International Journal of Engineering Sciences 2021 14(2) 56-63

INTERNATIONAL JOURNAL
OF
ENGINEERING SCIENCES

Comparative study of cyber-attacks focused on digital websites

Francisco Manuel Hilario Falcón, José Ogosi, Jorge Mayhuasca, Ciro Rodriguez*, Pervis Paredes
Universidad Nacional Federico Villarreal, Lima, Perú

(Received 23 May 2021; Accepted 25 July 2021)

DOI: https://doi.org/10.36224/ijes.140203

Abstract
The level of cyber-attacks that violate the devices and web platforms are tools of risk and damage that focus on subtracting private and restricted information of users without administrative permissions, that is why the proposal in this research is to raise cyber-attacks where operations are performed on a massive scale and through fraudulent techniques and strategies, under the tools of: (a) Nmap, (b) SQL Injection, (c) Fiddler, (d) Burp Suite performing a comparison study of these tools in order to be able to demonstrate how they are effective against web platforms and how the web administrator or technician should take the necessary care against these cyber-attacks. In summary, the Nmap and Injection SQL tools are contemplated to have free access for its variety of operating systems under the tool platform allowing to analyze the security of the system for sending packets to different devices. In addition, the Fiddler and Burp Suite tools have a paid license access due to the differences in their product costs. Finally, as a recommendation we can say that the study can be improved by implementing more selection criteria and adding more tools to expand the topic with classifications by type of structure.

Keywords: Cyber-attacks, Nmap, SQL Injection, Fiddler, Burp Suite.

1. Introduction

The largest network in the world called internet is the technology that provides the connection of different users in the world in a shared, private, mixed or hybrid network of different technologies or digital platforms (Chang, 2020; Sánchez, Mendoza and Garzón, 2020). This technology allows all users, entities and organizations to perform different processes to assist in work and daily activities: development of web platforms, communication through digital sites, connections from different parts of the world to communicate through networks (Sánchez, Mendoza and Garzón, 2020; Chang, 2020). All this makes technology advance by leaps and bounds, causing cybercriminals to seek new ways to circumvent security and affect different aspects of the platform or organization (Chang, 2020; Mondragón et al., 2017).

Websites or digital platforms are information platforms to be transmitted to a reference point or transmit data hosted on a main server that keeps the page online connection (Parrales et al., 2021). Therefore, cybercriminals perform malicious actions in order to alter or modify the server data or destruction of the website in order to access the resources of the platform in order to affect people in specific entities to eliminate, publish information and this generates uncertainty in users to perform activities on web platforms for fear of not having integrity and security (Chinguel et al., 2019). In addition, web platforms are always compromised with different technical risks, among the most main we have: SQL injections and extractions of data, user authentication or access patterns, login organization, sequence of different access modes by command in crossed web platforms, direct accesses to objects, risks of accesses through URLs, falsifying user accesses, poorly developed configurations and problems in the security of target protocols (Mondragón et al., 2017; Parrales et

*Corresponding author
Email address:crodriguez@unfv.edu.pe(Ciro Rodriguez)
ISSN 0976 – 6693.

al., 2021; Nope 2016).

The different attacks by cyberspace focused on digital sites are aimed at devaluing the integrity, availability and data security (Maca et al., 2017). These difficulties that web platforms go through make it necessary to implement systems or hardware that can perform backups in different recovery points or technology to mitigate the risks of existing anomalies within the parameter of digital platforms (Yancey, 2017). Currently, an excessive increase of cyber-attacks focused on different entities to put information at risk, damage data or expose private information by stealing privileged information; in addition, they consider modifying, deleting or altering important information from websites to damage the integrity of the data (Manrique, 2021). This article shows the comparison of cyber-attacks that affect both websites from software and hardware with the purpose that network technicians or network service managers of an entity can have these different cyber-attacks in order to foresee before a possible risk and to mitigate or eliminate these anomalies based on fundamental development criteria (Mondragón et al., 2017).

