On the review and setup of security audit using Kali Linux

Article · July 2018

DOI: 10.11591/ijeecs.v11.i1.pp51-59

4 authors, including:

Teddy Surya Gunawan
International Islamic University Malaysia
187 PUBLICATIONS **703** CITATIONS

SEE PROFILE

Nurul Zulkurnain
International Islamic University Malaysia
12 PUBLICATIONS **22** CITATIONS

SEE PROFILE

Mira Kartiwi
International Islamic University Malaysia
120 PUBLICATIONS **629** CITATIONS

SEE PROFILE

Indonesian Journal of Electrical Engineering and Computer Science
Vol. 11, No. 1, July 2018, pp. 51~59
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v11.i1.pp51-59

On the Review and Setup of Security Audit Using Kali Linux

Teddy Surya Gunawan[1], Muhammad Kassim Lim[2], Nurul Fariza Zulkurnain[3], Mira Kartiwi[4]
[1,2,3]Department of Electrical and Computer Engineering, Kulliyyah of Engineering,
[4]Department of Information Systems, Kulliyyah of ICT
The International Islamic University Malaysia (IIUM), Jalan Gombak, 53100 Kuala Lumpur, Malaysia

Article Info

Article history:

Received Jan 9, 2018
Revised Mar 27, 2018
Accepted Apr 11, 2018

Keywords:

Computer Security
Kali Linux
Penetration Testing
Security Analysis
Security Audit

ABSTRACT

The massive development of technology especially in computers, mobile devices, and networking has bring security issue forward as primarily concern. The computers and mobile devices connected to Internet are exposed to numerous threats and exploits. With the utilization of penetration testing, vulnerabilities of a system can be identified and simulated attack can be launched to determine how severe the vulnerabilities are. This paper reviewed some of the security concepts, including penetration testing, security analysis, and security audit. On the other hand, Kali Linux is the most popular penetration testing and security audit platform with advanced tools to detect any vulnerabilities uncovered in the target machine. For this purpose, Kali Linux setup and installation will be described in more details. Moreover, a method to install vulnerable server was also presented. Further research including simulated attacks to vulnerable server on both web and firewall system will be conducted.

Corresponding Author:

Teddy Surya Gunawan,
Department of Electrical and Computer Engineering,
Kulliyyah of Engineering
International Islamic University Malaysia
Email: tsgunawan@iium.edu.my

1. INTRODUCTION

Nowadays, computer is considered essential to everyone from young to old, students to the corporates. The number of computer is growing rapidly every year. This rapid growth of number of computer each year leads to the security concern. The computer security is vital because the adversaries are always looking for opportunity and vulnerability to challenge the security. According to [1], security is not just the notion of being free from danger, as it is commonly conceived, but is associated with the presence of an adversary. The presence of adversary who is always seeking to obtain sensitive and private personal information, threat the system, and use it against its legitimate use makes the computer security paramount.

(a) Desktop Operating Systems (b) Mobile Operating Systems

Figure 1. Market Share of Desktop and Mobile Operating Systems (StatCounter Global Stats, 2017)

The Operating System (OS) is a program comprises with million lines of coding that acts as an intermediary between a user of a computer and the computer hardware. There are lot of OS running on the computer, but only three of them are widely used, including Windows OS, Mac OS and Linux OS. Based on Figure 1(a), it can be seen that Windows OS is dominating the computer OS at 83.93%, Mac OS came at second with 10.29% and Linux OS at third with 3.76%. This means that Windows OS is exposed to lot of vulnerability because of it widely used. In [2], the author stated that the operating systems with vast number of users like Microsoft Windows or Linux is exposed to the malicious code attacks which comes from man-in-the-middle-attack (MITM).

For mobile operating systems, Android and iOS are dominating the operating systems in smartphone. Figure 1(b) shows that with 69.68% Android is currently leading the race leaving iOS at second with 19.35%. In the case of smartphone, Android is an open-source platform where there's no royalty's fee to develop for the platform. The source-code is there on the internet, and everybody can use it freely without violating any copyright acts. As mentioned in [3], the whole source code of Android Operating Systems is free to use which lying under the General Public License version 2 (GPLv2) where any improvisation on the source-code by any third-party developers must be remained under the open-source licensing agreement terms. Likewise, the Android framework which is distributed under Apache Software License (ASL/Apache2) permits the open and closed-code that have been derived from the original source code [3]. Because of this open-source code practices by Android and it widely used, it exposes to numerous malicious threats. In Cisco 2014 Annual Security report, they reported that the significantly rapidly growth of number of Android's users makes it becomes favourable target of malware attacks [4].

