©EIJEAS 2021 Volume: 6, Issue: 12, 1-19, Ohio, USA
Electronic International Journal of Education, Arts, and Science
http://www.eijeas.com

Analysis of Attacks Against an Educational Institution

Huseyin CAKIR
Gazi University / hcakir@gazi.edu.tr

Celebi ULUYOL
Gazi University / celebi@gazi.edu.tr

Hüsameddin DEMİR
Ostim Technical University / husameddin.demir@ostimteknik.edu.tr

Alpaslan DURMUS
Ostim Technical University / alpaslan.durmus@ostimteknik.edu.tr

Abstract

In this study, attacks on an educational institution over the network were analyzed. In this study, it is aimed to guide other institutions in terms of security. For security reasons, the name of the institution where the work was made is not included. Fourteen-day log records obtained from the firewalls were used in examining the attacks on the institution. The attacks examined in these records are; attack method, target port, target type, service, source country, and danger level. According to the results of the research, it was seen that the attacks concentrated on the sites prepared with CMS (Content Management Systems) and it was seen that the service disruption and SQL Injection attack experiments are weighted. Considering all these factors, it was determined that there are security vulnerabilities of prepared sites by CMS and that websites need to eliminate these shortcomings. As a result, it is stated that institutions should take security measures against the network attacks used presenting this study analysis.

Keywords: *network, attack, analysis, security.*

Introduction

Our information assets are valuable assets of which must be preserved and protected. Attacks on these assets are increasing day by day. The precautions to be taken by the information owners against these increasing attacks are also gaining importance day by day. For the owners of information assets to take precautions, they should first analyze and evaluate the risks and shape their measures according to the results of this assessment.

In their study, Canberk and Sagiroglu (2007) drew attention to being familiar with the methods and techniques used in attacks on computer systems, taking precautions on target systems, monitoring attack characteristics, eliminating vulnerabilities, and evaluating the structures of attackers in the precautions to be taken.

In the report prepared by Kaspersky in 2017, attacks on industrial systems were analyzed. In the study, it is stated that there is little difference between attacks on industrial computers and attacks on corporate computers. In this study, attacks were classified based on the target country. Turkey ranked fifteenth among the target countries. As can be seen in Table 1.1, Turkey is among the main countries targeted in the attacks (Altuntas, 2016).

Table 1. *Countries with the Most Attacks on Industrial Computers (Kaspersky, 2017)*

Ranking	Country	Percentage	Ranking	Country	Percentage
1	Vietnam	66,09	9	China	53,31
2	Algeria	65,56	10	Peru	53,08
3	Morocco	60,39	11	Chile	52,75
4	Tunusia	60,17	12	India	52,48
5	Endonesia	55,69	13	Egypt	51,61
6	Bangladesh	54,19	14	Mexico	49,58
7	Kazakhistan	45,14	**15**	**Turkey**	**46,20**
8	Iran	53,89			

Turkey is also among the top five countries where botnets, malware, and exploit kits are detected (Garnaeva, Sinitsyn, & Namestnikov, 2016). It is obvious that our country has been chosen as a target in cyber attacks. For this reason, measures to be taken against attacks are of vital importance.

For taking precautions against attacks, the current situation must be analyzed first. Attack and defense methods should be known, vulnerabilities and solutions should be identified. Threats should be identified and risks should be calculated (Ciylan, 2017). In this study, it is aimed to analyze the attacks on an educational institution to set an example in identifying threats and calculating risks.

In the research, the attacks on an educational institution will be analyzed while also analyzing if the attacks overlap with other examples in the world. The analysis of these findings aimed to guide the security measures that other institutions should take. The institution whose data were examined hosts many types of sites. When the research started, it was expected that attacks on some of these site types would intensify. At the same time, it was thought that solutions could be developed against these methods by examining the methods used in the attacks. It was thought that the identification of the attack source countries would be important in terms of the measures to be taken.

The attacks on the exemplary educational institution over the internet will be examined from various perspectives, and the security measures to be taken will be determined by drawing attention to the risks.

1) What are the methods and techniques used in network attacks against the educational institution?

2) Which ports were used in the attacks?

3) Which services have been attacked?

4) What are the targets of the attacks?

