DNS Cache Poisoning Attack

Federica Consoli - 1538420

April 22, 2018

Abstract

The goal of the assignment was to simulate a DNS Cache Poisoning attack. In this report I will discuss the steps taken to prepare for the hack, how it was implemented and what results were obtained.

1 Getting started

The idea behind this hack is to make the DNS accept a specially forged packet. By design, a DNS accepts a response packet only if it matches one of its pending queries. For this to happen, the following conditions need to be satisfied:

- the response arrives on the same UDP port it was sent from
- the response's query ID matches the one of the pending query
- the response's question section matches the one of the pending query

The first step is, of course, to obtain the query id and the source port from the DNS server.

In order to obtain these two information, I decided to use two sockets: one to query the DNS server and one to obtain its answer. The first sockets connects to the IP address of the DNS server on port 53, while the second one is listening on the same port, only this time on my machine.
I then crafted a query packet for the DNS, asking it to lookup the address for *badguy.ru* (which corresponds to my machine's address), and sent it to the DNS server via the first socket: within milliseconds, I received the information I needed on the second socket.

Using a similar approach, I queried the DNS server for the IP address of the name server responsible for the victim's domain. This step is necessary because

```
niccals@niccals-laptop:~/Desktop/DNS_Attack$ sudo python script.py
Listening on port 1337, waiting for secret...

QUERY ID: 26078 ; SOURCE PORT: 38561
The name server for ns.bankofallan.co.uk is at 10.0.0.1
```

Figure 1: First steps

the source ip for the forged DNS responses needs to be spoofed, or else the response would not be accepted by the DNS, since it is not coming from an authoritative server for the targeted domain. Once I obtained the IP address, I added it as a static address for one of my machine's interfaces using the command `ip addr add 10.0.0.1 dev lo`, which later allowed me to perform the spoofing.

2 The program