网络安全创新大会
Cyber Security Innovation Summit

RedTeam 视角下的二进制攻防研究

姓名 仙果

About Me

致力于网络攻防对抗研究

“APT” VS “红蓝对抗”研究

如何更好的利用漏洞

如何更隐藏的利用漏洞

对手是如何思考的

人与人之间的意识区别是什么

中国人 vs 外国人 思维陷阱

目录

关于“APT”的延伸话题

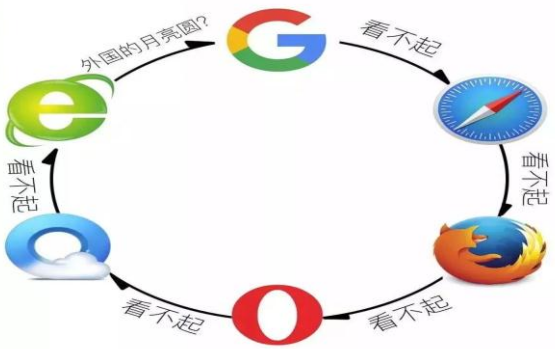
红队：仿真、模拟或以其他方式扮演某个、某组入侵者

1、“红蓝对抗”中的地位问题

1、“红蓝对抗”中的地位问题

浏览器

关系图：



测试

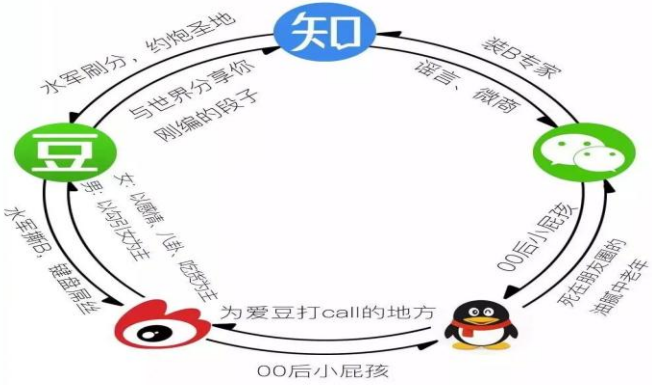
测试

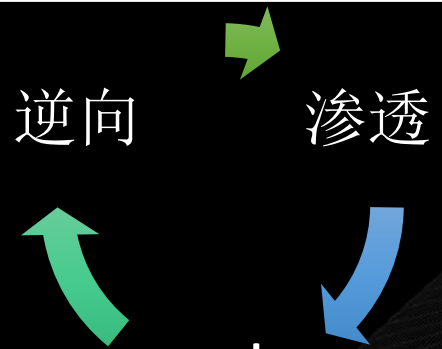
测试

发

常用APP

关系图：





高级渗透测试工程师（红队方向）

人数及地点

- 5人，坐标北京、武汉、重庆

岗位职责

- 1. 负责对企业网络进行安全评估（拿权限、拿数据，不限制攻击手段）
- 2. 前沿攻击技术的研究，攻击小工具的研发

任职要求：

- 1. 熟练掌握各种渗透测试工具并且对其原理有深入了解（不仅限于 Burpsuite、sqlmap、appscan、AWVS、nmap、MSF，cobalt strike 等等）
- 2. 至少掌握一门开发语言，操作语言不限 C/C++、Golang、Python、Java 都可，要求至少能上手写代码
- 3. 熟练掌握常见的攻防技术以及对相关漏洞（ web 或二进制）的原理有深入的理解
- 4. 具有丰富的实战经验可独立完成渗透测试工作
- 5. 能从防御者或者运维人员的角度思考攻防问题，对后渗透有深入了解者更佳
- 6. 对安全有浓厚的兴趣和较强的独立钻研能力，有良好的团队精神

