




# 级 CC 攻 击 防 御 工 具, 秒 级 检 查、


 Jager · 9 月 28 日 · 2015 年

 cckiller (//zhang.ge/tag/cckiller) · linux 安全设置

(//zhang.ge/tag/linux%e5%ae%89%e5%85%a8%e8%ae%be%e7%bd%ae) · WEB 防火墙

(//zhang.ge/tag/web%e9%98%b2%e7%81%ab%e5%a2%99) · 防火墙

(//zhang.ge/tag/%e9%98%b2%e7%81%ab%e5%a2%99)

 33729 次已读

张戈博客很久以前分享过一个 CC 攻击的防御脚本 (//zhang.ge/4649.html), 写得并不怎么样, 不过被 51CTO 意外转载了。博客从此走上了经常被人拿来练手的不归之路。

当然, 还是有不少朋友在生产环境使用, 并且会留言询问相关问题。根据这些问题的需求, 我花了一些时间重新写了一个比较满意的轻量级 CC 攻击防御脚本, 我给它取了一个比较形象的名字: CCKiller, 译为 CC 终结者。





(//res.zgboke.com/wp-content/uploads/2015/09/cckiller.jpg)

## 一、功能申明

分享之前我必须先申明一下, 众所周知, DDoS 攻击指的是分布式拒绝服务。而 CC 攻击只是 DDoS 攻击的一种, 本文所阐述的 CC 攻击, 指的是单个 IP 达到我们设定好的阈值并发请求, 而非海量 IP 的低并发攻击! 对于个人低配服务器, 除了使用 CDN 来防护, 至少我是没有想到如何抵挡海量 IP 攻击的! 因为每个 IP 都模拟正常的用户浏览器请求, 并不会触发防御阈值, 同时来 1000 个, 甚至上万个, 个人低配服务器的带宽在第一时间就会被占满, 就无法继续提供服务了。

当然, 用脚本也是无法防御 DDoS 大流量攻击的, 因为所有机房的防御带宽是有限的, 当攻击的流量超过了机房的防御带宽, 要么机房把你的服务器 IP 拉黑洞, 要么就一起死。因此, 如果你的服务器正遭受大流量攻击, 比如几十 G 上百 G, 一般机房或 CDN 节点都是扛不住的, 脚本也无能为力了, 赶紧换高防服务器吧!

## 二、功能介绍

通过以上申明, 也就大致给 CCKiller 一个定位: CCKiller 是用于个人低配服务器的轻量级 CC 攻击防御, 可以抵挡单个 IP 产生的高并发攻击。

目前设计的功能特性如下:

### ①、秒级检查

很多人写的防御脚本都是使用了Linux系统的计划任务 `crontab` 来定时检查的。而 `crontab` 的最细颗粒是 1 分钟, 也就是说脚本最快也只能 1 分钟检查一次。对于一些强迫症来说就会很不爽。

所以, 我还是按照以前分享的思路, 利用 `while` 循环实现秒级检查, 实现更细的颗粒。当然, CCKiller 更是被我写成了系统服务, 更加灵活稳定。

## ②、拉黑时长

CCKiller 可以设置拉黑时长, 默认为 10 分钟。当发现有恶意请求时, 会自动拉黑目标 IP, 并在拉黑时长结束后自动释放, 这个功能算是对我之前写的脚本的一个大的改进。

## ③、并发阈值

CCKiller 可以设定单个 IP 的最高请求数, 如果某个 IP 同时请求数超过了设定的阈值, 就会被暂时拉黑一段时间。

## ④、邮件发送

这个功能没啥好说的, 意义并不大。而且发送成功率和服务器的环境也有很大关系。

## ⑤、并发显示

安装后, 直接运行 `cckiller` (`//zhang.ge/tag/cckiller`) 会列出当前系统的请求排行, 可以清晰的看到当前请求 IP 和并发数。使用 `-s` 参数还可以继续定制需求, 比如 `cckiller` (`//zhang.ge/tag/cckiller`) `-s 10` 就能显示当前并发数排行前 10 名的 IP。

## ⑥、手动拉黑

支持手动拉黑, 执行后会立即检查, 将并发请求超过 `n` 的 IP 拉黑一段时间, 比如 `cckiller` (`//zhang.ge/tag/cckiller`) `-k 100` 就会将目前超过 100 个请求的 IP 拉黑一段时间, 如果没有则不会执行任何拉黑操作。

# 三、工具安装

## ①、在线安装

由于我可能经常会更新一些功能, 或修复一些 BUG, 所以仅提供在线安装, 以保证脚本是最新的。

安装非常简单, 执行如下命令就能进入配置步骤了:  
(//zhang.ge)

```
1 | curl -ko install.sh https://zhang.ge/wp-content/uploads/files/ccki
```

