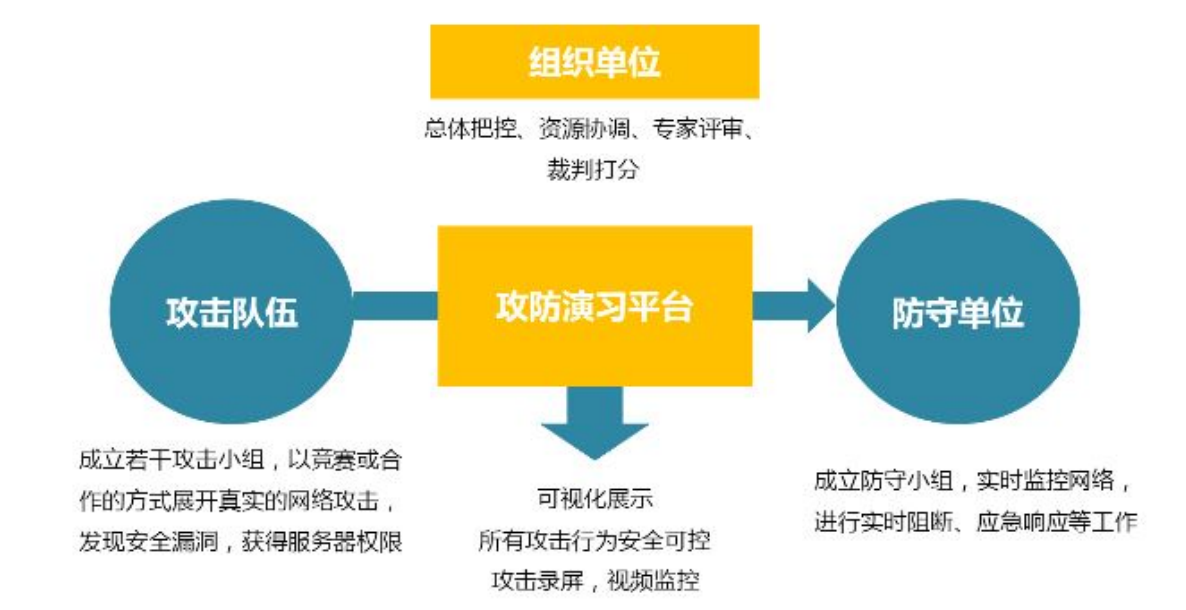


# 0X0001 什么是红蓝对抗

## 1、定义



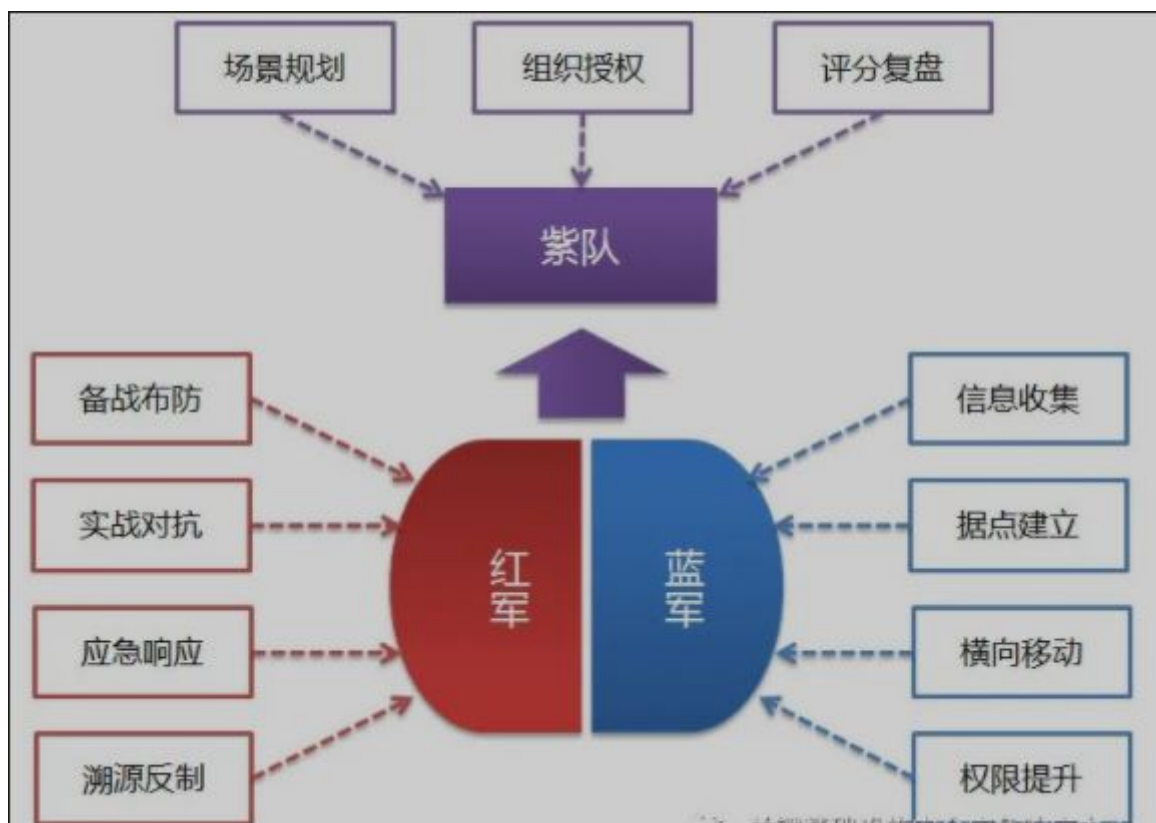
红蓝对抗目前常见的形式是网络实战攻防演练，是一场提前设定好游戏规则，指定奖惩制度，在一定时间范围内（或具体时间），以不明确攻击源、不明确攻击目标、不限制攻击手段的方式，蓝军（红队）对红军（蓝队）发起的一场黑客模拟攻击，目的在于挖掘红军更多的风险脆弱点，为后续的网络与信息安全建设提供强有力的支持。

渗透测试	红队
<p>有详细计划的安全评估测试:</p> <ul style="list-style-type: none"><li>* 渗透测试前双方制定计划</li><li>* 信息收集</li><li>* 漏洞分析</li><li>* 漏洞利用</li><li>* 后渗透阶段</li><li>* 编写测试报告</li></ul>	<p>充满不定性的安全评估测试</p> <ul style="list-style-type: none"><li>* 情报收集</li><li>* 撕口子</li><li>* 持久性/本地提权</li><li>* 本地/网络信息盘点</li><li>* 内网横向渗透</li><li>* 寻找机密资料/窃取</li><li>* 域内提权/抓取域内用户哈希</li><li>* 编写测试报告</li></ul>
<p>范围:</p> <ul style="list-style-type: none"><li>* 有限制规则</li><li>* 1-2周的测试流程</li><li>* 有问题正常公告</li><li>* 发现漏洞</li></ul>	<p>范围:</p> <ul style="list-style-type: none"><li>* 没有规则</li><li>* 1周-6个月的测试流程</li><li>* 有问题暂不公告</li><li>* 测试蓝队的工作计划，工作策略，工具和技能</li><li>* 不能违法</li></ul>

红队的工作也与业界熟知的渗透测试有所区别。渗透测试通常是按照规范技术流程对目标系统进行的安全性测试；而红队攻击一般是只限定攻击范围和攻击时段，对具体的攻击方法则没有太多限制。渗透测试过程一般只要验证漏洞的存在即可，而红队则要求实际获取系统权限或系统数据。此外，渗透测试一般都会明确要求禁止使用社工手段（通过对人的诱导、欺骗等方法完成攻击），而红队则可以在一定范

围内使用社工手段。

## 2、组成



### 2.1、红队

Red Team的概念最早来源于20世纪60年代的美国军方。红队一般是指网络实战攻防演习中的攻击一方，是具有攻击性的安全专业人员，通常由独立的道德黑客组成，以客观的方式评估系统安全性。利用所有可用的技术来发现人员、流程和技术上弱点，以获取未经授权的资产访问权。一般会针对目标系统、人员、软件、硬件和设备同时执行的多角度、混合、对抗性的模拟攻击；通过实现系统提权、控制业务、获取数据等目标，来发现系统、技术、人员和基础架构中存在的网络安全隐患或薄弱环节。

