NETWORK SECURITY SYSTEMS AND ETHICAL HACKING

Table of Contents

Chapter 2: Literature review

2.1 Introduction

The advancement of science and technology has given tremendous pace to the business process. However, this has lead to various developments in the firm along with that it has brought some vulnerability as well. In recent time business data are mostly stored clouds and the hard drives. Hence the corporations and the individuals are required to keep their network secure against the data breaching through the hacking related issues. Hence, groups of professional, who are adept at the data breaching related issues and can resolve the situation, have emerged as the part of organizational and individual data protection. This process has been known as ethical hacking which is being done by the ethical professional in order to deploy the potential advantage of the technology in the positive approach.

Thus, in this particular research, the importance of the ethical hacking concerning business opportunity along with various implication of the ethical hacking has been considered as the subject to be studied. In addition to this, the core concept of the ethical hacking process and different penetration techniques into the networking sites have been described in this specific part of the study. Moreover, the importance of the ethical hacking and the issues related to the process has also been described in depth. Entire study has been summarized in the concluding part along with the germane discussion regarding the literature gap analysis.

2.2 Conceptual Framework

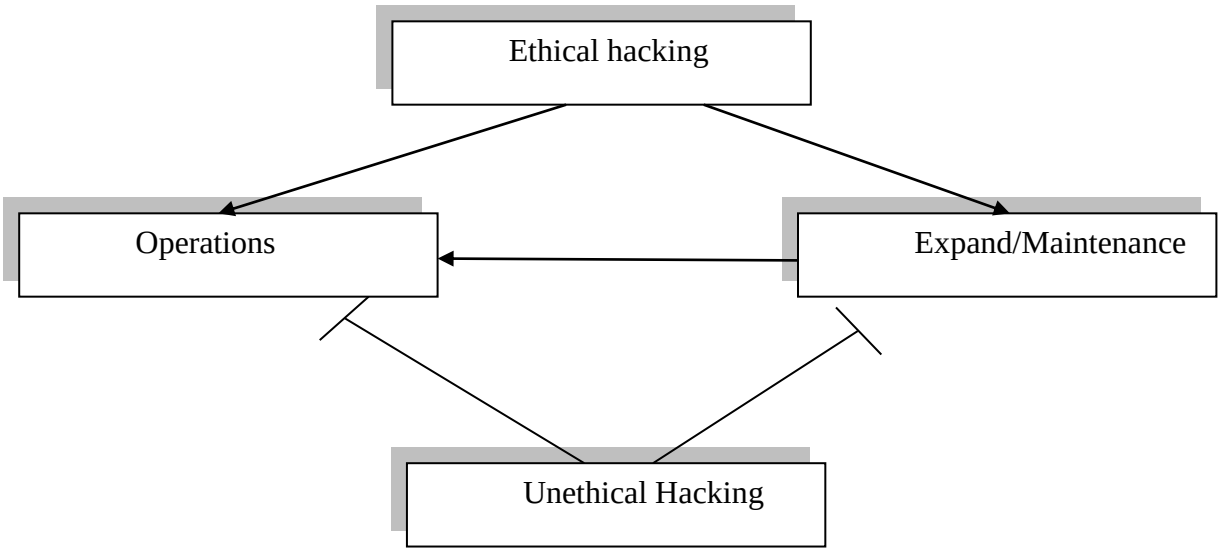

Figure 1: Conceptual framework

(Source: Created by author)

2.3 The concept of ethical hacking

As opined by Taylor *et al.*, (2014) hacking of data can be defined as the unauthorized access to the user account with an objective to get confidential information which has been barred by the user from accessing in public. Thus, the primary concept of hacking can be mentioned as unethical. However, ethical hacking is the term which has been coined in order to deal with the real time problems created by the hackers with ill motive. As described by Coleman, (2013) ethical hacking provides access to the data which has the reason to decode it for the greater benefit of society and a human being or the proper analysis of the security. ***For example,*** an ethical hacking process can be deployed by the national or regional investigating agencies regarding decoding any particular data from a target network for the greater benefit of the society. In contrast Berger and Jones, (2016) suggested that ethical hacking can also be described as the measure to analyze the level of security provided by the specific networking panel. Thus, with the help preexisting knowledge regarding the weakness of the network, a further security system can be arranged. Hence this can be mentioned as another important aspect of the ethical hacking.

