Journal of Physics: Conference
Series

PAPER • OPEN ACCESS

Nscanner: Vulnerabilities Detection Tool for Web Application

To cite this article: R. Utaya Surian *et al* 2020 *J. Phys.: Conf. Ser.* **1712** 012018

Nscanner: Vulnerabilities Detection Tool for Web Application

R. Utaya Surian[1,*], Nor Azlina Abd Rahman[2] and Yogeswaran Nathan[3]

[1,2,3]Asia Pacific University of Technology and Innovation Technology Park Malaysia, Bukit Jalil, Kuala Lumpur

[*]Corresponding author e-mail: utayasurian@yahoo.com

Abstract. Internet has been dominating the world nearly a decade. Web application is known to be the most widespread platform of the internet especially when it comes to share resources, e-commerce services, education and business platforms. Since the usage of web applications are increasing dramatically, it's becoming more vulnerable for security attacks. Each year, organizations facing many security attacks towards their web applications. Although many security practices and mitigations have been applying in web application, however there are still some security loophole issues can be found in web application. For instance, these loopholes can be referred as lack of secure coding (standards) implemented in web application, lack of formal security training approach for web developers and improper security testing for their web application. Besides, social engineering attacks also tremendously increasing each year. Many organizations were compromised through phishing attacks due to lack of awareness among users (employees). As a solution to overcome the issues, a research project will be carried out to implement a system called Nscanner to detect Structured Query Language injection (SQLi) and Cross-Site Scripting (XSS) vulnerabilities for web application. Moreover, the developer also will design a malware detection feature based on machine learning approach to detect malware found in attachments from emails in order to prevent malware phishing attacks.

Index Terms— Web Application Vulnerabilities, Phishing Attack, SQLi, XSS, Machine Learning , Hacking, Social Engineering

1. Introduction

Web application usage are increasing due to rapid development of technology. According to the analytical data of Internet User Survey (ISS) 2018 which analyzed by Malaysian Communication and Multimedia Commission, there was 87.4% of increment in 2018 compared in 2016 which was reached about 76.4% of internet users [17]. Since the usage of internet is increasing dramatically, the amount of data usage also generated in tremendous quantity. During the data sharing over the internet, many users may not aware of data transferring in the internet which means cyber attackers may spoofing, stealing or social engineer on users' data.

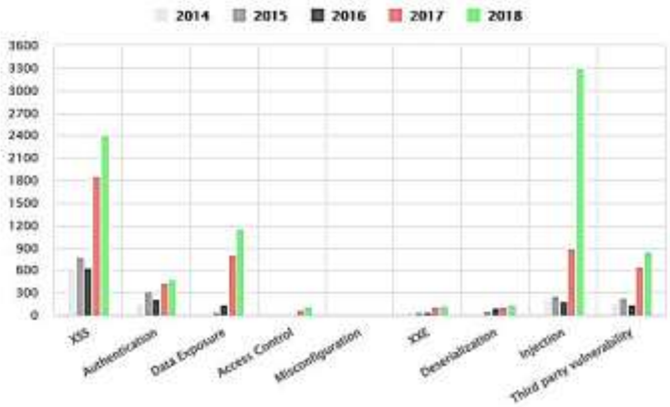


Figure 1. Web Vulnerabilities Statistics of 2014-2018 [9]

Each year, many cyber security researchers provide some statistical analysis on web vulnerabilities in order to create awareness amongst internet users, developers and security researchers. There are reports generated to investigate the amount of web vulnerabilities published in 2018 as shown in Figure 1. A simple analysis has been conducted on most trending and highly risks vulnerabilities based on some research papers which researchers were found the most dominant website attacks. From the latest report of 2018 which analyzed by the cybersecurity researchers from Imperva, common vulnerabilities such as the top two numbers of most attempted attacks known as SQLi and XSS. Statistic that tabulated in Figure 1 shows that injection attack which is rated at 3,294 in 2018. While XSS attack is rated at 2,410 in 2018 [9].

