

操作系统安全实验

信息安全认知实习

授课老师：颀夏青

xiexiaqing@bupt.edu.cn

网络空间安全学院实验中心

2018年9月14日

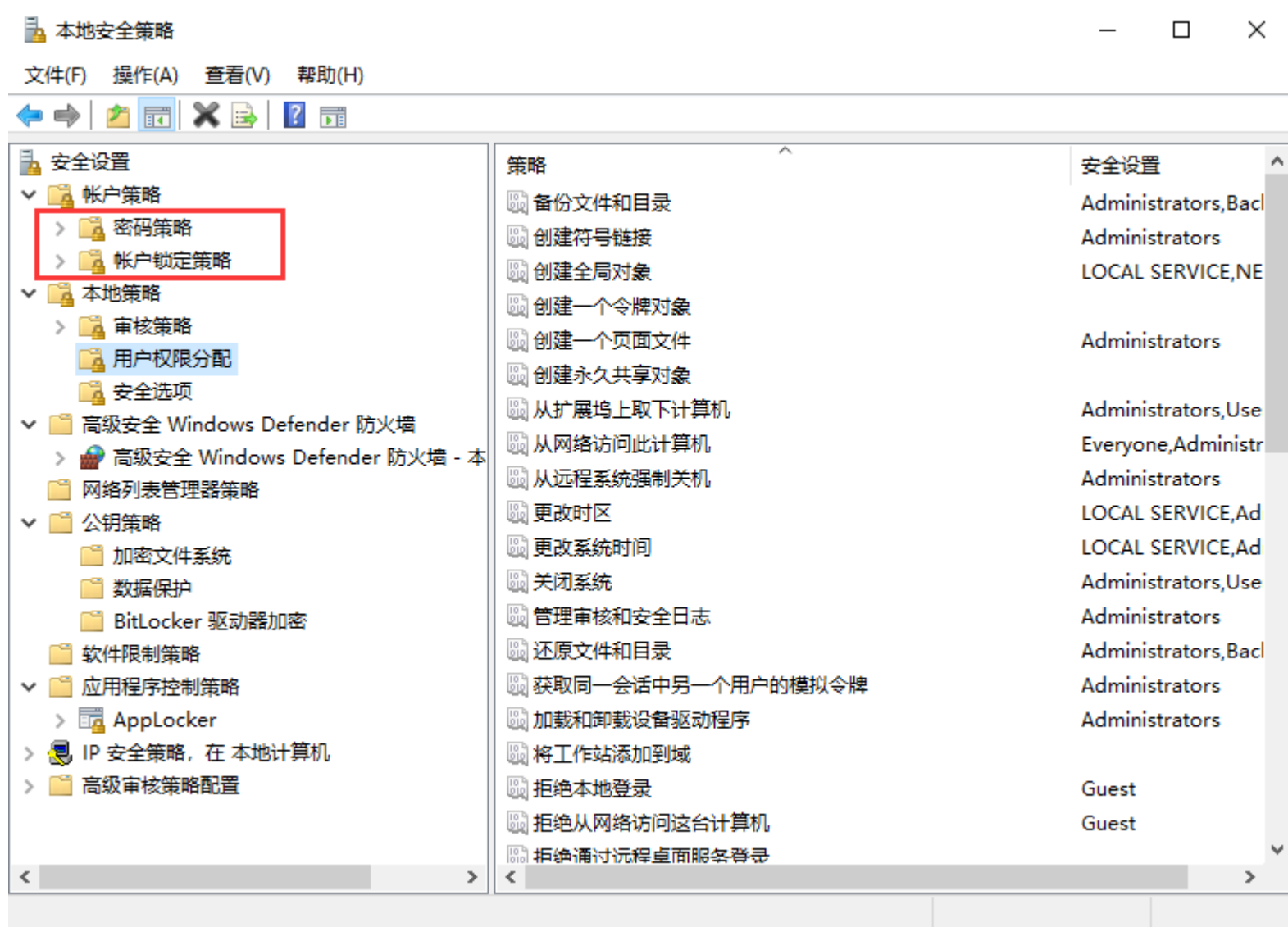
实验一：操作系统安全实验

- 请对你计算机windows系统，制定一套安全加固方案并加以配置使之生效。

至少包括以下内容：

- (1) 配置本地安全策略，如密码策略、账户锁定策略
- (2) 开启防火墙
- (3) 审核“windows日志”，查看是否有异常记录；如有，排查原因。
- 针对配置过程遇到的问题、发现的异常情况，请真实地记录你的分析过程；针对你认为值得深入研究的点，请将你思考的心得体会记录下来，完成实验实验报告。

实验一：操作系统安全实验



实验一：操作系统安全实验

The screenshot displays the Windows Event Viewer application. The left-hand navigation pane shows the 'System' log selected under 'Windows Logs'. The main pane lists several events, with event 10016 (DistributedCOM) highlighted. The right-hand pane shows the 'Operations' menu. Below the event list, a detailed view of event 10016 is shown, including its source (DistributedCOM), ID (10016), and level (Error).

| 级别 | 日期和时间 | 来源 | 事件 ID | 任务类别 |
|----|-------------------|----------------|-------|------|
| 错误 | 2018/8/7 14:55:26 | Distributed | 10016 | 无 |
| 信息 | 2018/8/7 14:25:50 | BROWSER | 8032 | 无 |
| 警告 | 2018/8/7 14:24:50 | BROWSER | 8021 | 无 |
| 信息 | 2018/8/7 14:12:39 | Service Co... | 7040 | 无 |
| 信息 | 2018/8/7 14:09:17 | Service Co... | 7040 | 无 |
| 信息 | 2018/8/7 14:08:11 | Service Co... | 7040 | 无 |
| 信息 | 2018/8/7 14:06:08 | Service Co... | 7040 | 无 |
| 信息 | 2018/8/7 14:03:38 | Ntfs (Micro... | 98 | 无 |
| 信息 | 2018/8/7 14:03:38 | Service Co... | 7040 | 无 |
| 信息 | 2018/8/7 14:03:17 | Service Co... | 7040 | 无 |
| 错误 | 2018/8/7 14:03:17 | Distributed | 10016 | 无 |
| 信息 | 2018/8/7 14:03:10 | e1dexpress | 33 | 无 |
| 信息 | 2018/8/7 14:03:10 | Power-Tro... | 1 | 无 |
| 信息 | 2018/8/7 14:03:08 | Netwtw06 | 7017 | 无 |
| 信息 | 2018/8/7 14:03:08 | Netwtw06 | 7010 | 无 |
| 警告 | 2018/8/7 14:03:08 | Time Service | 134 | 无 |

事件 10016, DistributedCOM

常规 详细信息

应用程序-特定 权限设置并未向在应用程序容器 不可用 SID (不可用)中运行的地址 LocalHost

日志名称(M): 系统
来源(S): DistributedCOM 记录时间(D): 2018/8/7 14:55:26
事件 ID(E): 10016 任务类别(Y): 无
级别(L): 错误 关键字(K): 经典
用户(U): SC-201807011105\Admini 计算机(R): SC-201807011105