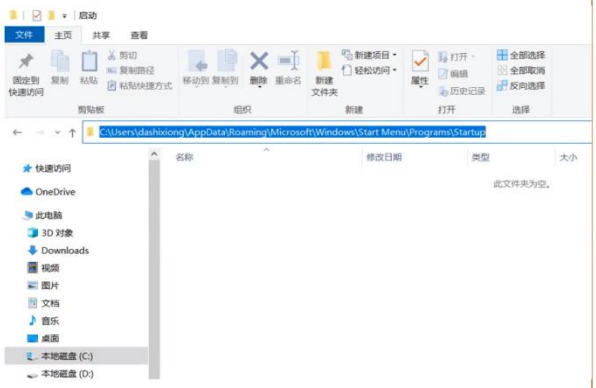
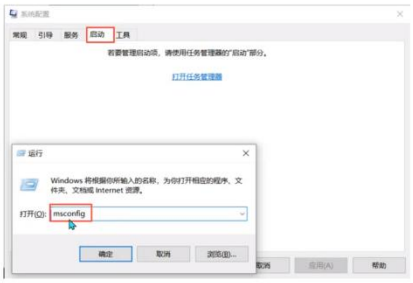
文件分析--开机启动文件

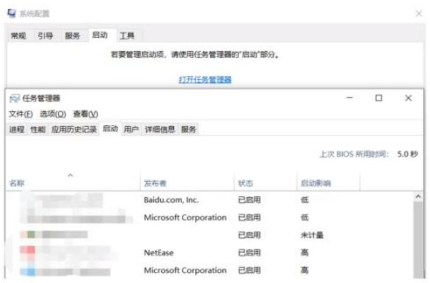
一、利用操作系统中的启动菜单
【win+R】---
【C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup】



文件分析--开机启动文件

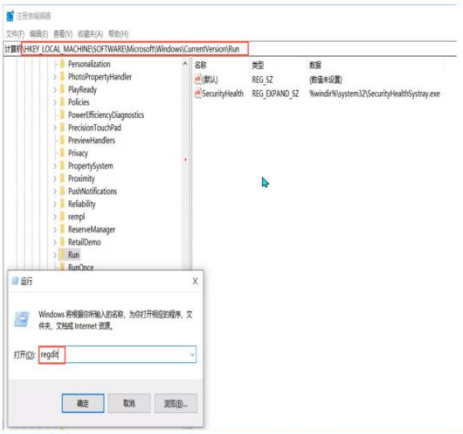
二、利用系统配置msconfig （ms代表微软，config代表配置）【win+R】---【msconfig】，查看是否存在可疑启动项





文件分析--开机启动文件

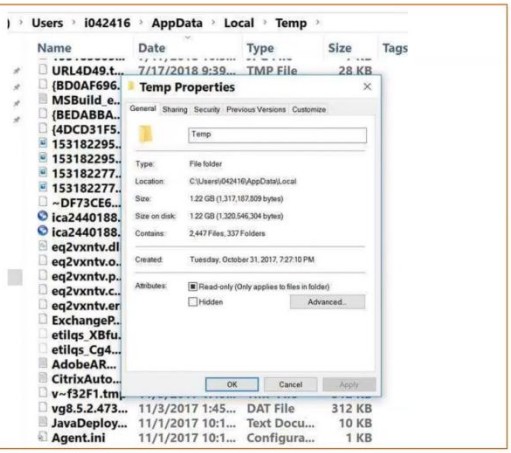
三、利用注册表regedit
【win+R】---【regedit】打开注册表，查看开机启动项是否正常。检查右侧是否有启动异常的项目，如有请删除，并建议安装杀毒软件进行病毒查杀，清除残留病毒或木马

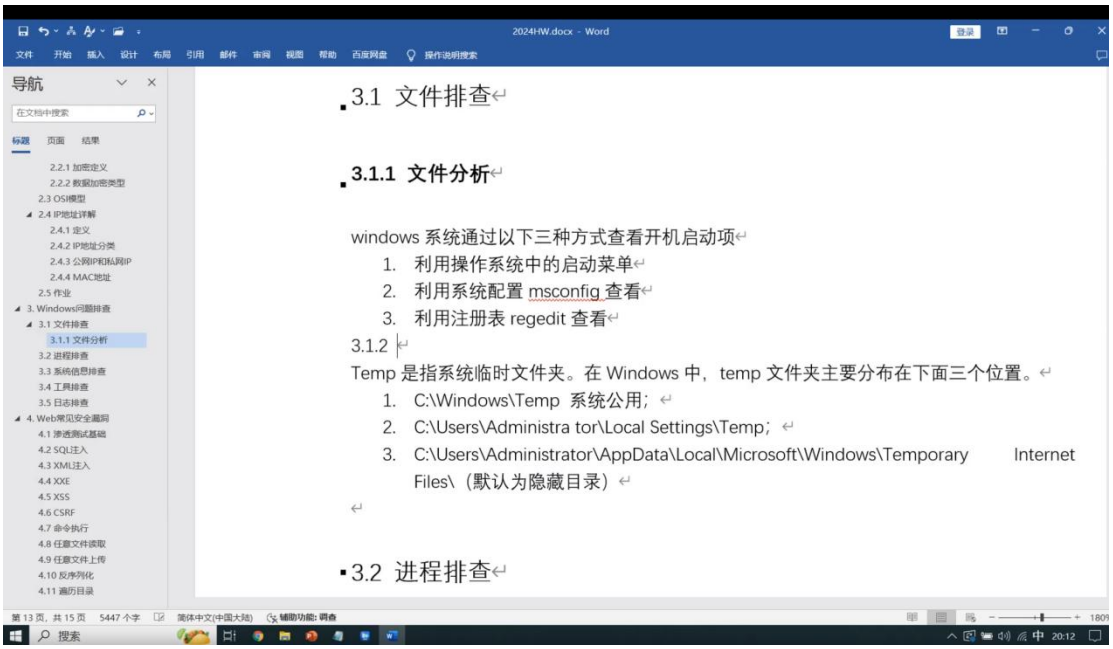


文件分析-- temp临时文件

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:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\（默认为隐藏目录）

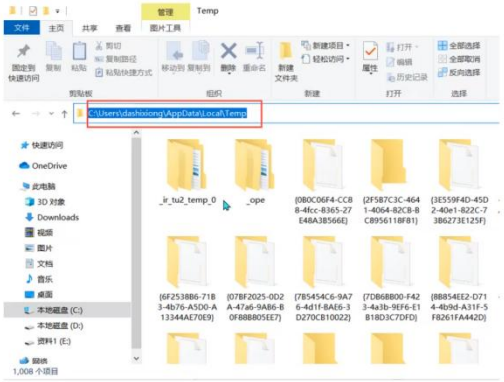




文件分析-- temp临时文件

【win+E】
【C:\Users\Administrator\AppData\Local\Temp】

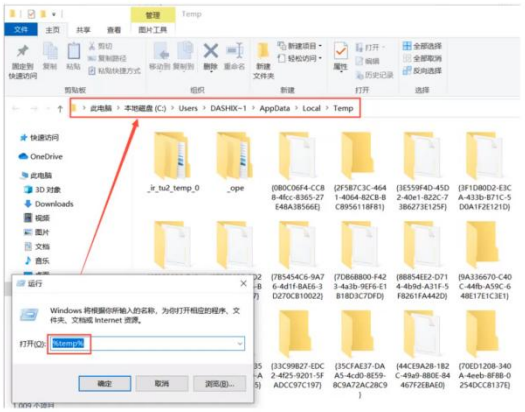
查看temp文件夹下的PE文件(exe , dll , sys) , 查看是否有特别大的tmp文件