2. Techniques and methods

Table 1:Software tools free from cyber-attacks

INDICATORS	**Free software tool**	
	NMAMP	Inyección SQL
YEAR OF INITIATION	1997 (Nmap, 2017)	1998 (López, 2017)
COUNTRIES IMPLEMENTED	España (Nmap, 2017)	Estados Unidos (López, 2017)
DEFINITION	NMap is one of the tools with open-source code originated by the varieties of operating systems in which it is employed so it is carried out a multiplatform tool. By which, it allows to evaluate the security of the computer system in which it is employed by sending a predefined package to different devices (Rodriguez, 2019, p. 25).	SQL injection is a known method for performing database attacks through forms containing text-type entries (Lopez, 2017).
CHARACTERISTICS	It allows to have host detection in which it is identified through computers connected to a network. Also, it identified the open ports on a computer. In such a way, it is specified which services are running at the same time. Finally, it was identified the operating system and version that is given computer use (Rodriguez, 2019).	A prevention is made to the web page in terms of an attack in terms of the difference of the GET method with the insertion of URL and placing a SQL statement. Therefore, it is carried out the web applications under attacks that will get requests and queries to the database to receive result, this means, that queries in terms of SQL with the code provided by the attacker. Therefore, it receives a result displayed in the web application (Lopez, 2017).
PROCESS	Loopack closed traffic is maintained and enables protocol connections, therefore, packets that are not valid by definition are rejected and incoming packets that may come from false addresses, allow	The method of SQL injection low in time where it is still the main thing to be able to optimize the database engines, since, the storage in which a huge amount of information is accumulated and continues to

	access through that way and thus be able to extract the information (Rodriguez, 2019, p. 31).	accumulate, not being constantly cleaned this provides that the response time is reduced in the queries and that is why it is one of the quickest ways to attack. (Lopez, 2017)
BENEFIT	Nmap is a tool that allows to obtain great information about network equipment, where it is able to perform that the hots are up, and even test if you have any open ports, if this is filtered on the ports you get to have the ports enabled and even know that the operating system is in use determined (nmap, 2017).	With the modernization of web applications, where most of them are dynamic, that ends up making it necessary to access information, where several ways to gain access to this data are chained together erratically, SQL injection attacks are widely used on the Internet (Lopez, 2017).
VERSIONS	Nmap v5.50, Nmap v6, Nmap v6.25, Nmap v6.40, Nmap v7, Nmap v7.50, Nmap v7.80, Nmap v7.90 (Nmap, 2017)	No record of versions (Lopez, 2017).
COST	The cyber attack in which it is employed is Open Source (Nmap, 2017).	Open source (Lopez, 2017)
OPERATING SYSTEM	Linux, Unix, Mac, Windows (Nmap, 2017)	Microsoft SQL Server (López, 2017)

Table 2: Licensed software tools for cyber attacks

INDICATORS	**Herramienta de software**	
	Fiddler	Burp Suite
YEAR OF INITIATION	2018	2006
COUNTRIES IMPLEMENTED	Estados Unidos, Reino Unidos, India, Bulgaria y Australia (Telerik, 2018).	Victoria Court, Bexton Road, Knutsford (Castañeda, 2015, p. 7)
DEFINITION	Fiddler is a most popular tool in web debugging that manipulates and logs the traffic of a user PC. That is, it inspects traffic through log files and HTTP applications based on Java and .NET (Telerik, 2018).	Burp Suite is a complex tool, it can help us find more specific and complex vulnerabilities of a Web application, as well as provide us with the tools for vulnerability exploitation (Ibarra et al., 2020, p. 92).
CHARACTERISTICS	HTTP and HTTPS web traffic is inspected; in this way, secure traffic is decrypted, where traffic obtained with collaborators of fake requests and responses is saved, shared and received; furthermore, requests and responses are modified to write new API requests (Telerik, 2018).	Under the features in which the Burp suite tool is obtained it allows intercepting proxies, tracking, automatic vulnerable detection, replay tool and ability to write own plugins (Lopez, 2017, p. 17)
PROCESS	It tests the various products that fits in the needs, in which it is integrated into your workflow for fast and elegant debugging and troubleshooting. Also, a benefit of the tool will start to be realized through the acceleration of time and cost savings (Telerik, 2018).	You have the student user login, open the BurpSuite tool, click on the voting module to obtain the URL, edit the intercepted URL to redirect you to the settings module and final close the BurpSuite tool (Castañeda, 2015, p. 7).
BENEFICIO	Fiddler has the functionality of a proxy	It has the benefits of scanner for

