Caller ID Spoofing

pentestlab.blog/category/voip/page/4

July 14, 2014

When conducting a VoIP security assessment against a PBX (Private Branch Exchange) it is important to perform tests against all the type of attacks. One of the attacks that exist for years in VoIP is called *Caller ID spoofing* and we are going to examine it in this article.Caller ID spoofing is a type of attack where a malicious attacker will impersonate a legitimate SIP user to call other legitimate users on the voice network. The implementation of this attack is fairly easy and it can be achieved with the use of the following tools:

- Metasploit
- Viproy
- Inviteflood

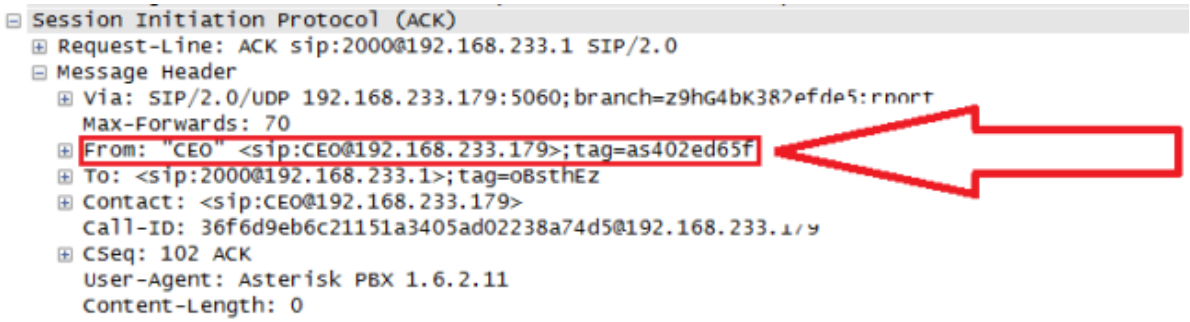
Let's see the details of this attack below.

Attack Scenario

An internal attacker is calling the Director of Finance of the company by pretending that he is the CEO and he is requesting to transfer X amount of money to his bank account. The attacker is changing the header of the SIP INVITE request in order to spoof his caller ID to CEO. The Director of Finance accepts the call as the caller ID seems to be from CEO which is considered trusted and initiates the phone conversation with the attacker.

Scenario

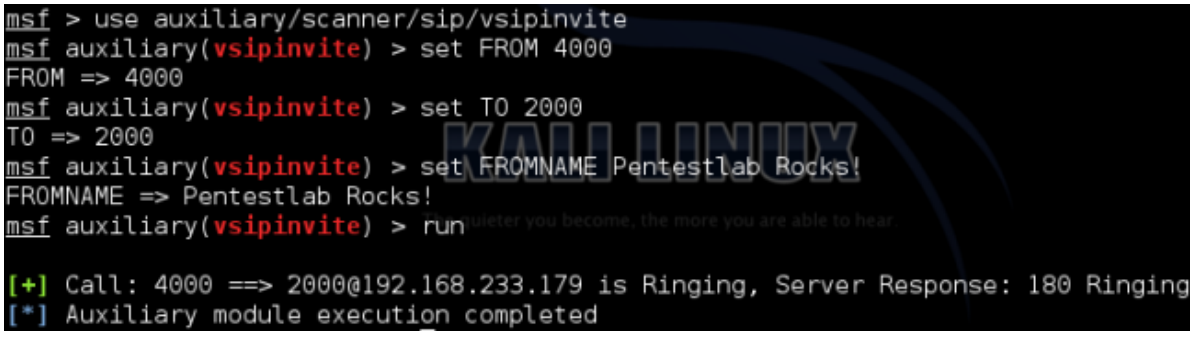
The crafted malformed SIP INVITE message can be seen below:



Now let's see how this type of attack can be conducted with the use of various tools.

