8505 Assignment 4 Design

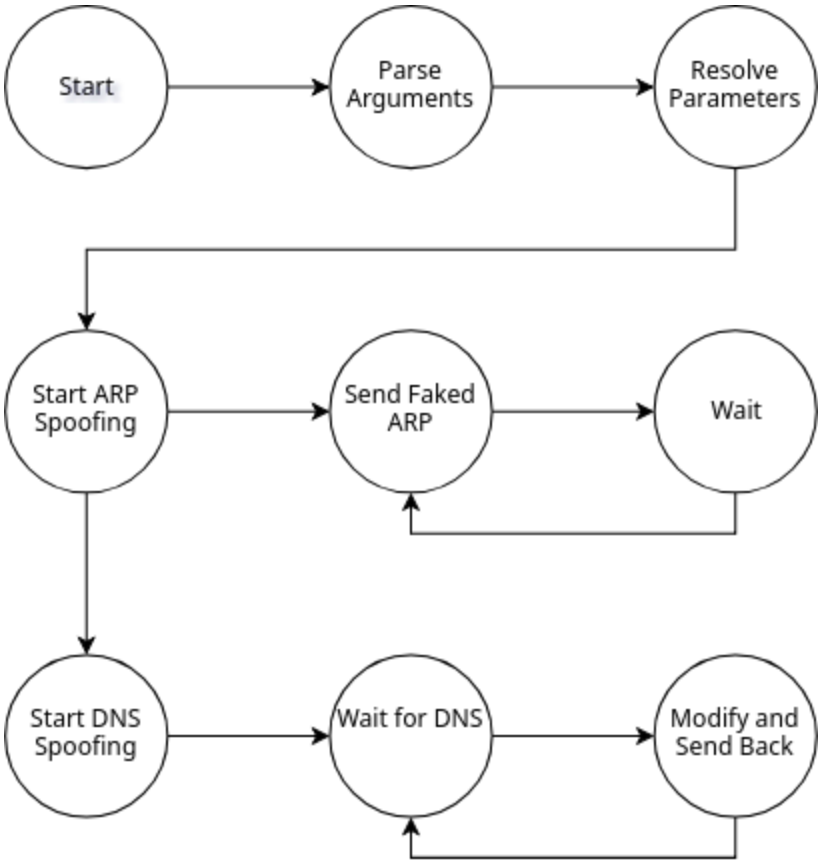
A thoroughbred mustang DNS server

Isaac Morneau; A00958405

Design Note

As can been seen in the FSM below this DNS spoofer is very quick due to the fact that there is no packet generation. Instead the packets are read in, modified, and sent back. This skips a lot of otherwise This, in practice is between 10 and 40 microseconds faster than the normal double buffered approach.

FSM



Pseudocode

Start

Initialize the program
Goto Parse Arguments

Parse Arguments

Ensure that the target, the redirection, and the interface have been specified
Goto Resolve Parameters

Resolve Parameters

From the passed parameters get the MAC addresses and IPs as needed
Goto Start ARP Spoofing

Start ARP Spoofing

Create the ARP packets
Make a new thread
On the new thread
Goto Send Faked ARP
On the main thread
Goto Start DNS Spoofing

Send Faked ARP

Send the premade arp to the poison client
Send the premade arp to the gateway
Goto Wait

Wait

Wait for 1 second to avoid DoSing the client
Goto Send Faked ARP

Start DNS Spoofing

Initialize the buffers
Set the socket filter to only capture dns requests

Goto Wait for DNS

Wait for DNS

Read in the dns packet
Goto Modify and Send Back

Modify and Send Back

Append the response data to the buffered packet
Set the flags to be response
Swap the source and dest information
Recalculate length and checksums
Send packet back out
Goto Wait for DNS