The IP Smart Spoofing

Althes (http://www.althes.fr)
Revision 1 - October 2002
Laurent Licour (llicour@althes.fr)
Vincent Royer (vroyer@althes.fr)

1 Abstract

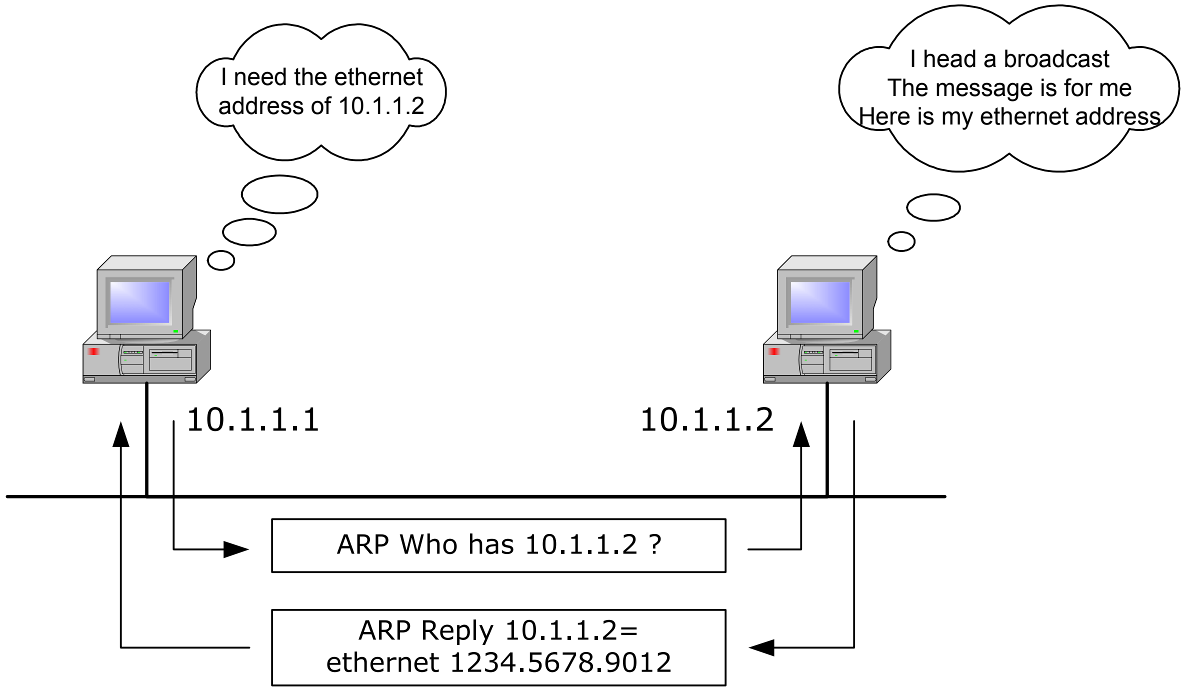
This paper describe a new technique for spoofing an IP address with any networking application. IP spoofing is not new and various hacking tools have been developed to exploit it. In the following, we will discuss on the way to use it with any standard application. As a result, we will explain why IP based access control is not reliable in many cases, and should not be used in many corporate networks.

2 Introduction

The IP smart spoofing use a combination of ARP cache poisoning, network address translation and routing. It doesn't require any sophisticated hack.

3 The ARP Cache poisoning

A computer connected to an IP/Ethernet network has two addresses. A globally-unique MAC address for each network interface and a logical IP address assigned by software. The ARP protocol build the association between these two addresses. When a computer needs to send a packet to an IP address located in the same network, it broadcast a message "ARP who has ?". As shown in the following figure, the IP address's owner responds with its Ethernet address.


I need the ethernet address of 10.1.1.2
I head a broadcast The message is for me Here is my ethernet address
10.1.1.1
10.1.1.2
ARP Who has 10.1.1.2 ?
ARP Reply 10.1.1.2= ethernet 1234.5678.9012

To minimize ARP broadcast, operating systems keep a cache of ARP replies. Unfortunately, ARP is stateless and most operating systems update their cache when receiving ARP reply, regardless of whether they have sent out an actual request. By sending forged ARP replies, a target system could be convinced to send frames destined for a computer to another computer. This process is referred as “ARP Cache poisoning”.

Depending on the target operating system, cache poisoning may be achieved through eight types of ARP message with the following characteristic :

- ARP message forwarded in a MAC broadcast or MAC unicast.
- Operation code may be “ARP Who is” or “ARP Reply”.
- ARP message is a gratuitous message or not (embedding the same IP addresses for source and destination)

