

DNS SPOOFING

**2003A53001 P. Shashi Preetham**

**2003A53010 M . Koushik**

To

**Dr. Sampath Kumar Tallapally**

Assistant Professor

in

School of Computer Science And Engineering

**01 . ABSTRACT :-**

Domain name system is among the core part of TCP/IP protocol suite and the standard protocol used by internet . The domain name system consists of mapped website names with internet protocol , which facilitates the browsing by not requiring the users to remember the numeric notation addresses . Nature of system which involves the transferring of information in plain – text , makes it vulnerable to security attacks . DNS suffers from the suffering from spoofing & cache poisoning the attacks that are intended to steal the private information of users . Proposed to prevent the aforementioned attacks by using an asymmetric cipher to encrypt the important data / information in messages and to protect these messages from manipulation . These implemented and examine in the Linux platform and C programming languages , this protects the DNS against the spoofing and poisoning attacks while resulting the delay in time comparing with applied DNS .

**02 . INTRODUCTION :-**

To know better about the DNS Spoofing Let’s get some questions about it to know briefly about them :-

a) What is DNS Spoofing?

b) What is meant by DNS Spoofing?

c) Why is DNS Spoofing is a problem?

d) How to prevent a DNS Spoofing?

e) Explain some example attacks of DNS Spoofing?

First of all what is DNS Spoofing it is an combination of two words i.e., DNS & Spoofing –

“DNS is the term Domain Name System that translates human readable domain names for (example [www.amazon.com](http://www.amazon.com) to machine readable IP address i.e., 192.0.2.44” ).

“Spoofing is the term that indicates the threat actor is using a malicious site that resembles the official website a user knows” .

Since DNS is an critical part of internet that communicates , poising entries give an attacker perfectly do the phishing attack scenario to collect the sensitive data . So first let’s know about the “phishing attack it is a form of social engineering where attackers deceive people into revealing the sensitive data / information / installing the malware such as ransomware” .

Because users often fall victim to do phishing attack in a DNS Spoofing attack, to threat a data to privacy . Privacy spoofed data depends upon the attacker goals to explain we take an example to know better that is an attacker wants to steal banking information , the first step to find a popular banking site , download the code and stealing the files , passcodes , login credentials , money etc., and upload there malicious machine used to hijack the connections of overall bank system .

Any user’s that access the internet from public wi-fi is vulnerable to DNS spoofing to protect the

DNSSEC(Domain Name System Security Extensions Cryptographic) –> These includes some of the forms they are “lack of data confidentiality , complex deployment , zone enumeration” which adds the cryptographic digital signature that entries required by resolves before they accept DNS lookups as authentic .

Standard DNS is not encrypted these it’s not programmed to ensure that changes & resolved the changes and resolved the lookups are form legitimate servers & users that acts the digital signatures that has the component of process that verifies the updates and ensure the DNS spoofing is blocked that threatens to breach user data privacy across any public Wi-fi or any public internet access to the mobile or a system .

There are different types of DNS Spoofing attacks that are used for the hijacking the login credentials , passwords of the user’s who are accessing their websites that have malicious information into it &they also called as methods of DNS Spoofing .

* Email Spoofing :-

These tricks user’s into believing the email came from someone that they were not known . these spam can be done in phishing attacks to take the risks and tricks the user’s to have messaging between two or more user’s via client server model/technique and takes the sensitive data i.e., face id , passcodes etc.,

By the statistical data from all the nations that have given the information 3.1 Billion domain spoofing emails are sent on each day that is more than 90% of cyber attacks to start the email phishing attacks & estimated that throughout worldwide it costs the $26 billion since 2016 . In 2019 the FBI reported that the 467,000 cyber attacks were successfully and 24% of them were email based attack , the average scam tricked user’s out of $75,000 as an fraud or manipulated from the user’s data into it .

* Website / URL Spoofing :-

It is an fraudulent link that is masked to look like a legitimate source in order to steal the data from the user’s , sometimes by clicking the spoofed URL is enough to infect the device with malware other times the website will be designed to look identical to one other trust of it.

* Caller id Spoofing :-

These is a practicing of causing the telephone network that indicates the receiver of a call that the originator of the call is a station other than the true originating station of it is said to be caller id spoofing.

