Application Firewall Security for Web and SQL Services[1]

IACOB, Nicoleta Magdalena
Spiru Haret University
Scientific Research Center in Mathematics and Computer Science
nicoleta.iacob_2007@yahoo.com

DEFTA, Costinela-Luminiţa
Spiru Haret University
Scientific Research Center in Mathematics and Computer Science[2]
lumi.defta@yahoo.com

Abstract

In this paper we will categorize the most frequent security threats associated with web and sql servers and present the ways to mitigate some application security threats such as sql injection and denial of service attack using the capabilities of a network device from a recognized leader in network security.

Keywords: *SQL injection, security, SQL services, web services*

ACM/AMS Classification: 68P15

1. ***Introduction***

As networks grow and support more and more services and applications, they become more vulnerable to security threats ([6], [7]). To combat those threats and ensure that applications are not hacked, security techniques must play a fundamental role in any type of environment.

Web applications are exposed to some specific vulnerabilities ([4], [5]) due to their method of access (web browsers) and integration with databases in backend. The actual web servers configurations commonly presents to users multiple web applications running on a single server and available through some standard network ports (80 and 443), giving attackers a big area to compromise.

2. ***Web and database servers security threats***

There are many common attacks that can occur against different applications servers and they depend on the installed applications (for example, web, sql, erp

[1] Citation: Iacob N.M., Defta C.-L., *Application Firewall Security for Web and SQL Services*, ”An. Univ. Spiru Haret, Ser. Mat.-Inform.”, 12(2), pp. 25-30, 2016.

[2] Invited Researcher.

services), operating system running on the server (for example, Windows or Linux), and environment (network where the server is running). In this section we will briefly describe some of the generic attacks that can compromise a server [1]:

- *Denial of Service (DoS)* is an attack in which one system attacks another with the intent of consuming all the resources on the system (such as bandwidth or processor cycles), leaving nothing to use for other legitimate requests from normal clients. This is accomplished by increasing traffic on web site so much that the victims server becomes unresponsive.
- *Distributed Denial of Service (DDoS)* is an attack similar with DoS, but at a larger scale, because the attack is orchestrated from multiple systems from many countries around the globe. The most common DDoS attacks are:

  a) *port scanning attack.* A port scanning attack is performed by systematic scanning of a host using some programs. For example, an attacker can scan a Web server with the intention of finding exposed services or other vulnerabilities that can be further exploited;

  b) *ping flooding attack.* A ping flooding is a classical type of attack where the attacker sends ICMP echo requests packets as fast as possible without waiting for replies;

  c) *SYN flooding.* This attack requires knowledge of the TCP/IP protocol suite because this is a network protocol targeted type of attack. In SYN flood the attacker sends a SYN packet to target host which then respond with SYN acknowledgement. In the end of communication, the attacker does not send any ACK packet back to the target host and this causes the connection to remain in half open state. TCP connection established to the attacker host is not ending, waiting for the session to expire. The attacker continues sending new SYN packets until TCP SYN queue is filled and cannot accept any new connections;

  d) *IP packet fragmentation attack.* In this attack, an attacker change the TCP/IP protocol behavior to break packets up into smaller pieces, or fragments, that bypass most intrusion-detection systems.

- *Password attacks.* Password attacks can be implemented using different methods, including brute-force attacks and packet sniffers. Although packet sniffers can reveal user accounts and passwords, from network packet captures where an attacker can see in clear or decrypt some passwords, password attacks usually refer to specific attempts to identify a user account, password, or both. A brute-force attack is performed using some programs that run across the network and attempt to log in to the attacked server using various users and passwords. When a user account is compromised and if this account has enough privileges, the attacker can gain access to the system.
- *Cross-site scripting or XSS* is a technique that makes use of vulnerabilities in web applications. In a cross-site scripting attack, data is entered into an application which is later written back to another user. If the application is not coded in such a way to validate the data correctly, it may simply echo the input back allowing the insertion of malicious code into the web page.

- *SQL injection* type of attack search for a vulnerability in the database associated with a web application. The malicious code is inserted into strings that are later passed to the SQL server, parsed, and executed.
- *Malware* is a malicious software. It consist of viruses, bots, spyware, worms, trojans, rootkits, and any other software intended to disrupt normal user activity and collect personal data.