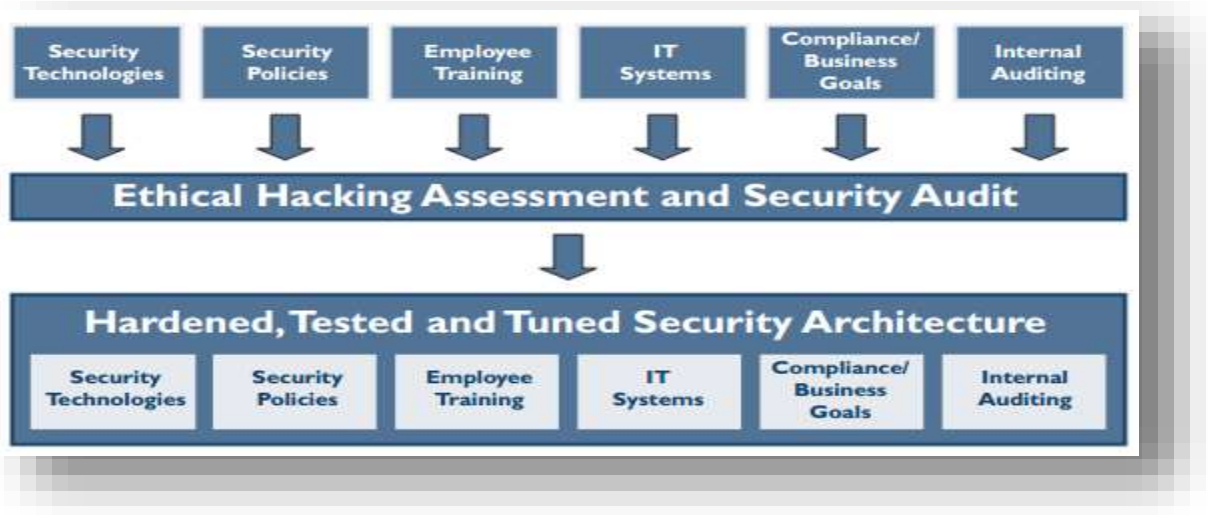

Figure 2: Role of ethical hacking in organizational security analysis

(Source: Berger and Jones, 2016)

Ethical hacking involves several different components and the vast range of testing capability of the existing security model of the networks. As described through the pictorial depiction it can understand that the ethical hacking strive to corroborate the safety of the data while analyzing the gaps and the probable flaws through unethical hacking may proceed, as stated by Summers *et al.*, (2013). This ethical hacking also involves the automated tools and the manual techniques along with the intense help of the existing the networking sites, as opined by Kallberg, (2015). This may also help in the systematic review of the database and network security, which is needed to be maintained and updated with the regular intervals for better protection of the data from cyber criminals and the unethical hackers as well (Summers *et al.*, 2013).

Figure 3: List of certification required for ethical hacking

(Source: Berger and Jones, 2016)

2.3.1 Different tools of ethical hacking and requirement of the process

As per the views of Warren and Leitch, (2016) there are several organization has come up with the group of ethical hackers who can invade the security systems and the existing firewall of the organizational network or individual devices connected to the internet. This can be done through the simplest form like inserting a bug in the system or disrupting the entire firewall of the organization while using more complex penetration processes, which have been discussed in the following section of this study.

There are several services which are provided by the ethical hackers, which may include the following:

External network hacking: Through this approach the ethical hackers strives to hack the external networks like the routers , servers and the service providers as well, as described by Pleban *et al.*, (2014). This approach helps identifying the external vulnerabilities of the network.

Internal network hacking: Internal hacking testing is needed to be done in order to secure the network from internal network, As opined by Gomzin, (2014) if any of the employee or the stakeholders of the business can strive to disrupt the security system , then the internal network is the best aperture to upload the virus or bug. Thus, hacking of the internal server and associated network can also help in preventing the network from unexpected scenarios due to insider attacks, as suggested by Behera and Dash, (2015).

War dialing: Through this approach the modems through which the internet calling is being done are hacked and checked for the vulnerability.