加分项：

- 具备渗透大型目标的经验
- 熟悉常见 Windows,Linux 安全机制，具备一定的安全开发能力以及problem solving能力

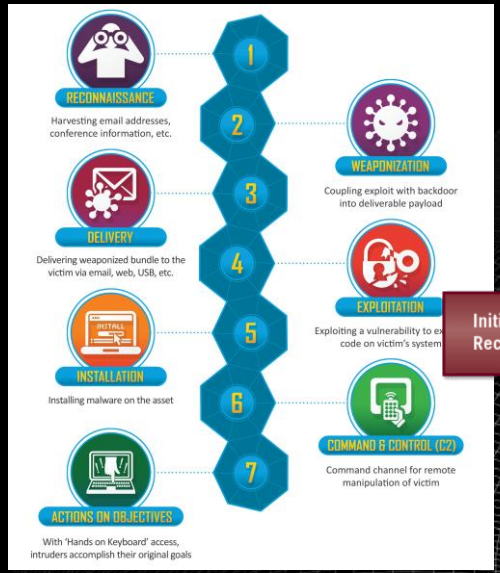
2、“Kill Chain”的作用域

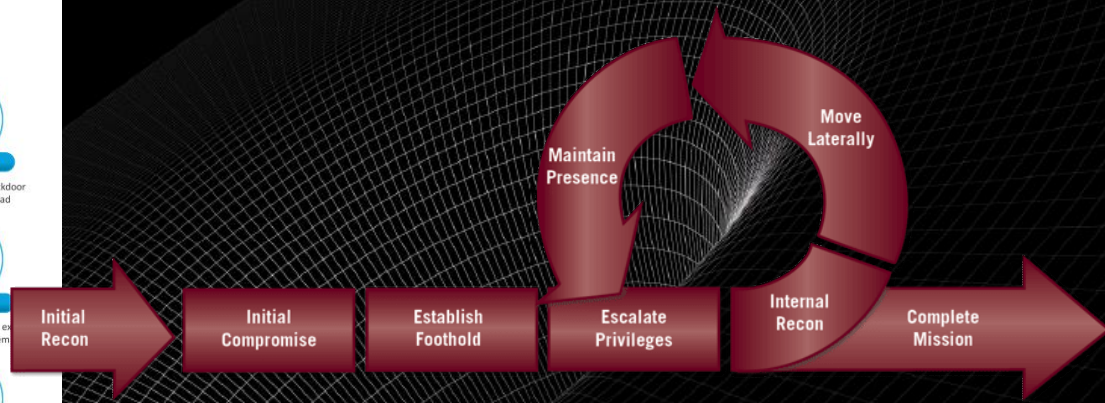
2、“Kill Chain”的作用域

渗透前的信息收集

渗透阶段

后渗透阶段





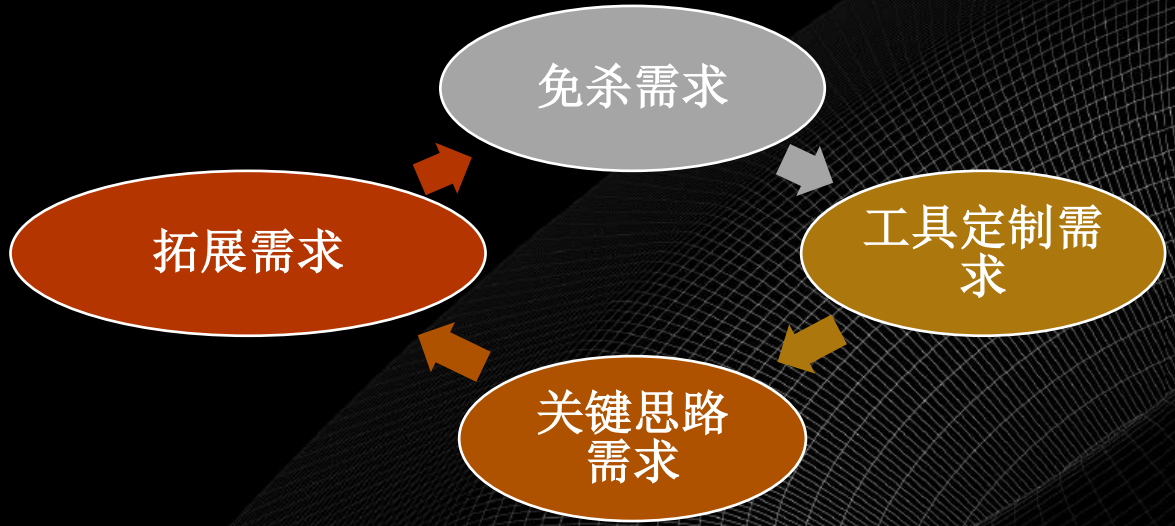
2、“Kill Chain”的作用域-信息获取

渗透前的信息收集