文件分析-- temp临时文件

【win+R】---【%temp%】

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



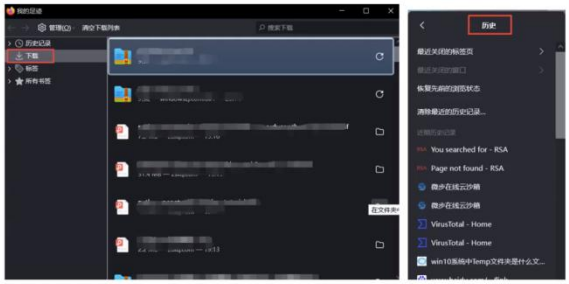
文件分析--temp临时文件

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。

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



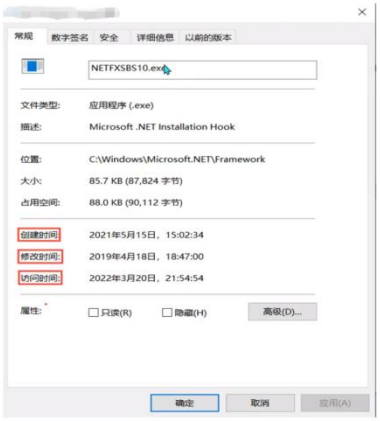
文件分析--时间属性分析

在Windows系统下，文件属性的时间属性具有：

- 创建时间
- 修改时间
- 访问时间

如果修改时间要早于创建时间那么这个文件存在很大可疑。（中国菜刀等工具可修改）

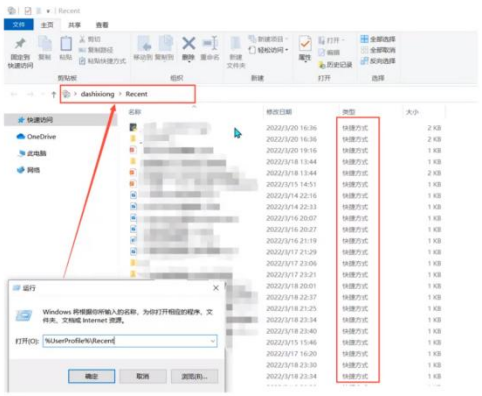
选中文件【右键】---【属性】



文件分析--最近打开文件分析

Windows系统会记录系统中最近打开使用文件的快捷方式，通过以下方法可查看最近打开的文件：

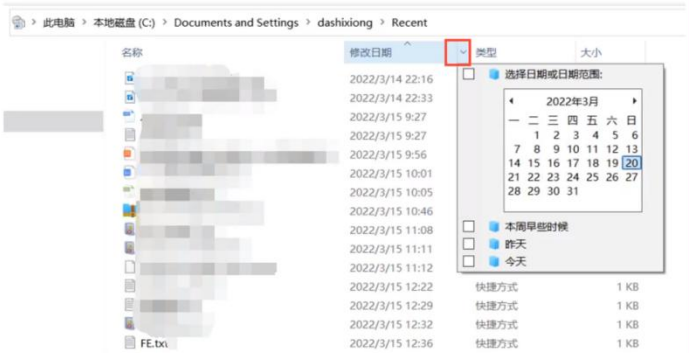
- 【win+E】---【C:\Documents and Settings\Administrator\Recent】
- 【win+E】---【C:\Users\Administrator\Recent】
- 【win+R】---【%UserProfile%\Recent】



文件分析-最近打开文件分析

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



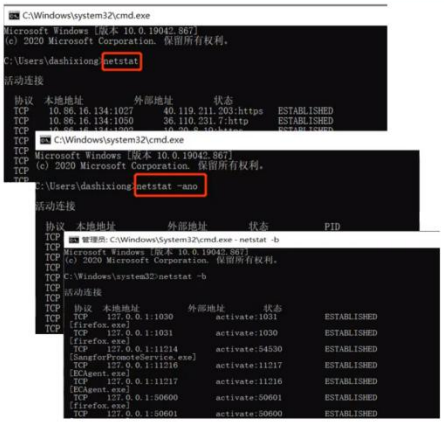
进程排查

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

进程排查

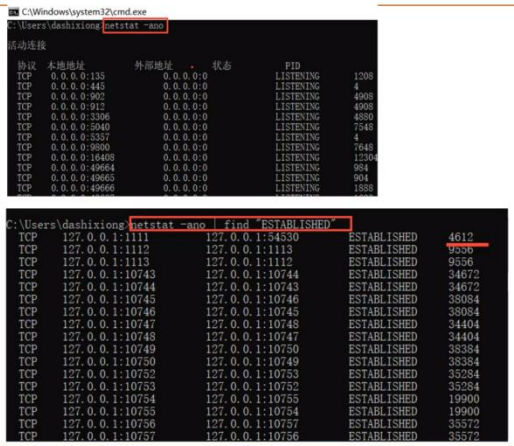
- ✓ 查看所有的端口占用情况命令netstat -ano
- ✓ 参数说明：
  - -a 显示所有网络连接、 路由表和网络接口信息
  - -n 以数字形式显示地址和端口号
  - -o 显示与每个连接相关的所属进程 ID
  - -r 显示路由表
  - -s 显示按协议统计信息、 默认地、 显示IP



进程排查

记录一次进程排查：

1. 查看所有的端口占用情况命令netstat -ano
2. 查看端口中状态为established的所有进程
   netstat -ano | find "ESTABLISHED"
3. 发现”可疑进程”定位PID值为4612



进程排查

查看PID对应的进程命令：tasklist | findstr "XXX"

- 杀死（结束）该“可疑进程“：taskkill /f /t /im SangforPromoteService.exe

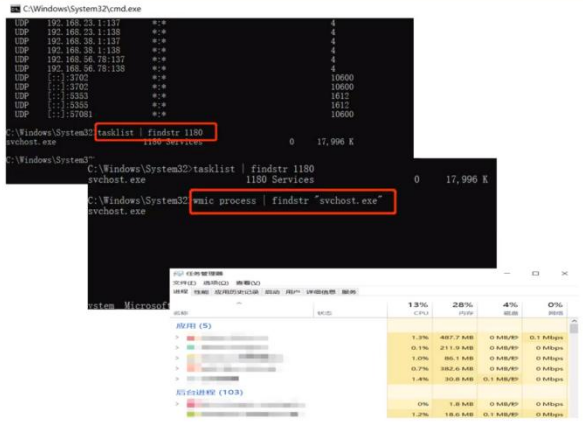
```
C:\Users\dashixiong>tasklist|findstr "4612"
SangforPromoteService.exe      4612 Services                   0     10,264 K

C:\Users\dashixiong>
```

