DNS Spoofing Application

Design work

Danny Lieu

2018

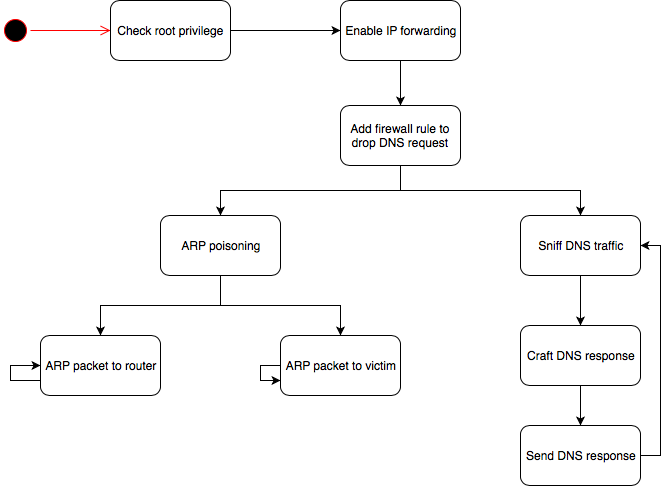
Table of Contents

[Diagram 2](#_Toc515752426)

[Description 2](#_Toc515752427)

[Pseudocode 2](#_Toc515752428)

# Diagram



# Description

* Check root privilege: check if the user is the root user
* Enable IP forwarding: enable IP forwarding to act as a router
* Add firewall rule to drop DNS request: drop any DNS packet to prevent DNS lookup
* ARP poisoning: start a new thread and do ARP poisoning
* ARP packet to router: send ARP packet which pretend to be the victim machine to router
* ARP packet to victim: send ARP packet which pretend to be the router to victim
* Sniff DNS traffic: sniff for any UDP traffic to port 53 (DNS)
* Craft DNS response: craft a new DNS packet which will be sent back to victim
* Send DNS response: send the new DNS packet to the victim

# Pseudocode

*DNS Spoofing*

*Check if user is root user*

*Enable IP forwarding*

*Add firewall rule to drop DNS request to port 53*

*Start ARP poisoning thread:*

*While True*

*Send ARP packet to router*

*Send ARP packet to victim*

*Endwhile*

*Start sniffing thread:*

*While True*

*Receive DNS request from the victim machine*

Craft a new DNS response to match DNS request

Send back DNS response to the victim

Endwhile