Computer security can be perceived at two different perspectives: computer that is connected to the network and the one who does not. The primarily concern about the security is the computer which is connected to the network since most of the computers in this era are connected to the network. Secure computing is achieving the goals of security in information environment from threats; the goals are confidentiality, integrity, availability and resilience [1]. Confidentiality is about retaining either personal data or organizational data exclusive. Integrity is preserving the system or the data from being altered or changed illegally by non-authorized users [5]. Availability means being able to use the system as anticipated. And resilience is what allows a system to endure security threats instead of critically failing.

Kali Linux is the most popular software package for penetration testing and security audit, in which many books have been written in this topic [6-10]. The objective of this paper is to provide a comprehensive review on the security penetration and security audit using Kali Linux. Section 2 describes the penetration testing, while Section 3 explains about the role of security analysis. Section 4 describes security audit, while Section 5 describes the setup of Kali Linux. The last section concludes this paper.

2. PENETRATION TESTING

Penetration testing is a legitimate exercise of exploiting a system with real life attacker scenario including illegal access and the practice of malicious activities. The process of penetration testing starts from identify the system's vulnerabilities, stage an exploitation, vulnerabilities' discovery and reporting, and dissolving the vulnerabilities that can cause harm to the system. According to [11], the process of penetration testing could illustrate the level of severity could be done on the system during the real life attack thus help the organization to prevent it before it is too late. There are numerous attacks that can cause damage to one organization's system. According to Open Web Application Security Project (OWASP) there are top 10 vulnerabilities that been leaving severe impact to web application and four of them including SQL injection, Cross Site Scripting (XSS), Local File Inclusion (LFI), and Remote File Inclusion (RFI) as mentioned by [11].

2.1 SQL Injections (SQLi)

Structured Query Language (SQL) is normally used as intermediate between web applications and database. SQL responsible in taking care of request and retrieve of data from client side to database and back and forth. According to [12], SQL plays a significant role in the Relation Database Management System (RDBMS) due to its simplicity and straightforwardness. SQL injection occurs when an attacker injects the SQL queries with new parameters into the input values to enter and gain access to the database unauthorized. The attack occurs when keywords or operators obtain from the user by the application server executed to the compromised updated SQL query.

2.2 Cross Site Scripting (XSS)

XSS is a technique where the JavaScript, VBScript, ActiveX, Flash or HTML is planted along with the malicious XSS link. When the infected link is executed or loaded, the attacker will obtain root privilege

and all the sensitive data and information will be left exposed to the attacker. In [13], the authors stated that there are distinct numbers of way approached by the attackers like hijacking the session, taking advantage of user's privileges by stealing data, posting ads in hidden IFRAME and pop-up to encode the malicious code to maintain the originality of the infected code therefore it cannot be detected by the users. XSS could be initiated through sending email, stealing user's cookies, sending an unauthorized request, and XSS attack in comment field.

2.3 Local File Inclusion (LFI) and Remote File Inclusion (RFI)

Local File Inclusion (LFI) is an attack where the attacker executes commands in some files located in the web server after exploiting the web applications. The word "Local" referred to the location of the file executed, which is inside the web server. The exploitation occurs due to misuse of prebuilt programming functions/methods other than invalid parameter chose by the user [14]. A dynamic file inclusion mechanism is approached to counter this vulnerability.

Remote File Inclusion (RFI) occurs when any type of user input is remotely accepted without going through any proper validation and sanitization by the server. RFI and LFI are not much different where RFI includes dictionary writeable, i.e. the path of certain file included as input received by the webpage is not comprehensively inspected [14]. This RFI attack is severely dangerous as personal and sensitive data could be steal and manipulated and, could paralyze the web server operation.

