实战攻防演习解读

护网定义：

护网行动是由公安机关组织的"网络实战攻防演习"。

护网规则：

1. 每支队伍 3-5 人组成
2. 明确目标系统
3. 不限攻击路径
4. 获取到目标系统的权限、数据即可得分
5. 禁止对目标实施破坏性操作，对目标系统关键区域操作需得到指挥部批准

护网攻防演习目的：

1. 及时发现并整改网络安全深层次问题隐患，检验并提升国家关键信息基础设施安全防护能力和应急处置能力
2. 进一步加强重点单位，社会力量与公安机关的协同配合和联合作战能力
3. 通过攻防实战，提高攻防双方技术对抗，决策指挥及应急处置能力

演练流程：

统筹阶段->自查阶段->演练阶段->实战阶段->总结阶段

实战攻防演习过程与内容

攻防演习流程

1. 准备阶段
   a) 防守方案编制
   b) 防守工作启动会
   c) 人员结构组织
   d) 目标系统梳理
   e) 网络架构检查
   f) 安全防护设备、厂商梳理了解
   g) APT 检测、流量分析、态势感知等安全检测设备梳理了解
2. 自查阶段
   a) 互联网资产扫描探测
   b) 漏洞扫描
   c) 渗透测试
   d) 安全风险检查
   e) 安全基线/配置核查
   f) 安全设备策略有效性检查
   g) 日志审计情况检查
   h) 重大活动或之前进行的安全评估结果复查
   i) 安全检测、防护设备补充完善
   j) 安全整改加固
3. 演练阶段
   a) 授权与备案
   b) 预演习攻击
   c) 预演习防护
   d) 问题分析总结

e) 安全整改与加固

4. 实战阶段
   a) 安全事件实时监测
   b) 安全事件分析
   c) 应急响应和决策处置
5. 总结阶段
   a) 针对演习结果，对在演习过程中还存在的脆弱点，开展整改工作，进一步提高目标系统的安全防护能力。

安全设备：

1. 边界隔离：网闸、下一代防火墙/UTM
2. 旁路检测：IDS/CS，网络审计、数据库审计、APT、全流量分析系统
3. 数据传输加密：VPN、加密机
4. WEB 服务器重点防护：服务器区前端部署 WAF、部署网页防篡改系统
5. 终端管控：EDR
6. 平台监控：安全管理平台
7. 其他设备：漏洞扫描、基线核查、威胁情报系统、蜜罐、攻防演练平台

实战攻防演习防守事件分类

1. 木马后门事件
   a) WEB Shell 脚本木马
   b) 远程控制
   c) 键盘记录
   d) Rootkit
2. 异常登录事件
   a) 应用系统和服务器中检测存在克隆账号
   b) 隐藏账号
   c) 存在未授权用户
   d) 异常时间
   e) 异常来源
3. 钓鱼邮件事件
   a) 邮箱附件
   b) 恶意代码
   c) 恶意链接
4. 漏洞攻击事件
   a) 攻击人员漏洞扫描探测发现漏洞后对漏洞点进行分析并深入利用，从存在漏洞系统获取敏感信息甚至拿下系统的控制权限
5. 暴力破解事件
   a) 对主机、终端设备、应用系统账号密码的暴力破解
   b) 通过收集信息，生成暴力破解字典
   c) 根据已泄露的密码进行撞库
6. 数据窃取事件
   a) 敏感信息爬取
   b) 利用任意文件读书漏洞窃据敏感文件

c) 利用 SQL 注入漏洞等窃取数据库敏感信息
d) 入侵成功后拖取数据库

7. 拒绝服务事件
   a) CC 攻击
   b) DOS 攻击
   c) DDOS 攻击
   d) DRDOS 攻击
   e) 遭受拒绝服务攻击，导致服务器宕机，网络阻塞
8. 事件分级
   a) 一级：演习目标被控制
   b) 二级：重要系统或设备被控制
   c) 三级：内网一般设备被控制
   d) 四级：DMZ 一般设备被控制
   e) 五级：DMZ 区设备遭到攻击或内网终端遭到攻击

实战攻防演习防守事件流转

1. 事件流转
   a) 按照扁平化指挥原则，通过建立护网行动即时通讯群组，统一进行调度
2. 事件处置方式
   a) 技术研判组报告事件情况
   b) 应急处置组开展应急处置工作
   c) 事件上报组进行通报
3. 木马后门事件处置方法
   a) 现针对出现木马后门设备进行断网隔离处理
   b) 同时将该设备日志进行设备留存分析入侵途径
   c) 随后对操作系统进行重新部署或病毒软件进行全盘查杀
4. 异常登录事件
   a) 先将相关账号下线并留存账号相关日志
   b) 随后针对问题账号采取修改口令或删除账号等方式进行处理
5. 钓鱼邮件事件
   a) 对邮件内链接仔细核查朔源
   b) 删除相关邮件
   c) 对收到钓鱼邮件的主机进行病毒查杀
6. 漏洞攻击事件
   a) 无补丁情况，采用“白名单”策略，对正常服务的路径进行加白
   b) 在主机配置强制访问控制策略，对进程、驱动纯资源进行枪支管理
   c) 有补丁情况，加强信息系统漏洞巡检和补丁修复，采取相应技术手段，检查漏洞修复情况，并督促整改
7. 暴力破解事件
   a) 针对产生暴力破解事件的相关攻击 IP 进行有效封锁
   b) 并关注出现被暴力破解事件系统运行状态
8. 数据窃取事件
   a) 组织技术研判组对失窃数据内容及范围进行研判，根据研判结果向相关业务

