A Method for attacking a Protected Site by a Clean Intruder

Mohammad Ala'a AL-Hamami*

m_ah_1@yahoo.com

Abstract:

The appearance of the Internet is considered to be one of the major events of the last years; information become available on-line, all users who have a computer can easily connect to the Internet and search for information they want to find. The result is that everybody can read the latest news on-line and also consult digital libraries, read about firms, universities, cultural events, exhibitions, etc. So, sensitive Internet sites must be protected against the intentional hostile intrusion by strong protection systems. Althogh the strongness of these protection systems, there are alwayes vulnerabilites in them and give the intruders a big chance to penetrate the protected sites.

This research proposd a method to attack the protected site by taking the advantage of the **NTFS** (New Tecnology File System) and **ADS** (Alternete Data Stream) properties as a security holes.

This method has two steps: ***The first***, the attacker (clean intruder) using the IP Address Spoofing Attack to make authorized access to the protected site. ***The secod***, the clean intruder could insert any malicious programs in any others of NTFS, without any changes to these files especially their size. The result is, the clean intruder (by inserted malicious programs) will determine the holes and vulnerabilities of the protection system to penetrate the security in simple and efficient way.

Keywords

Internet attack, clean intruder, NTFS, ADS, Firewall, Address Spoofing Attack.

---

* AL-Rafidian University College, Computer science department.

1- Background on Internet Security [1 - 3]:

The information on the Internet sites are readily available to any user, but in truth there is sensitive information must be protected. So, data security on Internet site must attempt to protect the privacy of users and their data, control access to restricted data and resources and fraudulent transaction. An ***attack*** is generally unwanted intrusion. Attack strategies often concentrate on vulnerabilities (also called holes or backdoors) of specific operating system of networks or hardware of network.

There are two general types of attacks ***Passive Attack*** and ***Active Attack***. Such attacks include masquerades by IP address spoofing, modification or fabrication of files or messages and the use of the available resource.

For that many types of protection systems are appears such as

1-Firewall protection system, which has many types of firewalls installed on many types of configuration, it tend to differ in its approach but can be characterized as firewalls block traffic and firewall permit traffic. **2- Intruder detection,** which tend to monitor and audit the behavior of the user to detect if the user was author or an intruder. **3-Anti viruses**, some characterize viruses by their "signatures". The others called heuristic scanners they work in general with specific types of viruses have no signature.

2- The Possible Attacks on the Protected Site [4]:

a- SYN Flooding Attack:

This attack associated with the three handshaking of TCP session. TCP session begin with a three-way handshake between the two endpoints of the connection. Assume host A wants to make a SYN Flooding attack to host B called victim host. A sends a SYN packets to B, these sent packets have unreachable source IP address host. B replies with a SYN/ACK packet to the unreachable address. So, B would wait the

unreachable address host forever to finish the three-way handshake with a TCP ACK packet. This will drag the machine's performance down (host B).

b- Ping of Death Attack:

Ping is an Internet Control Message Protocol (ICMP) echo request packet. In this attack the attacker faking a source address (impersonate the source address of the victim server) and sending numerous ICMP packets to different destination addresses. So these ICMP echo reply send to the victim machine (the attacker impersonate its address) instead to send them to the spoofed machine. When the victim machine receives these ICMP s echo reply from many nodes, probably be unable to perform any useful functions. This attack is not really a network problem but rather a buffer overflow problem.

c- IP Address Spoofing Attack:

The most dangerous active attack on the Internet is IP spoofing, because the attacker uses one machine to impersonate an author machine. So, attacker would communicate with protected site as authorized person. IP spoofing summarized in the following points:

(1) Attacker makes Denial-of-Service attack to the authorized machine. Denial-of-Service Attack means the attacker floods the server with requests to connect to other servers that don't exist. The server tries to establish connection with the none exist servers and wait for response while being flooded with thousands of other bogus connection request. This causes the server to deny service to legitimate users because it is overwhelmed trying to handle the bogus request. The denial-of-service attack may forward directly to the servers in the protected site.

(2) After making denial-of-service attack on the authorized machine, attacker makes hardware address spoofing is, to a certain extent, also dependent upon the card connect the computer with the network.

