ISSN 1512-1232

EVALUATION OF NETWORK AND SYSTEMS SECURITY USING PENETRATION TESTING IN A SIMULATION ENVIRONMENT

[1]Fashoto, SG, [2]Ogunleye, GO and [3]Adabara, I

[1]Department of Computer Science, University of Swaziland, Kwaluseni, Swaziland
[2]Department of Computer Science, Federal University, Oye-Ekiti, Nigeria
[3]Department of Computer Science, Kampala International University, Kampala, Uganda

Abstract

Penetration testing can provide Network and System Administrators with a realistic assessment of security posture by identifying the vulnerabilities and exploits that exist within the computer network infrastructure. Penetration testing uses the same principles as crackers or hackers to penetrate computer network infrastructure, thereby verify the presence of flaws and vulnerabilities, and help to confirm the security measures.

The aim of this paper is to explore the use of penetration testing in the assessment of network infrastructure in a simulation environment, and to demonstrate attacks and intrusion into the network infrastructure. Vulnerability assessment is presented as a part of the penetration test also classifications and phases of a penetration test are described. Some free and open source tools (Nessus, OpenVAS), techniques are used to simulate possible attacks. After the theoretical part, these tools are used to exploit and discovered vulnerabilities in the Network Infrastructure by using appropriate publicly known exploits. This paper shows that if penetration testing is conducted in a methodological manner it could assist Systems and Network administrators improve the security of their network infrastructure.

Keywords: *Nessus, OpenVAS, Penetration testing, University*.

1.0 Introduction

Organizations (government or nongovernmental organization) heavily rely on information systems for essential operations, administration, research, and sharing of information. Emphasizing the functionalities of organizational information system, [1], asserts that any organization information system has to provide information about research and scientific cooperation offers, businesses and further education capabilities. In the views of [2], heavily relying on computers and other technology poses a new set of security needs. The information systems and the networks are faced increasingly with security threats from a wide range of sources including computer-assisted fraud, attacks from hackers within or outside the network. There are many threats to information systems and networks infrastructure today, which threaten the reliability of information systems in our society. Some examples of common threats that will be exposed to hackers, computer viruses, spams, Denial of Service (DoS), Domain Name Service (DNS) spoofing.

According to [3], most private organization Information systems can be considered more complex than the usual information systems used in commercial organization. It is often difficult to secure organization networks (institution, banks etc.) due to the large numbers of users, the broad categories of network users, the open access nature of some of these organizations where faculties and departments are autonomous. Organization networks may be vulnerable to physical attacks on network components, social engineering attacks and cyber-attacks where malicious attackers are able to have access to some restricted resources over network connections. This research focuses on

ISSN 1512-1232

assessment of an organization network against network-based attacks. These include attacks launched by malicious outsiders on the Internet and malicious insiders directly connected to internal networks. Both types of attackers can take advantage of vulnerabilities in network infrastructure and in systems such as servers (e.g. web servers, application servers, mail server etc.), routers, gateways, and firewalls. Protection against network-based attacks is complex because compromising one system often provides a platform that can be used hackers to launch further attacks.

The approach mostly used by Systems and Network Administrators in some universities around the world is securing the network by performing an initial configuration and hardening of the systems and after that, they just monitor various parameters of the systems, network infrastructure and observe their functionality. During this processes of monitoring the network if authorized activities were detected by the monitoring devices, they react and fix the problem. This approach in protecting the university information systems may be ineffective and inadequate in preventing network-based attacks on the network. These reactive ways of protecting systems and network infrastructure may not be adequate in protecting critical assets because it places the attacker always ahead of the systems administrators, it may lead to irreversible damage (Data theft, system compromise, disruption, reputation damage, DOS , etc.).

A better approach for protection of systems and network infrastructure is proactive security. In this approach, the organization actively tests its own systems and networks using vulnerability assessment and penetration testing to find vulnerabilities before real attackers does. This method enables the organization to proactively mitigate any potential vulnerability and be ahead of the attackers.

Penetration testing is a practical oriented type of security assessment available today. It simulates the behaviour of skilled attackers who are actively testing the security of the target system, searching for vulnerabilities and exploiting them. However, instead of damaging the system, the tester reports the problems to the executive management in order for the systems to be fixed and the security holes patched.