3. ***SQL injection and DOS attacks***

In the diagram ([2], [3]) below (Figure 1), we figured a typical network and systems architecture, consisting of a database server and a web server to serve client requests. We choose an Adaptive Security Appliance from Cisco to defend servers from various security threats. Cisco ASA provides an end to end security solution, offering protection from OSI (Open Systems Interconnection model) layer 2 to 7.

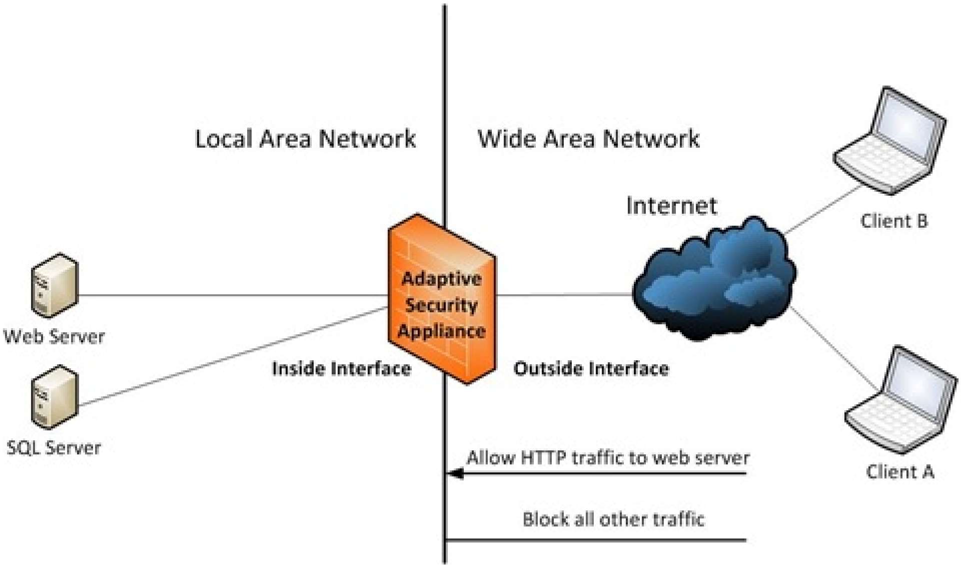

Figure 1. *Typical network and systems architecture*

The proposed defense system will be active at 2 OSI layers:

- *layer 3* – ip layer;
- *layer 7* – application layer.

As a layer 3 firewall, we configured an access list on appliance that permits to enter in local area network only http traffic destined for the web server and have applied this access list on outside interface (the interface facing Internet). All other traffic will be dropped at the outside interface by the security appliance. By using such an inbound ip packet filter, the sql server is not exposed to the Internet and web server is exposed only on port 80 (required to server http requests to students using e-learning web platform). If a packet is denied by the access list, the security appliance discards the packet and generates a syslog message indicating that such an event has occurred.

As a layer 7 firewall application, we configured the appliance to protect servers from a SQL injection attack and denial of service attack.

3.1. **SQL injection attack**

To understand what is a sql injection attack, we analyze the implementation of a login page that searches for records in a database which matches the given username and password, like in example below:

$ *sql = "SELECT * FROM users WHERE username= n '* $ *username n ' AND password= n '* $ *password n '; ";*

If the input is not validated correctly, it would be possible to set $ username and $ password to be "' OR '1'='1". The resulting SQL query would be:

*SELECT * FROM users WHERE username=" OR '1'='1' AND password=" OR '1'='1';*

This SQL query will always return a non-empty result, bypassing the login procedure and enabling the attacker to access the application. By successfully exploiting an SQL injection vulnerability, the attacker could gain administrator access to the application or even the operating system where database is installed.

