Network Security Analysis in the Enterprise LANs

Leonard L. Mutembei
College of Informatics and Virtual Education
The University of Dodoma
P.O.Box 490
Dodoma, Tanzania

Aloys N. Mvuma
College of Informatics and Virtual Education
The University of Dodoma
P.O.Box 490
Dodoma, Tanzania

Tabu S. Kondo
College of Informatics and Virtual Education
The University of Dodoma
P.O.Box 490
Dodoma, Tanzania

ABSTRACT
Enterprise Local Area Networks (ELANs) have been expanding following an increase in the number of staff which necessitates establishment of new offices. However, reliability and security of services provided by ELANs need to be ensured at all times to meet expectations of users. In this paper, the network security holes existing within the ELANs were investigated. Vulnerabilities and threats were critically examined in one of the ELANs. It was observed that known vulnerabilities were still around within the network. Based on the findings, the paper suggests that all software used in the networking devices need to be updated; unneeded open ports need to be closed; cache servers and security policy need to be implemented. The suggestions will ensure stability of the network during scaling out as the number of staff continues to grow.

General Term
Network security

Keywords
Network security analysis, Network Security, Network Vulnerability

1. INTRODUCTION
Internet usage has been expanding exponentially globally over the past decade. Table 1 shows the world Internet usage as of June 2012 according to the Internet World Stats [1] website. However, developing countries including Tanzania have also witnessed a sharp expansion of Internet connectivity and usage.

Table 1: Internet World Usage

WORLD INTERNET USAGE AND POPULATION STATISTICS June 30, 2012						
World Regions	Population (2012 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2012	Users % of Table
Africa	1,073,380,925	4,514,400	167,335,676	15.6 %	3,606.7 %	7.0 %
Asia	3,922,066,987	114,304,000	1,076,681,059	27.5 %	841.9 %	44.8 %
Europe	820,918,446	105,096,093	518,512,109	63.2 %	393.4 %	21.5 %
Middle East	223,608,203	3,284,800	90,000,455	40.2 %	2,639.9 %	3.7 %
North America	348,280,154	108,096,800	273,785,413	78.6 %	153.3 %	11.4 %
Latin America / Caribbean	593,688,638	18,068,919	254,915,745	42.9 %	1,310.8 %	10.6 %
Oceania / Australia	35,903,569	7,620,480	24,287,919	67.6 %	218.7 %	1.0 %
WORLD TOTAL	7,017,846,922	360,985,492	2,405,518,376	34.3 %	566.4 %	100.0 %

According to Tanzania Communications Regulatory Authority (TCRA) report [2], penetration of Internet in Tanzania has been increasing since 2005 to June, 2010 as shown in figure 1. Furthermore, the report estimated the number of Internet users in Tanzania to have reached 4.8 Million.

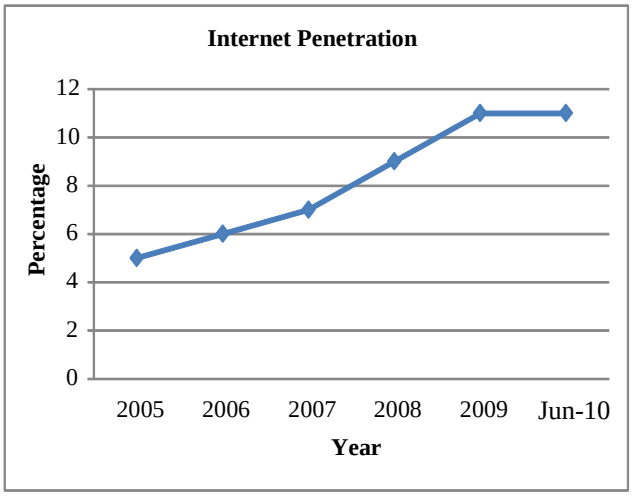

Figure 1: Internet Penetration in Tanzania

Moreover, the Internet infrastructure is becoming more complex as the number of hosts expands, thus posing security and management challenges. According to Internet Systems Consortium [3], the population of hosts on the Internet reached to about one billion by January 2014. The Internet infrastructure therefore leaves the hosts in the networks prone to attacks which may compromise confidentiality, availability and integrity of information. There is therefore an urgent need for institutions, government organizations, military and companies to prioritize security of their networks connected on the Internet as a strategy to act and fight against attacks.