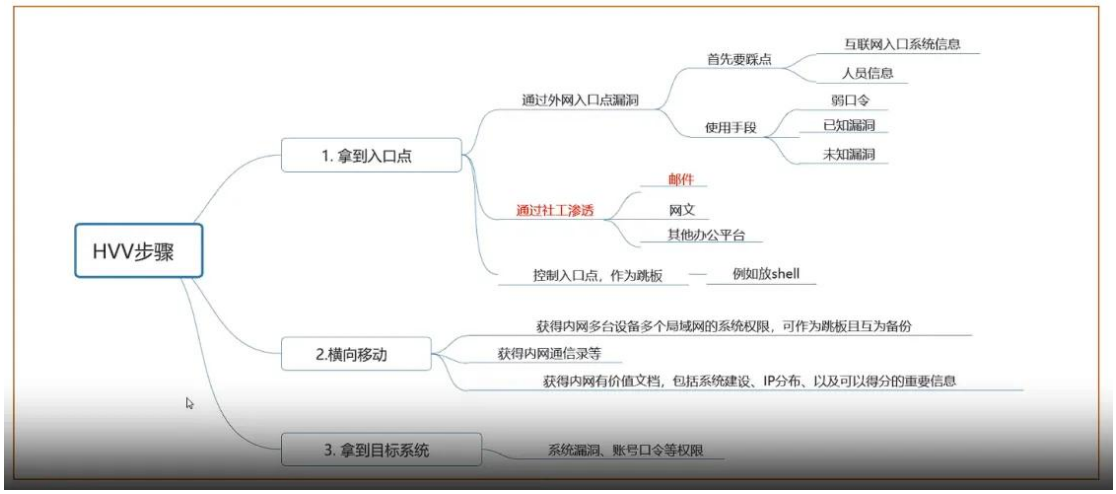
主管部门进行通报

b) 收到通报后在第一时间根据技术研判建议采取相关处置措施，防止事件升级

9. 拒绝服务事件
   a) 借助互联网出口运营商防护资源实现拒绝服务流量近源清晰
   b) 关注出现拒绝服务器攻击事件系统的运行状态

护网总结

1. 护网变化
   a) 社工攻击使用增加，花样更多
   b) 0day 漏洞利用成热门，得手后快速擦除痕迹
   c) 信息采集途径和范围增多，发现薄弱点并进行横向移动，寻找薄弱点作为突破口
   d) 攻击不受工作时间限制，非工作时间实施攻击增多
   e) 攻击者不断更换攻击 ip 和被攻击目标
2. 攻击手段
   a) 弱口令：有简单的突破方式为什么要选择复杂的
   b) 0day：本次护网过程中爆发多种 0day 漏洞，简单粗暴
   c) 钓鱼邮件：一旦成功，可能会获取比较重要内部敏感信息。
   d) 优先攻击集中管控类设备，如：堡垒机，终端管理，域控
   e) 分布式扫描：分散防守方注意力，获取有效信息
3. 攻击方式

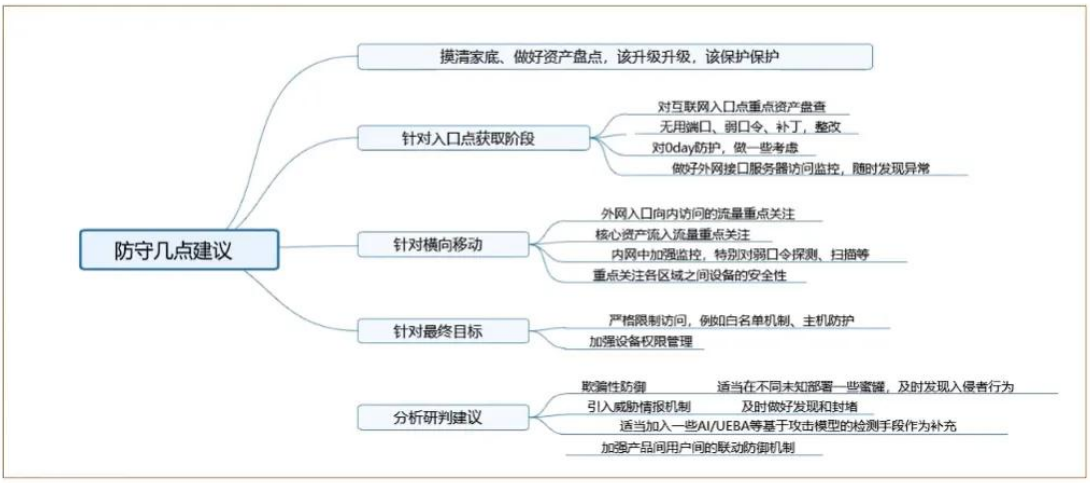


4. 防守手段
   a) 个体问题解决：分析原因，形成解决方案，解决个体问题
   b) 整体能力提升：横向借鉴，发散思维，关口前移
   c) 加强攻击对抗分析：持续细化攻击分析，借鉴 killchain,att&ck 提升智能威胁分析，积极防御能力
   d) 完善纵深防御体系：以"面向失效的设计"为原则，加强网络安全信息统筹机制，手段，平台建设
   e) 有效的安全管理与运营：加强安全意识的教育摸清家底，认清风险专业的安

全运营队伍加强应急指挥能力建设

5. 防守措施

基于攻击的防守应对措施



网络基础知识

常用协议分析

1. 常用协议分析—HTTP
   a) 定义：超文本传输协议，是一种用于分布式，协作式和超媒体信息系统的应用层协议，是万维网的数据通信的基础。
   b) 主要功能：包含了命令和传输信息，用于 web 访问，其他的 internet,内联网应用系统之间的通信
   c) 工作原理：http 协议采用了请求/响应模型。
      i. 客户端向服务器发送一个请求报文；
      ii. 请求报文包含：请求的方法，url,协议版本，请求头部和请求数据。
      iii. 响应的内容包括：协议的版本，成功或者错误代码，服务器信息，响应头部和响应数据。
   d) 协议的特点
      i. 无连接：服务器每次处理请求数为 1；客户端应答后断开连接
      ii. 无状态：协议对事务处理无记忆能；服务器发送信息后不会记录

2. 常用协议分析—DHCP
   a) 定义：是一个局域网的网络协议。是由服务器控制一段 IP 地址范围，客户机登陆服务器就可以自动获得服务器分配的 IP 地址和子网掩码
   b) 主要功能：集中的管理、分配的 IP 地址，提升网络环境中的主机动态获得 IP 地址、Gateway 地址、DNS 服务器地址等信息
   c) 工作原理：一种使网络管理员能够集中管理和自动分配 IP 网络地址的通信协议。
   d) 协议的特点
      i. 即插即用
      ii. 允许地址重用
      iii. 支持移动用户加入网络
      iv. 临时性

3. 常用协议分析—NAT
   a) 定义：NAT(网络地址转换）协议是将 ip 数据报头中的 ip 地址转换为另一个 ip 地址的过程
   b) 主要功能：NAT 不仅能解决 ip 地址不足的问题。
   c) 工作原理：
      i. 私有网络发送对 Internet 访问请求，并在组织出口位置部署网关
      ii. 报文离开私网时，源 IP 替换公网地址
      iii. 请求到达后，出口网关将目的地址替换为私网地址并返回请求
   d) 协议的特点
      i. 节省合法注册地址
      ii. 重叠地址提供解决方案
      iii. 提升连接到因特网的灵活性
      iv. 网络变化时避免重新编址

