解压密码

容器密码 `2ej)!,[JN-U;wm19J=d9sZt_L6#bf+}[`

题目链接

链接：https://pan.baidu.com/s/1iThyL6YCEM0vIRg9wvCgQg
提取码：7179

流量分析

1.计算流量包文件的SHA256值是？[答案：字母小写][★☆☆☆☆]

2.流量包长度在“640-1279”之间的的数据包总共有多少？[答案：100][★☆☆☆☆]

3.黑客使用的计算机操作系统是？[答案：windows7 x32][★★☆☆☆]

4.黑客上传文件到哪个网盘？[答案：xx网盘][★★☆☆☆]

5.黑客上传网盘的中间件是？[答案：xxxx][★★☆☆☆]

6.黑客首次登陆网盘时间是？[答案：2000-01-01 01:00:33][★★☆☆☆]

7.黑客上传到网盘的txt文件的md5值是？[答案：字母小写][★★★☆☆]

8.黑客上传到网盘的txt文件第8行的内容是？[答案：XXX][★★★☆☆☆]

9.被入侵主机的计算机名是？[答案：XXXXXXXXXXX][★★★☆☆]

10.被入侵电脑的数据回传端口是？[答案：11][★★★☆☆]

11.流量包中ftp服务器的用户密码是？[答案：abcd][★★☆☆☆]

12.流量包中ftp服务器中的木马文件的md5值是？[答案：字母小写][★★☆☆☆]

13.木马文件伪造的软件版本是？[答案：0.0.0.0][★★☆☆☆]

14.黑客上传到网盘的压缩包解压密码是？[答案：XXXXXXXXXXX][★★★★★]

15.黑客上传到网盘的压缩包内文件的内容是？[答案：xxxxxxx][★★★★★]

16.分析技术人员电脑内的手机流量包，给出技术人员的虚拟身份账号是？[答案格式:13039456655][★★☆☆☆]

17.分析技术人员电脑内的手机流量包，给出技术人员的虚拟身份密码是？[答案格式:b3039456655][★★☆☆☆]

18.分析技术人员电脑内的手机流量包，分析技术人员的看过几段短视频？[答案格式:3][★★☆☆☆]

19.分析技术人员电脑内的手机流量包，分析技术人员最后打开的软件的程序名称是？[答案格式:微信][★★☆☆☆]

20.分析技术人员电脑内的手机流量包，分析安全防护的服务器地址是？[答案格式:127.0.0.1][★★☆☆☆]

##

移动智能终端取证

1.分析卡农手机，给出手机的SDK版本？[答案格式:28][★☆☆☆☆]

2.分析卡农手机，给出手机最近开机的时间？[答案格式:2023-05-18-19:09:59][★★☆☆☆]

3.分析卡农手机，给出高德地图关联的手机号是？[答案格式:13011221234][★★☆☆☆]

4.分析卡农手机，给出卡农内部聊天工具的昵称是？[答案格式:李多余][★★☆☆☆]

5.分析卡农手机，给出卡农的真实名字可能是？[答案格式:李多余][★★☆☆☆]

计算机取证

1.黑客计算机系统安装时间是？[答案格式:2000/01/01 01:00:01][★☆☆☆☆☆]

2.黑客计算机磁盘0的总磁道数？[答案格式:数字中无标点][★★☆☆☆☆]

3.黑客计算机的产品密钥是？[答案格式:字母大写][★★☆☆☆]

4.黑客计算机共有几次卷影拷贝服务关闭事件？[答案格式:1][★★☆☆☆]

5.黑客计算机的vc容器解密密码是？[答案格式:字母小写][★★★★★]

6.黑客计算机加密容器中共有几个docx文件？[答案格式:x][★★☆☆☆]

7.黑客计算机加密容器中记录的bt币地址有几个？[答案格式:x][★★★☆☆]

8.黑客计算机加密容器中记录的受害人共有多少人？[答案格式:xx][★★☆☆☆]

9.黑客计算机中win7虚拟机中www用户的登陆密码是？[答案格式:xxxxxxx][★★☆☆☆]

10.黑客计算机中win7虚拟机中chrome浏览“bjh.com”网站保存的密码是？[答案格式:xx][★★★☆☆]

