IP Spoofing

SHAGEER KHAN
GAURAV KUMAR
Mr. NAMIT GUPTA
MCA,CCSIT(TMU)
MCA, CCSIT(TMU)
Assistant prof: CCSIT(TMU)

shageerkhan96@gmail.com

gauravrajput15051999@gmail.com

Namit.k.gupta@gmail.com

***Abstract*—** This paper includes IP Spoofing which refers to Creation of Internet Protocol (IP) packets with a Forged source IP address called spoofing, with the Purpose of concealing the identity of sender or Impersonating another computer system. 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, with the purpose of concealing the identity of the sender or impersonating another computing system. On January 22, 1995, in an article entitled, ―New form of attack on computers linked to Internet is uncovered, John Mark off of the New York Times reported on the TCP/IP protocol suite's security weakness known as IP spoofing.

Keywords— Network security, IP Spoofing, Dos attack .

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. We would like to introduce and explain following types in this paper:

- DNS Spoofing
- IP Spoofing
- ARP Spoofing
- E-Mail Spoofing
- Web Spoofing

There are no legal or constructive uses for implementing spoofing of any type. Some of the outcomes might be sport, theft, vindication or some other malicious goal. The gravity of these attacks can be very severe, can cost us millions of dollars and should not be overlooked by the Internet security community.

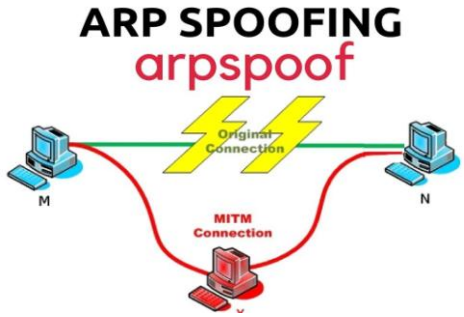
WHAT IS IP SPOOFING

IP spoofing is used to gain unauthorized access to a computer. The attacker forwards packets to a computer with a One of the major drawback with IP spoofing are that C never "sees" the responses from A. This is completely blind attack, much experience and knowledge of what to expect from the target's responses is needed to successfully carry out his attack. Some of the most common ways to avoid this type of attack are to disable source-routed packets and to disable all external incoming packets with the same source address as a local host.

ARP SPOOFING

ARP stands for Address Resolution Protocol. ARP is used to map IP addresses to hardware addresses. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address resolution in both directions [3]. When an incoming packet sent to a host machine on a network arrives at a router, it asks the ARP program to find a MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the network to determine if any

machine knows who has that IP address. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied. Here is a sample ARP broadcast query:



One might deduct that this addressing scheme could also be spoofed to provide a host with incorrect information "ARP Spoofing involves constructing forged ARP request and reply packets. By sending forged ARP replies, a target computer could be convinced to send frames destined for computer A to instead go to computer B." This referred to as ARP poisoning. There are currently programs that automate the process of ARP poisoning – ARPoison, Ettercap, and Parasite. All three have the capability to provide spoofed ARP packets and therefore redirect transmission, intercept packets, and/or perform some type of man in the middle attack. Either enabling MAC binding at a switch or implementing static ARP tables achieves prevention of ARP spoofing. MAC binding makes it so that once an address is assigned to an adapter; it cannot be changed without authorization. Static ARP management is only realistically achieved in a very small network. In a large dynamic network, it would be impossible to manage the task of keeping the entries updated. ARPWATCH, for UNIX based systems, monitors changes to the ARP cache and alerts administrator as to the changes.

E-Mail Spoofing

Spoofing is when an e-mail message appears to come from a legitimate source but in fact is from an impostor. E-mail spoofing can be used for malicious purposes such as spreading viruses, trawling for sensitive business data and other industrial espionage activities [8]. If you receive a snail mail letter, you look to the return address in the top left corner as an indicator of where it originated. However, the sender could write any name and address there; you have no assurance that the letter really is from that person and address. E-mail messages contain return addresses, too – but they can likewise be deliberately misleading, or "spoofed." Senders do this for various reasons, including:

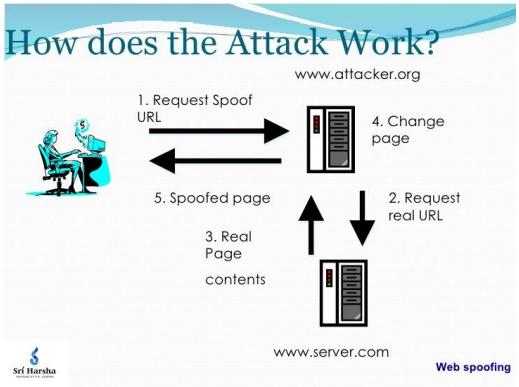
(E-mail ip spoofing figure)