Cornwall [4] argues that a hacker is simply a computer addict of any kind who loves working with the beasties for their own sake, as opposed to operating them in order to improve a company or research work. Therefore, hacking is the process of trying to make unauthorized access into computers and to explore what is there. Hence Internet connectivity has been assisting hackers on getting unauthorized access within computers connected on different networks.

Most attacks seem to target large networks like government institutions, military agencies and different organizations. According to Whittaker [5], the University of Exeter in England had been attacked by virus on its entire network. Hence the University had to shut down its network in order to handle the problem. The problem was due to vulnerability in Windows Vista which allows code to be executed remotely. This shows the possibility of other networks to be attacked by such kind of virus if appropriate security countermeasures are not implemented.

The vulnerabilities can be available due to poor network design, misconfiguration of the software or hardware, inherent technology weaknesses or end-user carelessness. Many devices have default configurations that allow some services to run without enabling. Some of default services are not vital to normal operation hence the attackers may use the loopholes found to invade the network [6].

1.1 Network Security

In the context of this work, network security can be defined as the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment [7]. A proper network security plan is developed with understanding of security issues, potential attackers, needed level of security, and the factors that make a network vulnerable to attacks [8].

Network security has to comprise with conditions and policies selected by network administrators to monitor and inhibit alteration, unauthorized access, misuse or denial of a computer network and network-accessible resources [9]. Network security is highly needed by different companies and institutions. Dowd and McHenry [10] said that most people discard security on their premises if it competes with performance which is true in most users. Most users feel bad if there is a need to do configurations about securing systems but we need to adhere with security because we are interconnected by using Internet all over the world.

1.2 Network Security Analysis

Network security analysis is the act of monitoring a network for flaws that may allow attackers from either inside or outside the network to view or intercept potentially sensitive information. There are a number of factors taken into account by a professional or specialist who is analyzing the security of a network. It may be most important for this specialist to ensure that all security components are functioning well and are up to date [11].

Network security analysis may begin with the authorization or authentication of users on the network. This is most commonly achieved by requiring a user to enter a name and password in order to log in. Because this information can sometimes be guessed or stolen by potential network intruders, an analyst will often check for factors such as password complexity. In more advanced systems, authentication may be checked through use of fingerprint or voice recognition [11].

1.3 Network Vulnerability

In order to provide the security of the network in every environment, vulnerability scanning is highly needed. Vulnerability is anything running on a computer system that could indirectly or directly lead to the breach or compromise of integrity, confidentiality or availability of services or information on the intended network [12]. Most vulnerability used to disseminate network viruses, spyware or worms then cause security problems. Vulnerable machines are the most wanted ones for the distributions of viruses and malwares. Vulnerabilities can be found on computers, switches, routers and servers within the network.

Securing available resources on any corporate or academic data network is of paramount importance because most of these networks connect to the Internet for commercial or research activities. Therefore, the network is under attack from hackers on a continual basis, so network security technologies are ever evolving and playing catch-up with hackers. Around 20 years ago the number of potential users was small and the scope of any activity on the network was limited to local networks only. As the Internet expanded in its reach across national boundaries and as the number of users increased, potential risk to the network grew exponentially [13]. Therefore, we need to analyze the security of the network regularly for the purpose of identifying the available security threats and hence implementing the security policy and mechanisms appropriate for both the servers and the clients in the ELANs.

The main objective of this study was to assess the ELANs so as to determine security vulnerabilities and threats on the existing network infrastructure for the purpose of protection.

2. EXPERIMENT SETUP

In finding available loopholes within the ELANs, penetration testing was conducted. According to Bacudio et al [14], penetration testing has three phases to be taken into consideration. Phase one is test preparation whereby all information were prepared and settled. Phase two is testing whereby automated tools used to perform the work as faster as possible. Phase three is analysis whereby the results were examined. Figure 2 illustrates penetration testing phases.

