A Proposed Firewall Security Method against Different Types of Attacks

Prof. Dr. Alaa AL-Hamami* Soukaena Hassan Hashem**

Received on: 17 / 7 / 2004

Accepted on: 30 / 12 / 2004

Abstract

There are measures that can be taken to protect users from objectionable or inappropriate Internet content and secure the LAN from theft, modification, or deletion of data. Firewall is one of many security measures that can be used to protect networks. Although firewalls are powerful, they suffer from many types of attacks.

This paper concentrates on one particular aspect, which is providing firewalls security against five types of attacks. These attacks are: SYN Flooding, Ping of Death, IP Address Spoofing, Impersonate one-half of a Session and Session Hijacking. This can be done by building a specific strategy for a firewall; a strategy that has three procedures, some of which could be stood for more than one attack.

الخلاصة

هناك العديد من طرق الحماية التي تؤخذ بنظر الاعتبار لحماية بيانات المستخدمين في الشبكات المحلية المرتبطة بالانترنيت من السرقة والتحوير والتدمير. اشهر طرق الحماية لمواقع الانترنيت هي أنظمة جدران النار، والتي برغم قوتها، فانها تكون معرضة لعدة انواع من الهجوم. يركز هذا البحث على بناء جدار ناري ضد خمسة انواع من الهجوم، وذلك من خلال احتوائه على ثلاثة اجراءات يستطيع بعضها مواجهة اكثر من هجوم واحد.

Keywords

Firewall, protection, Internet, attack.

1- Introduction

A firewall is a piece of hardware/software used to protect a computer network against Internet-based theft, destruction or modification of data. The National Computer Security Association (NCSA) in the USA classifies firewalls into three categories: First, **Packet Filters:** They examine data passing to and from a network and can block access according to rules restricting TCP/IP ports numbers, source and destination addresses or protocol types. Second, **Application-Level Proxy Servers:** They examine data in the upper level of this examination, which is different from one application type to another. Third, **Stateful Inspection:** It examines all the layers of OSI and TCP/IP to either accept or reject the requested communications [1].

An attack is generally unwanted intrusion [2]. Attack strategies often

*Department of Computer Science of Al-Rafidian University College.

***Department of Computer Science and Information System of the University of Teechnology.

concentrate on vulnerabilities (also called holes or backdoors) of specific operating system or hardware of networks [3,4]. There are two general types of attacks: ***Passive Attacks; w***here the intruder does not interfere with the system or attempt to cause any damage to it. But he simply monitors private data, usually in transit, and if necessary makes cryptanalysis to attempt to break any encryption in use, anyway it is also dangerous [2]. ***Active Attacks;*** where the intruder interferes with data or resources in the targeted system or network. Such attacks include masquerades by address spoofing, modification or fabrication of files or messages and the use of the available resource [2].

Computer criminals are kind of people who penetrate security of systems. They are defined as follows: **i)** H***ackers*** are people who gain unauthorized access to computer or telecommunications systems, often just for challenge of it. A hacker enjoys working with computers and spends numerous hours writing programs to penetrate secure systems. **ii)** ***Cracker***s are people who break into or otherwise violate the system integrity of remote machine, with malicious intend. Crackers, having gained unauthorized access, destroy vital data, deny legitimate users service, or basically cause problems for their target [4].

To ensure the security on the Internet there are specific and accurate requirements and techniques for these requirements interpreted in the following**: i) Secrecy** is concerned with ensuring that data can only be read by those authorized to do so. For data transiting a communication system, it is very difficult to prevent a sufficient well-equipped intruder from intercepting a message and reading its contents [2]. **ii) Authentication** is concerned with providing mechanism to allow an entity to prove its identity. **iii) Integrity** ensures that data and resources can not be modified by unauthorized persons [5]. **iv) Availability** protects system resources from attacks that might render them unusable. Such attacks may involve any thing from the actual destruction of hardware, to the introduction of malicious programs such as viruses, worms or Trojan horses into a system [2].

2- Attacks On Firewalls

Some of the most common attacks on firewalls are:

a- SYN Flooding Attack.

b- Ping of Death Attack.

c- IP Address Spoofing Attack.

d- Impersonate One Half Of A Session Attack.

e- Session Hijacking Attack.

2.1- SYN Flooding Attack

This attack is associated with the three handshaking of TCP session.

TCP session begins with a three-way handshake between the two endpoints of the connection as shown in Figure (1). Assume host A wants to make a SYN Flooding attack to host B called victim host. First, A sends 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 [4]. This will drag the machine's performance down (host B). A well- known trick is to send the victim a large number of SYN requests. The attacked machine does not only spend time sending back acknowledgement messages, but it also remains in a state that is waiting for the third part of the handshake [6].