The specific objective of this paper is to achieve the following.

- To investigate the use of penetration testing in a simulation environment using university network scenario
- Attempt to test the exploitability of a discovered vulnerability
- Determine the severity of a potential vulnerability on the network infrastructure
- To explore how a network or system administrator can use penetration testing to analyze and improve the security of a university network.

2.0 Overview of Information Systems Security

Information systems security refers to any activities designed to protect information systems. It consists of the technologies and processes deployed to protect computer systems from internal and external threats [4]. Systems security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations.

Penetration Test

Penetration test as defined by [5] is the simulation of a real-world attack against a target network or application, encompassing a wide range of activities and variations. Penetration Testing is a technique for assessing network security, by generating and executing possible attacks exploiting known vulnerabilities of operating systems and applications. Penetration test is a security oriented systematic probing of system (any combination of application, host or networks) from internal or external undertaken by a penetration tester or auditor to discover vulnerabilities that could be exploited by an attacker.

ISSN 1512-1232

In other word, penetration testing is the act of assessing all the IT infrastructure components including operating systems, communication medium, applications, network devices, physical security, and human psychology using similar or identical methods to that of an attacker but perform by the authorized and qualified IT professionals.

Difference between penetration tester and an attacker

The main differences used to distinguish a penetration tester from an attacker as suggested by [6] are the intent of the tester and the permission given to the tester by executive management.

Intent: The intent of a penetration tester is to exploit security weaknesses in an information system or network infrastructure, determine feasibility of an attack, the business impact and to report findings to the executive management [7]. The executive management will then expedite appropriate measures to make sure that the vulnerabilities are eliminated. In contrast, an attacker will exploit security weaknesses with the intention of gaining access to information or disrupting service.

Permission: A penetration tester has permission from the executive management to exploit security weaknesses while an attacker does not. Penetration testing must be performed with the permission and awareness of the executive management. It is important to notify management and staff of the organization of the penetration test throughout the testing period; since the tests may likely have some serious consequences on the systems, being tested such as system crashing and network congestion, which may result in critical system or network devices, going offline.

Types of Penetration Test

Penetration testing can be conducted in several ways. The most common difference is the amount of knowledge of the implementation details of the systems being tested supplied to the tester. The widely accepted approaches are Black-box, White-box and Grey box testing.

Black-Box Testing

According to [8]-[9] in black box testing, testers simulates the attack as someone who have no prior knowledge of the infrastructure to be tested by deploying the number of real-world attack techniques (e.g. Social Engineering, Network Scanning, remote access, Trojans etc.) and following an organized test plan. For example, testers will be only provided with the organization‘s website or network IP address rage. Therefore, the testers simulate all hacking techniques that may reveal some known and unknown set of vulnerabilities existed on the network.

White-Box Testing

According to [8]-[9] in this type of testing, the testers simulates an attack as someone who have complete knowledge of the infrastructure to be tested, often may include OS details, IP address schema and network layouts, source code, and even some passwords. The tester is provided as much information as possible so that the tester can gain insight understanding of the system and elaborate the test based on it.

As confirmed by [10] white box testing is designed to simulate an attacker who has intimate knowledge of the target organization‘s systems, such as an actual employee. Thus, the main goal behind the white-box penetration test is to verify the integrity of organizations network infrastructure and proactively minimize risks from an internal attacker such as a disgruntled employee [10].

Grey-Box Testing

When both types of penetration testing are used together, the combined approach provides a powerful insight for internal and external security viewpoints. This combination is known as Grey-Box testing. The key benefit of this approach is a set of advantages posed by both approaches mentioned earlier. Grey box penetration testing helps to eliminate any internal or external security issues lying at the institution‘s infrastructure environment that an attacker can exploit. According to

ISSN 1512-1232

[11] the gray box testing is a preferred method when cost is a factor as it saves time for the penetration testers to uncover information that is publicly available.

