

EUROPEAN JOINT MASTER PROGRAMME “POLICING IN EUROPE”



MASTER'S DISSERTATION **Procedures for Detecting Cybercrime Activities on Websites**

Ioan-Cosmin MIHAI



■ SITECH ■

The correction belongs to the author.

© 2017 Sitech Publishing, Craiova

All rights reserved. This book is protected by copyright. No part of this book may be reproduced in any form or by any means, including photocopying or utilized any information storage and retrieval system without written permission from the copyright owner.

SITECH Publishing is part of the list of prestigious Romanian publishing houses recognized by CNATDCU, for Panel 4, which includes the fields: legal sciences, sociological sciences, political and administrative sciences, communication sciences, military sciences, information and public order, economics sciences and business administration, psychological sciences, education sciences, physical education and sport.

Editura SITECH Craiova, România
Aleea Teatrului, nr. 2, Bloc T1, parter
Tel/fax: 0251/414003
E-mail: office@sitech.ro



ISBN 978-606-11-6119-5

ABSTRACT

The research “*Procedures for Detecting Cybercrime Activities on Websites*” aims to analyze the procedures for detecting the cybercrime activities on the websites compromised by cybercriminals. The research intends to emphasize the importance of cyberspace security and to propose methods to mitigate the cyber-attacks effects.

The specific objectives of the research are identification and classification of websites vulnerabilities, analysis of cyber-attacks evolution and structure, identification of best practices for cyber-attacks prevention and mitigation, improving methods for monitoring websites security, identifying methods for alerting websites owners in case of detection of intrusion or infection with malware, and enhancing cooperation between institutions involved in cyberspace security by providing procedures for preventing cyber-attacks and mitigating their effects.

The actuality of this research is determined by developing a study on the cybercrime activities on compromised websites for improving cyber-attacks detection capability and defining procedures for monitoring the cyberspace security. The added value of the research is given by the strategies analysis for remote monitoring of the websites security and the alerting methods of the administrators in case of detection of cybercrime activities, leading to a better protection of the cyber infrastructures and the maintenance of a secure cyberspace.

The research website, necessary for the visibility and the promotion of the results, is hosted on *web-scan.eu* domain. The purpose of this platform is to promote the procedures for detecting cybercrime activities on websites.

Keywords: cybercrime, cyber-attacks, cybersecurity, cyberspace, website scanner

TABLE OF CONTENTS

LIST OF ABBREVIATIONS AND ACRONYMS	8
---	----------

CHAPTER I

INTRODUCTION	11
1.1. Objectives of the research	11
1.2. The background to the research	11
1.3. Structure of the research report.....	14

CHAPTER II

THE STUDY OF CYBER-ATTACKS	17
2.1. Evolution of cyber-attacks	17
2.2. Classification of cyber-attacks	19
2.3. Structure of cyber-attacks	23
2.3.1. The Cyber Kill Chain intrusion model	23
2.3.2. Cyber-attacks analysis	25
2.3.3. Study of cyber-attack vectors	32
2.4. Methods to prevent cyber-attacks	35
2.5. Conclusions	37

CHAPTER III

MONITORING WEBSITES SECURITY.....	39
3.1. Developing an attack tree.....	39
3.1.1. The structure of an attack tree.....	40
3.1.2. Developing an attack tree for websites.....	42
3.2. Analysis of the impact of cyber-attacks.....	46
3.2.1. Vulnerabilities of websites.....	46
3.2.2. Impact of cyber-attacks on the websites.....	49
3.3. Monitoring websites security.....	51
3.3.1. Intrusion detection	51
3.3.2. Malware detection.....	54
3.3.3. Suspicious activities detection.....	55
3.4. Methods to alert the platform administrators.....	61
3.5. Conclusions	62

CHAPTER IV

DEVELOPING THE RESEARCH WEBSITE.....	64
4.1. The website aims and objectives.....	64
4.2. The website structure	65
4.3. Integration of the monitoring procedures into an app	66
4.4. Conclusions	71

CHAPTER V

CONCLUSIONS..... 73

5.1. The main issues presented in the research 73

5.2. Original contributions to the research..... 75

5.3. Methods of data collection and analysis 75

5.4. Perspectives for further development 77

REFERENCES 79

LIST OF ABBREVIATIONS AND ACRONYMS

A

AES – Advanced Encryption Standard

API – Application Programming Interface

APT – Advanced Persistent Threats

C

CERT-RO – Romanian National Computer Incident Response Team

CSRF – Cross-Site Request Forgery

D

DDoS – Distributed Denial of Service

DNS – Domain Name System

DoS – Denial of Service

H

HTML – Hyper Text Markup Language

I

ICMP – Internet Control Message Protocol

IDS – Intrusion Detection System

IP – Internet Protocol

IRC – Internet Relay Chat

L

LDAP – Lightweight Directory Access Protocol

M

MAC – Media Access Controller

MBR – Master Boot Record

O

OWASP – Open Web Application Security Project

P

PDF – Portable Document Format

PHP – Hypertext Preprocessor

PSK – Pre-Shared Key

R

RAISA – Romanian Association for Information Security Assurance

RDoS – Ransom Denial of Service

RAM – Random Access Memory

S

SHA2 – Secure Hash Algorithm 2

SMS – Short Message Service

SQL – Structured Query Language

SQLi – SQL Injection

SSID – Service Set Identifier

T

TCP – Transmission Control Protocol

U

UDP – User Datagram Protocol

URL – Uniform Resource Locator

USB – Universal Serial Bus

W

WAF – Web Application Firewall

WPA2 – Wi-Fi Protected Access 2

X

XPath – XML Path Language

XSS – Cross Site Scripting

CHAPTER I

INTRODUCTION

1.1. Objectives of the research

The research project “Procedures for Detecting Cybercrime Activities on Websites” aims to detect the cybercrime activities on websites compromised by cyber criminals. The research intends to emphasize the importance of online environment safety and to propose procedures to mitigate the cyber-attacks effects in the cyberspace.

The specific objectives of the project are:

- Identification and classification of computer vulnerabilities;
- Analysis of cyber-attacks evolution and structure;
- Identification of good practices on cyber-attacks prevention and mitigation;
- Improving methods for monitoring websites security;
- Identifying methods of alerting websites owners in case of detection of intrusion or infection with malware;
- Enhancing cooperation between institutions involved in cyberspace security by providing procedures for preventing cyber-attacks and mitigate their effects.

1.2. The background to the research

The online environment, which is in a continuous process of evolution, is generating both solutions for the development of the information society, as well

as risks related to its activities. The computer vulnerabilities that can be exploited by cyber criminals, makes cybersecurity a major concern.

From this perspective, at the national level, steps have been taken to adopt new policies on the fight against the phenomenon of computer-related. In Romania, *The Cybersecurity Strategy*¹ was adopted in 2013 in order to define and maintain a secure virtual environment, with a high degree of safety and reliability. This Strategy proposes regulatory and institutional framework to the dynamics of environmental threats, the establishment and application of minimal security requirements for national information infrastructures, ensuring their resilience and the development of cooperation at national and international levels.

Implementation of the Romanian Cybersecurity Strategy is based on the principles of coordination of the action plans designed to ensure information security, cooperation between all the entities concerned, both in the public and private sectors, the prioritization of critical national infrastructures and the dissemination of information, expertise and best practices in order to protect the cyber infrastructure.

An important role in cybersecurity has the *Romanian National Computer Incident Response Team (CERT-RO)*² – an independent structure of expertise, research and development in the field of cyber infrastructure protection, which provides the necessary capacity for prevention, analysis, identification and response to cybersecurity incidents of computer systems that provide functionality of public interest or ensures the services of the information society.

Increased attention is given both to the capacity of response to cyber-attacks, and to prevent and combat these kind of attacks. Combating the phenomenon of cybercrime is a priority for all of us, whether we are talking about intrusions into our private environment or to personal data, whether we are talking

¹ <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf>

² <https://www.cert.ro/>

about identity theft or fraud. Preventing cyber-attacks are a necessity especially for public authorities, who must have the ability to protect critical infrastructure that Romanian citizens rely in their work day by day.

Cyber-attacks have seen a huge diversification in recent times, some of which could be easily classified as global epidemics due to the large spreading speed. Specific threats to information systems are characterized by a dynamic and a global character, making them difficult to identify and counteract.

Starting with viruses create for fun in the mid of '80s, there are now computer worms used for industrial espionage. Moreover, today's sophisticated attacks can no longer be placed in well-defined types of attacks, showing the characteristic of either computer viruses, computer worms, or computer trojans. In other words, these malicious programs can multiply themselves (feature of computer worms), may create gaps in the systems security to facilitate access to the attacker (feature of computer trojans), and once installed in the operating system of the victim, may carry out destructive activities (feature of computer viruses).

The cyber threats from Romania complies with the trend of cyber threats in the world. However, due to the fact that a fairly percentage of the population uses counterfeit software products, many existing vulnerabilities increase the risk of infection. For this reason, many websites may be infected unintentionally due to the use of these counterfeit products. An infected website can have serious implications on the hosting server: infection can spread to all websites hosted on the server and then to all the visitors of those websites.

Due to the increasing number of threats, many security companies provide strong protection methods. However, the security of information in the online environment cannot be achieved only by technical measures, being mainly a human problem. Often security incidents are caused by inadequate management of security policies and less due to a deficiency of security mechanisms.

Definition of the research problem

In the actual context of cyber-attacks, it is necessary to develop strategies for monitoring the websites security, making it possible to alert administrators as soon as cybercrime activities are detected on the compromised platforms.

There are many infected websites that can be used by cybercriminals to develop activities like phishing, spoofing and spamming or to infect their visitors with malware. These cybercrime activities can be done without the knowledge of websites owners. For preventing these kind of activities, there are some integrated services for prevention and detection of intrusions and malware in websites. These kind of services, such as those provided by *Sucuri*³, *Quttera*⁴ or *WhiteHat Security*⁵, run as modules on online platforms and periodically scan webpages for intrusion detection, code insertion into the database, malware, or redirection to infected websites. There are also static scanning services, such as *Site Guarding*⁶, *Web Inspector*⁷ or *VirusTotal*⁸, which offers the ability to scan a website.

The actuality of this research is determined by developing a study on the cybercrime activities on websites for improving cyber-attacks detection capability and defining procedures for monitoring the safety of the online environment. The added value of the research is given by the strategies analysis for remote monitoring of websites security and alerting methods of the administrators in case of detection of cybercrime activities.

The procedures developed in this research can help to prevent and combat the cybercrime phenomenon, to have a safe and secure cyberspace.

1.3. Structure of the research report

The research report is structured in five chapters. *Chapter I* presents an introduction to the research project. It outlines the purpose, the objectives of the

³ <https://sucuri.net/>

⁴ <https://www.quttera.com/>

⁵ <https://www.whitehatsec.com/>

⁶ <https://www.siteguarding.com/>

⁷ <https://www.webinspector.com/>

⁸ <https://www.virustotal.com/>

research and the chosen topic, taking into account the current state of research in the field of websites security.

Chapter II investigates the cyber-attacks present in the online environment. The attacks are classified according to the target of cybercriminals and their access to cyber infrastructures. An analysis of cyber-attacks is carried out according to the *Cyber Kill Chain*⁹ intrusion model, defined by Lockheed Martin researchers, a seven-step model: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objective. At the end of this chapter, a security guideline is presented, which highlights the main methods used for preventing the cyber-attacks.

Chapter III presents strategies for monitoring cyberspace security. An attack tree is designed to simulate and analyze the impact of cyber-attacks to websites. Methods for monitoring websites security are being studied on three directions of action: intrusion detection, malware infections detection and suspicious activities detection. There are also analyzed the methods to alert the website administrators in case of detection of a security incident.

In *chapter IV* is presented the structure of the website developed in the research, hosted on *web-scan.eu*¹⁰ domain. The purpose of the platform is to promote the procedures for detecting cybercrime activities on websites. The platform tries to support *The Cybersecurity Strategy of the European Union*¹¹ goal: an open, safe and secure cyberspace. This chapter presents also an application designed to integrate the results obtained through the process of monitoring the websites security.

The final chapter presents the final conclusions, the original contributions made in the field of monitoring process of websites security and the future development perspectives of this research.

⁹ <http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html>

¹⁰ <http://www.web-scan.eu>

¹¹ http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

The researches carried out in this research have used both qualitative and quantitative methods. The methods used in the qualitative research were participatory observation, individual and group interview, case studies, comparative studies and analysis of the specialized references. Quantitative research has been geared towards verifying the theories obtained through qualitative research and has used experiments and surveys as methods.

CHAPTER II

THE STUDY OF CYBER-ATTACKS

The cyber-attack is a hostile activity carried out in the cyberspace that affects cybersecurity¹². Cyber-attacks have diversified and evolved a lot lately, some of which can be categorized as epidemics due to the global spread in a very short time. The specific threats to computer systems are characterized by an increased dynamic and by a global character, being much more difficult to identify and counteract.

2.1. Evolution of cyber-attacks

Starting from the computer viruses made for entertainment in the 1980s, cyber criminals have come to develop computer trojans and worms for industrial espionage. Moreover, today's sophisticated attacks can no longer be placed in well-defined types of attacks, showing the characteristic of either computer viruses, worms, or trojans.

In other words, these malicious programs can multiply themselves in networks (feature of computer worms), may create gaps in the systems security to facilitate access to the attacker (feature of computer trojans), and once installed in the operating system of the victim, can carry out destructive activities (feature of computer viruses).

Botnet networks are now a major part of the malware industry. Infected systems that are part of these networks can be used to launch DoS (Denial of

¹² <http://securitatea-cibernetica.ro/wp-content/uploads/2014/12/StrategiaDeSecuritateCiberneticaARomaniei.pdf>

Service) attacks, to host malware or phishing pages, to send spam messages, or to provide access as intermediary servers for various other attacks. Massive DDoS (Distributed Denial of Service) attacks have paralyzed the computer networks of Internet Service Providers and government agencies websites. Compared with classical attacks of this kind, involving infected systems from a botnet network, now millions of users have willingly made their computers available for these attacks, resonating with the ideas of the attackers (hacktivism).

Social networks have diversified and increased in the number of users, implicitly resulting in a high level exposure of personal information. Cybercriminals can corroborate all this information to launch targeted campaigns targeted to users or the companies in which they work (social engineering). By making a huge number of fake apps exposed on social networks, cybercriminals try to redirect the users to malware-infected websites or to cause them to download and install Adware or Spyware.

The development of smart phones has led to a spectacular increase in the number of applications for them. Application makers focus on adding new features rather than security, many applications having errors and vulnerabilities that can be exploited by cybercriminals. The large number of malware-infected applications and the fact that about 28% of users ignore security measures on mobile phones increases the number of cyber-attacks in this area by nearly 400% each quarter¹³.

The cyber threats from the Romanian cyberspace follow the trend of computer attacks in the world. Due to the fact that a high percentage of the population uses counterfeit operating systems or software, many existing vulnerabilities increase the risk of malware infection of the computer systems.

Online platforms, improperly protected or outdated, may be infected by cybercriminals, which may have serious implications for visitors or hosting

¹³ <http://www.mobileworldcongress.com/>

servers. In case of inappropriate configuration, infection can spread to other platforms hosted on the respective servers, and then transmitted to visitors. Cybercriminals can involve compromised platforms in various cyber-attacks, such as DoS (Denial of Service), phishing, or e-mail spamming.

2.2. Classification of cyber-attacks

The cyber-attacks can be categorized according to the target of the cybercriminals or access to cyber infrastructures.

Depending on the objective, cyber-attacks can be defined on three levels: opportunistic, intermediate, and complex attacks¹⁴.

Opportunistic cyber-attack is the most common type of attack encountered and is typically associated with the profile of the occasional attacker. In this category can come dissatisfied employees who have limited knowledge in the field of informatics.