#### 目标：

- 学习和利用已知真实攻击者的TTPs来用于攻击：因为Red Team是以情报和目标为导向的，因此我们需要通过威胁情报来了解已知真实攻击者的攻击目标和意图，以及通过ATT&CK和APT组织的分析报告来学习真实攻击者攻击不同行业的TTPs，这样有利于我们有针对性地模拟真实攻击者来攻击目标企业；
- 评估现有防御能力的有效性以及识别防御体系的弱点并提出具体的应对方案：这是Red Team最为人所知的目标之一，让Blue Team通过已发现的不足来强化防御能力和改进流程，并最终提高真实攻击者的攻击成本；
- 利用真实有效的模拟攻击来评估因为安全问题所造成的潜在的业务影响：这一点通常很容易被忽略，通过Red Team我们可以为企业管理者提供有效的数据来量化和衡量安全投入的ROI。

### 2.2、蓝队

蓝队一般是指网络实战攻防演习中的防守一方。是防御性安全专家，负责维护内部网络、防御所有网络攻击和威胁。

主要工作：前期安全检查、整改与加固、演习期间进行网络安全检测、预警、分析、验证、处置、后期复盘总结现有的防护工作中的不足之处，为后续常态化的网络安全防护措施提供优化依据。

实战攻防演习时，蓝队通常会在日常安全运维工作的基础上，以实战思维进一步加强安全防护措施、提升管理组织规格、扩大威胁监控范围、完善检测与防护手段、增加安全分析频率、提高应急响应速度，提升防守能力。

## 2.3、紫队

紫队，一般是指网络实战攻防演习中的组织方。紫队实在实战攻防演习中，以组织方角色，开展演习的整体组织协调工作，负责演习组织、过程监控、技术知道、应急保障、演习总结、技术措施与策略优化建议等各类工作。

紫队组织红队对实际环境实施攻击，组织蓝队实施防守，目的是通过演习检验参演单位安全威胁应对能力、攻击事件检测发现能力、事件分析研判能力和事件响应处置能力，提升被检测机构安全实战能力。

“紫队”与标准红队之间最重要的区别就是，其攻击和防御方法都是预先确定的。与传统红/蓝对抗的模式不同，紫队模式是协作而迭代的。通过更透明而持续的过程，紫队模式将红蓝两队拧到一起，帮助防御者更高效地缓解来自现实世界高度复杂的攻击。攻方（即红队）通告守方（即蓝队）预定的攻击计划，执行攻击，阐明所利用的安全漏洞，然后重放攻击，以便守方能立即改善其控制措施。

如此一来，安全团队便可以不再局限于识别漏洞并根据其初始假设进行工作。相反地，他们可以实时测试控件并模拟入侵者可能会在实际攻击中使用的方法类型，将测试从被动转变为主动。

总而言之，紫队模式旨在让公司企业可以在整个演练过程中持续提升安全态势，获得即时效益和长期价值。团队可以应用最激进的攻击环境，并采用更复杂的“假设”方案，通过这些方案来更全面地理解安全控制和流程，并在攻击发生之前完成修复，而不再是存粹的“对抗性”关系。

# 0X002 技能

## 1、流程

### 1.1、获取立足点

- **目标侦察**

利用一系列侦查手段获取目标的资产、人员、环境等信息，为实施攻击提供基础信息支持，信息的全面性和准确性很大程度确定攻击的路径、战果和效率。比如通过DNS域传送漏洞、域名注册信息反查、域名枚举等手段获取域名资产信息，通过域名解析、网段扫描等手段获取IP资产信息，通过网站扫描、端口探测等手段获取程序指纹信息，通过在搜索引擎、社交网站、网盘、Github等平台检索以及社工欺骗等手段获取组织架构、员工信息、源代码、账户密码、常用软件、常上网站、安全防护策略、外包服务供应商等信息，通过实地考察获取职场和机房的网络、门禁、办公等环境信息。

- **武器构建**

根据前期收集到的信息，针对性制作攻击代码。如果尝试对HR进行攻击，那么可以设计植入木马的简历文档，如果计划从线上服务入手，可以通过自动化扫描、人工测试等手段对目标资产进行漏洞探测，发现可利用的0day漏洞。在目前公开的APT案例中，至少有80%是从攻击员工办公电脑入手，因为人是系统最大的漏洞，利用社会工程学的攻击成功率高，同时攻陷员工电脑后更容易摸清内部网络及扩大控制范围。

- **攻击投放**

利用各种手段将攻击载荷投递到目标。比如利用命令注入、文件上传、SQL注入、SSRF、XSS、溢出等漏洞直接远程攻击线上服务，利用邮件钓鱼、U盘摆渡攻击、水坑攻击、软硬件供应链攻击、网络劫持等方式入侵服务器、员工电脑、网络设备。

- **执行利用**

不同环境采用不同的执行方式，在受限环境可利用系统组件或合法程序执行加载恶意代码，从而突

破系统限制或隐藏自身，达到木马顺利运行的目的。比如在Windows环境使用系统内置程序PowerShell执行脚本，恶意代码仅存在于内存中，文件不落地，类似可使用的执行方式非常多。

- **命令控制**

建立具有各种隐蔽级别的通道来操控目标设备或进入目标内网。比如通过WebShell（如Caidao、Weevely）、Reverse Shell（如Bash/Python/PowerShell）、远控木马RAT（如Cobalt Strike/Metasploit Meterpreter）、远程桌面访问软件（如TeamViewer/VNC），使用多层代理、传输加密、端口复用、Domain Fronting等方式、采用TCP/UDP/HTTP/HTTPS/DNS/ICMP/SMTTP等网络协议，甚至模仿其他正常应用通信流量，做到实时监控和遥控目标设备；通过端口转发（如netsh/iptables）、Socks代理（如ssh -D）、HttpTunnel（如reGeorg）、企业VPN通道等方式穿透企业内网，突破网络边界。

- **防御躲避**

利用检测对抗技术、攻击痕迹清除等方式逃避入侵检测、杀毒软件等安全系统的发现和追溯。比如使用肉鸡发起攻击避免暴露黑客真实IP，构造畸形请求包绕过WAF，将恶意代码注入到正常合法进程/文件内，利用白名单、反调试、无文件等手段绕过病毒检测（如使用知名企业合法数字证书给恶意程序签名），清除或破坏应用访问/系统登陆操作日志，降低行为活动频率等等。

- **权限维持**

通过劫持合法程序、驻留系统自启动后门、创建隐藏管理员账户等方式实现长期控制，即使系统重启或重装也不会消失。比如替换系统辅助功能（如放大镜、软键盘）、劫持动态连接库、利用Windows服务启动项/Linux定时任务crontab配置随系统自启动、设置suid特权程序、安装bootkit木马、盗用原有合法账户密码等等。

## 1.2、扩大控制权

- **权限提升**

利用系统弱点或配置不当等方式获取超级管理员级别权限。比如利用最新Windows/Linux内核提权漏洞，管理员权限运行的第三方软件存在漏洞可利用，管理员权限定时执行的程序文件因权限设置不当致使普通用户也可篡改程序，管理员密码随意存放在服务器普通文件里等等。

- **信息发现**

通过本地搜索、内网扫描和嗅探等方式确认已可以获取或控制的数据及进一步了解内部网络和可能利用的风险点。比如通过本机翻箱倒柜获取用户列表、进程列表、网络连接、配置文件、程序代码、数据库内容、运维操作记录、系统账户密码、浏览器保存密码、邮件内容等信息；通过内存导出、键盘记录、网络嗅探获取用户凭据；通过查询Windows域全部账户和主机，分析出企业完整的组织机构/人员、重要机器等信息；通过内网主机存活探测、远程服务探测描绘出内网结构拓扑图、内网应用服务以及可能的风险点；通过访问内部OA网站尤其是知识分享平台获取业务架构、代码、服务器等信息。