* Text message Spoofing :-

It involves the altering the sender information for fraudulent purposes , such as a phone number and a contact name that results fake text cannot be responded or blocked the based entirely on the text form to have closer inspection on it.

* Man-In-The-Middle attack :-

These type of attack can be seen in the cryptography and computer security that results the when perpetrator positions himself in a conversation between a user and an application that eithers the eavesdrop or to impersonate one of the parties, making them appear as if they were normal exchange of information is underway .

* ARP Poisoning :-

ARP Introduction : ARP or Address Resolution Protocol defines the mapping from "network" layer [MAC layer] to the "link" layer [IP/TCP layer]

Each system on a network maintains its own ARP table, which keeps on updating at regular intervals of time

Continuos updates to the ARP table are done by making use of the information catered from the received packets from all the nodes communicating to this machine.

Thus ARP poisioning can be readily implemented by sending a deceived ethernet packet containg the ARP packet, which misguides the destination system about the MAC address of the source it assumes the packet has been received from.

Goal : To modify the ARP table of the targeted machine.

Prerequisites : No support is expected from the targeted machine for the poisioning, but it does require the IP addresses of both the machine being poisoned as well as the IP address of the corresponding entry of the ARP table.

Strategy : The ARP packet can either be sent directly to the targeted machine or be broadcasted(broadcasting is more preffered or else the differences in the IP-MAC mapping of the systems in a network results in poisoning being caught).

Consequence : All the packets routed towards the victim by the target are caught by IP spoofing system(because of the MAC address)

Any personal communications without private key encryption techniques can be easily tracked of, thus destroying the privacy . Man in the middle attack is the greatest threat on security that follows:-

- Implemented ARP poisioning,

Source code : arp\_poisoning.py

ARP packets constructed through socket module only, are contained in the ethernet packet, and sent to the destination/broadcasted

ARP header contains our MAC address, target IP and victims IP.

MAC address need not be typed in by the spoofer, as it is automatically picked up by using some functions of "netifaces" module is implemented, but is not mandatory

Test command : sudo python arp\_poisoning.py "victim\_ip" "target\_ip"

Note : "netifaces" module needed beforehand

* HTTP spoofing :-

Spoofing is a situation in which a program successfully masquerades as another by falsifying data and thereby gaining an illegitimate.

Goal : Spoofing HTTP requests to a server by creating a

TCP handshake session and then sending a simultaneous ack-get

packet to successfully complete the handshake and receive a response.

Prerequisites :

Strategy : Check the refferer header of the HTTP request, and then implementing the neccesary modifications

Consequence : Allows users to gain unauthorized access to the materials in situations where ip\_address based authentication is used

