Fun with Online VoIP Hacking

del.icio.us

Discuss in Forums {mos_smf_discuss:Wilson}

By Brian Wilson, CCNA, CCSE, CCAI, MCP, Network+, Security+, JNCIA

Disclaimer: This paper and the topics covered in the paper are just for educational purposes and should not be tried on a network without permission from owner of the network/service you plan on testing. I hold no responsibility for any actions or damage that might accrue if you try anything explained in this paper.

Ok... We all have heard of Vonage and the other VoIP providers that will give you unlimited phone services over your broadband connection using your regular old phone. But there are other services that are similar but have a few extra fun options. Let's take a look.

VoIPBuster

Let’s cover one of the services I have started playing with http://www.voipbuster.com/. Now for legitimate use it is a very good provider, and I have enjoyed calling friends all over the world. Now we move on to cover the dark side of online VoIP providers. One thing to think about is where the provider is located (what country). This is important because there are different laws for different countries, and, if you use the service to harass people (which is really lame), you could find yourself in real trouble. The kind of fun I am talking about is Spoofing Caller ID and also Call Bridging. This is nothing new, but I just want to write a quick paper on it to get the word out. I was informed of VoIPbuster.com from a friend of mine, so a lot of the credit for this paper needs to go out to Toxic from http://www.csthis.com/. Now that I have given credit to the person that spiked my interest with this kind of VoIP Phrecking, I can get down to business.

Here you see the “Direct” tab for call bridging www.voipbuster.com

Direct or Call Bridging

This is the act of connecting two PSTN numbers from a 3rd party. Basically this function allows you to use software to call friends by having the VoIP service call your PSTN number 1st, and, after the call on your phone goes off hook, it will auto dial the remote end PSTN number. Since both land line phones where called, neither one of the landline phones will be billed for the call. The cool thing is that caller ID is sent in both directions from the numbers called, so your phone is

ringing with your remote numbers caller ID. When you pick the line up the other end starts ringing, and they see your caller ID. So there is no trace of the 3rd party connection other than the 1st line getting an auto ringing when it goes off hook to the remote line.

This service used legitimately is very useful and cool. But if you decide to use this for fun, then you can force anyone to call anyone else, and they will have no idea what is happening. To the end caller it looks like they are getting called from the other line. This is fun to do when you are around to see the faces of the people you are forcing to call each other.

Now for the dark side. If you call someone’s cell phone, keep them online and call it again while spoofing the number to match their cell phone, it should force you into their voicemail. The trick here is that some cell providers do not set passwords to voicemail if it is called from it’s own number (even if you are prompted for a password a lot of systems have default passwords that never get changed). Other fun things to do with caller ID are spoofing your outbound ID to show something funny (like “BellSouth”). The idea here is that the sky is the limit since the PSTN is permanently hooked to the internet. I am sure we will see a lot of hacks coming to exploit the fact that the internet and phone infrastructure are now merging.

Spoofing Phone Cards

Yet another trick you can use to have fun is Phone Card Spoofing. Again there are legitimate reasons to have this kind of card. You perhaps need to call someone to give them an anonymous tip but wanted to make sure your call was not traced (the card provider could still release the call logs to law enforcement). One of the more popular spoofing card providers is http://www.spoofcard.com/. Now with the different spoofing card providers they offer different features such as:

- the ability to change what someone sees on their caller ID display when they receive a phone call
- make calls truly private
- ability to record calls
- web based control panels
- ability to change your voice on the call

www.spoofcard.com

Sniffing VoIP Calls

Now there are a few good reasons for sniffing VoIP calls like to troubleshoot VoIP routing issues or to record you own calls. Now there are also many bad things that can come out of sniffing VoIP like the fact that if you are on a open WiFi AP, others can be recording your calls and even rerouting them. There are many kinds of sniffers out on the internet for free, but the only one I trust and endorse would have to be Cain & Able from http://www.oxid.it/. With Cain & Able you can do a lot of different kinds of sniffing including the capturing of passwords, RPD sessions, SSH, Telnet and VoIP calls. Cain can do a lot more than just that, but I recommend going to their site to read more.

www.oxid.it

Cain & Able is one of the most useful tools for network auditing and testing.

As everything moves to the internet there, will be many helpful advances in the way we live. But keep in mind that with every new convenience, there are risks associated with it. If you have any questions about VoIP or anything covered in this paper, feel free to Google your question first, and then join me in the forums here on www.ethicalhacker.net.

First picture of VoIP system curtesy of http://www.trust.com/products/info/voip/.

Brian Wilson (bwilson@ethicalhacker.net) has over 12 years experience in IT starting with a tour in the United States Army. He has worked in and out of the US Government in many different organizations and technical roles including a stint as a Cisco Certified Instructor. Currently he works for one of the largest US broadband providers (ISP) as a Senior Data/Voice Engineer supporting over 3 million High Speed Internet/ VoIP subscribers. He has attained a number of industry credentials covering many aspects of IT including CCNA, CCSE, CCAI, MCP, JNCIA, Network+, Security+, and many DoD Certifications. He also uses his knowledge of IT to benefit a number of charitable organizations. Clearly Brian's knowledge and interests are wide, and his affinity for philanthropy will be the overiding theme of his vast set of articles and videos.