

安全威胁与攻防





参考书:

网络攻防技术与实践 诸葛建伟 电子工业出版社,2011



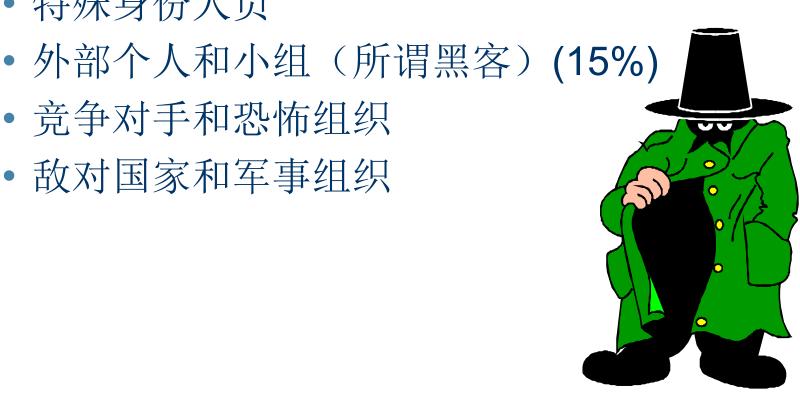
攻击者的来源



o按统计来分(FBI)



- 内部人员 (70%)
- 准内部人员
- 特殊身份人员
- 竞争对手和恐怖组织
- 敌对国家和军事组织





攻击的分类



OActive attack 主动攻击



It attempts to alter system resource or affect their operation.

包括: 网络扫描、拒绝服务攻击、缓冲区溢出、欺骗和网络钓鱼(Phishing)、信息篡改、会话劫持、隐密通道(covert channel)等攻击方法。

oPassive attack 被动攻击

It attempts to learn or make use of information from the system but does not affect system resources.

包括: 嗅探、流量分析、信息收集等攻击方法。

多数情况下这两种类型被联合应用



其他的分类方法:



● 从攻击的目的来看,可以有拒绝服务攻击(Dos)、 获取系统权限的攻击、获取敏感信息的攻击;



- 从攻击的切入点来看,有缓冲区溢出攻击、系统 设置漏洞的攻击等;
- 从攻击的纵向实施过程来看,有获取初级权限攻击、提升最高权限的攻击、后门攻击、跳板攻击等;
- 从攻击的目标来看,包括对各种应用系统的攻击(系统攻防)、对网络设备的攻击(网络攻防)



少 攻击的一般过程

攻击的发展, 这还适用吗? 有关攻击理论模型的研究



预攻击



后攻击



收集信息,进行进 一步攻击决策

获得域名及IP分布 获得拓扑及0S等 获得端口和服务 获得应用系统情况 跟踪新漏洞发布



进行攻击

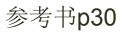
获得权限 进一步扩展权限 进行实质性操作



消除痕迹,长期维 持一定的权限

内容:

植入后门木马 删除日志 修补明显的漏洞 进一步渗透扩展





网络攻防活动与竞赛

0 会议:



- Defcon,Black Hat
- Xfocus的信息安全焦点峰会Xcon,8月北京



Forensic Challenge, CrackMe,ReverseMe

- o CTF(Capture the Flag)
 - 要找比赛: https://ctftime.org/
 - 顶级: Defcon CTF, CanSecWest的Pwn2Own竞赛
 - 高校: UCSB iCTF

"Teaching Hands-On Network Security: Testbeds and Live Exercises," by Giovanni Vigna, in *Journal of Information Warfare*, vol. 3, no. 2 February 2003 PDF.

中学生: <u>CSAW</u>, the Cyber Security Awareness Week
(<u>https://csawctf.poly.edu/</u>), NYU

免费教程: https://cyfor.engineering.nyu.edu/

○ 国内:

- 腾讯安全技术大赛
- 看雪论坛



网络攻防实验环境



●靶机:攻击的目标。



- o 攻击机 (attacker): 发起攻击的主机,常 安装有各种攻击软件。
- ●攻击检测、分析与防御平台:位于如靶 机的网关
- o网络
- ●可采用私有云架构



Kali Linux





- o渗透测试(Penetration Testing)和信息安全审计(information security auditing) Linux发行版本
- o http://www.kali.org/
- o前身: BackTrack (BT),





o 反汇编: OllyDbg,IDA Pro, C32asm, W32Dasm



o 反编译: JD-GUI,dcc,Boomerang alpha

● 静态分析:Peid,LordPE,Aspack unpacker,upx,fs,超级 巡警脱壳器

● 渗透攻击: Metasploit

o 网络扫描与嗅探: Wireshark, Nmap/Zenmap, Xscan, Snort

o 密码学工具CryptoCal, PrimeGenerator,RSAtools, DSAtools,Ultra Cracking Machine,MD5Crack

● 监视工具: WinDump,Process Explorer,Process Monitor



攻击的手段



o预攻击阶段(收集信息)



- 扫描: 主机扫描, 端口扫描, 漏洞扫描, 无线...
 - •操作系统类型鉴别,网络拓扑分析...
- 窃听,嗅探
- 利用一些信息服务: 搜索引擎,网站,出版 物
- 社会工程(SNS,)



攻击的手段(攻击阶段)







- 操作系统漏洞
- 应用服务缺陷
- 口令攻击
- 错误及弱配置攻击
- 欺骗, 伪造
- 信息窃取、窜改\插入,删除,重发
- 劫持
- -In-The-Middle(MITM)
- DOS/DDOS
- SPAM
- WEB攻击

- •BOTNET: P2P, SNS...
- •Zero-day
- Phishing/spear phishing
- APT (Advance Persistent Threat)
- Covert channel

•.....



攻击的手段



●后攻击阶段



- 后门木马
- 痕迹擦除



IP网络面临的安全威胁



恶意攻击

- 网络扫描
- **DDoS**



- 欺骗和网络钓鱼(Phishing)
- 会话劫持
- 消息窜改,插入,删除,重发
- 物理破坏

o 误用和滥用(内部和外部)

- 配置错误、缺省配置
- 内部窃取: 客户资料、充值卡等
- 内部越权
- 操作行为抵赖
- 垃圾流量、邮件、电话和短信

o 恶意代码:

- 病毒和蠕虫,木马
- 逻辑炸弹,时间炸弹

应用层

UDP TCP

LLC

MAC

物理层

IP网络各层的主要威胁

查询CERT/CC -CNCERT/CC - SANS 賞 方网站可以了解当前 最新的漏洞和安全事 件统计报告