- **横向移动**

通过内网渗透攻击获取更多服务器权限和数据。一般来说黑客偏爱攻击拥有企业网络、机器、数据相关管理权限的系统，比如说Windows域控、补丁服务器、邮箱系统、内部即时通讯工具、跳板机、运维运营平台、密码系统、代码管理平台等，道理很简单，一旦攻破这些系统就几乎能够控制全部机器，进而获取目标业务数据；黑客也喜欢攻击企业高管、目标业务员工、网络管理员的电脑，因为这些人员掌握的信息更重要，也更接近黑客目的。其中一种常见的内网渗透思路是由于大多数企业内部网络隔离精细度不足（尤其是大型企业服务器数量太多，隔离成本大），内网站点安全性低（重点防御外部攻击，内部系统安全投入少），内网高危应用服务没有鉴权认证（比如Docker/Kubernetes/Redis/Hadoop等应用在未鉴权的情况下可造成服务器直接被入侵控制，不少人以为内网很安全所以没有开启鉴权），服务器帐号密码普遍通用（为了方便管理甚至全部服务器密码都一样），这些情况可以让黑客在内网渗透时很轻易获取到一些服务器的控制权限，然后逐一登陆服务器抓用户登陆凭证（一台服务器存在多个账户），再使用这些凭证尝试登陆其他服务器，若登陆成功后又继续抓其他用户登陆凭证，这些新拿到的凭证又可能可以登陆其他服务器，通过反复尝试登陆、抓取凭证这一经典套路，逐步扩大服务器控制范围，最终甚至可能做到全程使用合法用户凭证登陆任意服务器，就好似运维管理员正常登陆进行运维一样。

1.3、达成目的

- 数据收集  
搜集源代码、数据库、资产信息、技术方案、商业机密、邮件内容等攻击目标数据。
- 数据窃取  
对数据进行加密、压缩、分段处理，通过HTTP(S)/FTP/DNS/SMTP等网络协议主动对外传送、使用Web对外提供访问下载、物理U盘拷贝，或业务接口直接查询回显等方式将数据传输到黑客手中。
- 篡改破坏  
通过修改数据进行非法获利，摧毁数据进行打击报复等。

2、ATT&CK

ATT&CK Matrix for Enterprise

layouts ▶ show sub-techniques ▶ hide sub-techniques

Reconnaissance 10 techniques	Resource Development 4 techniques	Initial Access 10 techniques	Execution 10 techniques	Persistence 10 techniques	Privilege Escalation 12 techniques	Defense Evasion 17 techniques	Credential Access 12 techniques	Discovery 23 techniques	Lateral Movement 8 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2) Github Action Host Information (2) Github Action Identity Information (2) Github Action Network Information (2) Github Action OS Information (2) Github Action OS Information (2) Github Action OS Information (2) Github Action OS Information (2) Github Action OS Information (2) Github Action OS Information (2)	Acquire Infrastructure (2) Compromise Accounts (2) Compromise Infrastructure (2) Develop Capabilities (2) External Remote Services (2) Open Capabilities (2)	Drive-by Compromise (2) Exploit Public-Facing Application (2) External Remote Services (2) External Remote Services (2) External Remote Services (2) External Remote Services (2) External Remote Services (2) External Remote Services (2) External Remote Services (2) External Remote Services (2)	Command and Scripting Interactions (2) Exploitation for Client Execution (2) Exploitation for Client Execution (2) Exploitation for Client Execution (2) Exploitation for Client Execution (2) Exploitation for Client Execution (2) Exploitation for Client Execution (2) Exploitation for Client Execution (2) Exploitation for Client Execution (2) Exploitation for Client Execution (2)	Account Manipulation (2) BITS Jobs (2) BITS Jobs (2) BITS Jobs (2) BITS Jobs (2) BITS Jobs (2) BITS Jobs (2) BITS Jobs (2) BITS Jobs (2) BITS Jobs (2)	Abuse Elevation Control Mechanism (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2)	Abuse Elevation Control Mechanism (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2) Access Token Manipulation (2)	Basic Profile (2) Credential Access (2) Credential Access (2) Credential Access (2) Credential Access (2) Credential Access (2) Credential Access (2) Credential Access (2) Credential Access (2) Credential Access (2)	Application Discovery (2) Application Discovery (2) Application Discovery (2) Application Discovery (2) Application Discovery (2) Application Discovery (2) Application Discovery (2) Application Discovery (2) Application Discovery (2) Application Discovery (2)	Archive Collected Data (2) Automated Collection (2) Automated Collection (2) Automated Collection (2) Automated Collection (2) Automated Collection (2) Automated Collection (2) Automated Collection (2) Automated Collection (2) Automated Collection (2)	Application Layer Protocol (2) Automated Collection (2) Automated Collection (2) Automated Collection (2) Automated Collection (2) Automated Collection (2) Automated Collection (2) Automated Collection (2) Automated Collection (2) Automated Collection (2)	Automated Estimation (2) Data Destruction (2) Data Destruction (2) Data Destruction (2) Data Destruction (2) Data Destruction (2) Data Destruction (2) Data Destruction (2) Data Destruction (2) Data Destruction (2)	Account Access Removal (2) Data Destruction (2) Data Destruction (2) Data Destruction (2) Data Destruction (2) Data Destruction (2) Data Destruction (2) Data Destruction (2) Data Destruction (2) Data Destruction (2)	

2.1 侦察

技术	子技术
主动扫描	T1595.001 扫描IP块 T1595.002 漏洞扫描
收集目标主机信息	T1592.001 硬件 T1592.002 软件 T1592.003 固件 T1592.004 客户端配置
收集目标身份信息	T1589.001 凭证 T1589.002 电子邮件地址 T1589.003 员工姓名
收集目标网络信息	T1590.001 域属性 T1590.002 DNS T1590.003 网络信任依赖项 T1590.004 网络拓扑 T1590.005 IP地址 T1590.006 网络安全设备
收集目标组织信息	T1591.001 确定物理位置 T1591.002 业务关系 T1591.003 确定业务时间 T1591.004 识别角色
*针对信息的网络钓鱼	T1598.001 鱼叉式服务 T1598.002 鱼叉式附件 T1598.003 鱼叉式链接
*获取非公开来源信息	T1597.001 威胁情报提供商 T1597.002 购买技术数据
搜索开放技术数据库	T1596.001 DNS/被动DNS T1596.002 WHOIS T1596.003 数字证书 T1596.0034 CDN T1596.005 扫描数据库
*搜索开放网站/域名	T1593.001 社交媒体 T1593.002 搜索引擎
搜索目标拥有的网站	

## 2.2 资源开发

技术	子技术
构建基础设施	T1583.001 域 T1583.002 DNS服务器 T1583.003 虚拟专用服务器 T1583.004 服务器 T1583.005 僵尸网络 T1583.006 Web服务
盗取账号	T1586.001 社交媒体账户 T1586.002 电子邮件账户
攻陷基础设施	T1584.001 域 T1584.002 DNS服务器 T1584.003 虚拟专用服务器 T1584.004 服务器 T1584.005 僵尸网络 T1584.006 Web服务
开发能力	T1587.001 恶意软件 T1587.002 代码签名证书 T1587.003 数字证书 T1587.004 漏洞利用
创建（钓鱼、社工）账户	T1585.001 社交媒体账户 T1585.002 电子邮件账户
获取公开第三方工具	T1588.001 恶意软件 T1588.002 工具 T1588.003 代码签名证书 T1588.004 漏洞利用(Exploits) T1588.005 漏洞(Vulnerabilities)

### 2.3 初始访问

技术	子技术
水坑攻击	
利用公开漏洞	
外部远程服务	
渗透到其他网络介质	
硬件攻击	
钓鱼	T1566.001 鱼叉式附件 T1566.002 鱼叉式链接 T1566.003 通过服务进行网络钓鱼
通过可移动媒体进行复制	
供应链攻击	T1195.001 利用软件依赖性和开发工具 T1195.002 攻击软件供应链 T1195.003 攻击硬件供应链
利用可信关系	
利用合法账号	T1078.001 默认账户 T1078.002 域账户 T1078.003 本地账户 T1078.004 云账户

