐藏文件
[3][风险] 黑客在2019-02-25 21:51:34时间，输入了恶意指令/root/LinuxCheck/README.md，反弹shell类：bash -c '$(curl -sSL https://raw.githubusercontent.com/al9ne/LinuxCheck/master/LinuxCheck.sh)'
[4][风险] 黑客在2019-03-11 23:31:02时间，进行了账户修改设置，用户 gddtest 可通过sudo命令获取特权
[5][可疑] 黑客在2019-03-18 23:41:48时间，输入了恶意指令/root/... 文件 /root/... 属于可疑隐藏文件
[6][风险] 黑客在2019-03-20 00:40:15时间，进行了cron后门植入，反弹shell类：53 23 * * * root /bin/bash -i /dev/tcp/127.0.0.1
[7][风险] 黑客在2019-03-26 11:24:50时间，输入Rootkit后门，匹配到名为Adore Rootkit的rootkit目录规则 /var/log/ssh
[8][可疑] 黑客在2019-03-26 15:31:12时间，进行了账户修改设置，存在免密登录的证书，证书客户端名称：grayddq@gmail.com & liqing@liqingdeMacBook-Pro.local & test
[9][风险] 黑客在2019-03-29 00:23:32时间，输入了恶意指令/root/test.py，反弹shell类：if (('bash' in content) and (('dev/tcp/' in content) or ('telnet ' in content) or ('nc ' in content) or (
[10][可疑] 黑客在2019-04-24 11:23:51时间，输入了webshell文件/usr/share/nginx/html/123.php
[11][可疑] 黑客在2019-04-25 00:12:15时间，进行了HOSTS安全配置设置，存在境外IP设置：22.35.55.212
[12][可疑] 黑客在2019-04-30 17:48:51时间，输入了恶意指令/root/...abc，文件 /root/...abc 属于可疑隐藏文件
[13][可疑] 黑客在2019-04-30 18:21:35时间，进行了账户修改设置，存在特权用户gddtest
[14][风险] 黑客在2019-04-30 18:25:07时间，进行了恶意指令，引用恶意指令/root/setuptools-19.6/README.txt，可疑内容：反弹shell类：> wget https://bootstrap.pypa.io/ez_setup.py -O - | python --user
[15][风险] 黑客在2019-04-30 18:25:07时间，进行了恶意指令，境外IP操作类：【3】行为：访问钓鱼管理后台数据 (http://45.199.104.126/admiq/mylist.asp)
[16][可疑] 黑客在2019-04-22时间，通过用户root进行了主机登录，境外IP使用root登录主机：66.42.77.63

初步处理方案如下：
[1] rm /root/setuptools-19.6/README.txt #删除恶意指令
[2] rm /usr/share/man/man1/.1.gz #删除恶意指令
[3] rm /root/LinuxCheck/README.md #删除恶意指令
[4] vi /etc/sudoers #删除sudo设置
[5] rm /root/... #删除恶意指令
[6] vi /etc/cron.d/aaa #删除定时任务设置
[7] rm -rf /var/log/ssh #删除rootkit恶意指令
[8] vi /root/.ssh/authorized_keys #删除证书设置
[9] rm /root/test.py #删除恶意指令
[10] rm /usr/share/nginx/html/123.php #删除webshell文件
[11] vi /etc/hosts #删除或者更改境外hosts配置
[12] rm /root/...abc #删除恶意指令
[13] vi /etc/passwd #删除用户root权限
[16] passwd root #更改某用户密码

-----
扫描完毕，扫描结果已记录到 /root/tools/GScan/log/gscan.log 文件中，请及时查看
[root@izbv551jtxp141nvy2z GScan] #
```

