IP SPOOFING

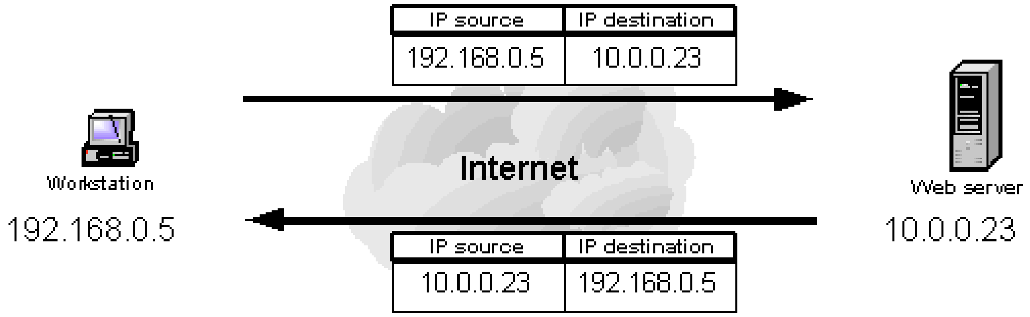
written by

Christoph Hofer, 01-115-682

Rafael Wampfler, 01-132-034

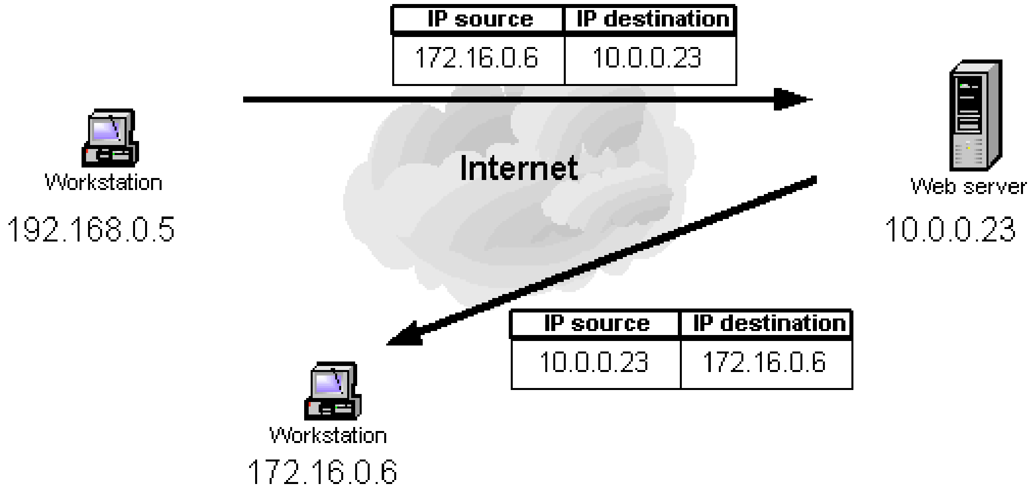
What is IP spoofing

IP spoofing is the creation of IP packets using somebody else's IP source addresses. This technique is used for obvious reasons and is employed in several of the attacks discussed later. Examining the IP header, we can see that the first 12 bytes contain various information about the packet. The next 8 bytes contains the source and destination IP addresses. Using one of several tools, an attacker can easily modify these addresses – specifically the "source address" field. A common misconception is that IP spoofing can be used to hide our IP address while surfing the Internet, chatting online, sending e-mail, and so on. This is generally not true. Forging the source IP address causes the responses to be misdirected, meaning you cannot create a normal network connection.



Normal network traffic

Valid source IP address, 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 (192.168.0.59) and its own IP address as the source IP address (10.0.0.23).



Network traffic with spoofed IP address

Spoofed source IP address 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 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.

IP ROUTING MECHANISM AND PROBLEMS

The IP routing mechanism is hop by hop. Every IP packet is routed separately. The route of a IP packet is decided by all the routers the packet goes through. IP address spoofing is possible because routers only require inspection of the destination IP address in the packet to make routing decisions. The source IP address is not required by routers and an invalid source IP address will not affect the delivery of packets. That address is only used by the destination machine when it responds back to the source.