Wireless LAN hacking: In this particular approach the tester strives to understand the probable flaws in the W-LAN connected with the system. W-LAN is the sources through which the hackers can get enter into the system (Kim, 2015). Thus, ethical hackers also strive to probe it manually as a part of ethical hacking services.

Trashing: In this case, ethical hackers make an effort to instigate the garbage and the trash files. It is possible that the sometimes the system is already being hacked covertly while the pen-testing is being done. As suggested by Huang, (2015) in this situation the specific files to be hacked can be renamed with a garbage file and can be moved into the trash section. Thus, the only way left for the ethical hackers to make an intensive research through the trash file for the ultimate recovery of the infected system (Rathod and Deshmukh, 2013).

These all techniques are utilized by the ethical hackers which are very necessary for the network related to risk management in the operation aspects of business regardless of the fields. Due to globalization the global market has opened its door to participating countries in a vast number, as mentioned by Robertson, (2012). Thus, increasing business opportunity is also ushering the sharp competition in which preserving the confidential organizational data is

becoming a chief threat when almost every organization is using the cloud based networking and remote operations. Subsequently, the needs of the ethical hackers have gone up with the time. As defined by Le Blanc and Freeman, (2016) these ***honest criminals,*** the ethical hackers, are like the army having positive motive which has the power to destroy the entire system but only deploys it to protect. As corroborated by Sanger *et al*., (2013) in 1996 US general office had received the data that almost 250,000 attacks has been attempted by the outside hackers to contaminate the network. These attacks have been discouraged and avoided as well only by the sincere efforts of ethical hackers employed by the US state general (Pence, 2015). Different attacks have been made which involves the ***fraudulent email attachment technique***, ***bug uploading, firewall disruption, entering through a proxy server in the network while concealing the IP address***. These can be described as the possible ways to enter a secure network. Detailed description of the process along with the specific model based theory has been provided in the following section.

2.4 Various types of hacking attacks in networks

In today's scenario there are several hackers are present on the internet, who are striving to erode away the security systems of the internet based computing system. This can lead to the data breaching, and the may also result in the disruption of the country's legal framework as well. Thus, it is very important to secure the data that have the potentials to become subject of threat depending on vulnerability. There is various stealth attacks have been already identified by the proficient pen-tester. For example, in ***1990*** the ***Microsoft Excel macro virus*** have been randomly deployed on the Internet which changed the zero in the excel sheets with capital 'O' (Chen *et al.,* 1999). It resulted in the random conversion of the number sheets into the text labels and generated trillions of bad data and mismatch in the balance sheets. That was a renowned case of stealth attack, for which the world has already suffered. Among the several attack style few has been described here in brief:

Fake wireless access point: It is one of the easiest ways of hacking seen over the internet. In this process the hacker provides fake wireless network, which can connect the user in minutes may or may not require a password. Through this approach the user system can be hacked and the data become vulnerable. It can then snatch away the saved password in the

systems and the user accounts in various networks can be in control of the cyber criminal in no time, without giving a slightest notification to the user.