- The e-mail is spam and the sender doesn't want to be subjected to anti-spam laws
- The e-mail constitutes a violation of some other law (for example, it is threatening or harassing)
- The e-mail contains a virus or Trojan and the sender believes you are more likely to open it if it appears to be from someone you know
- The e-mail requests information that you might be willing to give to the person the sender is pretending to be (for example, a sender might pose as your company's system administrator and ask for your network password), as part of a "social engineering" attack
- The sender is attempting to cause trouble for someone by pretending to be that person (for example, to make it look as though a political rival or personal enemy said something he/she didn't in an e-mail message) Here is an example of a spoofed email made out to look like it originated from administrator@puc.net

Web Spoofing

As with the other forms of spoofing Web or Hyperlink spoofing provides victims with false information. Web Spoofing is an attack that allows someone to view and modify all web pages sent to a victim's machine. They are able to observe any

information that is entered into forms by the victim. This can be of particular danger due to the nature of information entered into forms, such as addresses, credit card numbers, bank account numbers, and the passwords that access these accounts [4]. Web Spoofing works on both Internet Explorer and Netscape and is not necessarily prevented by secure connections. This is due the way that the SSL protocol uses certificates to authenticate websites. The attacker can observe and modify all web pages and form submissions, even when the browser is indicating that there is a secure connection. The attack can be implemented using JavaScript and Web server plug-ins, and works in two parts.

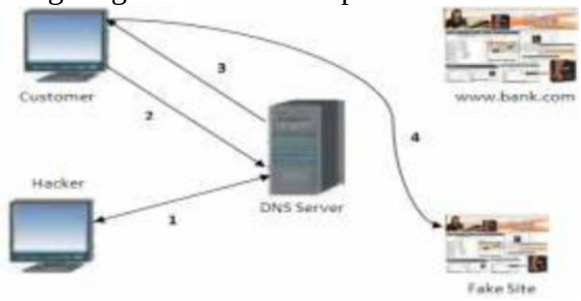


First, the attacker causes a browser window to be created on the victim's machine, with some of the normal status and menu information replaced by identical-looking components supplied by the attacker. Then, the attacker causes all Web pages destined for the victim's machine to be routed through the attacker's server. On the attacker's server, the pages are rewritten in such a way that their appearance does not change at all, but any actions taken by the victim (such as clicking on a link) would be logged by the attacker. In addition, any attempt by the victim to load a new page would cause the newly loaded page to be routed through the attacker's server, so the attack would continue on the new page. The attack is initiated when the victim visits a malicious Web page, or receives a malicious email message. Current browsers do not completely prevent Web Spoofing, and there seems to be little movement in the direction of addressing this problem. I believe that there can be no fully secure electronic commerce on the Web until the Spoofing vulnerability has been addressed.

DNS IP Spoofing

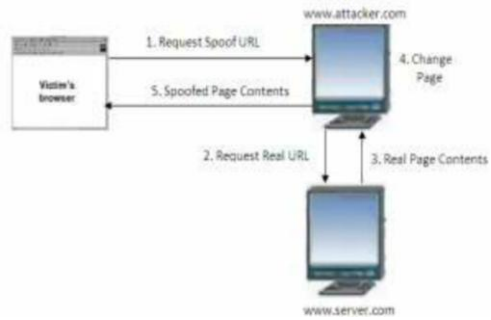
A DNS spoofing attack can be defined as the successful insertion of incorrect resolution information by a host that has no authority to provide that information. It may be conducted using a number of techniques ranging from social engineering through to exploitation of vulnerabilities within the DNS server software itself. Using these techniques, an attacker may insert IP address information that will redirect a customer from a legitimate website or mail server to one under the attacker's control – thereby capturing customer information through common man-in-the-middle mechanisms [9]. According to the most recent "Domain Health Survey" (Feb 2003), a third of all DNS servers on the Internet are vulnerable to spoofing.

Operating normally, a customer can expect to query their DNS server to discover the IP address of the named host they wish to connect to. The following diagram reflects this process.