IP ADDRESS SPOOFING

ASYMMETRIC ROUTING (SPLITTING ROUTING)

Asymmetric routing means traffic goes over different interfaces for directions in and out. In other words, asymmetric routing is when the response to a packet follows a different path from one host to another than the original packet did. The more correct and more general answer is, for any source IP address ‚A’ and destination ‚B’, the path followed by any packet (request or response) from ‚A’ to ‚B’ is different than the path taken by a packet from ‚B’ to ‚A’.

IMPLEMENTATION OF ASYMMETRIC ROUTING

Modern operating systems allows us to receive packets from an input interface, different from the output interface.

In Linux, we can implement asymmetric routing using iptables (linux 2.4):

```
iptables –A POSTROUTING –t nat –j SNAT –to 192.168.0.5 –o eth0
```

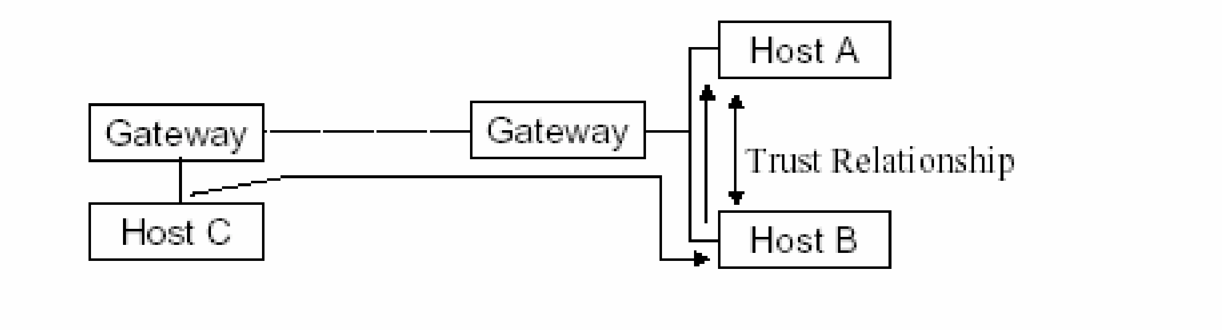
This means, for all the packets going out via eth0, their source IP address will be changed to 192.168.0.5. We also have to „disable“ reverse path filtering:

```
echo “0” > /proc/sys/net/ipv4/conf/all/rp_filter
```

IP ADDRESS SPOOFING ATTACKS

BLIND IP SPOOFING

Usually the attacker does not have access to the reply, abuse trust relationship between hosts. For example: Host C sends an IP packet with the address of some other host (Host A) as the source address to Host B. Attacked host (B) replies to the legitimate host (A).

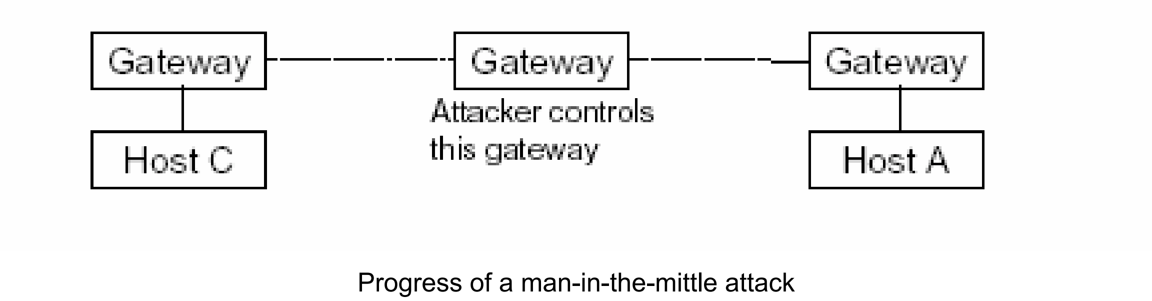


Progress of IP spoofing

MAN-IN-THE-MIDDLE ATTACKS

If an attacker controls a gateway that is in the delivery route, he can

- sniff the traffic
- intercept / block / delay traffic
- modify traffic



Progress of a man-in-the-mittle attack

This is not easy in the Internet because of hop-by-hop routing, unless you control one of the backbone hosts or source routing is used. This can also be done combined with IP source routing option. IP source routing is used to specify the route in the delivery of a packet, which is independent of the normal delivery mechanisms. If the traffic can be forced through specific routes (=specific hosts), and if the reverse route is used to reply traffic, a host on the route can easily impersonate another host.

