Chinapub读书会 第2期

黑客技术分享会

主办方：

媒体支持：

中国黑客联盟

读书会介绍

Chinapub读书会

“chinapub读书会”是互动出版网旗下读书交流品牌，旨在为会员提供线下技术交流、学习阅读的平台，主要集中在计算机、科技、经管等专业领域。

读书会每月不定期举行线下交流读书活动，只要成为chinapub读书会的会员，即可免费参加读书会全年线下交流活动，与作者面对面进行思想的碰撞。

第三期活动预告：GO语言与Docker技术分享会

读书会官方微信

活动QQ群： 429519341

嘉宾介绍

童进

网名cumirror，持有机械工程与心理学双学位，中南大学软件工程专业硕士，曾就职于山石网科研发中心，Ubuntu控，应用开发工程师，擅长Linux/Windows下C/C++应用开发及网络流量分析，熟悉国内各类防火墙/IDS产品。

由渗透测试到安全生态

分享嘉宾：童进

自我介绍

微博：cumirror

技术领域：Linux开发，TCP/IP，黑客技术

目前职业：创业公司从事硬件防火墙开发

兴趣爱好：Linux内核、编译原理、算法/架构　不懂的 :-)

休闲娱乐：各种漫画，各种小说，台球

联系方式：tongjinam@qq.com

渗透测试

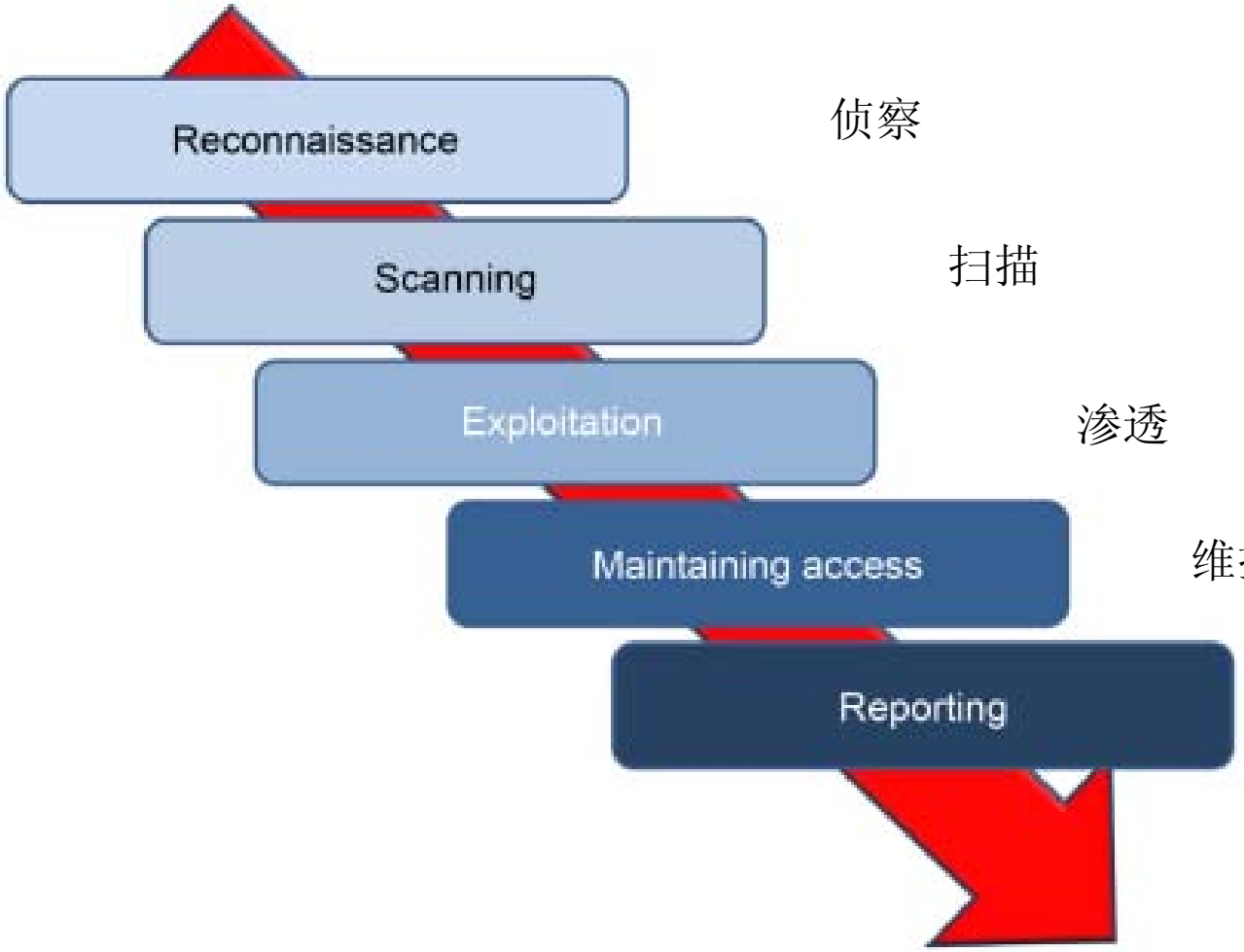
渗透测试：

测试人员在具体和授权条件下尝试规避信息系统的防护措施所使用的方法、过程和步骤，包括突破系统集成的安全特性。----《Hacking with Kali》