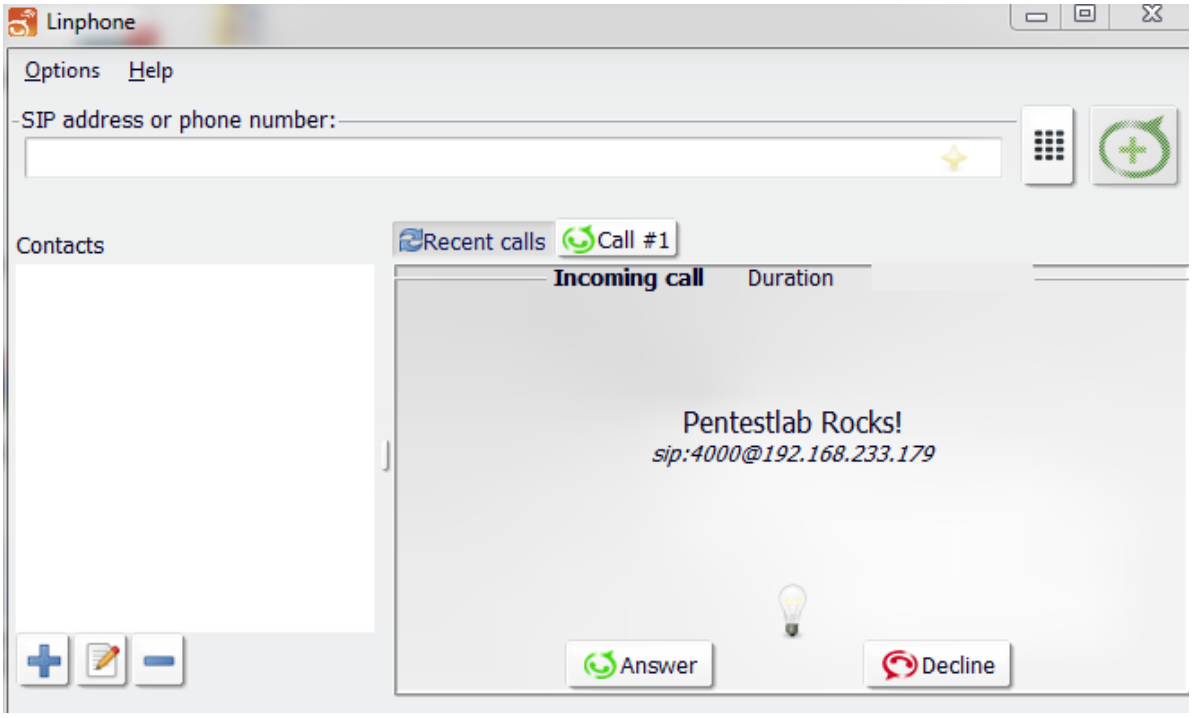
Viproy

Viproy is penetration testing toolkit for VoIP assessments. It has been developed by Fatih Ozavci and it can be loaded to the Metasploit Framework. There is a specific module that can be used for Caller ID spoofing and in the image below you can see the configuration of the module:



Spoofing the Caller ID with Viproy

This will cause the phone device to ring with the custom message of our choice even from phone extensions that are not valid.



