电子科技大学 计算机 学院

标 准 实 验 报 告

（实验）课程名称 信息对抗综合实验

电子科技大学教务处制表

电 子 科 技 大 学

实 验 报 告

学生姓名：黄鑫　学 号：2021050901013　指导教师：汪小芬

实验地点：主楼 A2-413-1　　实验时间：10.17

一、实验室名称：主楼 A2-413-1

二、实验项目名称：Windows 日志查看

三、实验学时：4

四、实验原理：

系统日志是 Windows 操作系统产生的记录信息、警告以及错误的重要存储之一。这些记录不仅提供了关于功能配置或运行成功的详细信息，还有助于查明系统在某些方面出现故障或表现不稳定的根本原因。

安全日志则专门用于记录审核事件的成功与失败。它们为我们提供了宝贵的信息，以便了解系统的安全审核状态和安全性的整体情况。

应用程序日志包含了应用程序产生的各类信息、警告以及错误的记录。这对于追踪应用程序运行时的问题、分析其性能以及及时解决错误非常重要。

五、实验目的：

对 Windows 日志进行查看

六、实验内容：

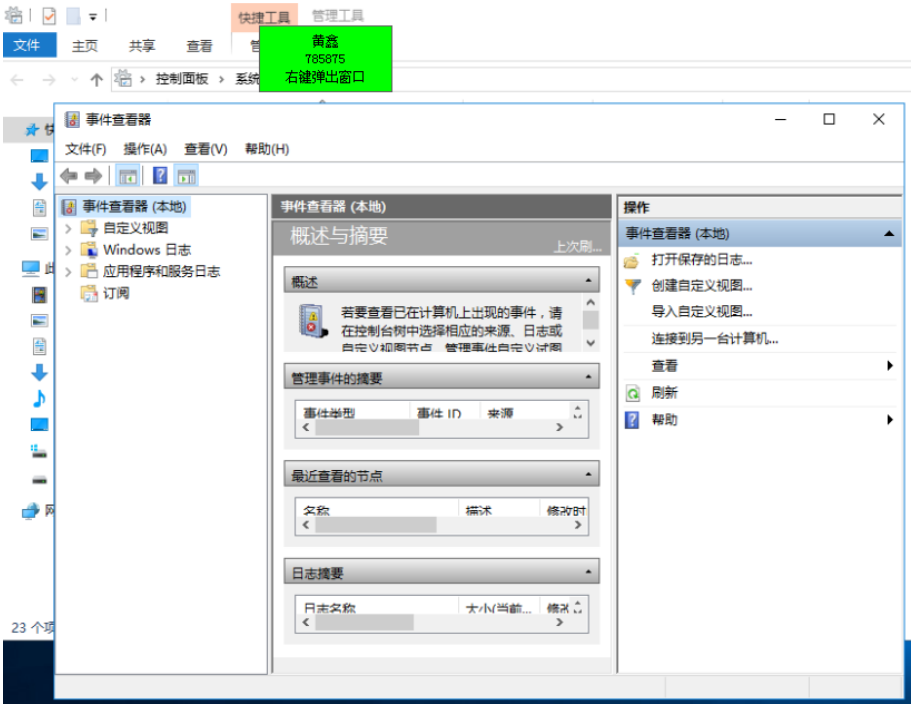
通过 Window 本地查看系统查看 Windows 日志，并提取信息进行分析

七、实验器材（设备、元器件）：

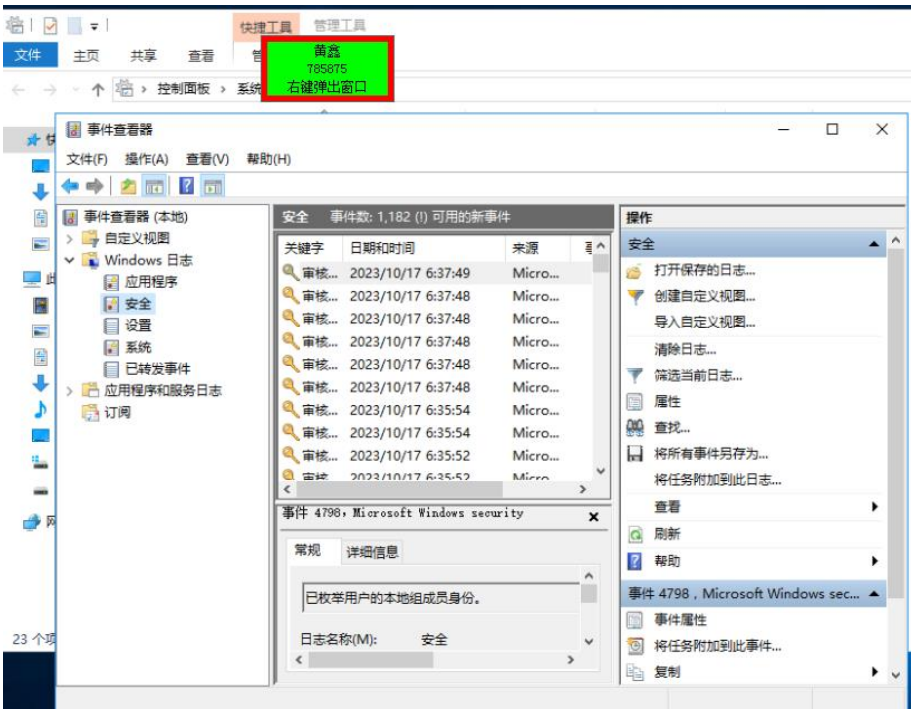
Windows Server 2016

八、实验步骤：

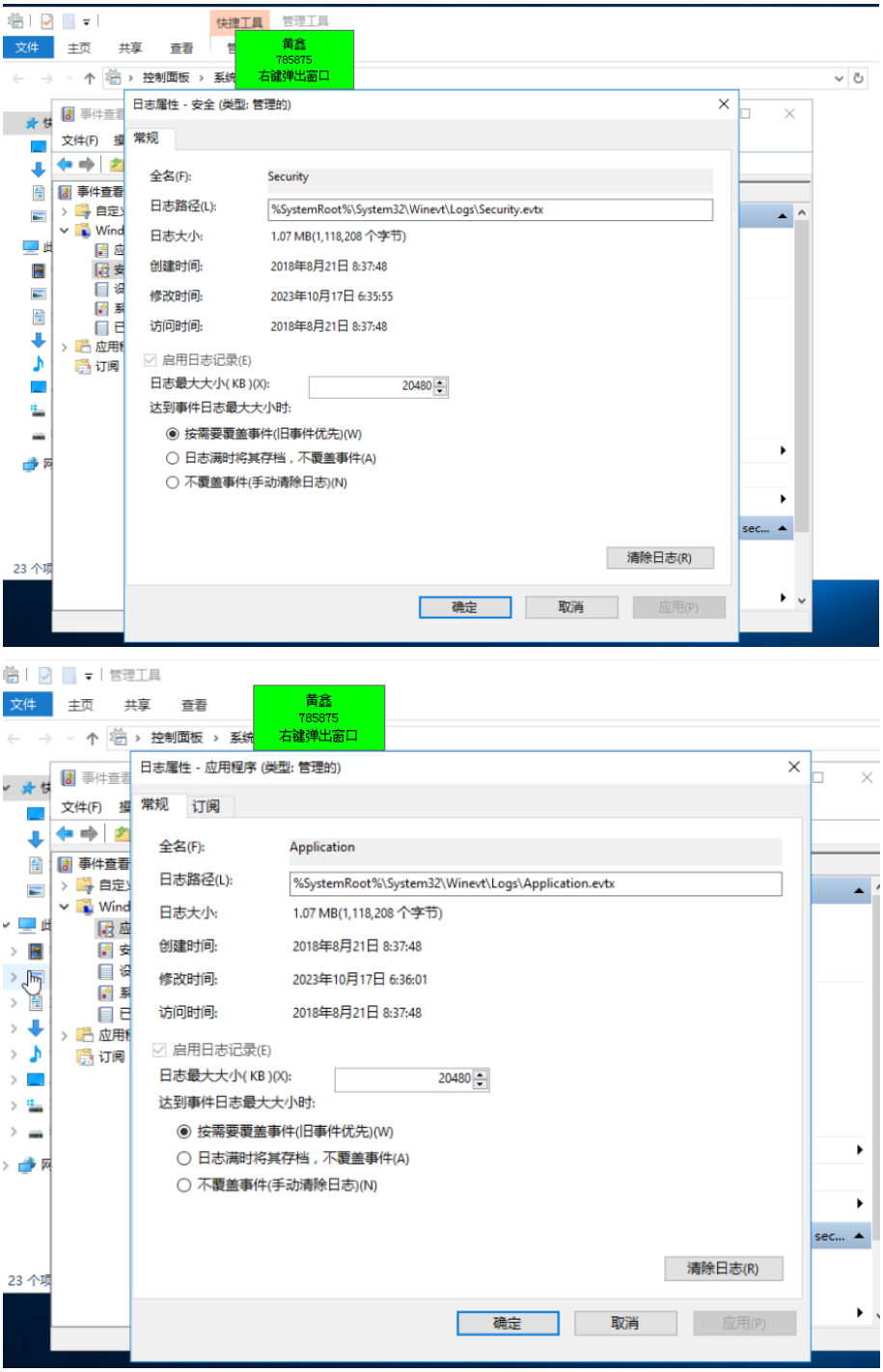
（1）单击“开始”→“Windows 管理工具”→“事件查看器”