(3) If the attacker success in spoofing and passing to protected site, he must create a more suitable hole through which to compromise the site (he should not be forced to spoof each time he wants to connect).

d- Impersonate One Half Of A Session:

If network traffic between two nodes flows in the clear and if you know the protocol that the nodes are using, you can disable one of the nodes and impersonate the node using IP Address Spoofing Attack.

e- Session Hijacking Attack:

Session hijacking is conceptually simple. Two endpoint nodes of communication session send traffic in the clear. Your location is such that all traffic between these two nodes must flow through a node that you control. On your node you sniff packets (listen to the packets) and create arbitrary IP traffic.

3- Windows NT [5 - 10]:

In the following sections some details will be given on windows facilities:

3.1- The Security of Windows NT:

Windows Network Technology (NT) support static packet filtering of IP traffic. While the capabilities of this filtering are somewhat rudimentary, they can be useful for providing some additional security. Since NT uses static packet filters, it is not capable of maintaining state. This means that NT's filters are unable to distinguish between legitimate acknowledgment traffic and possible attacks. Static packet filtering controls traffic by using information stored within the packet header. At the filtering device the attributes of the data stored within receives packets and the packet headers are compared against the access control policy. Depending on how this header information compares to access control policy, the traffic is either accepted or rejected. A static packet filter can use the following information when regulating traffic flow:

- Destinations IP address.
- Source IP address.
- Destination Port Number.
- Source Port Number.
- Flag (TCP only).

Windows NT does not allow you specify the direction of traffic when applying your packet filters. This means that if someone is able to compromise your system, NT's packet filters will be unable to prevent that attacker from relaying information off the system. Finally, NT does not allow you to filter on IP address. This means that any access control policy you create will be applied to all systems equally. In other words, you could not create an access control policy that only access from a specific subnet.

3.2- NTFS and ADS:

ADS means Alternate data stream which is a feature in Windows NT file system is named NTFS (New technology files system).

When the software companies shipped software with less bugs, a software was born, its named Windows NT but whenever the software was out to communicate with other software it was difficult to be compatible with other software like Mac cause apple used a language called Macintosh Hierarchical File System (HFS) and Windows NT used NTFS so they couldn't communicate properly so Windows company gave their software some special feature called additional data stream so that it exchange information with Mac.

Some of us who have used both Macintosh and Windows as OS ‘s might have come across a strange thing that unlike in windows in Mac OS files don’t generally extension’s like exe, doc , flat, txt and others but still the operating system is able to associate file .This is basically due to the fact that Macintosh files have two “forks”. The resource fork, which contains this information, and the data fork, which contains the executable code itself. Now more often than not there is a communication between windows box and a Mac now how the file association can be maintained and recognized was a bit problem so . When Windows NT 3.1 came out, it had compatibility support for AppleTalk, meaning that NT and MacOS users could easily exchange data.

This caused a problem however, since there was no way to copy the resource fork and the data fork of a file directly onto the NT file

system. Doing so would only copy the data fork, since the resource fork wasn't physically in the file, but in a separate stream. (In other words, the data and resource fork don't occupy the same cluster on disk, or are part of the same contiguous file). Microsoft then had to implement NTFS ADS, which meant that NT would see the resource fork as another stream, and would be able to copy it along with the file onto a Macintosh computer.

4- The Proposed Method:

The proposed method aims to penetrate the file system of the server in a protected site and inserts any malicious programs in any files in that server with hidden signature and without the knowledge of the site's administrator in an authorized manner. This accomplished according to the following steps:

1. Penetrates the protected site that the intruder wants to attack.
2. Using the weakness of the NTF and ADS in Windows NT to insert the malicious program to built new holes in the server which makes the intruder attacking this protected site in much more flexibility.

4.1- Penetration of the Protected Site:

A protection systems protects networked computers from intentional hostile intrusion that could compromise confidentiality or results in data corruption. See figure (1).