2.4 Distributed-Denial-of-Service (DDoS)

Distributed Denial of Service (DDoS) attacks are fatal. In this type of attack, legitimate users would not get access to a specific network resource because the network and services have been flooding with false service request. According to [15, 16], the DDoS attacks can be launched either by disturbing a legitimate user's connectivity or disturbing legitimates user's services.

2.5 Man-in-the-Middle (MITM)

MITM attack is type of attack where it violates two of security goals discussed earlier; confidentiality and integrity. In this attack, the attacker eavesdrops the data flows in communication link between endpoints. As mentioned in [17], in common MITM attack, three parties are involved; two victims that are communicating with each other and an attacker, in which the attacker exploits the communication channel between two victims and has the ability to manoeuvre the information exchanged. In [18], the authors stated that the MITM attack is including intercepting emails, logins, chat messages, cutting a victim's internet connection; and many others.

2.6 Zero-Day Vulnerabilities

Zero-Day vulnerabilities refers to the security risk which could be exploited by hacker but has yet known by the software vendor [19]. Once the vendor learns of the vulnerability, the vendor will usually create patches to mitigate it. One of the most notorious example of zero day attack is Stuxnet [20] which uses 4 Windows operating systems zero-day exploits. Stuxnet commanded the PLCs to speed up and slow down the spinning centrifuges, destroying some of them, while sending false data to plant operators to make it appear the centrifuges were behaving normally. Based on this Stuxnet attack, it is very significant to keep the integrity at all cost.

3. SECURITY ANALYST

Security analyst does comprehensive analysis based on the data gathered in the event of attack or attempt of attack or annual report to identify the vulnerabilities and holes in the systems. A comprehensive analysis means that, every piece of information and information gathered must be inspected, evaluated, investigated, and studied profoundly. Not only that, a security analyst must be able to do research on past cyber-attack events and being able to relate it to current cyber-attack. However, these methods are no longer enough to stop the attacks and considered obsolete. According to [21], a new age of war between attackers/hackers and security analyst has emerged where both parties employ new complicated schemes to disorient each other. Hence, new strategies are approached to prepare comprehensive forecast of imminent threat on important utilities; known as Predictive Cyber Situational Awareness (SA). These approaches involved deep knowledge on system weakness and how it could be used to abuse the system.

Security analyst is considered demanding job nowadays. The needs of having secure system both for individual and organizational uses make the security analyst is considered one of important job in these fast-evolving technologies. Security analyst or cyber defense analyst role dominating the operational aspects of preserving the security of the organizational. The capabilities of security analyst in examining the current and

incoming threats to the organization making the advantages' list of security analyst keep going on and on. Having said that, there are seven questions that security analyst needs to answer regarding the security level of an organization in respect to Cyber Situational Awareness framework as described in [21] and shown in Table 1.

Table 1. Seven questions in respect to Cyber Situational Awareness Framework [21]

No.	Questions	Explanations
1	Current situation	Is there any ongoing attack on the system? If there any, what is the level of severity of the attack and where is the attacker located?
2	Impact	How does the attack affect the organization or mission? Can the damage be assessed?
3	Evolution	How the attack is evolving? Can all the step of the attack be traced?
4	Behaviour	What are the expected behaviour of the attackers? What are their strategies in attacking the system?
5	Forensic	What is the objective of the attack? How did the attack deployed on the system?
6	Prediction	Can the future attack be predicted based on the current situation?
7	Information	What sort of information sources can be relied on? How is the quality of the information?

4. SECURITY AUDIT

In auditing process, the system security objectives and its implementation are screened and then verified. In [2], the author established that the security audits are responsible in evaluating the vulnerabilities found in the systems and find alternatives to reduce the area of vulnerabilities' exposure. The audit process involved log files analysis where the log files are useful for recording the events and timelines of the running processes. The processes of screening big and long log files are very time-consuming. Thus, with aid of tool like general audit software (GAS) is significant in helping such time-consuming tasks involving retrieval and analysis of significantly big and large data[22]. There are numerous number of popular tools used in auditing security and one of them is Lynis which can be downloaded at https://cisofy.com/lynis/. Lynis is an Open Source Unix-based system tools aims in scanning security aspect rather than scanning for vulnerabilities. Figure 2 illustrates the interface of the Lynis auditing tools.