## 2.4 执行



技术	子技术
命令和脚本解释器	T1059.001 PowerShell T1059.002 AppleScript T1059.003 Windows命令行Shell T1059.004 Unix Shell T1059.005 Python T1059.007 JavaScript/JScript T1059.008 网络设备CLI
利用客户端执行	
进程间通讯	T1559.001 组件对象模型(COM) T1599.002 动态数据交换
原生API	
计划任务/工作	T1053.001 At (Linux) T1053.002 At (Windows) T1053.003 Cron T1053.004 计划任务 T1053.005 系统计时器
共享模块	
软件部署工具	
系统服务	T1569.001 Launchctl T1569.002 执行服务
用户执行	T1204.001 恶意链接 T1204.002 恶意文件
Windows管理规范 (WMI)	

## 2.5 持久化

技术	子技术
账户操作	T1098.001 额外的云凭证 T1098.002 Exchange电子邮件委托权限 T1098.003 添加Office 365全局管理角色 T1098.004 SSH 授权密钥
Windows后台智能传输服务（BITS）操作	
引导或登录自动启动执行程序	T1547.001 注册表运行键/启动文件夹 T1547.002 身份验证程序包 T1547.003 时间提供商 T1547.004 Winlogon Helper DLL T1547.005 安全支持提供者 T1547.006 内核模块和扩展 T1547.007 重新打开应用程序 T1547.008 LSASS驱动程序 T1547.009 修改快捷方式 T1547.010 端口监视器 T1547.011 修改Plist T1547.012 打印进程
引导或登录初始化脚本	T1037.001 登录脚本（Windows） T1037.002 登录脚本（Mac） T1037.003 网络登录脚本 T1037.004 Rc.common T1037.005 启动项目
浏览器扩展插件	
修改二进制客户端软件	
创建（系统访问）账户	T1136.001 本地账户 T1136.002 域账户 T1136.003 云账户
创建或修改系统进程	T1543.001 启动代理 T1543.002 系统服务 T1543.003 Windows 服务 T1543.004 启动守护程序

技术	子技术
事件触发执行	T1546.001 更改默认文件关联 T1546.002 屏保 T1546.003 Windows管理规范 (WMI) 事件 T1546.004 .bash_profile 和 .bashrc T1546.005 陷阱 T1546.006 添加 LC_LOAD_DYLIB T1546.007 Netsh 帮助程序DLL T1546.008 辅助功能 T1546.009 AppCert DLLs T1546.010 APPInit DLLs T1546.011 应用 T1546.012 图像文件选项注入 T1546.013 PowerShell 配置文件 T1546.014 Emond T1546.015 组件对象模型(COM)劫持
外部远程服务	
劫持执行流	T1574.001 DLL搜索顺序劫持 T1574.002 DLL侧加载 T1574.004 Dylib劫持 T1574.005 可执行安装程序文件权限不足 T1574.006 LD_PRELOAD T1574.007 通过PATH环境变量进行路径拦截 T1574.008 通过搜索顺序劫持进行路径拦截 T1574.009 通过未引用路径截取路径 T1574.010 服务文件权限不足 T1574.011 服务注册表权限不足 T1574.012 COR_PROFILER
在云容器镜像中植入后门	
Office 应用程序启动	T1137.001 Office宏模板 T1137.002 Office测试 T1137.003 Outlook表格 T1137.004 Outlook主页 T1137.005 Outlook规则 T1137.006 加载项
操作系统前启动	T1542.001 系统固件 T1542.002 组件固件 T1542.003 引导程序 T1542.004 ROMMON套件 T1542.005 TFTP引导
计划任务/工作	T1053.001 At (Linux) T1053.002 At (Windows) T1053.003 Cron T1053.004 Launchd T1053.005 计划任务 T1053.006 系统计时器

技术	子技术
服务器软件组件	T1505.001 SQL存储过程 T1505.002 传输代理 T1505.003 Web Shell
构造特殊数据触发	端口敲门
有效账户	T1078.001 默认账户 T1078.002 域账户 T1078.003 本地账户 T1078.004 云账户

## 2.6 特权提升

技术	子技术
滥用权限提升机制	T1548.001 Setuid 和 Setgid T1548.002 绕过用户账户控制 (UAC) T1548.003 Sudo 和 Sudo缓存 T1548.004 提示立即执行
操控访问令牌	T1134.001 令牌模拟/窃取 T1134.002 使用令牌创建流程 T1134.003 制作和模拟令牌 T1134.004 父PID欺骗 T1134.005 SID历史记录注入
引导或登录自动启动执行	T1547.001 注册表Run键/启动文件夹 T1547.002 身份验证程序包 T1547.003 时间提供商 T1547.004 Winlogon Helper DLLs T1547.005 安全支持提供 T1547.006 内核模块和扩展 T1547.007 重新打开的应用程序 T1547.008 LSASS驱动程序 T1547.009 修改快捷方式 T1547.010 端口监视器 T1547.011 修改Plist T1547.012 打印进程
引导或登录初始化脚本	T1307.001 登录脚本 (Windows) T1307.002 登录脚本 (Linux) T1307.003 网络登录脚本 T1307.004 Rc.common T1307.005 启动项目
创建或修改系统进程	T1543.001 启动代理 T1543.002 系统服务 T1543.003 Windows服务 T1543.004 启动守护程序
修改域策略	T1484.001 修改组策略 T1484.002 修改与信任

技术	子技术
事件触发执行	T1546.001 更改默认文件关联 T1546.002 屏保 T1546.003 Windows管理规范(WMI)订阅 T1546.004 .bash_profile 和 .bashrc T1546.005 陷阱 T1546.006 LC_LOAD_DYLIB添加 T1546.007 Netsh Helper DLL T1546.008 辅助功能 T1546.009 AppCert DLLs T1546.010 AppInit DLLs T1546.011 Application Shimming T1546.012 图像文件执行选项注入 T1546.013 PowerShell配置文件 T1546.014 Emond T1546.015 组件对象模型(COM)劫持
利用特权提升漏洞	
劫持执行流程	T1574.001 DLL搜索顺序劫持 T1574.002 DLL侧加载 T1574.004 Dylib劫持 T1574.005 可执行安装程序文件权限不足 T1574.006 LD_PRELOAD T1574.007 通过PATH环境变量进行路径拦截 T1574.008 通过搜索顺序劫持进行路径拦截 T1574.009 通过未引用路径截取路径 T1574.010 服务文件权限不足 T1574.011 服务注册表权限不足 T1574.012 COR_PROFILER
进程注入	T1055.001 动态链接库注入 T1055.002 PE可执行文件注入 T1055.003 线程执行劫持 T1055.004 异步过程调用 T1055.005 线程本地存储 T1055.008 Ptrace系统调用 T1055.009 Proc内存 T1055.011 额外的窗口内存注入 T1055.012 进程 Hollowing T1055.013 进程复制 T1055.014 VDSO劫持
计划任务/工作	T1053.001 At (Linux) T1053.002 At (Windows) T1053.003 Cron T1053.004 Launchd T1053.005 计划任务 T1053.006 系统计时器

技术	子技术
有效账号	T1078.001 默认账户 T1078.002 域账户 T1078.003 本地账户 T1078.004 云账户

2.7 防御绕过

技术	子技术
滥用权限提升机制	T1548.001 Setuid 和 Setgid T1548.002 绕过用户账户控制 (UAC) T1548.003 Sudo 和 Sudo缓存 T1548.004 提示立即执行
操控访问令牌	T1134.001 令牌模拟/窃取 T1134.002 使用令牌创建流程 T1134.003 制作和模拟令牌 T1134.004 父PID欺骗 T1134.005 SID历史记录注入
Windows后台智能传输服务 (BITS)	
反混淆/解码文件或信息	
直接访问逻辑卷	
修改域策略	T1484.001 修改组策略 T1484.002 修改与信任
执行范围	T1480.001 关键环境
绕过安全防护软件利用	T1222.001 Windows文件和目录权限修改 T1222.002 Linux 和 Mac文件和目录权限修改
修改文件和目录权限	
隐藏攻击痕迹	T1564.001 隐藏的文件和目录 T1564.002 隐藏的用户 T1564.003 隐藏的窗口 T1564.004 NTFS文件属性 T1564.005 隐藏文件系统 T1564.006 运行虚拟实例 T1564.007 VBA冲突
劫持执行流	T1574.001 DLL搜索顺序劫持 T1574.002 DLL侧加载 T1574.004 Dylib劫持 T1574.005 可执行安装程序文件权限不足 T1574.006 LD_PRELOAD T1574.007 通过PATH环境变量进行路径拦截 T1574.008 通过搜索顺序劫持进行路径拦截 T1574.009 通过未引用路径截取路径 T1574.010 服务文件权限不足 T1574.011 服务注册表权限不足 T1574.012 COR_PROFILER



