**江苏科技大学**

**实 验 报 告**

课 程： 入侵检测与入侵防御

课 题： 获取审计数据

学 院： 计算机学院

学 号： 182210710119

姓 名： 陈四贵

班 级： 1822107101

指导老师： 张笑非

# 实验目的

1、编程收集主机审计数据；

2、明确主机审计数据都需要哪些，并从哪里获得。

# 实验原理

主机审计和监控系统是Bring公司根据安全计算机通常出现的安全情况，独立研发的一款专门针对安全计算机系统进行控制、监控和审计的安全产品。该系统对主机的安全防护根据保密防护分成事前、事中和事后三个步骤基本原理，采用了三大手段：控制、监控、审计,统筹考虑三个环节中可能出现的各信息泄密途径，对计算机的软硬件资源、文件系统进行集中的监控与管理。同时，为了加强涉密计算机的管理，系统内置了注册管理功能，对计算机的IP地址、部门等信息进行集中管理，实现对计算机的实时跟踪和控制。

1、IP绑定功能：

防止用户有意、无意的地址修改避免网络地址资源冲突便于故障定位责任人/计算机硬件设备 收集各客户端硬件资料，形成内部资产表客户端硬件资源进行控制，防止各种usb设备接入系统；防止用户自行安 装各种程序；

2、U盘监控：客户端计算机移动存储介质监控(MP3，MP4，U盘，手机等)，避免内部信息丢失；避免网络染毒或其他非法行为

3、进程监控：设立进程黑白名单可以禁止用户启动未授权的程序

4、服务监控：设立服务黑白名单可以禁止用户启动未授权的服务

5、上网监控：禁止客户端用户非法接入互联网，保护内网信息安全以及防止互联网病毒进入

6、非法接入监控：对接入内网的所有计算机进行审核，禁止非授权计算机接入内网，阻止非法计算机的网络行为审计类功能

7、用户监控：收集客户端计算机内所有用户信息用户创建新的账户时，系统监控密码复杂度

8、软件列表：收集各客户端已安装软件列表方便管理员排除客户端故障协同其他功能，禁用禁止软件

9、文件监控：监视客户端计算机所处理的匹配类型的所有文件记录

10、日志监控：上传客户端计算机所有系统日志，协助管理员对客户端计算机故障定位

11、共享监控：监视客户端计算机上所有共享资源

12、打印监控：监视客户端计算机上所有打印内容的标题

13、网络监控：对客户端计算机的网络连接行为进行监控，便于发现异常的网络连接，确定网络故障

14、流量统计：对客户端计算机所有网络流量进行分析记录并可以图形化显示，便于发现内网的流量异常故障

15、浏览监控：详细记录客户端计算机所浏览的全部URL，以备管理员日后审计查看

# 实验环境

Windows PC机一台、IDEA、jdk 8

# 实验步骤

1. **package** Work.GET;
3. **import** java.io.BufferedReader;
4. **import** java.io.IOException;
5. **import** java.io.InputStreamReader;
7. **public** **class** Infor {
8. **public** **static** **void** main(String[] args) **throws** IOException {
9. System.out.println(Infor.isRunning("QQ.exe"));
10. }
12. **public** **static** **boolean** isRunning(String exeName) {
13. Process proc;
14. **try** {
15. proc = Runtime.getRuntime().exec("tasklist");
16. BufferedReader br = **new** BufferedReader(**new** InputStreamReader(proc
17. .getInputStream()));
18. String info = br.readLine();
19. **while** (info != **null**) {
20. System.out.println(info);
21. **if** (info.indexOf(exeName) >= 0) {
22. **return** **true**;
23. }
24. info = br.readLine();
25. }
26. } **catch** (IOException e) {
27. e.printStackTrace();
28. }
29. System.out.println(**false**);
30. **return** **false**;
31. }
32. }

# 实验结果

# 心得与体会

在进行此实验的相关操作时，我深刻认识到了自身理论知识的局限——首当其冲的就是对审计方面的不了解。在上网查阅了相关资料后，由于与底层相关，最开始我决定使用C++编程，但参考的代码总是出现各种各样的错误，之后迫于无奈，使用了JAVA来实现获取主机审计信息。通过这次实验，一方面我认识到了自身知识的匮乏，两方面我见识了互联网环境的鱼龙混杂，三方面我见识到了JAVA的强大，获益匪浅。