	in which it is handled, i.e., when notifying the WinINET network, where it acts as a proxy for browsers where the network communication of a web is executed (Telerik, 2018).	vulnerability identification, Spider with application recognition, for tracking domains, main URL relationship, subdomains, design directories and application configuration (Castañeda, 2015, p. 7).
VERSIONS	Fiddler v0.1.0, Fiddler v0.2.0, Fiddler v0.2.1, Fiddler v0.2.2, Fiddler v0.3.0, Fiddler v0.4.0, Fiddler v0.5.0, Fiddler v0.10.0, Fiddler 0.11.0, Fiddler v1.0.0, Fiddler v1.0.1, Fiddler v1.0.2, Fiddler v1.1.0, Fiddler v1.1.1, Fiddler v1.2.0, Fiddler v1.2.1, Fiddler v1.3.0, Fiddler v1.4.0, Fiddler v1.4.1, Fiddler v1.5.0, Fiddler v1.5.1, Fiddler v1.6.0, Fiddler v1.6.1, Fiddler v2.0.0, Fiddler 2.0.1, Fiddler v2.0.2, Fiddler v2.0.3, Fiddler v2.1.0 (Telerik, 2018).	Professional Burp Suite v2.0.13, Burp Suite v2.0.14, Burp Suite v2.0.15, Burp Suite v2.0.16, Burp Suite v2.0.17, Burp Suite v2.0.18, Burp Suite v2.0.19, Burp Suite v2.0.20, Burp Suite v2.0.21, Burp Suite v2.0.22, Burp Suite v2.0.23, Burp Suite v2.0.24, Burp Suite v2.0.25, Burp Suite v2.1.03, Burp Suite v2.1.05, Burp Suite v2.1.06 Edition Profesional Burp Suite v1.0.10, Burp Suite v1.0.11, Burp Suite v1.0.12, Burp Suite v1.0.13, Burp Suite v1.0.14, Burp Suite v1.0.15, Burp Suite v 1.0.16, Burp Suite v1.0.17, Burp Suite v1.1, Burp Suite v1.1.01, Burp Suite v1.1.02, Burp Suite v1.1.03, Burp Suite v1.1.04, Burp Suite v2020.1, Burp Suite v2020.2, Burp Suite v2020.4, Burp Suite v2020.4.1, Burp Suite v2020.4.3, Burp Suite v2020.6, Burp Suite v2020.7, Burp Suite v2020.10, Burp Suite v2020.10.1, Burp Suite v2020.11, Burp Suite v2020.12, Burp Suite v2021.1, Burp Suite v2021.3, Burp Suite v2021.3.1, Burp Suite v2021.4, Burp Suite v2021.4.1, Burp Suite v2021.6, Burp Suite v2021.8, Burp Suite v2021.8.1 Profesional / Community Burp Suite v2.1, Burp Suite v2.1.01, Burp Suite v2.1.02, Burp Suite v2.1.04, Burp Suite v2.1.07, Burp Suite v2020.1, Burp Suite v2020.2, Burp Suite v2020.2.1, Burp Suite v2020.4, Burp Suite v2020.4.1, Burp Suite v2020.5, Burp Suite v2020.5.1, Burp Suite v2020.6, Burp Suite v2020.7, Burp Suite v2020.8, Burp Suite v2020.8.1, Burp Suite v2020.9, Burp Suite v2020.9.1, Burp Suite v2020.9.2, Burp Suite v2020.11,

		Burp Suite v2020.11.1, Burp Suite v2020.11.2, Burp Suite v2020.11.3, Burp Suite v2020.12, Burp Suite v2020.12.1, Burp Suite v2021.2, Burp Suite v2020.2.1, Burp Suite v2021.3, Burp Suite v2021.3.2, Burp Suite v 2021.3.3, Burp Suite v2021.4, Burp Suite v2021.4.1, Burp Suite v2021.4.2, Burp Suite v 2021.4.3, Burp Suite v2021.5, Burp Suite v2021.5.1, Burp Suite v2021.5.2, Burp Suite v2021.5.3, Burp Suite v2021.6, Burp Suite v2021.6.1, Burp Suite v2021.6.2, Burp Suite v2021.7, Burp Suite v2021.7.1, Burp Suite v2021.7.2, Burp Suite v2021.8, Burp Suite v2021.8.1 Burp Suite v2021.8.2, Burp Suite v2021.8.3 (López, 2017)
COST	**Pro** $ 10 usd **Empresa** $25 usd (Telerik, 2018).	**Enterprise Edition Burp Suite Starter** - $6,995 Per year **Grow** - $14,480 Per year **Accelerate** - From $29,450 Per year **Burp Suite Profesional** 1 año: - $ 399,00 2 año: - $ 798,00 3 año: - $ 1,197,00 (López, 2017)
OPERATING SYSTEM	Windows, MacOs y Linux (Telerik, 2018).	Windows, MacOs y Linux (López, 2017, p. 17)

