A Novel Approach for Unique Address of the computer in Network Security Environment

Sanjay R Patel
Gujarat Technological University

Neha D. Parmar
Gujarat Technological University

Viral R Patel
Marwadi Education Foundation Group of Institute

Abstract: In computer networking, the term IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing. This paper contains an overview of IP address and IP Spoofing and its background. It also shortly discusses various types of IP Spoofing, MAC spoofing and how they attack on communication system. This paper also describes some methods to detection and prevention methods of IP spoofing and also describes impacts on communication system by IP Spoofing. Propose approach identifies the computer through defined unique identification address of computer.

Keywords: IP address, IP Spoofing, MAC Address, TCP/IP, Unique Address.

1. Introduction:

Spoofing can take on many forms in the computer world, all of which involve some type false representation of information. There are a variety of methods and types of spoofing. The basic protocol for sending data over the Internet network and many other computer networks is the Internet Protocol ("IP"). The header of each IP packet contains, among other things, the numerical source and destination address of the packet. The source address is normally the address that the packet was sent from. By forging the header so it contains a different address, an attacker can make it appear that the packet was sent by a different machine. The machine that receives spoofed packets will send response back to the forged source address, which means that this technique is mainly used when the attacker does not care about the response or the attacker has some way of guessing the response.

In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by spoofing the IP address of that machine.

In certain cases, it might be possible for the attacker to see or redirect the response to his own machine. The most usual case is when the attacker is spoofing an address on the same LAN or WAN. Hence the attackers have an unauthorized access over computers.

Literature Survey

2. IP Spoofing:

In a spoofing attack, the intruder sends messages to a computer indicating that the message has come from a trusted system. To be successful, the intruder must first determine the IP address of a trusted system, and then modify the packet headers to that it appears that the packets are coming from the trusted system. In essence, the attacker is fooling (spoofing) the distant computer into believing that they are a legitimate member of the network. The goal of the attack is to establish a connection that will allow the attacker to gain root access to the host, allowing the creation of a backdoor entry path into the target system.

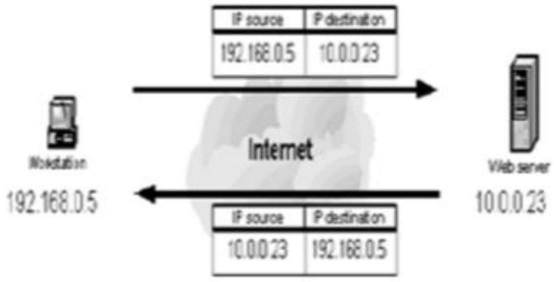


Figure 1: Valid source IP address

This figure illustrates a typical interaction between a workstation with a valid source IP address requesting web pages and the web server executing the requests. When the workstation requests a page from the web server the request contains both the workstation's IP address (i.e. source IP address 192.168.0.5) and the address of the web server executing the request (i.e. destination IP address 10.0.0.23). The web server returns the web page using the source IP address specified in the request as the destination IP address, 192.168.0.5 and its own IP address as the source IP address, 10.0.0.23.

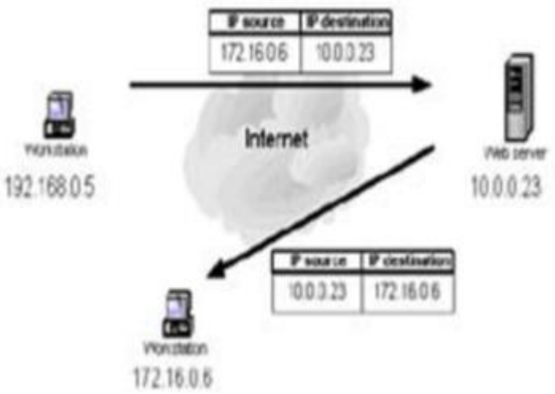


Figure 2: Spoofed source IP address

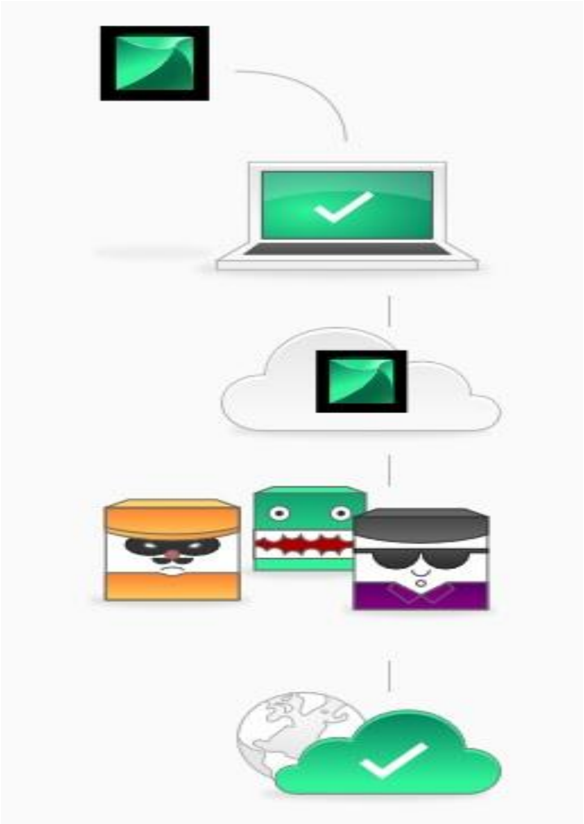
This figure illustrates the interaction between a workstation requesting web pages using a spoofed source IP address and the web server executing the requests. If a spoofed source IP address (i.e. 172.16.0.6) is used by the workstation, the web server executing the web page request will attempt to execute the request by sending information to the IP address [1] of what it believes to be the originating system (i.e. the workstation at 172.16.0.6). The system at the spoofed IP address will receive unsolicited connection attempts from the web server that it will simply discard.