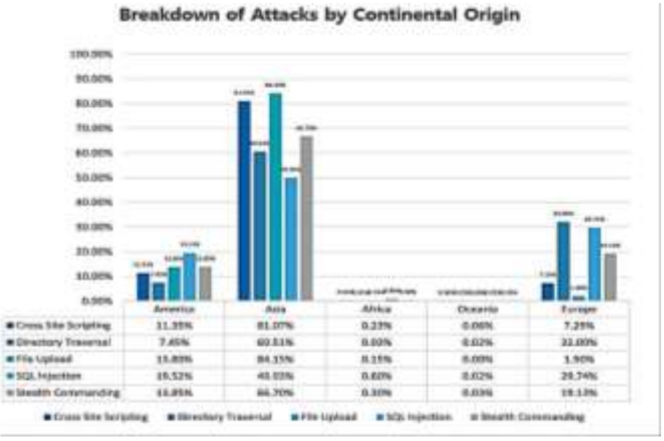
Social engineering attacks are escalating quickly in today's networks and weakening the cybersecurity firm [21]. In several studies shown that social engineering as manipulating and convince people to reveal sensitive information via online networks or by gaining access to systems [4]. According to Wenjun Fan, Kevin and Rong Rong, humans are the main factors that easily can be exploited by social engineering attackers. They stated that social engineering attacks emphasize on human element's psychological vulnerabilities rather than the traditional technical ones such as web application vulnerabilities. Therefore, a social engineering attacks are very difficult to defend by system administrators [15]. Social engineering attacks can be achieved in any form of techniques which has human interaction involves [10]. The most common strategies can be known as phishing attacks, spear phishing attacks, scareware, phone/email scams, reverse social engineering attack and so forth [22]. According to researchers, phishing attacks are the most common attacks amongst other techniques in social engineering [22]. Attackers simply sending emails and text messages and manipulate the target user to open attachment or click a link which malware has been embedded [10]. Once the user, opened/clicked, vulnerability will be exploited and cause infection on target's workstation or network.

Table 1. Statistic Analysis on social engineering attack[8]

Phishing Vectors	**Results**
Malware Phishing	50.7%
Credential Harvesting	40.9%
Extortion	8%
Spear Phishing	0.4%

Table 1 show the analysis that reported by Avanan, phishing attacks are increasing and difficult for humans and technologies to detect. Based on their analysis, over 561,947 emails from different organizations were compromised by attackers. Table 1 shows that malware phishing rated at 50.7%

than any other phishing vectors. Where attackers embed malicious content along via attachments or links. Besides, Avanan studies shown that phishing attack can easily bypassed Gmail and Office 365 are not reliable to block malicious emails [8].



	America	Asia	Africa	Oceania	Europe
Cross Site Scripting	11.35%	81.07%	0.23%	0.06%	7.29%
Directory Traversal	7.45%	60.51%	0.00%	0.02%	32.00%
File Upload	13.83%	84.15%	0.15%	0.00%	1.90%
SQL Injection	19.52%	49.93%	0.60%	0.02%	29.74%
Stealth Commanding	13.85%	66.70%	0.30%	0.03%	19.13%

Figure 2. Statistic Analysis (2017) of Most Web Application Attacks According to Region [20]

Based on a survey done by Penta Security, the number of XSS and SQLi attacks struck mainly Asian countries [20]. Figure 3 above, described that the number of SQLI and XSS attacks are mostly dominant in Asia and followed by Europe and America. Consumer News and Business Channel (CNBC) reported that the main reason of why Asia is amongst the most vulnerable region because of the cybersecurity awareness across Asia was comparatively lower than any other regions, such as Europe and America [12].

2. Literature Review on vulnerability detection tool

Some sources stated that almost 200% increase in data breach attacks in 2018 [25] [1]. Since the number of web attacks are increasing, it's considered as urgency to secure web applications from cyber attacks. Dr. Aswami Fadillah advised companies for regular security system vulnerability assessments in order to limit the impact of data or system loss [13]. Thus, security pentester, system administrator or system testers is required to critically assess application or network to secure prevent from any vulnerabilities.