In order to detect the SQL injection attack, adaptive security appliance uses regular expressions (regex) embedded with Modular Policy Framework to inspect specific HTTP data patterns ([8], [9]). It will check for the SQL command UNION ALL SELECT. With the regex supplied from vendor documentation, this is the configuration on the appliance:

```
regex SQL _ regex _ 1
[uU][nN][iI][oO][nN]([ % ]2[0bB] | [+])([aA][lL][lL]([ % ]2[0bB] | [+]))?[sS][eE][lL][eE]
regex SQL _ regex _ 2
[Ss][Ee][Ll][Ee][Cc][Tt]( % 2[0bB] | +)[ ^ n r n x00- n x19 n x7f n xff ]+( % 2[0bB]
| +)[Ff ][Rr][Oo][Mm]( % 2[0bB] | +) //regex definition
class-map WebServers
match port tcp eq www
class-map type inspect http match-any SQL-map
match request body regex SQL _ regex _ 1
match request body regex SQL _ regex _ 2
policy-map type inspect http drop-SQL
parameters
body-match-maximum 3000
class SQL-map
drop-connection log // when is a regular expression match, the ASA will drop the
HTTP connection and generate a log
policy-map SQL-traffic
class WebServers
inspect http drop-SQL
service-policy SQL-traffic interface outside //service policy for sql is applied in inter-
face outside
```

3.2. **DoS attack**

We will describe how to prevent network attacks by configuring threat detection on adaptive security appliance. Using basic threat detection, the security appliance monitors the rate of dropped packets and security events due to the following reasons:

- Denial by access lists;
- Bad packet format (such as invalid ip header);
- Connection limits exceeded;
- DoS attack detected (such as a Stateful Firewall check failure);
- Suspicious ICMP packets detected;
- Packets failed application inspection;
- Interface overload;
- Scanning attack detected (for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake).

To enable basic threat detection we have to enter the following command:

threat-detection basic-threat

Next, we will change the triggers used for detecting DoS attacks:

threat-detection rate dos-drop rate-interval 500 average-rate 50 burst-rate 100

To view the hosts that the security appliance decides are attackers and to view the hosts that are the target of an attack, we have to enter the following commands:

show threat-detection scanning-threat attacker

respectively

show threat-detection scanning-threat target

Based on the output of the above commands, if we see that a host is attempting to attack our network, then we can block (or shun) connections based on the observed source IP address and other parameters. No new connections can be made until we will remove the shun.

shun source ip destionation ip port
shun 10.10.10.1 4.4.4.4 80

4. ***Conclusion***

All type of servers that run in a network environment are exposed to various security threats and taking appropriate security practices is an essential step in order to operate and maintain a secure server, because security practices help ensure the confidentiality, integrity and availability of information system resources. All the security techniques described in this article help assure a basic protection for information systems and represent the baseline for advanced protection techniques that must be applied at all network levels.

References

1. T. Boyles, *CCNA Security Study Guide*, Wiley Publishing, 2010.
2. N.M. Iacob, *Information Security for Web and SQL Services*, ”Proceedings of the 9th International Conference on Virtual Learning 2014. Models & Methodologies, Technologies, Software Solutions”, University of Bucharest, Faculty of Psychology and Educational Sciences, Siveco Romania, October 24-25, 2014, pp. 408-412.
3. N.M. Iacob, C.L. Defta, *HTTP Protocol Security for E-Learning Platforms*, ”Knowledge Horizons – Economics”, 7(3), 2015, pp. 144-146.
4. M. Pirnau, *The Analysis of the .NET Architecture Security System*, ”Computers and Artificial Intelligence (ECAI)”, 2013.
5. C. Pirnau, M.A. Botezatu, I.S. Grigorescu, *Databases Role Correlated with Knowledge Transfer Between Entities of a Cluster,* ”Mircea cel Batran Naval Academy Scientific Bulletin”, Volume XVIII, Issue 2, 2016, Constanta, Romania, pp. 111.
6. D.A. Popescu, N. Bold, O. Domşa, *Generating Assessment Tests with Restrictions Using Genetic Algorithms*, ”12th IEEE International Conference on Control and Automation (ICCA)”, 1-3 June 2016.
7. D.A. Popescu, G. Boroghina, *Web-Based Programming Model*, ”6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO’15)”, May 27-29, 2015, Istanbul, Turkey, IEEE Xplorer, pp. 1-4.
8. www.cisco.com – ASA configuration guides, accesed 2016.
9. www.owasp.org, accesed 2016.