2017-12-13 补充: Ubuntu 系统请参考 joviqiao 的版本 => 传送门

(//zhang.ge/goto/aHR0cHM6Ly9naXRodWluY29tL2pvdmlxaWFvL0ND52lsbGVy)

2017-09-06 补充: CCKiller 代码早已提交到 Github, 有网友问到, 就来补充说明下 => 传送门

(//zhang.ge/goto/aHR0cHM6Ly9naXRodWluY29tL2phZ2VyemhhbmcvQ0NLaWxsZ)

## ②、工具配置

因为每个服务器的情况可能不一样, 所以有一个自定义配置的过程。

执行上述安装命令后, 将会进入自选配置部分, 如图:

```
#####
# CCKiller version 1.0.1 Author: Jager <ge@zhangge.net> #
# For more information please visit http://zhangge.net/5066.html #
#-----#
# Copyright @2015 zhangge.net. All rights reserved. #
#####

Do you want to use the default configuration? (y/n):
```

(//res.zgboke.com/wp-content/uploads/2015/09/CCKiller1.png)

提示否使用脚本默认配置, 如果选择是 (y), 那么显示默认配置, 并询问是否继续:

```
#####
# CCKiller version 1.0.1 Author: Jager <ge@zhangge.net> #
# For more information please visit http://zhangge.net/5066.html #
#-----#
# Copyright @2015 zhangge.net. All rights reserved. #
#####

Do you want to use the default configuration? (y/n): y

You choice the default configuration:
Configure info,Please Review:
=====
The Time interval : 20 s

The Forbidden Time: 600 s

Adminstrator Email: root@localhost

Connections Allow: 100
=====
Press any key to continue...
```

(//res.zgboke.com/wp-content/uploads/2015/09/CCKiller2.png)

默认配置如下:  
随机推荐: 替换WordPress默认搜索为百度站内搜索(知更鸟主



(//feed) x



The Time interval : 20 s  #每隔20s检查一次系统请求情况

The Forbidden Time: 600 s #拉黑时长设为 10 分钟

Adminstrator Email: root@localhost #邮件对象设置为  
root@localhost (即关闭邮件发送)

Connections Allow: 100 #单个 IP 并发限制为 100

如果不符合你的需求, 你可以使用 `ctrl + c` 组合键终止脚本, 或者先继续安装, 因为工具设计了配置修改的功能, 所以无需着急。

如果不使用默认配置 (n), 则会要你输入参数来自定义配置:

```
#####
# CCKiller version 1.0.1 Author: Jager <ge@zhangge.net> #
# For more information please visit http://zhangge.net/5066.html #
#-----#
# Copyright @2015 zhangge.net. All rights reserved. #
#####

Do you want to use the default configuration? (y/n): n

Please Input The Time interval of CCKiller Check(default: 20s): 10

Please Input the Forbidden Time of banned IP(default: 600s): 300

Please Input the E-mail of Adminstrator(default: root@localhost): ge@zhangge.net

Please Input the Maximum number of connections allowed(default 100): 60

Configure info,Please Review:
-----
The Time interval : 10 s

The Forbidden Time: 300 s

Adminstrator Email: ge@zhangge.net

Connections Allow: 60
-----
Press any key to continue...
```

(//res.zgboke.com/wp-content/uploads/2015/09/CCKiller3.png)

如图, 我将参数依次定义为每 10 秒进行检查, 拉黑时长为 300 秒, 发件人设置为博客邮箱, 并发限制设置为 60, 回车后会弹出一个提示, 让你检查, 如果没问题你直接回车就会安装并启动:



```
Installing CCKiller version 1.0.1 by zhangge.net
Download source files.....done

Starting cckiller ... [ OK ]

Installation has completed.

Config file is at /usr/local/cckiller/ck.conf

You can post comments and/or suggestions on http://zhangge.net/

[root@MyAlyServer ~]#
```

(//res.zgboke.com/wp-content/uploads/2015/09/CCkiller4.png)

### ③、服务控制

安装后, 会将 cckiller 注册成系统服务, 这时你就可以使用 service 来控制 cckiller 了。

使用标准的 service 定义, 支持 start | stop | restart | status 四个参数。所以, 你可以使用

service cckiller stop 来停止 cckiller, 也可以使用 service cckiller status 来查看状态。

### ④、集成命令

成功安装后, 系统还会多出一个 cckiller 的命令, 这个命令现有功能如下:

cckiller -h 可以调出帮助信息:

```
1 CCKiller version 1.0.0 Author: Jager <ge@zhang.ge>
2 Copyright ©2015 zhang.ge. All rights reserved.
3 Usage: cckiller [OPTIONS] [N]
4 N : number of tcp/udp connections (default 100)
5 OPTIONS:
6 -h | --help: Show this help screen
7 -k | --kill: Block the offending ip making more than N connections
8 -s | --show: Show The TOP "N" Connections of System Current
```