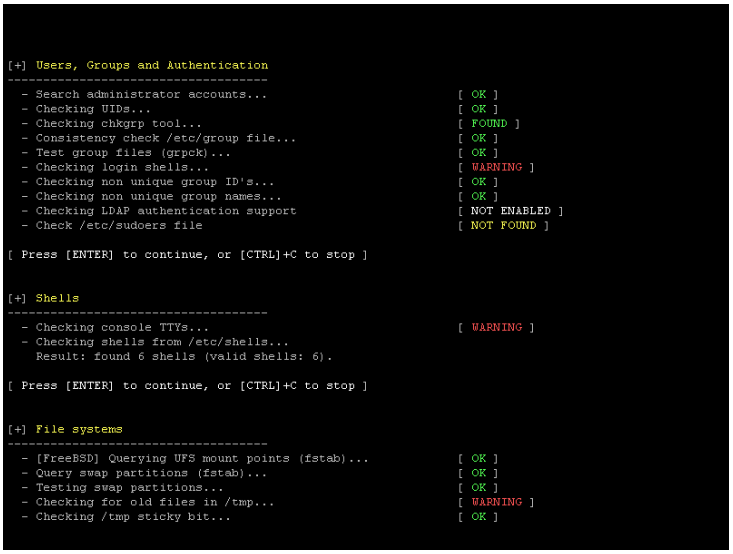


Figure 2. Lynis Security Auditing Software

5. KALI LINUX SETUP

This section describes the brief history of Kali Linux, installing and setup Kali Linux on the virtual machine, and installing a vulnerable server.

5.1 History of Kali Linux

Kali Linux is a Debian-derived Linux distribution and it is a freeware and can be downloaded for free at http://www.kali.org as illustrated in Figure 3. Previously, Kali Linux was knows as BackTrack which merged three different Linux distribution, including IWHAX, WHOPPIX, and Auditor [6]. Kali Linux version 1.0 was released on March 2013. As of March 2018, the latest version is 2018.1 and is compatible for i386, amd64, armel and armhf machine architecture, even on Raspberry Pi [23]. Kali Linux has now more than 600 penetration testing tools, free, Filesystem Hierarchy Standard (FHS) compliant, and wide-ranging wireless device support [24]. Kali Linux is the most popular penetration testing platform as stated in [19].

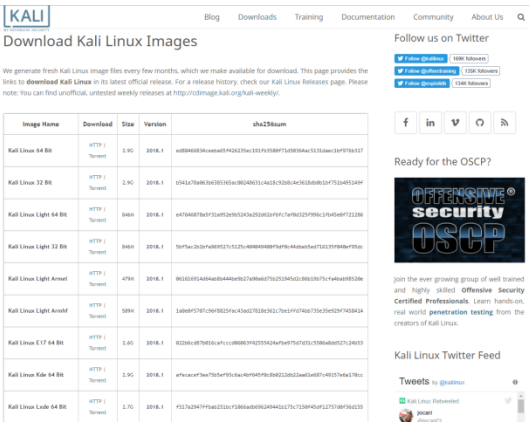


Figure 3. Kali Linux Official Website

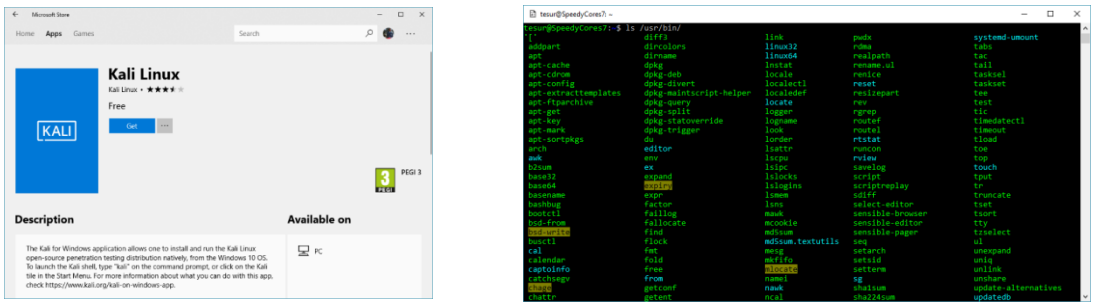


Figure 4. Kali Linux on Windows 10

The installation of Kali Linux requires a minimum 20GB of disk space and 1GB RAM. Kali Linux can be installed using two ways: USB bootable drive or DVD drive. In this paper, we will boot Kali Linux on virtual machine and attack the main machine (Windows 10). As of February 2018, Kali Linux can be installed and used on Windows 10 directly as part of Windows Subsystem for Linux (WSL) as shown in Figure 4.