Opportunistic cyber-attacks have the following features:

- The attacker has a general goal and uses a wide range of targets. The immediate impact of this attack may be the denial of the services offered by web servers, FTP or e-mail servers;
- The attacker uses downloaded tools from the Internet to scan the type of computer system and take advantage of any vulnerabilities discovered;
- The attacker can penetrate inside the target system through a spam attack using an e-mail virus;
- The attacker has limited knowledge of the security system, processes, or applications installed in the computer system;
- There is a high frequency of these types of cyber-attacks;

¹⁴ https://link.springer.com/chapter/10.1007/978-3-642-31869-6_40

- Computers infected and involved in the attack are named zombies or drones¹⁵ and can be used to attack other networks or online platforms;
- These types of attacks have a relatively low impact on well-administered and secure information systems, but there are exceptions¹⁶.

Protective methods used against opportunistic attacks are firewalls that control access, monitor the system, network connectivity apps to detect intrusions, and antivirus programs that detect malware. These programs need to update frequently their version and database to be effective against the latest types of attacks.

The intermediate cyber-attack has an organized target. The attacker who performs such an attack is usually better trained than the occasional attacker and will be able to better conceal his criminal activity. The attacker scans the target to discover the security breaches or vulnerabilities existing in the system or in applications. Such an attack has the following features:

- The attack may compromise, in a first phase, an external computer system of trust, the attack then expanding to other systems;
- The attacker usually presents patience and skills in computer science;
- There is a high probability of success of this type of attack, compared to the opportunistic type of attack and a high probability that some of the essential services of the system will be affected.

The complex cyber-attack has a specific target and can greatly affect the main services of the target computer system. The attacker may try to compromise the company's internal staff – the attack being also named social engineering. Although the current defensive systems are focused on both detection and prevention, complex attacks have a very high probability of success. If a company

¹⁵ http://www.cert-ro.eu/files/doc/915_20150325000331012990800_X.pdf

¹⁶ Gorman, S. and Barnes, J., *Cyber Combat: Act of War*, 2011

has been the target of a complex attack, the most important thing is the recovery of compromised data and services.

The complex attack has the following features:

- The attacker is usually patient, waiting for the right moment to launch the attack;
- The attacker has set a well-defined target;
- The attacker will allocate sufficient time to gather information about the architecture of the computer system, applications and services installed;
- The attacker has the ability to modify or create their own software tools used to launch the attack;
- There is a very high probability of success of this type of attack.

Depending on the type of access to cyber infrastructures, attacks are divided into three general categories: attack by access to users, attack by access to network components, and attack by access to applications¹⁷.

The attack by access to users requires access to database with the system users who have certain privileges. The steps used by an attacker in this type of attack are the following:

- *The pre-attack phase.* A scan of the target computer system is performed to obtain the data necessary to identify security breaches. This process is usually automated by using specific applications. The vulnerabilities found may exist in the operating system or in the installed applications, may result from system configuration errors or system administration errors¹⁸, or may appear in the wrongly implemented security policies;

¹⁷ Tidwell, T., Larson, R., Fitch, K. and Hale, J., Modeling Internet Attacks, 2001.

¹⁸ Cowan, C., Wagle, P., Pu, C., Beattie, S. and Walpole, J., Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade, DARPA Information Survivability Conference and Expo (DISCEX), 2000.

- *Phase of attack.* Exploiting a security breach is done to gain access to information about the target system. In the first stages of an attack, vulnerabilities can come from information such as computer names or user account names;
- *The post-attack phase.* Effects resulting from an attack like this are data modification, access to confidential information, or the establishment of connections to certain applications.

Attack by access to network components creates denial of service by sending errors requests. Due to the large number of requests, the time needed for their processing is delayed a lot, leading to the interruption of the service. The steps used in this type of attack are:

- *The pre-attack phase.* In the initial phase, the components of the target system and the open communication ports are identified;
- *Phase of attack.* Very large number of messages are transmitted to the open communication ports;
- *The post-attack phase.* The effects resulting from the attack cause the network components to overload or even discontinue their function.

The attack by access to applications sends erroneous data to the installed applications in the computer system by properly formatting the data traffic. The steps used in this attack are the following:

- *The pre-attack phase.* Start by identifying the target application. This can be a network application such as a web, FTP or email server, web browser, or an Office application;
- *Phase of attack.* The data stream is sent directly or indirectly to the target application identified in the pre-attack phase;
- *The post-attack phase.* As a result of such attacks user files can be copied or deleted and user account settings can be changed.

2.3. Structure of cyber-attacks

The essence of an intrusion lies in the fact that the cybercriminal must create a way to penetrate the security system, place itself in a secure environment, and therefore act on the targets, violating the confidentiality, integrity and availability of data, applications, or equipment in that computer environment. The structure of cyber-attacks has been defined by Lockheed Martin researchers using the *Cyber Kill Chain*¹⁹ intrusion model.

2.3.1. The Cyber Kill Chain intrusion model

An intrusion model is a systematic process of tracking and capturing your opponent in order to obtain the desired effects. The American military doctrine²⁰ defines the steps of this process:

- *Finding*: identifying adverse targets for capture;
- *Localization*: establishing the coordinates of these targets;
- *Tracking*: observation and monitoring of activities;
- *Targeting*: Use of appropriate weapons to obtain the desired effects;
- *Capturing*: catching the opponent;
- *Evaluation*: estimate the produced effects.

This point-to-point integrated process is described as a “chain” because any deficiency at any level will interrupt the operation of the whole process.

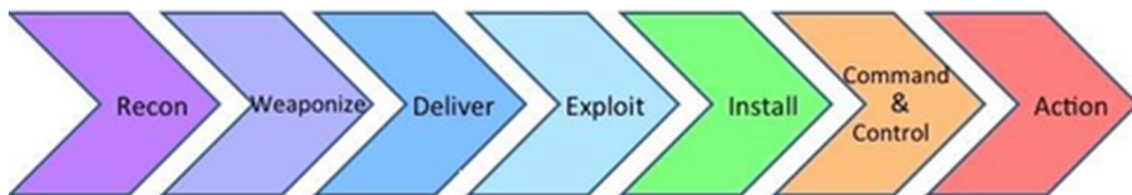


Fig. 1: *Cyber Kill Chain* intrusion model²¹

¹⁹ <http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html>

²⁰ http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf

²¹ <https://www.darkreading.com/attacks-breaches/leveraging-the-kill-chain-for-awesome/a/d-id/1317810>

The intrusion model consists of reconnaissance, weaponization, delivery, exploitation, installation, command and control and action on objective.

Under the terms used to describe the attack on a cyber-infrastructure or to spy traffic from a computer network, the above steps consist of:

- *Reconnaissance* - research, target identification and selection: it may be looking for e-mail addresses, social relationships, or data about a particular technology, information displayed on various websites;
- *Weaponization* - making a malware application (for example, a computer trojan) that, combined with an exploitable security breach, allows remote access. Moreover, PDF (Portable Document Format)²² files or Microsoft Office suite-specific files can be regarded as weapons available to the attacker;
- *Delivery* - transmitting the weapon to the target environment. The main ways of transport are e-mails (attachment of infected files), web platforms (running malware scripts), or removable USB memories;
- *Exploitation* - after the weapon is delivered to the victim, follows the targeting of an application or vulnerability of the operating system. The infected file can be used by the self-execution facility to launch the malware code, or it can be executed by the user himself;
- *Installation* - infecting a victim system with a computer trojan, backdoor or other malware application of this type that ensures the attacker's presence in the target environment;
- *Command and control* - usually an infected host must be accessible outside of the local network to establish a command and control channel between the victim and the attacker. Once this bidirectional communication has been made, an attacker has access inside the

²² <https://www.symantec.com/content/dam/symantec/docs/infographics/istr-zero-day-en.pdf>

target environment and can usually control the activity by manually launching commands;

- *Action on objective* - after the first six phases, an attacker can act to achieve the goals. These actions typically consist of collecting information, modifying data integrity, or attacking the availability of services and devices, but the victim system can also be used as a starting point for infecting other systems or for expanding access to the local network²³.

The *Cyber Kill Chain* intrusion model is a new way of analysis used by security analysts to understand what information is available to perform defensive actions.

2.3.2. Cyber-attacks analysis

The main cyber-attacks today are malware attacks: computer viruses, trojans, worms, adware, spyware, ransomware, rogueware, or scareware, DoS (Denial of Service) attacks, e-mail and web based attacks²⁴.

Malware Attacks

Malware attacks (computer viruses, trojans, worms, adware, spyware, ransomware, rogueware, and scareware) represent the most common forms of attacks targeting e-mail and web applications.

*The computer viruses*²⁵ are application with mostly destructive effects, designed to infect a computer system. The virus has two main features: it self-runs and self-multiplies in the infected system. A computer virus can affect the hard disk MBR (Master Boot Record) sector, executable files, system or Office

²³ Majority Staff Report, A “Kill Chain” Analysis of the 2013 Target Data Breach, 2014

²⁴ Mihai, Ioan-Cosmin, Information security. Second Edition, Revised and Expanded, Ed. Sitech, 2014

²⁵ <http://www.securitatea-informatiilor.ro/tipuri-de-atacuri-informatic/analiza-virusilor-informatici/>

files, directory structure, or certain applications. From the operating point of view, viruses are classified into:

- *Invisible viruses* - use viral code masking techniques to hide the fact that the computer system has been infected;
- *Polymorphic viruses* - use an encryption technique to modify their own viral code. Through this mutation process, a virus can change its signature and size, making it much harder to detect;
- *Viruses resident in computer memory* – install themselves in the RAM memory to infect applications and Office files that are released in the computer system.

*Computer trojans*²⁶ are applications that give the impression of performing legitimate operations, but actually try to explore computer system vulnerabilities and open ports in the operating system to allow attackers to access the system. Trojans are basically composed of three modules: *the server* - used to infect the victim system, *the client* - used to connect the attacker to the infected system and send commands and *the editing module* - used to configure the server.

Depending on the purpose, computer trojans are divided into the following categories:

- *Backdoors* – create breaches in the defense system by opening ports and connecting with the cybercriminals;
- *Password stealer*: retrieves keyboard data and stores them in files transmitted to the attacker's email account;
- *Logical bombs*: performs various operations that compromise the security of the computer system when certain conditions are met;
- *Denial of Service*: Send data sequences to a victim system to interrupt the services installed on that system.

²⁶ <https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html>

*Computer worms*²⁷ are applications with destructive effects that infect the computer system and spread over the Internet. The computer worms look for computer systems with vulnerabilities, infect them and perform destructive operations, then try to propagate further.

From the point of view of propagation, the computer worms are classified as follows:

- *Email worms*: spread through links from compromised websites or through attachments to email messages;
- *Messaging worms*: spread through instant messaging by sending messages containing links to compromised websites;
- *Internet worms*: spread through computer networks, searching for vulnerable cyber infrastructures to infect;
- *IRC worms*: spread through chat channels that send malware or links to compromised websites to all users;
- *File worms*: spread through shared folders on the network.

*Adware*²⁸ is an application that installs in the operating system and aggressively display the ads to users. Ads are displayed in the browser window or in pop-up windows. This type of apps are used to advertise certain products.

Adware applications have the effect of interrupting or distracting the user from the current activity, often leading to system memory loading and, implicitly, to degradation of computer performance. Internet browsers are most affected by adware, changing their homepage, bookmarks, or even settings.

*Spyware*²⁹ is an application that has the role of capturing various information about Internet users' activity in secret. This information can be sent to people who created spyware and can be used to send unsolicited advertisements

²⁷ <https://www.lifewire.com/how-computer-worms-work-816582>

²⁸ <https://usa.kaspersky.com/resource-center/threats/adware>

²⁹ <https://www.avast.com/c-spyware>

to the user. Some spyware can redirect the activity of the Internet browser or modify search engine results to redirect the user to certain compromised websites.

Spyware can be delivered with other software or by using computer viruses or worms. Spyware infection leads to increased processor activity, increased memory usage and network traffic. Stability issues of the operating system, hindering or blocking certain applications or slowing down network traffic are common to spyware infection. Spyware can change computer settings, the home page of the Internet browser, or even create security breaches in the operating system.

*Ransomware*³⁰ is a malware application that restricts access to the infected computer system or files and requires a ransom to remove it. Some types of ransomware encrypt data on the system's hard disk, while others can simply block the computer system and display messages to persuade the user to pay.

Ransomware applications are propagated through email attachments, infected websites, or network service vulnerabilities. The program, once installed, will encrypt files on the hard drive. Some ransomware can encrypt the victims' files using a random symmetric key and a fixed public key. The malware author is the only person who knows the private decryption key needed to decrypt the data. Other types of ransomware just restrict user access to the operating system.

Rogueware is an application that misleads users to pay for removing false infections detected in the operating system. Most of the time, this type of application claims to remove the malware found on computers, but in reality installs applications with destructive effect.

Rogue apps are propagated through websites that show false reports to visitors of malicious malware found in their system, trying to get them to install or buy antivirus-like apps. In most cases, infections detected on user computers

³⁰ <https://www.microsoft.com/en-us/wdsi/threats/ransomware>

are not real and applications indicated to be downloaded doesn't not work or contain malware.

Scareware is an application that causes users to fear in order to market certain fake applications. Spyware attacks can use adware, spyware, or ransomware. Scareware applications produce security alerts or even threats for installing false antivirus, firewall, or registry cleaners from the operating system.

DoS (Denial of Service) attacks

*DoS attacks*³¹ has the effect of compromising the operation of certain Internet services. One of the most common DoS attacks is the flood packet attack, which sends a large number of packets to the victim's system and has the effect of blocking open connections and charging network traffic, leading to disruption of the services offered by the attacked system. If these types of cyber-attacks come from many sources, they are called DDoS (Distributed Denial of Service) attacks³².

From the point of view of the type of packets transmitted, Denial of Service attacks are classified into:

- *SYN flood attacks*³³: a large number of TCP (Transmission Control Protocol) packets are sent to a server, leading to overloading traffic and the failure of services to respond to other requests;
- *Fraggle attacks*³⁴: UDP (User Datagram Protocol) packets are sent to the broadcast address of a computer network. UDP packages are transmitted to all systems from that network, resulting in increased traffic within the network;

³¹ <https://www.us-cert.gov/ncas/tips/ST04-015>

³² Preimesberger, Chris, DDoS Attack Volume Escalates as New Methods Emerge, eWeek, 2014

³³ <https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-34/syn-flooding-attacks.html>

³⁴ <https://security.radware.com/ddos-knowledge-center/ddospedia/fraggle-attack/>

- *Smurf attacks*³⁵: ICMP (Internet Control Message Protocol) packets are sent with the source IP (Internet Protocol) address changed to the broadcast address of a computer network. The computers within that network will respond to the request to the IP address of the ICMP packets. This attack will generate traffic to the IP address set, possibly blocking the services installed on the victim's computer.

Denial of Service attacks represent a threat to computer systems that offer Internet services, resulting in interruption of traffic and services. As botnets have become more powerful, the number of DDoS for ransom attacks (RDoS attacks)³⁶ increased during this year.

Email based attacks

Lately, the number of cyber-attacks that use email services to spread has increased exponentially. Depending on the purpose of cybercriminals, email based attacks are of several types: email bombing, spoofing, spamming, and phishing.

*Email bombing*³⁷ attack consists of repeatedly sending an email with large attachments to a specific email address. This attack results in filling the available space on the server, making the email account inaccessible.

*Email spoofing*³⁸ attack consists of sending emails with the address of the sender modified. This attack is used to hide the real identity of the sender to find out confidential details or the data needed to access an account.

*Email spamming*³⁹ is an attack that consists of sending unsolicited email messages with commercial content. Often, files infected with malware are also sent through these spam messages. The purpose of these attacks is to get recipients of emails to visit certain websites and buy more or less legitimate products or services.