通常情况下，仅评估信息系统建立时的安全性。

实际情况：企业对安全评估不充分甚至忽视安全，漏洞提交到漏洞平台上才进行补救，而白帽子往往是在企业毫不知情的情况下进行测试。

基本步骤



侦察

扫描

渗透

维持访问

输出报告

实际操作

扫描->web渗透->放置webshell->提权->脱裤

|->注入漏洞->脱裤

|->xss。。。

|。。。

每一步要完成什么

有哪些工具可供使用

如何依据结果进行下一步处理

工具和环境推荐

工具：

1.kali

2.metasploit

2.wireshark

3.burpsuite

4.awvs

5.其它：御剑、Layer挖掘机等等

工具只是辅助，分析还得靠自己！

环境：

0.vmware

1.LAMP/IIS + SQL Server

2.discuze/wordpress/cms/其它

3.metaspolitable2

实践出真知

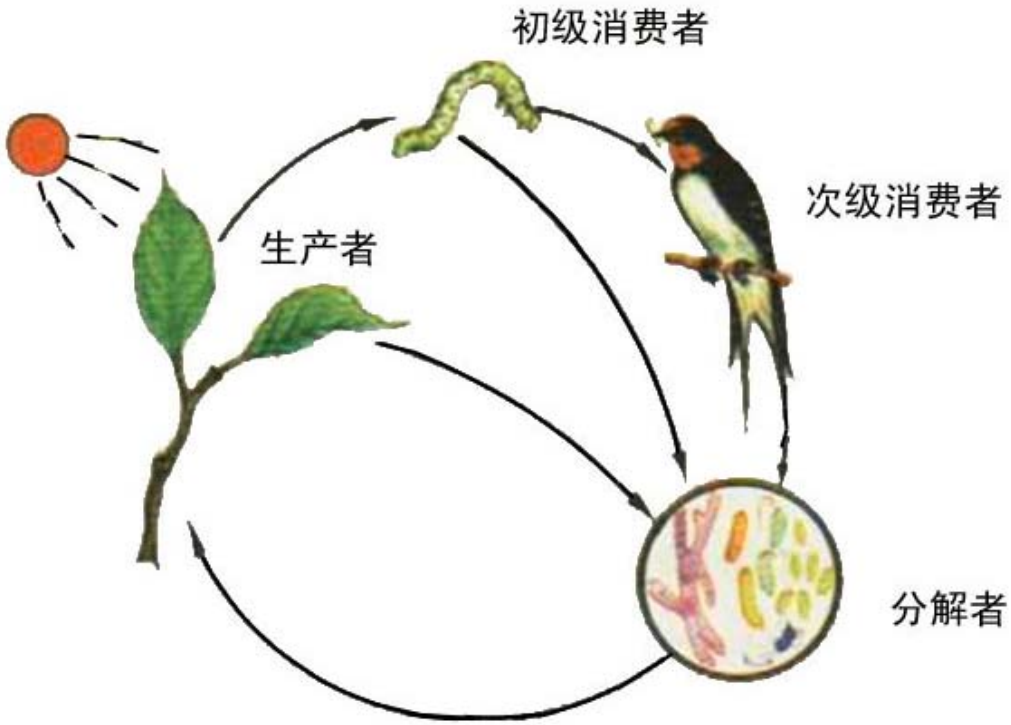
当我在潜心修炼渗透技能时，其他人在干什么？

外面的世界很精彩，欢迎来到安全界

安全生态圈

我给自己挖了一个坑

“我要爬出来！！！”



生产者、消费者和分解者

传统的安全生态

安全驱动力：

1.企业自身的安全意识（敏感行业，自身网络需求）

2.合规要求

服务提供者：安全厂商

服务消费者：企业（个人没有消费习惯）

服务形式：安全产品(硬件防火墙/杀毒软件/扫描器等)