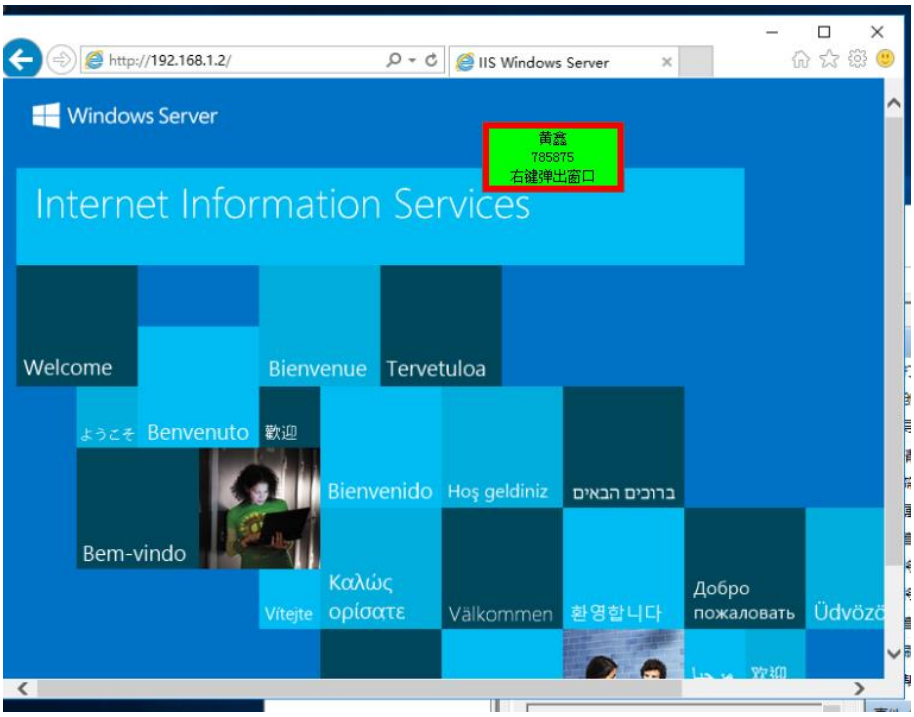
（2）点击 Windows 日志下的安全。



（3）在事件查看器中右键应用程序（或安全、系统、设置等）查看属性可以得到日志存放文件的路径，并可修改日志文件的大小，清除日志

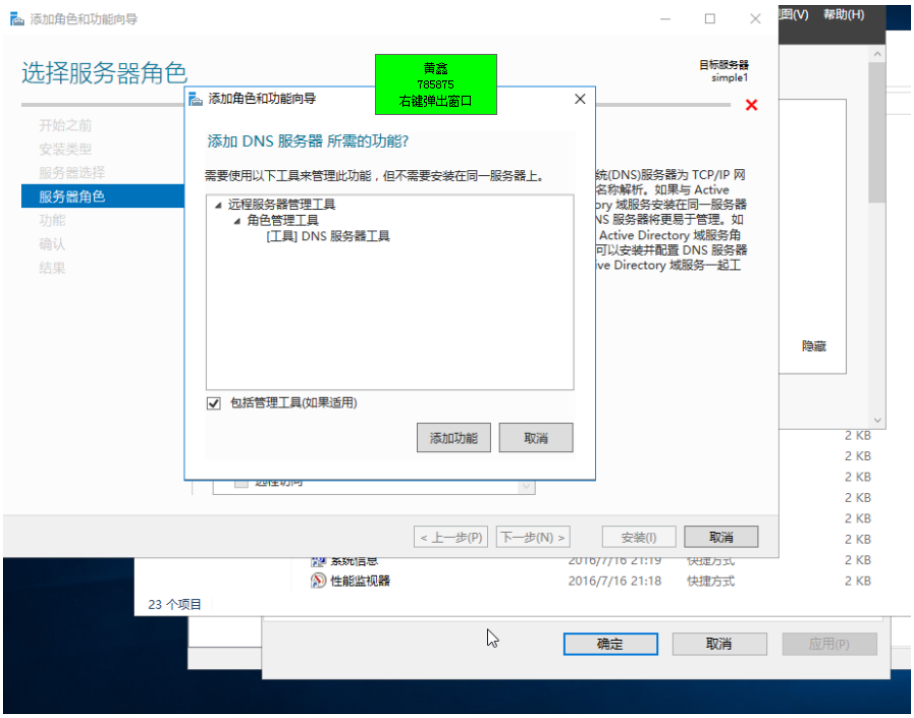


（4）查看做 web 服务器建立的网站日志文件夹下的日志文件，此处需要自行安装 Web 服务器（IIS），参考实验 Web 服务器的安装与配置，并访问 http://192.168.1.2 网页。



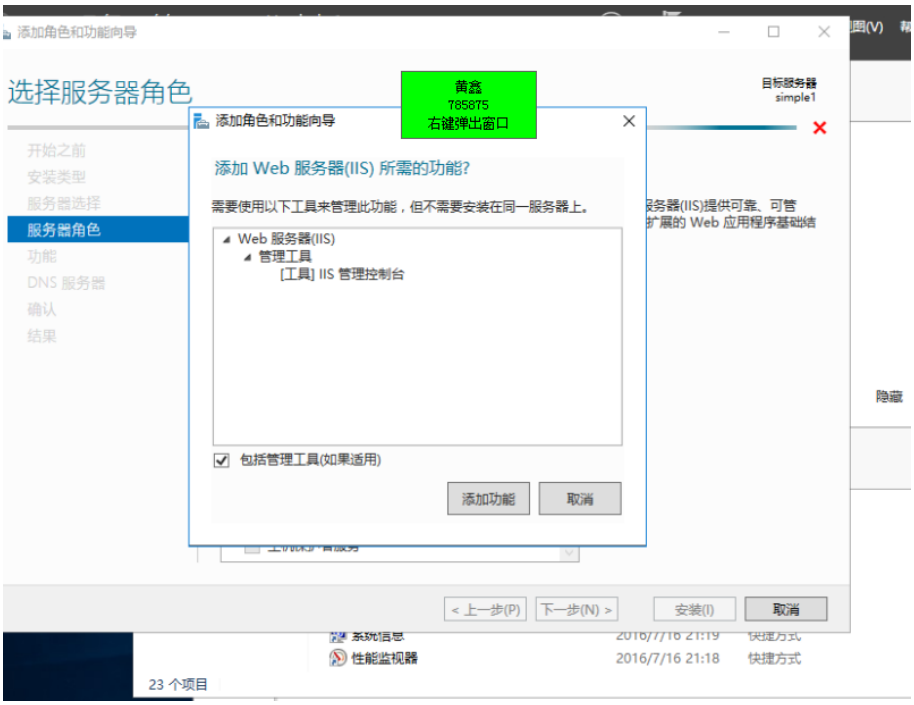
(5)Web 服务器的安装与配置步骤：打开“开始”——“服务器管理器——“仪表板”选项的“添加角色和功能”，持续单击“下一步”按钮，直到出现“选择服务器角色”窗口时勾选“DNS 服务器”、“Web 服务器”复选框，单击“添加功能”按钮.