³⁵ <https://www.techopedia.com/definition/17294/smurf-attack>

³⁶ <https://security.radware.com/ddos-threats-attacks/cyber-ransom-spring-2017/>

³⁷ <http://www.thewindowsclub.com/email-bombing>

³⁸ <https://blog.malwarebytes.com/cybercrime/2016/06/email-spoofing/>

³⁹ <https://runbox.com/email-school/what-is-spam-and-how-to-avoid-it/>

*Email phishing*⁴⁰ is a growing attack, consisting of sending messages to determine the recipients of emails to provide information about bank accounts, credit cards, passwords or other personal details. The sent messages use official visual texts and elements to be as credible as possible, bringing plausible arguments to the victims to enter the pages created by the attackers. The most common topics are changing bank account data, the attackers trying to persuade users to access the links provided and enter the pages created by them to fill in forms with confidential data. By providing confidential information as a result of these attacks, cybercriminals can withdraw money from victims' accounts, open new accounts, or commit offenses under the victim's identity.

Web based attacks

The spectacular development of web technologies has led to the development of interactive, dynamic content platforms that allow for high user interaction. These new platforms have vulnerabilities that can be exploited by cybercriminals to avoid security measures and to access unauthorized information in databases. Attacks to web applications consist mainly of exploiting vulnerabilities and inserting code sequences to modify the content of the platforms.

The most common attacks of web based attacks are:

- *SQLi attack* – SQL (Structured Query Language) injections: the attacker can insert certain data into an SQL query that is transmitted to the database, changing the logic of the query. In this way, the attacker can avoid authentication mechanisms from a website;
- *XSS (Cross Site Scripting) attack*: the attacker inserts in a website scripts that are executed in the victims' browsers when they visit the infected website;

⁴⁰ <https://kb.iu.edu/d/arsf>

- *CSRF (Cross-Site Request Forgery) attack* uses the trust relationships established between web applications and authenticated users. The attacker takes control of the victim's session, having the full control on the user account;
- *Man in the Middle attack*: the attacker intercepts the communication between the user and the website, and can retrieve the access data if they are not fully encrypted.

2.3.3. Study of cyber-attack vectors

Cyber-attack vectors are the methods used by cybercriminals to accomplish the purpose of an attack. A cybercriminal uses different attack tools and methods to take advantage of, and gain access to, the systems' vulnerabilities, in order to achieve their goals (illegal profits, fraud, information theft, sabotage, etc.).

The *Cyber Kill Chain* intrusion model is correlated with the notion of an attack vector, assuming that an intrusion pattern characterizes the different phases of an attack vector.

Targeted attacks

The *targeted attack*⁴¹ is built on specific information regarding the target, previously collected by the attacker. Using this information, the attacker sends messages or uses other mechanisms to deceive his victim. Once it arrives at the destination, the infected message is not recognized by the victim due to its usual content (includes references to current issues of the company or its staff).

Targeted attacks usually cover all phases of an intrusion model. Such an attack begins with the reconnaissance stage where data about the staff, structure, and other internal information in the company or other characteristics of the target are collected. It is followed by the weaponization stage (identifying the

⁴¹ <https://www.trendmicro.com/vinfo/us/security/definition/targeted-attacks>

appropriate malware to use). Delivery occurs when the victim is deceived and the exploitation stage takes place when the vulnerability that can be used in that attack is found. Finally, the installation of the malicious code that will create a communication channel with the opponent through which they will take over the command and control of the victim in the realization of the final objective.

Among the many forms of targeted attacks are *spear-phishing* (emails sent apparently by known people or partner companies that contain personalized messages and colloquial language) and the *watering hole attack* (an attack on a group by guessing or tracking websites often visited and infecting them with malware so that one of the members of the target group eventually gets infected).

Drive-by-download attack

In drive-by-download attack⁴², the victim uses a legitimate website, application, or webpage that, through various handling techniques (for example, code insertion), redirects the victim's browser to an infected website. It checks browser vulnerabilities and installs malware in the background to exploit the discovered vulnerabilities. Redirecting can be done by reading an email or by automatically opening a pop-up window (via HTML or widgets) in the browser without the victim realizing that he has accessed a compromised application.

This type of attack covers all phases of an intrusion model, less the reconnaissance phase. Weaponization occurs when scanning vulnerabilities in the victim's web browser. Delivery is made through downloader programs, and exploitation takes place after the execution of the downloaded code. Depending on the vulnerabilities found, the malware program downloads a malicious code (usually a computer trojan) that takes over the victim's computer (implementation of the command and control stage).

⁴² <https://heimdalsecurity.com/blog/how-drive-by-download-attacks-work/>

There are various variants of drive-by-download attacks that exploit vulnerabilities at the levels of the web browser, installed add-ons, operating system, or various installed applications (Microsoft Silverlight, Adobe Flash, Adobe PDF, or video players).

Watering Hole attacks

The Watering Hole attack⁴³ is based on infecting a legitimate website that a group of users (victims) frequently visit and trust, so they will be infected in turn. This attack can be considered complementary to phishing attacks, being effective if a group is resistant to such attacks.

This type of attack starts with the reconnaissance stage to identify the sites that the target group uses. The steps of a drive-by attack:

- Weaponization is done by scanning vulnerabilities of the victim's web browser;
- Delivery is done through downloader programs;
- Exploitation takes place after executing the downloaded code;
- The malware installed (usually a computer trojan) performs the command and control phase on the targets.

This type of attack is classified as a targeted attack because attackers can launch an attack on a specific target group (programmers, marketing activities, or media companies) by properly selecting the infected website.

Advanced Persistent Threats

*APT (Advanced Persistent Threats)*⁴⁴ attacks refer to restricted, targeted campaigns, launched by high-performance threat agents. Another feature of these attacks is persistence: they run for a long period of time (months or years).

⁴³ https://www.symantec.com/content/en/us/about/media/pdfs/b-istr_18_watering_hole_edits.en-us.pdf

⁴⁴ <https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html>

Performances usually consist of a high degree of orchestration of the attack, the use of advanced malware and a good knowledge of victim details. APT attacks are specific to espionage activities and require the allocation of generous resources to prepare for attack, recognition, programming, and vulnerability detection.

As a large-scale attack, APT covers all phases in the intrusion model (reconnaissance, weaponization, delivery, exploitation, installation, command and control, action on objective). Another important feature is the differentiation of APT attacks: depending on the target victim, the attacks are different from each other in terms of their preparation and execution. Attackers launching APT attacks are involved in espionage or sabotage, behind the attack being either a state actor or large companies that can sustain such a long and complex attack with well-coordinated activities.

2.4. Methods to prevent cyber-attacks

Protecting the servers against cyber-attacks involves the application of security measures both at a logical level (security of access and services) and at physical level⁴⁵.

Physical security consists in the closure of IT equipment in a dedicated space and the provision of access control.

Logical security consists in software that are necessary to control the access to information and services of a system. The logical level is divided into two categories: access security level and service security level.

Automatic update of the operating system from the servers is recommended for troubleshooting security breaches or uncovered programming errors. Updating installed applications in the operating system is only possible for licensed programs; the use of pirated programs can induce cybersecurity risks.

⁴⁵ Mihai, Ioan-Cosmin, Information security. Second Edition, Revised and Expanded, Ed. Sitech, 2014

Installing antivirus or anti-spyware applications is required to secure the operating system from the server. These applications typically have two components:

- A component automatically launched at the start of the operating system that runs in the background and monitors users activity (running programs, web browsing, launching email attachments, installing various applications);
- A component that is running on demand when it is intended to effectively scan the operating system to search for malware.

Installing a firewall application is an essential requirement in ensuring the security of any server. The role of this program is to control the flow of information flowing between the user computer and another destination (either from the local network or from outside it).

A firewall can filter, accept, or block the transfer of data according to established security policies (blocking data theft or illegal connections to the server).

Protecting personal data is an important aspect. The way how personal information is provided on websites, should be done as responsibly as possible. The users must be attentive when providing data that could lead to their identification or identity theft (name, surname, date of birth, personal identification number, address, telephone, bank card details, etc.).

Some basic steps in storing personal data are:

- The use of complex, unique, hard to guess or break passwords, consisting of numbers, upper/lower case letters and special characters;
- Storage the minimum required data online and maximum discretion in providing them to a third party (users, companies);

- Using encrypted versions of protocols when sensitive information is exchanged so as to ensure data confidentiality and prevent identity theft;
- Encrypting all personal information when saved on different storage media.

An additional risk occurs when personal information is stored in client accounts on commercial websites, which may become the target of cyber-attacks anytime, so stored data becomes vulnerable.

2.5. Conclusions

Due to the cross-border nature of the cyberspace, cyber-attacks have seen a great deal of diversification, some of which can be classified as global epidemics due to the high speed of Internet dissemination.

In this chapter, I analyzed the evolution of cyber-attacks, from computer viruses created for entertainment in the 1980s, to the creation of computer trojans and worms used for industrial espionage. I investigated comparative studies and case studies to classify cyber-attacks according to cybercrime targets (opportunistic, intermediate, and complex attacks), and access to cyber infrastructures (attack by access to users, attack by access to network components, and attack by access to applications).

The essence of an intrusion lies in the fact that the cybercriminal has to develop a method through which to penetrate the security system, place itself in the secure information environment, and act on the targets. I analyzed the structure of cyber-attacks using the *Cyber Kill Chain* intrusion model, defined by Lockheed Martin researchers, structured in seven steps: reconnaissance, weaponization, delivery, exploitation, installation, command and control and action on objective. The intrusion model is a new way of analysis used by security analysts to understand the attack model and what information is available in defensive actions.

As a result of the documentation at the institutions involved in the fight against cybercrime, I classified the main cyber-attacks as: malware infections: computer viruses (trojans, worms, adware, spyware, ransomware, rogueware, and scareware), DoS (Denial of Service) attacks, e-mail and web based attacks.

I studied the attack vectors, which represent the methods used by cybercriminals to accomplish the purpose of an attack. The *Cyber Kill Chain* intrusion model is correlated with the notion of the attack vector, which characterizes different phases of a cyber-attack.

In the end of this chapter I developed a guideline for protecting web servers against cyber-attacks and for assuring a safer cyberspace.

CHAPTER III

MONITORING WEBSITES SECURITY

Cybersecurity⁴⁶ represents the state of normality of digital information, resources and services offered by public or private entities in cyberspace. Monitoring cybersecurity is useful to confirm the functionality and effectiveness of implemented security measures. The monitoring process consists in collecting, analyzing and evaluating indicators and warnings on detecting and responding to security incidents.

The activity of monitoring the websites security consists of:

- Intrusion detection;
- Detection of vulnerabilities;
- Detection of malware infections;
- Detection of suspicious redirects;
- Application and server error analysis.

In the monitoring process that can be automated, data analysis involves human factors, and the assessment of the detected incidents is a process of decision-making by computer platform administrators.

3.1. Developing an attack tree

The attack tree⁴⁷ is a systematic method that characterizes the security of a computer system, based on cyber-attacks. Attack information is redefined,

⁴⁶ http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

⁴⁷ Schneier, B., Attack Trees: Modeling Security Threats, Dr. Dobb's Journal, 2003

identifying the means of compromising the security of a computer system as the root of the tree.

3.1.1. The structure of an attack tree

An attack tree consists of a root node and several nodes⁴⁸ located on multiple depth levels. The way in which a cyber-attacker can compromise the computer system is iteratively and incrementally represented as the nodes at the base level of the tree. Each computer system can be set up with an attack tree relevant to the operations made. The root of the tree is an event that can affect the security of the computer system.

Each attack tree presents methods by which a cyber-attacker can cause an incident. Each path within an attack tree represents a unique attack on the system.

The attack tree can be decomposed in two ways:

- *AND analysis* - all attacks must be completed in order for the global attack to succeed;
- *OR analysis* - any of the attacks can be accomplished for the global attack to be successful;

Attack trees can be represented either textually or graphically.

AND analysis for an attack tree is represented as follows:

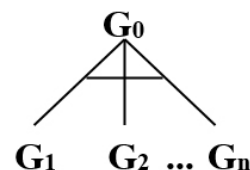
Target G_0

AND G_1

G_2

...

G_n



The target is the G_0 node and can be compromised if the attacker performs all the events from node G_1 to node G_n .

⁴⁸ https://www.schneier.com/academic/archives/1999/12/attack_trees.html

OR analysis for an attack tree is represented similar as AND analysis, textual or graphical.

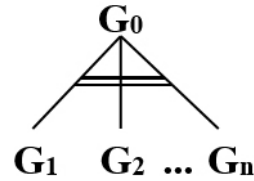
Target G_0

OR G_1

G_2

...

G_n



The target is the G_0 node and can be compromised if the attacker performs any of the events of nodes $G_1, G_2 \dots G_n$.

Attack trees consist of a combination of AND and OR analyzes. Intrusion scenarios are generated individually on an attack tree crossing the tree from the first to the last level in depth. Attack tree nodes are added as the scenario is generated. An OR analysis can lead to new scenarios that can be generated, while an AND analysis can lead to the extension of existing scenarios.

Attack trees allow cyber-attacks at a detailed level. They show the property of referential transparency characterized by S.J. Prowell: “*Referential transparency implies that the details of an entity's inferior relative level are theorized rather than omitted in a particular system to a description of a higher level, so that the description of the higher level contains everything that must be understood about the entity when it is put in a wider context*”.

This property allows the security administrator to explore in-depth certain methods of attack and generate intrusion scenarios that make sense in a particular context. In addition, by optimizing the branch of the attack tree that can generate other branches, scenario intrusion results in a lower abstraction level.

3.1.2. Developing an attack tree for websites

In developing the attack tree for a website, the root of the tree must represent the compromising security of the platform. I developed a high-level tree with the root node representing the compromising security of a website.

ROOT Compromise the security of a website

AND 1. Identifying vulnerabilities

OR 1. Scanning the vulnerabilities of the website

2. Analyzing the website activity and identifying the users

3. Developing social engineering attacks on users

2. Developing software tools for exploiting vulnerabilities

OR 1. Developing the tools required for cyber-attack

2. Configuring existing attack tools

3. Simulating cyber-attacks to the website

OR 1. SQLi (SQL Injection) attack

2. Brute Force attack

3. XSS (Cross-Site Scripting) attack

4. CSRF (Cross-Site Request Forgery) attack

5. DoS (Denial of Service) attack

4. Exploitation of vulnerabilities identified

5. Injecting scripts on the website

OR 1. Injecting malicious scripts

2. Injecting malware

6. Controlling the website

OR 1. Accessing the website administration panel

2. Accessing the website database

7. Creating damages to the website

OR 1. Retrieving data from the website database

2. Modifying the website files

3. Using the website for other cyber-attacks

Fig. 2: High-level attack tree for a website

The root branches of the tree represent an AND analysis and follow the steps of the *Cyber Kill Chain* intrusion model. Being an AND analysis, an attacker can compromise the security of the website G_0 by making all $G_1, G_2 \dots G_7$ events. Exception will be the case for the DoS - branch 3.5, which can compromise the website security only in the first 4 steps: $G_1 - G_4$, affecting the availability of the online platform.

The first branch of the top level of this attack tree deals with the first step in the *Cyber Kill Chain – Reconnaissance*. In this step, the cyber-attackers will investigate and identify the website vulnerabilities. The vulnerabilities of the website and also the vulnerabilities of the web and hosting servers will be scanned, users with access rights on the platform will be identified, and social engineering attacks will be performed to these users in order to obtain their accounts credentials.