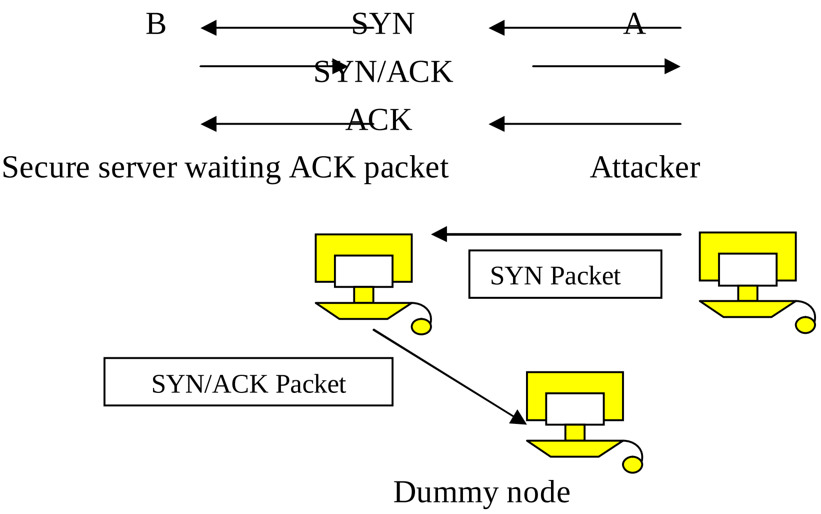


Figure (1) Three handshaking process with SYN Flooding Attack strategy

2.2- Ping of Death Attack

Ping is an Internet Control Message Protocol (ICMP) echo request packet, where, ICMP is a protocol used by IP when sends an error message and ICMP uses IP to transport messages [7]. In this attack, the attacker fakes a source address (impersonates the source address of the victim server, that the attacker wants to attack it) and sends numerous ICMP packets to different destination addresses (See

Figure 2). In new versions of this attack, an attacker sends ICMP packet with a broadcast address for the destination. The common ICMP message to send is echo request. This will be implemented at the application layer by the ping program. A probe is sent out on network to test the existence of a particular node by specifying a destination address. The nodes that receive the echo request send an ICMP echo reply to the source address that appears in the packet, so these ICMPs echo reply are sent to the victim machine (the machine that the attacker impersonate its address) instead of sending them to the spoofed machine. When the victim machine receives these ICMPs echo reply from many nodes it would probably be unable to perform any useful functions [6].

This attack is not really a network problem, but rather a buffer overflow problem [6].

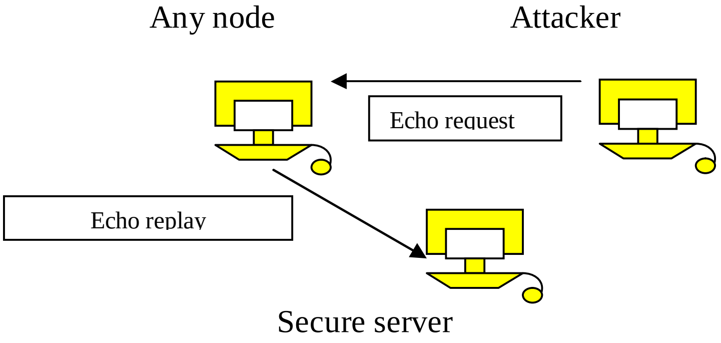


Figure (2) ping of death attack strategy

2.3- 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 as shown in Figure (3). So, attacker would communicate with protected site as authorized person [4]. IP spoofing is summarized in the following points:

a- Attacker makes Denial-of-Service Attack to the authorized machine [4]. 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 inexistent servers and wait for response while being flooded with thousands of other bogus connection requests. This causes the server to deny service to legitimate users because it is overwhelmed trying to handle the bogus requests. The Denial-of-Service Attack may forward directly to the servers in the protected site [3].

b- After making Denial-of-Service Attack on the authorized machine attacker make hardware address spoofing that is, to a certain extent, also dependent upon the card connection of the computer with the network [4].

c- If the attacker succeeds 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) [4].

