WiFi万能钥匙安全应急响应中心
WiFiMasterKey Security Response Center

一起做点有型的事情

Let's Do Someting Cool !

WIFI 万能钥匙 SRC 安全沙龙

成都　　2017/12/02

《SRC混子是如何炼成的？》

四叶草安全－残废

SRC到底应该怎么搞？

来自漏洞之王的回复

师傅好

请问如何才能像你一样，变成漏洞之王？

多想多找，想法越出其不意越好，多熟悉业务

来自月入几十万的大佬回复

黑色键盘

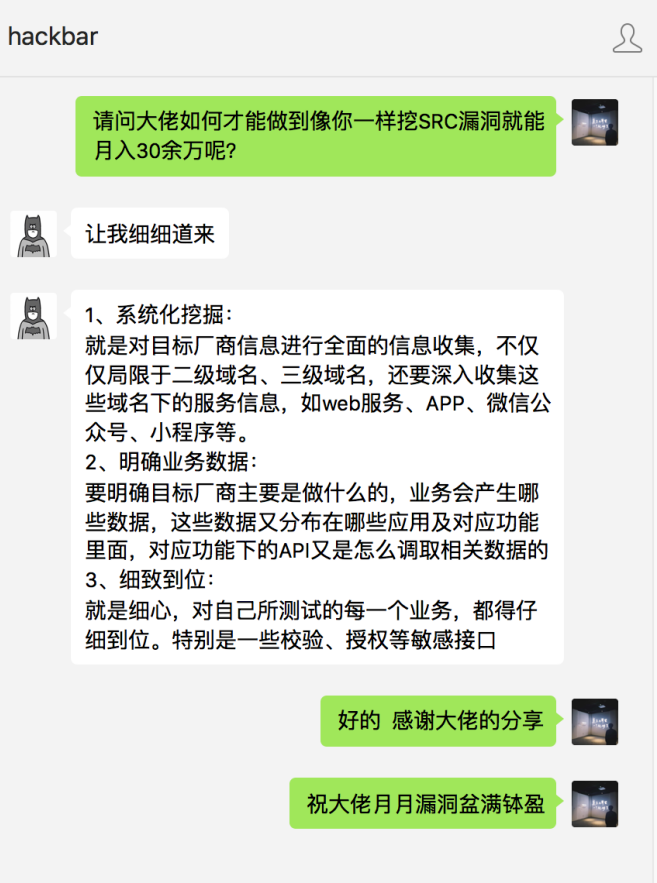
大佬

请问如何才能变成像你一样月入几十万的大神?

下午12:19

对他们的那些业务比较了解 信息搜集的全一点 正好那个月他们活动 每天都挖 因为他们分几个阶段 还有个最终大奖。如果第一阶段拿到奖 我就把漏洞都囤着 等第二阶段提交 以此类推 这样每个阶段都拿到了奖 时间点掐的准 这样一结合完美

又一个来自月入几十万的大佬回复



信息收集？
了解业务？

从基础架构分析

运维安全

业务安全

应用安全

内部安全

Web Server

基础服务

应用层

运维安全

网络

信息泄露

服务器&设备

rsync dns

elasticsreach smtp

ftp telnet

ldap 基础服务 ssh

database snmp

activemq

hadoop smb vnc

……


Bash
扫描
内网入口
网络
服务器&设备
SSL
本地提权
DDOS

Tomcat

Resin

JBoss

Web logic

WebServer

Apache

Jetty

Nginx

IIS

……

备份文件泄露

压缩文件泄露

敏感文件泄露

编辑器安全

Strut2

应用层

SVN

Git

cati

zabbix

jenkins

……

截图泄露

操作手册

代码泄露

信息泄露

PPT

内部帐号外部业务

Blog

……

营销活动

账号体系

业务安全

交易体系

风控体系

密码重置　　批量注册　　登陆防控

撞裤　　任意登录

账户体系

身份鉴定　　任意注册

身份盗用

风控缺陷

风控遗漏

风险控制

判定要素

机器识别

机器人　　垃圾注册

信用炒作

买家套现

营销活动

刷单

扫号　　刷券

反爬虫

薅羊毛

任意金额充值

一分钱续费

交易体系

一分钱充值

一分钱购物

绕不完的Filter

SSRF

失效的“云WAF”