1. Identifying vulnerabilities

OR 1. Scanning the vulnerabilities of the website

2. Analyzing the website activity and identifying the users

3. Developing social engineering attacks on users

Fig. 3: The first branch of the attack tree to a website

The second branch represents the *Cyber Kill Chain weaponization* step. The cyber-attackers will develop the software tools needed to exploit the vulnerabilities identified in the first step. If the cyber-attackers have advanced programming knowledge, they will create their own attack tools, otherwise they will use and configure tools downloaded from the Internet (Dark Market).

2. Developing software tools for exploiting vulnerabilities

OR 1. Developing the tools required for cyber-attack

2. Configuring existing attack tools

Fig. 4: The second branch of the attack tree to a website

The third branch of the attack tree represents the *delivery* – the transmission of the weapon in the target environment. The attackers will launch the cyber-attack on the target platform. Depending on the tools developed in step 2, SQLi, Brute Force, XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery), or DoS (Denial of Service) attacks may be initiated. In the case of DoS attack, the use of the attack tree will stop at point 4, this attack not allowing the last three steps of the intrusion model.

3. Simulating cyber-attacks to the website

OR 1. SQLi (SQL Injection) attack

2. Brute Force attack

3. XSS (Cross-Site Scripting) attack

4. CSRF (Cross-Site Request Forgery) attack

5. DoS (Denial of Service) attack

Fig. 5: The third branch of the attack tree to a website

The fourth branch of the attack tree is *exploiting* the vulnerabilities discovered in step 1 through the cyber-attack done in step 3.

4. Exploitation of vulnerabilities identified

Fig. 6: The fourth branch of the attack tree to a website

The fifth branch represents the *installation* of the scripts in the website. Thus, the cyber-attackers can insert various malicious scripts or iFrames to perform unwanted actions on the visitors, or malware that infects the users.

5. Injecting scripts on the website

OR 1. Injecting malicious scripts

2. Injecting malware

Fig. 7: The fifth branch of the attack tree to a website

These scripts installed in step 5 lead to the next command and control step of the cyber-attackers to the website.

The sixth branch of the attack tree – *Command and control*, shows that the cyber- attackers have access to the inside of the website and can control it. The attackers can access the website administration panel or the database.

6. Controlling the website

- OR** 1. *Accessing the website administration panel*
2. *Accessing the website database*

Fig. 8: The sixth branch of the attack tree to a website

The last branch, the seventh, represents the last step of the *Cyber Kill Chain* intrusion model – *Action on the objective*. After the first six steps, the cyber-attacker can act to achieve the proposed goals.

The cyber-attackers activities can consist of collecting database information, modifying data integrity, or attacking the online platform availability. The victim platform can also be used as a starting point for infecting other computer systems. Thus, the cyber-attacker can infect with malware the users who access the compromised platform, or can redirect them to other infected and controlled websites (clickjacking).

7. Creating damages to the website

- OR** 1. *Retrieving data from the website database*
2. *Modifying the website files*
3. *Using the website for other cyber-attacks*

Fig. 9: The sixth branch of the attack tree to a website

In order to compromise the website security, all the steps of the seven branches must be fulfilled (only four in the case of DoS attack – branch 3.5), being an AND analysis.

3.2. Analysis of the impact of cyber-attacks

3.2.1. Vulnerabilities of websites

In this chapter, I analyzed the main vulnerabilities of websites present in the top 10 vulnerabilities of OWASP⁴⁹ (Open Web Application Security Project).

Code injection

The attack that is based on this vulnerability consists of sending certain information, in text, to an interpreter as part of an order or queries⁵⁰. By this method, the attacker can mislead the interpreter to execute certain malicious commands or gain unauthorized access to certain information.

The most common code insertion attacks occur in SQL (Structured Query Language)⁵¹, XPath (XML Path Language)⁵², LDAP (Lightweight Directory Access Protocol)⁵³, in operating system commands, or as software arguments.

The impact of this vulnerability is one of the most serious, leading to stealing, modifying, deleting or corrupting data, altering user accounts, blocking access, or taking over a cyber-attacker's total control.

Broken authentication and session management

In some applications, the functions responsible for user session authentication and management are not properly implemented⁵⁴, allowing a

⁴⁹ https://www.owasp.org/index.php/Top_10_2017-Top_10

⁵⁰ https://www.owasp.org/index.php/Top_10_2017-A1-Injection

⁵¹ <https://www.techopedia.com/definition/1245/structured-query-language-sql>

⁵² <https://www.w3.org/TR/xpath/>

⁵³ [https://msdn.microsoft.com/en-us/library/aa367008\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa367008(v=vs.85).aspx)

⁵⁴ https://www.owasp.org/index.php/Top_10_2017-A2-Broken_Authentication_and_Session_Management

cyber-attacker to compromise passwords or substitution of session tokens, which may lead to possible identity theft.

Application developers typically create custom session authentication and management schemes, often with vulnerabilities in logout, password management, time-outs, account updates, etc. Attacks can come from both the outside and within the company, and the targeted accounts are both user-defined (limited) and broad-privileged.

XSS (Cross-Site Scripting)

The attack based on this vulnerability occurs when an application retrieves information and transmits it to a web browser without validating them correctly and deleting certain character strings⁵⁵. XSS is the most common attack in web applications; it allows the attacker to run scripts in the user's web browser, replacing the authentication session, rewriting a webpage's code, inserting unwanted content, or redirecting to infected websites. The vulnerability that allows the launch of an XSS attack may exist at server or client level.

Broken Access Control

Sometimes, different restrictions to users with access rights to a platform are not properly enforced⁵⁶. Cyber-attackers can exploit these vulnerabilities to access the platform, to have access to restricted data, to view all the users' accounts, to change the settings and the files from the platform.

Security Misconfiguration

A high level of security involves defining and applying security settings for applications, development environments, platforms, and servers⁵⁷. In launching

⁵⁵ [https://www.owasp.org/index.php/Top_10_2017-A3-Cross-Site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Top_10_2017-A3-Cross-Site_Scripting_(XSS))

⁵⁶ https://www.owasp.org/index.php/Top_10_2017-A4-Broken_Access_Control

⁵⁷ https://www.owasp.org/index.php/Top_10_2017-A5-Security_Misconfiguration

an attack, a malicious person can use default accounts, unused pages, unresolved vulnerabilities, unprotected directories and files, or unnecessary services. Defining, implementing and maintaining security policies and settings, as well as ongoing updating of applications, are mandatory actions for a high level of security.

Sensitive Data Exposure

Many web apps do not adequately protect sensitive information such as bank card number, taxpayer tax information, medical records, or user authentication information⁵⁸. An attacker can use such poorly protected information to launch cyber-attacks such as bank card fraud, identity theft, phishing, etc. Sensitive data must be encrypted when stored in databases or in transit between the client and the server, and must be handled carefully at the web browser level. When data is encrypted, the algorithms used and the encryption keys must be strong, and secure protocols (such as SSL - Secure Sockets Layer⁵⁹) must be used for their transfer.

Insufficient Attack Protection

Most of applications and APIs (Application Programming Interface)⁶⁰ don't have the basic ability to detect and respond⁶¹ to both manual and automated cyber-attacks. Attack protection have to involve automatically detecting, logging, and blocking exploit attempts.

CSRF (Cross-Site Request Forgery)

A CSRF attack⁶² forces the victim's browser (a logged-on user) to send a false HTTP request that includes the session cookie and other user authentication

⁵⁸ https://www.owasp.org/index.php/Top_10_2017-A6-Sensitive_Data_Exposure

⁵⁹ <http://info.ssl.com/article.aspx?id=10241>

⁶⁰ <https://techterms.com/definition/api>

⁶¹ https://www.owasp.org/index.php/Top_10_2017-A7-Insufficient_Attack_Protection

⁶² [https://www.owasp.org/index.php/Top_10_2017-A8-Cross-Site_Request_Forgery_\(CSRF\)](https://www.owasp.org/index.php/Top_10_2017-A8-Cross-Site_Request_Forgery_(CSRF))

information to a vulnerable web application that considers the victim's request as legitimate.

Using Components with Known Vulnerabilities

Certain components⁶³, like libraries or modules, are executed with full access rights. If such a vulnerable component is exploited, the attackers may gain access to a server or may cause loss, theft or corruption of data. The use of such vulnerable components allows for a wide range of possible attacks with the most undesirable effects.

Under protected APIs

Many applications often involve different APIs (Application Programming Interface), such as JavaScript in the browser and mobile applications⁶⁴. These APIs are not well protected and contain many vulnerabilities that can be exploited by cyber-attackers.

3.2.2. Impact of cyber-attacks on the websites

To investigate the impact of cyber-attacks to websites, I used the high-level attack tree, developed under subchapter 3.1.2, to simulate attacks on the platform created within this research and posted on the domain *web-scan.eu*. This study was based on the observation of simulated attacks, but also on real cyber-attacks, both random and target attacks, due to the area of interest of the platform.

Cyber-attacks targeting cyber platform vulnerabilities, such as SQLi or XSS (Cross-Site Scripting) inserts, are very hard to detect. To prevent code insertion attacks, the administrator must use some PHP filtering features⁶⁵ for forms displayed on the platform, such as:

⁶³ https://www.owasp.org/index.php/Top_10_2017-A9-Using_Components_with_Known_Vulnerabilities

⁶⁴ https://www.owasp.org/index.php/Top_10_2017-A10-Underprotected_APIs

⁶⁵ <http://php.net/manual/en/ref.filter.php>

- *htmlspecialchars ()* - converts all characters into HTML entities;
- *htmlspecialchars ()* - change special characters in HTML entities;
- *strip_tags ()* - removes the HTML and PHP tags from the character strings;
- *mysql_escape_string ()* - avoid string characters in MySQL queries;
- *mysql_real_escape_string ()* - Avoid special characters in the strings used in SQL statements;
- *addslashes ()* - quotes the character string with the "/" symbol.

An attack commonly encountered in the cyberspace, which the aim of breaking down the website admin accounts, is Brute Force⁶⁶. Attacks of this type try to guess the credentials of an admin account by repeated attempts of possible solutions, until the correct variant is found. The more configured passwords for admin accounts, the less likely the attack is to succeed. For example, for a simple, 6 characters' password, the number of possible combinations is approx. 300 million combinations and can break almost instantaneously. A 12 characters' password, including capitalized letters, numbers and special characters, can be broken in about 9,000 hours. These types of attacks can be avoided by installing plugins to restrict repeated access attempts in a short time.

When websites are not properly protected and broken, the attacker can perform a number of harmful actions, both for information from the online platform and for users visiting the site. Once the attacker has managed to avoid website protection, he can steal confidential information from the database. After the attacker takes over the data from the database, the compromised website can be used as a platform for distributing:

- Malware that can be downloaded by users;
- Hidden iFrames containing malware infections;
- Redirects to other infected websites;

⁶⁶ <http://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/#gref>

- Phishing messages delivered from the compromised website;
- Spamming messages delivered from the compromised website;
- Cookies⁶⁷ to monitor the activity of the website visitors.

The cyber-attackers can modify some information or change the compromised website's start page with another webpage, a cyber-attack called Defacement⁶⁸, or maybe even deactivate the entire platform.

If the attacker performs a DoS (Distributed Denial of Service) attack on the online platform, the effect of the traffic load is that it may interrupt the services offered by the web server, so the website cannot be accessed by users.

3.3. Monitoring websites security

The monitoring process of websites security can be done on the following activities:

- Intrusion detection;
- Detection of malware infections;
- Detection of suspicious activities.

When integrity or availability of websites files are compromised, malware, redirects to infected websites, phishing or spamming activities are detected, we can say that the security of the websites has been affected.

3.3.1. Intrusion detection

An IDS (Intrusion Detection System)⁶⁹ is an equipment or application that monitors events occurring a computer system, detecting incidents that constitute violations of established usage or security policies. For websites, an intrusion detection system can monitor the integrity of files and scan their content.

⁶⁷ <https://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro>

⁶⁸ <http://cybercrime.org.za/website-defacement>

⁶⁹ <https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids>

To monitor the integrity of files, cryptographic functions are used to calculate a fixed value for a file. At the smallest modification of the file, the result of such a function will be different. The safest hash function currently is SHA2 (Secure Hash Algorithm 2), used on 224, 256, 384 or 512 bits⁷⁰. Using these hash functions⁷¹, it can be detected whenever a file within the online platform changed. This can be detected, especially with dynamic platforms, when creating a new post, a new page, a new comment, or changing the content of the pages. In order not to generate a large number of alerts for dynamic platforms, it is possible to monitor only the core kernel files.

These types of functions must be integrated into dynamic platforms to monitor their performance. For static platforms, webpages can also be remotely monitored to verify their integrity.

Particular attention must be paid to the Brute Force attack, which aim the access to administration panel. When using a Framework⁷² to build an online platform, most of the time the administration panel access address remains unchanged and can be easily identified by attackers. At this default address, attackers will try to repeatedly access the administrator account until they identify the correct username and password. To avoid these attacks, the initial access to the platform administration panel must be changed, as well as the administrator's default name: admin. It is useful to integrate a module to limit unauthorized access attempts, thus blocking unlimited attempts.

Many Brute Force attacks have been recorded the *web-scan.eu* platform, attacks generated from multiple IP addresses. An example of such an attack was made on Jul 21, 2017, when there were about 200 attempts.

Username: admin

IP Address: 78.4.229.38

⁷⁰ <https://www.slideshare.net/sharifulr/secure-hash-algorithm-sha512>

⁷¹ <https://www.cs.hmc.edu/~geoff/classes/hmc.cs070.200101/homework10/hashfuncs.html>

⁷² <http://whatis.techtarget.com/definition/framework>

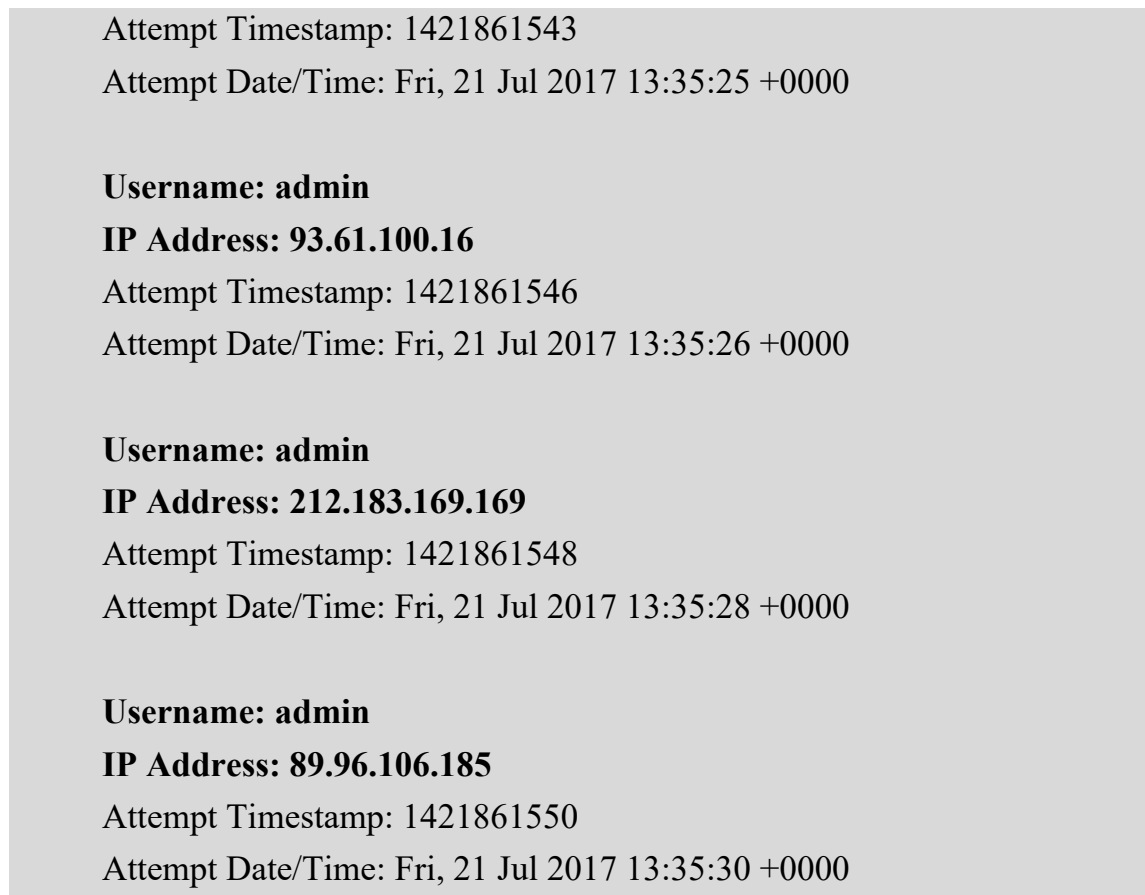


Fig. 10: Brute Force attacks to *web-scan.eu* website

As part of these cyber-attacks, the usernames used to attempt to break the administrator account were *admin*, *administrator*, *web-scan* and *web-scan.eu*. The most used names for the administrator account are *admin*, *administrator* and *domain name* on which the computer platform is located.