5) What are the danger levels of the attacks?

6) From which countries did the attacks take place?

The importance of the research is that it is a guide for the security of other institutions by examining the attacks on the exemplary educational institution.

Network attacks and security systems

The purpose of network attacks is to detect vulnerabilities and open ports by examining a network infrastructure and then to access, modify, replace, prevent or destroy information in system resources by taking advantage of these vulnerabilities. Attackers use many different methods and techniques to achieve their goals. Knowing the attack types, analyzing them correctly, and deciding on the necessary precautions are important in terms of ensuring information security (Canbek & Sagiroglu, 2007).

Network Attacks

Network attacks in general are generally treated as active and passive attacks per the attacker's approach. In passive attacks, the attacker is content with eavesdropping on the system, while active attacks aim to corrupt, destroy or change data. The most commonly used attack methods today are Passive attacks and Active attacks (Contar, 2016; Elbahadır, 2016; Gezgin and invention 2013; Mohan and Anuradha 2015).

Passive attacks

In passive attacks, the attacker does not try to damage the network directly. Yet, the attacker may be using passive attack methods to gather information for future damaging attacks. Passive network attacks can be examined under two headings as eavesdropping and trafficking analysis.

Eavesdropping: It can happen in the form of an attacker obtaining information such as an e-mail or message sent over a network or channel. In fact, the attacker can obtain the data by analyzing the electromagnetic waves emitted by a computer without the need for a network (Nakato, 2016).

Trafficking analysis: In this method, the attacker tries to obtain the data by analyzing the data exchange between the sender and the receiver. The target data may be encrypted. The attacker tries to reach the encrypted data using various tools.

Active attacks

These are the attacks that the attacker applies over the internal or external network to destroy the target or change its normal function. Active network attacks can originate from a local network or an external network. In these active attacks, the attacker tries to circumvent security systems. It is more difficult to detect attacks carried out over the local network than attacks from the external network (Nakato, 2016; Richhariya and Kaushik, 2014).

Denial of Service Attack (DOS): The purpose of DOS attacks is to hinder the operation of the system or prevent it from working. In these attacks, the data belonging to the victim cannot be accessed or damaged. Attempts are made to render the target inoperable through vulnerabilities in IP protocols or consumption of system resources. Here are the methods used in denial of service attacks (Contar, 2016; Elbahadır, 2016; Gezgin and Bulus, 2013):

SYN Flood Attack: When it is desired to establish a TCP connection between the client and the server, the protocol called the three-way handshake is applied. First of all, the client sends a syn message to the server to initiate a connection request and waits. Then the server sends the SYN-ACK message in response to the client informing the system structure. Finally, a TCP connection is established with the ack message that the client reports that it has received this message. During

connection establishment, the server keeps connection information in its memory (TCP/IP stack). After the connection is established, the information is deleted from the memory (Tanrikulu, 2009).

UDP Flood Attack: Unlike TCP, the UDP protocol does not control whether the data packages are transmitted to the client and the flow order of the packages. In this way, the data transmission time is shortened. In this attack method, a large number of UDP packages are sent to random ports of the server to try to consume the server's bandwidth. Fake IPs are used in these attacks (Nakato, 2016; Gezgin and Bulus, 2013).

ICMP Flood Attack: ICMP is used for the feedback mechanism of the IP protocol. It is often used with ping and trace route commands for troubleshooting purposes.

In the ICMP Leak Attack, large-sized ICMP packages are sent to the target for the purpose of filling the bandwidth (Antoniou, 2017).

Ping of Death: The ping command is used to detect the loss of connection between two devices or the IP of the opposite computer. The maximum size allowed for the ping command is 65535 bytes.

Ping of death attack is performed by exceeding this dimension. When large-sized packages are received, undesirable reactions such as crashing, freezing, and restarting may occur in systems [10,2].

Teardrop Attack: Over the network, IP packages are transmitted in small chunks. Packages are reassembled at the receiver.

Teardrop Attack also exploits vulnerability in this merge process. The data packages sent in the attack are similar to the real data packages, but they do not contain the offset fields used to join the fragments. Today, this attack method can be caught by security walls. Variations such as TearDrop2, Targa, New Tear, SynDrop, Boink, and Nestea Bonk are used against this method (Tanrıkulu, 2009; Gezgin and Bulus, 2013).