4. 常用协议分析—DNS
    a) 定义：DNS 全名域名解析协议，是互联网的一个服务。
    b) 主要功能：DNS 协议的主要功能是将域名解析为 IP。DNS 解析是互联网绝大多数应用的实际寻址方式。
    c) 工作原理：当 DNS 客户机需要查询程序中使用的名称时，它会查询本地 DNS 服务器来解析该名称。客户机发送的每条查询信息都包括 3 条信息，以指定服务器应回答的问题
    d) 协议的特点
        i. 每一个域名都对应一个唯一的 IP 地址
        ii. DNS 命名用于 internet 等 TCP/IP 网络中
        iii. DNS 是因特网的一项核心服务，它作为可以将域名和 IP 地址相互映射的一个分布式数据库。

5. 常用协议分析—TCP
    a) 定义：是一种面向连接的、可靠的、基于字节流的传输层通信协议
    b) 主要功能：确保数据的可靠传输
    c) 工作原理：三次握手
        i. 建立连接
        ii. 数据传输
        iii. 关闭连接
    d) 协议的特点
        i. 面向连接
        ii. 基于流的方式
        iii. 降低系统重传开销
        iv. 连接面向通信的两端点
        v. 可靠通信

6. 常用协议分析—UDP
    a) 定义：UDP 为应用程序提供一种无需建立连接就可以发送封装的 IP 数据库的方法
    b) 主要功能：作为无连接通信、并行性、使用底层的互联网协议、UDP 协议能够实现广播报文的中继转发。
    c) 工作原理：一种使网络管理员能够集中管理和自动分配 IP 网络地址的通信协议。
    d) 协议的特点
        i. 无连接性
        ii. 不可靠
        iii. 无阻塞控制
        iv. 面向报文

7. 常用协议分析—ARP
    a) 定义：地址解析协议（ARP）是根据 IP 地址获取物理地址的一个 TCP/IP 协议。
    b) 主要功能：使用 ARP，棵根据网络层 IP 数据包包头的 IP 地址信息解析出目标硬件地址（MAC 地址）信息，以保证通信的顺利进行。
    c) 工作原理：
        i. 第一步
            1. 主机的 ARP 缓冲区存在 ARP 列表
        ii. 第二步
            1. 网络上的主机接受到免费 ARP 报文时，更新自己的 ARP 缓冲区。将心的映射关系更新到自己的 ARP 表中
        iii. 第三步
            1. 主机发送报文时，检查 ARP 列表中是否有对应 IP 地址的目的主机的 MAC 地址
            2. 如果有则发送数据，如果没有就向本网段的所有主机发送 ARP 数据包
            3. 源主机收到 ARP 响应包后。就将目的主机的 ip 和 MAC 地址写入 ARP 列表
    d) 协议的特点
        i. 局域网络上的主机可以自主发送 ARP 应答消息，其他主机收到应答报文时不会检测该报文的真实性就会将其记入本机 ARP 缓存
        ii. ARP 命令可用于查询本机 ARP 缓存中 IP 地址和 MAC 地址的对应关系、添加或删除静态对应关系等

数据包加密

1. 数据包加密的简介
    a) 所谓数据加密（data encryption)技术是指将一个信息（或称明文，plain text)经过加密钥匙（encryptionkey)及加密函数转换，变成无意义的密文（cipher text),而接收方则将此密文经过解密函数，解密钥匙(decryption key)还原成明文。加密技术是网络安全技术的基石。
2. 数据加密类型-链路加密
    a) 对于在两个网络节点间的某一次通信链路，链路加密能为网上传输的数据提供安全保证
3. 数据加密类型-节点加密
    a) 节点加密要求报头和路由信息以明文形势传输，以便中间节点能得到如何处理消息的信息。安全性搞、密文传输
4. 数据加密类型-端到端加密
    a) 端到端加密允许数据在从源点到终点的传输过程中始终以密文形式存在
    b) 价格经济、可靠传输
5. 加密技术分类-分组密码
    a) 分组密码的数学模型是将明文消息编码表示后的数字序列，划分成长度为 n 的组，每组分别在密钥的控制下变换成等长的传输数字序列
    b) 常见分组密码

i. SM4、AES、RC4

6. 加密技术分类-公钥加密
   a) 公钥加密，也叫非对称加密，指的是由对应的一对唯一性密钥组成的加密方法
   b) 常见公钥密码
      i. RSA
      ii. Elgamal
      iii. 椭圆曲线
7. 加密技术分类-散列函数
   a) 散列函数即哈希函数，哈希函数指将哈希表中元素的关键键值射为元素存储位置的函数。
   b) 常见散列函数
      i. SHA1
      ii. MD5
      iii. SHA256

OSI 七层模型

1. 物理层
   a) 功能：定义物理设备的标准，主要对物理连接方式，电气特性，机械特性等制定统一标准，传输比特流。最小传输单位 bit.
   b) 对应协议：IEEE 802 1A、IEEE 802.2
2. 数据链路层
   a) 功能：主要是对物理层传输的比特流包装，检测保证数据传输的可靠性，将物理层接受的数据进行 mac 地址的封装和解封，也可以简单的理解为物理寻址。交换机就在该层工作，最小传输单位是帧。
   b) 对应协议：FDDI、Ethernet、Arpanet、PDN、SLIP、PPP、STP、HDLC、SDLC
3. 网络层
   a) 功能：控制子网的运行，图逻辑地址，分组传输，路由选择等。最小传输单位数据包（报）
   b) 对应协议：IP、ICMP、ARP、RARP、AKP、UUCP
4. 传输层
   a) 功能：义一些传输数据的协议和端口，传输协议同时进行流量控制，或是根据接收方接受数据的快慢程度，规定适当的发送速率，解决传输效率及能力的问题。
   b) 对应协议：TCP、UDP
5. 会话层
   a) 功能：负责在网络中的两节点建立，维持和终止通信。在这一层协议中。可以解决节点连接的协调和管理问题，包括通信连接的建立，保持会话过程通信连接的畅通，两节点之间的对话。
   b) 对应协议：SMTP、DNS
6. 表示层
   a) 功能：确保一个系统的应用层发送的消息可以被另一个系统的应用层读取，编码转换，数据解析，管理数据的解密和功能。