To remove these attacks, a WAF (Web Application Firewall)⁷³ was used to filter and block attempts to illegally access the platform.

⁷³ https://www.owasp.org/index.php/Web_Application_Firewall




IPs that are blocked from accessing the site	IPs that are Locked Out from Login	IPs who were recently throttled for accessing the site too frequently
<p> Germany IP: 82.165.157.95 [unblock] [permanently blocked] Reason: Manual block by administrator Hostname: s15739361.onlinehome-server.info <i>No attempts have been made to access the site since this IP was blocked.</i></p>		0 hits before blocked 0 blocked hits Permanently blocked
<p> Kharkiv, Ukraine IP: 176.102.37.58 [unblock] [permanently blocked] Reason: Manual block by administrator Hostname: bizsender.ru <i>No attempts have been made to access the site since this IP was blocked.</i></p>		0 hits before blocked 0 blocked hits Permanently blocked
<p> Milan, Italy IP: 83.211.84.67 [unblock] [permanently blocked] Reason: Manual block by administrator Hostname: ip-84-67.sn2.eutelia.it <i>No attempts have been made to access the site since this IP was blocked.</i></p>		0 hits before blocked 0 blocked hits Permanently blocked

Fig. 11: IP addresses blocked in the *web-scan.eu* website

Malicious code insertion attempts can be made both on the contact or access forms in the administration account, as well as on the comment forms. On July 21, 2017, a total of about 200 attempts to insert code have been blocked on the *web-scan.eu* website by the WAF (Web Application Firewall).

3.3.2. Malware detection

For detecting malware in websites, I chose to insert a malware script, to do some tests. For safety, I chose to work with iFrames. I pasted the script into a test page from *web-scan.eu* website and analyzed its content using the *Virustotal.com*⁷⁴ scanning platform. This platform provides the ability to scan a file or URL (Uniform Resource Locator)⁷⁵ with more than 60 anti-malware scanners. Following scanning, 7 of the 62 scanners detected the malware present in the webpage.

⁷⁴ <https://www.virustotal.com/#/home/upload>

⁷⁵ <http://searchnetworking.techtarget.com/definition/URL>

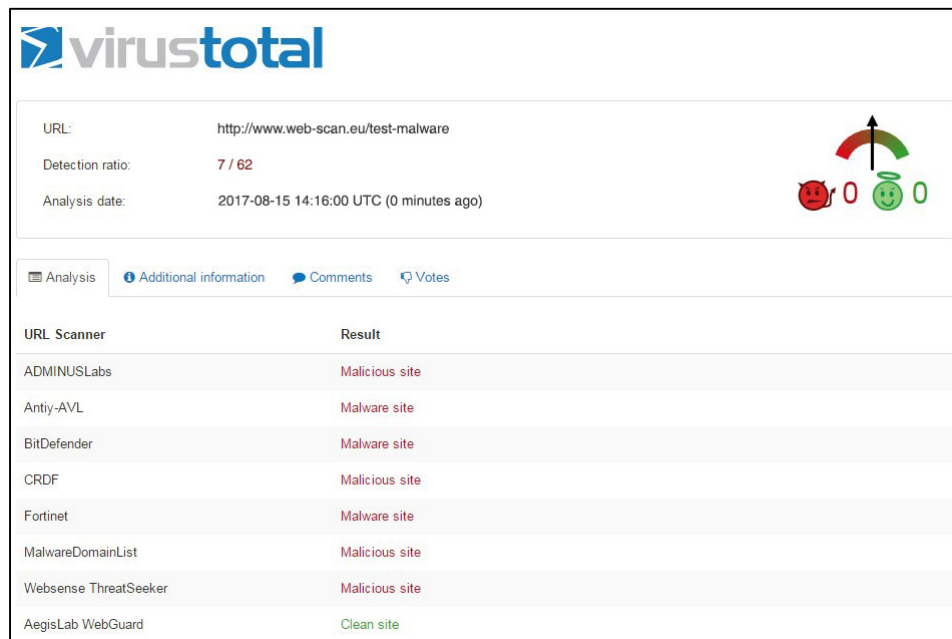


Fig. 12: Scanning an infected webpage with malware

*Virustotal*⁷⁶ offers the best chance to scan an online malware platform because it includes the best anti-malware applications such as *Avira*⁷⁷, *Bitdefender*⁷⁸, *Comodo Site Inspector*⁷⁹, *Esset*⁸⁰, *G-Data*⁸¹, *Kaspersky*⁸², or *Sucuri Site Check*⁸³.

3.3.3. Suspicious activities detection

If a website has been compromised, the cyber-attacker can perform various harmful activities to the users visiting the platform:

- Insertion of hidden iFrames containing malware infections;
- Redirects to other infected websites;

⁷⁶ <https://www.virustotal.com/>

⁷⁷ <https://www.avira.com/>

⁷⁸ <https://www.bitdefender.com/>

⁷⁹ https://app.webinspector.com/#_ga=2.218255002.206330403.1502641994-1636546089.1489848011

⁸⁰ <https://www.eset.com/>

⁸¹ <https://www.gdatasoftware.com/>

⁸² <https://www.kaspersky.com/>

⁸³ <https://sitecheck.sucuri.net/>

- Inserting cookies to monitor the activity of website visitors.

To detect these types of suspicious activities, platforms dedicated to these analyzes can be used, such as the *Sucuri*⁸⁴ platform. The analysis tools made available by *Sucuri* can be used online at the *sucuri.net* site or can be integrated into the websites.

For the *web-scan.eu* website, the tools provided by *Sucuri* have been integrated into the platform.

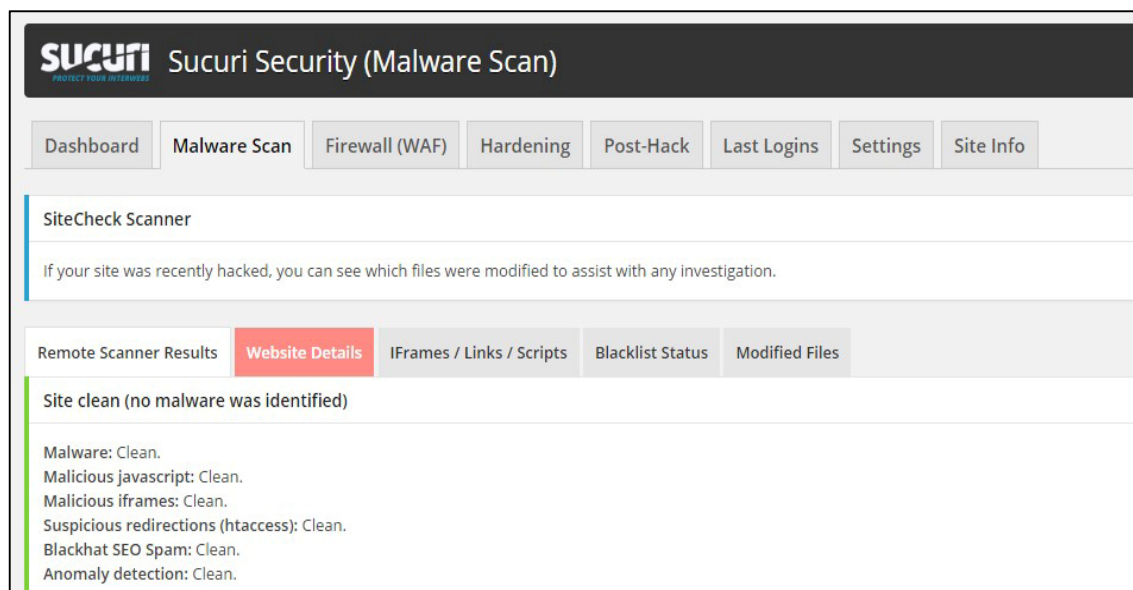


Fig. 13: Scanning a website with tools provided by *Sucuri*

As a result of scanning the website, no script or iFrame containing malware or other platform malfunctions has been detected. From the point of view of suspicious redirects, the *Sucuri* service scans and displays all links, iFrames or scripts that redirect to other websites.

Analysis of links and scripts on the websites can be done with any *Link Extractor*⁸⁵, such as the *Webmaster Toolkit* application. This app extracts all links

⁸⁴ <https://sucuri.net/>

⁸⁵ http://www.webmaster-tools.biz/link_extractor.php

to other websites from the platform and displays them according to the type of link. The website administrator can then see if suspicious redirects are present.

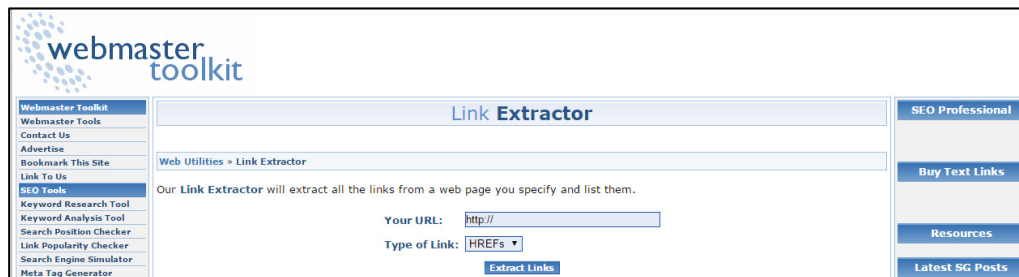


Fig. 14: Link Extractor

Another activity that can be deployed on a compromised platform is to generate spam or phishing email attacks from that domain. This activity can be detected by looking at whether the platform's domain has been marked in spam lists, called blacklists.

One of the applications used to check the domain in spam lists is *blacklistalert.org*⁸⁶, an application that checks for the largest databases with domains listed as compromised and used by attackers to generate spamming and phishing.

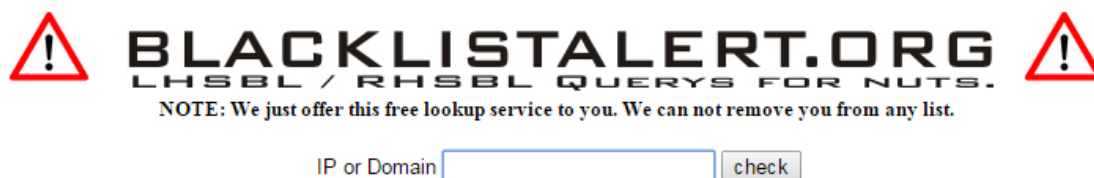


Fig. 15: Verifying the domain in the spam lists

⁸⁶ <http://blacklistalert.org/>

The *Sucuri*⁸⁷ application performs a number of similar analyzes, showing whether the domain was found or reported as compromised.

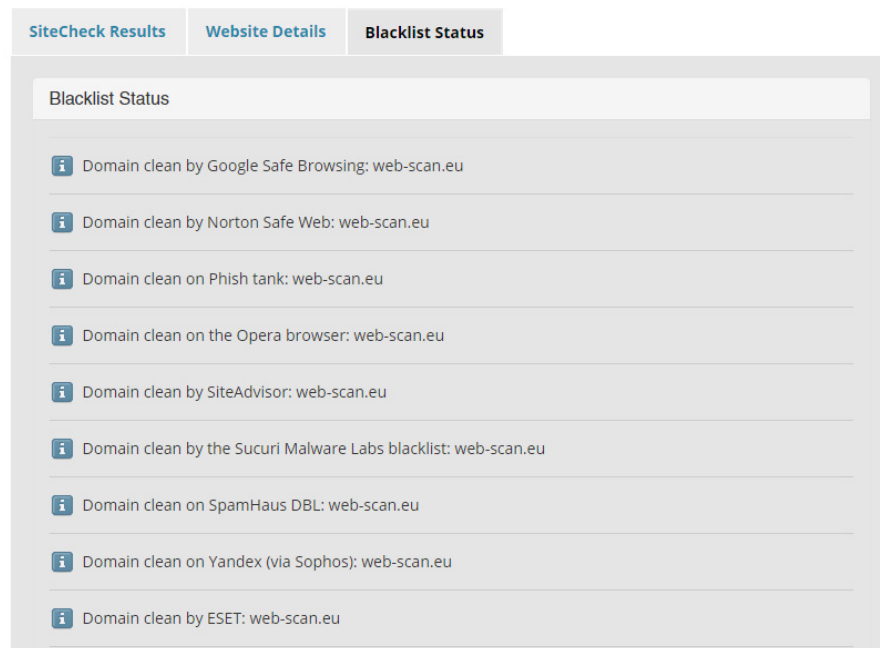


Fig. 16: Verifying the domain in the spam lists with Sucuri app

The cyber-attacker can install various cookies on a compromised website. A cookie⁸⁸ is text sent by a web server to an Internet browser and then retrieved by the browser whenever it accesses that web server. These cookies are used to authenticate or track the behavior of users who visit a site and make specific online orders.

Depending on the duration of cookies, there are:

- *Session cookies*: are deleted after the user closes the Internet browser;
- *Persistent cookies*: stay on user computers for a defined amount of time.

From the point of view of a website, there are several types of cookies:

⁸⁷ <https://sucuri.net/>

⁸⁸ <http://www.whatarecookies.com/>

- *First party cookies or local cookies*: they are set by a website and can be read by that website. This type of local cookies are used to make the website functional, especially for online shops;
- *Third party cookies*: are set by a third party that can be a traffic monitoring or service advertising company. These cookies are reread during the visit to other websites if collaboration links with the first website are completed, such as in some redirects, to see where customers come from;
- *Third party requests cookies*: are cookies that represent requests made to an external service. These requests can transfer information to a third party, such as tracking traffic by Google Analytics⁸⁹.

Cookies can be installed, intercepted, or even modified by cyber-attacker once the website security has been compromised. In order to observe the types of cookies set on a website, it can be used dedicated scanning and analyzing applications, such as the Cookie-Checker⁹⁰ website. This website analyzes and shows what types of cookies are set on a specific website.

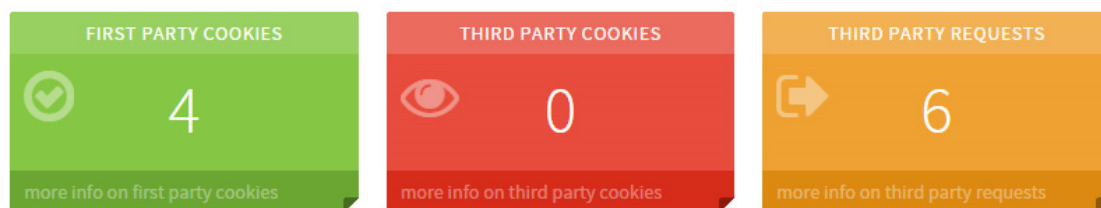


Fig. 17: Cookies from *web-scan.eu* website

By analyzing the cookies set by *web-scan.eu* website, it can be seen that there are 4 local cookies and 6 third-party application cookies, cookies required for *Google Analytics*, *Facebook* or *Twitter* modules.