(

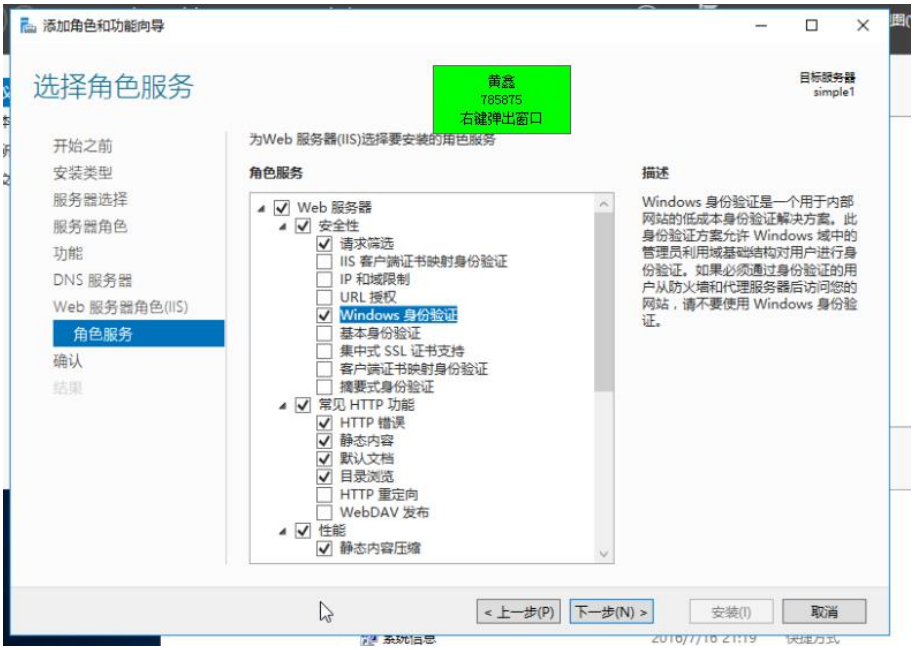


(6）单击“下一步”，没有其他需求的话，在“功能”窗口直接单击“下一步”

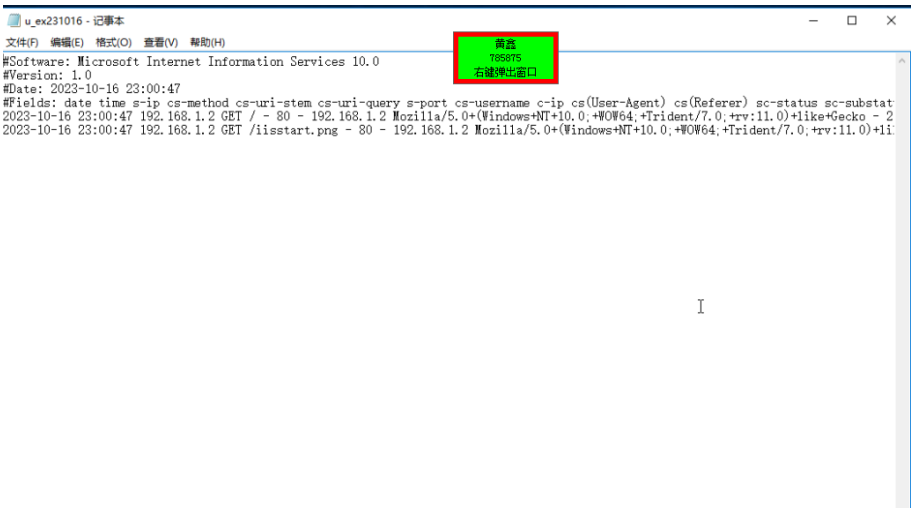
即可。



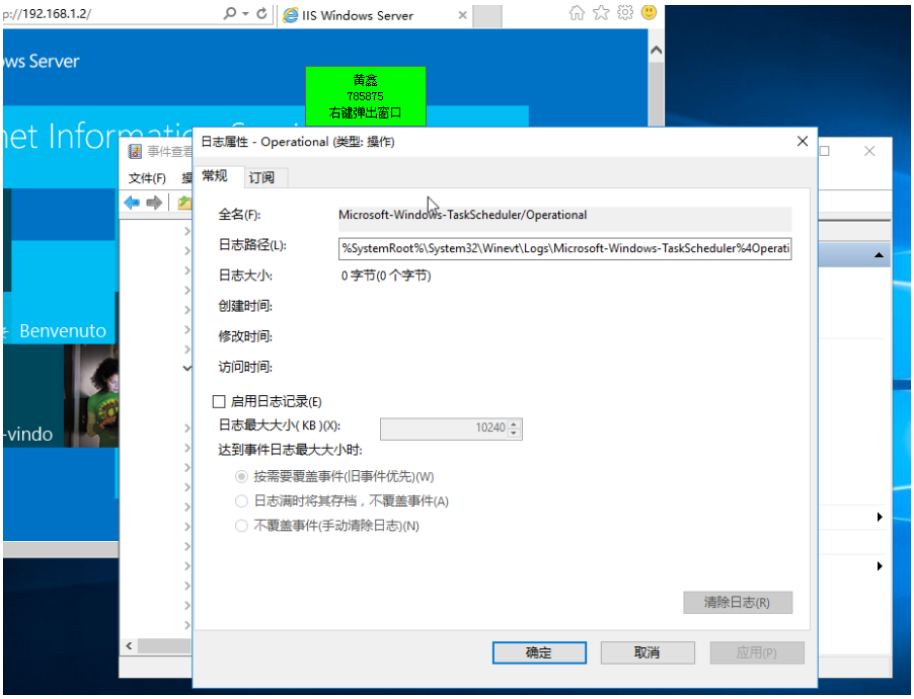
（7）在“角色服务”对话框勾选“Windows 身份验证”，单击“下一步”。



（8）点击完成。当我们对 www 服务中某一文件进行访问，则日志中则会有相应的日志记录。



（9）日志中记录了访问 www 服务的请求地址，管理员可以根据请求地址，发现网络上的攻击，管理员可根据日志信息，采取一定的防护措施。计划任务日志，当入侵者得到远程系统的 shell 之后，常会利用计划任务运行功能更加强大的木马程序，计划任务日志详细的记录的计划任务的执行时间，程序名称等详细信息。打开“事件查看器”，打开“应用程序和服务日志→Microsoft→Windows→TaskScheduler→Operational”，右键选择属性可查看计划任务日志，如图 7 所示。



九、实验数据及结果分析：

通过安装 Web 服务器，我们成功查看了做 web 服务器建立的网站日志文件夹

下的日志文件，日志中记录了访问 www 服务的请求地址。

十、 实验结论：

Windows 日志分为多个类别，包括应用程序日志、安全日志、系统日志和设备管理器日志等。每个类别都记录了不同类型的事件和信息，可以帮助我们定位和解决系统问题。

十一、总结及心得体会：

Windows 日志是解决系统问题的重要工具: Windows 日志记录了系统和应用程序的活动和事件,对于定位和解决系统问题至关重要。通过仔细分析日志条目，可以找到故障发生的时间、相关的应用程序或服务，并查找错误或警告消息，从而诊断和解决问题。

十二、对本实验过程及方法、手段的改进建议：

为了更好地说明 Windows 日志查看的应用场景和实际价值，可以引入一些实际案例或示例，展示如何通过查看日志解决具体的系统问题。

报告评分：

指导教师签字：

电子科技大学 计算机 学院

标 准 实 验 报 告

（实验）课程名称 信息对抗综合实验

电子科技大学教务处制表

电 子 科 技 大 学

实 验 报 告

学生姓名：黄鑫　学 号：2021050901013　指导教师：汪小芬

实验地点：主楼 A2-413-1　　实验时间：10.17

一、实验室名称：主楼 A2-413-1

二、实验项目名称：Windows 日志手动清除

三、实验学时：4

四、实验原理：

1. 系统日志的作用：

记录活动：系统日志文件记录了系统中发生的各种活动和事件，包括登录、文件访问、系统错误、网络活动等。

安全监控：系统管理员可以使用系统日志来监视系统的安全性。异常活动或入侵尝试通常会在日志中留下痕迹，允许管理员快速检测和应对潜在的问题。故障排除：系统管理员可以使用日志来分析问题，了解系统中出现的错误和故障，以便更好地进行故障排除和维护。