- 系统版本信息
- 网络环境信息
- 杀毒软件信息
- 软件版本信息
- 用户使用习惯信息

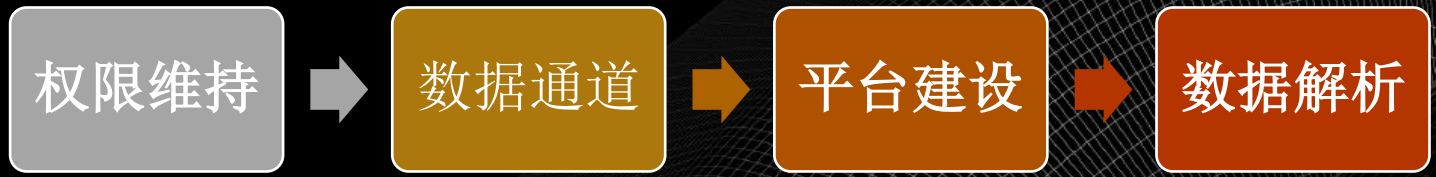
2、“Kill Chain”的作用域-渗透阶段

交互阶段



2、“Kill Chain”的作用域-后渗透阶段

服务阶段



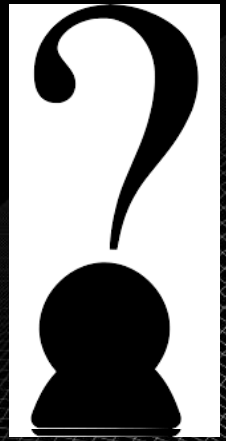
3、不仅仅是“响应”和“溯源”

3、不仅仅是“响应”和“溯源”

漏洞样本分析&木马样本分析

溯源 威胁情报分析

漏洞挖掘



还可以做什么？

还可以做更多

漏洞利用

漏洞利用

远控对抗

”红蓝对抗”