⁸⁹ <https://analytics.google.com/>

⁹⁰ <http://www.cookie-checker.com>

Another activity to be monitored is the DNS (Domain Name System)⁹¹ setting. DNS is a computer system used to identify websites. This system transforms the name of a website written by a user into an Internet browser into an IP (Internet Protocol) address. Monitoring this system can prevent cyber-attackers to redirect legitimate traffic to an infected website controlled by them.

If a website is subject to a DDoS (Distributed Denial of Service) attack, the effect of the traffic is to load the service, which may interrupt the services provided by the web server, since the online platform cannot be accessed by users. This attack can be monitored through dedicated platforms such as the *Monitis*⁹² platform.

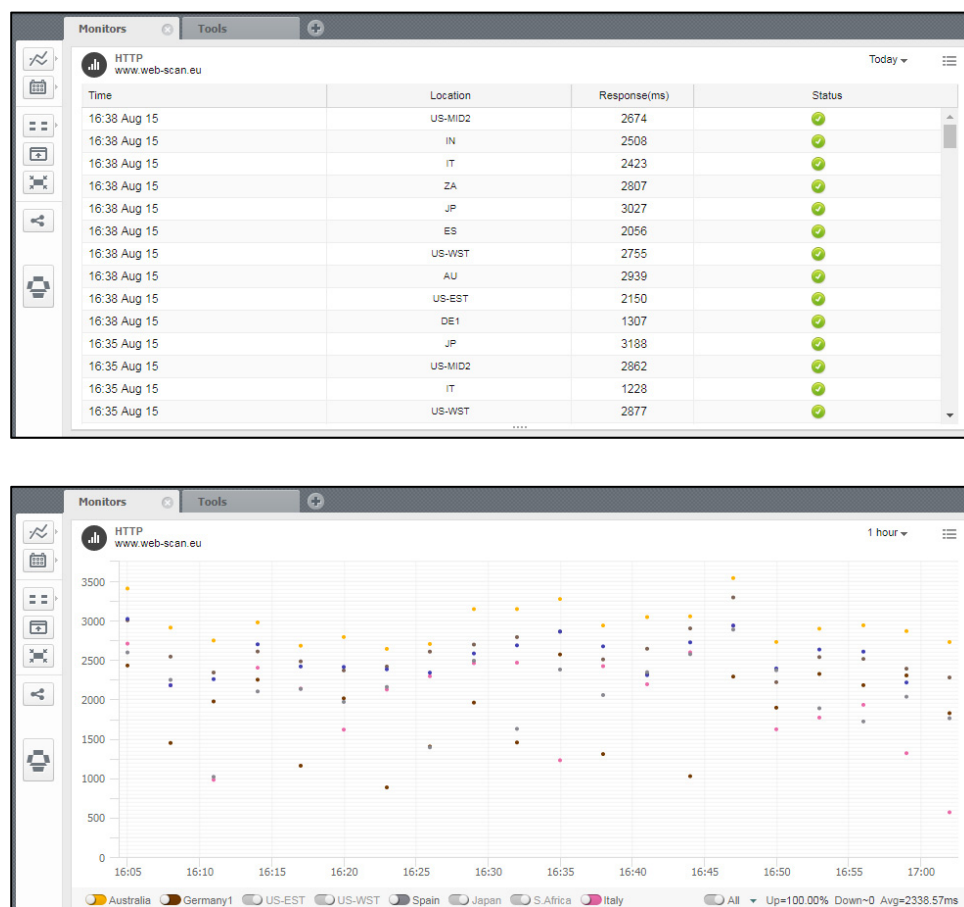


Fig. 18: Monitoring the availability of *web-scan.eu* website

⁹¹ <https://www.lifewire.com/definition-of-domain-name-system-816295>

⁹² <https://www.monitis.com/free-monitoring-sign-up>

All these possible activities can be monitored by integrating and configuring a WAF (Web Application Firewall) ⁹³ to alert the system administrator if an anomaly is detected in the platform activity.

3.4. Methods to alert the platform administrators

In the case of detection of a compromised website, urgent steps must be taken to stop the cyber-attackers from retrieving information from the platform's databases and not to affect the security of the visitors' computer systems.

If the monitoring process of websites security is done automatically, alerts can be sent via email or SMS (Short Message Service)⁹⁴, so website administrators can take quick action to remove the effects of cyber-attacks.

The email address of the website or server administrator can be taken from the contact section of the website, or it can be taken using the *Whois*⁹⁵ query. *Whois* is a response protocol that is used for querying databases that store the assignees of an Internet resource, such as a domain name. For a specific domain it can be used whois-search.com platform to find the email of the registrant company.



Fig. 19: Searching information about a specific domain

⁹³ https://www.owasp.org/index.php/Web_Application_Firewall

⁹⁴ <https://en.wikipedia.org/wiki/SMS>

⁹⁵ <https://whois-search.com/>

If the monitoring process is done manually, it would be advisable for this activity to take place regularly, at short intervals, to detect whether the security of the website has been compromised and to prevent malicious activities to be done by cyber-attackers to website visitors. If the malware infection is not detected shortly, the compromised website may be blacklisted and can be excluded from the search engines.

3.5.Conclusions

The monitoring process of websites is useful to confirm the functionality and effectiveness of implemented security measures. The monitoring process consists in collecting, analyzing and evaluating indicators, and warnings on detecting and responding to security incidents. In the monitoring activity, data analysis involves human factors and incidence assessment is a process of decision-making by websites administrators.

In this chapter I developed an attack tree with the root node representing the compromising of the website security. The attack tree⁹⁶ is a systematic method that characterizes the security of a website based on various types of cyber-attacks. An attack tree consists of a root node and multiple nodes located on multiple depth levels. The way in which a cyber-attacker can compromise a website is iteratively represented by lower-level nodes.

The attack tree developed in this chapter enumerates methods by which an attacker can cause a security incident to a website. This tree is useful for exploring some in-depth troubleshooting and for generating intrusion scenarios. The branches of the tree follow the steps of the *Cyber Kill Chain* intrusion model.

By studying the specialized references published by OWASP (Open Web Application Security Project), I analyzed the most frequently 10 vulnerabilities⁹⁷

⁹⁶ https://www.schneier.com/academic/archives/1999/12/attack_trees.html

⁹⁷ https://www.owasp.org/index.php/Top_10_2017-Top_10

of the websites, to understand how a cyber-attacker can exploit the websites vulnerabilities.

Using the attack tree and taking into account the vulnerabilities of the websites, I simulated attacks on the *web-scan.eu* website to analyze their impact on online platforms. Through repeated experiments and analysis, I studied the impact of cyber-attacks, both simulated by the attack tree and real by cyber-attacks recorded on *web-scan.eu* website in the cyberspace.

I identified possible activities taken by a cyber-attacker to a website by using experiments and case studies: inserting scripts used to involve the website in other cyber-attacks, inserting malware, inserting hidden iFrames containing malware, redirects to other infected websites, using the website in phishing attacks, sending spam emails, and inserting monitoring cookies.

In this chapter, I have developed strategies for monitoring the websites security on three action lines: detection of intrusions, malware infections and suspicious activities. The cyber-attackers can use the compromised website to perform illegal activities, like generating spamming and phishing messages, injecting malicious scripts or monitoring cookies for website visitors.

In the case of detection of a compromised website, urgent steps must be taken to stop the cyber-attackers. I analyzed some possibilities to alert the administrators of the compromised websites.

CHAPTER IV

DEVELOPING THE RESEARCH WEBSITE

4.1. The website aims and objectives

In this research I designed and developed a website, hosted on the domain *web-scan.eu*, in order to promote the results of the scientific research.

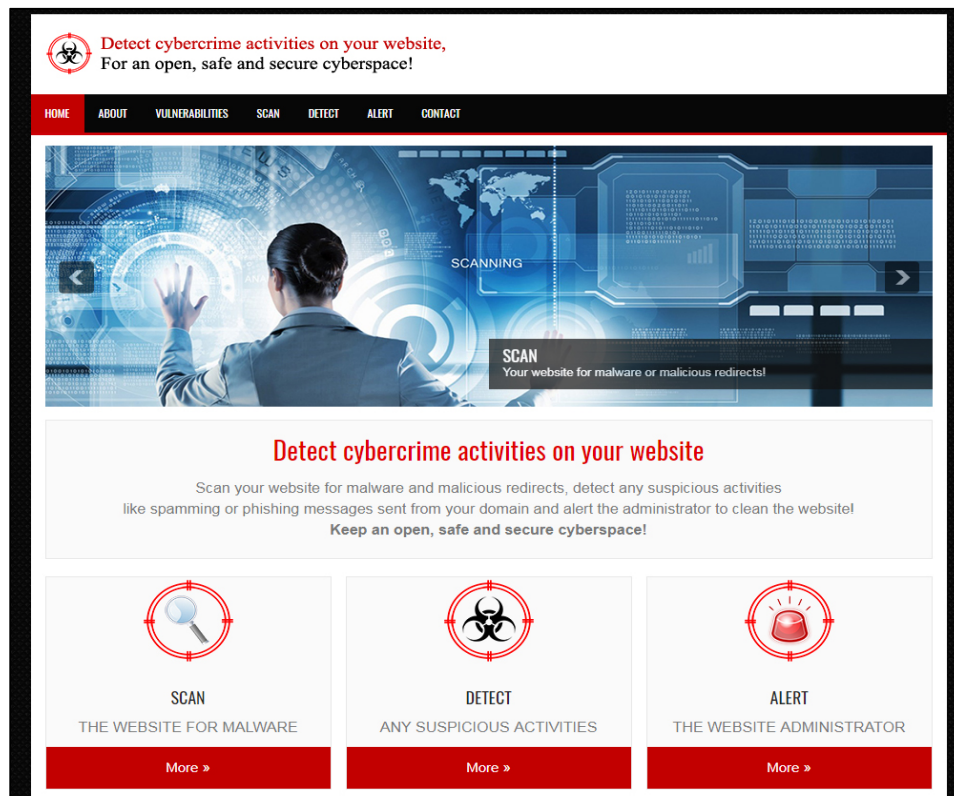


Fig. 20: The research website hosted at *web-scan.eu* domain

The objectives of the website are:

- Warning the public about the main threats and risks to websites security;

- Presenting the latest websites vulnerabilities discovered;
- Raising the level of education of the public in the field of cybersecurity;
- Promoting methods to investigate the cybercrime activities in cyberspace;
- Improving cooperation between the public, private and academic environment, by sharing experience and information to improve the level of websites security;
- Helping the community to ensure an open, safe and secure cyberspace.

4.2.The website structure

The research website was hosted on *web-scan.eu* domain, on a server with the following specifications:

- Operating system: Linux;
- Web server: Apache - version 2.4.x;
- PHP - version 5.3.x, MySQL - version 5.5.x;
- Hosting space: 500 MB;
- SSD server in RAID – 10 hardware array;
- Memory allocated: 1 GB.

I have structured this website in several categories to present information about:

- Home webpage;
- Information about the website aim and objectives;
- Websites vulnerabilities;
- Scan the website;
- Detect the suspicious activities on website;
- Alert the website administrator;
- Contact details.

4.3. Integration of the monitoring procedures into an app

Some of the procedures of monitoring the website security can be achieved by integrating a WAF (Web Application Firewall) into the platform. But this solution is pretty expensive and difficult to integrate with the website scripts. A solution to this issue would be to integrate these monitoring procedures into an IT application.

I developed an application in PHP language to record all the information gained from analyzing website security. The application uses a MySQL database.

The application database consists of 10 tables: *categories*, *features*, *settings*, *sites*, *sites_features*, *sites_status*, *users*, *users_permissions*, *users_roles*, and *users_roles_tables*.

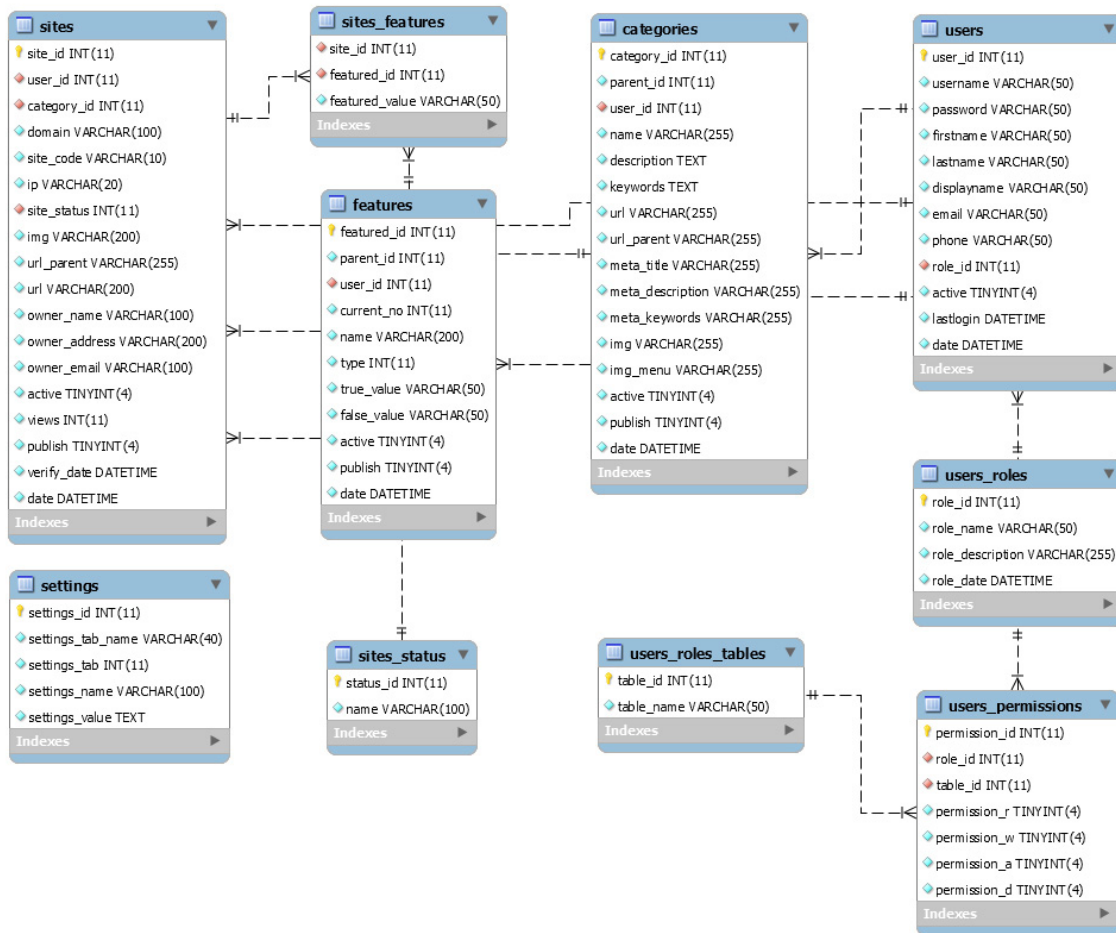


Fig. 21: The conceptual structure of the application database

Table	Action	Rows	Type	Collation	Size	Overhead
<input type="checkbox"/> categories	Browse Structure Search Insert Empty Drop	~4	InnoDB	utf8_general_ci	112 KiB	-
<input type="checkbox"/> features	Browse Structure Search Insert Empty Drop	~36	InnoDB	utf8_general_ci	16 KiB	-
<input type="checkbox"/> settings	Browse Structure Search Insert Empty Drop	~8	InnoDB	utf8_general_ci	16 KiB	-
<input type="checkbox"/> sites	Browse Structure Search Insert Empty Drop	~8	InnoDB	utf8_general_ci	16 KiB	-
<input type="checkbox"/> sites_features	Browse Structure Search Insert Empty Drop	~256	InnoDB	utf8_general_ci	16 KiB	-
<input type="checkbox"/> sites_status	Browse Structure Search Insert Empty Drop	~2	InnoDB	utf8_general_ci	16 KiB	-
<input type="checkbox"/> users	Browse Structure Search Insert Empty Drop	~2	InnoDB	utf8_general_ci	32 KiB	-
<input type="checkbox"/> users_permissions	Browse Structure Search Insert Empty Drop	~30	InnoDB	utf8_general_ci	48 KiB	-
<input type="checkbox"/> users_roles	Browse Structure Search Insert Empty Drop	~3	InnoDB	utf8_general_ci	16 KiB	-
<input type="checkbox"/> users_roles_tables	Browse Structure Search Insert Empty Drop	~10	InnoDB	utf8_general_ci	16 KiB	-
10 tables	Sum	359	InnoDB	latin1_swedish_ci	304 KiB	0 B

Fig. 22: The structure of the application database

Users who can access the application are declared in the users table. To each user is given a certain role and, depending on the permissions set on the roll, can access certain modules in the application.