我蹩脚的英文也能凑合解释一下功能了吧~

-k 是拉黑功能, 需要在后面带上你想拉黑的并发数, 比如 cckiller -k 100 就会拉黑当前请求数大于 100 的 IP 一段时间 (和拉黑时长一致)

-s 是显示并发排名, 也需要在后面带上数字, 比如 cckiller -s 10 就能显示当前并发数排行前 10 名的 IP。

## ⑤、文件结构

如上图所示, 脚本安装目录为 /usr/local/cckiller, 其结构如下:

```
1 cckiller/
2 └─ cckiller      #主程序
3 └─ log/          #日志目录 (ver 1.0.1新增特性)
4 └─ ck.conf       #配置文件
5 └─ ignore.ip.list #白名单
6 └─ install.sh    #安装和卸载脚本
7
8 0 directories, 5 files
```

很简单也比较规范的的结构, 当然, 后续功能如果越来越多, 此结构可能会有所更新, 这是后话。

如果你熟悉 vim 的话, 只要编辑 ck.conf 就可以定义工具参数了:

```
1 ##### Paths of the script and other files
2 PROGDIR="/usr/local/cckiller"
3 PROG="/usr/local/cckiller/cckiller"
4 LOGDIR="/usr/local/cckiller/log"
5 IGNORE_IP_LIST="/usr/local/cckiller/ignore.ip.list"
6 IPT="/sbin/iptables"
7 DKName=CCKiller
8 DKVer=1.0.5
9 ##### SLEEP_TIME设定检查频率, 单位为秒
10 SLEEP_TIME=10
11 ##### NO_OF_CONNECTIONS设定并发限制
12 NO_OF_CONNECTIONS=60
13 ##### EMAIL_TO设定邮件的发送对象(请改为自己的邮箱地址)
14 EMAIL_TO="xxxxx@qq.com"
15 ##### BAN_PERIOD设定拉黑时长, 单位为秒
16 BAN_PERIOD=300
17 ##### 设置忽略端口, 比如 21,2121,8000 (默认不忽略)
18 IGNORE_PORT=
19
20 ##### 定义日志级别 INFO,DEBUG,WARNING,OFF (默认 INFO)
21 LOG_LEVEL=INFO
```

如果不熟悉也没关系。你还可以执行 ./install.sh -c 进行工具初始化, 重新设定所有参数, 过程和首次安装时一致, 这里就不赘述了。

## ⑥、白名单



工具安装时会默认将系统所有IP都加入白名单, 避免自己把自己给拉黑的尴尬。  
如果你还有其他要加白的IP, 可以将IP加入到 cckiller 安装目录下的  
ignore.ip.list 文件中, 每行一个。

Ps: 目前白名单还不支持IP段, 敬请期待后续更新。

## ⑦、卸载工具

有心的朋友可能注意到了 install.sh 是可以带参数的。我写代码的时候已经设计了几个常用的安装卸载功能, 具体如下:

```
1  #直接执行./install.sh 将会显示如下帮助信息
2  #####
3  #  CCKiller version 1.0.5 Author: Jager <ge@zhang.ge>          #
4  #  For more information please visit https://zhang.ge/5066.html #
5  #-----#
6  #  Copyright @2015 zhang.ge. All rights reserved.              #
7  #####
8
9  Usage: configure.sh [OPTIONS]
10
11  OPTIONS:
12  -h | --help : Show help of CCKiller
13  -u | --update : update Check for CCKiller [not available now]
14  -c | --config : Edit The configure of CCKiller again
15  -i | --install : install CCKiller version 1.0.0 to This System
16  -U | --uninstall : Uninstall cckiller from This System
```

其中:

- u 参数用来升级工具, 不过目前由于没时间还没写, 所以不可用 (Ver 1.0.2 已支持在线更新)
- i 参数用来安装工具, 如果已安装则会提示并终止
- c 参数用来配置工具, 方便安装后随时修改工具配置
- U 参数用来卸载工具, 注意是大写哦!