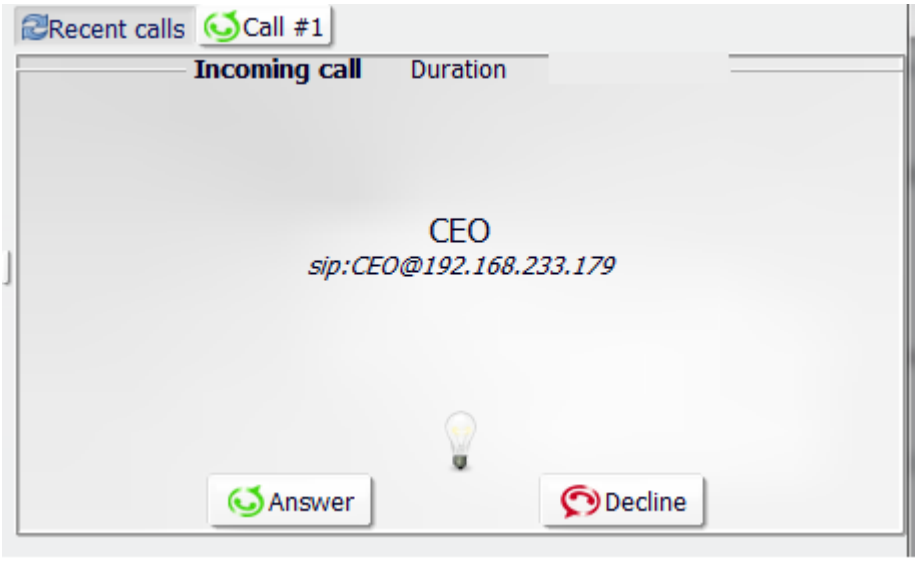
Spoofed Call – Viproy

Inviteflood

Spoofed INVITE requests can be sent and from another tool which is called inviteflood and it is part of the Kali Linux. The main purpose of inviteflood is to be used for DoS (Denial of Service) attacks against SIP devices by sending multiple INVITE requests but it can accommodate our need to spoof our ID with the following command:

Caller ID Spoofing – Inviteflood

The next image is showing the output and as we can see the phone is ringing with the ID of the CEO as per our scenario above.



Spoofed Call with the ID of CEO

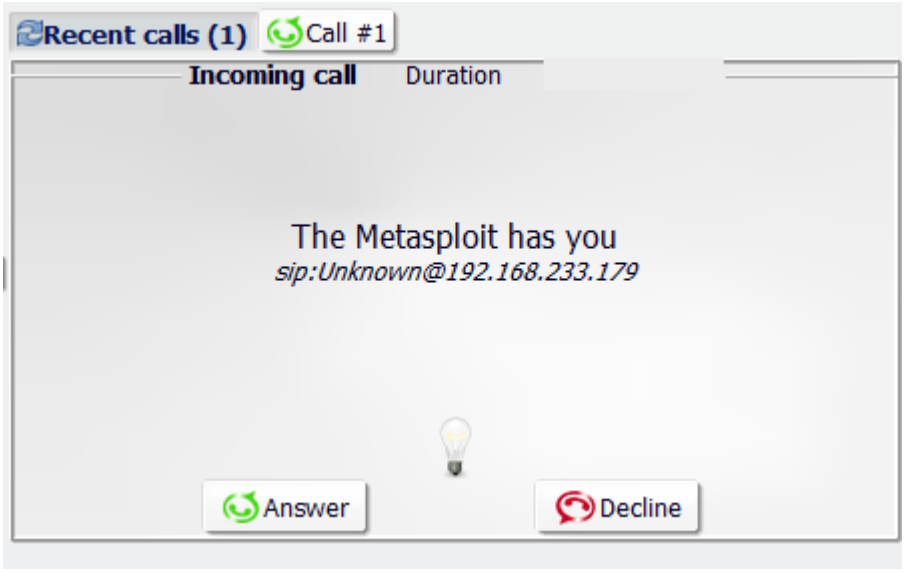
Metasploit

Metasploit framework contains as well an existing module which can send a fake SIP INVITE message to an existing extension:

```
msf auxiliary(sip_invite_spoof) > show options

Module options (auxiliary/voip/sip_invite_spoof):

   Name       Current Setting         Required  Description
   ----       ---------------         --------  -----------
   DOMAIN                             no        Use a specific SIP domain
   EXTENSION  2000                    no        The specific extension or name t
o target
   MSG        The Metasploit has you  yes       The spoofed caller id to send
   RHOSTS     192.168.233.179         yes       The target address range or CIDR
 identifier
   RPORT      5060                    yes       The target port
   SRCADDR    192.168.233.179         yes       The sip address the spoofed call
 is coming from
   THREADS    1                       yes       The number of concurrent threads

msf auxiliary(sip_invite_spoof) > run

[*] Sending Fake SIP Invite to: 2000@192.168.233.179
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Fake INVITE – Metasploit

The device will ring with the following message:



Spoofed Caller ID – Metasploit

Conclusion

In order for the attack to be successful the PBX needs to allow anonymous inbound SIP calls. It is very easy to be implemented even from people with limited knowledge about VoIP and hacking that's why systems owners need to ensure that their PBX's prevents anonymous inbound calls to reach their legitimate users in order to mitigate the risk of this attack.