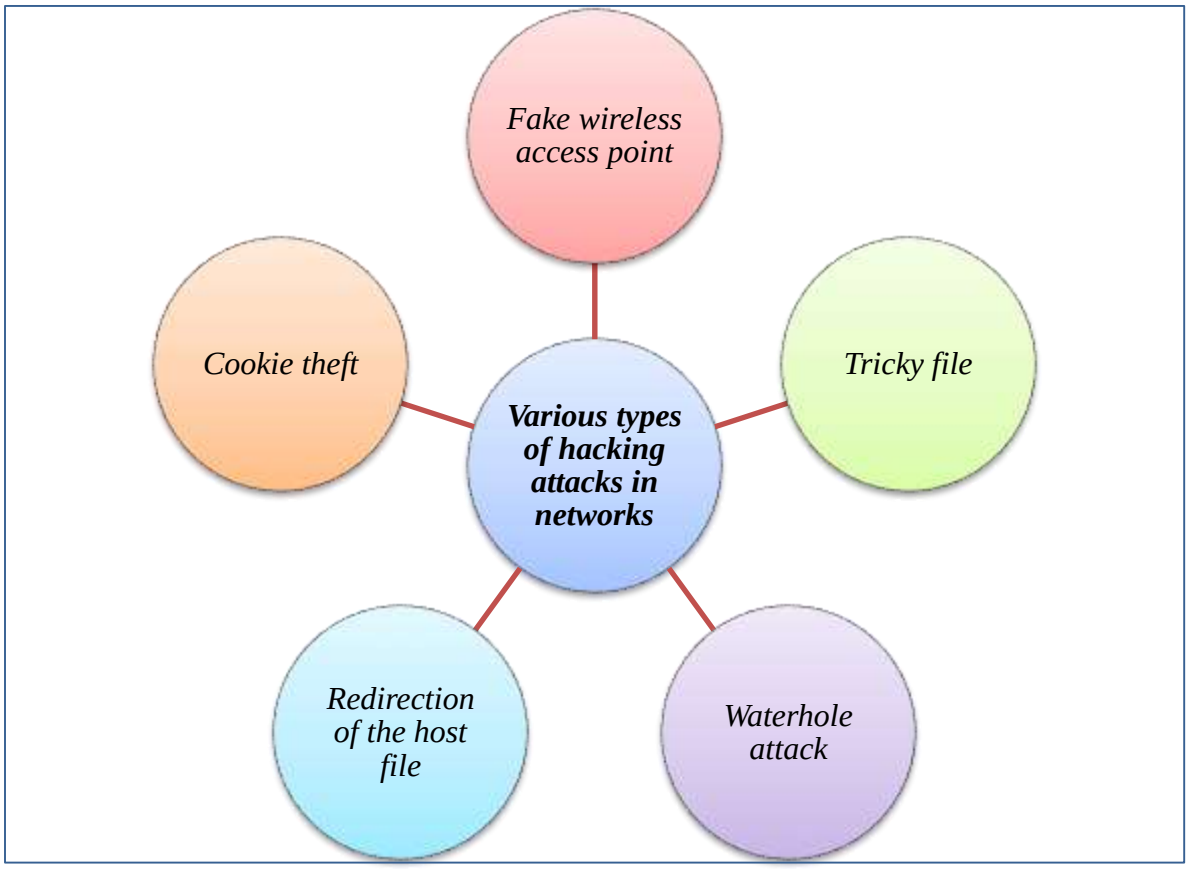

Figure 4: Different types of network attacks

(Source: Monte, 2015)

Cookie theft: Whenever roaming on the internet, it is possible that the various cookies may pop up in the browser's window. Some of them which are not from authenticated source may create severe issues for the users by hacking the data of that specific system. As opined by Ihsan and Saghar, (2016) this can be known as the bug uploading in the user system. ***For example***, in 2011 a special cookie was labeled as BEAST in the Firefox browser, which was efficient in connecting the user system to the hacker's network.

Tricky file: Some hacker uses this process to lure the users. In this case, the tricky file is named according to the browsers most visited sites and then strive to penetrate the entire firewall security of the computer system. For example, if any user uses the Netflix frequently for

watching movies, then the hacker might produce a file named as ***Netflix.zip.exe***, and if the user downloads this particular file, then the hacker gets the remote access of the specific computer system along with access to all confidential data.

Redirection of the host file: In this approach, a remote computer with DNS server plays the role from the hacker's part. As described by Robinson and Sullivan (2015) redirection of the host file in the different IP address is the key to hacking the data. In most of the cases, the file location looks similar in primary step, then whenever the user strive to save the file in the specified location the computer directly connects to the infected DNS server and the two copies of the file gets saved simultaneously. One of the copies gets save directly into the hackers system.

Waterhole attack: This is the most innovative way of hacking the data, in which the data is being hacked from the user when they are more relaxed situation Krombholz *et al.*, (2015). ***For example,*** in this approach, the hackers target the coffee shop or the restaurant of any organization, where the employees remain mostly relaxed and less concerned regarding their data security related aspects. Now the hacker provides a fake wireless connection or WAP network, which can be connected to the user's system, and the system is being hacked instantly. After that when the employee gets into the working area and somehow connect their device to the server network, the server network also gets exposed to the hacker's system and confidential organizational data can be hacked.