Software For IP Spoofing

1)Tor Browser

The Tor software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked[8].

2) SpotFlux



Spotflux is software that has to be install in our computer. Once we start this software it connects to its server. So whenever we makes request for internet that goes to its server first then this request is encrypted with new IP and goes to the specified server. So in this case we cannot identify original IP address of the computer [9].

There are many software other then this through which we can change our computer's IP address and hence we cannot take IP address as a unique address of the computer.

3. Spoofing Attacks:

There are a few variations on the types of attacks that successfully employ IP spoofing. Although some are relatively dated, others are very pertinent to current security concerns.

3.1 Non-Blind Spoofing

This type of attack takes place when the attacker is on the same subnet as the victim. The sequence and acknowledgement numbers can be calculated, eliminating the potential difficulty of calculating them accurately. The biggest threat of spoofing in this instance would be session hijacking. This is accomplished by corrupting the DataStream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine. Using the spoofing, the attacker interferes with a connection that sends packets along the subnet.

3.2 Man in the Middle Attack

Both types of spoofing are forms of a common security violation known as a man in the middle (MITM) attack. In these attacks, a malicious party intercepts a legitimate communication between two friendly parties. The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient. In this way, an attacker can fool a victim into disclosing confidential information by "spoofing" the identity of the original sender, who is presumably trusted by the recipient.

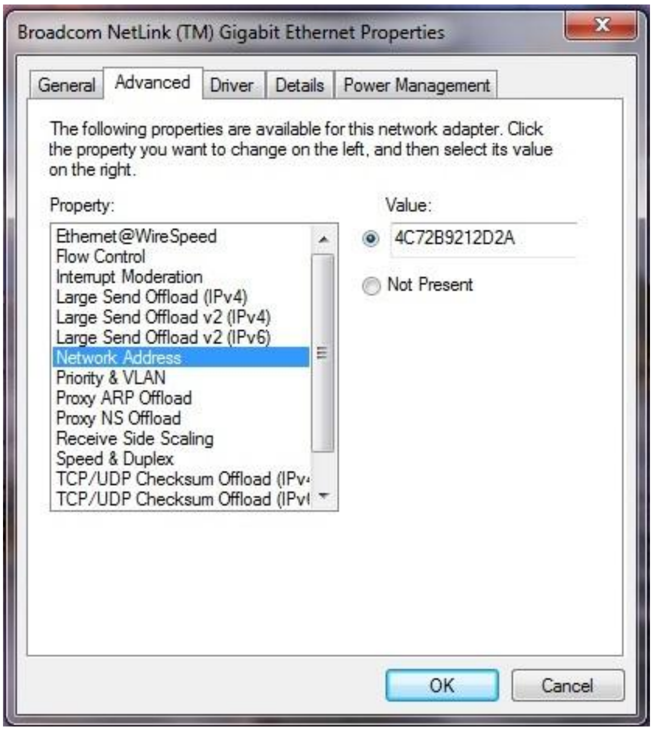
5.2 Software to Stop IP Spoofing:

We can use some software's to stop IP Spoofing:

- Stop Cut
- Find Mac Address pro
- Security Gateway for Exchange / SMTP
- Packet Creator
- Responder Pro

MAC Address Spoofing

A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sub layer of the OSI reference model[7].



Broadcom NetLink (TM) Gigabit Ethernet Properties

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

Ethernet@WireSpeed
Flow Control
Interrupt Moderation
Large Send Offload (IPv4)
Large Send Offload v2 (IPv4)
Large Send Offload v2 (IPv6)
Network Address
Priority & VLAN
Proxy ARP Offload
Proxy NS Offload
Receive Side Scaling
Speed & Duplex
TCP/UDP Checksum Offload (IPv4
TCP/UDP Checksum Offload (IPv6

Value:

● 4C72B9212D2A

○ Not Present

As shown in figure, windows operating system directly gives us the option for changing the MAC address value of the computer. So if we change the MAC then the outgoing request from the computer is with spoofed MAC address and hence we cannot identify original MAC address of the computer. Linux system has option of clone MAC address through which we can change our MAC address of the computer.