技术	子技术
攻击安全防御机制	T1562.001 禁用或修改工具 T1562.002 禁用Windows事件记录 T1562.003 破坏命令历史记录 T1562.004 禁用或修改系统防火墙 T1562.006 指示灯阻塞 T1562.007 禁用或修改云防火墙 T1562.008 禁用云日志
删除主机上的痕迹	T1070.001 清除Windows事件日志 T1070.002 清除Linux或Mac系统日志 T1070.003 清除命令历史记录 T1070.004 文件删除 T1070.005 删除网络共享连接 T1070.006 Timestamp
间接命令执行	
伪	T1036.001 无效的代码签名 T1036.002 从右到左覆盖 T1036.003 重命名系统实用程序 T1036.004 任务或服务 T1036.005 匹配合法名称或位置 T1036.006 文件名后的空格
修改身份认证过程	T1556.001 域控制器身份验证 T1556.002 密码过滤器DLL T1556.003 可插拔身份验证模块 T1556.004 网络设备认证
修改云计算基础架构	T1578.001 创建快照 T1578.002 创建云实例 T1578.003 删除云实例 T1578.004 还原云实例
修改注册表	
修改系统映像	T1601.001 修改系统映像 T1601.002 降级系统映像
网络边界桥接	T1599.001 网络地址转换遍历
混淆的文件或信息	T1027.001 二进制填充 T1027.002 软件包装 T1027.003 隐写术 T1027.004 传送后编译 T1027.005 去除工具特征
操作系统前启动	T1542.001 系统固件 T1542.002 组件固件 T1542.003 引导程序 T1542.004 ROMMON套件 T1542.005 TFTP引导

技术	子技术
进程注入	T1055.001 动态链接库注入 T1055.002 PE可执行文件注入 T1055.003 线程执行劫持 T1055.004 异步过程调用 T1055.005 线程本地存储 T1055.008 Ptrace系统调用 T1055.009 Proc内存 T1055.011 额外的窗口内存注入 T1055.012 进程 Hollowing T1055.013 进程复制 T1055.014 VDSO劫持
恶意域控制器	
Rookit	
受信任签名的二进制代理执行	T1218.001 编译的HTML文件 T1218.002 控制面板 T1218.003 CMSTP T1218.004 安装工具 T1218.005 Mshta T1218.007 Msiexec T1218.008 Odbcconf T1218.009 Regsvcs/Regasm T1218.010 Regsvr32 T1218.011 Rundll32 T1218.012 Verclsid
受信任的签名脚本代理执行	T1216.001 PubPrn
颠覆信任控制	T1553.001 绕过看门狗 T1553.002 代码签名 T1553.003 劫持SIP和信任提供者 T1553.004 安装根证书
模板注入	
构造特殊数据触发	T1205.001 端口敲门
受信任的开发人员实用程序代理执行	T1127.001 MSBuild
未使用/不受支持的云区域	
使用替代的身份验证资料	T1550.001 应用程序访问令牌 T1550.002 PTH (Pass the Hash) T1550.003 PTT (Pass the Ticket) T1550.004 Web 会话Cookie
有效账号	T1078.001 默认账户 T1078.002 域账户 T1078.003 本地账户 T1078.004 云账户

技术	子技术
虚拟化/沙箱逃逸	T1497.001 系统检查 T1497.002 基于用户活动的检查 T1497.003 基于事件的规避
弱加密	T1600.001 减少密钥空间 T1600.002 禁用加密硬件
XSL脚本处理	

2.8 凭证访问

技术	子技术
爆破	T1110.001 密码猜测 T1110.002 密码破解 T1110.003 密码喷射 T1110.004 凭证填充
密码存储中的凭证	T1555.001 Keychain T1555.002 安全存储器 T1555.003 来自Web浏览器的凭证
利用凭证访问8	T1606.001 Web Cookie T1606.002 SAML令牌
强制身份认证	
伪造Web凭证	
输入捕获	T1056.001 键盘记录 T1056.002 GUI输入捕获 T1056.003 Web门户捕获 T1056.004 凭证API Hooking
中间人	T1557.001 LLMNR/NBT-NS 和 SMB中继 T1557.002 ARP缓存中毒
修改身份验证过程	T1556.001 域控制器身份验证 T1556.002 密码过滤器DLL T1556.003 可插拔身份验证模块 T1556.004 网络设备认证
网络嗅探	
操作系统凭证转储	T1003.001 LSASS内存 T1003.002 SAM (security account manager) T1003.003 NTDS T1003.004 LSA Secrets T1003.005 缓存的域凭证 T1003.006 DCSync T1003.007 Proc文件系统 T1003.008 /etc/passwd 和 /etc/shadow
窃取应用程序访问令牌	
窃取或伪造Kerberos凭证	T1558.001 黄金票据 T1558.002 白银票据 T1558.003 Kerberoasting T1588.004 AS-REP Roasting
窃取Web会话Cookie	
双因子身份认证拦截	

技术	子技术
不安全的凭证	T1552.001 文件中的凭证 T1552.002 注册表中的凭证 T1552.003 Bash历史记录 T1552.004 私钥 T1552.005 云实例元数据API T1552.006 组策略首选项

2.9 发现

技术	子技术
账户发现	T1087.001 本地账户 T1087.002 域账户 T1087.003 电子邮件账户 T1087.004 云账户
应用程序窗口发现	
浏览器书签发现	
云基础设施发现	
云服务仪表板	
云服务发现	
域信任关系发现	
文件和目录发现	
网络服务扫描	
网络共享发现	
网络嗅探	
密码策略发现	
外围设备发现	
权限组发现	T1069.001 本地组 T1069.002 域组 T1069.003 云组
进程发现	
查询注册表	
远程系统发现	
软件发现	T1518.001 安全软件发现
系统信息发现	
系统网络配置发现	
系统网络连接发现	
系统所有者/用户发现	
系统服务发现	
系统时间发现	
虚拟化/沙箱逃逸	T1497.001 系统检查 T1497.002 基于用户活动的检查 T1497.003 基于时间的规避

## 2.9 横向移动

技术	子技术
利用远程服务	
内部鱼叉攻击	
远程服务会话劫持	T1563.001 SSH劫持 T1563.002 RDP劫持
远程服务	T1021.001 远程桌面协议 T1021.002 SMB/Windows管理员共享 T1021.003 分布式组件对象模型（COM） T1021.004 SSH T1021.005 VNC T1021.006 Windows远程管理
通过可移动介质复制	
软件部署工具	
污染共享内容	
使用替代的身份验证资料	T1550.001 应用程序访问令牌 T1550.002 PTH（Pass the Hash） T1550.003 PTT（Pass the Ticket） T1550.004 Web 会话 Cookie