b) 对应协议：Telent、Rlogin、SNMP、Gopher

7. 应用层
   a) 功能：文件传输，文件管理，电子邮件信息处理等
   b) 对应协议：HTTP、TFTP、FTP、NFS、WAIS、SMTP

网络组成组件

1. 网络组成组件-节点
   a) 节点是具有网络地址（IP）的设备的统称，是计算机与网络的接口
   b) 主要功能：信息发送、接受和转发工作
   c) 常用设备：PC、Linux 服务器、与网络打印机等
2. 网络组成组件-服务器主机
   a) 就网络连接的方向来说，提供数据以“响应”给用户的主机，都可以被称为一台服务器
   b) 主要功能：提供数据响应给主机
   c) 常见设备：Yahoo 是 WWW 服务器
3. 网络组成组件-工作站或客户端
   a) 任何可以在计算机网络输入的设备可以是工作站，一般 PC 就是客户端
   b) 主要功能：主动发起连接
   c) 常见设备：任何访问服务器的设备
4. 网络组成组件-网络接口
   a) 网卡利用软件设计出来的网络接口，主要是提供网络地址（IP）的任务
   b) 主要功能：提供网络地址的任务
   c) 常见设备：网卡、主机
5. 网络组成组件-网卡
   a) 网卡是内置或者是外接在主机上面的一个设备，是局域网中连接计算机和传输介质的接口
   b) 主要功能：提供网络连接
   c) 工作地址：数据链路层
6. 网络组成组件-网络形态或拓扑
   a) 指各个节点在网络上面的链接方式，一般讲的是物理连接方式
   b) 主要概念：用传输介质互连各种设备的物理布局
   c) 相同拓扑：内部的物理接线、节点间距离可能会有不同
7. 网络组成组件-网关
   a) 网络又称网间连接器、协议转换器。网关在网络层以上，是复杂的网络互连设备，仅用于两个高层协议不同的网络互连
   b) 主要功能：实现网络互连
   c) 应用场景：广域网、局域网

文件排查

1. 文件分析

通常情况下，各种木马病毒等恶意程序，都会在计算机开机启动的过程中自启动，在windows 系统中可以通过以下三种方式查看开机启动项
1.利用操作系统中的启动菜单
2.利用系统配置 msconfig 查看
3.利用注册表 regedit 查看

2. 文件分析-temp 临时文件

temp 是指系统临时文件夹。在 windows 中，temp 文件夹主要分布在下面三个位置。
1. c:\windows\temp 系统公用;
2. c:\users\administra tor\local settings\temp;
3. c:iusers\administrator\appdata\localmicrosoft\windows\temporary internet
发现可疑文件，如何检验是否为恶意文件：将可疑文件上传到在线网站 https://www.virustotal.com 或微步云沙箱 https://s.threatbook.cn/进行查看，检查是否为恶意文件

3. 文件分析—时间属性分析

黑客拿下服务器后，极有可能会使用浏览器进行网站访问。我们可查看浏览器记录
进一步分析:
查看浏览器下载记录，看是否被使用下载恶意代码及文件
查看浏览记录是否有浏览恶意网站等
在 windows 系统下，文件的时间属性具有:
创建时间
修改时间
访问时间
如果修改时间早于创建时间，那么这个文件将会具有很大嫌疑。(中国菜刀可以做到这点)

4. 文件分析—最近文件打开分析

除此之外，还可以自己手动寻找:
根据文件夹内文件列表时间进行排序，查找可疑文件。

也可以搜索指定日期范围的文件，快速定位筛选

进程排查

1. 进程排查 1

进程排查
本地计算机与外部网络通信是建立在 tcp 或 udp 协议上通过端口（0-65535)进行通信，通常计算机被中木马后，一定会与外部网络通信，此时可通过网络连接状态，找到对应的进程 id.
关闭进程 id(关闭进程 id 即意味着关闭连接状态）

状态	含义
listening	表示监听表示这个端口正在开放可以提供服务
closing	表示关闭的表示端口人为或者防火墙使其关闭（也许服务被卸载）
time wait	表示正在等待连接就是你正在向该端口发送请求连接状态
established	表示是对方与你已经连接正在通信交换数据

2. 进程排查 2

查看所有的端口占用情况命令 netstat-ano
参数说明:
-a 显示所有网络连接，路由表和网络接口信息
-n 以数字形式显示地址和端口号
-o 显示与每个连接相关的所属进程 id
-r 显示路由表
-s 显示按协议统计信息，默认地，显示 ip

3. 进程排查 3

也可以采用以下方法:
1.先根据 netstat 定位出
2.再通过 tasklist 命令进行进程定位，
3.根据 wmicprocess 获取进程的全路径任务管理器定位到进程路径

系统信息排查

进程排查
　　启动项枚举
　　wmic startup list full
　　计划任务枚举
　　schtasks /query /fo table
　　/v (执行前先执行 chcp437)

windows 账号信息，如隐藏账号等【开始始】---[运行】---[compmgmt.msc] [本地用户和组】---[用户】
命令行方式：netuser,可直接收集用户信息，若需查看某个用户的详细信息，可使用命令--netuserusername;

系统信息排查
查看 systeminfo 信息，系统版本以及补丁信息
github 源码：　https://github.com/neargle/win-powerup-exp-index

工具排查

1. Processexplorer
2. PC Hunter
3. Microsoft network monitor

procexp 是常用的进程查看工具：
　　打开 procexp,进程标识颜色不同是用于区分进程状态和进程类型，进程开始启动时为绿色，结束时为红色
　　可对某个进程进行操作，右键单击即可

日志排查

windows 登录日志排查
主要分析安全日志，可以借助自带的筛选功能

可以把日志导出为文本格式，
然后使用 notepad+打开，
使用正则模式去匹配远程登录过的 ip 地址，

在界定事件日期范围的基础使用正则表达式匹配

渗透测试介绍

什么是渗透测试

是指从一个攻击者的角度来检查和审核个网络系统的安全性的过程。受信任的第三方通过模拟黑客可能使用的攻击手段对目标系统的安全性作出风险评估并针对目标系统所存在的风险给出安全修复建议的一个测试过程。

渗透测试的意义

通过渗透测试，使系统管理人员，系统开发人员及时了解到系统潜在的"安全危机"(薄弱点）,并及时进行修复，加强系统的安全性，避免不必要的损失

渗透测试方法

渗透测试是经过客户授权、采用客户授权、非破坏性质的手段帮助客户提供加固建议提升安全性
渗透测试方法：
黑盒测试：只知道被测试的目标
白盒测试：可以通过正常渠道向被测试单位取得各种资料
灰盒测试：介于两者之中，属于较为隐蔽的测试，只有被测试单位中的少数人知晓

渗透测试目标

根据测试目标分类：
操作系统渗透：windows linux solaris aix sco
数据库系统渗透: mysql Oracle mssql Informix sybase
应用系统渗透: asp jsp php
网络设备渗透: 防火墙 入侵检测系统