Propose Approach

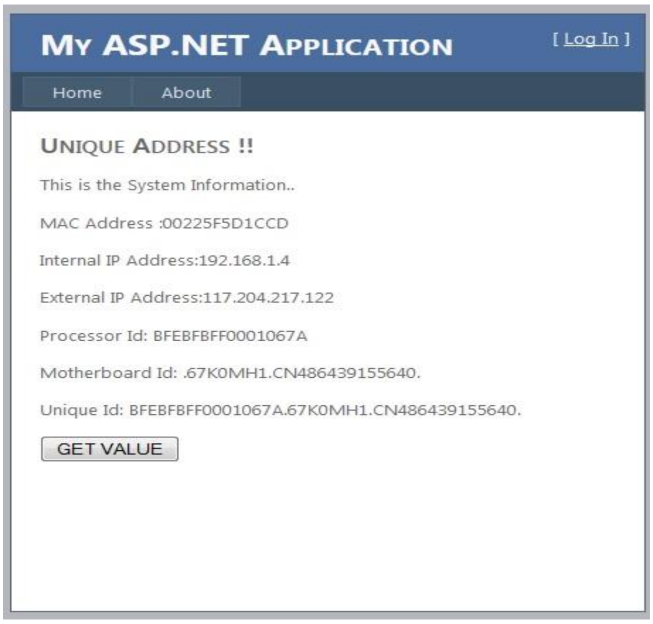
As we have seen that MAC address and IP address is not unique (Can be changed) and hence we are proposing one new address that is unique to the computer and also cannot be changed. Processor Id is a identification number of the CPU that is given to the processor of the CPU. Processor ID is binded to the processor, it's a hardware device and hence it is not going to change from CPU so we can use this address for identification of the computer. Processor ID is a 16 byte hexadecimal number so if we call function for Processor ID then we get BFEBFBFF000206A7 like 16 byte return value. For better security purpose we can take Mother Board ID and concate it with Processor ID address.

Implementation

We have developed our portal which shows us MAC, IP and Propose unique Address of the computer. Now this portal is uploaded on the free hosting site and then we have analyze various computer data.

From this we came to know that for the same PC IP and Mac address can be different (Spoofed) but the propose unique address is same in any case as it is not going to be change.

Result



UNIQUE ADDRESS !!

This is the System Information..

MAC Address :00225F5D1CCD

Internal IP Address:192.168.1.4

External IP Address:117.204.217.122

Processor Id: BFEBFBFF0001067A

Motherboard Id: .67K0MH1.CN486439155640.

Unique Id: BFEBFBFF0001067A.67K0MH1.CN486439155640.

Validation

Processor ID is associated to the Processor and to change the processor of CPU is not possible as it is the heart of the computer. So the unique address that we are proposing will not be change as the parameter that we have used in it will not going to be change and hence we can use this address for licensing purpose where unique address of the computer is necessary.

6. Conclusion

This paper describes the use of IP and MAC spoofing as a method of attacking a network in order to gain unauthorized access and some detection and prevention methods of IP spoofing. The goal of the attack is to establish a connection that will allow the attacker to gain root access to the host, allowing the creation of a backdoor entry path into the target system. We think that our proposed methods will be very helpful to detect and stop IP and MAC spoofing and give a secured communication system. Also this unique address will be useful for securing software licensing and tracing cyber crime.

References

[1] Leila Fatmasari Rahman, Rui Zhou. IP Address Spoofing, (December 16, 1997). CERT Advisory CA- 1997-28. IP Denial-of-Service Attacks. CERT/CC.

[2] Daemon9. IP Spoofing Demystified. Phrack Magazine Review, Vol 7, No. 48, June 1996, pp. 48-14.

[3] Computer Incident Advisory Committee (CIAC) (1995). Advisory Notice F-08 Internet Spoofing and Hijacked Session Attacks.

[4] Donkers, A. (1998, July). Are You really Who You Say You Are? System Administrator, Vol 7, No. 7, 69-71.

[5] D. Schnackenberg, K. Djahandari., and D. Sterne. Infrastructure for Intrusion Detection and Response. Proc. of the DARPA Information Survivability Conference and Exposition (DISCEX '00), 2000.

[6] S. Staniford-Chen and L. T. Heberlein. Holding Intruders Accountable on the Internet. Proc. of the 1995 IEEE, Symposium on Security and Privacy, , May 1995 Oakland, CA, pages 39-49.

[7] Mac Address [Online] Available at: http://en.wikipedia.org/wiki/MAC_address [Accessed: 21st January 2013]

[8] Tor Browser [Online] http://www.torproject.org.in/projects/torbrowser.html.en [Accessed: 21st January 2013]

[9] SpotFlux Prooxy Server [Online] http://www.spotflux.com/[Accessed: 21st January 2013]