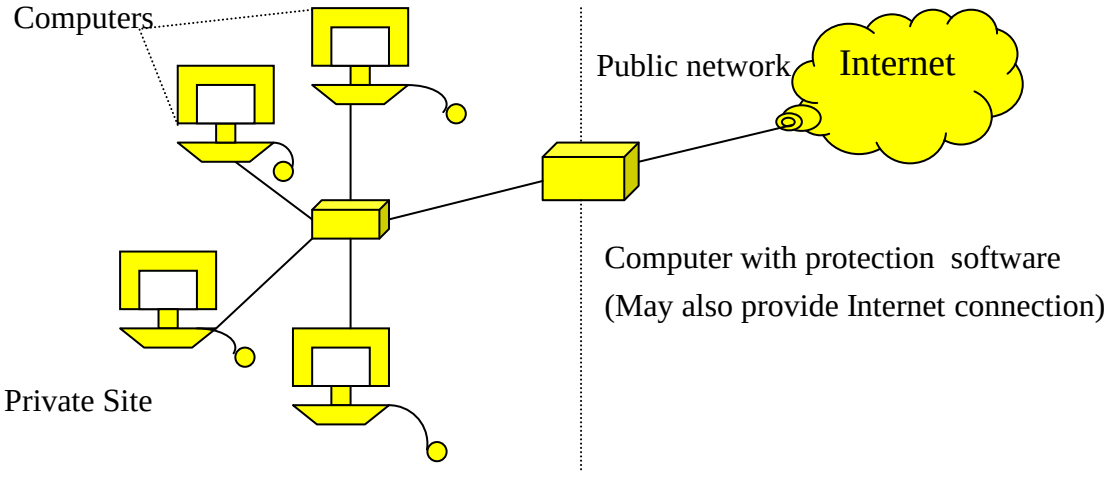

Figure (1) Computer with protection software.

A protection system is placed between the site and the rest of the Internet; as shown in figure (2).

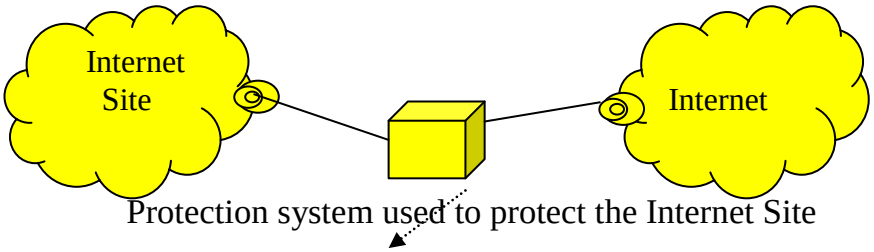

Figure (2) Position of the protection system used to protect the Internet site.

Generally all the types of attacks and types of protection systems on the Internet depend on packet analysis. The analysis may focus on the data in the packets or on specific fields of the TCP/IP protocols headers such IP, TCP, UDP, ICMP headers [4].

From this point the IP address spoofing attack would be the best one to penetrate the protected site. Most of these protection systems depend on analysis of the data and header of the packet to detect if the packet is authorized or not. There are no detection about the session request/acknowledgment stream. So the penetration would be done by the IP spoofing attack as declared in the previous sections and here the diagram of that attack would presented, see figure (3).

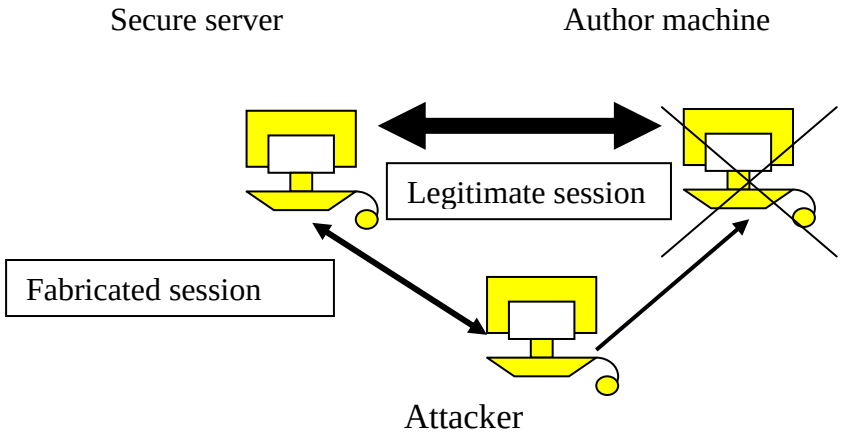

Figure (3) IP spoofing attack.

4.2 – Using the weakness of the Windows NT:

The current problem with streams is that many Windows NT users including (administrators) are not aware that streams exist and even if they know of them have no simply method of detecting them.