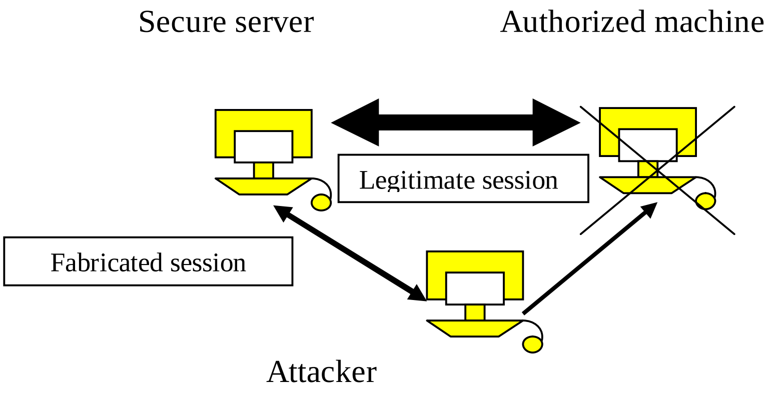


Figure (3) IP spoofing attack

2.4- 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 as shown in Figure (4).

Disabling a node is accomplished by physical storage or by flooding the target node with continual network traffic. This hack is different from others because the attack assumes that services of messages must be exchanged as a part of the protocol [6].

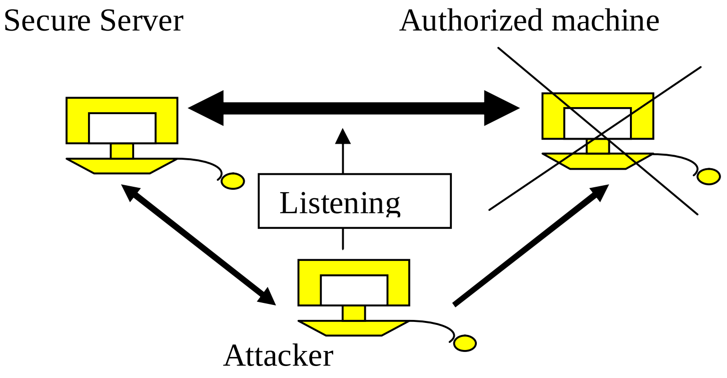


Figure (4) impersonate one half of a session

2.5- 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. You must handle both sides of the communication if you want to spoof both nodes into doing what you want [6] (see Figure 5).