因此, 我们可以使用 ./install.sh -U 如图卸载 CCKiller:



```
[root@MyAlyServer ~]# ./install.sh -U
#####
# CCKiller version 1.0.1 Author: Jager <ge@zhangge.net> #
# For more information please visit http://zhangge.net/5066.html #
#-----#
# Copyright @2015 zhangge.net. All rights reserved. #
#####

Uninstalling cckiller...

Shutting down cckiller ... [ OK ]

Deleting script files.....done

Deleting cron job.....done

Uninstall Complete
```

(//res.zgboke.com/wp-content/uploads/2015/09/CCKiller6.png)

## 四、攻防测试

成功安装并启用 CCKiller 之后,我们可以使用压力测试工具来测试拉黑和释放效果,比如 webbench 或 ab 等。

假如 CCKiller 设定的并发限制为 100,检查间隔为 10s,使用 webbench 如下测试:

```
webbench -t 60 http://www.yourwebsite.com/
```

启动测试后,你可以立即去服务器上查看

[防火墙](http://zhang.ge/tag/%e9%98%b2%e7%81%ab%e5%a2%99%) (//zhang.ge/tag/%e9%98%b2%e7%81%ab%e5%a2%99%) :

iptables

多刷几下,就可以看到 webbench 所在服务器 IP 已经在 DROP 规则中了。

确定已被拉黑之后,你等个 10 分钟再来看

[防火墙](http://zhang.ge/tag/%e9%98%b2%e7%81%ab%e5%a2%99%) (//zhang.ge/tag/%e9%98%b2%e7%81%ab%e5%a2%99%) , 可以发现 webbench 所在服务器 IP 已经消失了,成功释放!

Ps: 如果邮件发送功能无误,那么应该也收到了工具发来的告警邮件,比如有一个饱受 CC 攻击煎熬的站长给我发来的反馈:



(//res.zgboke.com/wp-content/uploads/2015/09/cckiller5.png)

## 五、更多说明

### ①、配置并发限制

CCKiller 配置最大连接数限制时，建议根据单个网页产生的并发数来判断。

**情况 A：** 你网站做了动静分离，那么静态的请求就到另一个域名了（假设静态资源托管在另一台服务器或是 CDN），单个 IP 请求一个页面可能就会产生若干并发（假设 5 个），我们假设某个用户很猛，他喜欢快速拖拽打开你网站的多个网页，比如同时打开 10 个，那么正常用户的正常最大并发你也可以基本确定了吧？即并发限制： $10 \times 5 = 50$ 。如果有人同时刷新你几十个页面，要说没恶意你也不相信吧？

**情况 B：** 如果没有做动静分离，那么一个页面产生的并发可能就比较多了，每个 css、js、图片都会产生一次请求。所以，在这种情况下就需要稍微计算一下你网站单个页面产生的并发请求，比如一个单页面会产生 30 个请求，那么你也需要考虑用户可能会连续拖拽多个页面的情况，假设我允许用户可以同时刷新 10 页面，那么并发限制就可以设置为 300 了，依此类推。

**容错：** 从 A 和 B 来看，CCKiller 其实是有一个盲点的，那就是如果用户 IP 是某个公司的统一出口，也就是代理上网 IP，那么工具就容易误杀无辜了。所以，除了 A 和 B，你还得考虑你网站的受众人群类型。比如，我就一个个人博客，同一时刻被一个公司的多名同时多窗口拖拽访问，这种情况也不多吧？如果可能存在于这种受众人群，那么这个并发限制可以设置大一些，避免错杀无辜。当然，拉黑也就 10 分钟而已，也不至于“一失足成千古恨”。。。

当然，不管哪种情况，并发限制都可以比预估设置高那么一些，这个自行斟酌吧！

### ②、不足与完善

随机推荐：《替换WordPress默认搜索为百度站内搜索(知更鸟主 (//feed) ×

CCKiller 是我最近利用闲暇时间,匆忙之作,难免会有各种问题。也没时间进行测试和完善。不过目前还是有数位站长在使用,暂未反馈异常。当然,我分享的是在线安装方式,也是为后续的更新提供方便。不过对比我以前写的防御脚本,CCKiller 算是有了长足的进步了,很简单的安装,更强大的功能!



## 功能计划:

### A. 在线升级功能

这个不用多说,现有的工具已经预留了,后面可能会加入版本判断和更新的功能。

### B. 加入其他安全防护设置

目前工具其实是赶鸭子上架一样,直接就检查,也没有对系统环境做一些初始化的设置。比如网站通用的 iptables 设置、sync 洪水攻击防御等。后续会在安装的时候会作为一个可选功能。

### C. 集成傻瓜式的

#### 防火墙 (/zhang.ge/tag/%e9%98%b2%e7%81%ab%e5%a2%99) 控制功能

并不是每个站长都会熟练操作 iptables,所以可能考虑给 cckiller 这个命令集成一个 ban 和 unban ip 的功能,比如禁止一个 ip,执行 cckiller -D \$ip 即可,降低 iptables 的使用门槛。

另外,值得说明是,CCKiller 只适合裸奔的网站,而不适合使用 CDN 的网站,因为使用 CDN 之后,请求过来的 IP 都是 CDN 节点,你总不能把 CDN 节点也拉黑了吧?(Ps: 其实也可以用,你把并发限制稍微设置高一些就好了,就算拉黑 CDN 节点也就拉黑 10 分钟而已,不至于影响过大)

针对这个问题,后续我会找时间研究下直接从 Nginx 日志里面取得真实来源 IP 来拒绝访问。目前已经有了阶段性的进展了,敬请期待!

