Analysis and Research of the Most Common Security Threats for Informational Corporate Network

Ihor Beliaiev, Yuri Dovbush

Abstract – **An analysis of the most widespread vulnerabilities and attacks of corporate infomedia performed. The protection resources against network attacks and unauthorized access to network resources proposed and implemented.**

Keywords – **information security, network attack, DDoS, unauthorized access**.

I. INTRODUCTION

Nowadays most people can't imagine their lifes without modern infocommunications. That is why information security issues are extremely relevant and important. They require in-depth analysis and study, because of simultaneous development of information technology and methods of attacks in cyberspace.

An analysis of the most common of remote attacks and threats for information networks has been carried out in this paper. An informational corporate network of a university was used as an example. The network cannot be protected only by analysis of the security threats. Therefore, after examination of information security, there are proposed and implemented methods and means of protection against network attacks and unauthorized access to network resources.

II. PROTECTION AGAINST «DISTRIBUTED DENIAL OF SERVICE» ATTACKS

Information security should provide three main functions: availability, confidentiality and integrity of information. Information systems are created to provide certain services, so if providing these services becomes impossible, it is harmful for all members of information relations. The first threat for the availability of network is called DDoS (Distributed Denial of Service) attack.

The DDoS attack is an attempt to make a computer or network resource unavailable to its intended users. Such attacks are organized by botnets - networks of infected hosts (bots). Bots are usual computers, which are infected with viruses and controlled by hackers via standard network protocols such as IRC and HTTP. One common method of attack involves saturating the target machine with external communications requests, so it cannot respond to legal traffic, or responds too slowly. Such attacks usually lead to a server overload. The principle of a classic DDoS attack can be described as: attacker connects to the control panel transmitting commands to the zombie agents, which in turn begin the DDoS attack.

Ihor Beliaiev – Lviv Polytechnic National University, 12, Stepan Bandera Str., Lviv, 79013, Ukraine
E-mail: me@theghost.ru, ihor@beliaiev.com

One of the most popular among DDoS botnets DarkSpy was used to analyze the level of protection of a corporate university network against network attacks. It can execute several types of attacks, such as UDP flood, SYN flood, HTTP flood. The web page, which created the largest number of queries to the database of the corporate network, was chosen for the first attack. The central server of university network was overloaded just by a several tens of bots. None of the legitimate users could access to the information resources of the university.

The main weaknesses of the university's network were identified and several measures for protection against network attacks were proposed. There are few of them:

- web resources of the university's network were moved to a new and powerful server. This is necessary for processing a large number of requests, which are generated by infected attacker's hosts;
- the server was connected to a 1Gb channel. This is necessary to protect network against attacks such as UDP-flood, which overload the communication channel with generating harmful traffic;
- the server of the university used Apache as a web server. When there are many connections from remote hosts to server, Apache consumes all resources of this server. It was decided to use “light” web server Nginx as a front-end to Apache (so Apache was used as back-end). Webserver Nginx – is an optimum variant for the distribution of static content, it uses few system resources and consumes much less memory for concurrent requests than Apache, is has high fault tolerance and simple load control;
- a program for protection against network was created on the basis of the research. An algorithm of program is presented below (Fig.1). The program creates an array named MasIP. In this array there is a list of IP addresses, which request network resources, and the number of these requests from every address per second. If a host generates a large number of requests (N> 10) it is automatically blocked for a certain time (Tblok [k] = 10 min) and its address is added to an array MasIPtmp. Hosts that generate fewer queries (N <10) are considered as legitimate users and gain access to network resources. Elements from the array MasIPtmp are analysed again after time interval Tblok [k]. If the host continues to make many queries, it is considered to be infected and is added to array MasIPblock. If the network receives a request from an address, which is in the array MasIPblock, all requests from this address are rejected. The maximum allowable number of requests from one IP address per second can be chosen depending on the power of attack, server equipment and configuration.