其实我是来吐槽的

其实我也是一名程序员：

设计应用识别引擎

做过SSLVPN模块

HA高可靠性，没有问题

做过安全应急响应：攻击分析，IPS事件添加

但是：

1.听说设备卖了后，没上电

2.上电了，但只开启了网络转发功能，ips/av等安全防护功能没开

3.咦，运行了一个月，没有IPS/AV告警日志！！！

设备到底怎么了？？？

1.对于大部分厂商，防御能力弱于攻击能力

2.对于大部分客户，并不真正重视安全

这些厂家在干嘛？？？

启明星辰　　天融信　　绿盟　　山石网科　　网康　　深信服

传统生态的特点

客户主要来自政府、金融、国企和教育行业

驱动力主要是合规要求。

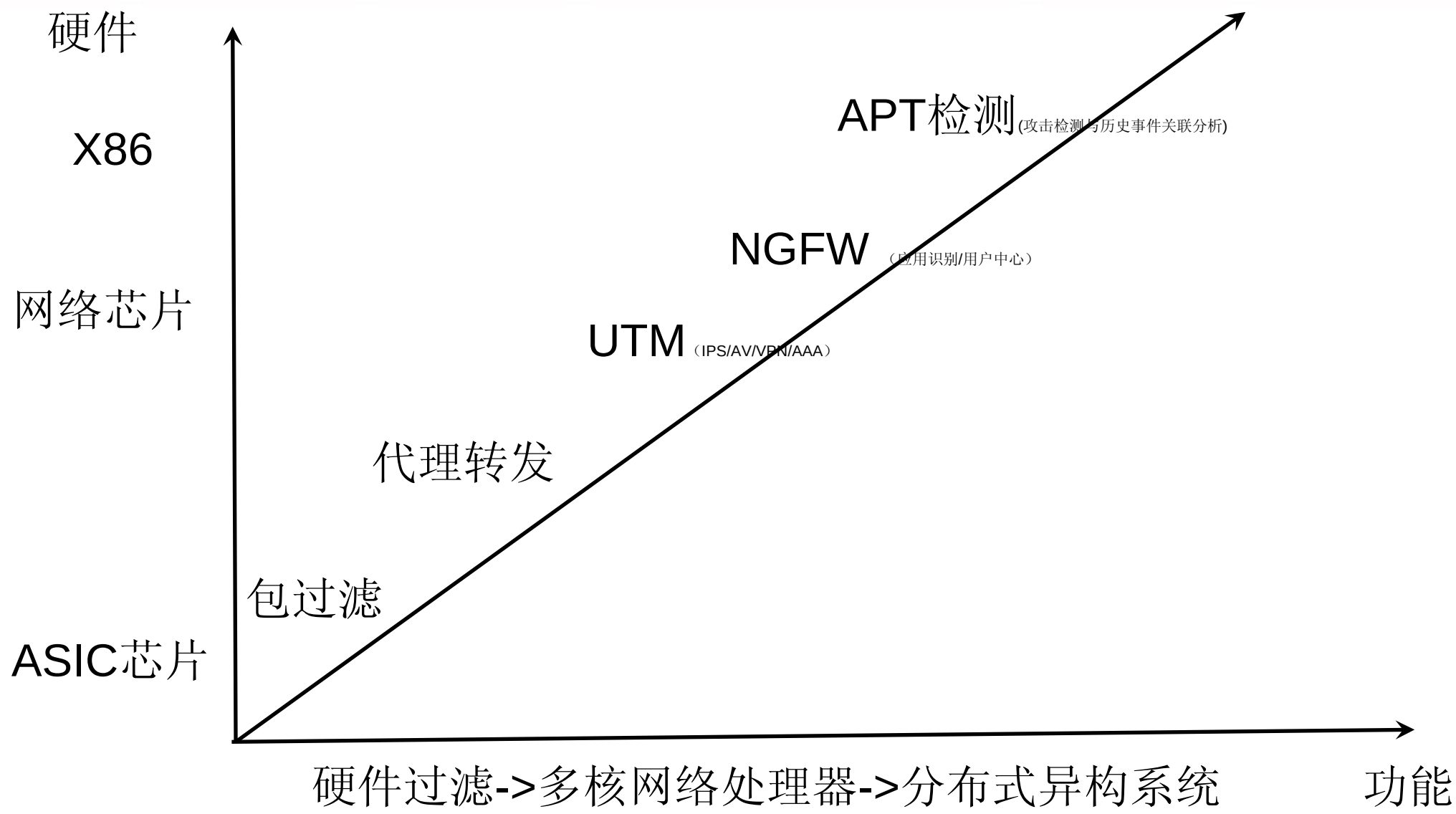
高技术门槛，但缺少活力

面对机会，但缺少动力

合规要求，导致产品大而全，但又无实际效果

关键功能：1.VPN接入；2.AAA认证；3.用户行为管理

防火墙的发展


硬件
X86
网络芯片
ASIC芯片
包过滤
代理转发
UTM（IPS/AV/VPN/AAA）
NGFW（应用识别/用户中心）
APT检测(攻击检测与历史事件关联分析)
硬件过滤->多核网络处理器->分布式异构系统
功能

新兴的安全生态

背景：

1.电商的发展，唤醒了用户的安全意识

2.频发的安全事件给企业敲响了警钟

3.Web项目的快速迭代开发加剧了网络风险