5.2 Installing Kali Linux on Virtual Machine

In our research, Kali Linux will be installed on the VMware virtual machine. VMware is a software which allowed a virtual machine (which uses some CPUs, RAM and storage from the main machine) to be operated like normal computer. That means there are two operating system running simultaneously on a machine. Therefore, in this research two operating system (Windows 10 host and Kali Linux virtual machine) will run at the same time. Figure 5 shows the configured Kali Linux virtual machine, in which it uses 4 CPU Cores, 2 GBytes of RAM, and 60 GB of harddrive. The download page of Kali Linux website offered Kali Linux 64 bit VMware VM, 32 bit VMware VM PAE, 64 bit and 32 bit Vbox.

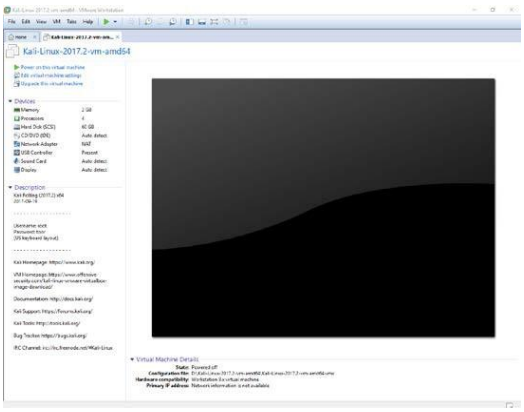


Figure 5. Kali Linux on VMware Virtual Machine

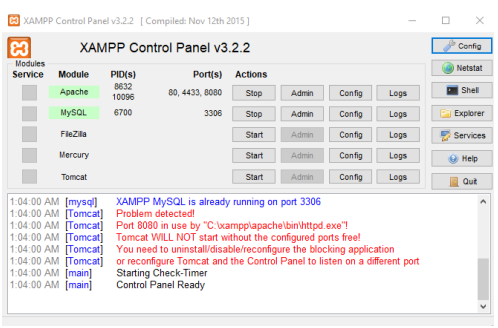
Kali Linux consists of hundreds of pre-built tools. The tools are divided into sections to its functionality and utilities. Each section carries out different task but with same objective; to do penetration testing. The followings are the sections the tools divided into [6]:

- *Information gathering*: Important tools to collect information about the target
- *Vulnerability analysis*: Tools for scanning weakness in the system
- *Wireless attack*: Tools carry out attack on wireless protocol
- *Web application*: Used to attack Web Site, Web Server and Web Application.
- *Sniffing and spoofing*: Tools used to monitor and capture the network traffic and manipulating it
- *Exploitation tools*: Tools used to identify the vulnerabilities in a system
- *Forensic tools*: Focused on monitoring and analyzing system's network traffic and program.
- *Stress testing*: Tools used to measure how much a system can handle a heavy load of network traffic and information (DDoS attack).
- *Password attacks*: Deal with brute force of a system; identifying, finding and cracking password of a system
- *Maintaining access*: Used to keep the access on the system that has been exploited i.e. backdoor.
- *Reverse engineering*: Identify how a system is produced so it might be duplicated or changed
- *Hardware hacking*: Focused on gaining access over small electronic devices like android and Arduino.
- *Reporting tools*: Used for post penetration testing; gather information and provide proper documentation to report on the organization

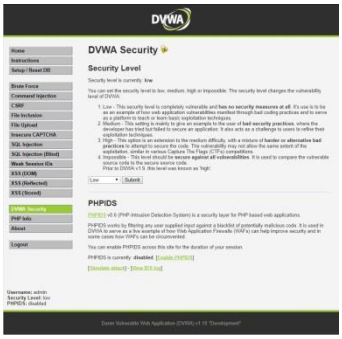
However, there are still lot of Open-Source tools that are available online and can be downloaded and installed on the Kali Linux system. Most of them are accessible in GitHub site. Command git clone execute in the Kali Linux terminal is used to download the tools from the GitHub.