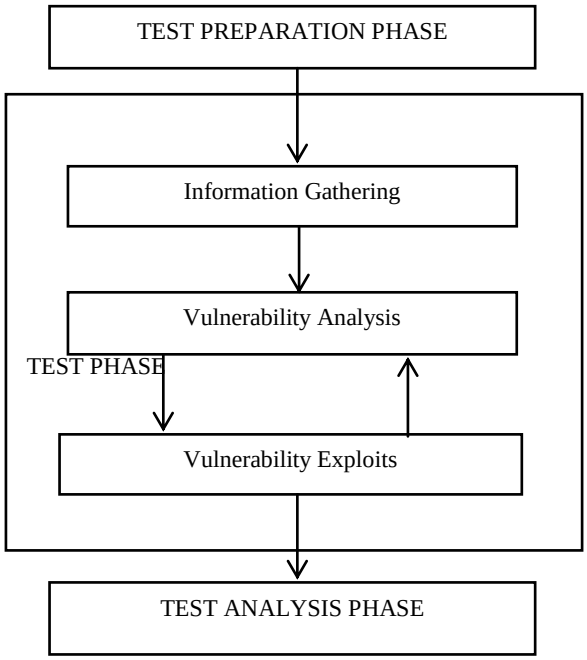

Figure 2: Penetration Testing Phases

The penetration testing phases shown in figure 2 were adopted and led to the results which are so useful to the Enterprise LANs. However, fixing or patching the vulnerabilities discovered does not mean that it is the end of security doubts, but it should be the beginning of a never ending routine as explained by Tilak [15]. This activity should be a perpetual rotation which will reduce the risk of whatever happens in the network.

In this study, laptop computer with BackTrack 5 R2 [16] installed was used for testing purposes. Nessus 5.0 [17] was used and integrated inside the BackTrack to find vulnerabilities within the Enterprise LANs. Nessus provides the information if the exploit is available in the public or not, this reduces the time for the attacker to start writing his or her own exploit. During the experiment, testing computer was connected in the ELANs and the results were analyzed.

3. RESULTS AND DISCUSSION

3.1 Penetration Testing Results

The penetration test revealed that some commonly known ports were open. It was further found that the open ports were running services that may threaten the security of the network. These weaknesses can easily be used by attackers to launch attacks by spreading Trojans and other malicious programs. Moreover, the test showed that some of the applications used in the networking devices were found to have weaknesses that are likely to cause the compromise. In this regard, the Nessus scanner performed automated tests and showed the possibility of exploits to be launched by attackers. Table 2 depicts the vulnerable applications and possible attacks found in the ELANs.

Table 2: Vulnerable Applications and possible attacks found in the ELANs

Vulnerable Applications	Possible Attacks
Apache server	Buffer overflow attacks
Cisco IOS software	Cross-Site Scripting attacks
FTP weaknesses	Default SNMP can be guesses
Linksys router problem	Denial of Service (DoS) attacks
Microsoft windows remote desktop vulnerabilities	Information disclosure attacks
PHP affected by multiple vulnerabilities	Injection attacks
SMB weaknesses	Man-In-The-Middle attacks
	Remote code execution attacks

Furthermore, table 3 illustrates the vulnerable services which are found in various devices of the ELANs. The Nessus scanner provided risk levels of each service and described the needed amount of consideration to a problem. Vulnerability can lead to critical risk, high risk, medium risk, low risk, or none. Having low risk can be used by attacker to launch exploits. However, services which are running in the ELANs can lead to great risks as shown in vulnerability information column of table 3. Therefore, the ELANs have to act upon all risk levels even if it is informational only.

Table 3: List of common vulnerabilities

Service	Severity	Vulnerability information
HTTP	Critical	Buffer overflow
Cifs	Critical	Buffer overflow
RPC	Critical	Denial of service
HTTP	Critical	Default password
HTTP	Critical	Cross site scripting
HTTP	Critical	Information disclosure
LLMNR	Critical	Remote code execution
SNMP	High	SNMP can be guessed
MSRDP	High	Remote code execution
HTTP	High	Denial of service
Telnet	Low	Unencrypted Telnet server
mDNS	Medium	Information disclosure
DNS	Medium	Cache snooping attacks
MSRDP	Medium	Man-in-the-middle attack

In addition, table 4 depicts percentage of open ports in the ELANs whereby LAN E and LAN C has 21% each followed by LAN A with 20%. These three LANs have more ports open which can be used by hackers for invasion. In the ELANs three risk factors were taken into considerations to oversee how different LANs are affected by known vulnerabilities. The critical risk has to be given the first priority, followed by the high risk and the last is the medium risk which also has to be taken seriously.

