金将军的服务器也有漏洞？

这是一个创建于 79 天前的主题，其中的信息可能已经有所发展或是发生改变。

长期以来，我对朝鲜的网络很好奇，时不时就要来一次扫描，自认为这只是徒劳，毕竟金将军的网络系统应该不至于轻易让一个无业青年搞定。前段时间发现过 Windows XP ，后来就销声匿迹了，转而变成 RHEL 。今天我又扫描，不光发现 XP ，而且还发现 XAMPP ，然后 MySQL Root ，不说你也懂。 提权过后， 3389 ，安装屏幕阅读器，打开 CMD ，尝试追踪路由，网络质量让我大跌眼镜。 这回总算意外地实现了梦想——进入一个几乎封闭的国家的电脑系统来上网，本打算直接在朝鲜的电脑上登陆 V2EX ，后来发现要解决语言包的问题实在太麻烦，然后就作罢了。

第 1 条附言 • 78 天前
看到很多回复，实在是感谢万分。
第 2 条附言 • 77 天前
好了，金将军的服务器容易被肉鸡这件事应该可以收尾了，因为，他不通过修复漏洞来解决问题，而只是简单地利用了快照功能，每隔一段时间就自动恢复到创建快照的状态。小伙伴们想要玩请继续玩，我抽身了。
第 3 条附言 • 74 天前
现在算是完全被玩坏了，我一直搞不懂是小伙伴们太会玩还是金将军太不耐玩。
将军 朝鲜 扫描 XAMPP
183 回复 | 直到 2016-04-17 13:22:03 +08:00

1 2 1 ‹ ›

1
wm5d8b 79 天前 via Android
国防部吗

2
ETiV 79 天前 via iPhone ♥ 30
卧槽，你别七搞八搞的把朝鲜导弹发出来……
2333333

3
skydiver 79 天前 via iPad
在朝鲜的电脑登陆了 V2EX ……然后直接暴露了自己是谁

4
towser 79 天前


大浦洞已就绪


5
chenyao168 79 天前
C:\>tracert -d www.v2ex.com

Tracing route to v2ex.edge.zgslb.net [23.251.121.133]
over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 10.191.0.33
2 <1 ms <1 ms <1 ms 172.16.0.30
3 * <1 ms <1 ms 172.16.9.1
4 59 ms 59 ms 59 ms 172.16.10.1
5 59 ms 59 ms 61 ms 219.158.39.41
6 216 ms 222 ms 217 ms 63.218.61.25
7 231 ms 231 ms 235 ms 63.218.174.105
8 227 ms 227 ms 227 ms 63.217.254.186
9 225 ms 227 ms 226 ms 192.254.91.26
10 247 ms 235 ms 226 ms 192.254.91.2
11 229 ms 229 ms 229 ms 23.251.121.133

Trace complete.


6
hjq98765 79 天前
又不是物理隔离怎么可能没漏洞


7
lwbjing 79 天前
@ETiV 大半夜把楼下的猫都笑出来了。。


8
ZGLHHH 79 天前
@chenyao168 219.158.39.41 震惊……


9
DesignerSkyline 79 天前
@ZGLHHH 联通的，不要震惊


10
ZGLHHH 79 天前
@DesignerSkyline 之前看到说朝鲜网络接的中国线路，没想到是真的


11
wzymmy 79 天前
把朝鲜的电脑系统打包发回来给大伙玩玩呗


12
miyuki 79 天前
999999999


13
BXIA 79 天前
应该留一条消息 hello from pentagon
然而我们就有好戏看惹


14
zxy 79 天前
先留民，我勒个去


15
akw2312 79 天前
話說說明下這延遲這麼高的原因 其實就是因為外面連到朝鮮這段幾乎都繞 sprint 美國的關係(
(聯通只給了 SPRINT 的路由)
16
zxy 79 天前