2.6 Concept of penetration techniques

As opined by Steinmetz, (2016) penetration testing which is also known as pen-testing in the professional fraternity is the process through which the system vulnerability can be comprehended. It is a methodical process that helps in identifying the possible loopholes of the system and the associated network. In the more tangible expression, it is the professional exploitation of the net work security to analyze the possible vulnerability of the system. Engebretson, (2013) described that pen-testers are also hackers who have the ability and expertise to invade the authorization of a system, just the ethical stringency is the fine line between the cyber criminal and the ethical hackers. Thus, it can be mentioned as the way of

analyzing the system vulnerabilities through the eye of an expert hacker who strive to identify the possible threats and resolve it rather than taking unethical advantage of it.

Rushing *et al.*, (2015) suggested that this pen-test can be done through the various automated software, rather than involving any human individual which can become a bigger risk as well. However, Kim *et al.*, (2014) argued that this is also evident that data hacking is an art and has endless ways to find the possible crack in the system, which can not only be regulated through software which checks the regular parameters only. Thus, it is important to involve an expert a human mind for efficient data tracking and resolve the system vulnerabilities.

2.6.1 Different types of the penetration techniques and vastness of usage

Penetration techniques can be classified three different kinds which have been described below in brief:

Black Box Testing (BBT): This testing is done while providing little or no information to the tester regarding the vulnerability of the system. In this approach the tester applies the brute force and run trial and error method to break into the system, like an external; hacker, as suggested by Duchene *et al.*, (2014). Hence it may take a longer time to be completed. Mostly automated process is being used in this approach.

White Box Testing (WBT): In contrast with the BBT, white box testing methods allows the tester to have entire information regarding the exposed vulnerability of the system in details. Antunes and Vieira, (2014) has mentioned it as the ***clear box approach*** as well. This approach helps in the classification of the system vulnerabilities while analyzing the software codes and debugger's report.

Grey Box Testing (GBT): This the mixed approach, where the tester has the partial knowledge regarding possible vulnerabilities in the system and depending on intensive knowledge the tester strive to understand which are the possible source of security holes through which data can be hacked.

Type of testing	Advantages	Disadvantage
BBT	Mostly provides real world results along with less cost and risk.	The most intensive effort required.
WBT	Provides holistic analysis and efficient results	Larger project volume and costly.
GBT	The best process provides the combination of black and white box approach.	Rigorous and meticulous project planning required

Table 1: Comparative analysis of the penetration testing processes

(Source: Duchene *et al.*, 2014)

As far as the real world usage are concerned, a white box and gray box techniques are mostly utilized due to the through approach and cost effective measures provided by that two approach. Black box method is also used in the case of the high-security area which has been secured through the pen testing at every possible level, as suggested by Rushing *et al.*, (2015).

2.6.2 Advantages and disadvantages of the penetration techniques

As of now the intense discussion regarding the infiltration, technique has been described in details. However, these techniques are not entirely perfect and have some pros and cons as well. Penetration testing alone is not sufficient at all to understand the entire system protection while it can fix-up some major issues of the network associated with the vulnerability related aspects. The advantages and limitation of the penetration testing system are discussed below:

Advantages

- Pen-test can help in mapping different vulnerabilities of the specified network. It is quite possible that the attacks made on the system will not be identical. For example ***SQL injection*** using ***cruder method*** lures the user while making an attempt to provide the unwanted but lucrative file to the user Hanmanthu *et al.*, (2015). A specific parameter based pen-test can help in identifying the underlying weakness of the network due to which the system is getting vulnerable. Eventually, that can be fixed up.

- Classification between the vulnerabilities depending on the degree of severity can be achieved through the appropriate penetration testing method, as suggested by Agten *et al.*, (2012). Small vulnerabilities may include the weakness related to the software or coding related issues. On the other hand, bigger weaknesses are the proxy network, the fraudulent server with unauthenticated IP address which strives to enter the system through the unprotected or permeable firewall of the system, as addressed by Rathod and Deshmukh, (2013). These classifications through the pent-test may help in resolving the specific issues.
- Manual intervention based pen-test also help in identifying the special cracks in the system which not all possible to be detected through the automated security check. As opined by Rushing *et al.*, (2015) penetration testing software works on the principle of preset theory and models. Thus, it may become tough for the software to detect flaws, which is present in the system and have not been described yet through any established model. Thus, pen-test done by the ethical hackers with the manual intervention can be the best option to reduce the risk of vulnerability.
- Testing through penetration checking is also helps in strengthening a network and checks made in the regular interval are also essential for the sustainable security of the system and associated network, as opined by Engebretson, (2013). It helps in increasing the robustness of the system and meanwhile increases the security of the network.