- Implemented HTTP spoofing,

Source code : http\_spoofing.py

Test command : sudo python spoofed\_ip server\_ip port

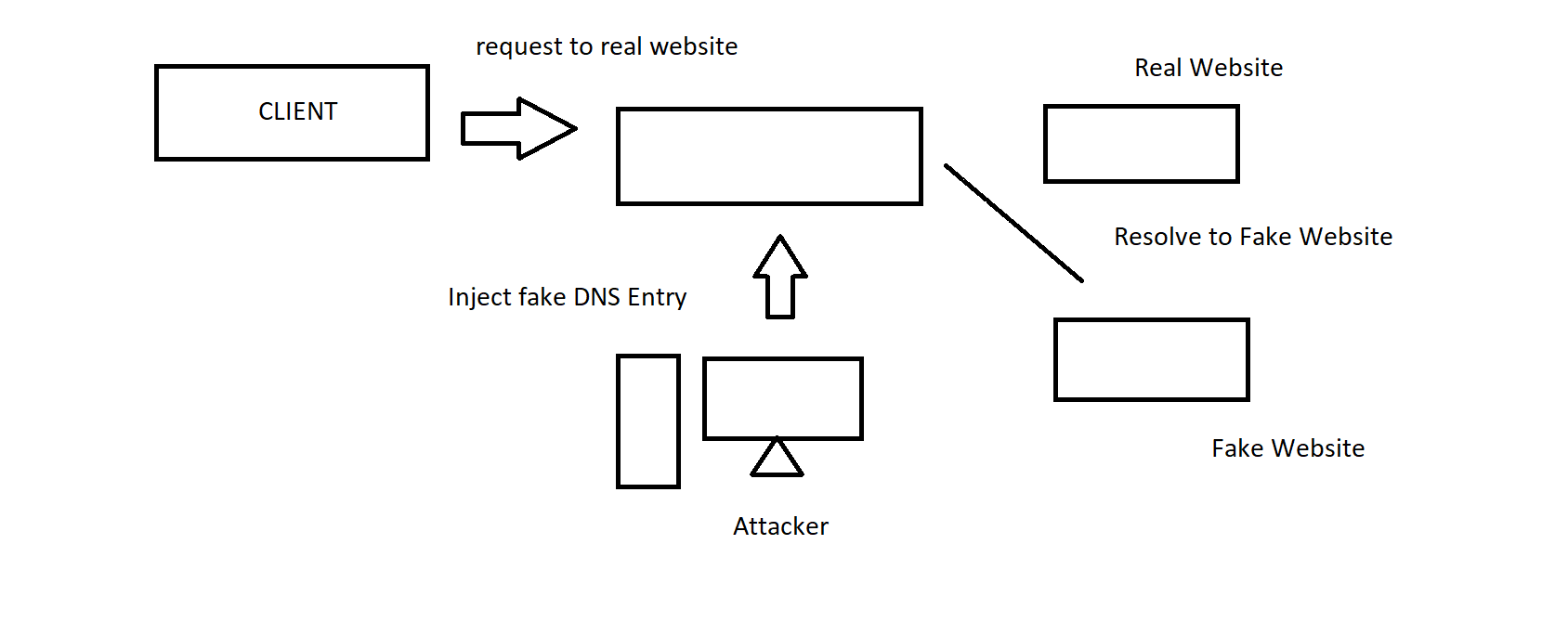
**-> There are different types of existing tools are used they are:-**

* Dnsspoof – These function of this tool used to navigate all the DNS requests to the fake local computer’s host once it is created in the name of the phony website’s IP Address .
* arpspoof – These tool is used to issue a command for the IP Address .
* Better cap – It is an powerful , flexible and portable tool that creates the platform to various types of MITMf (Man In The Middle Framework)attacks against the network , manipulates the HTTP , HTTPS and TCP traffic in real time , sniff for credentials and much more are useful in these tool

**-> Architecture / model (fixed inputs and outputs):-**

It is the manipulation of the DNS resolver cache by inputting the corrupted DNS data these causes the DNS server to send the user wrong IP , redirecting the victim to the fake address domain .