Smurf Attack: Smurf Attack is a type of ICMP attack. The attacker shows the broadcast address of the network as the target of the package. Thus, the router will make an ICMP request to all clients on the network. The large number of ICMP packages that will occur renders the network inoperable. It is usually regulated against ISPs (Internet Service Provider) (“Smurf Attacks” ISP’leri Nasıl Sakatlar? 2017).

Land Attack: This attack is organized by sending a TCP SYN package to the target with the IP which the target has and the same port number used by the target. In this case, the system tries to respond to the package but instead, it seems like having come from itself and falls into the loop (Gezgin and Bulus, 2013).

DDoS Attacks (Distributed Denial of Service Attacks): The type of attack that aims to disable the system by consuming the network-system resources or by separating the vulnerabilities in the IP structure organized by more than one source to a target is called DDoS. To achieve this goal, the attacker needs a large number of devices from which they can attack. In the attack, systems called zombie computers and softwares which have been seized with various methods are used (Arora and Kumar, 2015).

Access Attacks

These attacks are organized in order to access sensitive information in the systems. The main methods are:

Man-in-the-middle attack: In MITM attack, the attacker intercepts the communication between the transmitter and the receiver. It can listen, delete and modify the data transmitted in this communication. However, neither the receiver nor the transmitter is aware of the situation. With ARP poisoning in networks or by obtaining keys in encrypted communications using SSL, the attacker can intercept or eavesdrop on the communication by interfering between the receiver and the transmitter (Mohan and Anuradha, 2015).

Exploit: In the network systems created by the computer, there are hierarchical authorization rights with different processing rights for the use of the system. The administrator has full authority on the system. Yet, the user cannot use administrative rights. For this reason, when the attacker captures the passwords of the user account, they cannot achieve their purpose because they do not have the rights for damaging the system.

The attacker's exploitation of the vulnerabilities left during the coding of operating systems and other software is named as exploiting. The tools that perform this operation are called exploits. By overflowing the area allocated for it in the memory of the attacker application (Buffer Overflow), it can read the memory and run the codes that it wants (Format String) (Canbek and Sagiroglu, 2007).

Database attacks: The attacker can create a new database, add a new table to the database, change privileges, add new information, pull information, update and delete the database by taking advantage of the security vulnerabilities. SQL is the structure used to manage and access the database. SQL Injection is the insertion of some characters into the database using the vulnerabilities that occur while writing SQL codes. Thus, the attacker can capture and manage the database (Contar, 2016).

Cross-site Scripting (XSS): In this method, vulnerabilities caused by errors in the coding of dynamic websites and the lack of necessary filtering are used. It may conclude with a user accessing other users' information or accessing information stored on the server.

When the cookies and session information used in the connection between the client connecting to a website and the server are captured by the attacker, the attacker can enter the system as a client (Contar, 2016; Ozfidan, Savas, & Demir, 2019). A Reflected XSS attack, on the other hand, is organized by using sites that users frequently visit and trust. The attacker detects XXS vulnerabilities on these trusted sites. By exploiting this vulnerability, the attacker redirects the user from the trusted site to the site with malicious content. Thus, the attacker obtains the user's information (Elbahadir, 2016).

Vulnerability detection attacks: The aim of these attacks is to detect the security vulnerabilities in the target system. The purpose here may be a preparation for subsequent attacks.

Port scanning: Vulnerabilities in networks are usually in the services running on ports. If there is any vulnerability in the software used on the server, it becomes much easier for the attacker to take over the target system. Hence, the attacker tries to detect open ports on the target system. For this purpose, TCP Connect, TCP SYN, TCP FIN, TCP ACK, TCP Null, TCP Xmas, TCP Window, UDP scans can be made on the target system. Port scanning practices made with the nmap application are given below (Elbahadir, 2016).

TCP Syn Scan: This method uses the triple handshake feature of TCP. In this type of scanning, in which the scanning machine starts by sending a TCP SYN flagged packet to the target machine, most of the ports will probably be closed during the scanning. When it is off, the target machine will rotate RST + ACK flagged packet: If it is on, the SYN + ACK flagged packet will rotate. The scanning machine disconnects by sending a RST flagged packet, and therefore the triple handshake is not completed (Altuntas, 2016).

