DNS Spoofing Application

User manual

Danny Lieu

2018

Table of Contents

[Diagram 2](#_Toc515752426)

[Description 2](#_Toc515752427)

[Pseudocode 2](#_Toc515752428)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Test # | Description | Tools used | Expected results | Actual results | Status |
| 1 | Application parse all user input from command-line arguments. | Python | Get all input from user and print out. | Victim IP, router IP and redirected IP are printed out. | Passed. See below for more details. |
| 2 | ARP poisoning the victim machine | Python, Wireshark | The victim machine sees the attacker machine as the router | Running Wireshark, the victim machine receives ARP packet indicating the attacker machine is router | Passed. See below for more details. |
| 3 | DNS Spoofing a normal website such as google.com | Python, Firefox | The victim will be lead to the fake website running on the attacker’s Apache server. | The victim go to the fake website. | Passed. See below for more details. |
| 4 | DNS Spoofing a high security website such as facebook.com | Python, Firefox | The victim will be lead to the fake website running on the attacker’s Apache server. | Firefox shows the error indicating SSL is SSL\_ERROR\_RX\_RECORD\_TOO\_LONG | Failed. See below for more details |

# Test outline

# Test description

## Test #1

Application parse all user input from command-line arguments.

## Test #2

ARP poisoning the victim machine

## Test #3

DNS Spoofing a normal website such as google.com

## Test #4

DNS Spoofing a high security website such as facebook.com