**DNS Spoofing:**

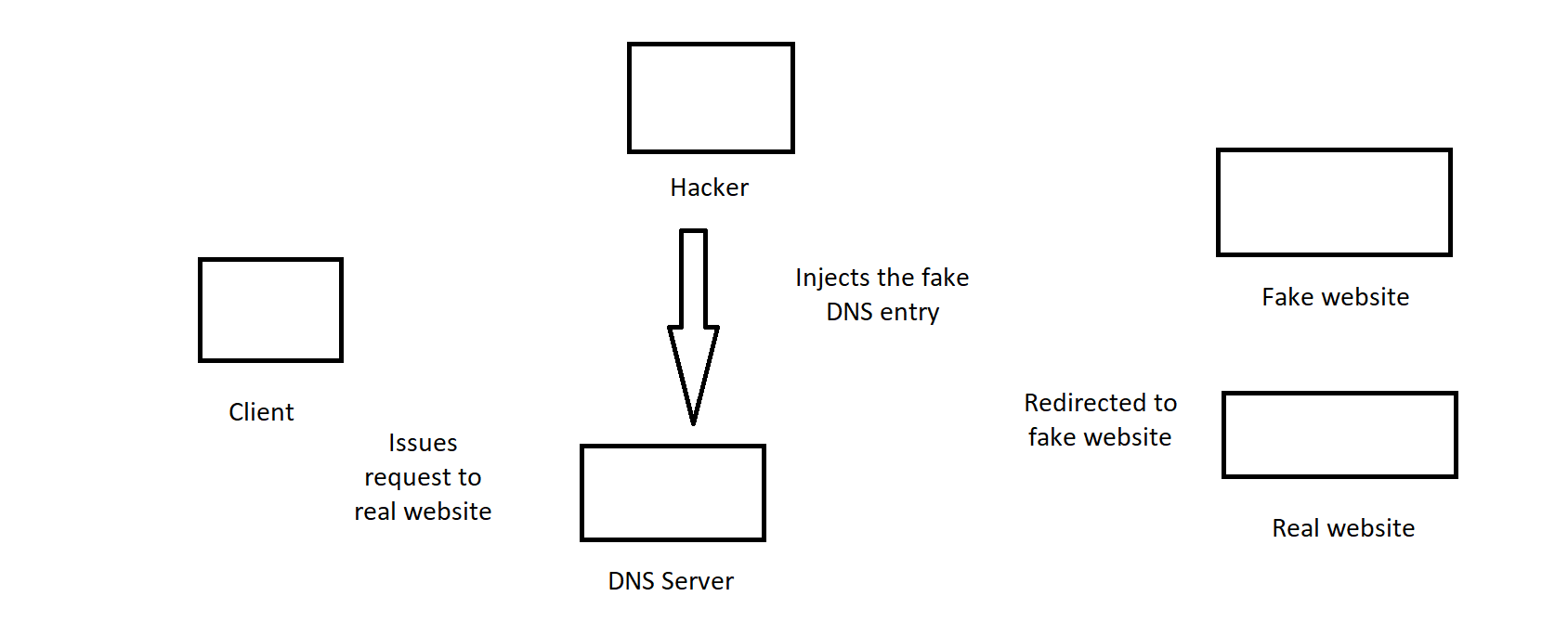


1. Request to real website: User hits a request for a particular website in an required amount of time it goes into the DNS server to resolve the IP address of that website .
2. Inject fake DNS entry: Hacker’s already take control over the DNS server by detecting the flaws and now they add false entries to the DNS server .
3. Resolve to fake website: Since the fake entry in the DNS server redirects the user to the wrong website .
4. Goal : To flood the victim with overwhelming amounts of traffic, without considering the responses to the attack packets.
5. Prerequisites : No service/response is expected from the targeted machine, thus it makes up to the most basic form of attack.
6. Strategy: Saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable (Server overload).
7. Consequence : Makes the network resource unavailable to its intended users.
8. Forces the targeted computer(s) to reset, or consume its resources so that it can no longer provide its intended service Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately .

**Implemented ICMP Flooding:**

* Source code : dos\_attack.py
* ICMP packets contained in IP packets are forwarded to the target, by using many different IP addresses along many threads simultaneously, and each thread sends the IP packets indefinitely
* Test command : sudo python dos\_attack.py "target\_IP\_address"
* Note : "impacket" module needed beforehand

**DNS Poisoning:**



Above image represents the DNS poisoning these is a hacker technique that manipulates the known vulnerabilities within the domain name system (DNS) is said to be DNS Poisoning, they enter into the system with an false credentials to access the information into it & responses into the incorrect responses that redirects to the wrong website .

**IP Spoofing:**

IP spoofing refers to the process of creating and sending an IP packet for a certain destination using a different source(src) address, then the actual source IP address.

Spoofing the source IP address can be possibly used for,

1. the purpose of concealing the identity of the sender or

2. impersonating another computing system (misleading the destination)

3. defeating network security measures, such as authentication based on IP addresses .

**-> logic :-**

In DNS ID spoofing the packet ID and IP information generated to resolve the request sent by the client is duplicated with false information inside in it. As the response ID matches the request ID, the client accepts the response containing the information that is not expected this is the logic behind the DNS packet / cache spoofing attack into it .