进程排查

也可以采用以下方法：

1. 先根据netstat定位出pid
2. 再通过tasklist命令进行进程定位，
3. 根据wmic process 获取进程的全路径任务管理器定位到进程路径



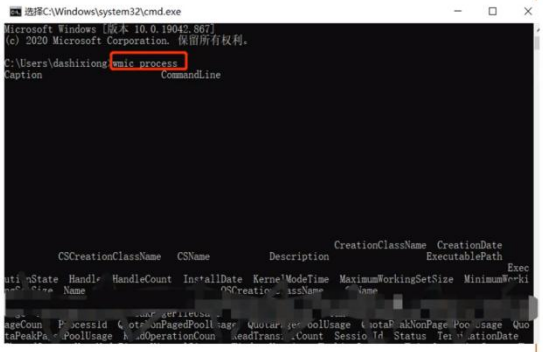
进程排查

✓ 查询进程

- wmic process （带有cmdline）
- wmic process list brief
- wmic process where name= “xxxx” get executablepath

✓ 删除进程

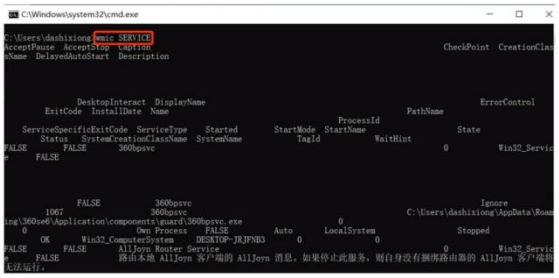
- wmic process where processid="2345" delete



进程排查

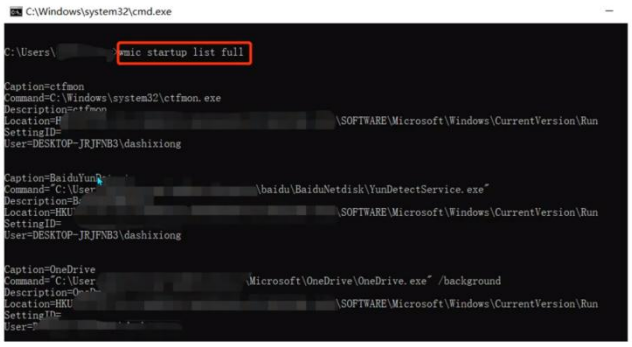
✓ 查询服务

- wmic SERVICE （涵盖服务关联所有信息）
- wmic SERVICE where caption(name)=” XXX” call stopservice
- wmic SERVICE where caption(name)= “XXX" call delete



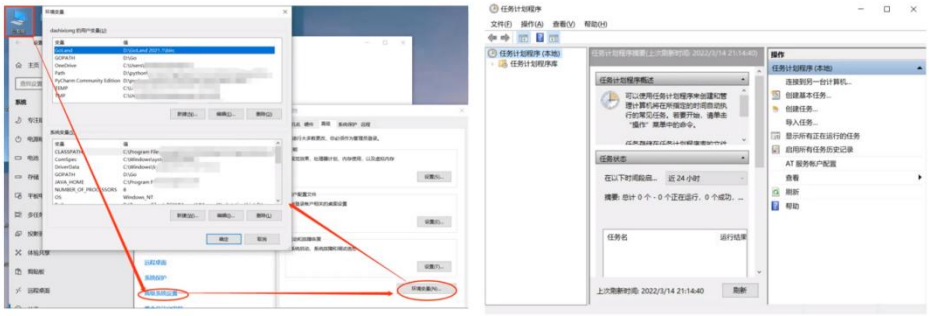
进程排查

- ✓ 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chcp 437）



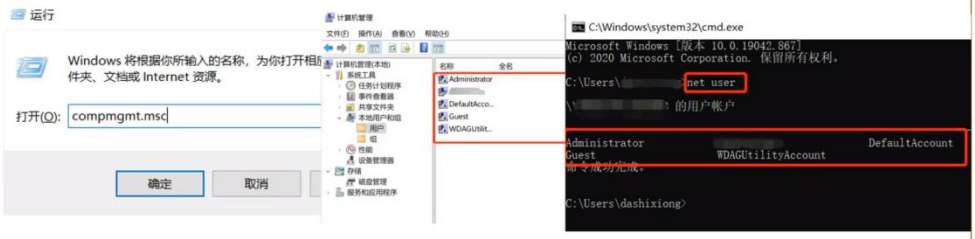
系统信息排查

- ✓ 查看环境变量的设置【我的电脑】---【属性】---【高级系统设置】---【高级】---【环境变量】
- ✓ Windows 计划任务【程序】---【附件】---【系统工具】---【任务计划程序】



系统信息排查

- ✓ Windows帐号信息， 如隐藏帐号等【开始】 ---【运行】 ---【compmgmt.msc】 ---【本地用户和组】 ---【用户】 (用户名以$结尾的为隐藏用户)
- ✓ 命令行方式： net user， 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--- net user username;

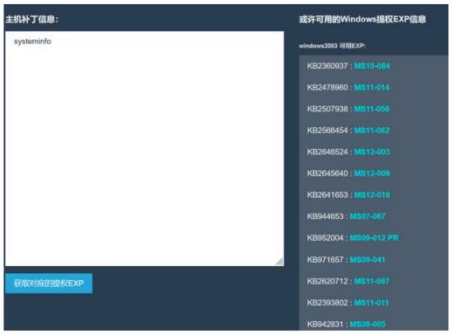


系统信息排查

- ✓ 查看当前系统用户的会话使用➜ query user 查看当前系统的会话， 比如查看是否有人使用远程终端登录服务器
- ✓ logoff 踢出该用户

系统信息排查

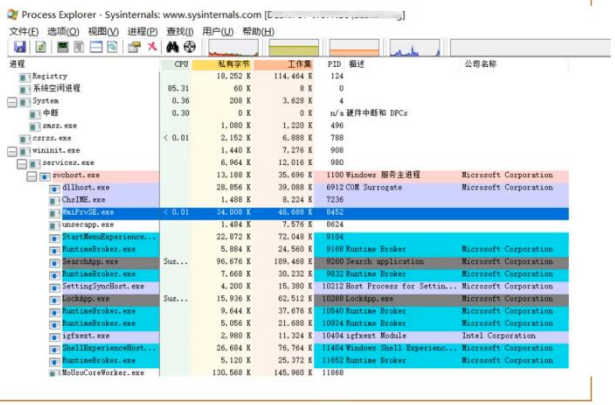
- ✓ 查看systeminfo信息， 系统版本以及补丁信息
- ✓ Github源码： https://github.com/neargle/win-powerup-exp-index