## 附录: 更新记录



### 2015-09-23 Ver 1.0.1:

- 支持白名单为 IP 段,格式为 IP 段通用格式,比如 192.168.1.0/24;

随机推荐:《替换WordPress默认搜索为百度站内搜索(知更鸟主)



(/feed) x

- 新增拉黑改为判断 iptables 是否已存在操作 IP 的判断方式;
- 增加日志记录功能, 每天一个日志文件, 位于安装目录下的 log 文件内;
- 集成手动拉黑 IP 和解封 IP 功能, 使用 cckiller -b IP 拉黑, 使用 cckiller -u IP 解封。

## 2015-11-29 Ver 1.0.2:

- 新增在线更新功能, 执行 `./install.sh -u` 即可检测是否有新版本:

```
=====
Local Version: 1.0.1

Remote information:

version:1.0.2
configure:updated
Update content:
Add 2 functions:
1. Added ignore ports of check, you could define some ports like 21,2121 that you wantn't check;
2. Added upgrade function of CCKiller.

=====
New Version Found, Do You Want Update Now? (y/n, default y):
```

(//res.zgboke.com/wp-content/uploads/2015/09/cckiller10212.png)

如果发现有新版本则显示更新内容, 并提示是否执行更新。选择之后将会更新到新版本, 需要重新配置, 但是 IP 或端口白名单会保持不变。

- 新增端口白名单功能

应网友需求, 新增了这个端口白名单功能。在配置 CCKiller 的最后一项会提示输入端口白名单:

```
Do you want to use the default configuration? (y/n): n

Please Input The Time interval of CCKiller Check(default: 20s):
The Time interval of CCKiller Check will set default 20s

Please Input the Forbidden Time of banned IP(default: 600s):
The Forbidden Time will set default 600s

Please Input the E-mail of Adminstrator(default: root@localhost): 287988783@qq.com

Please Input the Maximum number of connections allowed(default 100): 150

Please Input the ignore Ports of check like 21,8080,1080(default null): 21,8080,1080
```

(//res.zgboke.com/wp-content/uploads/2015/09/cckiller1022.png)

如果需要排除某些端口, 请如图最后一行所示, 输入端口并已逗号分隔, 比如 21,2121,8000

本次更新为非必须功能, 在用的朋友可以按需更新, 当然新增了在线更新这个功能, 也强力推荐更新一下, 方便后续检测 CCKiller 是否是最新版本。

更新难免存在不可意料的纰漏, 使用中存在任何问题请留言告知, 谢谢!

## 2016-06-20 Ver 1.0.3:

- 增加“永久”拉黑时长



(//zhang.ge)



有网友反馈, 需要设置更长的拉黑时间。原先的机制来看, 如果设置拉黑时间过长, 那么可能会产生很多后台释放黑名单脚本, 占用系统资源。

因此, 1.0.3 版本加入永久拉黑设置。只要在安装的时候, 设置拉黑时长为 0, 则 CCKiller 不会再产生后台释放脚本, 也不会释放已拉黑的 IP 了:

```
#####
# CCKiller version Author: Jager <ge@zhangge.net>
# For more information please visit http://zhangge.net/5066.html#
# Copyright ©2015 zhangge.net. All rights reserved.
#####

Do you want to use the default configuration? (y/n): n
Please Input The Rate(seconds) of cckiller check(default: 20):
The Time interval of CCKiller Check will set default 20s

Please Input the Forbidden Time(seconds) of banned IP(default: 600, if set 0 ip will banned until Restart System or iptables ): 0
Please Input the E-mail of Administrator(default: root@localhost):
The Administrator E-mail will set default root@localhost

Please Input the Maximum number of connections allowed(default 100):
The Max number for connections Allowed will set default 100

Please Input the ignore ports of check like 21,8080,1080(default null):
The ignore Ports of check will set default null

Configure info,Please Review:
=====
The Time interval : 20 s
The Forbidden Time: 0 s
Administrator Email: root@localhost
Connections Allow: 100
Ignore Port:
=====
Press any key to continue...
```

(//res.zgboke.com/wp-content/uploads/2015/09/cckiller1023.png)

但是, 考虑到灵活性问题, 并没有在新版中加入 `service iptables save` 的保存命令, 所以当你重启系统或者重启 iptables, 这些拉黑的 IP 都将得到释放。当然, 如果你真的想永久拉黑, 请手动执行 `service iptables save` 即可。