Microsoft does not provide tools for reporting what streams exist!. NTFS supports multiple data streams, where the stream name identifies a new data attribute on the file. A handle can be opened to each data stream. A data stream, then, is a unique set of file attributes. Streams have separate opportunistic locks; file locks, and sizes, but common permissions. This feature enables you to manage data as a single unit. The following is an example of an alternate stream:

myfile.dat:stream2

A library of files might exist where the files are defined as alternate streams, as in the following example:

library:file1
:file2
:file3

A file can be associated with more than one application at a time, such as Microsoft® Word and Microsoft® WordPad. For instance, a file structure like the following illustrates file association, but not multiple files:
program: source_file
:doc_file
:object_file
:executable_file

You can have a file with 1 byte in the official main data stream and some hundred MB in one or more alternate data streams. What do you expect the dir command, file manager or explorer to show as the size of this file? It is 1 byte! That means a freak can hide quite a lot of data in alternate data streams and nobody will know.

So What's Wrong With ADS

Well anyone who has access to your computer can play a dirty trick like the one I am going to mention. IT is possible to create a text file lets say 1 byte file and can add a 4 GB data to it in alternate stream. Your 4 GB space will be eaten up and what happens when you check that innocent text file. The windows explorer will show it's size only a s 1 byte and will give you no information about 4 GB data associated with that file in Alternate data stream. Also the dir command will too fail to give you any information about alternate data stream.

One of the worst things that can be done is to attach a binary file or exe to a text file. Every time that text file is run the exe will also run without knowledge. CTRL_ALT_DEL will also be helpless in detecting the exe and to tell you a virus writer could possibly attach a virus or Trojan in your explorer.exe as alternate stream. This means the virus/Trojan will run every time your PC starts without your antivirus getting any air of it.

The information in this research applies to:
Microsoft Win32 Application Programming Interface (API), when used with:

The operating system: Microsoft Windows NT 3.1
The operating system: Microsoft Windows NT 3.5
The operating system: Microsoft Windows NT 3.51
The operating system: Microsoft Windows NT 4.0
The operating system: Microsoft Windows 2000
The operating system: Microsoft Windows XP

4.3 – After the Clean Intrusion:

Now after the penetration of the protected site is done and clean intrusion, insert malicious programs, is completed. The intruder surely would has get much more known about the holes and vulnerabilities of this site or get sensitive data files from the intruded server. This is done according to the inserted programs type.

Because all the protected sensitive sites always make updating to their servers and operate many scanners on the data resides on them, so the clean intruder always must change the manner by inserting different malicious programs and changes the files used to be infected with these malicious programs.

5- Conclusion:

The proposed method represents a new approach in intrusion. To apply the proposed method, it needs a knowledge and expertise from the intruder in all different types of attacks, protection systems and good understanding of Windows NT principles. The IP address spoofing is the most suitable attack to penetrate the protected sites, because it has a very precision steps and much less protection systems tracking the session request/acknowledgement stream. Windows NT famous as the secure OS, so many sensitive sites make it the basic of its security, from that the intruder would take the advantages of weakness in it as declared in the previous sections and make clean intrusion hard to be detected. By that intrusion which include insertion of intruder programs, the human intruder would discover many holes that make the data in the server of this site readily available to him.

6- References:

1. Binnion .R . , Ltd .T .D . , **" Network and Internet Security Issue and Solutions "**, Town send , Taphouse, 1999.
2. Banks .M .A ., **"Computer Security"** , SYBEX, Inc., 2001.
3. ZDNet Research center Business and Technology , White Papers , **" Intrusion Detection -Deploying The Shomiti Century Tap –"**, METAS , ZCInc.ZDNet, 2001. **http://WWW.ZDnet.com.**
4. Unix Propeller Head ,**" Maximum Security : A Hacker's Guide to Protecting Your Internet Site and Networks"**, Macmillan Computer Publishing, Sams Net, 2000.
5. Al-hamami,A.H & S.H.Hassan, " Selecting Controllers for Networking Environment.", Al-Rafidain Magazine, No. 14, 2003, Al-Rafidain University College, Baghdad, Iraq.
6. Al-Hamami,A.H & S.H.Hassan, " A proposed Firewall Security methods against different types of attacks.", Computer Magazine, No. 12, University of Technology, 2004, Baghdad, Iraq.
7. www.windowsecurity.com/articles/Alternate_Data_Streams.html.
8. www.networkoverload.net/files/docs/ads.pdf.
9. www.cknow.com/vtutor/vtntfsads.htm.
10. Stallings .W. , **"Operating System Internet and Designees Principle"**, Third Edition, U.S.A, 1998.