ATTACKS CONCERNING THE ROUTING PROTOCOLS

A host can send spoofed RIP packets in order to “inject” routes into a host. This is easy to implement, it only requires IP/UDP spoofing. On a LAN with RIPv2 passwords have to be used for updating routes, but plaintext passwords are used. The plaintext passwords can be sniffed.

IP address spoofing attack with ICMP

ICMP is short for Internet Control Message Protocol, an extension to the Internet Protocol (IP) defined by RFC 792. ICMP supportspackets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an internet connection.

ICMP ECHO ATTACKS

Map the hosts of a network: The attack sends ICMP echo datagram to all the hosts in a subnet, then he collects the replies and determines which hosts are alive.

Denial of service attack (SMURF attack): The attack sends spoofed (with victim‘s IP address) ICMP Echo Requests to subnets, the victim will get ICMP Echo Replies from every machine.

ICMP REDIRECT ATTACKS

ICMP redirect messages can be used to re-route traffic on specific routes or to a specific host that is not a router at all.

The ICMP redirect attack is very simple: just send a spoofed ICMP redirect message that appears to come from the host‘s default gateway.

For example: Host A sends a forged ICMP packet to host B, saying the route through A is a better way to internet. The source IP address of this forged ICMP packet is the gateway’s IP address C. Then all the traffic from B to internet will go through A.

ICMP DESTINATION UNREACHABLE ATTACKS

ICMP destination unreachable message is used by gateways to state that the datagram cannot be delivered. It can be used to cut out nodes from the network. It is a denial of service attack (DOS)

Example: An attacker injects many forged destination unreachable messages stating that 100.100.100.100 is unreachable) into a subnet (e.g. 128.100.100.*). If someone from the 128.100.100.* net tries to contact 100.100.100.100, he will immediately get an ICMP Time Exceeded from the attacker‘s host. For 128.100.100.* this means that there is no way to contact 100.100.100.100, and therefore communication fails.

UDP attacks

UDP is an unreliable transport layer protocol. It relies on IP, it is connectionless, and its checksum is optional. Therefore, the delivery, integrity, non-duplication and ordering are not guaranteed. It is easy to send a forged packet to the target. Compared with this, TCP is connection oriented and the TCP connection setup sequence number is hard to predicated, so it is hard to insert forged packet into the TCP connection. Therefore UDP traffic is more vulnerable for IP spoofing than TCP.

TCP attacks

Although it is hard to do IP spoofing on TCP, it is still can be realized on the specific operating system. The attack aims at impersonating another host mostly during the TCP connection establishment phase. For example:

1) Node A trusts node B (e.g. login with no password)

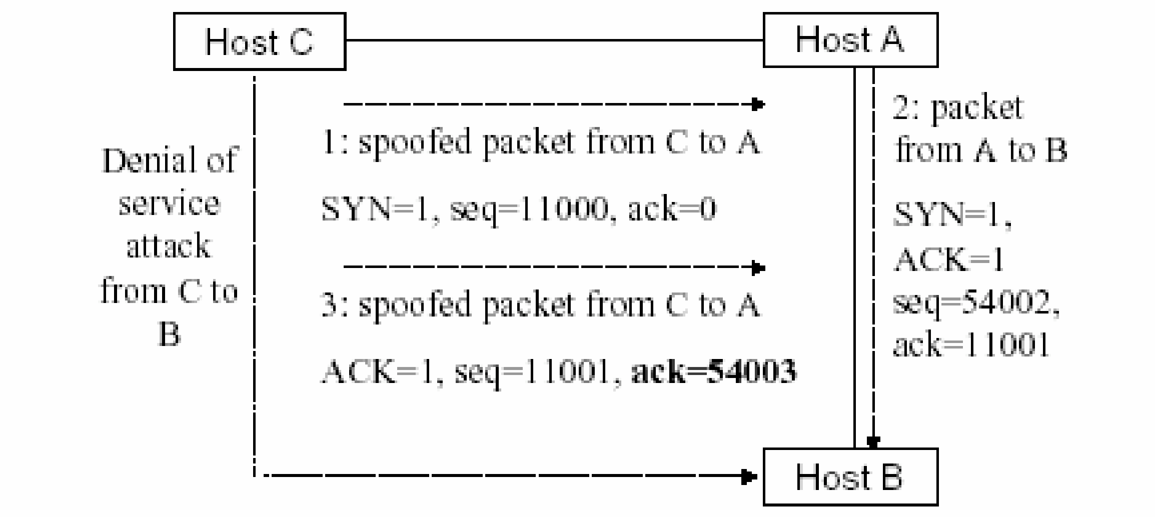
2) Node C wants to impersonate B with respect to A in opening a TCP connection

3) C kills B (flooding, redirecting or crashing) firstly

4) C sends A an TCP segment in a spoofed IP packet with B‘s address as the source IP and 11000 as the sequence number.