- 注册开机启动

新版本已将 CCKiller 服务注册到了开机启动服务列表, 重启系统不用在担心未启动 CCKiller 了。

- 兼容 Centos 7

目前博客运行在 Centos 7 系统, 所以将 CCKiller 也做了一下兼容, 其实就是在 Centos 7 上安装了 iptables。并且修复了 Centos7 系统对已拉黑 IP 的判断问题。

Ps: 以上功能如果你觉得有用, 可以执行 `install.sh -u` 进行在线更新, 记得是小写 u 哦。

2016-10-09 Ver 1.0.4:

- BUG 修复

随机推荐: 《替换WordPress默认搜索为百度站内搜索(知更鸟主



(//feed) ×



根据网友反馈, 发现攻防测试中一个IP不能被拉黑, 经过分析发现命中了白名单。而实际上白名单中并没有IP段, 只因IP同属于一个网段。因此, 在是否属于IP段的判断中, 加入对斜杠的筛选, 也就是说只判断白名单中存在斜杠(/)的条目, 简单粗暴!

**2017-05-20 Ver 1.07** (中间漏记了2个小版本, 也不记得修复了啥)

- 日志级别、开关

根据网友建议, 新增日志控制开关, 参数为 LOG\_LEVEL, 支持 INFO、DEBUG 和 OFF 3 个参数, 其中 INFO 表示仅记录拉黑和释放 IP, DEBUG 记录全部日志, 包括拉黑、释放的报错信息, OFF 表示关闭日志。

如果需要使用该功能, 可以执行 ./install.sh -u 在线更新或直接重新安装。

¥ 6 7 8 9 10 182

## ☆ 相关文章

太狗血了! 分享一下张戈博客百度收录排名异常的检查记录

11月1日 · 2015年

(//zhang.ge/5070.html)

浅谈个人博客网站 or 屌丝 vps 服务器暴露真实 IP 的危险性

4月4日 · 2015年

(//zhang.ge/5029.html)

阿里云盾网站安全防御 (WAF) 的正确使用方法

2月28日 · 2015年

CVE-2015-0235:Linux glibc 高危漏洞的检测及修复方法

1月29日 · 2015年

随机推荐: 《替换WordPress默认搜索为百度站内搜索(知更鸟主



(/feed) ×



(//zhang.ge)



(//zhang.ge/5018.html)

(//zhang.ge/5015.html)

## 259 条回应

欢迎来到张戈博客, 请留下有营养的评论~

昵称



提交评论



qz

2018-2-23 · 13:39  
(//5066.html?replytocom=19646#respond)

你好, 请问能只监控指定端口的访问吗? 例如只监控 80 端口, 22 端口, 因为我服务器上也运行了爬虫, 结果把别人服务器给 ban 了。爬不动了



诗人博客

2018-2-27 · 9:50  
(//5066.html?replytocom=19646#respond)

还不错, 订一下,  
ps: 评论框的动画效果可以去了, 整个网页都抖动, 不太友好。  
另, 能加个友链吗?



Jager

2018-2-27 · 10:37  
(//5066.html?replytocom=19647#respond)

@ 诗人博客

(//zhang.ge/goto/aHR0cHM6Ly93d3cuQmx1ZU5vb2luY29t) 评论工具  
条上是有个关闭震动按钮的, 同一个浏览器关闭一次即可。



qu

2018-3-3 · 16:18  
(//5066.html?replytocom=19677#respond)

安装的时候提示 ./usr/local/cckiller/cckiller: 37: /usr/local/cckiller/cckiller: Syntax error: Bad for loop variable  
怎么办?



feiji

2018-3-3 · 16:19  
(//5066.html?replytocom=19674#respond)

IP 并发 50 会否屏蔽掉搜索引擎蜘蛛呢 ! ! ! ! ! ! ! !



SaFly.ORG

2018-3-18 · 10:34  
(//5066.html?replytocom=19701#respond)

赞一个!  
想问一下对 IPv6 支持怎么样~



ゝ相生相克

2018-3-20 · 19:19  
(//5066.html?replytocom=19711#respond)

这个帖子真心有用哈哈

随机推荐: 《替换 WordPress 默认搜索为百度站内搜索(知更鸟主)》 (//feed) ×





啊啊啊



(//zhang.ge)

2018-3-25 · 11:37  
(/5066.html?)

安装后, cc 是不怕了, 但有个进程占用我 95 以上 cpu。卸载了才恢复正常。这是啥情况



Jager

2018-3-25 · 11:44  
(/5066.html?)

@ 啊啊啊 什么进程呢?

replytocom=19729#respond)



啊啊啊

2018-3-25 · 14:10  
(/5066.html?)