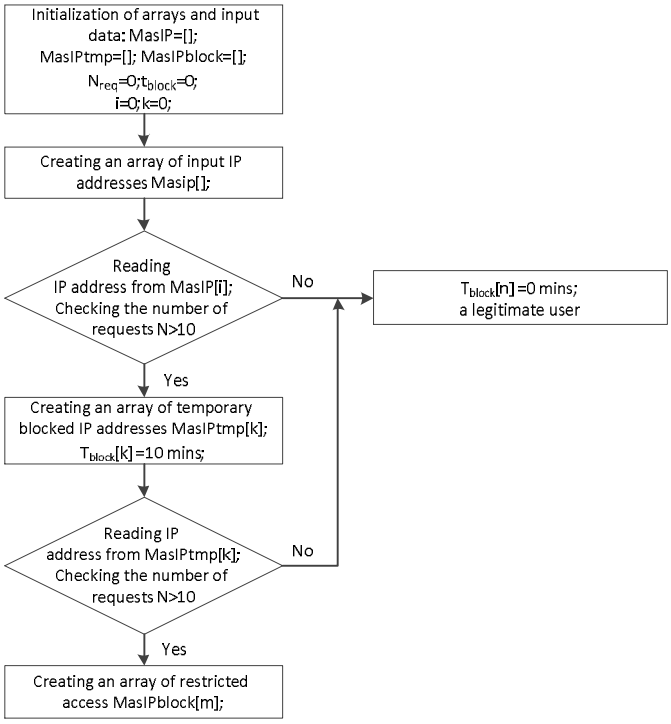

Fig.1. Algorithm of incoming network traffic analysis for protection against DDoS attacks

Those measures for corporate network defence agains DDoS attacks allowed protecting informational resources of university during powerful network attacks of several thousand of bots.

III. Protection against unauthorized access.

The main threats for confidentiality and integrity of information are: unauthorized access to confidential data, data interception and replacement, etc. Confidentiality and integrity of information may be compromised by few methods: identification of network services and exploration network, port scanning, interception of traffic, etc.

A security audit of the information network of the university was started from identification of network services and exploration network. It may help to get information about the system of the university. In our case, some useful information was obtained: the type of operating system of the server - FreeBSD; versions and types of content management systems (cms) of web sites - typo, joomla, phpbb; list of services - mysql, http, php 5.2.6, etc; list of domain names and subdomains, which are placed on the server.

Attempts to access "directly" to these services haven't provided any results, so it was decided to check all domains that are located on the university server. On one of the domains were found a few vulnerabilities. So an access to the site's administration panel was obtained using an appropriate exploit.

Then the search for possibility of uploading php files to the server using the administration panel was made. After analysis of all services and applications of administration panel, an obsolete version of html-editor FCKeditor was found. It allowed uploading any php file to the server. Specially formed packet for remote administration - so-called shell was uploaded to the server. It opened access to many functions including the command line one.

Shell, which was downloaded to the server opened access to all web resources of the university but with limited rights. Full access (root) to the informational corporate network of the university was received using exploits fot the FreeBSD 6.1.

As a result of the security audit there were found few critical vulnerabilities in the protection system of the university network. They provided full root access to all resources of the network. If actions mentioned above was made by an attacker then any information from the server, e.g. user passwords from different services and databases could be in his hands (Fig.2).

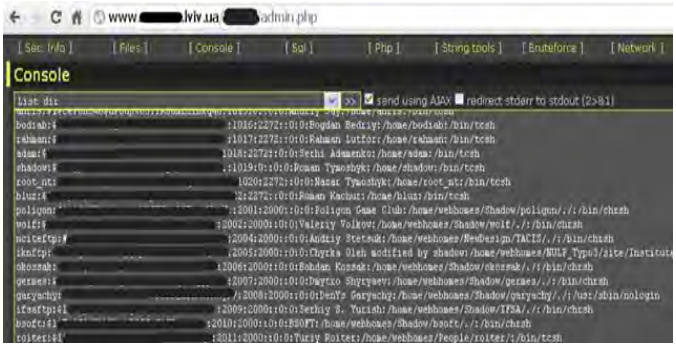

Fig.2. Passwords of the corporate university network users

For protection against unauthorized access a number of measures were proposed and implemented by cooperation with system administrators of the university:

- the operating system was updated;
- all content management systems, modules and software were updated;
- separation and limits of user access rights were set;
- information about the software and all server modules were hidden, which significantly complicates the network exploration;

IV. Conclusion

The main threats for information networks were considered. The list of usual weaknesses in the protection system of most web sites was created.

A set of measures for defence against unauthorized access and DDoS attacks was proposed and implemented by cooperation with system administrators of the university. These measures allowed improving protection level of the corporate network against network attacks and unauthorized access to information resources.

References

[1] Easttom, C., "Computer Security Fundamentals (2nd Edition)" Pearson Press, 2011.

[2] Flenov M.E. « Web-server through the eyes of the hacker. 2nd Edition » — BHV-Petersburg, 2007.