Moreover, table 4 depicts critical risks, high risks and medium risks respectively on different LANs examined. LAN C and LAN E have more machines having known vulnerabilities because there is high usage of computers compared to other LANs. At LAN E, 46% of the used machines found to have critical risks, 44% found to have high risks and 33% found to have medium risks. Other LANs have low percentage compared to LAN E. Hence LAN C and LAN E were used to simulate attacks in few machines because working on real environment might cause disruptions to machines and users.

Table 4: Open Ports and risks levels

ELANs	Open Ports	Critical risks	High risks	Medium risks
LAN A	20%	15%	9%	13%
LAN B	12%	8%	9%	12%
LAN C	21%	11%	27%	17%
LAN D	12%	10%	3%	10%
LAN E	21%	46%	44%	33%
LAN F	14%	10%	8%	15%

3.2 Tested Attacks

It is well known that an attacker need just single point of loophole to invade the network. Therefore, security testing was conducted in the ELANs so as to find out if the hacking process can be done by the attacker. Hence, few attacks were

tested in the ELANs. Figure 3 illustrates how researchers gained access to the remote machine by using Metasploit tool. After gaining remote computer session, attacker can navigate inside the computer and perform unauthorized activities that may lead to compromise the network. Figure 4 illustrates how researchers managed to use the available loophole and be able to create a login account.