@Jager (//zhang.ge/) Top 看是个 Python。具体我也不知道啥小白。卸载了就没有了 centos7 系统

replytocom=9730#respond)



Jager

2018-3-25 · 17:41  
(/5066.html?)

@ 啊啊啊 这个是 shell 脚本, 并不涉及 python, 估计是其他原因

replytocom=31#respond)



CE 安全网

2018-4-30 · 12:52  
(/5066.html?)

感谢 Jager 大哥的工具, 受益匪浅。  
另外想申请个友情链接, 本站已经添加。  
友联通过与否都请通知下。谢谢拉~

replytocom=19811#respond)



狂放

2018-5-1 · 0:35  
(/5066.html?)

Nginx 是可以通过'XFF'之类的字段取得 ip 的, 但是不用中间件你也屏蔽不了啊

replytocom=14#respond)



小熊

2018-5-3 · 18:21  
(/5066.html?)

service cckiller start 提示没有这个服务的, 需要安装这个  
yum install which -y

replytocom=19824#respond)



减压玩具网

2018-5-4 · 16:37  
(/5066.html?)

感谢博主的分享, 现在已经成我建站必装的工具了 😊

replytocom=19827#respond)



农业微信群孵化

2018-5-9 · 14:50  
(/5066.html?)

签到成功! 签到时间: 下午 2:40:06, 每日签到, 生活更精彩!  
我就想说说你们这些站长是不是什么都会啊! 唉 自叹不如, 你这个防攻击脚本非常好, 对于我们这些不会的很有帮助, 谢谢了, 找时间我参照着部署下。  
我的网站是热农网热农网, 农业微信群孵化  
(//zhang.ge/goto/aHR0cDovL3d3dy5yZW5vbmducubmV0) 站长有时间的话给我指导下, 没丁点流量 运行快半年了

replytocom=19845#respond)



哩啦啦

2018-5-15 · 16:11  
(/5066.html?)

前端有反向代理, 有没有方法取到真实 ip 呢?

replytocom=19871#respond)



杨小杰

2018-6-10 · 8:09  
(/5066.html?)

Jager 大哥, 请问这个工具能识别真实 ip 吗? 我看服务器识别的 ip 很多都是 cdn 节点 ip, 要是节点 ip 拉黑了那不就完蛋了

replytocom=19900#respond)

**Jager**

(@//zhang.ge)

reply to 2018-7-1 19:58 (respond)

@ 杨小杰 (//zhang.ge/goto/aHR0cDovL3d3dy55b3VuZ3hqLmNu) 基于 4 层 TCP 和 iptables 实现, 无法识别真实 IP, 并且 iptables 无法间接拉黑真实 IP, 只能拉黑直接访问 IP (CDN 节点 IP)

**W**

请问一下 安装的时候卡住了, 是哪里出问题?

2018-6-15 · 21:04  
(/5066.html?  
replytocom=19946#respond)

**Jager**

@W 重新安装试下

2018-7-1 · 19:54  
(/5066.html?  
replytocom=19988#respond)

**W**

请问一下安装失败是哪里出了问题?

2018-6-15 · 21:22  
(/5066.html?  
replytocom=19947#respond)

**Liues**

在使安装了宝塔的情况下, 能使用吗?

2018-7-27 · 18:13  
(/5066.html?  
replytocom=20077#respond)

**哩啦啦**

发件人 ROOT 能否更改呢, 多个服务器无法分辨

2018-7-28 · 15:31  
(/5066.html?  
replytocom=20088#respond)

**CCKiller 卸载**

张哥, 卸载不掉。在 centos\_7\_04\_64 里面有兼容性的问题, 卸载之后卸载不掉。期待收到你的回复谢谢。

2018-12-3 · 16:33  
(/5066.html?  
replytocom=20423#respond)

**Jager**

@CCKiller 卸载 卸载不了是什么表现?

2019-1-20 · 13:50  
(/5066.html?  
replytocom=20423#respond)

**雅、涵**

http\_cf\_connecting\_ip  
如果使用 cfcdn 的, 可以用这个取得真实 ip  
还可以利用 api 在 cdn 上直接封禁, 而不是本机抵抗  
建议更新加入 CF 功能

2018-12-13 · 7:47  
(/5066.html?  
replytocom=20330#respond)

**Jager**

@ 雅、涵 (//zhang.ge/goto/aHR0cDovL3d3dy55b3VuZ3hqLmNu) 嗯, 如果是有用 CDN, CDN 一般都应该有自己的一套防护机制, 不需要用这个脚本。

2019-1-1 · 16:50  
(/5066.html?  
replytocom=20142#respond)

**明天**

这个脚本目前似乎与宝塔面板互相突出了。宝塔版本为 6.4.1, Nginx 2014.2.2, php7.3, centos7.6, 安装此脚本后, 测试是可以防御, 但是重启 Centos 后, 发现网站访问不了, 且排除自己 IP 拉黑的情况, 可以 ping 通, 也可以 SSH 登入。不知道其他朋友有没有反馈此问题。

2018-12-21 · 21:56  
(/5066.html?  
replytocom=20142#respond)

**Jager**

@ 明天 可以登进去看下 iptables 规则是什么情况: iptables -nB70#respond)

2019-1-1 · 16:44  
(/5066.html?  
replytocom=20142#respond)

随机推荐: 《替换WordPress默认搜索为百度站内搜索(知更鸟主 (//feed) x



Akun

请问有防止海量 IP 低频攻击的办法吗?