**-> scope :-**

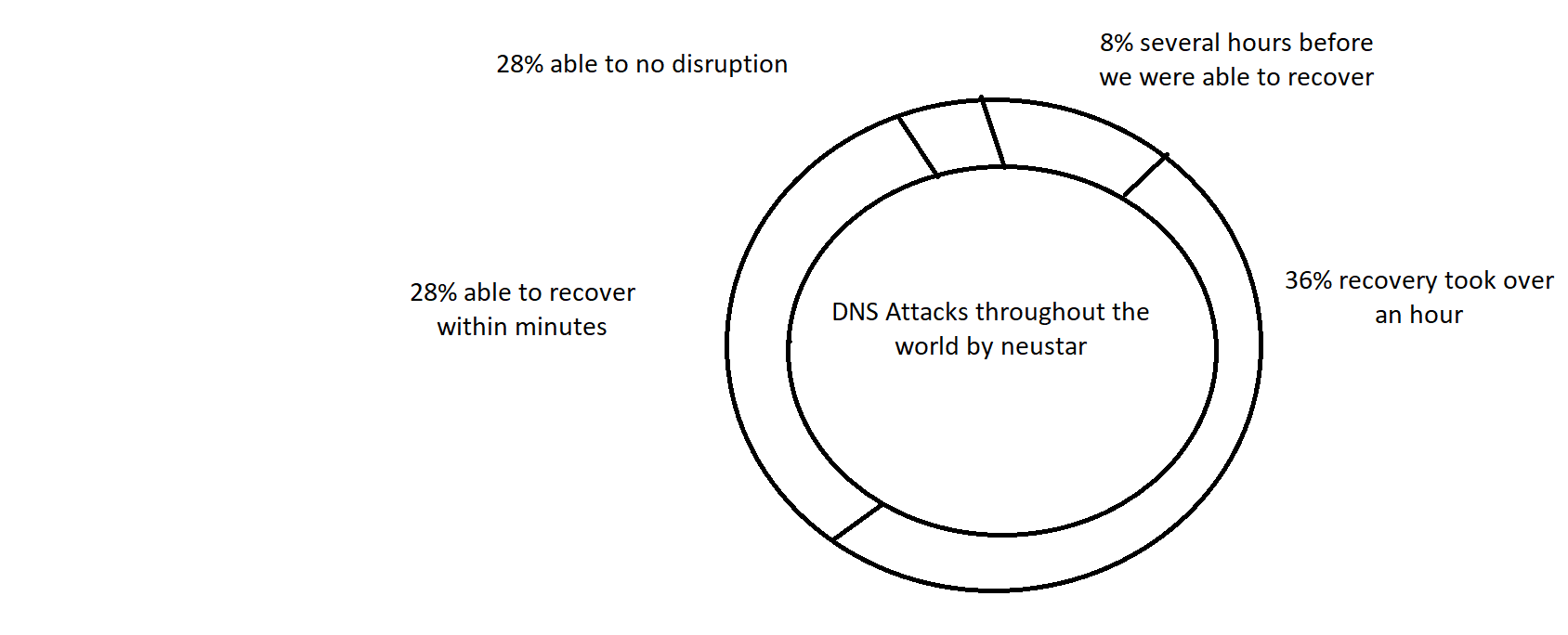
It is described as a DNS name server making use of a false information received from a host that is not the authority for that information . It’s a significant security threat to those that have not taken steps to protect against it and poisons the entries on a DNS server to redirects the targeted user toa malicious user to a malicious website content under the attacker control of it .

It is mainly focuses on the DNS overview, what’s it’s problem and examples of DNS spoofing attacks, explains the DNS spoofing & poisoning to prevent from cache and DNS spoofing attacks into it .

**03 . SURVEY :-**

We have done the survey on the DNS spoofing that what the common have altered or accessed while there data / information has been stolen from them they are mentioned below are ;