工具排查

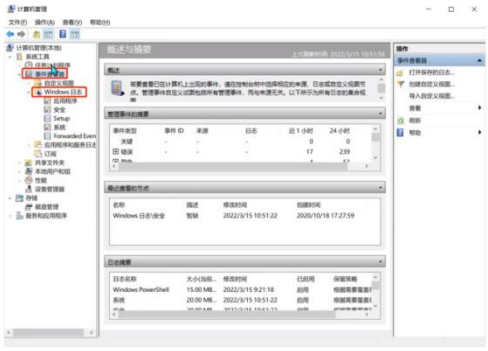
Procexp是常用的进程查看工具：

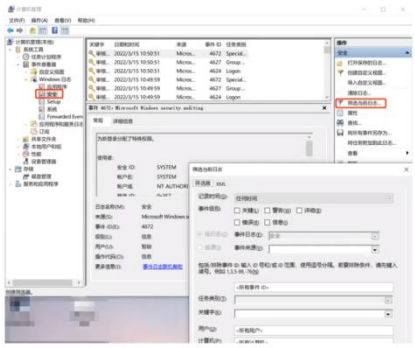
- ➢ 打开procexp，进程标识颜色不同是用于区分进程状态和进程类型， 进程开始启动时为绿色， 结束时为红色
- ➢ 可对某个进程进行操作， 右键单击即可



日志排查

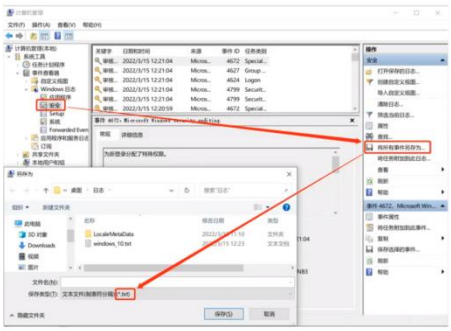
- ✓ Windows登录日志排查
- ✓ 主要分析安全日志， 可以借助自带的筛选功能





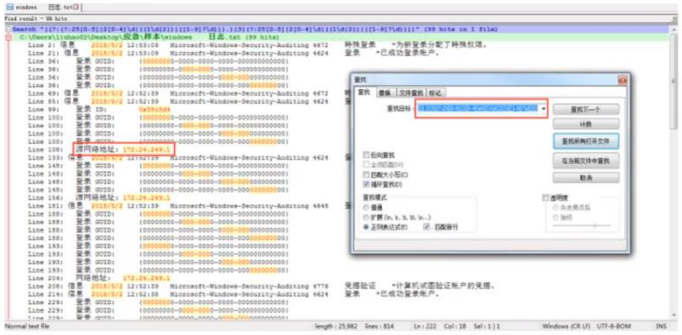
日志排查

- ✓ 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



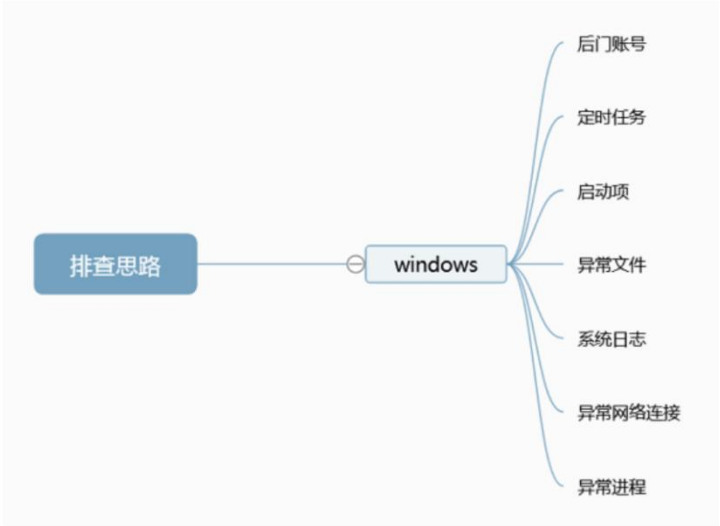
日志排查

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



一、Windows 问题排查

排查思路



应急响应（Incident Response Service，IRS）是当企业系统遭受病毒传播、网络攻击、黑客入侵等安全事件导致信息业务中断、系统宕机、网络瘫痪，数据丢失、企业声誉受损，并对组织和业务运行产生直接或间接的负面影响时，急需第一时间进行处理，使企业的网络信息系统在最短时间内恢复正常工作，同时分析入侵原因、还原入侵过程、评估业务损失、溯源黑客取证并提出解决方案和防范措施，减少企业因黑客带来的相关损失。本文主要讨论 windows 被入侵后的排查思路。

windows 入侵排查利器：火绒剑

0x01 分析入侵过程

攻击者入侵 windows 系统往往从弱口令、系统漏洞以及服务漏洞进行切入，获得一个普通的系统权限，再经过提权后进行创建启动项、修改注册表、植入病毒和木马等一系列操作，从而维持对目标主机的控制权。而与此同时操作系统也会出现异常，包括账户、端口、进程、网络、启动、服务、任务以及文件等，系统运维人员可以根据以上异常情况来知道攻击者从何处入侵、攻击者以何种方式入侵以及攻击者在入侵后做了什么这几个问题的答案，从而为之后的系统加固、安全防护提供针对性建议。

暴力破解：针对系统有包括 rdp、ssh、telnet 等，针对服务有包括 mysql、ftp 等，一般可以通过超级弱口令工具、hydra 进行爆破

漏洞利用：通过系统、服务的漏洞进行攻击，如永恒之蓝、Redis 未授权访问等

流量攻击：主要是对目标机器进行 dos 攻击，从而导致服务器瘫痪

木马控制：主要分为 webshell 和 PC 木马，webshell 是存在于网站应用中，而 PC 木马是进入系统进行植入。目的都是对操作系统进行持久控制

病毒感染：主要分挖矿病毒、蠕虫病毒、勒索病毒等，植入病毒后往往会影响受感染电脑的正常运作，或是被控制而不自知，电脑正常运作仅盗窃资料、或者被利用做其他用途等用户非自发引导的行为

0x02 入侵排查方法

一、检查系统账号安全

攻击者面对 windows 系统会先从用户密码入手，首先是通过 rdp 服务对 Administrator、Guest 等默认账户的口令爆破，如果爆破没结果的话会固定密码，对用户账号进行爆破，再之后加入还是失败的话就是社工生成账号、密码字典，运气好那么就可以直接登录到管理员账号。在拿到系统权限后，权限维持则是必不可少的一步，创造一个新的管理账号方便后期登录查看就是一个不错的方法，当然为了增加隐蔽性该账号可以是影子账户。根据这几方面，检查看系统账号时可以重点关注弱口令、可疑账号、影子账户。

（一）排查服务器弱口令

检查方法：

尝试使用弱口令登录爆破或直接咨询管理员

（二）排查可疑账号、新增账号

检查方法：

1、打开 cmd 窗口，输入 lusrmgr.msc 2、查看是否存在可疑账号，特别是管理员群组（Administrators）中的新增账号，如果存在需要立即删除或禁用

（三）排查隐藏账号

检查方法 1：

打开注册表，查看管理员对应键值 1、在桌面打开运行（可使用快捷键 win+R），输入 regedit，打开注册表编辑器 2、选择 HKEY_LOCAL_MACHINE/SAM/SAM，默认无法查看该选项内容，右键菜单选择权限，打开权限管理窗口 3、选择当前用户（一般为 administrator），将权限勾选为完全控制，然后确定并关闭注册表编辑器 4、再次打开注册表编辑器，即可选择 HKEY_LOCAL_MACHINE/SAM/SAM/Domains/Account/Users 5、在 Names 项下可以看到实例所有用户名，如出现本地账户中没有的账户，即为隐藏账户，在确认为非系统用户的前提下，可删除此用户