(//zhang.ge)

2019-1-21 · 13:55  
(/5066.html?  
replytocom=20429#respond)



Jager

@Akun 这个就比较困难了, 一般需要将所有 IP 记录下来, 做分析字典库。很多大型防御系统, 比如腾讯的大禹才会做这类识别系统。

2019-1-21 · 13:59  
(/5066.html?  
replytocom=20432#respond)



Akun

@Jager (//zhang.ge/) 你好, 我最近遭受一个海量 IP 攻击, IP 地址前两段是固定的, 后两段都是变化的, 手动拉黑也拉不完全, 请问有什么办法整体拉黑或者防御吗? 比如 220.110.xxx.xxx 的所有 IP 地址能不能用一个 IP 地址段就能完全表示?

2019-1-21 · 14:54  
(/5066.html?  
replytocom=20441#respond)



Jager

@Akun 可以啊, 封锁整个 IP 段, 只要你不怕误封了同网段的正常 IP。我看了下这个应该是日本的段, 你执行:

2019-1-21 · 15:45  
(/5066.html?  
replytocom=20444#respond)

```
1 | iptables -I INPUT -s 220.110.0.0/10 -j DROP
```

即可生效, 如果需要保存这个规则, 则执行 `service iptables save`



教书先生

脚本失效, 请更新下

2019-1-27 · 22:20  
(/5066.html?  
replytocom=20465#respond)



Jager

@教书先生 🐱 只是域名换了而已, 已更新。

2019-1-27 · 22:35  
(/5066.html?  
replytocom=20466#respond)



明月清风

感谢博主的无私奉献。

2019-2-3 · 11:47  
(/5066.html?  
replytocom=20504#respond)



hi

如果从 4 层取 IP 的话是只能取得 `remote_addr`, 不能获取代理的 IP 地址, 假如网站前面放了 CDN, 就需要获取 XFF 中的 IP 地址了, 不知道能不能改进一下

2019-2-15 · 18:11  
(/5066.html?  
replytocom=20515#respond)



Jager

@hi 关键是这个脚本是通过 iptables 封堵的, 只能支持直接来源 IP, 也就是和网站服务器接触最近的那个 IP, 搞不了。如果用了 CDN 则只能用 nginx 获取真实 IP 然后来封堵。

2019-2-16 · 19:43  
(/5066.html?  
replytocom=20534#respond)



尚寂新

话说这个可以跟宝塔一起跑吗

2019-2-25 · 12:16  
(/5066.html?  
replytocom=20573#respond)



buxia

如果加了 cdn 的话, 会拦截 cdn 节点 ip 吗?

2019-3-1 · 18:20  
(/5066.html?  
replytocom=20582#respond)





博客之家



(//zhang.ge)

2019-5-11 13:25  
replytocom=20598#respond



现在对攻击只有无奈 + 无言.....



Lhaihai

2019-4-30 17:17  
(/5066.html?replytocom=20598#respond)

你好, 安装 install 脚本在 Centos7 运行成功, 但是在 Debian8 系统安装失败  
报错信息:  
./install.sh: 316: ./install.sh: Syntax error: "(" unexpected



Jager

2019-5-2 15:11  
(/5066.html?replytocom=20598#respond)

@Lhaihai 目前只支持 centos, 如果你熟悉 debian 可以去 github fork 一份修改即可。



优启梦

2019-5-10 9:52  
(/5066.html?replytocom=20598#respond)

大佬, 能不能改成判断 UA 的, 检测大量重复 UA 直接拉黑这个 UA 的 IP 毕竟攻击的话, ua 重复很多

< Previous (//zhang.ge/5066.html/comment-page-2#comments)

1 (//zhang.ge/5066.html/comment-page-1#comments)

2 (//zhang.ge/5066.html/comment-page-2#comments) 3

Copyright © 2013-2019 张戈博客 保留所有权利 . 网站统计 (https://tongji.baidu.com/web/welcome/ico?s=28cbd48a7fec21f3444ffc66121ea67d)

s=28cbd48a7fec21f3444ffc66121ea67d)

博客稳定运行: 5年199天1时8分41秒