## 2.10 收集

技术	子技术
存档收集的数据	T1560.001 通过应用程序存档 T1560.002 通过库存档 T1560.003 通过自定义方法存档
音频捕获	
自动化收集	
剪贴板数据	
来自云存储对象的数据	
来自配置存储库的数据	T1602.001 SNMP (MIB Dump) T1602.002 网络设备配置转储
来自信息存储的数据	T1213.001 Confluence T1213.002 SharePoint
来自本地系统的数据	
来自网络共享驱动器的数据	
来自可移动介质的数据	
暂存数据	T1074.001 本地数据分段 T1074.002 远程数据暂存
电子邮件收集	T1114.001 本地电子邮件收集 T1114.002 远程电子邮件收集 T1114.003 电子邮件转发规则
输入捕获	T1056.001 键盘记录 T1056.002 GUI输入捕获 T1056.003 Web门户捕获 T1056.004 凭证API挂钩
浏览器身份复用	
中间人	T1557.001 LLMNR/NBT-NS中毒 和 SMB中继 T1557.002 ARP缓存中毒
屏幕捕获	
视频捕获	

## 2.11 命令与控制



技术	子技术
应用层协议	T1071.001 Web协议 T1071.002 文件传输协议 T1071.003 邮件协议 T1071.004 DNS
通过可移动介质进行通信	
数据编码	T1132.001 标准编码 T1132.002 非标准编码
数据混淆	T1001.001 垃圾数据 T1001.002 隐写术 T1001.003 协议模拟
动态解析	T1568.001 快速流量DNS T1568.002 域生成算法 T1568.003 DNS计算
加密通道	T1573.001 对称密码学 T1573.002 不对称密码学
备用通道	
传输入侵工具	
多阶段通道	
非应用层协议	
非标准端口	
协议隧道	
代理	T1090.001 内部代理 T1090.002 外部代理 T1090.003 多跳代理 T1090.004 域名前置
远程访问软件	
构造特殊数据触发	T1205.001 端口敲门
网络服务	T1102.001 Dead Drop Resolver T1102.002 双向通讯 T1102.003 单向通讯

## 2.12 数据外传

技术	子技术
自动提取	T1020.001 流量复制
数据传输大小限制	
通过替代协议外传	T1048.001 通过对称加密的非C2协议进行渗透 T1048.002 通过非对称加密非C2协议进行渗透 T1048.003 通过未加密/混淆的非C2协议进行渗透
通过C2通道进行外传	
通过其他网络介质进行外传	T1011.001 通过蓝牙渗透
物理介质上的外传	T1052.001 通过USB的渗透
通过Web服务外传	T1567.001 渗透到代码存储库 T1567.002 渗透到云存储
计划转移	
传输数据到云账户	

## 2.13 影响

技术	子技术
用户访问权限删除	
数据销毁	
数据加密产生的影响	
数据修改	T1565.001 操作存储的数据 T1565.002 操作传输数据 T1565.003 操作运行时的数据
数据污染	T1491.001 内部污染 T1491.002 外部污染
磁盘擦除	T1561.001 磁盘内容擦除 T1561.002 磁盘结构擦除
终端拒绝服务	T1499.001 OS泛洪 T1499.002 服务耗尽 T1499.003 应用程序耗尽 T1499.004 攻击应用程序或系统
固件损坏	
禁用系统恢复	
网络拒绝服务	T1498.001 直接网络泛洪 T1498.002 反射放大
资源劫持	
停止服务	
系统关机/重启	

# 0X003 法律法规

## 1、《网络安全法》

1	《中华人民共和国网络安全法》全文
2	目 录
3	第一章 总 则
4	第二章 网络安全支持与促进
5	第三章 网络运行安全
6	第一节 一般规定
7	第二节 关键信息基础设施的运行安全
8	第四章 网络信息安全
9	第五章 监测预警与应急处置
10	第六章 法律责任
11	第七章 附 则
12	第一章 总 则

13 第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织  
14 的合法权益，促进经济社会信息化健康发展，制定本法。

15 第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

16

17 第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方  
18 针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全  
19 网络安全保障体系，提高网络安全保护能力。

20

21 第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域  
22 的网络安全政策、工作任务和措施。

23

24 第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护  
25 关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩  
26 序。

27

28 第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社  
29 会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

30

31 第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流  
32 与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

33

34 第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部  
35 门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督  
36 管理工作。

37

38 县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

39

40 第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，  
41 诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

42

43 第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性  
44 要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违  
45 法犯罪活动，维护网络数据的完整性、保密性和可用性。

46

47 第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安  
48 全保护，提高网络安全保护水平，促进行业健康发展。

49

50 第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水  
51 平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

52

53 任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得  
54 利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破  
55 坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、  
56 传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

57

58 第十三条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害  
59 未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

60

61 第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部  
62 门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

63

64 有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

65

66 第二章 网络安全支持与促进

67

68 第十五条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据  
69 各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业  
70 标准。

49 国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

50

51

52 第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构 and 高等学校等参与国家网络安全技术创新项目。

53

54 第十七条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

55

56 第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

57

58 国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

59

60 第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

61

62 大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

63

64 第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

65

66 第三章 网络运行安全

67 第一节 一般规定

68

69 第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

70

71 （一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

72

73 （二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

74

75 （三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

76

77 （四）采取数据分类、重要数据备份和加密等措施；

78

79 （五）法律、行政法规规定的其他义务。

80

81 第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

82

83 网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

84

85 网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

86

87 第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

88

89 第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，  
或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供  
90 真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

91 国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之  
92 间的互认。

93 第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻  
击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，  
并按照规定向有关主管部门报告。

94 第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻  
95 击、网络侵入等网络安全信息，应当遵守国家有关规定。

96 第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危  
97 害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等  
危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告  
推广、支付结算等帮助。

98 第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术  
99 支持和协助。

100 第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，  
101 提高网络运营者的安全保障能力。

102 有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期  
103 向会员进行风险警示，支持、协助会员应对网络安全风险。

104 第三十条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需  
105 要，不得用于其他用途。

106 第二节 关键信息基础设施的运行安全

107 第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业  
108 和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利  
109 益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体  
范围和安全保护办法由国务院制定。

110 国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

111 第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织  
112 实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

113 第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术  
114 措施同步规划、同步建设、同步使用。

115 第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：  
116  
117 （一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；  
118  
119 （二）定期对从业人员进行网络安全教育、技术培训和技能考核；  
120  
121 （三）对重要系统和数据库进行容灾备份；  
122  
123 （四）制定网络安全事件应急预案，并定期进行演练；  
124  
125 （五）法律、行政法规规定的其他义务。  
126  
127  
128

129 第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

130

131 第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

132

133 第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

134

135 第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

136

137 第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

138

139 （一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

140

141 （二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

142

143 （三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

144

145 （四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

146

147 第四章 网络信息安全

148 第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

149

150 第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

151

152 网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

153

154 第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

155

156 网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

157

158 第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

159

160 第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

161

162 第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

163

164 第四十六条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

165



166 第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输  
167 的信息的，应当立即停止传输该信息，采取删除等处置措施，防止信息扩散，保存有关记录，并向有关  
168 主管部门报告。

169 第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、  
170 行政法规禁止发布或者传输的信息。

171 电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定  
172 行为的，应当停止提供服务，采取删除等处置措施，保存有关记录，并向有关主管部门报告。

173 第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受  
174 理并处理有关网络信息安全的投诉和举报。

175 网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

176 第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发  
177 布或者传输的信息的，应当要求网络运营者停止传输，采取删除等处置措施，保存有关记录；对来源于  
178 中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

179 第五章 监测预警与应急处置

180 第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网  
181 络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

182 第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监  
183 测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

184 第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事  
185 件应急预案，并定期组织演练。

186 负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期  
187 组织演练。

188 网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并  
189 规定相应的应急处置措施。

190 第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程  
191 序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

192 （一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

193 （二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、  
194 影响范围和危害程度；

195 （三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

196 第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评  
197 估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布  
198 与公众有关的警示信息。

199 第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险  
200 或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行  
201 约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

202 第五十七条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事  
203 件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者  
批准，可以在特定区域对网络通信采取限制等临时措施。



204

## 205 第六章 法律责任

206 第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

207

208 关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

209

210 第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

211

212 （一）设置恶意程序的；

213

214 （二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

215

216 （三）擅自终止为其产品、服务提供安全维护的。

217

218 第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

219

220 第六十二条 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

221

222 第六十三条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节严重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

223

224 单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

225

226 违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

227

228 第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

229

230 违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

231

232 第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

233

234 第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外  
提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚  
款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接  
负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

