CyberSecurity Reloaded: Ultimate Caller ID Spoofing

Ramiro Gonzalez

Delivery Date : January 30, 2020

At the end of this project you will be able to develop social engineering attacks and deploy them using caller ID spoofing. Terminology such as **spoofing**, **vishing**, **attack vector**, and **Open Source Intelligence** (OSINT) will be defined. From now on you will be able to protect yourselves from malicious actors

Disclaimer

Improper use of the following information may lead to legal trouble. Using the following information for malicious purposes will get you arrested and prosecuted to the full extent of the law.

When performing attacks make sure to have explicitly written permission otherwise contact your lawyer and tell your kids, friends, family and mistress that you may not be around.

Background

Successful phishing campaigns relies on having a large emailing list and acting as a reliable source (**spoofing**), and voice phishing is no different (**vishing**). First we must design an attack vector using the internet to find freely available personal information about our target (**OSINT**), so that the target is more likely to fall.

The following activities will show you how to use automated systems to manage your **vishing**(Voice Phishing) attacks.

Material

- ☐ Computer/Phone
- ☐ Pen or pencil
- ☐ Internet Connection
- ☐ Ethical Foundations

Rules and Guidelines

Those who are assigned an even number will pair up with an odd number. Even numbers will take on the role of a *Malicious actor* and odd numbers will take on the role of *target* for the first round.
Please follow instructions carefully, do not read ahead

Disclaimer

1. Do not investigate individuals, websites, or servers or conduct any illegal activities on any system you do not have permission to analyze.
2. Information provided in **CyberSecurity Reloaded** workshop is for educational purpose only.
3. We will not be responsible for any direct or indirect damage cause due to the usage of information provided.

Task 1

With your partner set terms, conditions and ask for permission.

Signature: _____

Signature: _____

Information Gathering

In order to simulate a vishing related scenario, we must take into account *human error*, convenience, and social norms. *Social norms* instruct people on how to react in social situation, such behavior is effective for avoiding socially awkward situations. It is easier to say "yes" than to say "no" because refusing to do something requires an explanation, therefore people will say "yes" for convenience and because it is a social norm to be polite.

Task 2

Let's play a game.

- ☐ If you wrote your name on the name tag (you lost).
- ☐ If you stood up you lost.
- ☐ Write your name below if you won.

.

Open Source Intelligence

A digital footprint is established the moment one connects to the internet. Regardless of how skilled you are advanced methods exists to recover that trail of data. In this task we will be using "soft skills" to gather information.

Task 3

- ☐ Go around and collect as many names as possible.
- ☐ Using the search engine of your choice try to find the meaning of some name(s).
- ☐ Find etymology and history of your partners name and craft a attack vector.

.

Spoofing

There are many forms of spoofing, the most common and readily available is caller ID spoofing. Note: SMS spoofing is not readily available. In this task you will simulate caller ID Spoofing.

Task 4 (Malicous actor)

- ☐ Get your phone ready.
- ☐ Head to https://bluffmycall.com/
- ☐ Follow instructions
- ☐ Deploy your attack vector created in task 3. Take not of information gathered.

Task 5

- ☐ Malicious actor becomes target
- ☐ Target becomes malicious actor
- ☐ Refer task 4

Notes

.