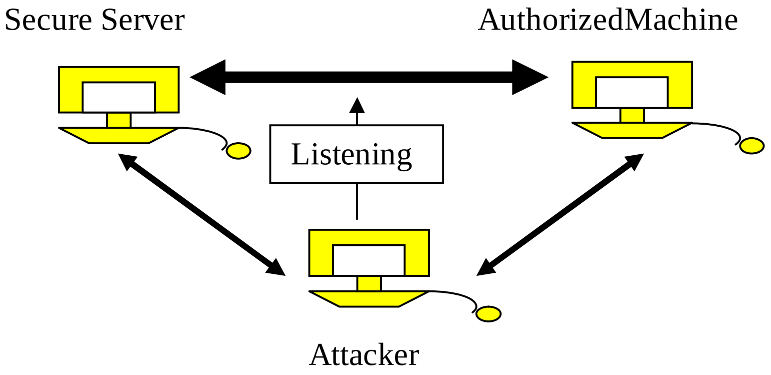


Figure (5) session hijacking attack

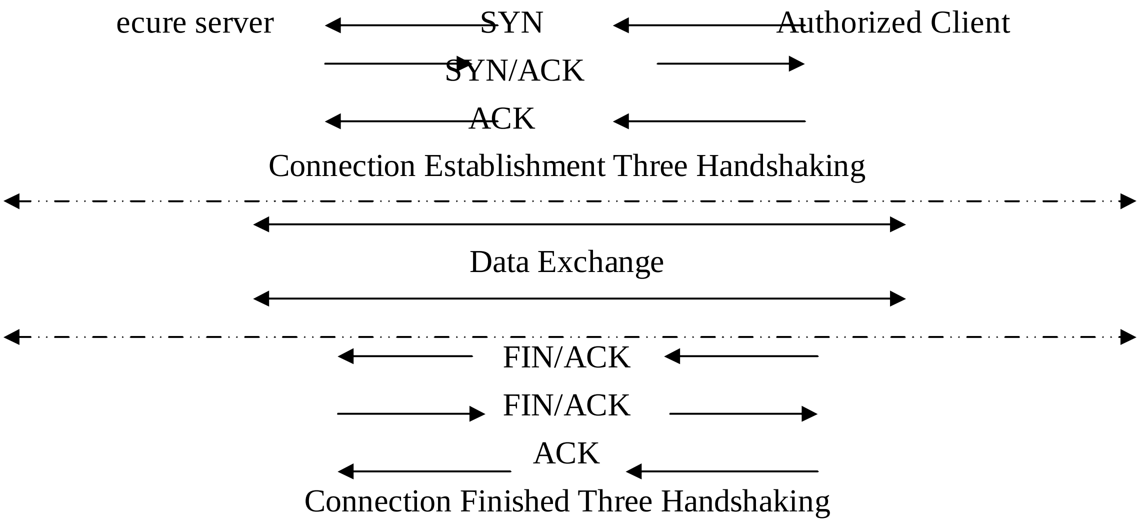
3- The Proposed Protection Strategy

The proposed strategy includes three procedures to face some famous types of attacks on the firewalls protection systems. These procedures are declared in the following sections:

3.1- SYN/ACK Check Up procedure

It is the most important procedure in the proposed protection strategy. This procedure in common provides security with TCP connection (TCP session).

As known, TCP is a connection-oriented and reliable transport protocol. When the authorized host communicates with the secure server: first, establish a connection by three handshaking, then exchange data and at last finish the connection by ending three handshaking as shown in the following algorithm:


ecure server
SYN
Authorized Client
SYN/ACK
ACK
Connection Establishment Three Handshaking
Data Exchange
FIN/ACK
FIN/ACK
ACK
Connection Finished Three Handshaking

TCP header contains the SYN field, which identify the number of bytes in the TCP segment and ACK field, which detect that the recipient receives these bytes and expects the next byte. This rule would be very important in security as declared in the following points:

1- SYN/ACK checkup in the connection establishment of three handshaking. The legitimate and secure three handshaking depend on checking the ACK found in the received packet by the secure server during connection establishment:

IF (ACK (in received packet) = SYN (previous packet sent) + 1)

THEN

It legitimates and secures three handshaking.

The intruders who stay in the middle between authorized client and secure server can not know any thing about the SYN/ACK of three handshaking for connection establishment because the entire packet must be encrypted when sent from or to secure server. This point in this procedure represents the **circuit level firewall**.

2-For data exchange after connection establishment three handshaking, the SYN/ACK must be checked up by the secure server to guarantee the intruders can not send their packets after three handshaking because the SYN/ACK in the packets transmitted between the two hosts aren't checked.

The check up for data exchange detected by the following equation:

IF (ACK (received packet) = SYN (previous packet sent) + BUFFER (previous packet) THEN

It legitimates and secures three handshaking.

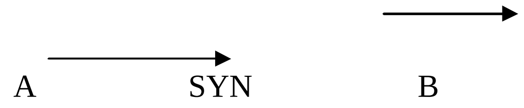
This procedure provides good protection against the SYN Flooding Attack, IP Impersonation Attack, and Ping of Death Attack. This can be done by the assurance that the complete session is legitimate.

3.2- Three Handshaking Proxy Procedure

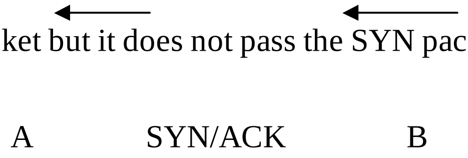
In a normal case when packets pass the protected site to servers these packets must pass through a Bastion host to be submitted to a specific procedure.

We propose a protection procedure for servers to be used for defending against a SYN flooding attack. The SYN flooding attack works by sending SYN packets with the source address of unreachable hosts that would not reply to the SYN/ACK packets sent by the destination. The three handshaking proxy counters the attack by making sure that the three-way handshaking is actually completed between the secure authorized site and bastion host before sending a SYN packet to the secure server, destination of connection. To declare this procedure, let secure server be S, Bastion host be B, authorized site be A, and note the following points:

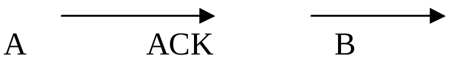
1. Suppose A requests connection to secure server. First, A sends SYN packet to B.



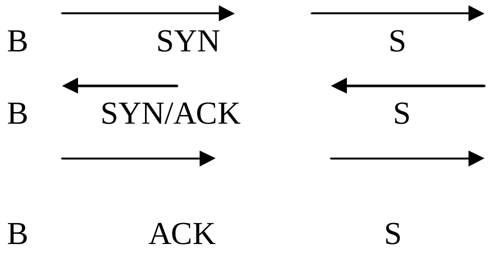
2- B receives the SYN packet but it does not pass the SYN packet to S, B rather sends SYN/ACK to A directly.



3- If A sends ACK packet to B, then the connection is established between A and B.