11.分析技术人员电脑，请给出电脑系统安装时间（UTC-0）?[答案格式:20000-01-01 00:00:00][★★☆☆☆]

12.分析技术人员电脑，请给出电脑内用户John的SID？[答案格式:x-x-x-x-x-x-x-x][★★★☆☆]

13.据技术人员交代，其电脑连接过nas服务器，请给出该nas服务器的iqn名称？[答案格式:iqn.xxx][★★★☆☆]

14.分析技术人员电脑，请给出该技术人员使用的隐写工具名称？[答案格式:xx][★★☆☆☆]

15.接上题，请给出使用该隐写工具隐写文件所使用的密码？[答案格式:xx][★★★☆☆]

16.据技术人员交代，其电脑内存过一个名为“财务流水.rar”的文件，请给出该文件的SHA-1?[答案格式:字母小写][★★★★☆]

APK

1.分析技术人员的模拟手机，给出安全防护的验证码是？[答案格式:11226655][★★★★★]

2.分析技术人员的模拟手机，给出安全防护的推送服务的调证值是？[答案格式:11226655][★★★★★]

3.分析技术人员的模拟手机，给出老板的联系方式是？[答案格式:11226655][★★☆☆☆]

4.分析技术人员的模拟手机，给出办公场所是？[答案格式:北京市朝阳区中山路25555号][★★★☆☆]

5.分析技术人员的模拟手机，给出技术人员聊天工具的用户ID是？[答案格式:QN11AATT][★★★☆☆]

二进制文件分析

1.分析黑客电脑，控制端程序传输协议是什么协议？[答案格式:http][★★☆☆☆]

2.分析黑客电脑，控制端程序接收数据缓冲区大小是多少？[答案格式:100][★★☆☆☆]

3.分析黑客电脑，控制端程序接收并判断几种指令？[答案格式:1][★★★☆☆]3

4.分析黑客电脑，控制端程序连接结束指令是什么？[答案格式:xxx][★★★☆☆]

5.分析黑客电脑，控制端程序配置文件解密函数是什么?[答案格式:x_x][★★★☆☆]

6.分析黑客的木马程序，该程序控制端ip是？[答案格式:127.0.0.1][★★★☆☆]

7.分析黑客的木马程序，程序在地址0x00410CA4处调用了Sleep函数，请问该函数会暂停几秒？[答案格式:3][★★★☆☆]

8.分析黑客的木马程序，该程序“png”型资源下有两张图片，程序图标对应图片的MD5值是？[答案格式:字母小写][★★★☆☆]

9.分析黑客的木马程序，哪个函数直接调用了HOST型资源？[答案格式:sub_1234][★★★☆☆]

10.分析黑客的木马程序，该程序会绕过哪个杀毒软件？[答案格式:腾讯][★★★★★]

物联

1.分析扫地机器人数据，robot1.bin采用的压缩算法是？[答案格式:xxxx][★★☆☆☆☆]

2.扫地机器人使用的软件版本是？[答案格式:0.0.0][★★☆☆☆☆]

3.扫地机器人id是？[答案格式:21243245838790][★★☆☆☆]

4.扫地机器人云证书的前6位是？[答案格式:sdfead][★★☆☆☆]

5.扫地机器人连接过的wifi的ssid是(channl1)？[答案格式:xx_xx_xx][★★☆☆☆]

6.扫地机器人连接过的wifi的密码是(channl1)？[答案格式:xxxx][★★☆☆☆]

7.扫地机器人的时区是？[答案格式:xx/xx][★★☆☆☆]

8.扫地机器人的名称是？[答案格式:xxxxx][★★☆☆☆]

9.无人机飞行纬度前两位是？[答案格式:xx][★★☆☆☆]

10.无人机的快门速度是？[答案格式:x/xxx][★★☆☆☆]

11.分析智能门锁数据包，请给出用户“wonderful”首次开门时间？[答案格式:2000-01-01 00:00-00:00][★★☆☆☆]

12.分析智能门锁数据包，请给出智能门锁MAC地址？[答案格式：字母大写][★★☆☆☆]

服务器取证

1.请分析服务器，给出NAS服务器系统账号密码？[答案格式:xx@xx][★★★☆☆☆]