5.3 Installing a Vulnerable Server

To experiment with penetration testing following the ethical hacking guideline, we must do all the penetration testing on our own environment. That been said, we must not do penetration testing on private webserver or private firewall machine. Hence, we need to setup a simple webserver for the purpose of penetration testing. A software called XAMPP server is installed on the main machine (Windows 10) which is simple and useful. XAMPP stands for X – cross platform, A – apache server, M – Maria DB, P – PHP, and P – PERL, as shown in Figure 6(a).



(a) XAMPP Control Panel



(b) Setting DVWA Security Level

Figure 6. XAMPP Control Panel and Setting DVWA Security Level

By completing the installation of XAMPP server, we can now proceed to creating our own website to be attacked for. However, there is a tool called Damn Vulnerable Web Application (DVWA) that save us from spending time on creating real website and webserver. XAMPP is compulsory in order for DVWA to work. DVWA is an open source tools which can be easily downloaded from http://www.dvwa.co.uk/. DVWA provides the environment for penetration testing for the most popular web attack like SQL injection, XSS and Brute Force. The most interesting part of the DVWA is that the security level of the website and webserver can be modified based on the intended experiment. It can be set to four level of security: low, medium, high and impossible as illustrated in Figure 7(b). In this research, we set the security level to low, in which it is completely vulnerable and has not security measures at all.

6. CONCLUSIONS AND FUTURE WORKS

This paper has presented a review of penetration testing, security analysis, and security audit. On the penetration testing, we reviewed the most popular techniques including SQLi, XSS, LFI, RFI, DDoS, MITM, and zero-day vulnerabilities. On the other hand, Kali Linux is the most popular penetration testing and security audit platform with advanced tools to detect any vulnerabilities uncovered in the target machine. Brief history of Kali Linux has been presented, along with the setup and installation. For testing purpose, we have installed and configure vulnerable server. Further research including simulated attacks to vulnerable server on both web and firewall system.

ACKNOWLEDGEMENT

The authors would like to express their gratitude to the Malaysian Ministry of Higher Education (MOHE), which has provided funding for the research through the Fundamental Research Grant Scheme, FRGS14-139-0380.

REFERENCES

[1] P. W. Singer and A. Friedman, *Cybersecurity: What everyone needs to know*, Oxford University Press, 2014.
[2] R. R. Brooks, *Introduction to Computer and Network Security: Navigating Shades of Gray*, CRC Press, 2013.
[3] J. Annuzzi Jr, L. Darcey, and S. Conder, *Introduction to Android application development: Android essentials*, Pearson Education, 2014.
[4] D. J. Tan, T.-W. Chua, and V. L. Thing, "Securing android: a survey, taxonomy, and challenges," *ACM Computing Surveys (CSUR)*, vol. 47, pp. 58, 2015.
[5] B. Kesler, "The vulnerability of nuclear facilities to cyber attack; strategic insights: Spring 2010," *Strategic Insights, Spring 2011*, 2011.
[6] L. Allen, T. Heriyanto, and S. Ali, *Kali Linux–Assuring security by penetration testing*, Packt Publishing Ltd, 2014.
[7] J. Muniz, *Web Penetration Testing with Kali Linux*, Packt Publishing Ltd, 2013.
[8] R. S. Patel, *Kali Linux Social Engineering*, Packt Publishing Ltd, 2013.
[9] R. W. Beggs, *Mastering Kali Linux for advanced penetration testing*, Packt Publishing Ltd, 2014.
[10] C. P. Schultz and B. Perciaccante, *Kali Linux Cookbook*, Packt Publishing Ltd, 2017.
[11] P. S. Shinde and S. B. Ardhapurkar, "Cyber security analysis using vulnerability assessment and penetration testing," in *Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), World Conference on*, pp. 1-5, 2016.