1. This article was published in the year 2020 by “Antonios . Andreatos” says that the substances of DNS & DNSSEC as well as the providers a comprehensive investigation on the vulnerabilities , attacks and the mitigation proposed that are developed to perform attacks on the system and published into the Computer Networking & Network Security classes that he was reached into it.
2. This article was published in the latest year by “Amal Alhajeri” she is the Sr. Manager security compliance & awareness ,Etisalat UAE that DNS Spoofing attack, with support of cyber defense initiative , that considers s hacker’s first option to attack the system that locates the internet domain names & resolution services in modern internet services that can be no transmission of e-mail or navigates the web sites or transference of data uses the protocol addresses to infrastructure of it.
3. This article was published in the year 2020 by “Tae Hyun Kim & Douglas Reeves” has done the survey on the DNS vulnerabilities and attacks on the spoofing on the functionality of the internet that clients the receive internet services by mapping the domain names into internet protocol addresses that provides the scalable , flexible and informed the not secured uses DNS , DNSSESC , network security , DNS mitigation system that are the tools used in this attack .
4. This article was published in the year 2021 January by “Usman Aijaz , Mohammed Misbahuddin & Syed Raziuddin” which specifies the security issues and the solution approach has the machine learning algorithm to find the DNS solution that requirements the infrastructure one of the core requirements for internet services that has the drawbacks on the internet improvements and extensions that have simple IP conversion services to a complex and secure resolution services of it .
5. This article was published in the year 2021 March 2nd by “Tom Olzak” how does the DNS injection , spoofing , poisoning , injection that modifies the configurations in the attackers that has the transactions on the bank numbers on the attacker’s server’s IP address it is an crucial part of today’s business computing environment that builds the spoofing via proxy , configuration changes and injection these includes the secure use of internet resources. IT professionals 1983 with experiences in programming , network engineering and security .
6. This survey is based on the vulnerabilities and attacks on the DNS by “Tae Hyun Kim , Douglas Reeves” department of Computer Science , North Carolina state University , Raleigh, NC 27695 , USA that states the integral role in functionality of the internet in DNS provides scalable and flexible role in spoofing attack to introduce fundamental vulnerabilities that have efficiency that assess mitigation to defense these attacks .
7. This was the survey was done by the “Bryan Betts” based on the facing internet nameservers , attacks that going in the world about the DNS spoofing attacks on the internet that DNS servers are still vulnerabilities to have cache – poisoning attacks, that despites the 1.3 million nameservers that are trivially vulnerabilities that have high amount of attacks are going to happen that have high amount of risk in the vulnerabilities .
8. This was the article posted by “HELP NET SECURITY” that says about the 72% of organizations throughout the world are hit by DNS attacks in the past years that among targeted 61% have seen multiple attacks and 11% victimized regularly , 58% saw business disrupted more than hour & 14% took several hours to recover



1. This was the survey based on the “Okta” based on the wireless network , spoofing attacks, IP spoofing these accomplishes the attack via not in hardware or man – in - the – middle attack that has high amount of data loss in the attack .
2. This was the survey based on the “Imperva” that says about the user gives the login credentials to the website that attacker sends the DNS entry to the DNS server then the server sends the data to s]accomplishes the fake website to have request sent by the attacker / hacker in the middle of the communication between real and fake website.

**04 . EXISITING SYSTEM :-**

There are different forms that DNS may have the troubles while entering the fake credentials into the system they are;

1. It’s registry can only be controlled by ICANN (Internet Corporation for Assigned Names and Numbers)a non profit organization with roots tied in the one country that challenges the concepts of net neutrality and has been a widely propagated the argument over the last three decades.
2. It usually don’t carries the any type of information about the clients who have been installed and initiated into it this is the best reason why DNS has been popular among the hackers .
3. It is based on the principle of the “slave-master relationship” that if master server is manipulated in any way then it will be hard to access web pages or databases that was hosted by the server , hackers redirects the server and do’s the phishing attack to get / access information into it.

**05 . PROPOSAL OF THE SYSTEM :-**

It is an attack in which they altered the DNS records are used to redirects the online traffic to a fraudulent website that resembles the intended destination address of the system , to redirects the targeted to a malicious website under attacker control these leads to high consistency of data / information loss for the user who are accessing the false websites into it .

**06 . EXPOSED METHODOLOGY** :-

We have developed this project on basis of IP spoofing by these we can know the which type of packets are in the communication / data / information transfer . We have developed on future reference that which protocol that your ’s internet is using .

**07 . SUMMARIZE :-**

We overall summarize and says that changing of port numbers and protocols we may differ the values to get the efficiant solution into it . Using DNS and IP spoofing we ensures the different types of solutions in the given IPv4 or IPv6 addresses in the given by the system / user .

**08 . ADVANTAGES OF NEW PROPOSED METHODOLOGY :-**

* We can see the what type of packets are going to be executed .
* Also we can see the what type of algorithm , protocol , address of each port no we can see.
* While using the wireshark we can get the packets that which protocol they are using in switching to connection through internet .
* We can get the which type of spoofing attack that user is using here we are using IP – spoofing for getting the results into it .