TCP Connect Scan: This scan is similar to TCP SYN Scan. The similarity is the RST-ACK packets that the target will send if the ports are closed. If it is open, the scanning machine ends the scanning by sending an ACK flagged packet (Altuntas, 2016).

UDP Scan: Here the scanning machine sends UDP packets to the target machine. If the target machine responds with UDP packets, it means that the ports are open (Contar, 2016).

Operating System Detection: The operating system of the target computer can be detected via NMAP.

Intrusion Detection Systems

Preventive precautions are needed to prevent network attacks. Intrusion detection systems are the systems that detect and report attacks against the system, perform alarm mechanisms and apply predetermined procedures. The detections of intrusion detection systems are not always accurate.

Errors made by intrusion detection systems are divided into two [8,2]. False Positive Detections; Intrusion Detection System detects traffic as an attack even though it is not an attack. A high number of false positives is not considered as a security vulnerability [8]. False Negative Detections; Intrusion Detection System cannot detect the attack. The high number of false negative detections poses a security risk. Intrusion Detection Systems can be classified according to their different features. According to the method used to detect attacks, Intrusion Detection Systems are classified as follows (Oktay, 2013):

Signature-based intrusion detection systems: It is an intrusion detection system that tries to detect attacks by comparing the activity in the network with foreknown attack signatures. As signature-based STSs identify mobility by comparing it with the database, there is no possibility of false alarms. Additionally, when an attack occurs which is not included in the database, STSs cannot recognize this attack (Vacca, 2009).

Anomaly-based intrusion detection systems: These systems observe the traffic on the network and detect anomalies that occur there. In order to detect abnormal traffic, first of all, normal network traffic definitions should be made. Anomaly-based intrusion detection systems come to conclusion by comparing them. The most important advantage of this system is that it can detect attacks that have not been recorded in the database before (Nakato, 2016; Demir, Kapukaya, & Ozfidan, 2015).

Firewalls

As the use of network systems in the world increases, the security problems encountered in these systems also increase in number. Firewall is often the first obvious option when it comes to network security. The main purpose of the firewall is to protect the local network from external threats. Firewalls check packets sent between the internal network and the external network, as well as between devices on the same network, and allow a secure traffic. Firewalls can be classified under four titles (Demir, 2009).

Packet filtering firewalls: A packet filtering firewall analyzes network traffic, allowing only specific packets, protocols, or traffic passing through certain ports [8].

Circuit-level firewall: The client behind the circuit-level firewall cannot see the machines on the other side of the firewall. Incoming packets are allowed to pass after being verified as connection packets. Circuit-level firewalls operate at the transport layer. Due to the NAT tables kept, it is ensured that the appropriate package is forwarded to the right machine (Vacca, 2009).

Dynamic packet filtering firewalls: In these firewalls, unlike other firewalls, incoming packets are stored in memory and tracked. This way, instead of making decisions based on IP or protocol, filtering can be applied according to the structure of the communication, as well (Nakato, 2016).

Proxy firewalls: In this type of firewall, the connection is not established between the client and the server. The entire connection passes through proxy servers. They work at the application level. When the client wants to log in to the server, the request is forwarded to the Proxy and the Proxy logs in to the server. In other words, Proxy isolates client and server from each other (Contar, 2016).

Method

Two-week log records of the year 2017 belonging to the firewalls which protects the servers of an educational institution were obtained. In this study, the name of the institution is not included for security reasons. The data were analyzed by statistical methods, and the distribution of the data was revealed with frequency distribution tables. In order to underline the important points, the relative frequency distribution data are included from time to time. Some data are presented by comparing with quota frequency tables.

The data sets received from the institution were examined and analyzed by frequency analysis method. The attacks were examined from the point of method, source country, destination port, target site type and attack level and solutions were offered.

Findings

In this section, the attacks on the Educational Institution are examined from various perspectives. The attacks were classified according to the method, port, service type, target site type, level of danger, and frequency analyzes were made. Numerical data about the findings are presented. The attacks were examined in terms of the relation between the site type and the attack method, by comparing the threat level of attacks and site type.