渗透测试攻击流程

渗透攻击流程：
明确目标 -> 信息收集->信息整理->信息分析->漏洞探测->漏洞验证->获取所需->形成报告

信息收集

信息收集:

- 域名与 IP
- 企业关系网
- 信息泄露
- 员工信息

风险利用

风险利用:

- 弱口令/通用口令
- 信息泄露
- Nday 漏洞
- 社工

渗透常用工具

渗透常见工具:

- Metasploit
- Wireshark
- Nmap
- Sqlmap
- Burpsuite
- goole/hacking
- 御剑

总体项目流程

总体项目流程

- 确认目标企业
- 签订保密协议
- 环境准备
- 开始攻击
- 成果输出

靶场

Django SQL注入漏洞(CVE-2022-28346)	tomcat后台getshell
HMS SQL注入(CVE-2022-25491)	ghostscript命令执行(CVE-2018-16509)
FineCMS XSS(CVE-2017-11629)	pbootcms1.21命令执行
GOCD任意文件读取(CVE-2021-43287)	Tomcat远程代码执行(CVE-2017-12615)
Jetty WEB-INF文件读取	PHPMailer远程命令执行
Webgrind任意文件读取漏洞	shiro-550反序列化(CVE-2016-4437)
SimplePHP任意文件读取	log4j2远程代码执行(CVE-2021-44228)
FFmpeg文件读取漏洞	Typecho反序列化漏洞getshell
jquery文件上传(CVE-2018-9207)	TomcatS2-001远程代码执行
禅道后台文件上传(CNVD-C-2020-121325)	Struts2S2-037命令执行漏洞
monstra 文件上传(CVE-2020-13384)	Apache Shiro授权绕过漏洞（CVE-2022-32532）
WordPress文件上传 稻草人企业站Getshell	Zabbix SAML SSO认证绕过漏洞 (CVE-2022-23131)
Twonkyserver目录遍历(CVE-2018-7171)	MetInfoV4越权漏洞
DVWA综合实验靶场	pikachu综合实验靶场

常见 Web 安全漏洞解析

SQL 注入

原理：

SQL 注入：通过把 SQL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令

危害：
(1)未经授权可以访问数据库中的数据，盗取用户的隐私以及个人信息，造成用户的信息泄露。
(2)对数据库的数据进行增加或删除操作(私自添加或删除管理员账号)
(3)篡改网页且发布违法信息(网站目录存在写入权限，写入网页木马)
(4)获取服务器最高权限(提权),远程控制服务器，安装后门，修改或控制操作系统

修复方案：
1、代码中的数据库操作采用 sql 语句预编译和绑定变量，避免直接使用参数值拼接字符串。可从根本上杜绝 SQL 注入；
2、在代码中对用户输入的数据进行严格过滤。对涉及到数据库的操作的所有参数，过滤危险字符串，如 select µunion sleep:(from where concat char 等敏感字符；
3、对所有传入 SQL 语句的变量进行处理，比如字符串变量单引号包裹并转义、数字类型变量进行强制类型转换等；
4、在网络层面，部署 Web 应用防火墙；
5、在数据库层面，对数据库操作进行监控；
6、做好数据库用户权限控制，比如对数据库配置使用最小权限原则，线上尽量不使用 root、sa 等高权限用户连接数据库。
核心：防御 SQL 注入的核心思想是对用户输入的数据进行严格的检查，并且对数据库的使用采用最小权限分配原则

Xpath 注入

原理：
XPath 注入攻击，是指利用 XPath 解析器的松散输入和容错特性，能够在 URL、表单或其它信息上附带恶意的 XPath 查询代码，以获得权限信息的访问权并更改这些信息。XPath 注入攻击是针对 Web 服务应用新的攻击方法，它允许攻击者在事先不知道 XPath 查询相关知识的情况下，通过 XPath 查询得到一个 XML 文档的完整内容。Xpath 注入攻击本质上和 SQL 注入攻击是类似的，都是输入一些恶意的查询等代码字符串，从而对网站进行攻击。

危害：
1、在 URL 及表单中提交恶意 XPath 代码，可获取到权限限制数据的访问权，并可修改这些数据
2、可通过此类漏洞查询获取到系统内部完整的 XML 文档内容；
3、逻辑以及认证被绕过，它不像数据库那样有各种权限，xml 没有各种权限的概念，正因为没有权限概念，因此利用 xpath 构造查询的时候整个数据库都会被用户读取。

修复方案：
1、数据提交到服务器上，在服务端正式处理这批数据之前，对提交数据的合法性进行验证；
2、检查提交的数据是否包含特殊字符，对特殊字符进行编码转换或替换、删除敏感字符或字符串，如过滤口“and or 等，像单双引号这类，可以对这类特殊字符进行编码转换或替换

XXE 注入

原理：
XXE 漏洞全称 XML External Entity Injection 即 xml 外部实体注入漏洞，XXE 漏洞发生在应用程序解析 XML 输入时，没有禁止外部实体的加载。

危害：
当允许引用外部实体时，通过构造恶意内容，导致可加载恶意外部文件和代码，造成任意文件读取、命令执行、内网端口扫描、攻击内网网站、发起 Dos 攻击等危害。

修复方案：
1.处理 XML 时禁止引用外部实体，比如 php 可调用 libxml_disable_entity_loader(true)、java 可调用 factory.setProperty(XMLInputFactory.SUPPORT_DTD,false)等；
2.如有用到 libxml2 库，检查其版本是否为 2.9.0 或以上版本，如版本较低建议升级；
3.尽量不要让用户直接提交 XML 代码，如果业务需要得做好过滤等处理。
4.限制用户输入数据类型

XSS 注入

原理：
XSS(Cross Site Scripting):即跨站脚本攻击，在页面中注入恶意的脚本代码，当受害者访问该页面时，恶意代码会在其浏览器上执行，XSS 不仅仅限于 JavaScript,还包括 flash 等其它脚本语言。
分类：
根据恶意代码是否存储在服务器中，XSS 可以分为存储型的 XSS 与反射型的 XSS。
反射型(非持久):主要用于将恶意代码附加到 URL 地址的参数中，常用于窃取客户端 cookie 信息和钓鱼欺骗。
存储型(持久型):攻击者将恶意代码注入到 Web 服务器中并保存起来，只要客户端访问了相应的页面就会受到攻击。