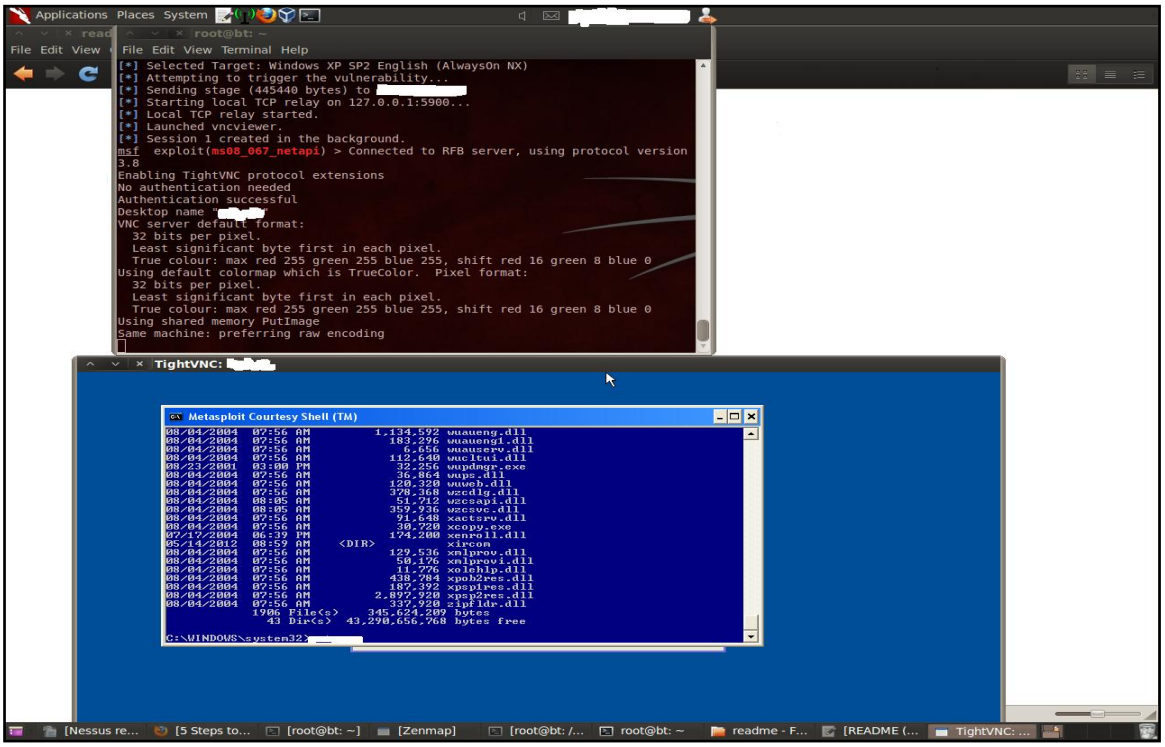

Figure 3: Remote computer session

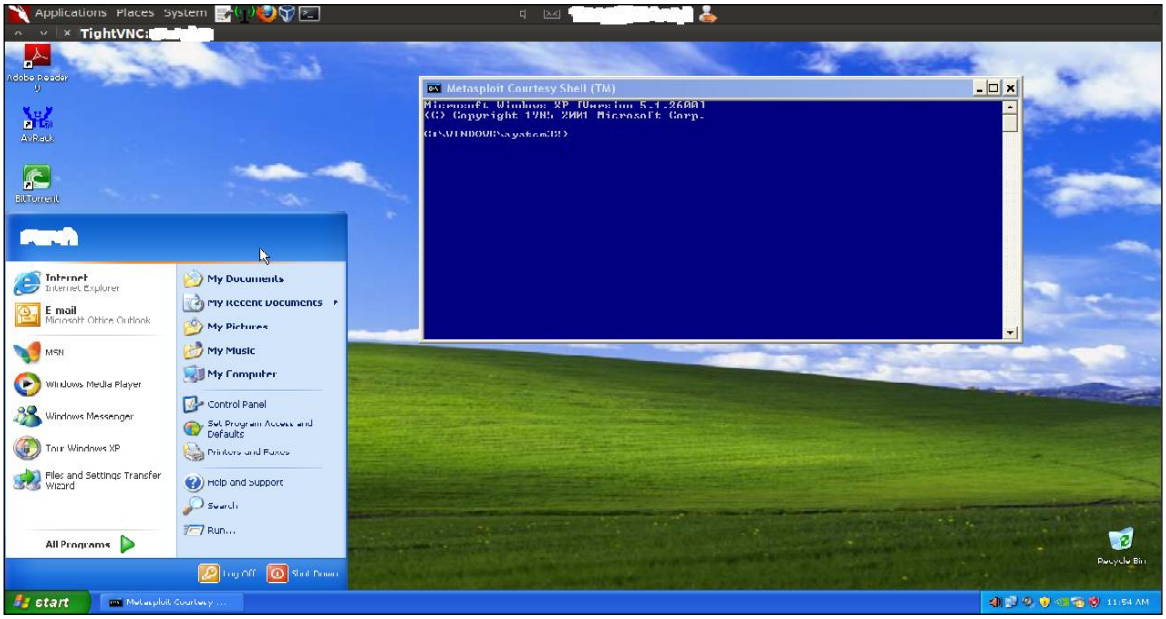

Figure 4: Remote computer accessed

Figure 5 illustrates one of the ELANs devices that researchers were able to access through the web browser. The Internet Protocol (IP) address was easily found by using Zenmap [18] as a scanner. The IP address has been erased to provide privacy. Moreover, default password was used to login within the device.

