Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 11; October-December 2014 pp. 45-49
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/jbaer.html

A Comparative Study of IP Spoofing with Other Types of Network Attacks

Kelvinkumar Kalariya[1], Jay Chapla[2], Tushar Lakhani[3] and Deepak Upadhyay[4]

+M.E. Student, Department of Instrumentation and Control, Atmiya Institute of Technology & Science, Rajkot
[2]Field Engineer, Fiber Optic Department, HFCL PVT LTD, Ahmedabad
[3]M.E. Student, Department of Computer and Science, Saffrony Institute of Technology, Linch (Mehsana)
Department of Computer & Science, Atmiya Institute of Technology & Science, Rajkot
E-mail: [1]kalariya_kelvin36@yahoo.in,[2]chaplajay@gmail.com,
[3]tusharpatel.5412@gmail.com, [4]upadhyay.deepak0@gmail.com

Abstract: *With increased usage of internet in many fields, many security threats affect our network. IP Spoofing plays major role among all other types of network attacks. For example, we generally click on unwanted website link & fill our personal information asked on that website which leads to be misuse of our personal information, even your IP addresses and MAC addresses of your system. Thus, it is very important that we should know that such techniques exist & what we should do for avoid such act. This study paper shows comparison of IP Spoofing with other types of attacks. In this paper, we will give a brief introduction of the spoofing techniques & how it is related with IP Spoofing. IP spoofing is a very basic technique used by the attackers and it is used to steal our personal information misusing it. In reality the attacker is fooling (spoofing) the distant computer into believing that they are a genuine member of the network. The aim is to establish a connection that will allow the attacker to gain root access to the host, permitting the creation of a back door entry path into the target system.*

1. INTRODUCTION TO IP SPOOFING

The Spoofing is the creation of TCP/IP packets using other’s IP address. That address is used by the target machine only when it answers back to the source. IP spoofing is a central part of many network attacks that do not need to see responses (blind spoofing). In [11]this attacker gains an unauthorized access to a computer or a network by making it apparent that a malevolent message has come from a trusted machine by “spoofing” the IP address of that machine. Criminals have learned the tactic of masking their true identity, from disguises to pseudonyms to caller-id blocking. A common misconception was that "IP spoofing" can be used to hide your IP address while sending e-mail, chatting on-line, surfing the Internet, and so on. This is normally not true. Forging the source IP address causes the responses to be misused, sense you cannot create a normal network connection.

Spoofing is the action of making something look like it is not in order to gain unauthorized access to a user's personal information. There are in [12] following type-

- IP Spoofing
- URL Spoofing
- Email Spoofing
- DNS Spoofing
- Caller id spoofing
- Voice mail spoofing

Even the attackers are classified in [4] as:-

- Dos (Denial of service)
- DDos (Distributed Denial of service)
- Non-Blind Spoofing
- Blind Spoofing
- Man In The Middle Attack

Attacks are aimed at preventing customers from accessing a service. We are concentrating only on the IP address or IP spoofing in this paper.IP Spoofing used to create DoSattacks.

2. TYPES OF ATTACK

In network generally these four types of attacks play major role. insulation of winding from the direct contact of atmospheric oxygen.

2.1 Man In The Middle Attack(Mitnick Attack)

The attack– IP spoofing and abuse of trust relationships between a user channel and attacker channel. In this type of attack in which attacker are create the one sequence number at that time server are response and generate one SYN key.

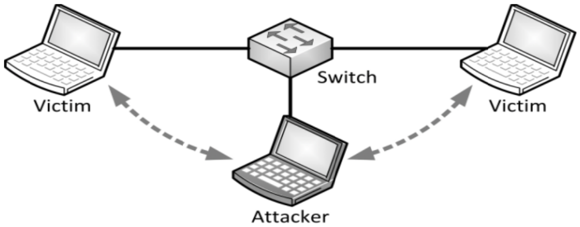


Fig. 1: Mitnick Attack

Now user got the key now user are generate ACK key [13]. Than successfully done work. At the end of here one communication channel are established.

Here in man in middle attack one other type are there that call Session Hijack. IP spoofing used to eavesdrop takes control of a session. Attacker normally with in a LAN on the communication path between server and client. Not blind, since the attacker can see how much traffic from both server and client. Here in session hijack normally attacker told to server, I am a user and attack told user, I am the server. In between her attacker all communication channel create normally [7].