危害：
(1)窃取管理员帐号或 Cookie(恶意操纵后合数据)
(2)窃取用户的个人信息(登录帐号、冒充用户身份进行各种操作)
(3)网站挂马
(4)发送广告或者垃圾信息(利用 XSS 漏洞植入广告、发送垃圾信息)
(5)劫持用户(浏览器)会话，从而执行任意操作(非法转账、强制发表日志、电子邮件)
(6)进行大量的客户端攻击，如 DDoS 等
(7)获取客户端信息，如用户的浏览历史、真实 ip、开放端口等
(8)控制受害者机器向其他网站发起攻击

修复方案：
1)输入编码转义

对输入的数据进行 HTML 转义，使其不会识别为可执行脚本
(2) 增加过滤器 XssFilter
(3) web,xml 增加过滤器配置
(4)白名单过滤

CSRF 注入

原理：
CSRF(Cross-site request forgery):跨站请求伪造，是指利用受害者尚未失效的身份认证信息(cookie、会话等),诱骗其点击恶意链接或者访问包含攻击代码的页面，在受害人不知情的情况下以受害者的身份向(身份认证信息所对应的)服务器发送请求，从而完成非法操作(如转账、改密等)。

CSRF 与 XSS 的区别
XSS:跨站脚本攻击，在用户的浏览器中执行攻击者的脚本，来获得其 cookie 等信息。
CSRF:借用用户的身份，向 web server 发送请求，因为该请求不是用户本意，所以称为“跨站请求伪造”。

危害：
1.完成受害者所允许的任一状态改变的操作(邮件、发消息、购买商品、更新账号、注销、登录等)
2.修改受害者的网络配置(修改路由器 DNS、重置路由器密码)
3.获取用户的隐私数据、机密资料
4.用户财产安全
5.配合其他漏洞攻击
概括：盗用受害者身份，受害者能做什么,攻击者就能以受害者的身份做什么

修复方案：
1.验证 http referer 字段
2.在请求地址中添加 token 并验证
3.在 http 头中自定义属性并验证
4.其他防御方法
<1>关闭页面时要及时清除认证 cookie,对支持 tab 模式(新标签打开网页)的浏览器尤为重要。
<2> 尽量少用或不使用 request() 类变量，获取参数指定 request.form() 还是 request.querystring().(增加了攻击难度)。

命令执行

原理：
应用有时需要调用一些能执行系统命令或者代码的函数，当用户能控制这些函数中的参数时，就可以将系统命令或者执行系统命令的代码插入其中，从而造成命令执行攻击。
如在 PHP 中，System()、exec()、shell_exec()、passthru()、popen(、proc_popen()等函数可

以执行系统命令，攻击者控制函数参数，将恶意的系统命令拼接到正常命令中，造成命令执行攻击
命令执行主要是对输入的命令没有进行过滤，攻击者使用&、&&、、等命令拼接自己想要查看的信息的相关命令，攻击者的命令就会一起执行

危害：
(1)继承 Web 服务器程序权限--执行系统命令
(2)继承 Web 服务器权限--读取文件
(3)反弹 Shell
(4)控制整个网站
(5)控制整个服务器

修复方案：
(1)严格过滤用户输入的数据，禁止执行系统命令。
(2)使用动态函数之前，确保使用的函数是指定函数。
(3)在执行命令函数，对参数进行过滤，并对敏感字符进行转义。
(4)使用函数替换命令执行，并且参数值尽量使用引号包括

任意文件读取

原理：
通过传入参数，篡改要读取的文件路径，直接读取服务器上的任意文件，造成敏感信息泄露，甚至可以读取重要文件，比如与用户密码相关的文件进行进一步攻击。

危害：
直接读取服务器上的文件，权限够大的话可读取任意文件，危害包括但不限于：
1、网站源码泄露。
2、账号密码有关等敏感数据泄露。
3、可能利用 SSRF 并攻击内网系统。

修复方案：
1、正确使用文件读取或文件包含函数，禁止读取或包含非预期的文件；
2、对参数作处理，设置白名单或者过滤，防止通过/目录穿越进行绕过；
3、以最低权限原则运行网站等应用，限制可访问的目录。

文件包含

原理：
文件包含(File Inclusion)指当服务器开启 allow_url_include 选项时，就可以通过 php 的某些特性函数(include().require()和 include_once()利用 url 去动态包含文件，若没有对文件来源严格审查，导致任意文件读取或者任意命令执行。

文件包含漏洞分为本地文件包含漏洞与远程文件包含漏洞，远程文件包含漏洞是因为开启了 php 配置中的 allow_url_fopen 选项(选项开启之后，服务器允许包含一个远程的文件)。
1././php.ini 读取 ini 文件
2././phpinfo.php 读取指定文件

危害：
1、敏感信息泄露
2、获取 Webshell
3、任意命令执行(脚本被任意执行，导致网站被篡改)
3.1 篡改网站；
3.2 执行非法操作；
3.3 攻击其他网站；
文件包含漏洞是一种常见的依赖于脚本运行而影响 web 应用程序的漏洞。

修复方案：
设置白名单
过滤危险字符
设置文件目录
关闭危险配置 PHP 中的 allow url include 选项

任意文件上传

原理：
文件上传漏洞(File Upload):对上传文件的类型、内容没有进行严格的过滤、检查，攻击者上传木马获取服务器的 webshell 权限；上传一个 webshell 到一个 Web 可访问的目录上，恶意文件传递给解释器去执行后，可以在服务器上执行恶意代码，进行数据库执行、服务器文件管理，服务器命令执行等恶意操作。Apache、Tomcat、Nginx 等都曝出过文件上传漏洞。

危害：
(1)网站被控制(文件增删改查，执行命令，链接数据库)
(2)导致服务器沦陷(服务器长久未更新--利用 exp 提权)
(3)服务器相关服务沦陷

修复方案：
(1)上传文件的存储目录不给执行权限
(2)文件后缀白名单，注意 0x00 截断攻击(PHP 更新到最新版本)
(3)不能有本地文件包含漏洞(includedama.jpg)
(4)及时更新 web 应用软件避免解析漏洞攻击

弱口令

原理：
一段很容易猜测到的简单密码例如 123456、13579、qwerasdf 等，还包括使用与用户相关的名字、生日。例如张三，生于 1999.10.10 日于是他设置的密码为 zhangsan10.10、zs10.10、1999.10.10 这些都是一些很容易被信息搜集之后猜测到的密码

危害：
直接获得系统控制权限

修复方案：
对于客户：
1.针对管理人员，应强制其账号密码强度必须达到一定的级别
2.建议密码长度不少于 8 位，且密码中至少包含数字、字母和符号
3.不同网站应使用不同的密码，以免遭受“撞库攻击”
4.避免使用生日，姓名等信息做密码，远离社工危害
对于修复人员：
1.建议规定用户在设置密码时的长度和密码的必需使用大小写加数字组合的形式，严禁使用空口令
2.禁止用户使用与用户名一致的密码