2. 日志文件的特殊性：

访问权限：通常，系统日志文件的访问权限受到高度控制，一般用户无法直接修改或删除它们，以确保日志的完整性和可靠性。

格式：系统日志文件通常遵循特定的格式，这些格式有助于系统管理员以结构化方式查看和分析日志数据。这使得日志文件与普通文本文件不同。

3. 黑客对日志的攻击：

删除日志：黑客可能尝试删除或清空系统日志文件，以消除他们的痕迹。这是相对简单的攻击方法，但通常会引起管理员的怀疑。

修改日志：更高级的黑客可以尝试修改日志文件中的记录，以隐藏其活动。这可以包括修改登录记录或事件时间戳，使追踪更加困难。

工具和技术：黑客可能会使用专门设计用于篡改或删除日志的工具和技术，例如所提到的 Zap 和 Wipe。

对于系统管理员来说，维护日志的完整性和安全性至关重要。这包括设置适当的访问控制、定期备份日志、将日志发送到安全的外部服务器以防止篡改，并实施实时监控来检测潜在的异常活动。这些措施有助于保护系统免受潜在的黑客入侵和数据泄露。

五、实验目的：

1. 熟悉 web 日志存放的默认位置，查看方式；
2. 熟悉 IIS，读懂 IIS 日志的内容；
3. 手动清除本机上的 IIS 日志。

六、实验内容：

通过 Window 本地查看系统查看 Windows 日志，并且并提取信息进行分析后进行手动删除操作。

七、实验器材（设备、元器件）：

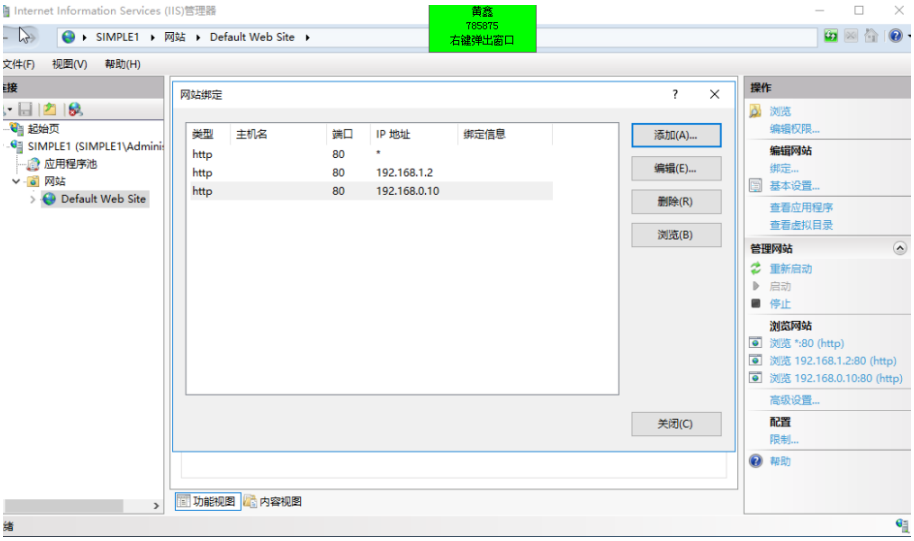
Windows Server 2016

八、实验步骤：

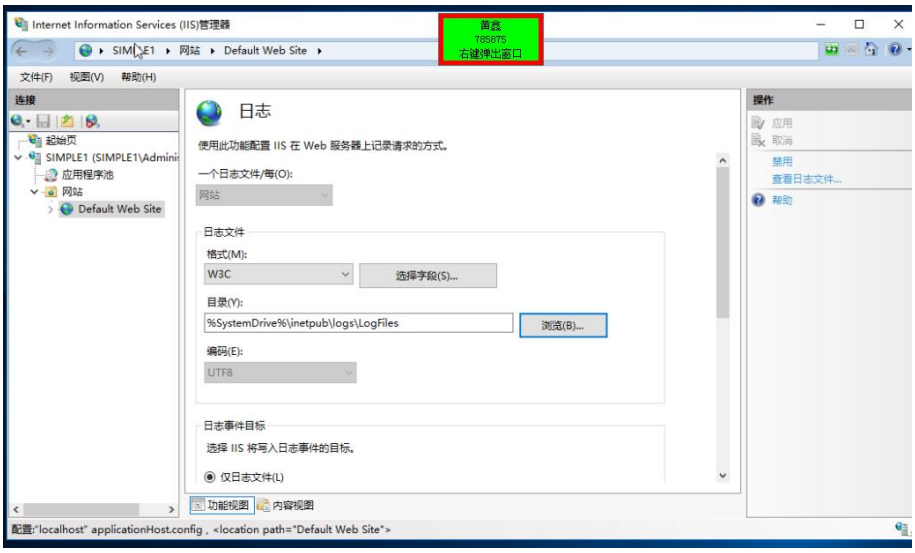
（1）首先需要安装 Web 服务器，参考实验 Web 服务器的安装与配置，安装完成.

（2） 单击“开始”→“Windows 管理工具”→“InternetInformationServices（IIS）管理器”。

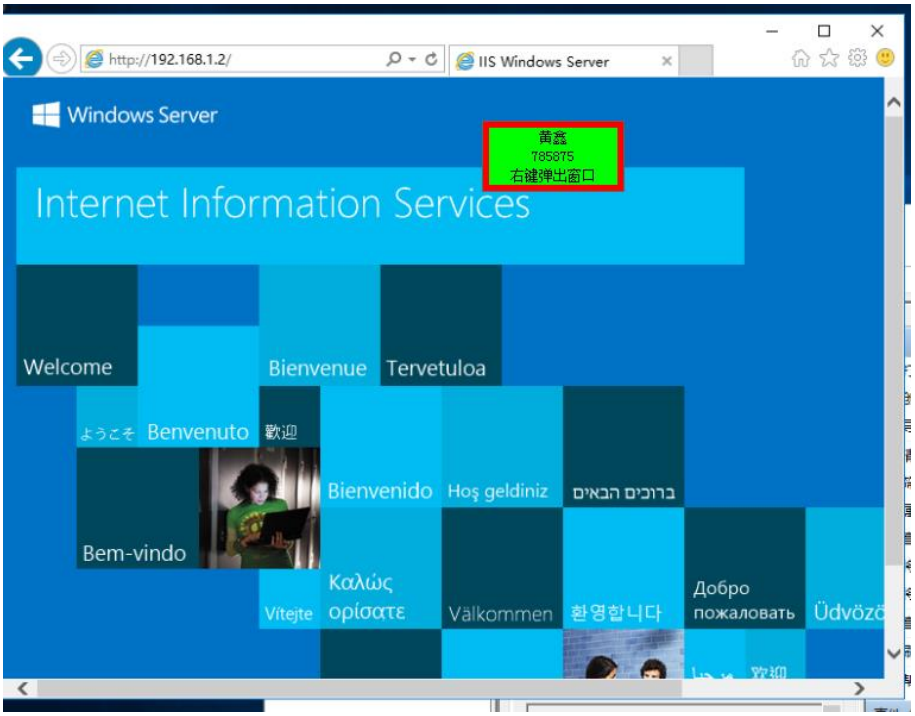
（3）在左侧中点击服务器名，点击“Default website（默认站点）”，在最右侧的选项中选择“绑定”，可以对服务器的 IP 地址进行绑定。



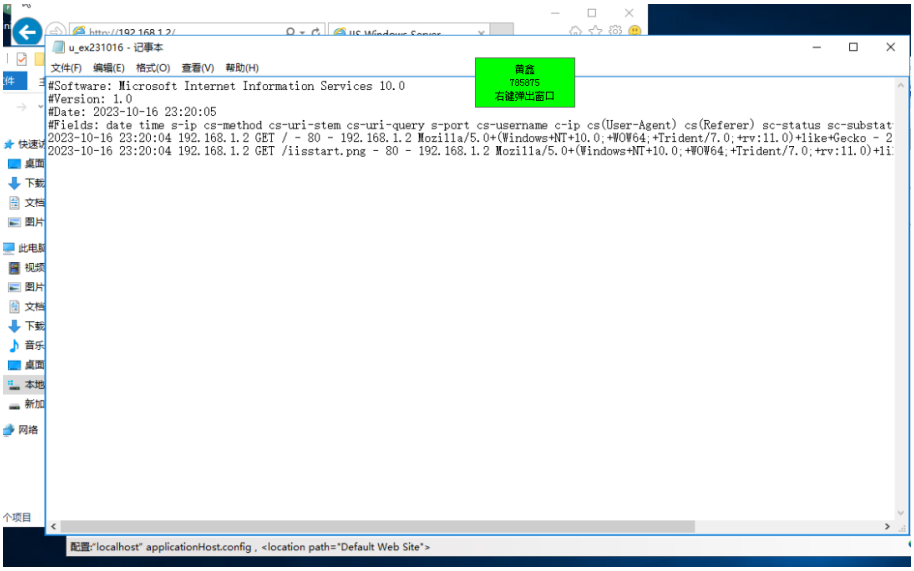
（4）点击“Default Website”后，在功能视图中，拖动滑动条，找到日志图标，双击“日志”，进入日志文件编辑状态。在该页面中可以对日志文件格式，存放位置，日志文件更新形式等进行设置。