3.0 Setup and Configuration

Two high-end laptops were used to create the penetration-testing environment. Both the laptops were networked using a crossover cable; no other network components were used. This setup was created to isolate the testing environment from the production environment. The laptops as shown in figure 1 had Linux based operating systems installed on them. One laptop was used for conducting penetration test, had a kali Linux rolling installed on it. Kali Linux rolling, an Ubuntu based distribution. Using VMware pro (version 12), three separate virtual machines were created on the next laptop. VMware is virtualization software, which allowed installing different operating systems on separate virtual machines on the same physical machines, to emulate a cross-platform environment. Two servers and one-client virtual machines were created on the laptop. All three virtual machines including the physical laptop served as the target machines throughout the test. Windows Server 2008 Standard Service Pack 2 64-bits, Windows 7 Professional Service Pack 1 64-bits, Metasploitable 15.04 LTS were the operating system installed on those virtual machines.

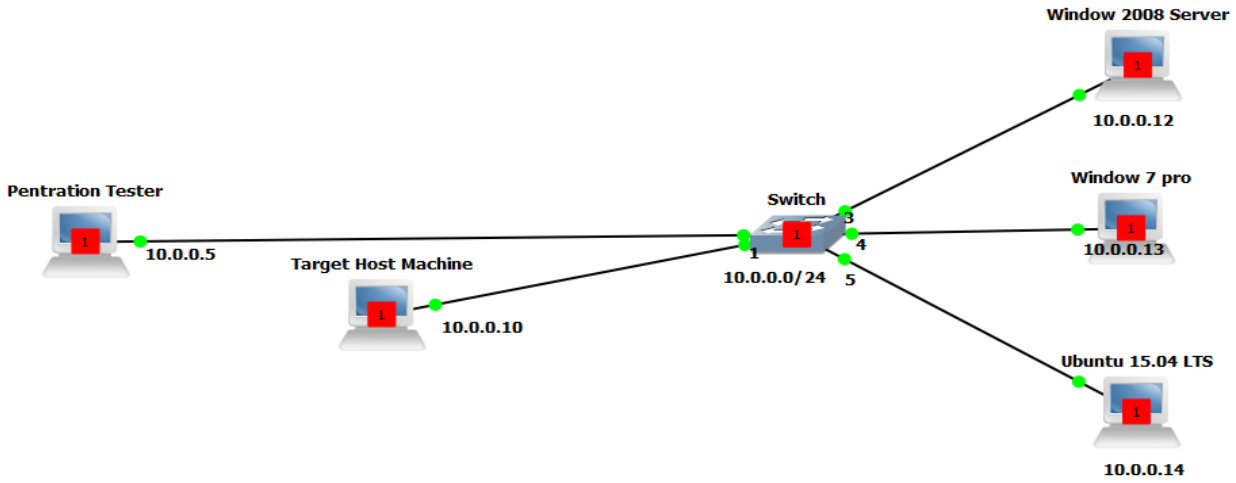

Figure 1. Penetration Testing Simulation Environment

From this point, laptop that had three separate virtual machines inside was referred as Target Host Machine and the other laptop was referred as Penetration tester's Machine throughout this testing. Ubuntu 15.4 LTS was installed on Target Host machine. Windows 2008 server, Ubuntu 15.04 LTS (Metasploitable), and Windows 7 professional were installed on separate virtual machines inside Target Host machine and these machines were referred as Host machines throughout this testing. Target Host Machine was configured as a DHCP server and this machine acted as a gateway. This Target Host machine simulated a basic networked computer environment with two servers and two clients' machines in a 10.0.0.0 network. Hence, the above shown simulation environment in Figure 1 was further simplified in Figure 2