Vulnerability scanner is a tool to help pentester or web developer for assessing web application or network in order to find its vulnerabilities. It can be known as an automated tool to audit web application for security vulnerabilities, without the need for system tester to test the application's source code to find for security bugs [14]. There are many vulnerability scanners are available in today's technology. However, choosing the right vulnerability scanner for penetration testing will produce a significant quality assessment due to capabilities and convenient. The researcher has selected three different tools to identify its' drawbacks for vulnerability assessment. The following shows the three types of vulnerability scanners for web applications:

2.1. Acunetix

Acunetix is also known as WAVS tool for penetration testing. It's can discover multiple vulnerabilities including XSS and SQLi [14]. It's one of most widely used tool in security assessment. Acunetix software is based on commercial package where customer required to purchase for license according to available subscriptions [2]. Its application is based GUI based desktop application where provides user to conveniently interact. Moreover, it enables reporting management for user such as generating results and remediation advices on identified security vulnerabilities of the application. All detected vulnerabilities will be remarked based on status such as open or fixed [3].

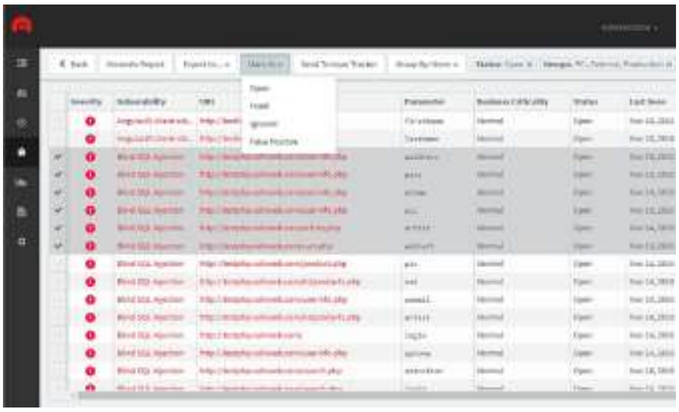
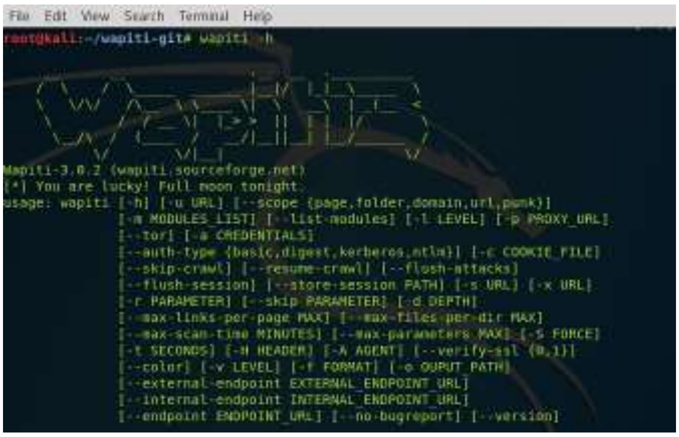


Figure 3: Acunetix (Similar System 1) [3]

2.2. Wapiti



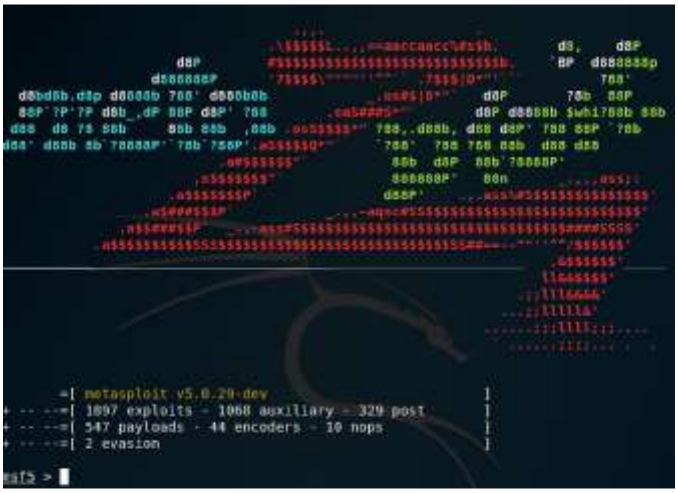
```
root@kali:~/wapiti-git# wapiti -h

Wapiti-3.0.2 (wapiti.sourceforge.net)
[*] You are lucky! Full moon tonight.
usage: wapiti [-h] [-u URL] [--scope {page,folder,domain,url,punk}]
              [-m MODULES_LIST] [--list-modules] [-l LEVEL] [-p PROXY_URL]
              [--tor] [-a CREDENTIALS]
              [--auth-type {basic,digest,kerberos,ntlm}] [-c COOKIE_FILE]
              [--skip-crawl] [--resume-crawl] [--flush-attacks]
              [--flush-session] [--store-session PATH] [-s URL] [-x URL]
              [-r PARAMETER] [--skip PARAMETER] [-d DEPTH]
              [--max-links-per-page MAX] [--max-files-per-dir MAX]
              [--max-scan-time MINUTES] [--max-parameters MAX] [-S FORCE]
              [-t SECONDS] [-H HEADER] [-A AGENT] [--verify-ssl {0,1}]
              [--color] [-v LEVEL] [-f FORMAT] [-o OUPUT_PATH]
              [--external-endpoint EXTERNAL_ENDPOINT_URL]
              [--internal-endpoint INTERNAL_ENDPOINT_URL]
              [--endpoint ENDPOINT_URL] [--no-bugreport] [--version]
```