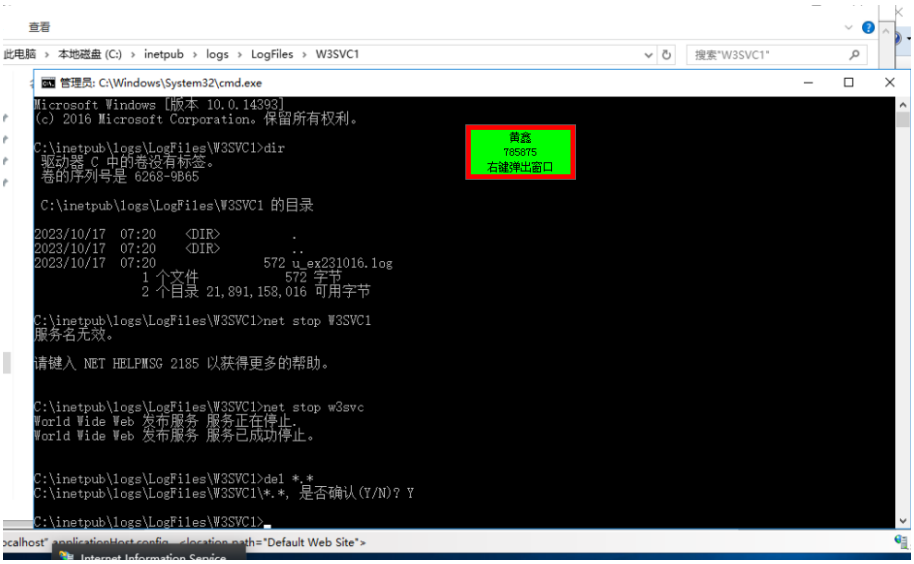
（5）首先需要访问网页 `http://192.168.1.2/` ,产生日志记录



（6）日志文件的名称格式是：ex+年份的末两位数字+月份+日期。IIS 的日志文件都是文本文件，可以使用任何编辑器打开。文本内记下了连接时间、远程客户端的 IP 地址、端口、请求动作等信息。



（7）IIS 的日志删除，右键开始，点击运行，输入 cmd，进入命令行，DOS 命令下，找到日志文件的位置，输入命令先停止 w3svc 服务，再输入删除命令



（8）回到日志存放目录下，查看日志已被删除，如图 16 所示。

九、实验数据及结果分析：

通过命令行输入删除指令手动删除日志文件，并于本地进行对比，成果删除日志文件。

十一、　实验结论：

Windows 日志可以通过手动进行删除。

十一、总结及心得体会：

这个实验着重介绍了系统日志的作用，特殊性，以及黑客可能采用的攻击手法。通过实验，我们了解了如何查看和管理 IIS 日志，并学会了手动删除日志文件。这次实验使我们更深入地认识到系统日志的重要性，以及如何采取措施保护日志文件的完整性和安全性。

十二、对本实验过程及方法、手段的改进建议：

本次实验强调了在信息安全和系统管理中，对系统日志的重要性。系统管理员需要及时监控和分析日志，以及保护它们免受潜在的黑客攻击。手动删除日志文件的过程也提醒了我们，数据的删除需要慎重，确保不会丢失重要信息。这次实验提供了有关日志管理和安全性的有益经验，有助于提高我们的系统管理和信息安全技能。

报告评分：

指导教师签字：

电子科技大学 计算机 学院

标 准 实 验 报 告

（实验）课程名称 信息对抗综合实验

电子科技大学教务处制表

电 子 科 技 大 学

实　验　报　告

学生姓名：黄鑫　学 号：2021050901013　指导教师：汪小芬

实验地点：主楼 A2-413-1　　实验时间：10.17

一、实验室名称：主楼 A2-413-1

二、实验项目名称：Windows 日志工具清除实验 1

三、实验学时：4

四、实验原理：

1. 系统日志的作用：

记录活动：系统日志文件记录了系统中发生的各种活动和事件，包括登录、文件访问、系统错误、网络活动等。

安全监控：系统管理员可以使用系统日志来监视系统的安全性。异常活动或入侵尝试通常会在日志中留下痕迹，允许管理员快速检测和应对潜在的问题。故障排除：系统管理员可以使用日志来分析问题，了解系统中出现的错误和故障，以便更好地进行故障排除和维护。

2. 日志文件的特殊性：

访问权限：通常，系统日志文件的访问权限受到高度控制，一般用户无法直接修改或删除它们，以确保日志的完整性和可靠性。

格式：系统日志文件通常遵循特定的格式，这些格式有助于系统管理员以结构化方式查看和分析日志数据。这使得日志文件与普通文本文件不同。

3. 黑客对日志的攻击：

删除日志：黑客可能尝试删除或清空系统日志文件，以消除他们的痕迹。这是相对简单的攻击方法，但通常会引起管理员的怀疑。

修改日志：更高级的黑客可以尝试修改日志文件中的记录，以隐藏其活动。这可以包括修改登录记录或事件时间戳，使追踪更加困难。

工具和技术：黑客可能会使用专门设计用于篡改或删除日志的工具和技术，例如所提到的 Zap 和 Wipe。

对于系统管理员来说，维护日志的完整性和安全性至关重要。这包括设置适当的访问控制、定期备份日志、将日志发送到安全的外部服务器以防止篡改，并实施实时监控来检测潜在的异常活动。这些措施有助于保护系统免受潜在的黑客入侵和数据泄露。

五、实验目的：

1. 了解 IIS 日志文件清除的基本原理。
2. 掌握 CleanIISLog.exe 工具的使用方法和各项功能。
3. 通过使用 CleanIISLog.exe 工具清除本机上的 IIS 日志。
4. 掌握针对日志清除攻击的防御方法。