3. Results and discussion

Rodriguez (2019) mentioned that the open source Nmap tool performs cross-platform functions allowing to evaluate the security of a computer system for him to send packets to different devices, this is similar to the study of Lopez (2017) described that his method that performs simultaneous attacks to database through forms containing text type input in order to extract specific parameters and damages or alters information. On the other hand, in the characteristics criterion focuses on the study of Lopez (2017) since it performs forecasts to the web page focusing on performing attacks through GET method, URL insertion and SQL statements, that is why every web page will receive requests and queries in the database and thus obtain the information of the website. This result is different from Rodriguez (2019) as it allows host detection through an interconnected network, identifying free access ports, services that are running in real time the operating system and host version. On the other hand, Rodriguez (2019) mentioned that it maintains the traffic of protocol connections, rejects packets that are not validated and

incoming packets that comes from false addresses, allowing access by that way and thus being able to extract the information, this study is different from Lopez (2017) since the SQL injection method focuses on times and optimization of database engines since each engine stored a lot of information and by not being constantly cleaned queries are performed and information can be extracted from digital pages. Otherwise, the benefit criterion in Nmap (2017) described that it is a tool capable of obtaining a large amount of information about other network equipment, allows to activate the hosts of a network even test if there is open access through that channel by filtering the enabled and disabled ports focused on the operating system, this study is different from Lopez (2017) focuses on the modernization of applications, websites allowing access to information erratically thus being widely using the network. In addition, in the cost criterion in the Nmap (2017) study mentioned that it is open source, this study is similar to Lopez (2017) since SQL injection is open source. Finally, Nmap (2017) mentioned that it focuses on different operating systems for its functions, such as: (a) Linux, (b) Unix, (c) Mac and (d) Windows, this study is different from Lopez (2017) that focuses on a Microsoft SQL Server operating system.

According to Telerik (2018) mentioned that the Fiddler tool has been implemented in the following countries: (i) United States, (ii) United Kingdom, (iii) India, Bulgaria and (iv) Australia, this study is different from Castañeda (2015) because it focuses on: (a) Victoria Court, (b) Bexton Road, (c) Knutsford. On the other hand, Ibarra et al. (2020) mentioned that it is a complex tool that apart from place to find specific and complex vulnerabilities of a web platform also allows to provide tools for the exploitation of that vulnerability, this study is different from Telerik (2018) since the tool focuses on debugging by manipulating and logging the traffic of a host inspecting through log files and HTTP applications. On the other hand, in the feature criteria in the Lopez (2017) study the Burp suite tool allows capturing proxies, tracking users, vulnerability detection, replay tool and developing own plugins, this study is different from Telerik (2018) since the tool inspects HTTP and HTTPS network traffic by decrypting secure traffic where it stores, stores and shares fake requests and responses to alter requests and responses to spoof API requests. In another way, Castañeda (2015) described that the tool allows to obtain the user login with simple functions of the module to intercept the URL and be able to have the information, this study is different from Telerik (2018) described that the tool adapts to the user needs by integrating the workflow to debug and alter the information data quickly and simply in order to save time and cost. On the other hand, Castañeda (2015) mentioned some benefits of this tool such as vulnerability identification scanning, application recognition, tracking domains relationships with the main URL, subdomains, design directories and application configurations, this study is different Telerik (2018) Fiddler tool focuses on managing proxies to identify and debug the network of a web. Otherwise, Telerik, 2018 the Fiddler tool offers a pro service at 10 USD and an organizational service at 25 USD, being different from Burp Suite (2017) study since it has high regime service such as: from 399 pro service to 29,450 organizational service. Finally, Telerik (2018) employs the fiddler tool in different operating systems such as: (a) Windows, (b) MacOs and (c) Linux, this result is similar to the study of Lopez (2017) who uses the burp suite tool on the same operating systems such as: (i) Windows, (ii) MacOs and (iii) Linux.

4. Conclusion

It is concluded to have the different tools for cyber-attacks for which 4 types of web applications for attacks were used in research.

The Nmap tool is more complete because of its free access to its varieties of operating systems and multiplatform tool allowing to evaluate the security of a system to send predefined packets to different devices. In addition, based on the characteristics SQL injection performs prevention to the web

page in terms of attacks based on the GET method with the insertion of URL and placement in the SQL statement, which is why the application will receive requests and queries to the database to obtain information, it means that it will get the data from a web system.