Disadvantages

- As per the views of Lins *et al.* (2015) trustworthiness of the tester is the most important aspect. It is possible that the tester may turn the back to the organization and can become a possibly tremendous threat as well. They will know all the loop-wholes of the system and the possible flaws that remain in the network. Hence, the tester can also infect the system unless the regular checks are being made through a series of the tester. A possible solution to this problem is to select the tester from the authorized organization with proven track record and the shuffle the tester in regular interval.

- Another possible disadvantage is the selection of the testing parameters by the tester, which might lead to the unrealistic test conditions. For example, if any pen test is organized by the corporation while announcement regarding the pen-test has been done earlier then it is quite possible that the attackers will be forewarned and will try to make no mistakes in that specific time, or will plan to execute it before the pen-test. Thus, it is required to be while marinating complete confidentiality.

Depending on the discussion made in this section regarding the advantages and the disadvantages of the penetration testing process, it can be declared pen-testing is an indefensible process for the organizational data security. However, it is required to be done with proper diligence while following the stringent ethical codes of practices. In order to minimize the risks from the testers and ethical hackers itself, government and international legislative organization are required to enact special acts and the set rules for the non-compliance of the ethical codes. This approach may discourage the violation of ethical codes in pen-testing gradually.

2.7 Gap in the literature

In this particular study several network related attacks and the concept of ethical hacking to curb the practices have been described. Additionally, the in-depth reviews of the literature have also revealed the various types of the penetration testing approach in network security measurement. However, the specified mind map of the hacker not discussed in length as this was not that much relevant to the objective of the study. This analysis will reveal several data and facts regarding the appropriate way of hacking and the ways through which the unethical hackers strive to get access to the unauthorized data. Thus, it can be mentioned as the gap in the literature depending upon which future research can be conducted in this particular field of study.

2.8 Summary

In this entire study, the concept of ethical hacking and the importance of penetration level testing system have been discussed in depth. However, the brief opportunity of discussion has left the core areas untouched like the in-depth process of the data hacking and the prevention related aspects. In contrast, the advantages and the disadvantages of the ethical hacking based

pen-testing method have helped in generating practical comprehension regarding the imperativeness of ethical hacking and pen-testing. The disadvantages are quite lower in number than the advantages but are potent in doing harm to the system and associated network. Various approaches like the black, white and gray box approach of the ethical hacking and penetration system have helped in gaining knowledge regarding the hacking related aspects. Also, the gap analysis of the literature ahs also directed towards the possible area of further research in this particular field.

References

Agent, P., Nikiforakis, N., Strackx, R., De Groef, W. and Piessens, F., 2012, Recent developments in low-level software security. In *IFIP International Workshop on Information Security Theory and Practice* (pp. 1-16). Springer Berlin Heidelberg

Antunes, N. and Vieira, M., 2014. Penetration testing for web services.*Computer*, *47*(2), pp.30-36.

Behera, M.P.C. and Dash, M.C., 2015. Ethical Hacking: A Security Assessment Tool to Uncover Loopholes and Vulnerabilities in Network and to Ensure Protection to the System, *Journal of International Communication*, 11(5), pp. 173-179

Berger, H. and Jones, A., 2016,. Cyber Security & Ethical Hacking For SMEs. In Proceedings of the The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society (p. 12). ACM.

Chen, E.Y., Ro, J.T., Deng, M.M. and Chi, L.M., Trend Micro, Incorporated, 1999. System, apparatus and method for the detection and removal of viruses in macros. The Security Systems, 9(2), pp. 78-112

Coleman, E.G., 2013. Coding freedom: The ethics and aesthetics of hacking. Princeton University Press.

Duchene, F., Rawat, S., Richier, J.L. and Groz, R., 2014,. KameleonFuzz: evolutionary fuzzing for black-box XSS detection. In*Proceedings of the 4th ACM conference on Data and application security and privacy* (pp. 37-48). ACM

Engebretson, P., 2013. The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier.