#	Name	Type	Collation	Attributes	Null	Default	Extra
<input type="checkbox"/> 1	user_id	int(11)			No	None	AUTO_INCREMENT
<input type="checkbox"/> 2	username	varchar(50)	utf8_general_ci		No	None	
<input type="checkbox"/> 3	password	varchar(50)	utf8_general_ci		No	None	
<input type="checkbox"/> 4	firstname	varchar(50)	utf8_general_ci		No	None	
<input type="checkbox"/> 5	lastname	varchar(50)	utf8_general_ci		No	None	
<input type="checkbox"/> 6	displayname	varchar(50)	utf8_general_ci		No	None	
<input type="checkbox"/> 7	email	varchar(50)	utf8_general_ci		No	None	
<input type="checkbox"/> 8	phone	varchar(50)	utf8_general_ci		No	None	
<input type="checkbox"/> 9	role_id	int(11)			No	None	
<input type="checkbox"/> 10	active	tinyint(4)			No	1	
<input type="checkbox"/> 11	lastlogin	datetime			No	None	
<input type="checkbox"/> 12	date	datetime			No	None	

Fig. 23: Structure of the *users* table in the database

In close connection with the *users* table, there are several tables: *users_roles*, *users_permissions*, and *users_roles_tables*. These rows store the roles and permissions each user has in the app.

The monitored websites are stored in the *sites* table.

#	Name	Type	Collation	Attributes	Null	Default	Extra
<input type="checkbox"/> 1	site_id	int(11)			No	None	AUTO_INCREMENT
<input type="checkbox"/> 2	user_id	int(11)			No	None	
<input type="checkbox"/> 3	category_id	int(11)			No	None	
<input type="checkbox"/> 4	domain	varchar(100)	utf8_general_ci		No	None	
<input type="checkbox"/> 5	site_code	varchar(10)	utf8_general_ci		No	None	
<input type="checkbox"/> 6	ip	varchar(20)	utf8_general_ci		No	None	
<input type="checkbox"/> 7	site_status	int(11)			No	None	
<input type="checkbox"/> 8	img	varchar(200)	utf8_general_ci		No	None	
<input type="checkbox"/> 9	url_parent	varchar(255)	utf8_general_ci		No	None	
<input type="checkbox"/> 10	url	varchar(200)	utf8_general_ci		No	None	
<input type="checkbox"/> 11	owner_name	varchar(100)	utf8_general_ci		No	None	
<input type="checkbox"/> 12	owner_address	varchar(200)	utf8_general_ci		No	None	
<input type="checkbox"/> 13	owner_email	varchar(100)	utf8_general_ci		No	None	
<input type="checkbox"/> 14	verify_date	datetime			No	None	
<input type="checkbox"/> 15	date	datetime			No	None	

Fig. 24: Structure of the *sites* table in the database

Checking a website is based on several criteria: security report, malware scan, cookie scan, and spam listing. These criteria are stored in the *featured* table. Depending on these criteria, the website may receive a certain status: *clean website* or *infected website*.

When a new website has to be verified, more domain-related information needs to be added: the IP address, the category to which it belongs, the name, address, and contact details of the holder.

Websites are added and listed by category for better records and management. When introducing a new website, all platform security testing criteria and results are added.

The screenshot shows the 'ADMIN' interface with a sidebar menu on the left containing links to Dashboard, Sites, Features, Categories, Posts, Pages, Galleries, Settings, Users, and Roles. The main content area is titled 'Add New Site' and features a tabbed interface. The 'General Info' tab is selected, displaying the following fields: 'Site Status' (dropdown menu set to 'Clean website'), 'Domain' (text input 'www.web-scan.eu'), 'IP Address' (text input '128.140.230.164'), 'Category' (dropdown menu set to 'Presentation website'), 'Owner Name' (text input 'Ioan-Cosmin MIHAI'), 'Owner Address' (text input 'Bucharest'), 'Owner Email' (text input field with a blacked-out email address), 'Upload Image' (button 'No file selected' and 'Choose File'), and 'Date' (calendar icon, date '16-08-2017', and time '08:50'). At the bottom of the form are three buttons: 'Save & Publish Site' (green), 'Save Site' (blue), and 'Cancel' (grey).

Fig. 25: Adding a new website in the database

In the process of adding a new website in the database, there are 5 tabs that have to be completed: *General Info*, *Security Report*, *Malware Scan*, *Cookies Scan*, and *Spam Listing*. The *General info* window contains the following fields: website domain, IP address, website category, website owner, address, e-mail, website image, and date. Most of this data can be retrieved using *Whois*⁹⁸ query, described in chapter 3.4.

The *Security Report* contains information about the result of on-line scanning: malware infections, suspicious redirects, monitoring cookies, etc.

⁹⁸ <https://whois-search.com/>

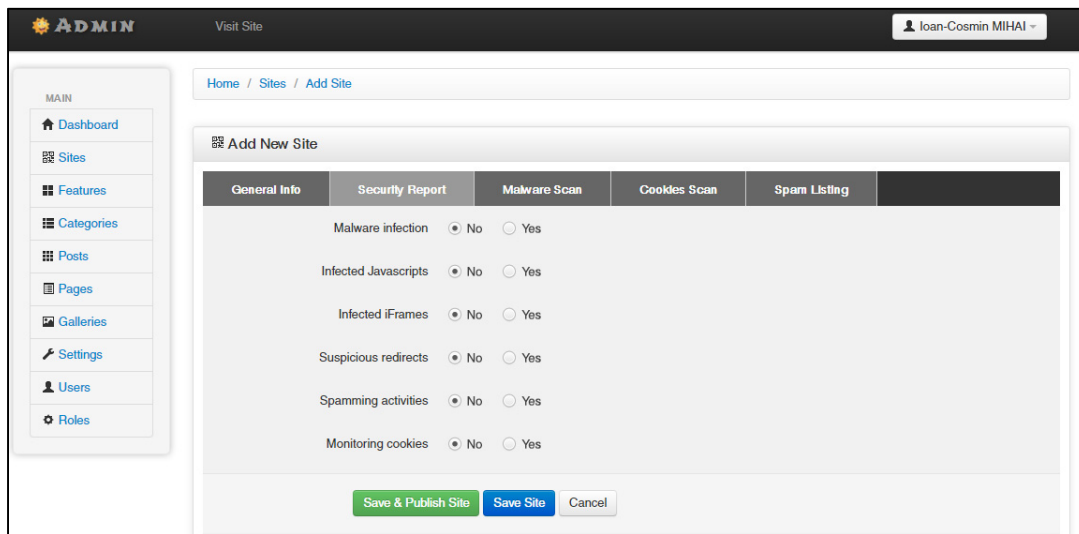


Fig. 26: The *Security Report* tab

The *Malware Scan* tab shows the results from the major anti-malware applications: Avira⁹⁹, Bitdefender¹⁰⁰, Comodo¹⁰¹, Esset¹⁰², etc.

The *Cookies Scan* tab shows the type and number of cookies¹⁰³ detected on websites.

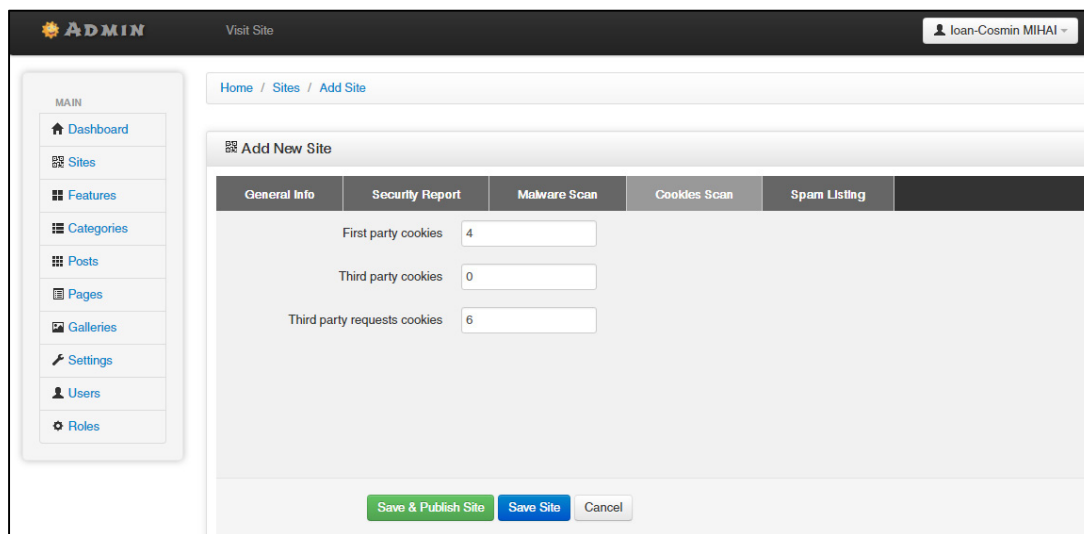


Fig. 27: The *Cookie Scan* tab

⁹⁹ <https://www.avira.com/>

¹⁰⁰ <https://www.bitdefender.com/>

¹⁰¹ <https://www.comodo.com/>

¹⁰² <https://www.eset.com/>

¹⁰³ <http://www.onlinecookieaudit.com/>

The last tab *Spam List* displays whether the domain has been found or reported to be compromised on the main spam lists: *Esset*, *Google Self Browsing*, *McAfee Site Advisor*, *Norton Safe Wale*, *Malware Juices*, etc.

4.4.Conclusions

In this research I designed and developed a website, hosted on the domain *web-scan.eu*, in order to promote the results of the scientific research.

The objectives of the website are:

- Warning the public about the main threats and risks to websites security;
- Presenting the latest websites vulnerabilities discovered;
- Raising the level of education of the public in securing the websites;
- Promoting methods to investigate the cybercrime activities;
- Improving cooperation between the public, private and academic environment, by sharing experience and information to improve the level of websites security.
- Helping the community to ensure an open, safe and secure cyberspace.

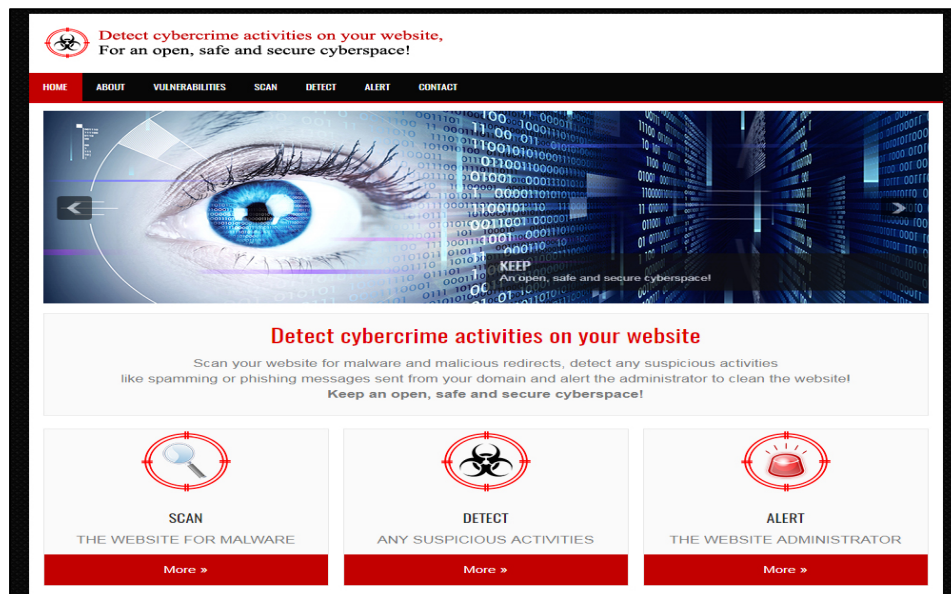


Fig. 28: The research website hosted at *web-scan.eu* domain

I developed an application in PHP language to record all the information gained from analyzing website security. The application uses a MySQL database. The application database consists of 10 tables: *categories*, *features*, *settings*, *sites*, *sites_features*, *sites_status*, *users*, *users_permissions*, *users_roles*, and *users_roles_tables*.

When a new website has to be verified, more domain-related information needs to be added: the IP address, the category to which it belongs, the name, address, and contact details of the holder. Most of this data can be retrieved using *Whois* query.

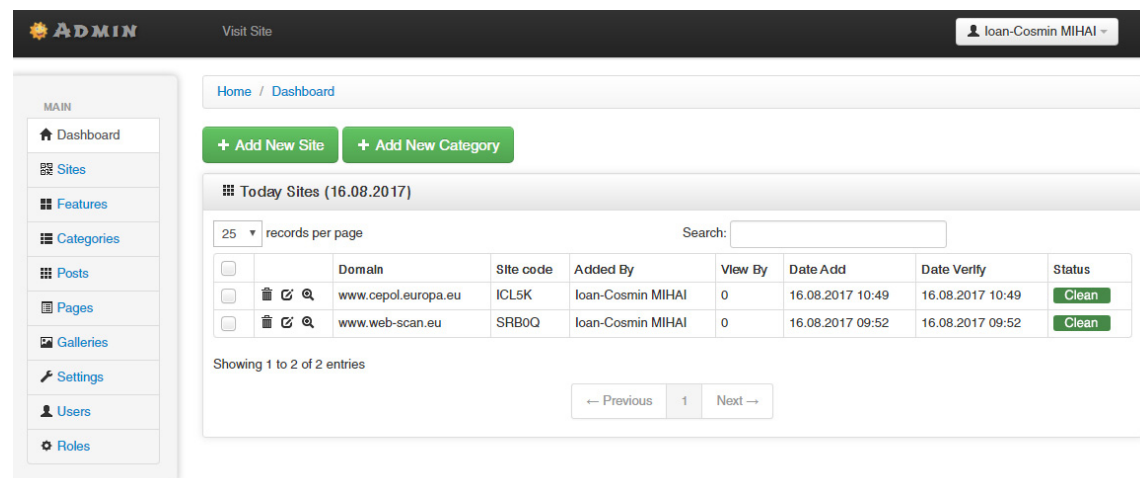


Fig. 29: The application developed for recording websites scanned

Websites scanned are added and listed by category for better records and management in the database. When introducing a new website, all platform security testing criteria and results are added. In the process of adding a new website in the database, there are 5 tabs that have to be completed: *General Info*, *Security Report*, *Malware Scan*, *Cookies Scan*, and *Spam Listing*.

CHAPTER V

CONCLUSIONS

5.1. The main issues presented in the research

In this research, I analyzed the evolution of cyber-attacks, from attacks created for fun in the 1980s, till the creation of complex attacks used for industrial espionage.