六、实验内容：

通过 CleanIISLog.exe 工具清楚本机上的 IIS 日志，掌握针对日志清除攻击的防御方法。

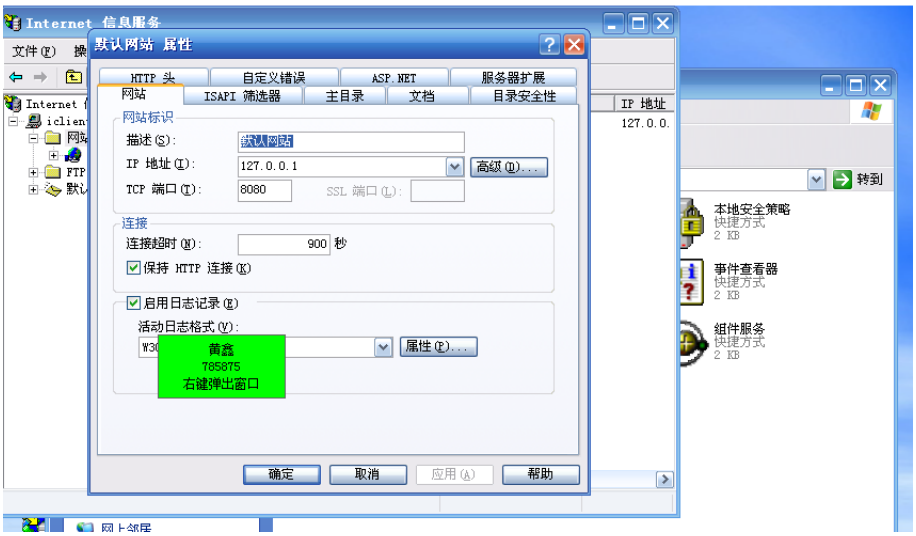
七、实验器材（设备、元器件）：

Windows Server 2016

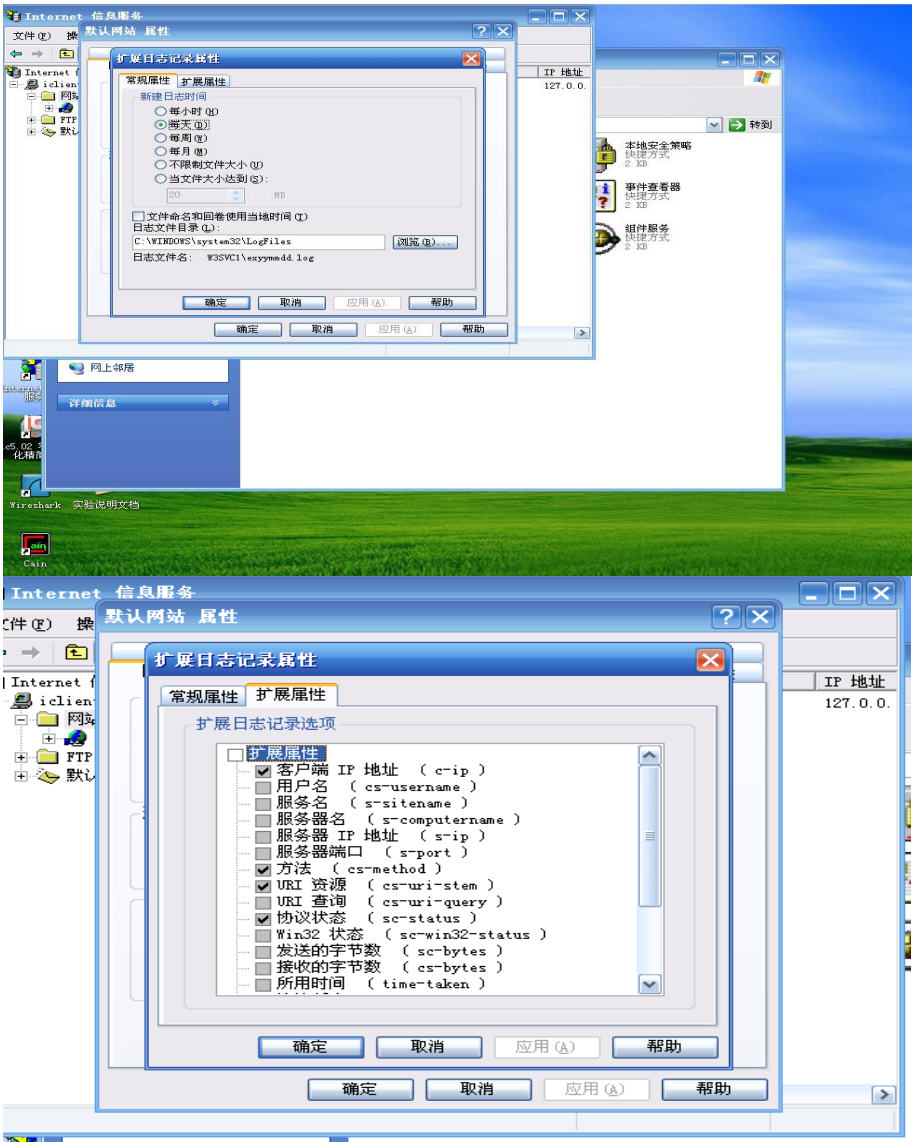
CleanIISLog.exe 工具

八、实验步骤：

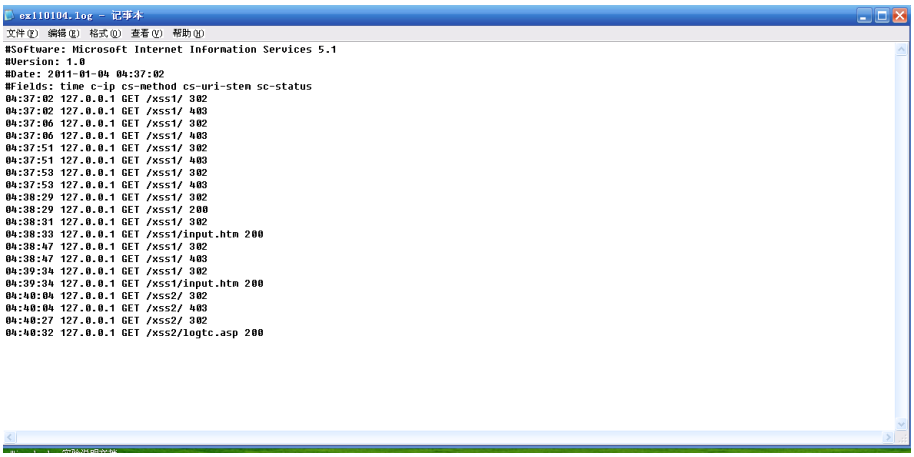
（1）获取 IIS 日志文件的存放路径和文件名通过 “控制面板”-“管理工具”-“Internet 信息服务”打开 Internet 信息服务管理器，从“Internet 信息服务”依次展开至“网站”-“默认网站”，然后右键单击选择“属性”，打开默认网站属性配置窗口。



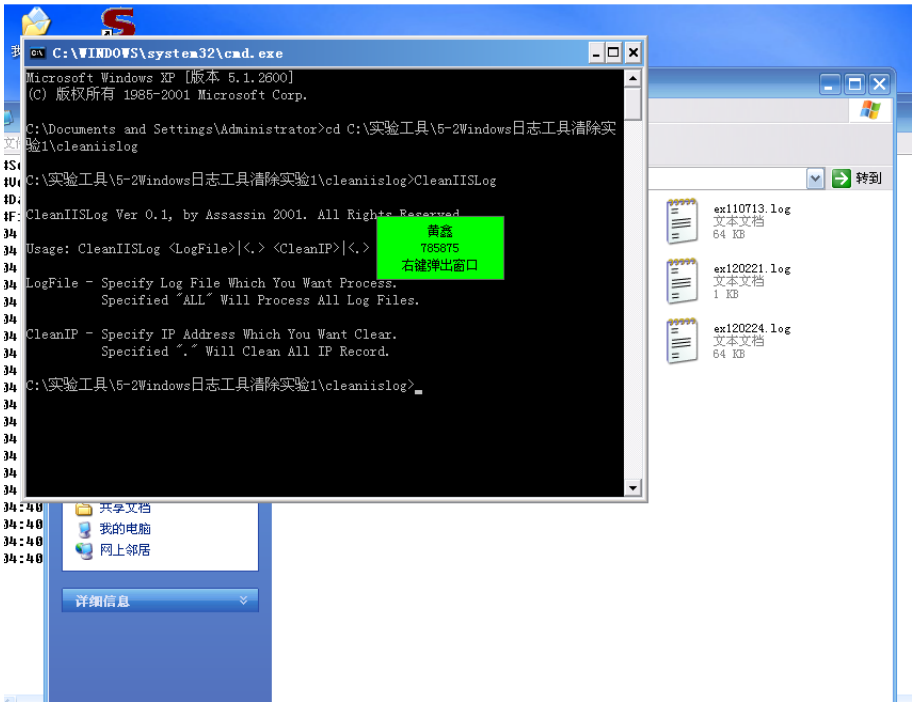
（2）查看“W3C 扩展日志文件”的保存位置。在网站“属性”配置中，如果没有启用日志记录，则在系统中不会记录 IIS 的日志，默认是启用日志记录。单击活动日志格式下面的“属性”按钮，在弹出的窗口中可以看到日志记录的保存位置，如图查看 W3C 扩展日志文件的保存位置所示，单击“扩展属性”可以查看日志记录的详细设置选项。



（3）如果在 IIS 配置中启用了日志记录，则用户在访问网站时，系统会自动记录 IIS 日志，并生成 log 文件。在本案例中直接打开“C:\WINDOWS\system32\Logfiles\W3SVC1\ex100507.log”日志文件，如图打开日志文件所示，其中包含了用户访问的 IP 地址，访问的网站文件等信息