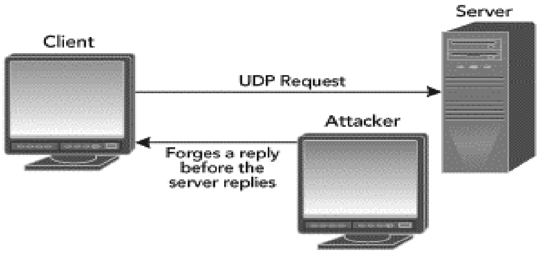


Fig. 2: Session Hijack

2.2 Dos (Denial of service)

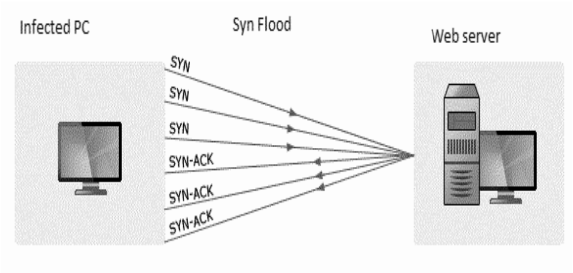


Fig. 3: DOS attack

The attacker spoofs a large number of requests from various IP addresses to full a Services queue. With the services queue fully filled, legitimate users cannot use the service. And it will attack thorough the fake User. That user is already spoofed by attacker. IP Spoofing can be used to create DoS attacks [3].

2.3 DDos (Distributed Denial of service)

Many other types of DDos are possible.DoS becomes more dangerous if spread to multiple computers. Here Attacker makes large number of SYN connection to requests a target servers on the half of a DoS'd server. Then Servers send SYN and ACK to spoofed server, are cannot respond. It is already DoS'd server user very fast fill, [10] as each connection request will have to go through a process of sending several SYN and ACKs before it times out [5].

Attacker makes large number of SYN connection to requests a target servers on the half of a DoS'd server. then Servers send SYN and ACK to spoofed server, are cannot respond. It is already DoS'd server user very fast fill, as each connection request will have to go through a process of sending several SYN and ACKs before it times out [6].

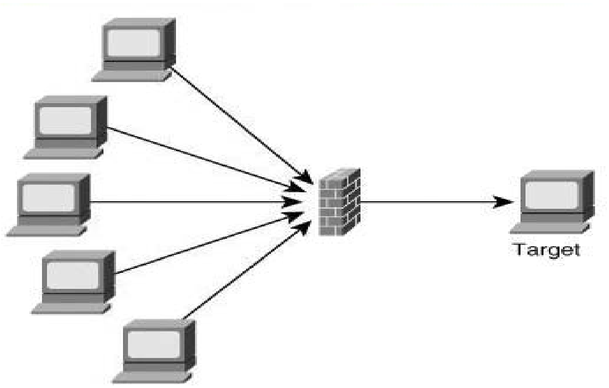


Fig. 4: D'DOS attack

3. BACKGROUND

3.1 IP Spoofing

IP spoofing attack is when an intruder attempts to costume itself by pretending to have the source IP address of a trusted host to access to specific resources on a trusted network. And also we can say that we track the trusted IP address and we use that IP address and attack to the server and we download the all the data [2]. IP spoofing is basically forging or falsifying (spoofing) the source IP addresses in IP packets.

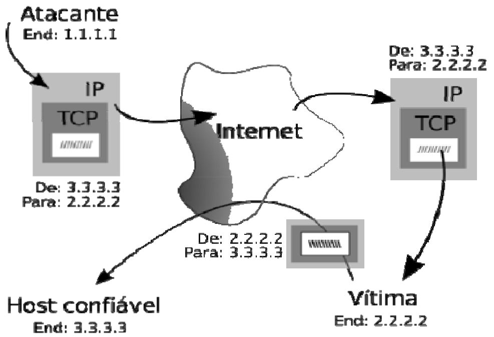
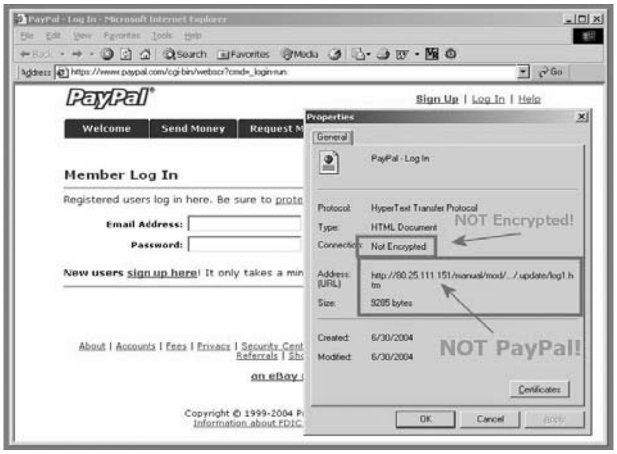


Fig. 5: IP Spoofing

IP spoofing is one of the most common methods of on-line cover-up. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appeared that a mean message has come from a trusted server by "spoofing" the IP address of that computer.