@chenyao168 截屏看看吧👆

17


wavingclear 79 天前 via iPhone ♥ 1
连的联通那是不是自动被墙
也许那句世界上只剩两个国家不允许上 facebook 是不对的

18


manoon 79 天前
呃，多来点信息嘛，吊味口，哼哼。

19


lyragosa 79 天前
多年以后，面对行刑队，李二狗准会想起，在许多年前见证一位中国黑客发射了朝鲜核弹的那个遥远的午夜。

20


MajestySolor 79 天前
WW3 的起源？

21


InneRs 79 天前
留名
LZ 如果把这条发到乌云上去能拿多少 rank ？

22


zhaojjxvi 79 天前 via iPhone
666

23


esxivistawrt 79 天前
175.45.176.0/22

24


Hello1995 79 天前 via Android
@wzymmy 搜 Red Star OS 3 iso ，应该有，长得像 OS X 的 Linux 。

25


aprikyblue 79 天前
@lyragosa 百年孤独？

26


2232588429 79 天前
大浦洞 1 号已瞄准，楼主吃顿好。 2333

27


stabc 79 天前
LZ 家方圆 100 里平民需要紧急疏散。

28


Testalias 79 天前
朝鲜网络一直都是联通提供的，这点是公开的信息

29


Testalias 79 天前
发乌云小心三胖抗议，说你是阶级敌人，干涉内政，要抓你去舞水端里挖煤

30


JackBlack2006 79 天前
不要总想搞个大新闻 斜眼

31


aalska 78 天前
搭载大浦洞的光明星 4 号有话要讲

32


shengyu 78 天前 via Android
注意安全，转发到知乎上

33


243205964 78 天前
公布漏洞，让大家爽爽啊

34


DesignerSkyline 78 天前
@ZGLHHH 还有老毛子的卫星段呢，只不过不知道而已哈

35


VmuTargh 78 天前
@DesignerSkyline 据说老毛子的卫星段是没有墙的，是朝鲜这边自己搞了一个

36


DesignerSkyline 78 天前
@VmuTargh 卧槽，我刚才搜到了，有那个 IP 段通过 satgate 分配给朝鲜。。老毛子那个肯定没墙啊， 233
话说那个联通段甚是诡异啊，路由追踪里看貌似动了手脚的

37


letv 78 天前
擦，好想学学这门技术啊

38


jesse_luo 78 天前
我就想问下 1z 哪里人……

39


BryanOZ 78 天前 via Android
我就想知道你从哪里找到的 ip 段

40


TrustyWolf 78 天前
@BryanOZ 之前 V2 就有帖子说这事，然后我记得当时提到了这个网页：https://nknetobserver.github.io/。
老外很早就扫过三胖的 IP 段。

41


chenyao168 78 天前
至于截图的问题，我操作不方便啊。另外，至于墙的问题，我敢保证，发文前没有发现被封的网站，下面发上到达 Facebook 和 Twitter 的 tracert 。

42


BryanOZ 78 天前 via Android
@TrustyWolf 咦？好神奇，试试

43


chenyao168 78 天前
另外，大家可以使用朝鲜的 DNS 服务器，注意使用 TCP 协议，你懂的：
175.45.178.5
175.45.178.88
最后，我并不想制造啥大动静，不过 V2 上头一次碰到主题跑到首页上，至于漏洞吗，我想 IT 圈混的都知道怎么根据楼主的提示找，因此在下不要再继续班门弄斧了。

44


chenyao168 78 天前
Tracing route to twitter.com [104.244.42.65]
over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 10.191.0.33
2 <1 ms <1 ms <1 ms 172.16.0.30
3 <1 ms <1 ms <1 ms 172.16.9.1
4 59 ms 60 ms 60 ms 172.16.10.1
5 60 ms 60 ms 61 ms 219.158.39.41
6 230 ms 229 ms 229 ms 144.232.0.209
7 220 ms 219 ms 219 ms 144.232.0.208
8 221 ms 219 ms 219 ms 144.232.25.98
9 225 ms 225 ms 225 ms 129.250.196.94
10 * * * Request timed out.
11 220 ms 224 ms 220 ms 104.244.42.65

Trace complete.

45

chenyao168　　78 天前
Tracing route to star-mini.c10r.facebook.com [31.13.95.36]
over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 10.191.0.33
2 <1 ms <1 ms <1 ms 172.16.0.30
3 <1 ms <1 ms <1 ms 172.16.9.1
4 60 ms 60 ms 60 ms 172.16.10.1
5 60 ms 60 ms 60 ms 219.158.39.41
6 236 ms 235 ms 233 ms 144.232.0.209
7 221 ms 223 ms 223 ms 144.232.0.208
8 400 ms 408 ms 408 ms 144.232.25.98
9 433 ms 445 ms 449 ms 129.250.3.26
10 616 ms 613 ms 616 ms 129.250.2.131
11 448 ms 481 ms 457 ms 129.250.6.144
12 399 ms 398 ms 385 ms 129.250.2.222
13 386 ms 385 ms 386 ms 129.250.2.93
14 399 ms 399 ms 435 ms 203.131.241.62
15 454 ms 441 ms 439 ms 173.252.64.174
16 532 ms 519 ms 509 ms 173.252.65.73
17 379 ms 379 ms 379 ms 31.13.95.36

Trace complete.