ISSN 1512-1232

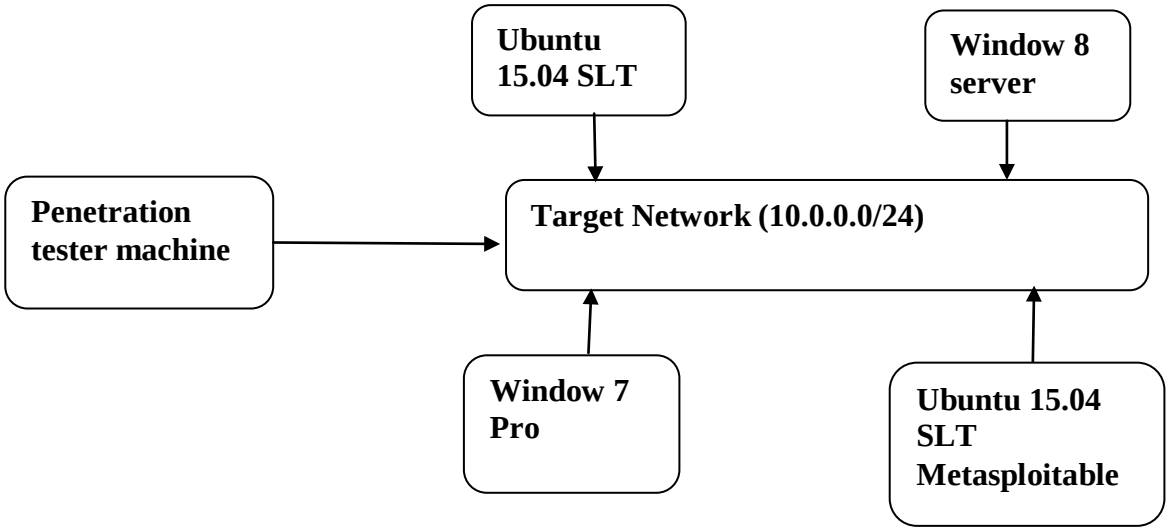

Figure 2. Penetration Testing Topology

Target Host machine simulated a networked computer environment but the concept of defense-in-depth was into consideration. This meant no defense mechanism such as firewalls and intrusion detection systems were installed on the any of the target machines. This consideration was intentional because including defense mechanism would have affected the actual goal behind this setup and exploitation of a system or network was often easier without firewall and IDS/IPS.

4.0. Results and Discussions

This section describes the results obtained during the execution of Nessus and OpenVAS scanners against the target host machines. It will also demonstrate how the scanners with different configurations performed during scanning and vulnerability assessment phase. In the last section, result from a separate comparison between Nessus and OpenVAS will be explained in brief. This comparison was intended to investigate how two separate scanners can affect the detection rate in the same test environment.

4.1. Vulnerability Assessment using Nessus

Nessus Home Free edition was used for assessing the vulnerability against the target hosts in the simulation network. All the plug-in were installed and updated before the scan. Using default scan policy in Nessus client, scans were executed in two configurations:

• Uncredentialed scan and Credentialed scan with safe checks option enabled
• Uncredentialed scan and Credentialed scan with safe checks option disabled

Two separate scans were performed, using first configuration. First scan was performed without credentials, and second scan was performed with credentials with safe checks option enabled in both the scans. Using the second configuration, again, two separate scans were performed, first scan was performed without credentials, and second scan was performed with credentials with safe checks option disabled in both the scans. All the scans were executed against the hosts on 10.0.0.10, 10.0.0.12, 10.0.0.13 and 10.0.0.14. Credentialed scan performed local security checks on both Linux and Windows based system. Credentialed scans were performed by enabling SSH local security checks on Linux systems and Windows logins on Windows bases systems. A separate user accounts were created on both Linux and Window systems, and these accounts credentials were used to perform credentialed scans.

During credentialed scan, Nessus discovered 634 and 621 vulnerabilities with safe checks options disabled and en- abled respectively. When the same scan was conducted without credentials, Nessus only discovered 163 and 168 vulnerabilities with safe checks options disabled

ISSN 1512-1232

and enabled respectively. Each ’red’ and ’blue’ bar in Figure 3 represented a scan per- formed during Nessus scanning and vulnerability assessment. Red bars indicate that credentialed scans were run, and blue bars indicate un-credentialed scans were run for simulation network.