```
[1]Webshell安全扫描          [ 存在风险 ]
.....
根据系统分析的情况，溯源后的攻击行动轨迹为：
[1][风险] 黑客在未知时间，植入了恶意文件/root/setuptools-19.6/README.txt，反弹shell类： > wget https://bootstrap.pypa.io/ez_setup.py -O - | python - --user
    排查参考：[1]rpm -qa /root/setuptools-19.6/README.txt [2]strings /root/setuptools-19.6/README.txt
[2][可疑] 黑客在2017-03-23 08:15:00时间，植入了恶意文件/usr/share/man/man1/.1.gz，文件 /usr/share/man/man1/.1.gz 属于可疑隐藏文件
    排查参考：[1]ls -l /usr/share/man/man1/.1.gz [2]strings /usr/share/man/man1/.1.gz
[3][风险] 黑客在2019-02-25 21:51:34时间，植入了恶意文件/root/LinuxCheck/README.md，反弹shell类：bash -c "$(curl -sSL https://raw.githubusercontent.com/al0ne/LinuxCheck/master/LinuxCheck.sh)"
    排查参考：[1]rpm -qa /root/LinuxCheck/README.md [2]strings /root/LinuxCheck/README.md
[4][风险] 黑客在2019-03-11 23:31:02时间，进行了账户修改设置，用户 gddtest 可通过sudo命令获取特权
    排查参考：[1]cat /etc/sudoers
[5][可疑] 黑客在2019-03-18 23:41:48时间，植入了恶意文件/root/.... 文件 /root/... 属于可疑隐藏文件
    排查参考：[1]ls -l /root/... [2]strings /root/...
[6][风险] 黑客在2019-03-20 00:40:13时间，进行了cron 后门植入,反弹shell类：53 23 * * * root /bin/bash -i /dev/tcp/127.0.0.1
    排查参考：[1]cat /etc/cron.d/aaa
    排查参考：[1]ls -a /var/log/ssh
[7][可疑] 黑客在2019-03-26 11:24:50时间，植入了Rootkit后门，匹配到名为Adore Rootkit的rootkit目录规则 /var/log/ssh
    排查参考：[1]cat /root/.ssh/authorized_keys
[8][可疑] 黑客在2019-03-29 00:23:32时间，植入了恶意文件/root/test.py，反弹shell类： if (('bash' in content) and (('dev/tcp/' in content) or ('telnet ' in content) or ('nc ' in content) or (
    排查参考：[1]rpm -qa /root/test.py [2]strings /root/test.py
[9][风险] 黑客在2019-04-24 11:23:51时间，植入了webshell文件/usr/share/nginx/html/123.php
    排查参考：[1]cat /usr/share/nginx/html/123.php
[10][可疑] 黑客在2019-04-25 00:12:15时间，进行了HOSTS安全配置变更，存在境外IP设置：22.35.55.212
    排查参考：[1]cat /etc/hosts
[11][可疑] 黑客在2019-04-30 17:48:51时间，植入了恶意文件/root/...abc，文件 /root/...abc 属于可疑隐藏文件
    排查参考：[1]ls -l /root/...abc [2]strings /root/...abc
[12][可疑] 黑客在2019-04-30 18:21:35时间，进行了账户修改设置，存在特权用户gddtest
    排查参考：[1]cat /etc/passwd
[13][风险] 黑客在2019-04-30 18:25:07时间，进行了恶意操作，引用恶意文件/root/setuptools-19.6/README.txt，可疑内容：反弹shell类： > wget https://bootstrap.pypa.io/ez_setup.py -O - | python - --user
    排查参考：[1]cat /home/gong/.bash_history
[14][风险] 黑客在2019-04-30 18:25:07时间，进行了恶意操作，境外ip操作类：【3】行为：访问钓鱼管理后台数据（http://45.199.104.126/admiq/mylist.asp）
    排查参考：[1]cat /home/gong/.bash_history
[15][可疑] 黑客在2019-04-22时间，通过用户root进行了主机登陆，境外IP使用root登陆主机：66.42.77.63
    排查参考：[1]who /var/log/wtmp

初步处理方案如下：
[1] rm /root/setuptools-19.6/README.txt #删除恶意文件
[2] rm /usr/share/man/man1/.1.gz #删除恶意文件
[3] rm /root/LinuxCheck/README.md #删除恶意文件
[4] vi /etc/sudoers #删除sudo设置
[5] rm /root/... #删除恶意文件
[6] vi /etc/cron.d/aaa #删除定时任务设置
[7] rm -rf /var/log/ssh #删除rootkit恶意文件
[8] vi /root/.ssh/authorized_keys #删除证书设置
[9] rm /root/test.py #删除恶意文件
[10] rm /usr/share/nginx/html/123.php #删除webshell文件
[11] vi /etc/hosts #删除或者更改境外hosts配置
[12] rm /root/...abc #删除恶意文件
[13] vi /etc/passwd #删除用户root权限
[16] passwd root #更改某用户密码

.....
扫描完毕，扫描结果已记入到 /root/tools/GScan/Log/gscan.log 文件中，请及时查看
```

## 参考链接

- <http://www.chkrootkit.org>
- <https://github.com/CISOfy/lynis>
- <http://rkhunter.sourceforge.net/>
- <https://github.com/stamparm/maltrail>