Figure 4: Wapiti (Similar System 2) [6]

Wapiti is a WAVS tool for security auditing for web applications. It used to perform black-box testing such as Metasploit, Acunetix and other WAVS. It can be known as an open source platform and CLI based interface [16] and also able to scan for multiple modules according to vulnerabilities including SQLi and XSS. It has the similar feature with Metasploit and Acunetix where it can crawl entire webpages of a website, targeting for scripts and forms to inject payloads to find for vulnerabilities [23]. Wapiti also has capability on generating reports and can be analyzed through web browser [16].

2.3. Metasploit

Metasploit is considerably known as Web Application Vulnerability Scanner (WAVS) which developed by Rapid7 security team [19]. It's available in two variants: commercial and community. A commercial version Metasploit required license subscription while a community version can be known as open source platform (free version) [18]. Metasploit does supports GUI interaction. User can launch Metasploit in web UI mode. It's capable to run web assessment such as SQLi and XSS detection. In addition, Metasploit also able to scan web application by using additional plugin called Nexpose [11]. Nexpose available in web GUI and CLI interfaces.



```
      =[ metasploit v5.0.29-dev                          ]
+ -- --=[ 1897 exploits - 1068 auxiliary - 329 post       ]
+ -- --=[ 547 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 >
```

Figure 5: Metasploit (Similar System 3) [7]

2.4 Comparative Analysis of Existing Systems

Table 2 showing the comparative analysis between three identified systems based some similarities on proposed system. However, there are few drawbacks has been identified by the researchers. For instance, Wapiti doesn't provide GUI interface for most users to interact. By default, Metasploit doesn't support frequent patches (updates) to keep the application up to date except for commercial package. To update the Metasploit in open source, user required to manually update the module according on user. Apart from that, Acunetix and Wapiti don't provide additional features such as social engineering kits. For example, Metasploit provides phishing attacks that available from its social engineering module. Thus, Acunetix and Wapiti have limitation on penetration testing. Acunetix only available upon license subscription. The disadvantage of using Metasploit and Wapiti can be considered as the limitation on multi-platform supports such as operating systems. Although Metasploit can be installed in Windows operating system, however security researchers have found that it has some certain bugs [24].

✓ = Available ✗ = Not Available

Criteria	Metasploit	Acunetix	Wapiti
GUI Interaction	✓	✓	✗
CLI Interaction	✓	✗	✓
Frequent Patches	✗	✓	✓
SQLi Detection Feature	✓	✓	✓
XSS Detection Feature	✓	✓	✓
Social Engineering Feature	✓	✗	✗
Open Source Software	✓	✗	✓
Multi-Platform	✗	✓	✗

Figure 6: Comparative Analysis of Similar Systems

To conclude the research on similar system studies, researcher's proposed system can provide additional benefits for user according to those criteria mentioned in Table 2. The proposed system can be considered as a WAVS tool for pentester, web developer and normal user. The proposed system called Nscanner can help in penetration testing for web applications to find out severe vulnerabilities such as SQLi and XSS. In addition, it's also functions as multi-purpose tool such as scanning attachments via emails to detect malicious programs using machine learning way for normal email users. Due to the project scope limitation, in future of development, developer of Nscanner will also concentrate on developing additional features such as network assessment. Eventually, the proposed system may help the organizations to save more money, time and resources when it comes to web assessment.