3.2 URL Spoofing

URL spoofing is the process of creating a fake URL which impersonates a reasonable and secure website. The spoofed URL or website address looks like the original and safe URL, but actually it is (Hyperlinks) redirecting all the traffic to a ‘booby trapped’ website.


PayPal - Log In - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Go
PayPal
Sign Up | Log In | Help
Welcome
Send Money
Request M
About | Accounts | Fees | Privacy | Security Cent
Referrals | Sh
on eBay
Properties
General
Certificates
OK
Cancel
Apply
NOT Encrypted!
NOT PayPal!

Address: https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Member Log In

Registered users log in here. Be sure to prote

Email Address:

Password:

New users sign up here! It only takes a min

Copyright © 1999-2004 P
Information about FDIC

PayPal - Log In

Protocol: HyperText Transfer Protocol
Type: HTML Document
Connection: Not Encrypted
Address: (URL) http://80.25.111.151/manual/mod/.../update/log1.htm
Size: 9285 bytes
Created: 6/30/2004
Modified: 6/30/2004

Fig. 6: URL Spoofing

Such websites and forged URLs are primarily used in cybercrimes such as identity theft, phishing, and various scams. The forged or spoofed URL is [14] sent to as many target victims as possible through different means, including emails, texts, and instant messaging.

Type of URL spoofing

- popup windows
- unwanted advertisement
- instant massaging

This kind of link set up has also included one or more null characters before the '@' sign to disguise the true destination of a link and prevent it from displaying correctly in the browser address bar or status bar. This URL spoofing (or URL cloaking) is a vulnerability in some browsers like Mozilla and Internet Explorer. Try this next link to see if your browser is vulnerable to this exploit and observe the shocking result if it isgoogle.com.

If your browser is vulnerable, you may seehttp://www.yahoo.com in your browser status bar while the mouse is positioned over the link or if you click on the link, you may found http://www.yahoo.com in your browser address bar, while our home page is displayed in the

Browser window. The above URL uses multiple null characters which has the effect pushing part of the full URL out of the visible part of some browser's status bar, thereby only showing http://www.yahoo.com. In other cases, including Microsoft's Outlook, it can take only one null character. If your browser is not page show, patch Internet Explorer browsers will show the page cannot be displayed as an error in the opening of that page.

Insert the following script into the HTML of your page and spoofurl.com are automatically writeagain your outgoing links for you.

```
<scriptsrc="http://spoofurl.com/spoofurl.js"
type="text/javascript"></script>
```

Spoof URL also supports embedded JavaScript redirects from your page. This allows you to handle out links to your site which will automatically redirect through SpoofURL and onto your affiliated link, while maintaining the reference header as your site. It's easy to do, [8] simply embed the following in between the <head> tag of a page that you can control (exampledomain.com/1.html):

```
<script>
Var redirect Url=
"http://spoofurl.com/301/merchantsite.com/affiliateId.html"
<script
src=https://spoofurl.com/spoofurlRedirect.js"type=text/javascr
ipt"></script>
```

3.3 Email Spoofing

E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of Attacker often use spoofing in an attempt to get recipients to open, and possibly even respond to, there solicitations. Spoofing is used legitimately. Classic examples of senders who might prefer to disguise the source of the e-mail include a sender reporting mistreatment by a spouse to a welfare agency or a "whistle-blower" who fears retaliation. However, spoofing anyone other than yourself is illegal in some jurisdictions [9].

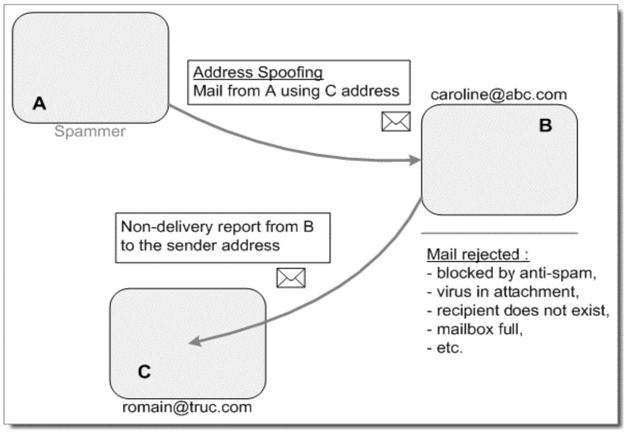


Fig. 7: Email spoofing

3.4 DNS Spoofing

DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is entered into a Domain Name System (DNS) name server's cache database, causing the name of server to back an incorrect IP address, diverting traffic to other computer (often the attacker's). DNS spoofing is [1] another one of the man-in-the-middle attacks that can force victims to navigate to a fake website purporting to be a real one.