Gomzin, S., 2014. Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions. John Wiley & Sons.

Hanmanthu, B., Ram, B.R. and Niranjan, P., 2015, SQL Injection Attack prevention based on decision tree classification. In *Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on*(pp. 1-5). IEEE.

Huang, C.W., 2015, September. Security system and actual operation benefit of data transmission on heterogeneous network. In *Security Technology (ICCST), 2015 International Carnahan Conference on* (pp. 165-168). IEEE.

Ihsan, A. and Saghar, K., 2016, Formal verification of a remote serial network. In *2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)* (pp. 361-366). IEEE

Kallberg, J., 2015. A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs. *IT Professional*, *17*(1), pp.30-35.

Kim, B.J., Ho, J.K. and Hwang, Y.C., 2014. Prediction of Shear Wave Velocity on Sand Using Standard Penetration Test Results: Application of Artificial Neural Network Model. *Journal of the Korean Geotechnical Society*,*30*(5), pp.47-54.

Kim, C.S., 2015. Study on the System for Prevention of Harmful Invasion with Access from Wireless LAN Access Point. *network*, *1*, p.3.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E., 2015. Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, pp.113-122.

Le Blanc, K. and Freeman, S., 2016. Investigating the Relationship Between Need for Cognition and Skill in Ethical Hackers. In *Advances in Human Factors in Cybersecurity* (pp. 223-228). Springer International Publishing.

Lins, S., Thiebes, S., Schneider, S. and Sunyaev, A., 2015,. What is really going on at your cloud service provider? Creating trustworthy certifications by continuous auditing. In *System Sciences (HICSS), 2015 48th Hawaii International Conference on* (pp. 5352-5361). IEEE.

Monte, M., 2015. Network Attacks and Exploitation: A Framework. John Wiley & Sons.

Pence, H.E., 2015. Will Big Data Mean the End of Privacy?. *Journal of Educational Technology Systems*, *44*(2), pp.253-267.

Pleban, J.S., Band, R. and Creutzburg, R., 2014, Hacking and securing the AR. Drone 2.0 quadcopter: investigations for improving the security of a toy. In *IS&T/SPIE Electronic Imaging* (pp. 90300L-90300L). International Society for Optics and Photonics.

Rathod, R.H. and Deshmukh, V.M., 2013. Roll of Distributed Firewalls in Local Network for Data Security. *International Journal Of Computer Science And Applications*, *6*(2).

Robertson, R., 2012. Globalisation or glocalisation?. *Journal of International Communication*, *18*(2), pp.191-208.

Robinson, G. and Sullivan, K., Openwave Mobility, Inc., 2015. *Routing of IP traffic directed at domain names using DNS redirection*, *Journal of International Communication*, 3(2), pp.227-259

Rushing, D., Guidry, J. and Alkadi, I., 2015,. Collaborative penetration-testing and analysis toolkit (CPAT). In *2015 IEEE Aerospace Conference* (pp. 1-9). IEEE.

Rushing, D., Guidry, J. and Alkadi, I., 2015,. Collaborative penetration-testing and analysis toolkit (CPAT). In *2015 IEEE Aerospace Conference* (pp. 1-9). IEEE.

Sanger, D.E., Barboza, D. and Perlroth, N., 2013. Chinese Army Unit is seen as tied to Hacking against US. *The New York Times*, *21*.

Steinmetz, M., 2016. Critical Constrained Planning and an Application to Network Penetration Testing. In *The 26th International Conference on Automated Planning and Scheduling* (p. 141).

Summers, T.C., Lyytinen, K.J., Lingham, T. and Pierce, E.A., 2013, September. How Hackers Think: A Study of Cybersecurity Experts and Their Mental Models. In *Third Annual International Conference on Engaged Management Scholarship, Atlanta, Georgia*.

Taylor, R.W., Fritsch, E.J. and Liederbach, J., 2014. *Digital crime and digital terrorism*. Prentice Hall Press.

Warren, M. and Leitch, S., 2016. The Syrian Electronic Army–A Hacktivist Group. *Journal of Information, Communication and Ethics in Society*, *14*(2), pp. 76-89