3. Analysis on participants awareness on several types of Web attacks

Researcher conducted a survey on web vulnerability and social engineering awareness amongst different participants. The researcher gathered sampling data through questionnaire. The survey took 12 days to finalize for the requirement analysis phase according to the Rapid Application Development (RAD) methodology. All the data analyzed will be reflected to the requirement analysis stage of RAD. There are total of 53 participants involved during the survey. Different types of participants involved in the survey such as web developer, pentester, lecturer, and student who have interest in Information Technology (IT) security. Therefore, they can provide the developer with more reliable feedbacks and information to carry out this research. Besides, they also aware of web applications attacks and social engineering. Thus, it helps the researcher to investigate every aspect from participants more accurately.

3.1. Research Findings

According to the findings, most participants are aware of social engineering attacks that increasing drastically. Besides, to mitigate social engineering attacks that affecting many organizations, they suggested that organizations can provide security awareness training for users. And make some improvement in current technology which capable to protect firms from social engineering attacks.

Over 43.4% of participants having a limited knowledge on SQLi and XSS vulnerabilities. Thus, the awareness amongst the users on web vulnerabilities still considered as low. Ideally, most participants mentioned that vulnerability scanner provides flexibility when it comes to automated security testing. Which means help security auditors to find bugs easily and faster than code analysis. Thus, it helps in saving time. However, few participants mentioned that some vulnerability scanners may provide some false positive results. Moreover, participants also stated that some vulnerability scanners are user friendliness due to its simplicity.

Apart from that, survey shows that 100% of total participants stated that vulnerability scanner provides beneficial for security assessment for web application. Within the context of security assessment for web application, majority of participants specified that it provides benefits for web developers, pentesters and bug hunters to find bugs. In addition, majority of participants also suggested malware detection as recommended additional feature for the Nscanner application.

In conclusion based on the overall findings, researcher has proposed Nscanner application as the newly improved version of vulnerability scanner with the capability of malware detection using machine learning method. Thus, it provides the significant to the research on improvement of current security assessment.

4. Nscanner Framework

The researcher has proposed highly dynamic and flexible automated approach to detect SQLi and XSS vulnerabilities. Besides, it also capable to detect malware using machine learning formula to prevent false positive results.

Figure 7 shows the proposed model of the proposed solution. There are two different phases involve such as web application vulnerability testing and file scanner. The web application vulnerability testing is for run security assessment on website to detect SQLi and XSS. Besides, in file scanning phase is for malware detection. There is not database management system is required since the al the output of the analysis will be stored locally.

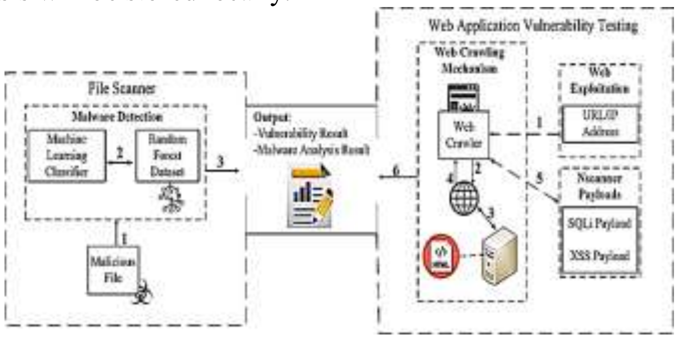


Figure 7: Nscanner System Architecture

Figure 7 showing the detail processes that involve in web application vulnerability testing and file scanner which of Nscanner system architecture. The following Table 2-3 showing the processes of two different phases of Nscanner application:

Table 2. Web Application Vulnerability Testing Phase

Identity of Each Process	Process Explanation
1	Before user proceed with testing, it's is compulsory for the user to connect user's computer to the network in order for Nscanner to get access to an internet. First step, user required to choose which type of web exploitation to be tested for a website such as SQLi or XSS. Once a user selected any option, he/she is required to provide an URL or IP address of a website to run the vulnerability testing.
2	Once user provided a valid URL or IP address of a testing website, a request will be made to Nscanner's crawler mechanism. The web crawler will automatically communicate through the internet to find for the website based on the domain. A domain is used to identify server which hosting that particular website.
3	Once the web crawler found the related server which hosts the website, crawler will request a connection to server in order to access the web application. Once server responded back to Nscanner's web crawler, a connection will be established between server and crawler. At this stage, crawler will begin to crawl all possible form based webpages and webpages that accepting parameter as input from that particular website. All webpages will be determined based on domain and its' subdomains.
4	At this stage, server will accomplish all possible request made by Nscanner at previous stage via the World Wide Web (internet).
5	This is the important stage where bugs will be identified by Nscanner. During at this stage, Nscanner will inject payload according to the selection of vulnerability testing made at process 1 previously. Payload will inject to every page that crawler retrieved at process 3. Since this is known to be an iteration process it may consume time until the injection process reaches its end.
6	Finally, Nscanner will generate an instant report of the vulnerability assessment as outcomes. User can either save the report of the assessment.

Table 3: File Scanner Architecture Phase

ID of Each Process	Process Explanation
1	The first step in malware detection is user required to upload any of sample/file which they found malicious to Nscanner.
2	Once user uploaded successfully to the Nscanner, the core malware detection will automatically begin the dynamic analysis for the user. For example, a machine learning classifier model that designed based on Random Forest algorithm. The role of this classifier is to help in detect the

ID of Each Process	Process Explanation
	sample according to *PE header*, *section table* and *PE file sections*. All this information will be referred from local dataset of random forest. When each time classifier detects, a new sample information will be generated which called as decision tree. A decision tree can be considered as dataset. Thus, many decision trees will be generated during the training process. This is used to identify the behavior of a sample. Classifier will use the dataset to scan malicious file. If a malicious sample is matched against of the highest accuracy from a decision tree based on a certain prediction, it can be considered as a malware file.
3	Finally, a malware analysis report will be generated by Nscanner for user to know the outcome of the scanning.

5. Conclusions

Based on the overall research, web-based attacks are still remain as potential threats that can cause data breaches or web defacement. Typically, web attacks are caused by security flaws that can be found from web applications. Those security flaws can be determined as web vulnerabilities where it capable in poisoning the web applications to cause disaster according to the type of vulnerabilities such as SQLi, XSS and others. A flaw in a web application is caused by most web developers. For instance, most SQLi and XSS vulnerabilities are caused by lack of secure coding procedures implemented by web developers. A common mistake are no proper validation and sanitization on input data that implemented by the programmers from client side. Thus, such common mistakes made by web developers will cause the entire web application and its' users into harmful. Several facts stated that human is the weakest link when it comes to phishing attacks. Due to lack of awareness among email users, they are vulnerable to malware attacks. Most of them having the curiosity to open attachments without properly investigate the mail header of that phishing mail. Once they opened the content from the attachment, they may get infected by malicious program. Besides, due to lack of accuracy trigger by anti-spam feature in the email system, it can easily reach user's mailbox. Therefore, users can open the email contents without noticing it was a phishing mail.

As a conclusion to the research, researcher has proposed the system called Nscanner application where it helps most web developer, security auditor (pentester) to assess their web application. Due to the its automate capabilities, it can scan the entire websites to detect for severe vulnerabilities rapidly such as SQLi and XSS. Once the detection succeeds, a report will be generated for user to analyze the results. Asides from web assessment, a normal user can scan any content of malicious file to detect malware programs. The result of the malware detection will be generated in a report for user to analyze. Eventually, this research also may help in create cyber security awareness among most internet users in Malaysia. Most working adults and non-working adults required to develop their skills and knowledge in defending themselves from cyber-attacks. Technology should always play significant role in preventing against most malicious activity by cyber criminals.