4. Now B would make a connection establishment between B and S but it would use the SYN and ACK of A.



This procedure represents generic proxy, because it works with any application. It provides good protection against the SYN Flooding Attack by making bastion host as a proxy to establish the connection between the secure authorized site and the secure server.

3.3- Encapsulation and De-Encapsulation Procedure

All packets related to secure server must be secure packets. These secure packets are any packets passing to the secure server or out from this secure server. In the proposed protection strategy, a procedure called **tunnel mode of Encapsulation Security Payload (ESP)** is used as shown in Figure (6). In this figure, we see that the ESP header contains SPI field. This field specifies a security association with the digital signature and sequence number (a monotonically increased value) and there is **no ESP Trailer** because the digital signature which is used by RSA does not need any padding in its algorithm. Here the shaded area is that encrypted by **Digital Signature**.

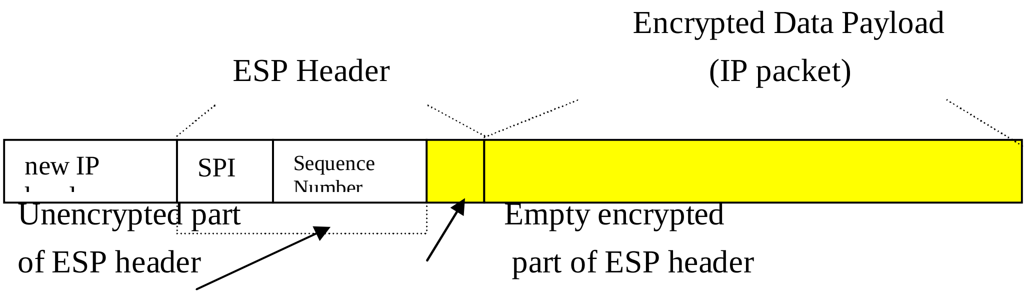


Figure (6) ESP tunnel mode; shaded area encrypted by digital signature.

For each secure packet enters to secure server this procedure would de-encapsulate and decrypt the entire packet. For each secure packet leaves the secure server this procedure would encrypt the entire packet and then encapsulate the encrypted packet. For secrecy and authenticity of data, in fact for secrecy and authenticity of the entire packet during its travel over the Internet the best solution is to use Digital Signature method of the RSA encryption system.

This procedure provides good protection against the Impersonate One Half of A Session and Session Hijacking Attacks. The reason is that this procedure encrypts the entire packets when they travel over the

Internet, so the information of network layer, transport layer and applicatin layer is completely disguised.

4- Conclusions

The study shows the possibility of defending firewalls against some specific types of attacks that faced them. This is done by using a strategy having three procedures added to the firewall software to improve the firewall security. Each procedure in the proposed strategy has a specific role, as declared in the following points:

1-The Three-Handshaking Proxy procedure protects server from the SYN Flooding Attack. This is done by making the bastion host as a victim host.

2-SYN/ACK checkup procedure protects server from the SYN Flooding Attack, Ping Of Death Attack, and IP Spoofing (IP Impersonation) Attack. This is done by checking up the SYN/ACK of all packets that enter and leave the protected site along the session (not only in the three handshaking).

3-Encapsulation and De-Encapsulation procedure in the firewall aims to provide secrecy, authenticity and privacy for entire packets that travel over the Internet. Digital Signature encryption system is good encryption mechanism in networks of open nature and we do not need to trail the packet encrypted to complete the 32-multiple words as in the DES encryption mechanism. This procedure protects the firewall against impersonate one half of a session and session hijacking attacks.

References

1- Binnion R., Ltd. T.D., ” **Network and Internet Security Issue and Solutions”**, Town send, Taphouse, 1999.

2- Mackenzie L., **"Communication and Networks”**, Mc-Graw Hill International (UK), 1998.

3- Cold J. E., Rawles P. T., **"Local Area Network: A Business-Oriented Application"**, Second Edition, John Wiley & Sons Inc., 2000.

4- Unix Propeller Head, **"Maximum Security: A Hacker’s Guide to Protecting Your Internet Site and Networks”**, Macmillan Computer Publishing, Sams Net, 1997.

5- Pfleeger C. P., **”Security in Computing”**,Prentice-Hill International Editions , 1989.

6- Escamilla T., ”**Intrusion Detection Network Security Beyond The Firewall”**, John Wiley & Sons Inc., 1998.

7- Comer D. E., ”**Computer Network and Internets with Internet Application“**, Third Edition, Prentice-Hall Inc., 2001.