5) A replies with a TCP SYN/ACK segment to B with 54002 as the sequence number

6) C does not receive the segment from A to B, but in order to finish the handshake it has to send an ACK segment with 54002+1 as the acknowledge number to A. C has to guess or predicate the value of 54002.


Host C
Host A
Host B
Denial of service attack from C to B
1: spoofed packet from C to A
SYN=1, seq=11000, ack=0
3: spoofed packet from C to A
ACK=1, seq=11001, ack=54003
2: packet from A to B
SYN=1, ACK=1 seq=54002, ack=11001

Progress of a TCP attack

Stopping IP address spoofing attack

PACKET FILTERING

The router that connects a network to another network is known as a border router. One way to mitigate the threat of IP spoofing is by inspecting packets when they the leave and enter a network looking for invalid source IP addresses. If this type of filtering were performed on all border routers, IP address spoofing would be greatly reduced. Outgoing filtering checks the source IP address of packets to ensure they come from a valid IP address range within the internal network. When the router receives a packet that contains an invalid source address, the packet is simply discarded and does not leave the network boundary. Incoming filtering checks the source IP address of packets that enter the network to ensure they do not come from sources that are not permitted to access the network. At a minimum, all private, reserved, and internal IP addresses should be discarded by the router and not allowed to enter the network.

LIMITS OF PACKET FILTERING

Packet filtering normally may not prevent a system from participating in an attack if the spoofed IP address used could fall within the valid internal address range. However it will simplify the process of tracing the packets, since the systems will have to use a source IP address within the valid IP range of the network.

Instances where you might need to disable packet filtering include:

- If you want to do asymmetric routing (accepting returning packets inbound an interface other than the outbound interface).
- If the box has multiple interfaces up on the same network.
- If you are using special VPN interfaces to tunnel traffic (e.g. FreeS/WAN) Another problem is that many ISPs do not have the technical ability to arrange packet filtering to block packets with spoofed source addresses. Also, packet filtering reduces equipment performance.

Can you answer the following questions?

1. What is IP spoofing?

2. Why is IP spoofing possible?

3. What is the reason to spoof an IP address?

4. Can you use IP spoofing for anonymous web surfing?

5. What can you do against IP spoofing?

Answers

1. IP spoofing is to fake IP packets with a foreign IP source address

2. Because the IP protocol is very limited and the network routers do not care about source IP addresses.

3. The main purpose is hacking

4. No, because the packets does not find back the way to you (your source address is spoofed)

5. You cannot do anything to be completly secure. But there are same technics to reduce the problem of IP spoofing:

- Use ICMP packets instead of IP packets
- Packet filtering
- Encrypt the data so the hacker cannot abuse the connection

Resources

BOOKS

- Computer Networks (Andrew S. Tanenbaum)
- Hack Proofing Your Network (Ryan Russell)

WEB SITES

- http://www.securityfocus.com/infocus/1674
- http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Spoofing/default.htm
- http://www.linuxgazette.com/issue63/sharma.html
- http://ciac.llnl.gov/ciac/bulletins/g-48.shtml

PDF

- http://www.giac.org/practical/gsec/Victor_Velasco_GSEC.pdf
- http://www.fatelabs.com/library/non-blind-hijacking.pdf
- http://doe-is.llnl.gov/ConferenceProceedings/DOECompSec97/hacking.pdf
- http://www.informatik.hu-berlin.de/~kuehnlen/spoofing/spoofing.pdf
- http://www.cs.uni-magdeburg.de/~guidiri/seminar_netzwerk/Spoofing.pdf
- http://www.lasr.cs.ucla.edu/classes/239_1.spring03/slides/lecture2.pdf