Analysis of Attacks According to the Methods Used

When the log records of the firewall are examined, 11689 attacks detected are classified as follows.

Table 2. *Classification of attacks according to the method applied*

Attack Method	Number of Attacks	Attack Method	Number of Attacks
WordPress.xmlrpc.Pingback.DoS	6793	Jboss.Application.Server.Admin.Interface.Unauthorized.Access	4
HTTP.URI.SQL.Injection	3765	WordPress.WP.Symposium.Arbitrary.File.Upload	4
ZmEu.Vulnerability.Scanner	563	HTTP.Accept-Language.Header.Buffer.Overflow	3
Apache.Struts.Jakarta.Multipart.Parser.Code.Execution	139	WordPress.RevSlider.Arbitrary.File.Upload	3
OpenSSL.Heartbleed.Attack	64	MS.IIS.WebDAV.Authentication.Bypass	2
Apache.Struts.2.DefaultActionMapper.Remote.Command.Execution	57	MS.Windows.HTTP.sys.Request.Handling.Remote.Code.Execution	2
Zynos.ROM0.Config.Password.Retriever	56	WordPress.Download.Manager.wpdm_upload_icons.Code.Execution	2
Muieblackcat.Scanner	50	WordPress.Web.API.Endpoint.Privilege.Escalation	2
Web.Server.Password.Files.Access	34	WordPress.WP.Mobile.Detector.Arbitrary.File.Upload	2
HTTP.GET.Request.Directory.Traversal	31	Worm.PhpInclude	2
WordPress.Slider.Revolution.File.Inclusion	25	Bash.Function.Definitions.Remote.Code.Execution	1
DLink.Devices.Unauthenticated.Remote.Command.Execution	18	Joomla.list.select.Parameter.SQL.Injection	1
Jboss.JMX.Console.Beanshell.Deployer.War.Upload	17	MVPower.DVR.Shell.Unauthenticated.Command.Execution	1
Joomla.JCE.Extension.Remote.File.Upload	15	NetworkActiv.Web.Server.XSS	1
Joomla.Core.Session.Remote.Code.Execution	14	Snort.TCP.SACK.Option.DoS	1
PHP.CGI.Argument.Injection	11	Apache.Commons.Collection.InvokerTransformer.Code.Execution	1
HTTP.URI.XSS	5		
Grand Total		**11689**	

When Table 2 is examined, it is seen that 58.11% of the attacks are denial of service attacks against WordPress-based sites on servers. According to the number of attacks, SQL Injection attempts are in the second place with 32.02%. It is seen that the other 31 attack methods are only 9.67% of the total number of attacks.

Analysis of Attacks by Target Ports

The attacks detected by the firewall are examined in terms of target ports.

Table 3. *Examination of organized attacks according to target ports*

Port Number	Number of Attacks
80	11594
443	85
8080	7
81	3
Grand Total	11689

When Table 3 is examined, it is seen that 99.19% of the attacks target the port number 80. 0.81% of the attacks were organized on ports 443, 8080 and 81, respectively.

Analysis of Attacks by Target

The sites on the servers were classified according to their types and the attacks were examined in terms of these site types.

Table 4. *Examination of organized attacks by site type*

Site Type	Number of Attacks
CMS	6878
PHP	4519
FLASH	105
JAVA	79
EMAIL	59
SERVER	49
Grand Total	**11689**

When Table 4 is examined, it is seen that 58.85% of the attacks were directed against ready-made sites created with the Content Creation System (CMS). The rate of attacks on sites that were

developed with PHP is 38.66%. The remaining attacks are (2,49%) respectively; Flash-based sites, Java-based sites, and email servers.

Investigating the Relationship between Site Type and Attack Methods

The methods and site types used in the attack were discussed as a pair and the following table was obtained.