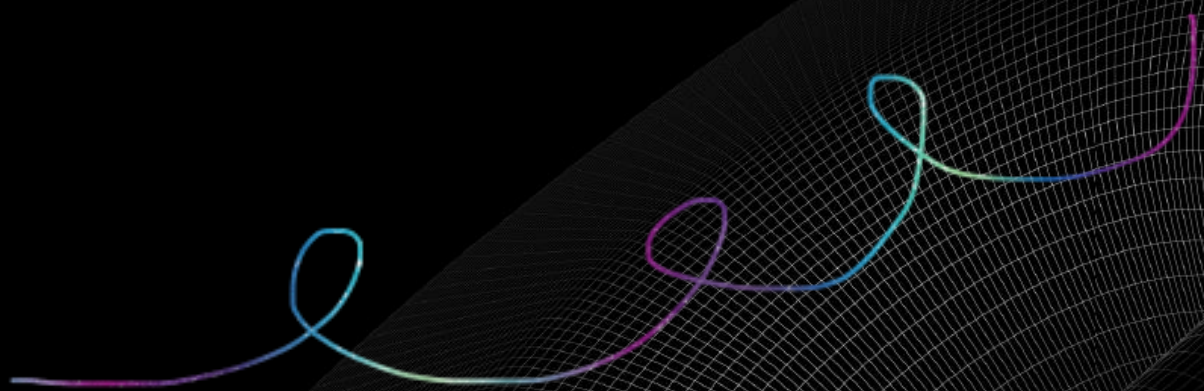
攻防对抗工具研发

4、技术提高途径

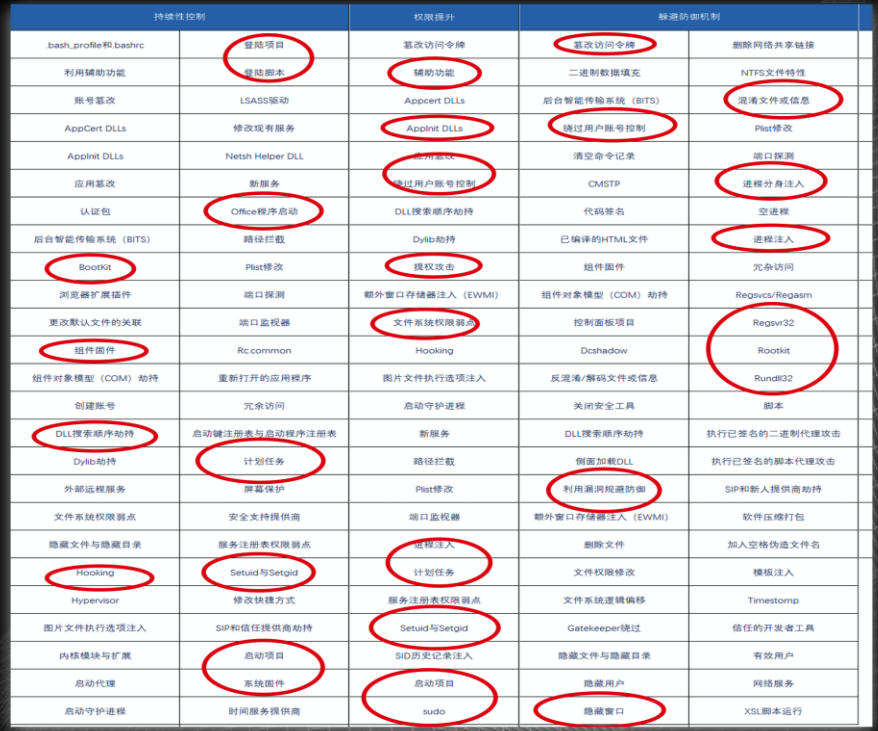
学习曲线

Web安全

逆向



技能树



持续性控制		权限提升	躲避防御机制	
.bash_profile和.bashrc	登陆项目	篡改访问令牌	篡改访问令牌	删除网络共享链接
利用辅助功能	登陆脚本	辅助功能	二进制数据填充	NTFS文件特性
账号篡改	LSASS驱动	Appcert DLLs	后台智能传输系统（BITS）	混淆文件或信息
AppCert DLLs	修改现有服务	AppInit DLLs	绕过用户账号控制	Plist修改
AppInit DLLs	Netsh Helper DLL	应用篡改	清空命令记录	端口探测
应用篡改	新服务	绕过用户账号控制	CMSTP	进程分身注入
认证包	Office程序启动	DLL搜索顺序劫持	代码签名	空进程
后台智能传输系统（BITS）	路径拦截	Dylib劫持	已编译的HTML文件	进程注入
BootKit	Plist修改	提权攻击	组件固件	冗余访问
浏览器扩展插件	端口探测	额外窗口存储器注入（EWMI）	组件对象模型（COM）劫持	Regsvcs/Regasm
更改默认文件的关联	端口监视器	文件系统权限弱点	控制面板项目	Regsvr32
组件固件	Rc.common	Hooking	Dcshadow	Rootkit
组件对象模型（COM）劫持	重新打开的应用程序	图片文件执行选项注入	反混淆/解码文件或信息	Rundll32
创建账号	冗余访问	启动守护进程	关闭安全工具	脚本
DLL搜索顺序劫持	启动键注册表与启动程序注册表	新服务	DLL搜索顺序劫持	执行已签名的二进制代理攻击
Dylib劫持	计划任务	路径拦截	侧面加载DLL	执行已签名的脚本代理攻击
外部远程服务	屏幕保护	Plist修改	利用漏洞规避防御	SIP和新人提供商劫持
文件系统权限弱点	安全支持提供商	端口监视器	额外窗口存储器注入（EWMI）	软件压缩打包
隐藏文件与隐藏目录	服务注册表权限弱点	进程注入	删除文件	加入空格伪造文件名
Hooking	Setuid与Setgid	计划任务	文件权限修改	模板注入
Hypervisor	修改快捷方式	服务注册表权限弱点	文件系统逻辑偏移	Timestomp
图片文件执行选项注入	SIP和信任提供商劫持	Setuid与Setgid	Gatekeeper绕过	信任的开发者工具
内核模块与扩展	启动项目	SID历史记录注入	隐藏文件与隐藏目录	有效用户
启动代理	系统固件	启动项目	隐藏用户	网络服务
启动守护进程	时间服务提供商	sudo	隐藏窗口	XSL脚本运行