References

[1] ACE Accelerator, 2019. Almost 200% increase in data breach attacks since 2018. [Online] Available at: https://www.acegroup.com.my/insights/almost-200-increase-data-breach-attacks-2018,[Accessed 8 January 2020].

[2] Acunetix, n.d. Pricing and Ordering Information of Acunetix. [Online] Available at: https://www.acunetix.com/ordering/ [Accessed 9 January 2020].

[3] Acunetix, n.d. Vulnerability Management Software | Acunetix. [Online] Available at: https://www.acunetix.com/vulnerability-scanner/vulnerability-management-software/[Accessed 9 January 2020].

[4] Aldawood, H. & Skinner, G., 2019. A Taxonomy for Social Engineering Attacks via Personal Devices, Volume 178, p. 1.

[5] Anon., n.d. [Online] Available at: https://www.acunetix.com/vulnerability-scanning-tool/

[6] Anon., n.d. [Online] Available at: https://sectechno.com/wapiti-web-application-vulnerability scanner/
[7] Anon., n.d. [Online] Available at: https://medium.com/@jamiepegg/spy-on-windows- achines using-metasploit-758dbf72bb90
[8] Avanan, 2019. Global Phish Report 2019, s.l.: Avanan.
[9] Avital, N., 2019. The State of Web Application Vulnerabilities in 2018. [Online] Available at: https://www.imperva.com/blog/the-state-of-web-application-vulnerabilities-in-2018/[Accessed 9 April 2019].
[10] Bansla, N., Kunwar, S. & Jain, K., 2019. Social Engineering: A Technique for Managing Human Behavior, p. 19.
[11] Choudary, H., 2017. NeXpose scanner via metasploit, s.l.: YouTube.com.
[12] Choudhury, S. R., 2016. Four reasons why Asia is a prime target for cybercriminals, s.l.: CNBC.
[13] Ehsan, N., 2019. CyberSecurity Malaysia: Watch out for cyberattacks ahead of Malaysia Day. [Online] Available at: https://www.thestar.com.my/tech/tech-ews/2019/09/13/cybersecurity-malaysia-watch-out-for-cyberattacks-ahead-of-malaysia-day. [Accessed 2020].
[14] Erturk, E. & Rajan, A., 2017. Web Vulnerability Scanners: A Case Study, p. 2.
[15] Fan, W., Lwakatare, K. & Rong, R., 2017. Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations, p. 1.
[16] Latest Hacking News, 2018. Wapiti – The Black Box Vulnerability Scanner for Web Applications. [Online] Available at: https://latesthackingnews.com/2018/10/18/wapiti-the-black-box-vulnerability-scanner-for-web-applications/ [Accessed 9 January 2020].
[17] Malaysian Communications and Multimedia Commision, 2018. Internet Users Survey 2018. [Online] Available at: https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2018.pdf [Accessed 2 December 2019].
[18] Mammadov, E., 2017. Application of Metasploit in Web Penetration Testing, p. 11.
[19] Pegg, J., 2019. Spy On Windows Machines Using Metasploit. [Online] Available at: https://medium.com/@jamiepegg/spy-on-windows-machines-using-metasploit-758dbf72bb90 [Accessed 8 January 2020].
[20] Penta Security Systems Inc., 2018. Web Application Threat Trend ReportTrends for 2017, p. 11.
[21] Salahdine, F. & Kaabouch, N., 2019. Social Engineering Attacks: A Survey, p. 1.
[22] Salahdine, F. & Kaabouch, N., 2019. Social Engineering Attacks: A Survey, pp. 2-3.
[23] Sec Techno, 2019. Wapiti – Web-application vulnerability scanner. [Online] Available at: https://sectechno.com/wapiti-web-application-vulnerability-scanner/ [Accessed 9 January 2020].
[24] Stack Exchange, n.d. Disadvantages of metasploit Framework for windows. [Online] Available at: https://security.stackexchange.com/questions/14310/disadvantages-of-metasploit-framework-for-windows [Accessed 9 Jan 2020].
[25] YUNUS, R., 2019. Almost 200% increase in data breach attacks since 2018. [Online] Available at: https://themalaysianreserve.com/2019/10/17/almost-200-increase-in-data-breach-attacks-since-2018/ [Accessed 8 January 2020].