Table 5. *Relationship between attack method and site type*

ATTACK METHOD	SITE TYPE						
	Server	**Cms**	**Email**	**Flash**	**Java**	**Php**	**Total**
WordPress xmlrpc Pingback DoS	-	-	-	-	-	4	6793
HTTP URI SQL Injection	1	23	-	-	-	3741	3765
ZmEu Vulnerability Scanner	41	23	30	15	67	387	563
Apache Struts Jakarta Multipart Parser Code Execution	-	-	8	84	-	-	139
OpenSSL Heartbleed Attack	-	-	-	-	-	64	64
Apache Struts 2 DefaultActionMapper Remote Command Execution	2	3	4	2	4	42	57
Zynos ROM0 Config Password Retriever	2	3	4	1	5	41	56
Muieblackcat Scanner	3	-	-	-	-	38	50
Web Server Password Files Access	-	6	-	-	-	28	34
HTTP GET Request Directory Traversal	-	1	-	-	-	30	31
WordPress Slider Revolution File Inclusion	-	8	-	-	-	17	25
DLink Devices Unauthenticated Remote Command Execution	-	-	2	-	-	15	18
Jboss JMX Console Beanshell Deployer War Upload	-	-	1	2	-	-	17
Joomla JCE Extension Remote File Upload	-	-	-	-	-	15	15
Joomla Core Session Remote Code Execution	-	11	-	-	-	3	14
PHP CGI Argument Injection	-	2	-	-	-	9	11
HTTP URI XSS	-	-	-	-	-	5	5

Jboss Application Server Admin Interface Unauthorized Access	-	-	-	-	-	4	4
WordPress WP Symposium Arbitrary File Upload	-	3	-	-	-	1	4
HTTP Accept-Language Header Buffer Overflow	-	-	-	-	-	3	3
WordPress RevSlider Arbitrary File Upload	-	2	-	-	-	1	3
MS IIS WebDAV Authentication Bypass	-	-	-	-	2		2
MS Windows HTTP sys Request Handling Remote Code Execution	-	-	1	-	-	1	2
WordPress Download Manager wpdm_upload_icons Code Execution	-	1	-	-	-	1	2
WordPress Web API Endpoint Privilege Escalation	-	1	-	-	-	1	2
WordPress WP Mobile Detector Arbitrary File Upload	-	2	-	-	-	-	-
Worm PhpInclude	-	-	-	-	-	2	2
Apache Commons Collection InvokerTransformer Code Execution	-	-	-	1	-	-	-
Bash Function Definitions Remote Code Execution	-	-	-	-	-	1	1
Joomla list select Parameter SQL Injection	-	-	-	-	-	1	1
MVPower DVR Shell Unauthenticated Command Execution	-	-	-	-	-	1	1
NetworkActiv Web Server XSS	-	-	-	-	-	1	1
Snort TCP SACK Option DoS	-	-	-	-	-	1	1
Grand Total	**49**	**6878**	**59**	**105**	**79**	**4519**	**11689**

When Table 5 is examined; it is seen that vulnerability scanning is performed for all site types (ZmEu Vulnerability Scanner and Muieblackcat Scanner). It is also seen that 0.33% of CMS sites were scanned for vulnerability. On PHP sites, this rate is 9.4%. Again, as stated above, DoS attacks on CMS sites and SQL injection attacks on PHP sites have strong influence.

Analysis of Attacks by Danger Level

Attacks are classified according to the level of danger defined by the firewall.

Table 6. *Classification of attacks by attack level*

Attack Level	Number
Medium	6966
High	3831
Low	613
Critical	279
Total	**11689**

When Table 6 is examined, it is seen that 59.59% of the attacks are defined as medium level, 32.6% as high level, 5.24% as low level and 2.38% as critical level by the firewall.

The relationship between the attack level and the site type is given in Table 7. The relationship between the attack level and the site type is classified according to the level of danger defined by the firewall.

Table 7. *Relationship between attack level and site type*

Level of Danger	Server	Cms	Email	Flash	Java	Php	Total
Critical	2	14	13	87	4	159	279
High	1	34	1	2	-	3793	3831
Low	44	23	39	15	67	425	613
Medium	2	6807	6	1	8	142	6966
Total	49	6878	59	105	79	4519	11689

When Table 7 is examined, it is seen that 79.53% of attacks on PHP sites are critical and high risk. The rate of critical and high-risk attacks is only 0.69% on CMS sites. 98.96% of attacks on CMS sites are classified as moderate attacks. It is noteworthy that 82.85% of attacks on flash-based sites are classified as critical.

