DNS Spoofing Application

User manual

Danny Lieu

2018

Table of Contents

[Diagram 2](#_Toc515752426)

[Description 2](#_Toc515752427)

[Pseudocode 2](#_Toc515752428)

# Requirements

In order to run this application, the machine need to have the following requirements:

* Python 2.x.x (prefer Python 2.7.10)
* Root privilege to run the script
* The machine that DNS requests are directed to has HTTPD service running.

# Configuration

Go to /etc/httpd/conf and open the file httpd.conf. We will look for the line that is Listen 80 and add one more line Listen 443 as the following:

# Usage

First of all, scapy module is required in order to run the application. To install scapy, type the following command:

root$ pip install scapy

In order to run the application, victim IP address and router IP address are required. Here is the application usage:

python DNSSpoofing.py -v VICTIM [-l LOCAL] -r ROUTER [-re REDIRECT]

Required arguments:

|  |  |
| --- | --- |
| -v <victimIP>, --victim <victimIP> | IP address of the victim |
| -r <routerIP>, --router <routerIP> | IP address of the router |

Providing one of the following arguments:

|  |  |
| --- | --- |
| -l <localIP>, --local <localIP> | IP address of the local machine. Specify this one if forwarding DNS requests to the attacker machine. |
| -re <redirectedIP>, --redirect <redirectedIP> | IP address of where victim’s DNS requests will be directed to. |