46
hinate　　78 天前
  三胖不是要屏蔽推特和脸书了吗

47
jasontse　　78 天前 via iPad
看起来是标准的三层拓扑啊，高端的一笔。

48
GKLuke　　78 天前
我怎么记得某次在网上看到金将军的国家图书馆之类的网站都用的是 10 网段大内网呢，难道 175 这个网段是给国外人用的？

49
VmuTargh　　78 天前
@GKLuke 所谓内外有别
@DesignerSkyline 毛子的网路一向很牛，比咱 TC 好多了，全俄各地互联延迟不超过 100ms

50
DesignerSkyline　　78 天前
@VmuTargh 那是全俄，最多就是跨一个亚欧大陆而已啊。。。。但是毛子网络与全球网络是绕路的。。。到处绕。。。国际延迟比较高

51
InneRs　　78 天前
你好， chen

52
InneRs　　78 天前
Tracing route to www.google.com [172.217.1.228]
over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 10.191.0.33
2 <1 ms <1 ms <1 ms 172.16.0.30
3 <1 ms <1 ms <1 ms 172.16.9.1
4 83 ms 59 ms 61 ms 172.16.10.1
5 62 ms 59 ms * 219.158.39.41
6 223 ms 221 ms 220 ms 219.158.32.198
7 222 ms 223 ms 222 ms 72.14.194.10

```
8 226 ms 226 ms 227 ms 209.85.248.62
9 225 ms 225 ms 225 ms 209.85.142.185
10 219 ms 225 ms 220 ms 209.85.247.97
11 225 ms 213 ms 217 ms 64.233.174.176
12 220 ms 216 ms 216 ms 64.233.174.191
13 213 ms 214 ms 213 ms 209.85.253.185
14 204 ms 210 ms 204 ms 172.217.1.228

Trace complete.
```

53

chenyao168 78 天前

Hi OrWell!

54

TrustyWolf 78 天前

@GKLuke https://en.wikipedia.org/wiki/Internet_in_North_Korea ，公网 IP 也是用的，不过 NAT 太狠，基本都至少两层 NAT ，所以公网 IP 需求很少， IPv6 就更无从谈起了。

55

xiaozhizhu1997 78 天前 via Android

@wavingclear 这种服务类似于 IP Transit 。并非自带墙。

56

metrotiger 78 天前

楼主，你哪个单位的？你怕不怕炮决和犬决？

57

GKLuke 78 天前

@TrustyWolf 原来如此， wikipedia 什么时候不 Q 了，曾记得一度各种语言都 Q 了

58

VmuTargh 78 天前

@DesignerSkyline 出口现在很多走 ROTACS 了，中转阿姆斯特丹 or 伦敦，然后后面转多次才是费时

59

DesignerSkyline 78 天前

@VmuTargh 那不就对了吗？到阿姆斯特丹和伦敦能跑满的只有移动了，电信和联通必然跑不满

60

VmuTargh 78 天前

@DesignerSkyline 但是很奇怪的是 ROTACS 原本设计要铺到东京釜山还有魔都的，这一段好像搁浅了似得

61

DesignerSkyline 78 天前

@VmuTargh 因为没钱吧 233333333333

62

maskerTUI 78 天前

搜了一下发现了 ip ， 175.45.176.0 175.45.179.255 175.45.176.0/22 1024 个

我就不作死了

63

zxy 78 天前

装个 SS 给大家当梯子，脑洞大开～

64

chenyao168 78 天前

@zxy 你不说我还真的忘了，待会看看。

65

jacy 78 天前

搭个 ss，上网都显示来自曹县，高大上

66

DesignerSkyline 78 天前

@chenyao168 23333333333


67
wawehi 78 天前
留 名

68
isnowify 78 天前 via iPhone
@chenyao168 火前留名!
lz 在用讲述人 /VoiceOver ？

69
chenyao168 78 天前
现在在 Github 能弄到的最新版 SS 是 1.8.4 版，请问这有啥问题吗？

70
chenyao168 78 天前
@isnowify 是的，在用这类辅助工具，例如 Windows 的 Narrator ， Android 的 Talkback 。

71
InneRs 78 天前
@chenyao168 我比较怀疑系统资源够不够

72
InneRs 78 天前
@chenyao168 为什么要用讲述人？

73
chenyao168 78 天前
为什么会用讲述人之类的应用程序，这个应该不用说你也懂。

74
nevermlnd 78 天前
@InneRs 怎么发现在用讲述人?