检查方法 2：

通过 D 盾 web 查杀工具进行检测，其中集成了对克隆账号、隐藏账号检测的功能

（四）结合日志排查用户是否出现异常

检查方法 1：

1、在桌面打开运行（可使用快捷键 win+R），输入 eventvwr.msc 命令 2、打开时间查看器，分析用户登录日志

检查方法 2：

通过 LogFusion 查看日志记录

二、检查异常端口、进程

端口作为计算机内部与外部数据交互的窗口，在攻击者眼里也是作为香饽饽的存在，在入侵系统后，攻击者可以在计算机上开启专属的端口来访问被害主机或植入病毒用于挖矿等，熟悉计算机的朋友应该都知道常用的端口也就那么几个，所以通过排查可疑端口能确定主机是否存在后门、是否被植入挖矿病毒等，再根据端口的 PID 对可疑进程对应的程序排查，确定是否为恶意程序。

（一）排查可疑端口

检查方法 1：

1、使用 netstat 命令查看当前网络连接，定位可疑的 ESTABLISHED 连接

netstat -ano

2、根据 PID 编号通过 tasklist 对进程进行定位

tasklist | findstr "PID"

检查方法 2:

通过 D 盾 web 查杀工具进行端口查看

（二）排查可疑进程

检查方法 1：

1、在桌面打开运行（可使用快捷键 win+R），输入 msinfo32 命令 2、依次点击 “软件环境 - 正在运行任务” 就可以查看到进程的详细信息，比如进程路径、进程 ID、文件创建

日期以及启动时间等。

检查方法 2：

打开 D 盾_web 查杀工具的进程查看，关注没有签名信息的进程

检查方法 3：

通过微软官方提供的 Process Explorer 等工具进行排查

在查看可疑的进程及其子进程。可以重点观察以下内容：

1、没有签名验证信息的进程 2、没有描述信息的进程 3、进程的属主 4、进程的路径是否合法 5、CPU 或内存资源占用长时间过高的进程

三、检查启动项、计划任务和服务
启动项、计划任务、服务是攻击者维持权限的惯用手段。在入侵 windows 计算机后，攻击者可以通过修改注册表、替换粘滞键程序在系统启动时就获得权限，也能够在管理员权限下设置计划任务，因为计划任务后门分为管理员权限和普通用户权限两种。管理员权限可以设置更多的计划任务，例如重启后运行等。也可以通过 meterpreter 创建后门服务。

（一）排查异常启动项

检查方法 1：

单击【开始】>【所有程序】>【启动】，默认情况下此目录在是一个空目录，确认是否有非业务程序在该目录下。

检查方法 2：

在桌面打开运行（可使用快捷键 win+R），输入 msconfig，查看是否存在命名异常的启动项目，是则取消勾选命名异常的启动项目，并到命令中显示的路径删除文件。

检查方法 3:

在桌面打开运行（可使用快捷键 win+R），输入 regedit，打开注册表，查看开机启动项是否正常，特别注意如下三个注册表项：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce
检查右侧是否有启动异常的项目，如有请删除，并建议安装杀毒软件进行病毒查杀，清除残留病毒或木马。

检查方法 4:

利用安全软件查看启动项、开机时间管理等。

检查方法 5:

在桌面打开运行（可使用快捷键 win+R），输入 gpedit.msc 查看组策略

（二）排查计划任务

检查方法 1：

1、在桌面打开运行（可使用快捷键 win+R），输入 control 打开控制面板 2、在 系统与安全 中查看计划任务属性，便可以发现木马文件的路径。

检查方法 2：

1、在桌面打开运行（可使用快捷键 win+R），输入 cmd 打开命令行窗口 2、检查计算机与网络上的其它计算机之间的会话或计划任务，如有，则确认是否为正常连接，其中计划任务在 windows7 及之前版本的操作系统中使用 at 命令进行调用，在从 windows8 版本开始的操作系统中使用 schtasks 命令调用。

windows server 2016 下执行 schschtasks

windows 7 下执行 at

检查方法 3：

利用安全软件查看计划任务。

（三）排查服务自启动

检查方法：

1、在桌面打开运行（可使用快捷键 win+R），输入 services.msc 2、注意服务状态和启动类型，检查是否有异常服务

四、检查系统相关信息
系统本身如果存在漏洞，那么结果往往是致命的，如果计算机存在永恒之蓝漏洞且未采取防护措施。那么攻击者就能直接通过 MSF 的漏洞利用程序获取目标 windows 系统的 system 权限。与此同时，攻击者在进入系统后往往也会留一些蛛丝马迹，如未将上传文件清除、浏览器浏览记录未删除、下载的文件未删除等。在检查系统相关信息时就需要重点关注系统本身存在的漏洞以及攻击者使用过的文件。

（一）查看系统版本以及补丁信息

检查方法：

1、在桌面打开运行（可使用快捷键 win+R）输入 systeminfo 2、查看系统信息和补丁状态

3、将内容导入文本，利用 windows-exploit-suggester 对系统补丁进行漏洞利用分析

python windows-exploit-suggester.py --database 2021-08-26-mssb.xls --systeminfo systeminfo.txt
1

（二）查看可疑目录及文件

检查方法 1：

查看用户目录，是否存在新建用户目录

Window 2003 版本 : C:\Documents and Settings
Window 2003 以后版本 : C:\Users\

检查方法 2：

1、在桌面打开运行（可使用快捷键 win+R）输入 %UserProfile%\Recent 2、分析最近打开的可疑文件

检查方法 3：

1、点击文件资源管理器，查找服务器内中的各个文件夹 2、将文件夹文件按时间进行排序，查找可疑文件，其中修改时间在创建时间之前的为可疑文件，也可以在搜索中搜索某一时间

修改的文件。重点关注 windows\system32 的 sethc.exe 是否被替换为 cmd 程序

检查方法 4：

针对回收站、浏览器下载目录以及历史记录进行排查

（三）查看隐藏文件

检查方法 1：

1、在桌面打开运行（可使用快捷键 win+R），输入 control，进入控制面板 2、找到文件资源管理器选项，点击 查看 后，取消”隐藏受保护的操作系统文件“勾选，在隐藏文件和文件夹下面的单选选择显示隐藏的文件、文件夹和驱动器

检查方法 2：

如果操作系统版本够高的话直接在资源管理器中设置

检查方法 3：

借助 fileseek 查看文件

五、日志分析
主要查看系统日志和 web 日志，通过日志可以帮助我们验证对入侵过程的判断和发现其他入侵行为。但它的前提则是日志记录已开启的情况下才能获取。这块具体会在之后的日志分析篇提到

（一）系统日志

分析方法：

1、在桌面打开运行（可使用快捷键 win+R），输入 eventvwr.msc 2、找到事件查看器，查看 windows 日志（包括应用程序、安全、Setup、系统、事件）