The SQL injection tool focused on time optimizes the database engines since each engine stores a large amount of information and by not being performed or changed and by performing different queries the information can be extracted.

Nmap is a tool that allows to obtain the information of all the devices of a network until raising the hosts and even to see the accesses of the open ports to filter and to be able to subtract the specific information. On the other hand, the Nmap tool focuses on performing different tests on different platforms in operating systems such as: Linux, Unix, Mac and Windows, while SQL injection focuses Microsoft SQL Server. On the other hand, the Fiddler tool focuses on debugging websites to manipulate and log host traffic by inspecting traffic through log files and HTTP applications.

The Burp suite tool allows intercepting proxies, tracing, vulnerability detection and overwriting proprietary plugins. On the other hand, the Fiddler tool adapts to different needs by integrating a workflow for debugging and troubleshooting to save time and cost. On the other hand, SQL injection allows to scan for vulnerabilities, recognize applications, trace domains, subdomains, design managers and obtain a simple configuration of network access.

Fiddler is that tool that can be obtained at a simple cost from 10 to 25 dollars being a regime suitable for a person or an entity and its functions are optimal.

Fiddler and SQL injection share the same operating systems to test and see the functions of each tool such as: Windows, MacOS and Linux.

5. Recomendation

The recommendations of this research are the following: This qualitative study can be continued in a quantitative way by assigning variables, numerical and statistical data with the objective of being able to measure the selected and mentioned indicators to be able to evaluate different cyber-attacks and their derivatives for the effect on tests and results. To carry out a classification study is a good option to obtain more results in front of different cyber-attacks that can help administrative technicians to be able to make a more adequate decision at the moment of the development of websites. Develop the research work using the convergent mixed method to obtain qualitative and quantitative data and compare the information in search of similarity and/or difference.

References

[1] Burp Suite (2017). Burp Suite is the choice of security professionals worldwide. PortSwigger. Disponible enhttps://portswigger.net/burp
[2] Castañeda A. F (2015). Identification and exploitation of vulnerabilities in web applications.
[3] Chang J. E. A. (2020). Analysis of cyber attacks against Ecuador. Deputy Editor, 2, 18.
[4] Chinguel S. F., Arcila J. C., Tuesta V. A., y Mejia H. I. (2019). Evaluation of SMO, BayesNet and J48 algorithms for the identification of web site attacks using server log. Perspectivas, 15(16), pp. 88-91
[5] Ibarra H. J., Zenteno A. C., Santiago M. D. C., y Rubín G. T. (2020). Security Through an Audit Plan. Contributions and Applications in Computer Science., (4609)
[6] López R. E. (2017). Penetration testing of web applications using ethical hacking. RevistaTecnológica; 10
[7] Maca O. E. M., Arcos A. F. M., Urcuqui C., y Cadavid, A. N. (2017). Security control for website defacement. Sistemas & Telemática, 15(41), pp. 45-55.
[8] Manrique J. I. T. (2021). Cyberterrorism: perspectives from fundamental rights.Revista Argumentum-Argumentum Journal of Law, 22(2), pp. 819-848.

[9] Mondragón O. E., Mera A. F., Urcuqui, C., & Navarro, A. (2017). Validation and testing of a security control for defacement on web sites. Sistemas &Telematica, 15(41), pp. 45-56.
[10] Nmap (2017). Nmap segurity. Disponible en https://nmap.org/
[11] Nope O. A. (2016). The government and its responsibilities regarding the secure code (Bachelor's thesis, Universidad Piloto de Colombia).
[12] Parrales M. P. M., Castro J. C. M., Hernández M. M. O., y Lino E. A. M. (2021). analysis of tools and techniques used in penetration testing for the detection of vulnerabilities in web applications. UNESUM-Sciences. Revista Científica Multidisciplinaria. 5(1), pp. 135-144. ISSN 2602-8166
[13] Rodríguez E. (2019). Defense of a public server against network attacks using IPTables (Bachelor's thesis).
[14] Sánchez J. G., Mendoza M. N., y Garzón G. M. (2020). Vulnerabilities of governmental websites in Ecuador: An exploratory pre-sampling study. Revista Ibérica de Sistemas e Tecnologias de Informação, (29), pp. 67-78.
[15] Telerik (2018). Modern UI Made Easy. Disponible en https://www.telerik.com/
[16] Yancey J. (2017). Cyber attacks and their global political repercussions.