DNS spoofing is based on presentation of fake DNS information to a victim in response to their DNS request and, as a result, forcing them to visit a site which is not the real one

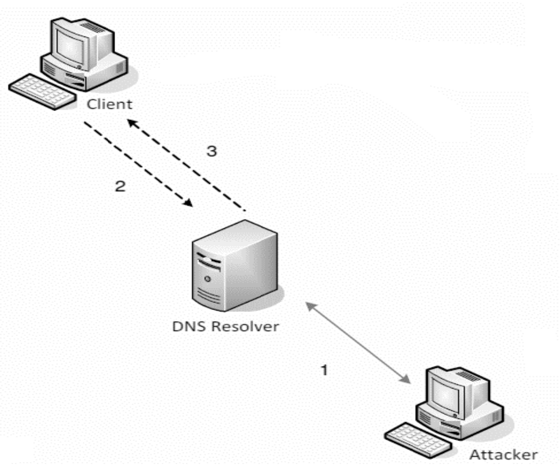


Fig. 8: DNS Spoofing

4. RELATION BETWEEN IP SPOOFING AND OTHER TYPES

4.1 URL Spoofing with IP spoofing

In URL spoofing we know that any website have same IP address and when we click on the URL at that time we are spoofed Here it is based on IP spoofing. Here in URL Spoofing when we click on URL at that time generate the on packet at that packet have on source address and one destination address. Here the over IP address trace to the attacker and attacker are miss used over IP Address.

Source IP	URL Packet	Destination IP

Fig.9 - URL packet

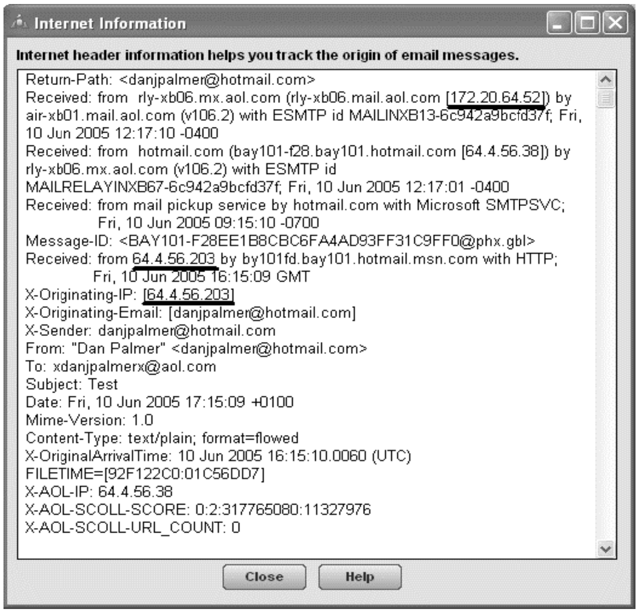
4.2 Email Spoofing with IP spoofing

In email spoofing, when we reply any email at the same time that email have same IP address. Here at email, it has header with same IP source IP address and destination IP address. In this email same attacker add same effective mater put at that time we click on any link or we also reply at that email at that time two condition are there .one is when we click on the link at that time URL type spoofing are assure. And second condition are there when we reply that email at that time over IP address are transfer or attach with Email header now attacker reader over IP address.

4.3 DNS Spoofing with IP spoofing

DNS spoofing, attacker create the Omni DNS server at the time when user open any site using the same server, the site bounce the address and the user get connected to the fake server but that fake are operated with the attacker now attacker are hack over IP address and over your information.

Here while DNS spoofing is also spoofed becoming the base of IP spoofing [1].