路径遍历

原理：
web 应用通过传入参数，拼接查看的网站目录，攻击者通过篡改要读取的目录路径，直接读取或者查看服务器上的任意目录。应用系统在处理下载文件时未对文件进行过滤。
系统后台程序中如果不能正确地过滤客户端提交的./和/之类的目录跳转符，攻击者可以利用路径回溯符*/跳出程序本身的限制目录实现上传、下载、删除、读取任意文件等。例如 Web 应用源码目录、Web 应用配置文件、敏感的系统文件(/etc/passwd、/etc/paswd)等

危害：
直接读取服务器上的目录，权限够大的话可读取任意目录，危害包括但不限于：
1、网站源码路径信息泄露；
2、可查看网站任意文件的路径，尝试通过外网进行 url 访问；
3、发现可利用的网站配置文件，或者 webshell 等。
一个正常的 Web 功能请求：
http://www.test com/get-files.jsp?file=report.pdf
如果 Web 应用存在路径遍历漏洞，则攻击者可以构造以下请求服务器敏感文件：
http://www.test com/get-files.isp?f

修复方案：
1.正确使用文件读取或文件包含函数，禁止读取或包含非预期的文件；
2.对参数作处理，设置白名单或者过滤，防止通过/目录穿越进行绕过；

3.以最低权限原则运行网站等应用，限制可访问的目录。

越权

原理：

越权访问漏洞(Broken Access Control)指绕过正常的权限控制，可以实现非法访问无权限资源的一种漏洞。常见的有垂直(纵向)越权漏洞和水平(横向)越权漏洞。

水平越权漏洞：是一种基于数据的访问控制”设计缺陷引起的漏洞，是由于服务器端在接收到请求数据进行操作时，没有判断被请求数据的归属，而导致的越权数据访问漏洞。

垂直越权漏洞：也称权限提升漏洞，是一种基于 URL 的访问控制”设计缺陷引起的漏洞，由于应用没有做权限控制或仅依赖菜单做权限控制，恶意用户只要通过 URL 就可以直接访问或控制其他角色所有的数据或页面达到权限提升的目的。

危害：

1.泄露敏感信息：攻击者可以通过越权漏洞获取到未被授权的敏感信息，比如用户信息、交易记录等。

2.篡改数据：攻击者可以通过越权漏洞修改系统中的数据，比如更改账户余额、修改订单状态等。

3.执行非法操作：攻击者可以通过越权漏洞执行系统中未被授权的操作，比如删除数据、创建用户等。

修复方案：

在进行用户操作时，从 session 或者 Token 获取用户 id,将传入的参数与用户的身份做绑定校验。以下代码与上述功能相同，但是附加了一个当前授权用户的查询限制。

对于垂直越权访问需要严格进行权限控制，即在调用相关功能之前，验证当前用户身份是否有权限调用相关功能(推荐使用过滤器)。

后端程序中禁止直接使用前端传递表示权限的字段，当前用户身份权限信息必须从可信区域中获取，从如 session 或 token 中获取用户信息后再获取权限信息，不使用前端上送的权限字段来判定当前用户的权限信息。在应用程序中，一般使用 session 或者 cookie 记录用户是否登录，以及该用户的权限，我们可以通过全局过滤器来检测用户是否登录，是否对资源具有访问权限。

蓝队防守技术

总体概述

定义：
指借助安全设备(WAF、IDS、IPS 等)开展安全事件实时监测，对发现的攻击行为进行确认，详细记录攻击相关数据，为后续处置工作开展提供信息的一种工作。

工作内容：
负责安全事件分析监测，策略调整，状态巡检，协助封堵；负责保障事件的上报，统计汇总，定期形成工作报告/总结报告等

重要性：
整个防护体系的最前沿，安全事件的第一发现者
事件分析的前提，后续流程运转的基础
快速遏制攻击行为，可调整策略阻挡攻击

工作职责和模式

岗位职责：
安全事件的分析监测
1. 从行内的背景流量 SQL 注入攻击中，甄别出真实攻击，第一时间向上报送，完成处置
2. 演练刚开启前期，大量扫描探测行为，及时　2.新出现的安全漏洞针对性增加规则封禁可有效阻断攻击方对资产信息的收集
3. 从多条告警中形成对攻击者的画像

安全事件的策略调整
1.根据行内的业务和日常告警日志，优化整体策略
2.新出现的安全漏洞针对性增加规则
3.发现攻击者成功利用某种漏洞，针对漏洞优化规则

事件上报一般性原则(重点)
1.上报事件查 IP 归属地
2.IP 上报不重复
3.重点关注事件响应动作为 PASS 的
4.攻击频率高要上报
5.漏洞利用类要重点上报
6.低危事件大量扫描必上报(批量)
7.国外 IP 要上报处置

8.确定恶意攻击必上报
9.一个 IP 对多个资产进行攻击要上报
10.高危事件重点关注(敏感文件访问、文件上传、或者 webshell 连接等)
11.监控事件遵循原则：先看相应动作，再看详细报文分析，再看 IP

安全设备

安全检测类：IDS、IPS、APT、邮件管理
安全防护类：防火墙、WAF、网页防篡改、抗 DDOS
安全分析类：入侵分析、流量分析
安全管理/展示类：安全运营平台、态势感知

WAF

特点：
1. 基于算法引擎和特征引擎双引擎检测方法
2. 针对 Web 服务器进行 HTTP/HTTPS 流量检测和防御。

防护场景：
恶意扫描防护；漏洞利用防护；暴力破解防护；SQL 注入防护；XSS 注入防护；
敏感信息泄露防护；Web 网站应急保障

WAF 日志分析
一键请求头信息提取：XSS 防护、SQL 注入防护、事件引擎在首页上报了事件，可点击事件详情支持请求头信息提取，便于分析报文。

Web 应用漏洞事件分析：
合理利用互联网资源 拿到请求头信息去网上查一下
根据事件名称搜集漏洞相关信息，初步了解攻击原理。
提取事件请求头信息和原始报文。
根据用户环境分析是否真实攻击。

IPS

天清入侵防御系统是网络型入侵防御产品，其主要特点有
1.深层防御、精确阻断
2.可及时准确发现入侵攻击行为

3.实时精确阻断
4.主动高效

IPS 日志分析
合理使用日志过滤功能，提高事件分析的效率，常用过滤动作：pass
点击事件右侧内容可以根据报文详细信息进一步分析攻击行为。
针对攻击事件存在误报可能性，具体可通过安域 IP 列表查询。