(Normal DNS Motion Process),

1. The customer queries the DNS server – "What is the IP address of www.bank.com?"
2. The DNS responds to the customer query with "The IP address of www.bank.com is 150.10.1.21"
3. The Customer then connects to the host at 150.10.1.21 –
   expecting it to be www.bank.com.
   However, with a successful DNS spoofing attack, the process has been altered. The following diagram reflects this process.



(motion process having fallen victim to a DNS spoofing attack image),

1. The attacker targets the DNS service used by the customer and adds/alters the entry for www.mybank.com – changing the stored IP address from 150.10.1.21 to the attacker's fake site IP address (200.1.1.10)

2. The customer queries the DNS server "What is the IP address of www.bank.com"

3. The DNS responds to the customer query with "The IP address of www.bank.com is 200.1.1.10" – not the real IP address.

4. The Customer then connects to the host at 200.1.1.10 – expecting it to be www.bank.com, but in fact reaching the attackers fake site.

AVOIDANCE OF SPOOFING

The Packet filtering is the best method to avoid various spoofing attacks. In this section we have described three packet filtering methods which are used to filter the spoofed packets, they are

A. Ingress Filtering Method - IFM
B. Egress Filtering Method - EFM
C. Spoofing Prevention Method – SPM

A. Ingress Filtering Method

- Ingress filtering is a technique used to make sure that incoming packets are actually from the networks that they claim to be from [7]
- Networks receive packets from other networks. Normally a packet will contain the IP address of the computer that originally sent it. This allows other computers in the network to know where it came from, which is needed for things like sending a packet back to the sending computer [7]
- In certain cases, the sending IP address will be spoofed. This is usually done as part of an attack, so that the attacked computer does not know where the attack is really coming from [7].
- Filtering a packet is when the packet is not processed normally, but is denied in some way. The computer processing the packet might simply ignore the packet completely, or where it is possible it might send a packet back to the sender saying the packet is denied.
- In ingress filtering, packets coming into the network are filtered if the network sending it should not send packets from IP addresses of the originating computer.
- In order to do ingress filtering, the network needs to know which IP addresses each of the networks it is connected to may send. This is not always possible. For instance, a network that has a single connection to the Internet has no way to know if a packet coming from that connection is spoofed or not [7].
- Ingress filtering is a packet filtering technique used by many Internet service providers to try to prevent source address spoofing of Internet traffic, and thus indirectly combat various types of net abuse by making Internet traffic traceable to its source [7].
- Ingress filtering is a "good neighbor" policy which relies on mutual cooperation between ISPs for their mutual benefit.
- There are many possible ways of implementing this policy; one common mechanism is to enable reverse path forwarding on links to customers, which will

- indirectly apply this policy based on the provider's route filtering of their customers' route announcements [7].

B. Egress Filtering Method

- Egress filtering is the practice of monitoring and potentially restricting the flow of information outbound from one network to another. Typically it is information from a private TCP/IP computer network to the Internet that is controlled [7].
- TCP/IP packets that are being sent out of the internal network are examined via a router or firewall. Packets that do not meet security policies are not allowed to leave - they are denied "egress" [7].
- Egress filtering helps ensure that unauthorized or malicious traffic never leaves the internal network [7].
- In a corporate network, typically all traffic except that emerging from a select set of servers would be denied egress. Restrictions can further be made such that only select protocols such as http, email, and DNS are allowed. User workstations would then need to be set to use one of the allowed servers as a proxy. Direct access to external networks by the internal user workstation would not be allowed [7].
- Egress filtering may require policy changes and administrative work whenever a new application requires external network access. For this reason egress filtering is an uncommon feature on consumer and very small business networks [7].

C. Spoofing Prevention Method (SPM)

A new approach for filtering spoofed IP packets, called Spoofing Prevention Method (SPM). The method enables routers closer to the destination of a packet to verify the authenticity of the source address of the packet. This stands in contrast to standard ingress filtering which is effective mostly at routers next to the source and is ineffective otherwise. In the proposed method a unique temporal key is associated with each ordered pair of source destination networks (AS's, autonomous systems). Each packet leaving a source network S is tagged with the key K(S;D), associated with (S;D), where D is the destination network. Upon arrival at the destination network the key is verified and removed. Thus the method verifies the authenticity of packets carrying the address s which belongs to network S. An efficient implementation of the method, ensuring not to overload the routers, is presented [5]. The major benefits of the method are the strong incentive it provides to network operators to implement it, and the fact that the method lends itself to stepwise deployment, since it benefits networks deploying the method even if it is implemented only on parts of the Internet. These two properties, not shared by alternative approaches, make it an attractive and viable solution to the packet spoofing problem.