75
InneRs 78 天前
@chenyao168 我真不懂，给点提示

76
chenyao168 78 天前
@InneRs 因为我视觉有问题。

77
isnowify 78 天前 via iPhone
@chenyao168 talkback 的蛋疼 feedback …
l z 还是早日入 Apple 用 VoiceOver 对用户友好很多
什么时候弄个 s s 啊？ 233

78
MrMario 78 天前
root 是空口令啊...楼主注意安全，小心菊花不保

79
chenyao168 78 天前
@isnowify 一直在搞，现在是：

```
C:\shadowsock>shadowsock -c config.json -S
Initialising ciphers...
The method is not supported.
Initialisation failed.
Controller is not valid. Maybe improper setup?
```

然后 config.json 是这样配的，不知道问题出在哪儿？

```
{
"server":"0.0.0.0",//尝试更换过 ipconfig 显示的 IP ，问题依旧。
"server_port":10080,
"password":"123456",
"timeout":120,
"method":"rc4-md5",
}
```

最后是关于屏幕阅读器，说实话，早再去年我曾经用过 MAC 下的 VoiceOver ，结果的确人性化了，但是我对 Apple 封闭的生态圈不太感冒。

80

JJaicmkmy 78 天前 via iPad

@chenyao168 把 method 改成 table 试试？（不过好像有点作死）

81

agentmario 78 天前

@chenyao168 可能是你的发行版有点旧 试试装个 python 然后 pip 安装 python 版

82

BryanOZ 78 天前 via Android

@agentmario 两层 NAT ， SS 连不上吧…

83

InneRs 78 天前

@chenyao168 我已经把 shadowsocks 弄好了，但是建议先不要公布 ip ，除非把洞都补上

84

InneRs 78 天前

@chenyao168 请看 C:\To Chen.txt

85

esxivistawrt 78 天前

Tracing route to 192.88.99.1 over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 10.191.0.33
2 <1 ms <1 ms <1 ms 172.16.0.30
3 <1 ms <1 ms <1 ms 172.16.9.1
4 59 ms 59 ms 59 ms 172.16.10.1
5 59 ms 59 ms 59 ms 219.158.39.41
6 207 ms 205 ms 206 ms 219.158.102.126
7 210 ms 211 ms 210 ms 64.71.137.1
8 210 ms 210 ms 211 ms 72.52.92.121
9 208 ms 208 ms 208 ms 192.88.99.1

Trace complete.

86

chenyao168 78 天前

@InneRs 表示非常感谢。

公布 IP 的问题非常滴矛盾，不公布吧，建立出来不让大大家享用，何必还要建立呢？公布了需要补上漏洞，这个改动比较大，万一惊动了金将军，肿么办？

87

esxivistawrt 78 天前

@chenyao168 金将军把你抓去做香饽饽。

88

sigone 78 天前

金将军有高射炮！楼主家肯定没有水表！

89

sigone 78 天前

你这是在破坏友邦信息安全 ... ... 强烈抗议 ... ... 不希望再有类似事件发生 ... ...

90

chenyao168 78 天前

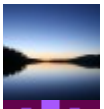
不知道你在 HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList 里面隐藏账号没有？不隐藏，欢迎屏幕会显示出来，并且还可能把 Administrator 隐藏掉。

91

InneRs 78 天前 via Android

@chenyao168 我觉得还是补上吧，主要就是加密码。我上传那个 webshell 可以留着但是要放到一个隐蔽的地方。这服务器弃置很长时间了应该不会惊动朝方。

92



InneRs 78 天前 via Android
@chenyao168 我没有隐藏。我现在得睡觉了(时差)，你能帮我隐藏一下吗?

93

chenyao168 78 天前
@InneRs 好的，我可以帮你隐藏起来。

94

chenyao168 78 天前
后来，那个服务器不知道是被哪个熊孩子给 Shut Down 了。

95

chenyao168 78 天前
看来是让金将军搞定了，剩下的另外几台 XP 都消失得无影无踪，如果是被人破坏那我也只能表示很无言。

96

chenyao168 78 天前
看来是他们重装了系统，真够折腾的， 233 。

97

jasontse 77 天前 via iPad
@chenyao168 别当恩恩不上 V2 ，楼主把恩恩吓得今天早上表示要和谈。

98

npc0der 77 天前 ♥ 1
建议楼主还是删帖 删掉所有和这个相关的信息。。。。不是怕三胖来突突突你，是怕这事情弄大了 曹县的某些技术员要被送去挖煤突突突了。。。。人命关天啊！！！

99

DesignerSkyline 77 天前
@chenyao168 还有洞吗？ 2333

100

chenyao168 77 天前
@npc0der 放心啦，以前 anonymous 放话要入侵曹县的网络，结果人家也只是用断网这种优雅的方式解决了问题，并没有用枪决、炮绝、犬绝等不符合色会主义核心价值观的方法解决问题啊， 233333 。