应用安全

推不动的SDL

事件响应不及时

漏洞组合利用

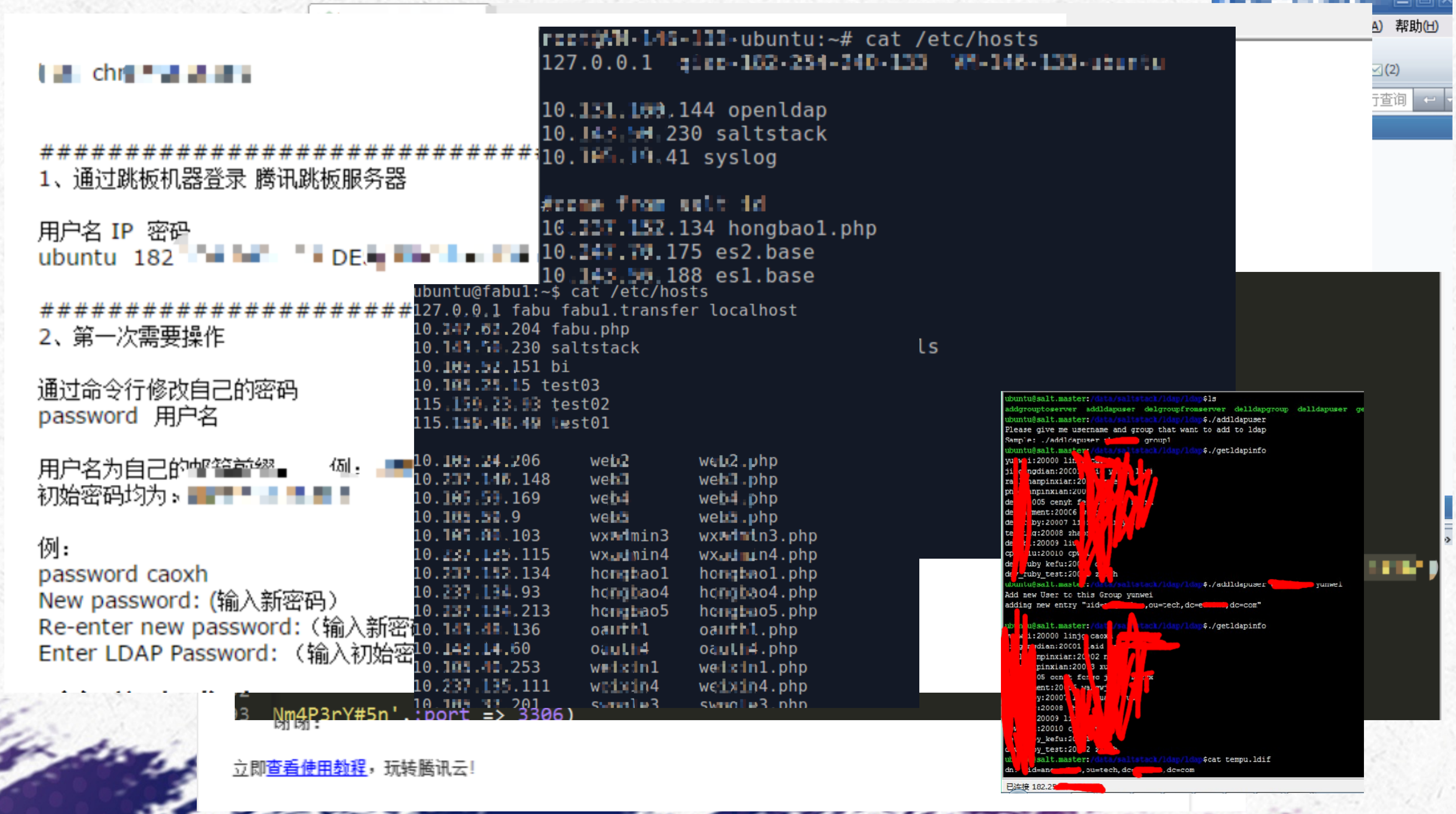
人员意识

内部安全

办公网络

WiFi万能钥匙安全应急响应中心
WiFiMasterKey Security Response Center

一起做点有型的事情
Let's Do Someting Cool!



信息收集

User List → username password mobile mail 角色

Domain List → 二级、三级… 备案 whois 第三方 业务资产

IP List → 外网IP 内网IP C段 IP 办公网IP 端口

Web List → 中间件 CMS 数据库 基础服务

Mail List → user mail 业务mail 公用mail

work os → oa gitlab jenkins wiki Jira VPN SSO 后台

了解业务

业务内容　　业务资产　　业务应用

边缘资产比核心更容易出问题

安全总是相对的

三分看命运，七分天注定

WiFi万能钥匙安全应急响应中心
WiFiMasterKey Security Response Center

Thanks