1. 为增强操作系统安全性，修复OpenSSL BUG，请使用OpenSSL软件包 “/examdata/soft.iso/openssl-1.0.2k.tar.gz”完成OpenSSL升级，并确保SSH功能正常。

评分因素和命令

1)执行命令 openssl version|grep 1.0.2k,能grep 到则正确

1. 安全漏洞扫描监测到openssh需要升级安全加固到6.5及以上版本，openssh介质安装所需介质在/examdata/soft.iso下。

评分因素和命令

1. 执行命令 ssh -V >/ssh\_version.txt 2>&1
2. cat /ssh\_version.txt |grep OpenSSH\_5.3p1,能过滤到则正确
3. 写脚本监控 web站点目录（ /examdata/training/www）下所有文件是否被恶意篡改（文件内容被改了），如果有就打印改动的文件名（发邮件，可不做，只写命令），写定时任务，每3分钟执行一次。(这题建议不要了，用来做练习可以，考试太花时间）

这题需要改动，方便做评分：

监控 web站点目录（ /examdata/training/www）下所有文件是否被恶意篡改（文件内容被改了），请尝试修改/examdata/training/www/audisp/plugins.d/af\_unix.conf 文件，并执行检查文件是否有变动的命令，然后将输出信息保存到/examdata/result/check\_file\_modify里，监控方法请参考（指纹库 答案文档）

评分因素和命令

1）cat /examdata/result/check\_file\_modify|grep "af\_unix.conf: FAILED",能过滤到则为正确

1. 开启系统SYN Cookies功能，用来防范SYN攻击

评分因素和命令

1. sysctl -p|grep "net.ipv4.tcp\_syncookies = 1"，能过滤到则正确，只关注grep的内容即可，第2）点的报错不会理会

2）过滤的时候可能会有下面的报错，这是因为系统没有加载bridge模块，请忽略：

error: "net.bridge.bridge-nf-call-ip6tables" is an unknown key

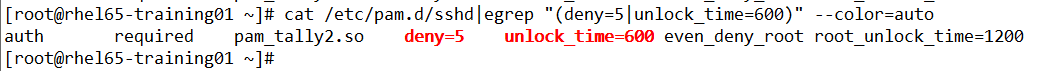
error: "net.bridge.bridge-nf-call-iptables" is an unknown key

error: "net.bridge.bridge-nf-call-arptables" is an unknown key

1. 设置系统用户登陆系统错误5次就锁定，解锁时间为10分钟

评分因素和命令

1. 执行命令：cat /etc/pam.d/login|egrep "(deny=5|unlock\_time=600)"，过滤结果含有 deny=5和unlock\_time=600的则正确



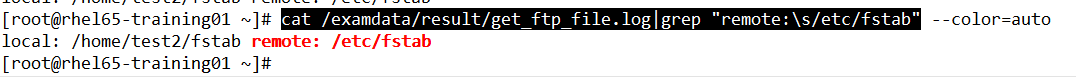
1. 使用test用户，将 /etc/ssh/sshd\_config 文件上传到它的FTP目录里

这题改为使用test2用户，将本机的 /etc/fstab 文件下载到它的FTP目录里，把下载过程中屏幕显示的日志复制到/examdata/result/get\_ftp\_file.log

评分因素和命令

1. 执行命令 diff /etc/fstab /home/test2/fstab 比较两文件是否一致，无内容输出则这一步正确

2) cat /examdata/result/get\_ftp\_file.log|grep "remote:\s/etc/fstab",通grep到 则正确，如下图所示：



3）cat /examdata/result/get\_ftp\_file.log |grep "received\sin" --color=auto ，能grep 到 received in则正确，如下图所示：