4.传统安全厂商提供的安全服务有限

新兴的安全生态

1.大企业自身进行安全团队的建设

a)内部安全流程规范

b)安全事件应急响应

2.企业提供的服务带有安全属性

3.安全的微创新

他们在做什么？？？

360：已能控制传统边界，360Vulcan，补天，web安全检测

乌云漏洞平台：曝光安全风险，聚集白帽子，提供众测平台

知道创宇团队：加速乐，zoomEye

Freebuf：黑客媒体，安全招聘，提供众测平台

安全狗：专注于web服务器的安全防护

日志宝：（被360收购）

安全宝：（刺被阿里从新收编，刚被百度收购）

腾讯/阿里/百度

新兴安全生态的特点

1.对安全的理解发生了变化：

安全不再是附加服务，而是产品自身的属性。

2.安全防护的对象发生了改变：

安全防护不再仅仅是为了保护资产，而是为了保护用户信息。因为用户才是互联网公司最重要的"资产"。

3.漏洞平台使得攻击防护不再被动

4.安全形式多元化：

众测被越来越多的企业所接受。

实践出真知

安全的世界很精彩

欢迎来到安全界

Thank you

图书推荐

《 Kali渗透测试技术实战》

作者：IDF实验室成员

国际著名信息安全专家亲笔撰写，IDF实验室成员倾情翻译，著译双馨。

全面而系统讲解Kali渗透测试的各种技术细节和方法，包含丰富示例，为快速掌握Kali渗透测试技术提供翔实的指导。