I made a classification of cyber-attacks according to the target of cybercriminals (opportunistic, intermediate and complex attacks) and to the access to cyber infrastructures (attacks by access to users, components, and applications).

I analyzed the structure of cyber-attacks using the *Cyber Kill Chain* intrusion model, defined by Lockheed Martin researchers, which involves 7 steps: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objective. The intrusion model is a new way of analysis used by cybersecurity analysts to understand what information is available to perform defensive actions.

I studied the most important cyber-attacks: malware: computer viruses, trojans, worms, adware, spyware, ransomware, rogueware, and scareware, Denial of Service attacks, email and web based attacks.

I presented the attack vectors, which represent the methods used by cyber attackers to accomplish the purpose of an attack. The *Cyber Kill Chain* intrusion model is correlated with the attack vector, and characterizes different phases of a cyber-attack.

To ensure a better cybersecurity on web servers, I developed a guideline to prevent cyber-attacks and limit their effects.

I developed an attack tree whose root node represents the compromised security of a website. The attack tree is a systematic process that characterizes the security of a computer system based on various types of cyber-attacks. The attack tree presents methods by which a cyber-attacker can cause a security incident on a website. This tree is useful for generating intrusion scenarios to a website.

I investigated the main vulnerabilities of the online platforms using OWASP (Open Web Application Security Project) research for analyzing the impact of cyber-attacks on websites.

Using the attack tree and taking into account the vulnerabilities of the websites, I simulated attacks on the research website hosted on *web-scan.eu* for analyzing their impact on websites. Through repeated experiments and participatory analysis, I studied the impact of cyber-attacks on a website.

I identified the possible activities of an attacker on a website: inserting malicious scripts to involve the platform in other cyber-attacks, inserting malware, inserting hidden iFrames containing malware, redirects to other infected websites, the use of the website in phishing or spamming attacks, and insertion of monitoring cookies.

I developed and tested the monitor process of websites security on three lines of action: intrusion detection, malware infections and suspicious activities.

I designed and developed a website hosted on *web-scan.eu*, in order to promote the results of the scientific research and to test the procedures of monitoring the websites security.

I developed an application to record all of the information gained from analyzing the websites security. For each platform added to the database, a security report is generated that contains information about the result of websites scanning: malware infections, suspicious redirects, monitoring cookies.

5.2. Original contributions to the research

1. I made a classification of cyber-attacks according to the objective of cybercriminals and the access to cyber infrastructures.

2. I developed a guide to preventing cyber-attacks and limiting their effects on computer systems.

3. I developed an attack tree whose root node represents the compromised security of a website. The attack tree presents methods by which a cyber-attacker can generate security incidents on a website.

4. I studied the impact of cyber-attacks on the research website hosted on *web-scan.eu*.

5. I identified the possible activities of cybercriminals on websites: inserting malicious scripts to involve the platform in other cyber-attacks, inserting malware, inserting hidden iFrames containing malware, redirects to other infected sites, using the platform in phishing and spamming attacks, insertion of monitoring cookies.

6. I developed and tested the strategies of monitoring the websites security on three lines of action: detection of intrusions, malware infections and suspicious activities.

7. I designed and developed a website hosted on *web-scan.eu* domain. The purpose of the platform is to promote the results of scientific research.

8. I developed an application to record all the information obtained from the websites security analysis.

5.3. Methods of data collection and analysis

The research methodology consisted of qualitative research (specialized bibliography, case studies, participatory observation, interviews with specialists) and quantitative research (experiments and surveys).

During this research, I visited professional associations and institutions to analyze different study cases in the field of website security and I made a lot of

experiments, to observe the impact of cyber-attacks on websites. I could also observe the impact of real cyber-attacks targeted to the *web-scan.eu* website, developed in this research.

On March 23, 2017, I organized the workshop “*Challenges and Opportunities in Cyberspace*”, at *The Romanian Centre of Excellence for Cybercrime* from “Alexandru Ioan Cuza” Police Academy.



Fig. 30: The workshop “Challenges and Opportunities in Cyberspace”

This workshop goal was exchanging ideas, expressing opinions and communicating the latest research results in the field of cybersecurity and cybercrime, to establish strategies for information and infrastructures protection and to identify concrete, effective and pro-active measures to combat cybercrime. One of the subjects discussed on this workshop was procedures for detecting cybercrime activities on websites. The workshop “Challenges and Opportunities in Cyberspace” represented a very good source of information necessary for this research.

The most important interviews with experts from the field of cybersecurity, taken for this research, have been published in IJISC – International Journal of Information Security and Cybercrime (ISSN: 2285-9225, DOI: 10.19107/IJISC), a scientific journal indexed in many international databases.

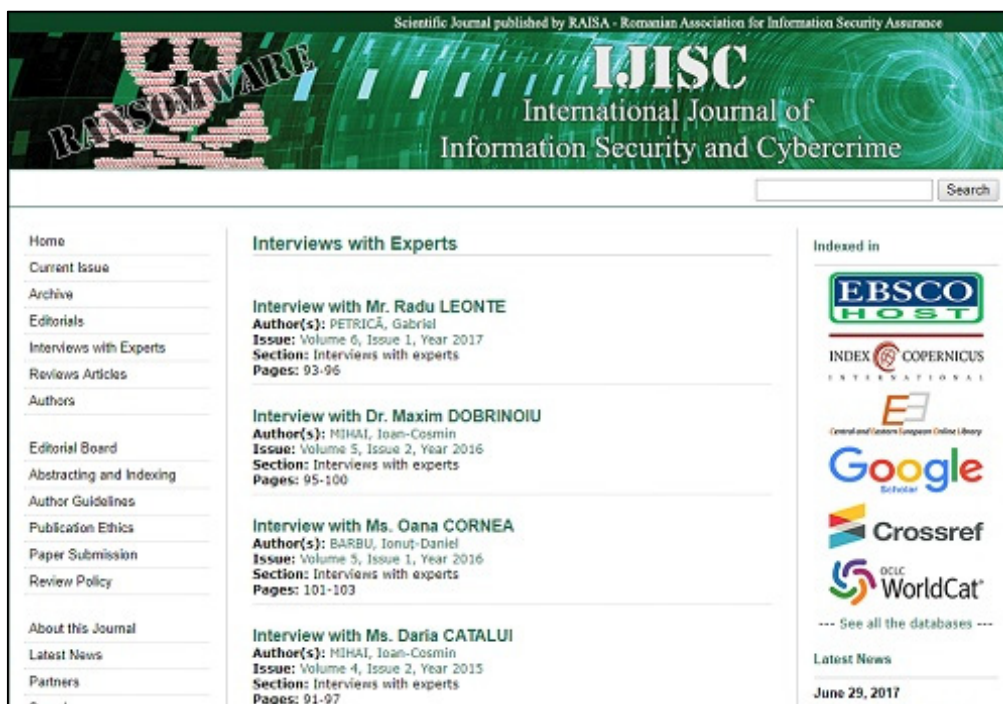


Fig. 31: Interviews with experts on cybersecurity and cybercrime published in IJISC – International Journal of Information Security and Cybercrime

The surveys conducted for this research were posted on two websites on cybersecurity (www.securitatea-informatiilor.ro and www.securitatea-cibernetica.ro), developed by RAISA – Romanian Association for Information Security Assurance.

5.4. Perspectives for further development

A development perspective is to improve the development of the web-scan.eu website, which is useful for promoting awareness campaigns about the

threats and risks present in cyberspace, guides and solutions for websites security. With the help of the information and guidelines posted on this website, the level of knowledge of the public in the field of cybersecurity can be raised.

This website can contribute to the development of cooperation between the public, private and academic environments through the exchange of experience and information to improve the level of security in cyberspace.

The second development perspective is to develop an automated process of monitoring the websites security. The application developed to record all of the information about the websites security could be developed so that websites can be monitored automatically at regular intervals of time.

The activities of cyber-attacker on websites, such as the insertion of malicious scripts to involve the platform in other cyber-attacks, the insertion of malware, the insertion of hidden iFrames containing malware infections, redirects to other infected sites, using of the platform in phishing and spamming attacks, or the insertion of monitoring cookies can be automatically monitored. I used in this research different platforms to detect these activities manually. Most of the platforms available offer APIs (Application Programming Interface) – interfaces to integrate them into other applications, for the automatic use of these services.

Integrating these services into the application could lead to automated monitoring of websites security. The name of the domain can be inserted into the application, and the security checks and report will be generated automatically. The application might also be set to automatically repeat these checks for a certain amount of time for a more effective monitoring of the website security.

Automating the websites scanning process would lead to a rapid detection of cyber-attack problems, and measures can be taken quickly to remove their effects from the verified websites. The application could be launched on a dedicated website, and could significantly contribute to a safer cyberspace.

REFERENCES

Books, publications, research papers

1. Cowan, C., Wagle, P., Pu, C., Beattie, S., and Walpole, J., Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade, DARPA Information Survivability Conference and Expo (DISCEX), 2000.
2. Gorman, S. and Barnes, J., Cyber Combat: Act of War, 2011.
3. Hutchins, M.E., Clopperty, M.J., and Amin, R.M., Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, 2011.
4. Majority Staff Report, A Kill Chain Analysis of the 2013 Target Data Breach, 2014.
5. Mihai, I.C., Information Security. Second Edition, Revised and Expanded, Ed. Sitech, 2014.
6. Preimesberger, C., DDoS Attack Volume Escalates as New Methods Emerge, eWeek, 2014.
7. Ramzan, Z., Phishing attacks and countermeasures, In Stamp, Peter. Handbook of Information and Communication Security, Springer, 2010.
8. Schneier, B., Attack Trees: Modeling Security Threats, Dr. Dobb's Journal, 2003.
9. Tidwell, T., Larson, R., Fitch, K., and Hale, J., Modeling Internet Attacks, 2001.

Internet resources

1. <http://blacklistalert.org/>
2. <http://cybercrime.org.za/website-defacement>
3. <http://info.ssl.com/article.aspx?id=10241>
4. <http://php.net/manual/en/ref.filter.php>
5. <http://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/#gref>
6. <http://searchnetworking.techtarget.com/definition/URL>
7. <http://securitatea-cibernetica.ro/wp-content/uploads/2014/12/StrategiaDeSecuritateCiberneticaARomaniei.pdf>
8. <http://whatis.techtarget.com/definition/framework>
9. http://www.cert-ro.eu/files/doc/915_20150325000331012990800_X.pdf
10. <http://criminalitatea-informatica.ro>
11. <http://www.cookie-checker.com>
12. http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf
13. http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
14. <http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html>
15. <http://www.onlinecookieaudit.com/>
16. <http://www.raisa.org/>
17. <http://www.securitatea-cibernetica.ro>
18. <http://www.securitatea-informatiilor.ro>
19. <http://www.securitatea-informatiilor.ro/tipuri-de-atacuri-informatic/analiza-virusilor-informatici/>
20. <http://www.securitatea-informatiilor.ro/tipuri-de-atacuri-informatic/analiza-cailor-troieni/>

21. <http://www.strategii21.ro/index.php/en/conferences-strategies-xxi/the-joint-operations-strategic-studies-and-security-department-conference>
22. <http://www.thewindowsclub.com/email-bombing>
23. http://www.webmaster-tools.biz/link_extractor.php
24. <http://www.whatarecookies.com/>
25. <http://yeehee.com/tools/bruteforcecalc/index.php>
26. <https://analytics.google.com/>
27. https://app.webinspector.com/#_ga=2.218255002.206330403.1502641994-1636546089.1489848011
28. <https://blog.malwarebytes.com/cybercrime/2016/06/email-spoofing/>
29. <https://en.wikipedia.org/wiki/SMS>
30. <https://heimdalsecurity.com/blog/how-drive-by-download-attacks-work/>
31. <https://kb.iu.edu/d/arsf>
32. https://link.springer.com/chapter/10.1007/978-3-642-31869-6_40
33. [https://msdn.microsoft.com/en-us/library/aa367008\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa367008(v=vs.85).aspx)
34. <https://runbox.com/email-school/what-is-spam-and-how-to-avoid-it/>
35. <https://security.radware.com/ddos-knowledge-center/ddospedia/fraggle-attack/>
36. <https://security.radware.com/ddos-threats-attacks/cyber-ransom-spring-2017/>
37. <https://sitecheck.sucuri.net/>
38. <https://sucuri.net/>
39. <https://techterms.com/definition/api>
40. <https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html>
41. <https://usa.kaspersky.com/resource-center/threats/adware>
42. <https://whois-search.com/>
43. <https://www.avast.com/c-spyware>
44. <https://www.avira.com/>

45. <https://www.bitdefender.com/>
46. <https://www.cert.ro/>
47. <https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-34/syn-flooding-attacks.html>
48. <https://www.comodo.com/>
49. <https://www.cs.hmc.edu/~geoff/classes/hmc.cs070.200101/homework10/hashfuncs.html>
50. <https://www.darkreading.com/attacks-breaches/leveraging-the-kill-chain-for-awesome/a/d-id/1317810>
51. <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf>
52. <https://www.eset.com/>
53. <https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html>
54. <https://www.gdatasoftware.com/>
55. <https://www.ijisc.com/>
56. <https://www.kaspersky.com/>
57. <https://www.lifewire.com/definition-of-domain-name-system-816295>
58. <https://www.lifewire.com/how-computer-worms-work-816582>
59. <https://www.microsoft.com/en-us/wdsi/threats/ransomware>
60. <https://www.monitis.com/free-monitoring-sign-up>
61. https://www.owasp.org/index.php/Top_10_2017-A10-Underprotected_APIs
62. https://www.owasp.org/index.php/Top_10_2017-A1-Injection
63. https://www.owasp.org/index.php/Top_10_2017-A2-Broken_Authentication_and_Session_Management
64. [https://www.owasp.org/index.php/Top_10_2017-A3-Cross-Site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Top_10_2017-A3-Cross-Site_Scripting_(XSS))

- 65.https://www.owasp.org/index.php/Top_10_2017-A4-Broken_Access_Control
- 66.https://www.owasp.org/index.php/Top_10_2017-A5-Security_Misconfiguration
- 67.https://www.owasp.org/index.php/Top_10_2017-A6-Sensitive_Data_Exposure
- 68.https://www.owasp.org/index.php/Top_10_2017-A7-Insufficient_Attack_Protection
- 69.[https://www.owasp.org/index.php/Top_10_2017-A8-Cross-Site_Request_Forgery_\(CSRF\)](https://www.owasp.org/index.php/Top_10_2017-A8-Cross-Site_Request_Forgery_(CSRF))
- 70.https://www.owasp.org/index.php/Top_10_2017-A9-Using_Components_with_Known_Vulnerabilities
- 71.https://www.owasp.org/index.php/Top_10_2017-Top_10
- 72.https://www.owasp.org/index.php/Web_Application_Firewall
- 73.<https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids>
- 74.<https://www.quttera.com/>
- 75.https://www.schneier.com/academic/archives/1999/12/attack_trees.html
- 76.<https://www.siteguarding.com/>
- 77.<https://www.slideshare.net/sharifulr/secure-hash-algorithm-sha512>
- 78.<https://www.symantec.com/content/dam/symantec/docs/infographics/istr-zero-day-en.pdf>
- 79.https://www.symantec.com/content/en/us/about/media/pdfs/bistr_18_watering_hole_edits.en-us.pdf
- 80.<https://www.techopedia.com/definition/1245/structured-query-language-sql>
- 81.<https://www.techopedia.com/definition/17294/smurf-attack>

- 82.<https://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro>
- 83.<https://www.trendmicro.com/vinfo/us/security/definition/targeted-attacks>
- 84.<https://www.us-cert.gov/ncas/tips/ST04-015>
- 85.<https://www.virustotal.com/>
- 86.<https://www.w3.org/TR/xpath/>
- 87.<https://www.webinspector.com/>
- 88.<https://www.whitehatsec.com/>