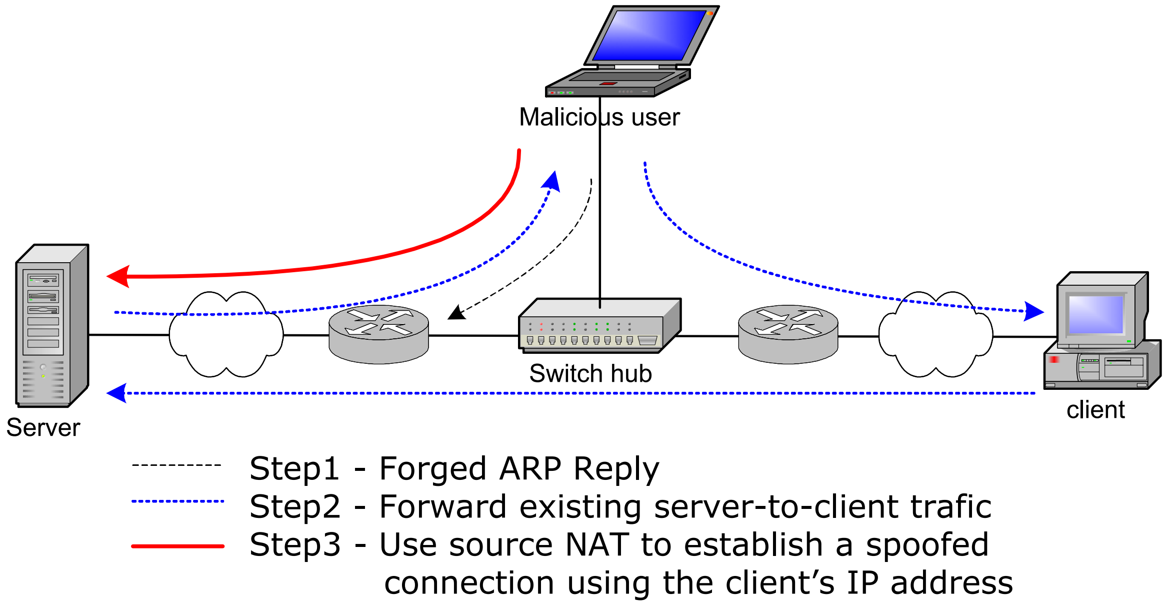
According to our tests on Windows 9x, NT, 2000, XP, Solaris 8, Linux kernel 2.2 and 2.4, Cisco IOS 12, Nokia IPSO 3.5 operating systems, there were always at least one kind of ARP message to poison the cache. Moreover, on Windows systems (9x/NT/2K), static ARP entry can always be overwritten using a fake ARP message.

Note that due to the MAC learning process on the switch hub, spoofing the source MAC address will cause the malicious user to receive all traffic intended to the spoofed system for a while, causing a short deny of service.

ARP cache poisoning may be used to perform “man-in-the-middle” attacks on switch hubs and sniff all traffic, gathering clear text passwords on the wire and much more…

4 The IP smart-spoofing

Using ARP cache poisoning, the malicious user inserts his computer into the server-to-client communication path. With IP forwarding, existing traffic is still routed to the client side. Of course, ICMP Redirect have been disabled on the malicious user’s computer. Finally, a source network translation is used by the malicious user to spoof the client’s IP address and established a new connection to the server.


Malicious user
Switch hub
Server
client
Step1 - Forged ARP Reply
Step2 - Forward existing server-to-client trafic
Step3 - Use source NAT to establish a spoofed connection using the client’s IP address

Then, the malicious user can then run any standard network applications to connect to the server using the client 's IP address. Any access control based on the client's IP address will be abused. Moreover, the existing trafic is not perturbed and, from the server side, the smart spoofing attack cannot be detected.

This thechnique has been sucessfully tested under Linux Redhat 7.3, with arp-sk (http://arp-sk.org) or arpsoof (http://naughty.monkey.org/~dugsong/dsniff/) and iptables. In addition, we have develop arp-fillup to maintains ARP entries on the spoofed host to avoid regular ARP broadcasts.

5 Impacts of smart spoofing

Network devices like routers or firewalls often use source IP address filtering. Theses rules can be bypassed from any computer located on the network path between the authorized client and the firewall. For example, in most corporate networks connected to the internet through a firewall, only few identified computers can directly access to the internet (the internal HTTP proxy hosting content or URL filtering, mail servers, etc …). With smart spoofing, any internal users can bypass theses rules (bypass the HTTP content or URL filtering, received/send SMTP emails directly, etc …).

In the same way, application whose access is restricted to specific IP addresses may be abused by any computer located on the network path between one authorized client and the server. This is the case for many application like Apache ACL, r-commands, NFS, TCP Wrapper, restricted administration tools, etc …

Moreover, SMTP anti-relaying controls based on the IP source address reverse-resolution may be abused. By spoofing the IP address of a SMTP relay A, a malicious user on the network path between A and B, can relay mails through the SMTP relay B, using a forged source email address from a mail domain hosted by A.

6 Conclusion

Due to security issues in the ARP protocol and the resulting smart spoofing attack, access controls relying on source IP address may be abused in many cases.

When sending spoofed ARP replies, most of network IDS listening on all ports on the switch hub, detects a duplicate IP address, but does not actually block the attack. In addition, this approach would require deployment of numerous NIDS on many networks.

Another approach would use Host-Based IDS to detect fake ARP messages and maintain consistency of the ARP table. Available on many UNIX platforms, *arpwatch* maintains a database of Ethernet MAC addresses seen on the network, with their associated IP pairs. Alerts the system administrator via e-mail if any change happens, such as new station/activity, flip-flops, changed and re-used old addresses.

Finally, a reliable access control should use strong authentication rather than source IP address identification or clear text password authentication. VPN protocols like SSH, SSL or IpSec can greatly improve security by achieving authentication, integrity and confidentiality.