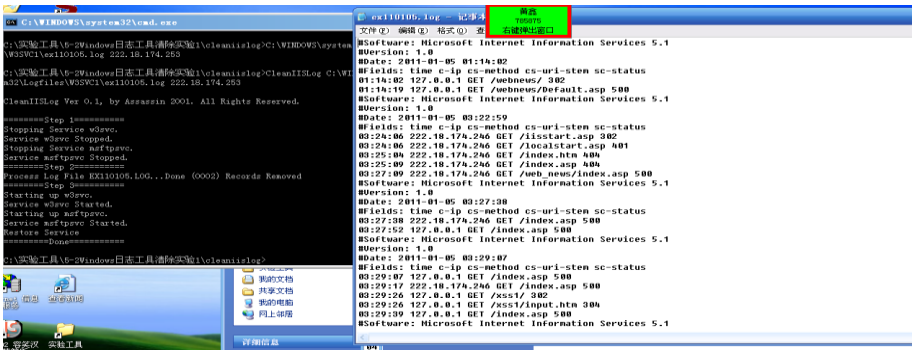


（4）测试 CleanIISLog 软件能否正常运行，启动 DOS 窗口，并到 CleanIISLog.exe 软件所在目录下，然后输入“CleanIISLog”命令；如果运行正常则会给出一些帮助信息，如图测试 CleanIISLog 软件所示；否则会提示错误信息



（5）使用 CleanIISLog.exe 清除 IIS 日志在 DOS 窗口中输入以下命令：CleanIISLog C:\WINDOWS\system32\Logfiles\W3SVC1\日志+ip，执行成功后，会提示

修改了多少处，如图 执行清除日志命令所示。如果是需要清除其他字符，则可以将 IP 地址更换为字符即可。再次打开日志文件，从中可以发现该日志中无删除 IP 地址信息，本地对应部分也被删除



九、实验数据及结果分析：

通过 CleanIISLog 成功删除日志文件后，在本地日志查看后已经不存在删除的信息。

十二、　实验结论：

Windows 日志可以通过 CleanIISLog 工具进行删除。

十一、总结及心得体会：

本次实验旨在教授关于 Windows 系统日志的重要性、作用以及如何清除 IIS 日志文件。实验提供了系统日志的原理和特殊性质，以及黑客可能采用的攻击方式。通过使用 CleanIISLog.exe 工具，我们学会了清除 IIS 日志文件，从而保护系统免受恶意攻击或数据泄露的威胁。

十二、对本实验过程及方法、手段的改进建议：

对本实验方法的改进建议包括提供更详细的背景知识，提供清晰的实验步骤和示范，增加练习机会，强调潜在风险和安全性，以及鼓励备份和还原操作。这些改进建议有助于学生更好地理解实验的背景和目的，提高实验的实用性和安全性，以及确保学生真正掌握了相关技能。

报告评分：

指导教师签字

电子科技大学 计算机 学院

标 准 实 验 报 告

（实验）课程名称 信息对抗综合实验

电子科技大学教务处制表

电 子 科 技 大 学

实　验　报　告

学生姓名：黄鑫　学 号：2021050901013　指导教师：汪小芬

实验地点：主楼 A2-413-1　　实验时间：10.17

一、实验室名称：主楼 A2-413-1

二、实验项目名称：Windows 日志工具清除实验 2

三、实验学时：4

四、实验原理：

1. 系统日志的作用：

记录活动：系统日志文件记录了系统中发生的各种活动和事件，包括登录、文件访问、系统错误、网络活动等。

安全监控：系统管理员可以使用系统日志来监视系统的安全性。异常活动或入侵尝试通常会在日志中留下痕迹，允许管理员快速检测和应对潜在的问题。故障排除：系统管理员可以使用日志来分析问题，了解系统中出现的错误和故障，以便更好地进行故障排除和维护。

2. 日志文件的特殊性：

访问权限：通常，系统日志文件的访问权限受到高度控制，一般用户无法直接修改或删除它们，以确保日志的完整性和可靠性。

格式：系统日志文件通常遵循特定的格式，这些格式有助于系统管理员以结构化方式查看和分析日志数据。这使得日志文件与普通文本文件不同。

3. 黑客对日志的攻击：

删除日志：黑客可能尝试删除或清空系统日志文件，以消除他们的痕迹。这是相对简单的攻击方法，但通常会引起管理员的怀疑。

修改日志：更高级的黑客可以尝试修改日志文件中的记录，以隐藏其活动。这可以包括修改登录记录或事件时间戳，使追踪更加困难。

工具和技术：黑客可能会使用专门设计用于篡改或删除日志的工具和技术，例如所提到的 Zap 和 Wipe。

对于系统管理员来说，维护日志的完整性和安全性至关重要。这包括设置适当的访问控制、定期备份日志、将日志发送到安全的外部服务器以防止篡改，并实施实时监控来检测潜在的异常活动。这些措施有助于保护系统免受潜在的黑客入侵和数据泄露。