（二）web 日志

分析方法：

1、找到中间件、应用、WAF 的日志（包括但不限于 IIS、Nginx、宝塔、网站等） 2、打包至本地进行分析，在编辑器中对关键字进行搜索

六、工具查杀

webshell 和病毒都是 windows 系统的大敌，它们可以维持攻击者的系统权限、盗窃资料、感染其他主机、加密文件等，对操作系统造成非常大的危害。这里推荐 D 盾以及火绒软件（当然查杀软件越多越好）。对病毒进行全盘扫描，而对 webshell 进行 web 目录扫描。

1.文件排查

1.1 文件分析

Windows 系统通过以下三种方式查着开机启动项：

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

1.2 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 torLocal Settings\Temp;

3.C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\(默认为隐藏目录)

快捷键【win+R】———【%temp%】

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，检查是否为恶意文件的网站：

1. https://www.virustotal.com
2. 微步云沙箱 https://s.threatbook.cn/

1.3 时间属性分析

1）查看浏览器记录：

1.查看是否被使用下载恶意代码及文件。

2.查看是否有浏览恶意网站的记录。

2）在 Windows 系统下，文件属性的时间属性具有:

- 创建时间
- 修改时间
- 访问时间

如果修改时间要早于创建时间那么这个文件存在很大可疑。(中国菜刀等工具可修改)

选中文件【右键】---【属性】

3）Windows 系统会记录系统中最近打开使用文件的快捷方式，通过以下方法可查看最近打开的文件:

【win+E】---【C:\Documents and Settings\Administrator\Recent】

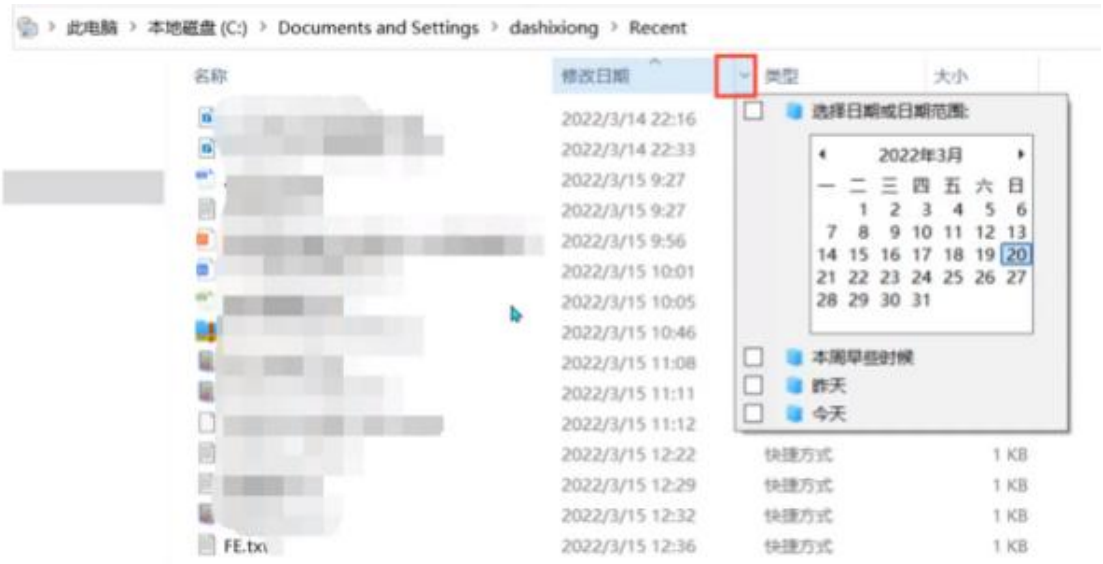
【win+E】---【C:\Users\Administrator\Recent】

【win+R】---【%UserProfile%\Recent】

4）除此之外，还可以自己手动寻找。

1.根据文件夹内文件列表时间进行排序， 查找可疑文件。

2.搜索指定日期范围的文件，快速定位筛选。



2.进程排查

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

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

记录一次进程排查过程:

1.查看所有的端口占用情况命令 netstat -ano

2.查看端口中状态为 established 的所有进程 netstat -ano |find "ESTABLISHED”

3.发现”可疑进程”定位 PID 值为 4612

4. 查看指定 PID 的占用情况：

netstat -aon | findstr "XXX” (XXX 代表的是具体进程的 PID 值)

```
C:\Users\dashixiong>netstat -aon|findstr "4612"
  TCP    127.0.0.1:1111         127.0.0.1:54530        ESTABLISHED     4612
  TCP    127.0.0.1:10017        0.0.0.0:0              LISTENING       4612
  UDP    127.0.0.1:40000        *:*                                    4612

C:\Users\dashixiong>
```

5.查看 PID 对应的进程命令：tasklist | findstr “XXX”

```
C:\Users\dashixiong>tasklist|findstr "4612"
SangforPromoteService.exe     4612 Services                   0     10,264 K

C:\Users\dashixiong>
```

6.杀死该可疑进程：taskkill /f /t /im SangforPromoteService.exe

也可以根据 wmic process 获取进程的全路径任务管理器定位到进程路径

Wmic process | findstr “svchost.exe”

- 查询进程
- wmic process(带有 cmdline)
- wmic process list brief
- wmic process where name= “xxxx" get executablepath
- 删除进程
- wmic process where processid="2345” delete
- 查询服务
- wmiG SERVICE(涵盖服务关联所有信息)
- wmic SERVICE where caption(name)=” XXX" call stopservice
- wmic SERVICE where caption(name)= “XXX" call delete
- 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 chcp 437)

3. 系统信息排查

- 查看环境变量的设置【我的电脑】---【属性】---【高级系统设置】 ---【高级】---【环境变量】
- Windows 计划任务【程序】---【附件】---【系统工具】---【任务计划程序】
- Windows 帐号信息，如隐藏帐号等【开始】---【运行】---【compmgmt.msc】---【本地用户和组】---【用户】(用户名以$结尾的为隐藏用户)
- 命令行方式: net user，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---net user username

- 查看当前系统用户的会话使用→ query user 查看当前系统的会话，比如查看是否有人使用远程终端登录服务器
- logoff 踢出该用户
- 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

4. 工具排查

ProcessExplorer

PC Hunter

Microsoft Network Monitor

5. 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
- 中间件日志(Web 日志 access log)nginx、weblogic、websphere、apache、iis、tomcat、jboss

二、Web 常见安全漏洞

1.渗透测试基础

渗透测试是什么(Penetration Test)

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。

2.渗透测试和黑客攻击的区别：

渗透测试是经过客户授权，采用可控制、非破坏性性质的方法和手段发现目标和网络设备中存在的弱点,帮助管理者知道自己网络所面临的问题，同时提供安全加固建议，帮助客户提示系统的安全性。渗透测试方法:

1）黑盒测试：渗透测试人员只知道被测试的目标，其余与目标相关的信息一无所知。特点:属于外部渗透测试，在前期需要对目标进行大量的信息收集，耗时较长。更有挖掘出系统潜在的漏洞、以及脆弱环节、薄弱点等。