235

236 第六十七条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络  
发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，

237

238 可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上  
五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

239

240 单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接  
责任人员依照前款规定处罚。

241

242 第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止  
传输、采取删除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；  
拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关  
闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元  
以上十万元以下罚款。

243

244 电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义  
务的，依照前款规定处罚。

245

246 第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者  
情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元  
以上十万元以下罚款：

247

248 （一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置  
措施的；

249

250 （二）拒绝、阻碍有关部门依法实施的监督检查的；

251

252 （三）拒不向公安机关、国家安全机关提供技术支持和协助的。

253

254 第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照  
有关法律、行政法规的规定处罚。

255

256 第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

257

258 第七十二条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有  
关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

259

260 第七十三条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用  
于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

261

262 网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

263

264 第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。

265

266 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

267

268 第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息  
基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机  
构、组织、个人采取冻结财产或者其他必要的制裁措施。

269

270 第七章 附 则

271 第七十六条 本法下列用语的含义：

272

273	（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。
274	
275	（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。
276	
277	（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。
278	
279	（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。
280	
281	（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。
282	
283	第七十七条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。
284	
285	第七十八条 军事网络的安全保护，由中央军事委员会另行规定。
286	
287	第七十九条 本法自2017年6月1日起施行。

## 2、保密方面

1	危害国家秘密安全的行为
2	
3	包括国家领土、主权独立不受侵犯：
4	国家秘密的密级
5	
6	绝密--最重要的国家秘密啊--使国家安全和利益遭受特别严重的损害--破坏国家主权和领土完整，威胁国家政权巩固，使国家政治、经济遭受巨大损失--全局性，战略性
7	机密--重要的国家秘密--使国家和利益遭受严重的损害--某一领域内的国家安全和利益遭受重大损失--较大范围
8	秘密--一般的国家秘密--使国家安全和利益遭受损害--某一方面的国家安全利益遭受损失--局部性
9	危害国家秘密安全的行为
10	
11	严重违反保密规定行为
12	
13	违反涉密信息系统和信息设备保密管理规定的行为：
14	违法国家秘密载体管理规定的行为
15	违反国家秘密信息管理规定的行为
16	定密不当行为
17	
18	定密不当包括对应当定密的事项不定密，或者对不应当定密的事项定密
19	对应当定密的事项不定密，可能导致国家秘密失去保护，造成泄密
20	对不应当定密的事项定密，会严重影响信息资源合理利用，可能造成较大负面影响
21	公共信息网络运营商、服务商不履行保密义务的行为
22	
23	互联网及其他公共信息网络运营商、服务商没有履行配合公安机关、国家安全机关、检察机关对泄密案件进行调查的义务；
24	发现发布的信息设计国家秘密，没有立即停止传输和保存客户发布信息的内容及有关情况记录，并及时向公安机关、国家安全机关、保密行政管理部门报告；
25	没有按照公安机关、国家安全机关、保密行政管理部门要求，及时对互联网或公共信息网上发布的涉密信息予以删除、致使涉密信息继续扩散
26	保密行政端粒部门工作人员的违法行为
27	

28 保密行政管理部门的工作人员在履行保密管理职责滥用职权、玩忽职守、徇私舞弊：

29

30 滥用职权是指保密行政管理部门工作人员超越职权范围或者违背法律授权的宗旨、违反法律程序行驶职权的行为：

31 玩忽职守是指保密行政管理部门工作人员严重不负责任，不履行或不正确履行职责的行为

32 徇私舞弊是指保密行政管理部门工作人员在履行职责过程中，利用职务之便，弄虚作假、

33 危害国家秘密安全的犯罪行为

34

35 危害国家安全的犯罪行为

36

37 掌握国家秘密的国家工作人员在履行公务期间，擅离职守，叛逃境外或者境外叛逃；

38 参加间谍组织或者接受间谍组织及其代理人的任务

39 为敌人指示轰击目标，为境外的机构，组织、人员窃取、刺探、收买、非法提供国家秘密或者情报

40 妨碍社会管理秩序的犯罪行为

41

42 以窃取、刺探、收买方法，非法获取国家秘密

43 非法持有属于国家秘密、机密的文件、资料或者其他物品，拒不说明来源与用途

44 渎职的犯罪行为

45

46 国家机关工作人员、非国家机关工作人员违反保守国家秘密法的规定，故意泄密国家秘密

47 国家机关工作人员、非国家机关工作人员违反保守国家秘密

48 军人违反职责的犯罪行为

49

50 以窃取、刺探、收买方法，非法获取军事秘密

51 为境外的机构、组织、人员窃取、刺探、收买、非法提供军事秘密

52 违反保守国家秘密法规，故意泄露军事秘密（战时有此行为会受到从重处罚）

53 违反保守国家秘密法规，过失泄露军事秘密（战时有此行为会受到从中处罚）

54 保护国家秘密相关法律

55

56 《保密法》2010年10月1日起正式施行的新《保密法》从四个方面明确了危害国家秘密安全你的行为的法律责任，是查处泄密违法行为有法可依、有章可循

57 严重违反保密规定的法律责任

58

59 《中华人民共和国公务员法》、《中华人民共和国行政监察法》、《行政机关公务员处分条例》

60 互联网及其他公共信息网络运营商、服务商的有关法律责任

61

62 《中华人民共和国治安管理处罚法》、《中华人民共和国电信条例》、《计算机信息网络国际联网安全保护管理办法》、《互联网信息服务管理办法》

63

64 侵犯商业秘密

65

66 商业秘密：不为公众所知悉、能为权利人带来经济利益、具有实用性并由权利人采取保密措施的技术信息和经营信息。技术信息类商业秘密包括由单位研制开发或者以其他合法方式掌握、未公开的设计、程序、产品配方、制作工艺、制作方法等信息，以及完整的技术方案、开发过程中的阶段性技术成果以及取得的有价值的技术数据，包括但不限于设计入职（含草图），实验结果和实验记录、样品、数据等，也包括针对技术问题的技术诀窍；经营信息类商业秘密包括经营策略、产销策略、管理诀窍、客户名单、货源情报、招投标中的标底书内容等信息

67 侵犯商业秘密的行为：

68

69 以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密

70 保护商业秘密相关法律法规

71

72 《中华人民共和国刑法》

73 《中华人民共和国反不正当竞争法》

74 《中华人民共和国合同法》

75 《中华人民共和国劳动合同法》

76 侵犯个人隐私信息行为：

77

78	未经他人同意，擅自公布他人的隐私材料，或者以书面、口头形式宣扬他人隐私
79	窃取或者以其他非法方式获取公民个人电子信息
80	出售或者非法向他人提供公民个人电子信息
81	网络服务提供者和其他企业事业单位在业务活动中未经过被收集者同意就收集、使用公民个人电子信息
82	对在业务活动中经被收集者同意手机的公民个人信息没有采取必要的保密措施
83	医疗机构及其医务人员泄露患者隐私或者未经患者同意，公开其病历资料、健康体检报告等行为
84	侵犯个人隐私信息犯罪行为：
85	
86	隐匿、毁弃或者非法拆开他人信件，侵犯公民通信自由权利，情节严重的；
87	邮政工作人员私自拆开或者隐匿、毁弃邮件、电报的
88	国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的；
89	窃取或者以其他方法非法获取公民个人信息，情节严重的
90	非法截获、篡改、删除他人电子邮件或者其他资料，情节严重的
91	人民警察泄露因制作、发放、查验、扣押居民身份证而知悉公民个人洗脑洗，情节严重的
92	