WAF-联动防护

TAR 联动
TAR 发现安全攻击通过 API 接口下发
封堵策略至 WAF 设备进行源 IP 封堵

全流联动
联动 NFT 取证，还原攻击过程

蜜罐联动
WAF 将攻击流量引流至蜜罐产品进行攻击捕获及反制

威胁情报联动
挖掘攻击者信息

IP:NFT 的设备 IP
协议：NFT 设备的访问方式
端口：NFT 设备的端口
外部系统 ID:在 NFT 设备上配置用于外部联动设备的标识
外部用户 ID:在 NFT 设备上配置，用于外部联动设备的用户访问
Appkey:NFT 上配置生成
Apptoken:NFT 上配置生成
时间偏移：获取镜像流量的时间偏移量

产品联动→业务审计联动→外联策略联动
TAR 下发封堵策略至全局访问控制黑名单

IPS-产品联动

场景
通过 restful 接收下发给 IPS 的阻断策略，可以与 SOC、TAR、IDS 联动实现自动阻断

配置

启用产品联动

监视器：显示给 IPS 下发过策略且未到老化时间的设备

联动日志：记录给联动操作，添加、查看、删除策略操作

阻断日志：记录命中联动策略的五元组信息

IPS-NFT 联动

全流联动，发现攻击直接下载原始数据包

填写 NFT 地址，协议为 https,端口为 41110 不可修改，外部系统 ID、外部用户 ID、Appkey、App token 从 NFT 用户管理获取填写，时间偏离即取多长时间内的五元组的数据包

安全设备日志分析

基础知识

常见编码：URL 编码、Base64 编码、16 进制编码、Unicode 编码

HOST:主机名，日志中源 IP 地址请求的域名，例如：www.baidu.com 中的 www

URL:统一资源定位符，用于表示互联网上标准资源的地址。例如：/cms/login.jsp

REFERER:引用，Referer 是 HTTP 协议消息头的一部分，当浏览器向 web 服务器发送请求的时候，一般会带上 Referer,告诉服务器我是从哪个页面链接过来的，服务器基此可以获得一些信息用于处理

告警日志类型

业务误报：由于开发代码不规范，或者安全设备拦截策略引起的误报

大量请求

触发漏洞类型类似

触发时间有一定规律

扫描器请求：僵尸网络批量全网扫描引发的攻击流量告警。或扫描器扫描引发的无意义的漏洞

大量请求、攻击频率高

攻击请求无明显特征征

攻击请求与实际环境有违背

攻击特征比较明显

告警真实攻击：由真实攻击者引发的攻击告警

攻击频率较低

攻击请求与实际环境相结合

攻击请求偏深度利用

异常属性

分析 ip 属于国内外云服务商应特别注意

攻击方有很多扫描器和 C2 服务器都部署在个人 vps 上以方便一键使用，这些 vps 有可能是个人购买的云服务器

告警日志分析

源地址：确认攻击来源

目的地址：判断被攻击目标

端口：源端口、目的端口

事件名称：结合安全设备分析请求信息

时间：确定可能受攻击的时间

规则 ID:匹配攻击规则库里的事件 ID
发生次数：确认攻击次数，对攻击类型进行判断分析

注意内容
请求的 url 过长
请求数据过长：过长的数据包可能绕过检测
异常请求数据
请求方式不合规

WEB 日志

常见 web 服务器
nginx 日志
a)默认储存位置：Windows:/Nginx/logs/;Linux:/var/log/apache2
b)日志文件：一般分为 access log 和 error log 两种
IIS 日志
a)默认储存位置：Windows:C:/WINDOWS/system32/LogFiles
apache 日志
a)默认储存位置：windows:/apache/logs;Linux:/var/log/apache
b)日志文件：一般分为 access log 和 error log 两种
tomcat 日志
a)日志文件：一般分为 catalina.out、localhost、managere

记录访问服务器的 ip 地址
记录浏览者访问的时间
记录浏览者访问的资源
记录访问服务器的工具

请求
请求类型：常见的请求类型主要是 GET/POST/HEAD
请求资源：请求的时访问资源的 URL
请求使用协议：显示 HTTP 协议和版本信息，通常是 HTTP/1.0 或 HTP/1.1

linux 日志查看命令
查看 access.log 日志出现的 IP: cat access.log | awk '{print$1}'

查看 access.log 日志出现 IP 次数： cat access.log | awk '{print$1}'| sort|uniq -c|sort -sn

查看 access.log 日志出现的所有 IP： cat access.log | awk '{print$1}'| sort|uniq -c|sort -sn|wc -|

查看 access.log 日志访问指定时间后(之间)的日志：

Cat access.log |awk '$5>="[28/Jun/2019:01:16:59"&&$5<="[28/Jun/2019:01:18:59"{print$5}'

查看指定资源的日志

cat access.log | awk '{print $10}' |grep /mobile/static/ |sortlunig -clsort -rn|more

主机日志分析

windows 日志类别

系统日志：系统日志主要是记录了系统组件产生的事件。系统日志主要记录的信息包括驱动程序产生的信息、系统组件产生的信息和应用程序崩溃的信息以及一些数据丢失情况的信息。

默认存放地址 C:\Windows\System32\winevt\Logs\System.evtx

应用程序日志：

一般指的的是微软开发的应用程序，第三发开发的基于系统的应用程序如果使用日志记录的函数，则这个应用程序将可以通过事件查看器查看其日志信息。

默认存放地址 C:\Windows\System32\winevt\Logs\Application.evtx

查看日志的重点内容

查看登录日志中暴力破解痕迹

默认路径：C:\Windows\System32\winevt\Logs\Security.evtx

目的：攻击者如果通过暴力破解入侵系统，不论是否成功，都会在日志中留下记录

常见的事件 ID 及含义

4624：用户登录成功

4625：用户登陆失败

查看账号管理日志中新增以及修改账号

默认路径：C:\Windows\System32\winevt\Logs\Security.evtx

目的：攻击者如果攻陷一台服务器后，为了方便后续访问，会创建后门账号并隐藏账号

常见的事件 ID 及含义

4727,4737,4739,4762，表示当用户组发生添加、删除时或组内添加成员时生成该事件。

查看远程桌面登录日志中的登录痕迹

默认路径：应用程序和服务日志->Microsoft->Windows->TerminalServices-RemoteConnectionManager->Operational

目的：攻击者如果建立建立账号后，会通过远程连接进入受害主机，此时的登录日志会记录到当前日志中

常见的事件 ID 及含义

1149：用户认证成功