Analysis of Attacks by Origin Countries

When the data received from the firewall were examined, it was observed that attacks came from 41 different countries. These attacks are grouped and listed by country.

Table 8. *Origin countries of attacks*

Country	Number of Attacks	Country	Number of Attacks
Vietnam	5299	India	39
Russian Federation	2144	Spain	32
United States of America	1467	Korea	21
France	322	Bulgaria	18
Netherlands	298	Pakistan	16
China	269	Iceland	11
Germany	268	Taiwan	10
Japan	219	Iran	9
Italy	181	Moldova	9
Croatia	157	Argentina	9
Turkey	**152**	Belarus	9
England	106	Denmark	9
Poland	92	Hungary	9
Australia	78	Kazakhistan	9
Canada	77	Romania	9
Malaysia	68	Sweden	7
Seychelles	61	Indonesia	5
Hong Kong	52	Finland	4
Brazil	50	Uzbekistan	2
Thailand	46	Belgium	1
Ukraine	45		

When Table 8 is examined, it is seen that 45.33% of the attacks came from Vietnam, 18.34% from the Russian Federation, and 12.55% from the United States. The ratio of attacks from the remaining 38 countries to all attacks is 23.77%. It is seen that the rates of attacks according to the country in which they were carried out coincide with Kaspersky's report (Kaspersky Lab, 2017).

Table 9. *Distribution of attacks continents*

Continents	Total Number of Attacks
Asia	8271
Europe	1676
America	1603
Australia	78
Africa	61
Grand Total	**11689**

When Table 9 is examined, it is seen that 70.7% of the attacks came from the Asian Continent, 14.3% from the European Continent, 13.7% from the American Continent. The overall rate of attacks from Africa and Australia remained at 1.1%.

Conclusion

Today, information assets are among our most important assets. For this reason, the protection of these assets has made information security indispensable.

The methods mentioned in the second part of this study are the methods frequently used in attacks against our information assets stored on web servers. In the third chapter, the attacks on an educational institution hosting different types of sites on its servers were examined and the following results were obtained.

In this study, when the attacks on educational institutions were examined on the basis of attack type, it was seen that Kaspersky's research on attacks on industrial computers overlapped [16, 18]. In both studies, it was determined that denial of service attacks were applied intensively. It is thought that it will be important for institutions to consider this issue in the security measures they will take.

When the attacks were analyzed on the basis of the source country, it was seen that most of the attacks came from three different countries. It is thought that it would be appropriate to identify the attack's source countries and block IPs to these countries, especially during periods when service disruption attacks are intensified.

The vulnerabilities in the code of CMS sites using open source, ready-made site templates are known to attackers. For this reason, it has been seen that vulnerability scanning is rarely used in attacks on these sites. In sites whose codes are written and printed by the site owners, the probability of the security vulnerabilities being known to the attackers is weaker than the CMS sites. In order for

the attacker to damage these sites, they must first detect the vulnerabilities. For this reason, it has been seen that attacks against vulnerability detection on such sites are 28 times more than CMSs. In other words, CMSs contain much more known vulnerabilities than other types of sites, and attackers do not make any effort to detect these vulnerabilities.

In terms of the total number of attacks, it was seen that the attacks concentrated on CMSs. The reason for this is the security vulnerabilities that CMSs contain and are known to attackers, as mentioned above.

In terms of the risk levels of the attacks, it is thought that the reason why the attacks on CMS sites are classified as medium level and the rate of high and critical level attacks remains low is that important security vulnerabilities in CMS sites are regularly closed with published patches.

Although important security vulnerabilities of CMS sites are closed with published patches, since they are open source code and are used on many sites, the content hosted on these sites is more at risk than the sites whose source code is not open. In terms of information security, it will be appropriate for educational institutions not to use these types of sites, if possible, to publish their content, but to use their constantly updated versions.

References

Altuntaş A. (2016). *Kali Linux.* (Fourth Edition). Istanbul: Kodlab Publishing, 78-98.

Arora K. and Kumar K. (2015). Impact Analysis of Recent Ddos Attacks. *International Journal on Computer Science and Engineering,* Vol. 3 No. 2 (877-884).