TRACEBACK MECHANISM

The basic idea of IP trackback approach based on packet marking is that the router marks packets with its identification information as they pass through that router. The mark overloads a rarely used field in IP packet header, i.e., 16-bit IP identification field. The identification of a router could be 32-bit IP address, hash value of IP address, or uniquely assigned number. In the last two cases, the length of identification information is variable and could be less than 16 bits. Since the marking space in packet header is too small to record the entire path, routers mark packets with some probability so that each marked packet carries the information of one node in the path. In addition, based on the length of router identification and the implementation of marking procedure, the router may only write part of its identification information into the marking space. While each marked packet represents only a small portion of the path it has traversed, the whole network path can be reconstructed by combining a modest number of such packets. This kind of approach is referred to as

probabilistic packet marking (PPM). The PPM approach does not incur any storage overhead at routers and the marking procedure (a write and checksum update) can be easily and efficiently executed at current routers. But due to its probabilistic nature, it can only trace the traffic that consists of a large volume of packets. In the PPM a packet stores the information of an edge in the IP header. The pseudocode of the procedure is given below for reference. The router determines how the packet can be processed depending on the random number generated. If x is smaller than the predefined marking probability pm, the router chooses to start encoding an edge. The router sets the start field of the incoming packet to the routers address and resets the distance field to zero. If x is greater than pm, the router chooses to end encoding an edge by setting the router's address in the end field.

Types of Spoofing

• Main categories of spoofing include the following:
– Blind spoofing
– Active spoofing
– IP spoofing
– ARP (Address Resolution Protocol) spoofing
– Web spoofing
– DNS (Domain Name System) spoofing

Blind Spoofing
• Any kind of spoofing where only one side of the relationship under attack is in view
• Hacker is not aware of all network conditions – But uses various means to gain access to the network

Active Spoofing
• Hacker can see both parties, observe the responses from the target computer, and respond accordingly
• Hacker can perform various exploits, such as – Sniffing data, corrupting data, changing the contents of a packet, and even deleting some packets

IP Spoofing
• Consists of a hacker accessing a target disguised as a trusted third party
• Can be performed by hackers through either blind or active methods of spoofing

ARP Spoofing
• Modifying the Address Resolution Protocol (ARP) table for hacking purposes
• ARP table stores the IP address and the corresponding Media Access Control (MAC) address
• Router searches the ARP table for the destination computer's MAC address
• ARP spoofing attack involves detecting broadcasts, faking the IP address
– And then responding with the MAC address of the hacker's computer

Web Spoofing
• Hacker spoofs an IP address through a Web site
• Hacker can transfer information or get information
• Hacker can spoof using a strategy – That ensures that all communication between the Web site and the user is directed to the hacker's computer
• Hacker may also falsely acquire a certificate used by a Web site

DNS Spoofing
• Hacker changes a Web site's IP address to the IP address of the hacker's computer
• Altering the IP address directs the user to the hacker's computer
• User is accessing the hacker's computer – Under the impression that he or she is accessing a different, legitimate, site

CONCLUSION

In this paper we discussed the IP spoofing based attack detection using route based information present in IP packet header i.e. the TTL and ID field of the packet also we introduced a traceback mechanism to trace back the attacker right at its origin. . The IP packet header information is efficiently handled by routers, hence proposing a

technique the uses the router specific features will be best suited for real time processing. We found the algorithm is well suited to detect the DDoS attack situations as long as the network is stable, i.e., the routing information is not changed.

REFERENCES

[1] The Swiss Education and Research Network, Default TTL values in TCP/IP. 2002 [Online]. Available http://secfr.nerim.net/docs/fingerprint/en/ttldefault. html.

[2] B. Krishnamurthy and J. Wang, "On network-aware clustering of web clients," in Proc. ACM SIGCOMM, 2000, pp. 97–110.

[3] Ishibashi, H., Yamani, N., Abe, K. and Matsuura, T.,"A protection method against unauthorized access and address spoofing for open network access systems", IEEE Pacific Rim Conference on Communication and Signal Processing, 2001.

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

[5] Daemon9. IP Spoofing Demystified. Phrack Magazine Review, Vol 7, No. 48, June 1996, pp. 48-14. Computer Incident Advisory Committee (CIAC) (1995). Advisory Notice

[6] F-08 Internet Spoofing a Hijacked Session Attacks.

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