需要掌握的能力

1. 技术笔记—文笔能力
2. Web方面能力
3. 渗透方面能力
4. 项目/ 产品能力
5. 客服能力
6. 组织能力

5、薪资往往不是问题

高级渗透测试工程师（红队方向）

岗位职责

- 1.负责对企业网络进行安全评估（拿权限、拿数据，不限制攻击手段）
- 2.前沿攻击技术的研究，攻击小工具的研发

任职要求：

- 熟练掌握各种渗透测试工具并且对其原理有深入了解（不仅限于 Burpsuite、sqlmap、appscan、cobalt strike 等等）
- 1.至少掌握一门开发语言，操作语言不限 C/C++、Golang、Python、Java 都可，要求至少能上手
- 2.熟练掌握常见的攻防技术以及对相关漏洞（ web 或二进制）的原理有深入的理解
- 3.具有丰富的实战经验可独立完成渗透测试工作
- 4.能从防御者或者运维人员的角度思考攻防问题，对后渗透有深入了解者更佳
- 5.对安全有浓厚的兴趣和较强的独立钻研能力，有良好的团队精神

加分项：

- 1.具备渗透大型目标的经验
- 2.熟悉常见 Windows,Linux 安全机制，具备一定的安全开发能力以及problem solving能力

岗位要求

任职要求：

1.熟悉网络安全攻防技术和工具,熟悉常见的Web/移动APP/系统安全漏洞及原理.

2.具备大型目标渗透经验，熟悉主流安全防护产品的绕过及对抗

3.有丰富的应急响应,事件调查经验,熟悉各类安全日志（如WEB访问,操作系统，安全设备等日志).

4.熟悉Linux/Windows系统原理,并能以Linux/Mac作为工作平台.

5.熟悉病毒木马,内核Rootkit的原理和行为,并对其做技术分析和逆向.

6.熟悉至少一种编程语言,如Python,shell,C,Java.GO等.

7.熟悉业界安全攻防动态,追踪最新安全漏洞,能够分析漏洞原理和实现PoC编写.

8.能够无障碍阅读英文技术Paper.

9.至少三年以上工作经验,35周岁以下.

10.热爱安全工作,具备优秀的逻辑思维能力，对解决挑战性问题充满热情，善于解决问题和分析问题.

加分项

1.在渗透测试,应急响应,漏洞挖掘,逆向分析,代码审计等安全领域至少有一个方面能力突出.

2.有安全工具开发经验，编写过漏洞利用POC经验.

3.有大型互联网企业安全工作经验.

4.发表过有深度的技术Paper或独立挖掘过知名开源应用/大型厂商高危漏洞经历.

5.有大型CTF比赛(DEFCON,XCTF,etc)获奖经历.

6.成功利用技术进行事件调查/追溯攻击者经历;有威胁情报分析,IoC大规模处理经验;有APT攻击和防御经验的均优先.

平台漏洞等；
告编写；

；
两门）

+ + + >_ 年薪

CIS 网络安全创新大会
Cyber Security Innovation Summit

Thanks

CIS 网络安全创新大会
Cyber Security Innovation Summit

https://github.com/NomadCN112/Chinese-translation-ATT-CK-framework


CIS
网络安全创新大会
Cyber Security Innovation Summit
THANKS