2.请分析服务器，给出NAS服务器的版本信息？[答案格式:xx-xx-xx][★★☆☆☆]

3.请分析服务器，给出NAS服务器内用户SMB的邮箱？[答案格式:xx@xx][★★☆☆☆]

4.请分析服务器，给出NAS服务器系统告警服务使用的邮箱？[答案格式:xx@xx][★★☆☆☆]

5.请分析服务器，给出NAS服务器内存储池名？[答案格式:xxx][★★☆☆]

6.请分析服务器，给出NAS服务器内有几个数据集和几个Zvol?[答案格式:0,0][★★★☆☆]

7.请分析服务器，给出该NAS服务器存储监听IP和端口？[答案格式:192.168.1.1:8080][★★★☆☆]

8.请分析服务器，给出NAS服务器内iSCSI目标为web的连接所使用的启动器组ID？[答案格式:xx][★★★☆☆]

9.请分析服务器，给出web服务器连接NAS服务器所使用的iqn？[答案格式:iqn.xxx][★★★☆☆]

10.请分析服务器，给出web服务器连接NAS服务器所使用的账号和密码？[答案格式:root/123][★★★★★]

11.请分析服务器，给出redis所使用的配置文件？[答案格式:/home/1.conf][★★☆☆☆]

12.请分析服务器，给出跑分网站后台根目录？[答案格式:/xx/xx][★★★☆☆]

13.请分析服务器，嫌疑人所使用的跑分系统可能来自哪，请给出网站？[答案格式:www.baidu.com][★★★☆☆]

14.请分析服务器，给出数据库root账号密码？[答案格式:password][★★★★★]

15.请分析服务器，给出数据库备份文件存放路径？[答案格式:/xx/xxx][★★★★★]

16.请分析服务器，给出数据库备份文件解压密码？[答案格式:password][★★★★★]

17.请分析服务器，给出数据库备份文件间隔多少天会删除？[答案格式:1][★★★★★]

18.请分析服务器，给出数据库每天几点会执行备份操作？[答案格式:00:00][★★★☆☆]

19.请分析服务器，给出跑分网站后台用户余额总计？[答案格式:1000][★★☆☆☆]

20.请分析服务器，给出跑分平台后天未处理的用户申请有多少个？[答案格式:1000][★★☆☆☆]

21.请分析服务器，给出会员聂鸿熙推荐人的姓名？[答案格式:张三][★★☆☆☆]

22.请分析服务器，给出给出跑分平台内用户银行卡所属银行共有几家？[答案格式:10][★★★★★]

23.接上题，请给出这些银行中用户数最多的银行名称？[答案格式:xx银行][★★★★★]

24.请分析服务器，给出用户"祝虹雨"通过审核的充值总额？[答案格式:10][★★★★★]

25.请分析服务器，给出该跑分团队可能的办公大楼有几个？[答案格式:1][★★☆☆☆]

26.请分析服务器，给出用户John共提了几次会议预约申请，通过了几个？[答案格式:1，1][★★☆☆☆]

27.接上题，用户John哪个时间段的会议预约申请次数最多[答案格式:2000-01-01 00:00-00:00][★★☆☆☆]

28.请分析服务器，给出用户Harvey预约了什么时间的会议？[答案格式:2000-01-01 00:00-00:00][★★☆☆☆]

29.会议管理系统的后台登陆地址是[答案格式:www.baidu.com:8080/login.php][★★☆☆☆]

数据分析

1.分析技术人员电脑内银行卡交易流水，给出转入的对手交易卡号有多少？[答案格式:10][★★☆☆☆]

2.分析技术人员电脑内银行卡交易流水，给出转出的对手交易卡号有多少个？[答案格式:1][★★☆☆☆]

3.分析技术人员电脑内银行卡交易流水，给出卡号"6233542760791453"金额转出比(保留两位有效小数)？[答案格式:10.21%[提示：注意文件编码][★★★★★]

4.分析技术人员电脑内银行卡交易流水，给出金额转出比最大的卡号？[答案格式:xxxx][提示：注意文件编码][★★★★★]

5.分析技术人员电脑内银行卡交易流水，给出收益最大的卡号？[答案格式:xxxxx][提示：注意文件编码][★★★★★]