Internet header information helps you track the origin of email messages.

```
Return-Path: <danjpalmer@hotmail.com>
Received: from  rly-xb06.mx.aol.com (rly-xb06.mail.aol.com [172.20.64.52]) by
air-xb01.mail.aol.com (v106.2) with ESMTP id MAILINXB13-6c942a9bcfd37f; Fri,
10 Jun 2005 12:17:10 -0400
Received: from  hotmail.com (bay101-f28.bay101.hotmail.com [64.4.56.38]) by
rly-xb06.mx.aol.com (v106.2) with ESMTP id
MAILRELAYINXB67-6c942a9bcfd37f; Fri, 10 Jun 2005 12:17:01 -0400
Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
          Fri, 10 Jun 2005 09:15:10 -0700
Message-ID: <BAY101-F28EE1B8CBC6FA4AD93FF31C9FF0@phx.gbl>
Received: from 64.4.56.203 by by101fd.bay101.hotmail.msn.com with HTTP;
          Fri, 10 Jun 2005 16:15:09 GMT
X-Originating-IP: [64.4.56.203]
X-Originating-Email: [danjpalmer@hotmail.com]
X-Sender: danjpalmer@hotmail.com
From: "Dan Palmer" <danjpalmer@hotmail.com>
To: xdanjpalmerx@aol.com
Subject: Test
Date: Fri, 10 Jun 2005 17:15:09 +0100
Mime-Version: 1.0
Content-Type: text/plain; format=flowed
X-OriginalArrivalTime: 10 Jun 2005 16:15:10.0060 (UTC)
FILETIME=[92F122C0:01C56DD7]
X-AOL-IP: 64.4.56.38
X-AOL-SCOLL-SCORE: 0:2:317765080:11327976
X-AOL-SCOLL-URL_COUNT: 0
```

Fig. 10: Email Header

5. CONCLUSIONS

With the current implementations of spoofing, the network security community needs to be aware of the magnitude and potential cost of these types of attacks. IP Spoofing is related with other types of spoofing like Email Spoofing, URL Spoofing, and DNS Spoofing and after study about the IP Spoofing we conclude that many types we can be attacked or many ways an attacker can misuse our information. Our study shows that IP Spoofing play major role compare to other network attacks so never click on any fake URL, never talk with the stranger, never reply the unwanted Email.

REFERENCES

[1] Simar Preet Singh, A Raman Maini,University College of Engineering, Patiala, Punjab,"*Spoofing Attacks of Domain Name System Internet*", Proceedings published in International Journal of Computer Applications(IJCA),2011

[2] Neil B. Riser *“Spoofing: An Overview of Some Spoofing Threats”* from SANS Reading room.

[3] Christoph L. Schuba, et. al., *“Analysis of a Denial of Service Attack on TCP,”* 2011 IEEE Symposium on Security and Privacy , May 2011, pp. 208.

[4] CERT Advisory CA-96.21, TCP SYN Flooding and IP Spoofing Attacks. September 19, 1996, http://www.cert.org/advisories/CA-1996-21.html -

[5] D.G.Raimagia, Singh. S., Zafar. S. “To Make Trust Relationship between BGP speakers with the Help of Secure Private Key”, 2012, 2nd International Conference on Engineering (NUiCONE–2012) PP 1-7.

[6] Frank Kargl,Joern Maier,Michael Weber,*"Protecting Web Servers from Distributed Denial of Service Attacks"* WWW10, May 1-5, 2001, Hong Kong,ACM 1-58113-348-0/01/0005.

[7] "*Security Technology White Paper*", Huawei Technologies Co., Ltd, Issue 01 (2012-10-30), Huawei Proprietary and Confidential

[8] Felten, Balfanz, Dean, Wallach D.S., *“Web Spoofing,An internet con Game”*,http://bau2.uibk.ac.at/matic/spoofinh.htm

[9] P. Ramesh Babu,D.Lalitha Bhaskari,CH.Satyanarayana, *"A Comprehensive Analysis of Spoofing"*,(IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 1, No.6, December 2010

[10] ICSNN/SSAC. *“ICANN SSAC Advisory SAC008 DNS Distributed Denial of Service (DDoS) Attacks.”* Mar. 2006.

[11] Leila Fatmasari Rahman and Rui Zhou “ *IP Address Spoofing”*, Albert-udwigs-Universität Freiburg, Institute for Computer Science.

[12] Mrs. Mridu Sahu,Rainey C. Lal,"*Controlling Ip Spoofing Through Packet Filtering"*,International Journal Computer Techology & Applications,ISSN:2229-6093,Vol 3 (1),155-159

[13] D.G. Raimagia, C.N. Chanda, “A Novel Approach to Enhance Performance of Linux-TCP Westwood on Wireless Link”, 2013, 3rd International Conference on Engineering (NUiCONE–2013), PP 1-6.

[14] ”*Web Spoofing: An Internet Con Game*”, Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Technical Report 540-96 (revised Feb. 1997), Department of Computer Science, Princeton University.