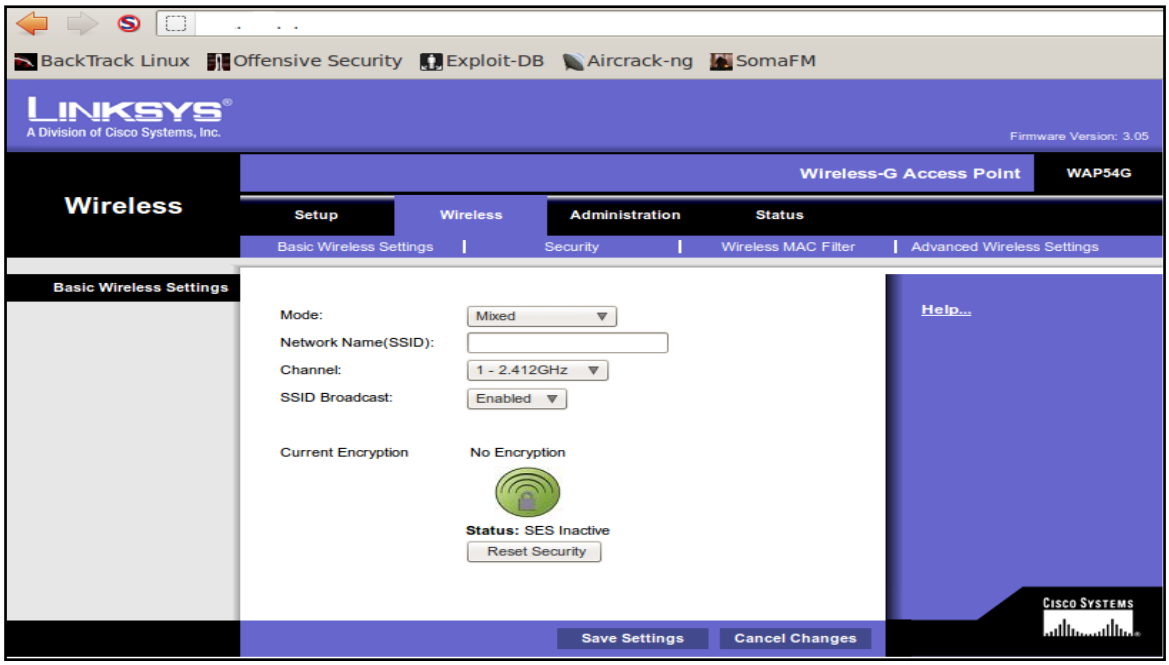

Figure 5: Captured Access Point settings

4. CONCLUSION

In this study, the available security holes in the ELANs were examined. Moreover, the security holes evaluated in this work allow the attackers to penetrate not only the selected ELANs used in this work but also any production network around the world. Researchers propose some security countermeasures to be taken. The proposed security countermeasures include but not limited to: changing default usernames and passwords, closing unused ports, updating the software used in networking devices, disabling unneeded services, and encryption. In addition, administrators have to block all traffic that need to access SNMP services by using firewall rules.

Having the reliable and secure services in the ELANs is most important to its users. Hence, there is a need for institutions, military, and companies to analyze their network infrastructure in a given timeframe in order to reduce the risks that might happen during the invasions.

5. FUTURE WORK

Future study should focus in finding the relationship among vulnerabilities, applications and operating systems in the ELANs.

6. ACKNOWLEDGMENTS

We would like to thank the Almighty God for enabling us to accomplish this work.

7. REFERENCES

[1] Internet World Stats, 2011. "World Internet Users and Population Stats", [http://www.internetworldstats.com/stats.htm], site visited on August 28, 2013.

[2] TCRA, 2010. "Report on Internet and Data Service in Tanzania" [http://www.tcra.go.tz/publications/InternetDataSurveryScd.pdf], site visited on 23, January 2012.

[3] Internet Systems Consortium, 2011. "Internet Domain Survey, July 2011", [ftp.isc.org/www/survey/reports/2011/07/], site visited on September 10, 2013.

[4] Cornwall, H. 1985. The hacker's handbook, Century Communications Ltd, Portland House, 12-13 Greek Street, London W1V 5LE.

[5] Whittaker, Z. 2010. "Virus attack Hits Vista machines, cripples university network", [http://www.zdnet.com/blog/igeneration/virus-attack-hits-vista-machines-cripples-university-network/3954], site visited on March 25, 2012.

[6] Alabady, S. 2009. "Design and Implementation of a Network Security Model For Cooperative Network," International Arab Journal of e-Technology, Vol. 1, No. 2.

[7] http://www.sans.org/network_security.php, site visited on October 10, 2013.

[8] Daya, B. 2011. "Network Security: History, Importance, and Future", [http://web.mit.edu/~bdaya/www/Network%20Security.pdf], site visited on February 19, 2012.

[9] ICT Headquarters, 2012. "Networking", [http://icthq.org/network-security], site visited on January 20, 2012.

[10] Dowd, P. W. and McHenry, J. T. 1998. "Network Security: It's Time to Take It Seriously", Computer, vol.31, no.9, pp.24-28.

[11] http://www.wisegeek.com/what-is-network-security-analysis.htm, site visited on October 10, 2013.

[12] Vulnerability scanning with SAINT scanner, [http://www.saintcorporation.com /solutions/vulnerabilityScan.html], site visited on March 28, 2012.

[13] Vacca, J. R. 2010. Network and System Security, Syngress

[14] Bacudio, G. A., Yuan, X., Chu, B. B. and Jones, M. 2011. "An overview of penetration testing", International Journal of Network Security & Its Application (IJNSA), Vol.3, No.6.

[15] Tilak, P. 2011. "Technical White Paper on Penetration Testing", [http://www.docstoc.com/docs/70280500/White-Paper-on-Penetration-Testing], site visited on July 17, 2012.

[16] BackTrack, [http://www.backtrack-linux.org/], site visited on February 5, 2012.

[17] TENABLE Network Security, "Nessus 5", [http://www.nessus.org/products/nessus], site visited on June 10, 2012.

[18] Nmap, [http://nmap.org/zenmap/], site visited on February 5, 2012.