利于

2）白盒测试：渗透测试人员可以通过正常渠道向被测试单位取得各种资料，包括网络拓扑结构图、员工资料、网站程序的代码片段，可以和单位其他员工进行面对面沟通。

特点:在前期对目标系统已经初步的了解。根据测试地点分为“从组织内部"与“从组织外部”两种大环境充分发挥"社会工程学的力量"，对企业内部雇员的越权操作进行测试。

3）灰盒测试：介于自盒测试与黑盒测试之间。

特点:被测试单位只有少数人知晓测试的存在，较好的检验单位中的信息安全事件监控、响应等是否到位，属于较为隐秘的测试。

3.根据测试目标分类：

1）操作系统渗透：Windovs、Linux、Solaris、AIX、SCO 等

2）数据库系统渗透：MySQL、Oracle、MSSQL、sybase、Informix

3）应用系统渗透：由 ASP、JSP、PHP 等组成的 web 应用(包括移动应用产品

4）网络设备渗透：防火墙、入侵检测系统等

4.渗透测试攻击流程

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

5.信息采集

- 域名与 IP：根据目标的主域名和企业关键字拼音或英文组成等进行子域名爆破和猜解，同时获取域名对应 IP 通过 C 段获取更多相关主机 IP，绕过 CDN 防护寻找目标真实 IP。
- 企业关系网：通过互联网上的公开信息，查询目标企业的关系网，包括投资人、控股人等的旗下产业信息，以及日标企业的各下属单位的相关信息。
- 信息泄露：从开源平台如 github 等收集目标企业可能泄露的源码、账号密码等信息。
- 员工信息：从互联网社交平台、开源平台、企业网站等地方尽可能收集员工相关的信息，包括员工号组成、姓名、部门、手机号、邮箱、生日等。

6.风险点利用

- 弱口令/通用口令：无论应用系统、服务器还是网络安全设备等，弱口令和通用口令一直都是一个比较严峻的问题，随着攻击手段变化，弱口令应该不能仅仅局限于简单数字字母组合这种常规的模式，还需关注连续有规律，使用频率高的口令，以及跟用户信息关联度高的口令组成，尤其是管理员。
- 信息泄露：信息泄露包括员工相关信息泄露，业务系统源码泄露日志敏感信息泄露等，无论在互联网还是内部网络当中，这些信息都能给攻击方带来巨大的攻击成效，包括用于社工钓鱼，分析审计系统漏洞，甚至直接账号登陆系统，接管服务器等。
- Nday 漏洞：在历年的红蓝对抗攻防演练当中，0day 和 1day 的使用都是最受关注的热点，尤其是 0day 的使用，往往防不胜防，而 1day 的使用多是捡漏，或者是对安全设备规则绕过的特定场景运用，所以 0day 危害巨大而 1day 多用于攻击边缘资产或者发现修复不全或未修复漏洞的遗漏主机。
- 社工：社工是在红蓝对抗攻防演练当中，与常规渗透服务最大的区别，其利用内部员工安全意识薄弱和人性弱点结合攻击手段，诱骗员工进行恶意操作，点击执行后门程序等，一般一旦攻击成功，将有极大可能直接进入企业内网。

7.渗透常用工具

Metasploit、Wireshark、Nmap、Sqlmap、Burpsuite、Google/hacking、御剑

8.攻击手段

常规漏洞分析攻击：包括 SQL 注入、XSS、件工作、文件包含、文件读取、命令执行等。

口令攻击：包括弱口令、通用口令、社工组合口令等。

Nday 攻击：包含 0day 和 1day 的攻击。

社工：包括鱼叉攻击、水坑攻击、电话等社交方式诱骗等。

9.攻击目的

以攻固防：从攻击方的角度，整体分析目标企业的安全状态，包括管理和技术两大层面，从全局最大限度的发现目标企业的潜在安全风险，并提供整体网络整改的方案，提高目标企业整体网络安全防护水平，达到以攻击验证防护手段加固防御。

1. SQL 注入

1.1 原理

SOL 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 SOL 命令。

1.2 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

1.3 修复建议

1、代码中的数据库操作采用 sg!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 SOL 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 union 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;长

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 SOL 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

2. XML 注入

1.1 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。

1.2 危害

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-Nm 可通过此类漏洞查询获取到系统内部完整的 XML 文档内容;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。

1.3 修复建议

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'"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。

3、对于系统出现的错误信息，屏蔽系统本身的出错信息或者用统一的报错页面代替(如 updataxml()这类)。

3. XXE 漏洞

3.1 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。

3.2 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。

3.3 修复建议

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(XMLInputFactery.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. XSS 漏洞

3.1 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 等其它脚本语言时，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。

3.2 危害

(1)窃取管理员帐号或 Cookie(恶意操纵后台数据)
(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

3.3 修复建议

(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

Spring HtmlUtils

String result = HtmlUtils.htmlEscape(source);

(2)增加过滤器 XssFilter

(3)白名单过滤

根据白名单的标签和属性对数据进行过滤，以此来对可执行的脚本进行清除(如 script 标签，img 标签的 onerror 属性等)

String result =Jsoup.clean(source, Whitelist.basic());

(4)web.xml 增加过滤器配置

5. CSRF 漏洞

3.1 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 和 XSS 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 webserver 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”。

3.2 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。

3.3 修复建议

(1)检查 Referer

(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)。

6. 命令执行

6.1

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。

6.2

(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

6.3

(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

7. 任意文件读取

7.1 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。

7.2 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

7.3 修复建议

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。

8. 文件包含

8.1 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

8.2 危害

8.3 修复建议

9. 文件上传

9.1 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 webshel 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。

9.2 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

9.3 修复建议

(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(include dama.jpg)(4)及时更新 web 应用软件避免解析漏洞攻击

10. 弱口令

10.1 原理

弱口令: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。

10.2 危害

10.3 修复建议

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

11. 路径遍历

11.1 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)

11.2 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.dom/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.jsp?f

11.3 修复建议

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。

12.越权

12.1 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。

12.2 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

12.3 修复建议

1.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)

2.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。

3.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。

一、监控设备
首先是设备，（本人）这次 HW 使用的安全产品主要有两个：天眼和椒图。

产品　　全称
天眼　　奇安信天眼威胁检测与分析系统
椒图　　奇安信网神云锁服务器安全管理系统
天眼负责流量分析，部署在旁路，对交换机镜像过来的流量进行监测、分析和溯源。

椒图负责服务器的系统防护，通过在服务器上安装的客户端，将收集到的主机信息发送到控制中心集中分析。

二、工作内容
防守方主要分为三个组：安全监控组、事件研判组、应急处置组。
1）监控组分析安全设备的告警，确定是攻击就提交给处置组封禁 IP；分析不出来就提交给研判组分析。
2）研判组负责分析监控组提交的告警是否为攻击，必要时可以访问受害网站复现攻击，或者联系受害网站的负责人验证是不是正常业务/人为操作。
3）处置组主要负责封禁 IP，如果是 webshell 这种攻击，还需要联系受害网站的负责人，协助修复漏洞或者加固网站。

三个组通过指挥调度管理系统进行协作防护：
大家上班第一件事就是登录管理系统，监控组向管理系统提交告警的攻击/受害 IP、告警类型以及 payload，处置组/研判组看到管理系统上有新的告警了就封禁 IP/分析告警事件。