Canbek G. and Sağıroğlu Ş. (2007). Bilgisayar Sistemlerine Yapılan Saldırılar Ve Türleri: Bir İnceleme (Attacks on Computer Systems and Their Types: A Research). *Erciyes University Institute of Science and Technology Magazine,* 23 1 - 12.

Ciylan B. (2017). Information Security Lecture Notes (Unpublished) Gazi University Department of Computer Forensics 1-8.

Contar F. (2016). *Ağ Ve Yazılım Güvenliği (Web and Software Security).* (Fourth Edition). Istanbul: Kodlab Publishing, 51-82.

Demir, N. (2009). *Gömülü Güvenlik Duvarı Yazılım Paketi (Embedded Firewall Software Package),* Postgraduate Thesis, Dokuz Eylül University Institute of Science and Technology Department of Computer Engineering, İzmir.

Demir, H., Kapukaya, K., & Ozfidan, B. (2015). Yabanci diller yüksek okullarinda görev yapan ingilizce okutmanlarinin sorunlari. *Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *12*(30), 113-138.

Elbahadır H. (2016). *Hacking Interface.* (Twelfth Edition). Istanbul: Kodlab Publishing, 57-125.

Garnaeva M., Sinitsyn F. and Y. Namestnikov (2016) Kaspersky Security Bulletin Overall Statistics For 2016.

Gezgin D. ve Buluş E. (2013). Kablosuz Ağlar İçin Bir Dos Saldırısı Tasarımı (Dos Attack Design for Wireless Networks). *Bilişim Teknolojileri Dergisi* (*Data Processing Technologies Magazine),* Vol. 6, No. 3.

Internet: "Smurf Attacks" ISP 'leri Nasıl Sakatlar? (How Do "Smurf Attacks" Disable ISP's?) URL: http://ekinoks.cu.edu.tr/internet/konu_46.htm Son Erişim Tarihi:19.12.2017.

Internet: Antoniou, S. The PING of Death and Other DoS Network Attacks. URL: https://www.pluralsight.com/blog/it-ops/ping-of-death-and-dos-attacks, Latest Access Date:19.12.2017.

Kaspersky Lab **(**2017) Threat Landscape for Industrial Automation Systems in The Second Half Of 2016: AO Kaspersky Lab**.**

Mohan V. and Anuradha J. (2015). Network Security and Types of Attacks in Network. *Procedia Computer Science,* 48 (2015) 503 – 506.

Nakato, H. (2016). *Ağ Güvenliği: Saldırılar Ve Zeki Güvenlik Duvarı Etmeni İle Savunma Mekanizmaları (Web Security: Attacks and Defense Mechanisms with Intelligent Firewall Factor)* Postgraduate Thesis, Sakarya University Institute of Science and Technology Department of Computer and Data Processing Engineering, Sakarya.

Oktay, U. (2013*). Bulut Bilişimde Vekil Ağ Saldırı Tespit Sistemi (Proxy Network Detection System in Cloud Computing),* Postgraduate Thesis, Air Force Academy Institute of Aviation and Space Technology, Istanbul.

Ozfidan, B., Savas, A. C., & Demir, H. (2019). The moderating effect of organizational justice on the relationship between integrity and organizational citizenship behavior in educational institutions. *Revista de Cercetare si Interventie Sociala*, *66*, 75.

Richhariya V. and Kaushik P. (2014). A Survey on Network Attacks in Mobile Ad Hoc Networks. *International Journal Of Advanced Research In Computer Science And Software Engineering,* Volume 4, Issue 5.

STM Defense Technologies (2016) 2016 Ekim-Aralık Dönemi Siber Tehdit Durum Raporu (October-December Term Cyber Threat Information Report).

STM Defense Technologies (2016) 2016 Türkiye Siber Tehdit Durum Raporu (Turkey Cyber Threat Information Report).

Tanrıkulu, H. (2009). *Saldırı Tespit Sistemlerinde Yapay Sinir Ağlarının Kullanılması (The Use of Artificial Neural Networks in Systems of Attack Detection),* Postgraduate Thesis, Ankara University Institute of Science and Technology, Ankara.

Vacca J. (2009). *Network and System Security*. Oxford: Syngress, 259-260.