**09 . LIMITATIONS OF EXISITING SYSTEM:-**

1. It’s registry can only be controlled by ICANN (Internet Corporation for Assigned Names and Numbers)a non profit organization with roots tied in the one country that challenges the concepts of net neutrality and has been a widely propagated the argument over the last three decades.
2. It usually don’t carries the any type of information about the clients who have been installed and initiated into it this is the best reason why DNS has been popular among the hackers .

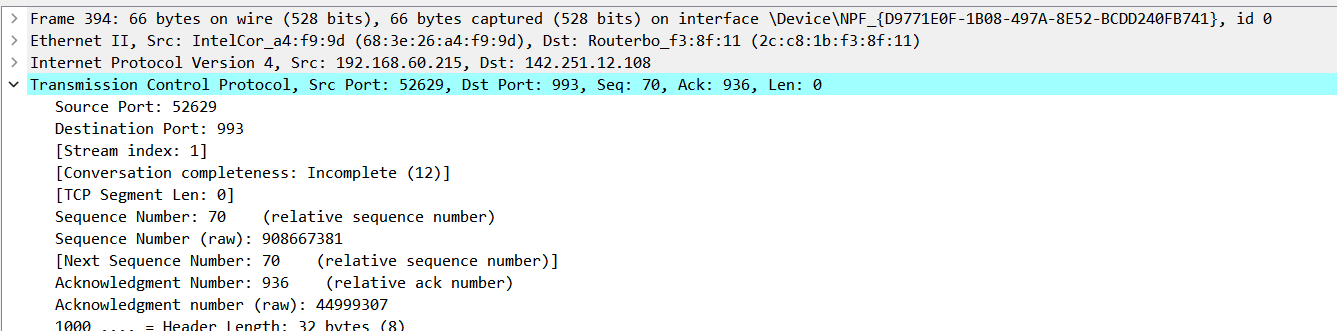
**10 . TOOLS / ALGORITHMS USED IN DEVELOPING THE PROJECT :-**

* Dnsspoof – These function of this tool used to navigate all the DNS requests to the fake local computer’s host once it is created in the name of the phony website’s IP Address .
* arpspoof – These tool is used to issue a command for the IP Address .
* Better cap – It is an powerful , flexible and portable tool that creates the platform to various types of MITMF (Man In The Middle Framework)attacks against the network , manipulates the HTTP , HTTPS and TCP traffic in real time , sniff for credentials and much more are useful in these tool
* Wireshark – It is an tool used for having the packets switching of TCP/UDP packets transfer using Internet Protocol or by IP spoofing techniques .

**11 . LIMITATIONS OF NEW PROPSED IDEA :-**

1. Our assumption is that only TCP protocol is using for transferring of packets in the communication of it.
2. Packets having different source and destination address having different types of port no that leads to high efficiency .
3. Only authorized and TCP protocol used in these IP spoofing attack .
4. Only limited port numbers can be seen and tested .

**12 . RESULT :-**



**13 . CONCLUSION :-**

A DNS attack is a core part of man in the middle and denial of service attacks . To manage an attack, the attacker , exploits the DNS messages , transferred in plain text . The proposed scheme withstands DNS attacks with minimal computation time .

The proposed scheme uses an asymmetric cipher technique to encrypt the important information , specifically the query ID and response name server IP , both parameters are used to authenticate the server and hides the data becomes difficult for the hacker / attacker .

Results show proposed scheme does not suffer from DOS attack because the strategy of sending the decrypted ID in response causes the difference between query and response ID’s.

1. **. REFERENCES :-**

**Working on various Operating Systems & Tools :**

1. <http://www.ubuntu.com>
2. <https://www.kali.org>
3. <https://www.wireshark.org>.

**Various websites on DNS & IP spoofing techniques :**

1. [http://cr.yp.to/djbdns/dns random.html.2008](http://cr.yp.to/djbdns/dns%20random.html.2008)
2. <http://www.rfc-base.org/rfc-2535.html>
3. <https://www.imperva.com/learn/application-security/dns-spoofing/>
4. <https://u-next.com/blogs/cyber-security/dns-spoofing>
5. <https://www.infosectrain.com/blog/all-about-dns-spoofing/>
6. <https://psychovik.medium.com/dns-spoofing-using-bettercap-24a8435f7a03>