原则上来说，我一个安全监控组，只需要盯着安全设备，简单分析一下然后提交告警就可以了。
由于公司就来了我一个，只要是我们产品相关的事，都会把我喊过去。
因此，除了设备监控外，我的工作还包括但不限于：分析 webshell 文件、分析病毒木马文件、升级/加固安全产品、对失陷主机进行后门扫描和病毒查杀、以及协助失陷网站修整加固。。。

三、安全事件
好了，撇开厕所不谈，下面分享几个印象比较深的攻击事件吧：

1）失陷主机排查
青藤云的蜜罐检查到，有个用户电脑访问了蜜罐的 80 端口，用户断网以后用 360 和火绒查杀了三个毒以后，重新上线，结果又踩了蜜罐，用户又用 360 和火绒扫了一遍，啥也没扫出来，就喊我过去处理。

当时我就一脸懵逼：这是我一个安全监控该干的事吗？
但架不住一群人直勾勾的盯着我，只能硬着头皮去干

先是用椒图扫了一遍 webshell 和后门文件。
确认没有后门以后，用专杀工具全盘扫描，扫出来 7 个病毒。

扔到 ti 威胁情报中心鉴定，确定就是高危病毒。
然后提交到二线做病毒分析，确认是远控木马类病毒，与触发蜜罐的告警有相关性。
最后删掉病毒，重新上线，没有再出现异常现象。

2）后门网站修复
椒图检测到一个服务器上存在 webshell，通知用户紧急下线网站，开始排查和加固。

一群人围在哪里分析了半天，然后理所应当的把这事扔给了我：“你们家的设备，当然要你去处理呀~”

老规矩，先用椒图扫一下 webshell 和后门，在 Temp 目录下扫出来一个 webshell。
跟用户的开发核实后，确认不是业务文件，是被人上传了文件。
于是删掉 webshell，取消了 Temp 目录的所有用户权限，在椒图上吧这台服务器的防护全部开启（默认只检测不拦截）。
开发也临时关闭了上传的功能，然后准备重新上线。

结果上线后，网站访问不了。。。

在重新部署了 n 遍项目，外加换了两台备用服务器后，时间已经来到了凌晨六点，距离规定的上线时间还差三个小时。
“实在不行，咱们就写个静态主页跳 404 吧，点啥功能都给跳到 404，最起码，他们一时半会儿不会怀疑是我们的问题，咱们也能多点时间排查问题。”
开发的嘴角慢慢上扬，空洞的眼神里重新亮起了光。

不幸的是，这话被项目经理偷听到了，在经理的谴责声中，我看到，开发的眼神，竟慢慢的黯淡下来，直到剩下两个黑黑的眼眶。

兴许是一晚上没去厕所的原因，在换到第三台备用服务器的时候，网站终于恢复了。

事后，我问开发：“你们的运维咋没过来呢？”

“我就是运维。”

“那，开发呢？”

“开发也是我。”

“？？？，那，你们项目组。。。”

“只有我自己~”

四、告警流量分析
平均下来，一天得有三千多条告警，但其中大部分都是误报，接下来分享一些简单的告警流

量特征。

1）信息泄露
看访问路径中是否存在特殊文件或路径。
比如，访问备份文件.zip

访问默认文件

或者特殊类型的文件

客户授权的话，可以访问该路径，查看返回结果中是否包含敏感信息，以判断是否攻击成功。

2）SQL 注入
看请求参数、请求头或请求体中是否包含 SQL 语句或关键字。

比如，GET 请求中包含 SQL 语句（联合查询注入）：

请求头中包含 SQL 语句：

POST 请求体中包含 SQL 语句：

为了方便绕过，还会改变 SQL 关键字的大小写或编码。

比如：大小写绕过：

编码绕过：

客户授权的话，可以复现 payload，根据页面的返回结果、响应时间来判断是否注入成功。

3）文件上传
看请求体中是否包含代码内容：

如果响应体中有 success 等上传成功的字样，或者有该文件的访问记录，则说明 webshell 上传成功。

4）XSS（跨站脚本）
看请求参数或请求体中是否包含 JavaScript 代码：

将响应体的数据复制到文件中执行，如果弹窗，就说明攻击成功。
如果没弹窗，就 Ctrl+F 搜 JS 代码，常见的有：

5）代码执行
看请求参数、请求头、请求体中是否包含恶意代码。

比如，请求体中包含 PHP 代码：

Dedecms V5.7 后台任意代码执行：

Fastjson 反序列化漏洞攻击：

ThinkPHP 5.0.x—5.1 远程代码执行：

一、监控值守介绍
1. 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一
- 快速遏制攻击行为，可调整策略阻挡攻击

旁路模式一般是指通过交换机等网络设备的“端口镜像”功能来实现监控质。
串联部署指串联在链路中，可以控制流量。

二、蓝队工作职责与模式

1. 岗位职责

设备监控岗:初步监控攻击事件，做简单分析并上报

分析研判岗:对攻击方式、路径、范围、结果等作分析研判，找到攻击者信息

应急响应岗:攻击事件影响分析，复现及溯源等

处置封禁岗:事件的处置，包括封禁 IP

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

安全设备状态巡检：

1） 每日经过流量的变化情况

2） 特征库授权，探针授权等等

3）设备磁盘，CPU 状态查看，长时间无新告警时的排查

2. 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

事件上报:

事件上报时须包括:攻击 IP，归属地，目的 IP，时间，事件类型。

3. 封禁记录

若担任有封禁 IP 任务的，在 IP 封禁后一般要填写封禁信息表

4. 工作汇报

每日事件统计时，注意统计的时间、区间，设备和事件的对应。

每日工作报告需包括:总体告警数量，上报事件数量，类型分布，重点关注事件等

三、安全平台/设备

1. 安全设备类别

- 安全监测类:IDS、IPS、APT
- 安全防护类:防火墙、WAF、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

2. 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 日志分析注意事项：

- 一键请求头信息提取
- 解码工具
- 安全事件日志导出
- Web 应用漏洞事件分析:合理利用互联网资源!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。

3. IPS：

特点:

- 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

IPS 日志分析:

- 双击入侵防御日志，查看日志内容，特征性质判定，特征处理流程。
- 日志内容最大长度为 4k。
- 解码工具支持 URL 编解码，16 进制解码，BASE64 解码。
- 标红部分为命中特征部分。

IPS 日志分析注意事项:

- 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。

4. IDS：

特点:

- 对攻击行为具有高精度的检测能力
- 对网络流量非常敏感
- 识别精度高

IDS 告警分析

- 通过页面告警信息和提取的原始报文，进行研判分析(查看请求方法，请求体，源目 IP。

5. 产品联动

WAF 联动

- 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

四、安全设备日志分析

1.安全设备日志分析

1.1 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/lgginjsp
- ✓ 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。

1.2WEB 日志分析

- ✓ 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

- ✓ 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

1.3 告警日志类型

- ✓ 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

常见 web 服务器

nginx 日志

a)默认储存位置:Windows:/Nginx/logs/;Linux:/var/log/apache24

b)日志文件:一般分为 access log 和 error log 两种

IIS 日志 e

a) 默认储存位置:Windows:C:/WINDOWS/system32/LogFilese

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.gut、localhost、manager

WEB 日志内容所需关注:

- 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