### 3、相关

1	网络犯罪行为
2	
3	破坏互联网运行安全的行为
4	
5	侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统
6	违反国家规定，侵入计算机系统，造成危害
7	故意制作、传播计算机病毒等破坏程序，攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损害
8	违反国家规定，擅自中断计算机网络或者通信服务，造成计算机网络或者通信系统不能正常运行
9	违反国家规定，对计算机信息系统进行删除、修改、增加、干扰、造成计算机信息系统不能正常运行
10	违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加
11	破坏国家安全和社会稳定的行为
12	
13	利用互联网造谣、诽谤
14	破坏市场经济秩序和社会管理秩序的行为
15	
16	利用互联网销售伪劣产品或者对商品、服务作虚假宣传
17	利用互联网损坏他人商业信誉和商品声誉
18	利用互联网侵犯他人知识产权
19	利用互联网编造并传播影响证券、期货交易或者其他扰乱金融秩序的虚假信息
20	在互联网上建立淫秽网站、网页，提供淫秽站点连接服务，或者传播淫秽书刊、影片、音像、图片
21	侵犯个人、法人和其他组织的人身、财产等合法权利的行为
22	
23	利用互联网侮辱他人或者捏造事实诽谤他人
24	非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密
25	利用互联网进行窃取、诈骗、敲诈勒索：利用网络写恐吓信或者以其他方法威胁他人人身安全的
26	利用网络捏造事实诬告陷害他人，企图使他人受到刑事追究或者受到治安管理处罚
27	利用网络对证人及其近亲属进行威胁、侮辱或者打击报复
28	利用网络多次发送淫秽、侮辱、恐吓或者其他信息，干扰他人正常生活
29	利用网络偷窥、偷拍、窃听、散布他人隐私
30	利用网络煽动民族仇恨、民族歧视，或者在网络中刊载民族歧视、侮辱内容
31	利用互联网实施以上四类所列行为以外的违法/犯罪行为
32	相关法律
33	
34	《刑法》
35	《关于维护互联网安全的决定》



# 0X0004 环境

## 1、工作环境搭建

### 1.1、系统







Commando VM：FireEye发布的一个包含超过140个开源Windows渗透工具包，红队渗透测试员和蓝队防御人员均拥有了顶级侦察与漏洞利用程序集。






- 原生支持Windows和Active Directory；
- 可作为C2框架的临时工作区；
- 更便捷的共享和交互式操作支持；
- 支持PowerView和BloodHound等工具；
- 对测试目标不产生任何影响。















### 1.2 常用工具

- Metasploit框架
- Cobalt Strike
- PowerShell Empire
- dnscat2
- p0wnedShell
- Pupy Shell
- PoshC2
- Merlin
- Nishang
- 各类Java中间件的各种已知Nday漏洞利用
- 针对各类Windows PHP集成环境

Active Directory Tools	2019/4/3 13:25	文件夹
Command & Control	2020/1/10 18:16	文件夹
Debuggers	2020/10/5 15:40	文件夹
Developer Tools	2020/10/5 13:40	文件夹
dotNET	2019/4/3 11:56	文件夹
Evasion	2019/4/4 11:09	文件夹
Exploitation	2020/1/10 18:09	文件夹
Information Gathering	2019/4/4 10:22	文件夹
Networking Tools	2020/1/10 16:15	文件夹
Password Attacks	2020/10/5 12:07	文件夹
Utilities	2020/1/10 17:17	文件夹
Vulnerability Analysis	2019/4/4 10:27	文件夹
Web Application	2020/1/10 18:14	文件夹
Wordlists	2019/4/3 17:43	文件夹

 Covenant	2020/1/10 18:10
 Elite	2020/1/10 18:16
 PoshC2-StartC2Server	2019/4/3 17:44
 PoshC2-StartC2Viewer	2019/4/3 17:44
 WMIImplant	2020/1/10 16:16
 WMIOps	2020/1/10 16:16

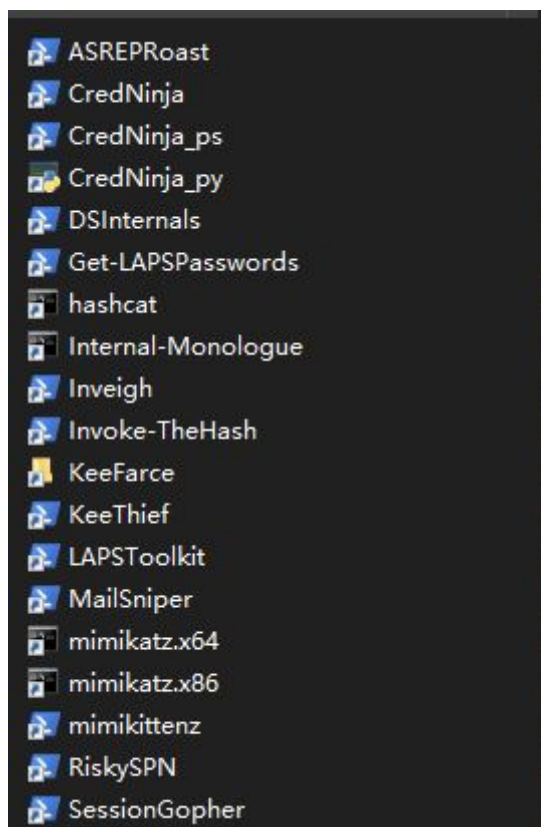
 snowman.ini	
 windbgx64	
 windbgx86	
 x32dbg	
 x64dbg	

 CheckPlease	
 demiguise	
 DotNetToJScript	
 Invoke-CradleCrafter	
 Invoke-DOSfuscation	
 Invoke-Obfuscation	
 Invoke-Phant0m	
 nps	
 pafishmacro	
 PowerLessShell	
 PowerShdll	
 PSAmsi	
 PSAttack	
 StarFighters	

- GhostPack
- impacket-examples-windows
- kali-windows-binaries
- metasploit
- PrivExchange
- ADAPE
- API Monitor x64
- API Monitor x86
- CrackMapExecWin
- DAMP
- Exchange-AD-Privesc
- Generate-Macro
- Invoke-ACLPwn
- Invoke-DCOM
- Invoke-GoFetch
- Invoke-PowerThIEf
- Invoke-PSImage
- luckystrike
- metatwin
- NetshHelperBeacon
- nishang
- Orca
- PowerLurk
- PowerPriv
- PowerShell-Suite
- PowerSploit
- PowerUpSQL
- PSReflect
- RedTeamPowershellScripts
- ruler
- SharpExchangePriv
- SharpSploit

- ADACLScanner
- ADExplorer
- ADOffline
- ADRecon
- BloodHound
- Get-ReconInfo
- gowitness
- nmap
- PowerView
- PowerView\_dev
- SharpHound.exe
- SharpHound.ps1
- SharpView
- SpoolerScanner
- zenmap





## 2、工作环境加固

### 溯源与反溯源

溯源让演习得以攻守互换，是防守方的重要工作之一。演习攻击方并不能毫无顾忌的肆意输出，首先需要考虑的是隐藏自身，这也让演习更加贴近于真实的攻击行动。这里讨论的溯源并不只是停留在分析攻击手法和定位来源IP上，更进一步需要关联到真实的行为人，所以攻击方使用匿名资源变得非常必要：

- VPN、匿名代理
- 纯净的渗透环境、虚拟机
- 匿名邮箱、手机号、VPS等
- 纯净的移动设备、无线设备等

实名的资源变得不太可靠，这并不是夸张，防守方通过各种途径可以反查到攻击者的踪迹，甚至动用“社工”等攻击手段，包括不限于博客、实名认证的社交账号、手机号、服务器等等。在攻防基础设施相对完善的前提下，很多溯源与反溯源的对抗会下沉到细节层面，比如攻击队员通过社交工具传递目标可疑URL时，如果误点击通过系统默认的浏览器打开，则可能会被JSOPN蜜罐捕获社交账号或者被抓到真实出口IP。当然这也对防守方的溯源分析能力是一个考验，从海量攻击数据中提取出有效的关键信息。现在大量的蜜罐等主动防御手段起到了不错的效果，需要注意的是蜜罐本身安全措施也需要隔离得当，避免造成安全隐患。

**作为应对，攻击方必须使用纯净的专用渗透环境进行攻击，完全与日常工作环境区分开来，并做测试环境的定期还原。**在识别蜜罐之后，可以通过投喂大量脏数据，甚至伪造一个反向蜜罐，诱导防守方进入并误导溯源或者消耗防守方的精力，这也是防守方需要甄别和解决的问题，在演习行动的过程中，溯源与反溯源的故事一直在继续。