[12] R. P. Karuparthi and B. Zhou, "*Enhanced Approach to Detection of SQL Injection Attack*," in Machine Learning and Applications (ICMLA), 2016 15th IEEE International Conference on, pp. 466-469, 2016.
[13] M. D. Ambedkar, N. S. Ambedkar, and R. S. Raw, "*A comprehensive inspection of cross site scripting attack*," in Computing, Communication and Automation (ICCCA), 2016 International Conference on, pp. 497-502, 2016.
[14] A. Begum, M. M. Hassan, T. Bhuiyan, and M. H. Sharif, "RFI and SQLi based local file inclusion vulnerabilities in web applications of Bangladesh," *in Computational Intelligence (IWCI), International Workshop on*, pp. 21-25, 2016.
[15] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE communications surveys & tutorials*, vol. 15, pp. 2046-2069, 2013.
[16] O. S. Nagesh, T. Kumar, and V. R. Vedula, "A Survey on Security Aspects of Server Virtualization in Cloud Computing," *International Journal of Electrical and Computer Engineering*, vol. 7, pp. 1326, 2017.
[17] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, pp. 2027-2051, 2016.
[18] M. Denis, C. Zena, and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies," in *Systems, Applications and Technology Conference (LISAT)*, 2016 IEEE Long Island, pp. 1-6, 2016.
[19] P. Engebretson, *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*, Elsevier, 2013.
[20] K. Zetter, *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*, Broadway books, 2014.
[21] A. Kott, C. Wang, and R. F. Erbacher, *Cyber defense and situational awareness*, vol. 62, Springer, 2015.
[22] N. Mahzan and A. Lymer, "Examining the adoption of computer-assisted audit tools and techniques: Cases of generalized audit software use by internal auditors," *Managerial Auditing Journal*, vol. 29, pp. 327-349, 2014.
[23] N. B. Al Barghuthi, M. Saleh, S. Alsuwaidi, and S. Alhammadi, "Evaluation of portable penetration testing on smart cities applications using Raspberry Pi III," in *HCT Information Technology Trends* (ITT), 2017 Fourth, pp. 67-72, 2017.
[24] KaliLinux, "What is Kali Linux?," [https://docs.kali.org/introduction/what-is-kali-linux], Retrieved on: March 2018.

BIOGRAPHY OF AUTHORS

Teddy Surya Gunawan received his BEng degree in Electrical Engineering with cum laude award from Institut Teknologi Bandung (ITB), Indonesia in 1998. He obtained his M.Eng degree in 2001 from the School of Computer Engineering at Nanyang Technological University, Singapore, and PhD degree in 2007 from the School of Electrical Engineering and Telecommunications, The University of New South Wales, Australia. His research interests are in speech and audio processing, biomedical signal processing and instrumentation, image and video processing, parallel computing, and information security. He is currently an IEEE Senior Member (since 2012), was chairman of IEEE Instrumentation and Measurement Society – Malaysia Section (2013 and 2014), Associate Professor (since 2012), Head of Department (2015-2016) at Department of Electrical and Computer Engineering, and Head of Programme Accreditation and Quality Assurance for Faculty of Engineering (since 2017), International Islamic University Malaysia. He is Chartered Engineer (IET, UK) and Insinyur Profesional Madya (PII, Indonesia) since 2016.

Muhammad Kassim Lim has completed his B.Eng. (Hons) degree in Computer Engineering from International Islamic University Malaysia (IIUM) in 2018. His research interests are in computer security, vulnerability assessment, penetration testing, and open source security analysis.

Nurul Fariza Zulkurnain received the B.Eng. degree in Computer and Information engineering from International Islamic University Malaysia, in 2002. She obtained her MSc in Systems Engineering with IT Applications from Cardiff University in 2005 and Ph.D. degrees in Computer Science (Data Mining) from the University of Manchester in 2012. In 2002, she joined the Department of Electrical and Computer Engineering, International Islamic University Malaysia, as a Lecturer. Since December 2012, she is currently with the Department of Electrical of Computer Engineering, International Islamic University Malaysia, as an Assistant Professor. Her current research interests include data mining, information security, neural networks, machine learning, and IoT.

Mira Kartiwi completed her studies at the University of Wollongong, Australia resulting in the following degrees being conferred: Bachelor of Commerce in Business Information Systems, Master in Information Systems in 2001 and her Doctor of Philosophy in 2009. She is currently an Associate Professor in Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia. Her research interests include electronic commerce, data mining, e-health and mobile applications development.