五、实验目的：

1、熟悉各种日志存放的默认位置，查看方式

2、掌握 aio 清除日志的方法

3、掌握针对工具日志清除的防御方法。

六、实验内容：

通过 aio 工具进行日志清楚并且进行删除检验。

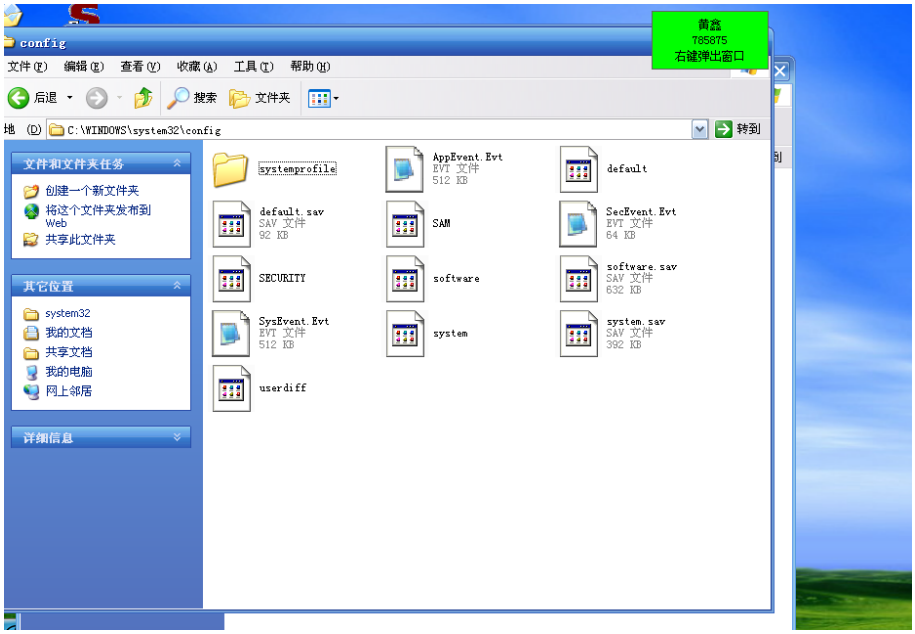
七、实验器材（设备、元器件）：

Windows Server 2016

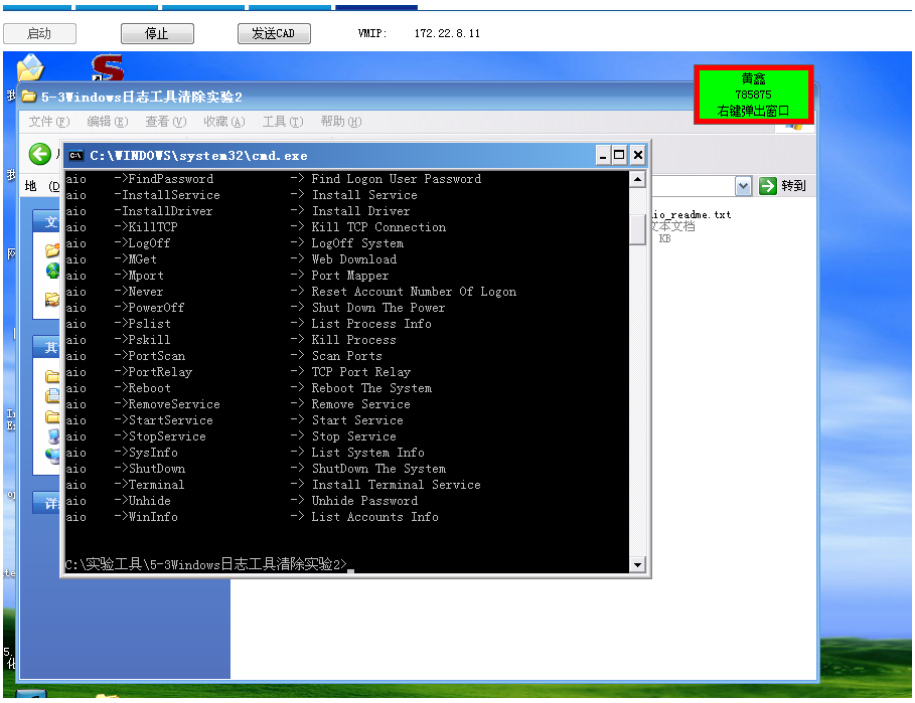
aio 日志编辑程序

八、实验步骤：

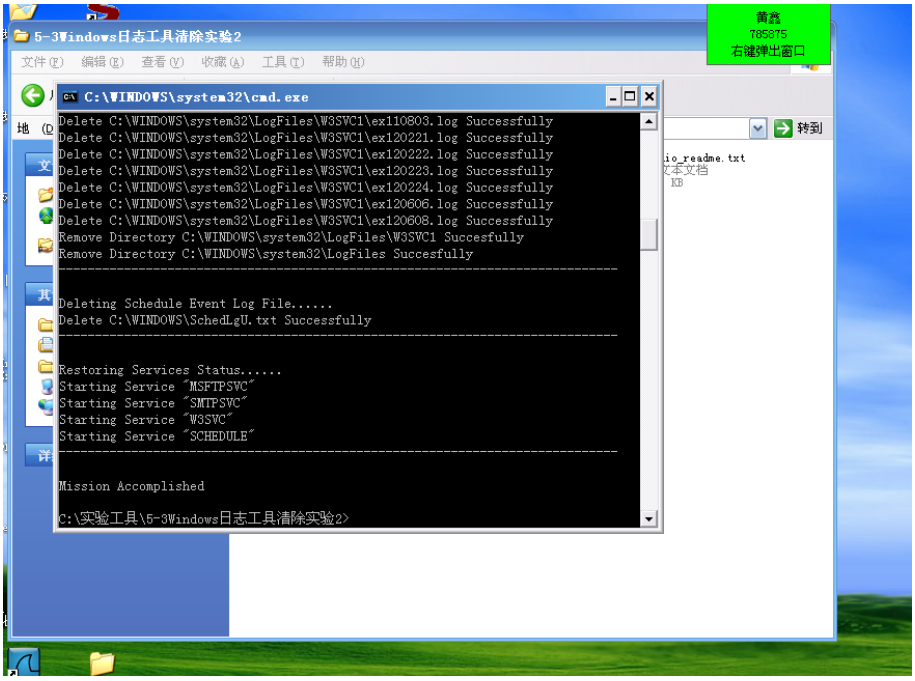
（1）查看 windows 日志，打开事件查看器（控制面板-管理工具-事件查看器），可以查看系统事件、安全日志、应用程序日志，找到系统日志、应用程序日志、IIS 日志的默认路径，系统日志、应用程序日志等默认路径在 C:\WINDOWS\system32\config 下，点击任意一个，用记事本方式打开，可以看到里面的内容。



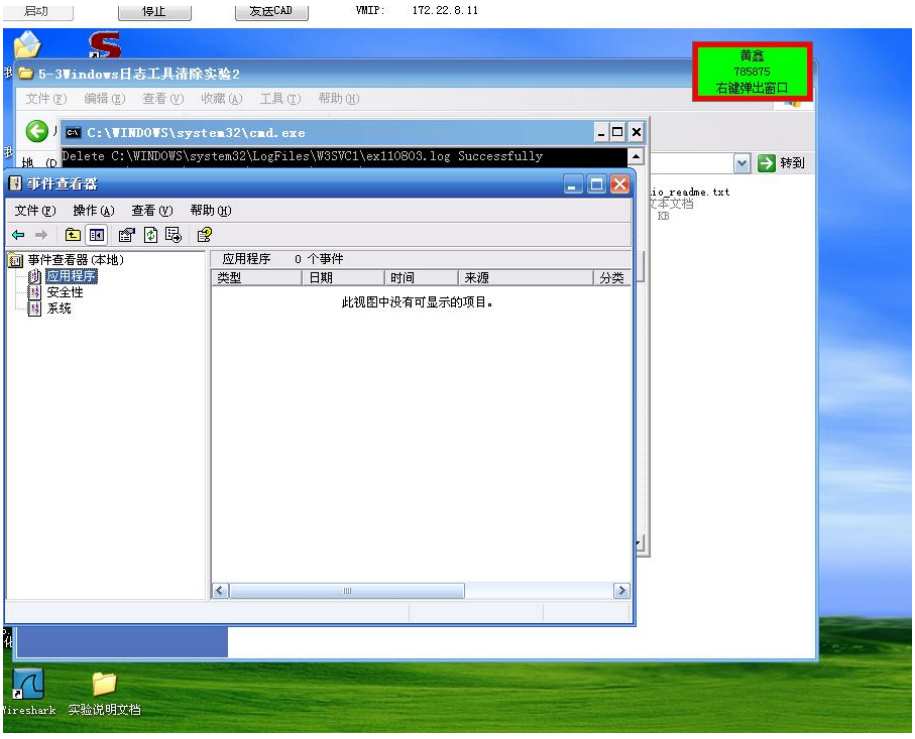
（2）运行 aio 程序，在 dos 下找到 AIO 程序所在位置，运行 aio，运行成功后，会显示所有参数及参数含义列表。

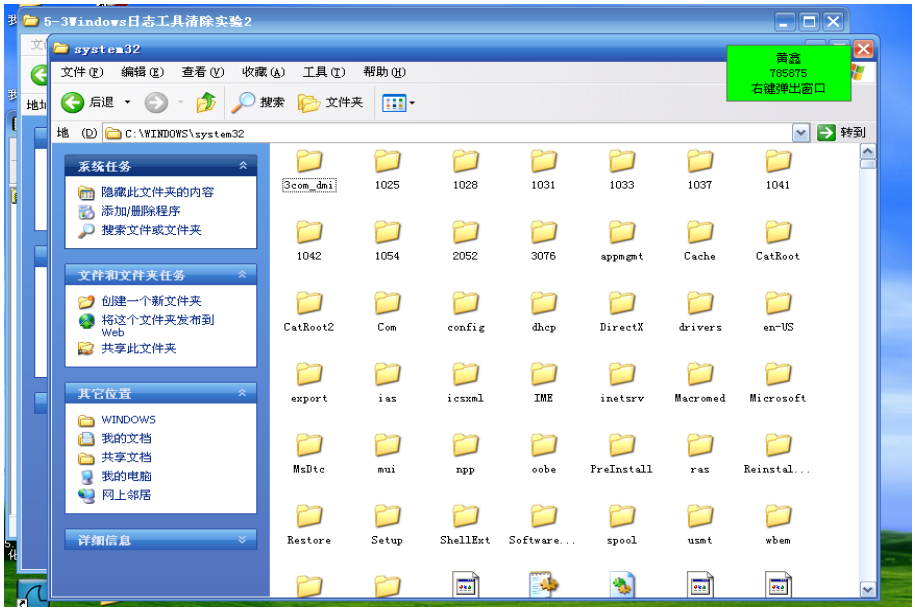


（3）运行删除日志命令，使用 aio　-cleanlog 删除默认位置的所有日志，出现日志删除命令执行界面



（4）删除检验，执行完后，在此回到事件查看器，查看目前事件情况，如图删除日志后的事件查看器情况所示，回到默认路径上，打开其中的应用程序日志，查看日志的变化情况。如图 5- 22 应用程序日志中内容变化所示；并且可以看到，默认路径下已经没有 IIS 日志所在的 logfile 文件夹了，如图没有了 logfile 文件夹所示。





九、实验数据及结果分析：

通过 aio 工具删除指令删除日志文件，并于本地进行对比，成果删除日志文件。

十三、　实验结论：

Windows 日志可以 aio 工具进行删除。

十一、总结及心得体会：

本实验旨在教授有关系统日志、日志文件的特殊性以及如何使用 aio 工具来清除日志文件。实验着重强调了系统日志的作用，包括记录活动、安全监控和故障排除。还介绍了黑客可能对日志进行的攻击方式，如删除和修改日志，以及相关工具和技术。通过使用 aio 工具，学生学习了如何清除默认位置的日志文件。

十二、对本实验过程及方法、手段的改进建议：

对本实验方法的改进建议包括提供更详细的背景知识，提供清晰的实验步骤和示范，增加练习机会，强调潜在风险和安全性，以及鼓励备份和还原操作。这些改进建议有助于学生更好地理解实验的背景和目的，提高实验的实用性和安全性，以及确保学生真正掌握了相关技能。

报告评分：

指导教师签字：