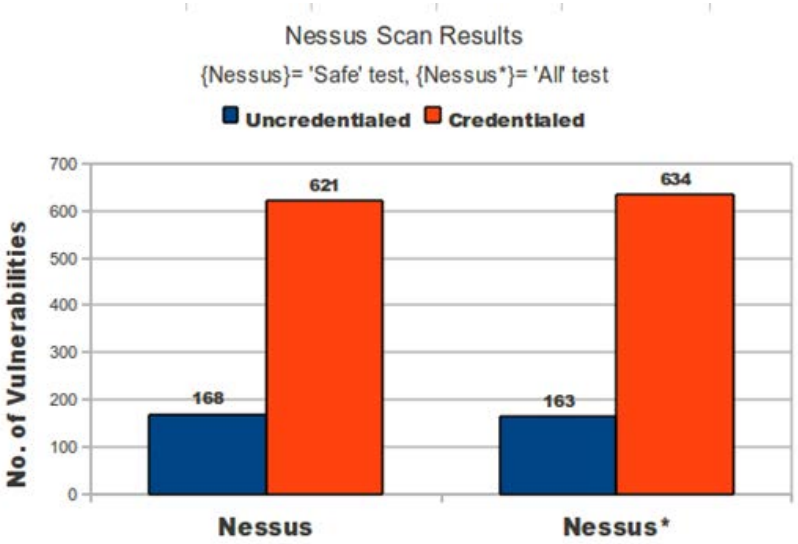

Figure 3. Nessus result summary

4.2 Vulnerability Assessment using OpenVAS

Under the similar configuration compare to Nessus, OpenVAS was also used to perform the scan against the same simulation network. Using initial global settings in OpenVAS client, scans were executed in two configurations:

- Un-credentialed scan and Credentialed scan with safe checks option enabled
- Un-credentialed scan and Credentialed scan with safe checks option disabled
- During credentialed scan, OpenVAS discoved 503 and 489 vulnerabilities with safe checks options disabled and enabled respectively. When the same scan was conducted without credentials, OpenVAS only discovered 124 and 173 vulnerabilities with safe checks options disabled and enabled respectively. Each ’red’ and ’blue’ bar in Figure 4 represents a scan performed during OpenVAS scanning and vulnerability assessment.

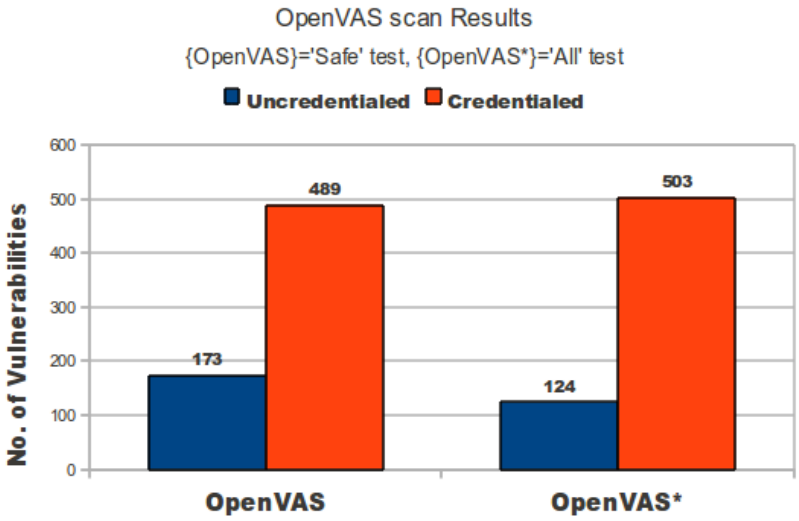

Figure 4. OpenVAS result summary

ISSN 1512-1232

Comparing the CVEs results from Nessus and OpenVAS

A brief comparison between the results from Nessus and OpenVAS was performed based on the Common Vulnerability and Exposure (CVE) identifiers. CVE was developed and maintained by the MITRE Corporation. It was used as the basis for the U.S. National Vulnerability Database (NVD); a new service supplied by the National Institute of Standards and Technology (NIST) which correlates all different sources of information and scores each monitored software vulnerability with an appropriate severity level, based on the Common Vulnerability Scoring System (CVSS) (National Vulnerability Database Version 2.2 Home Page). CVE were given names according to the years of their inclusion and the order in which they were added to the list in that year. For example, CVE-2009-3103 refers to the Microsoft SMBv2 negotiations Protocol Remote Code Execution Vulnerability that was caused by array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Server 2008 (CVE-2009-3103). Both Nessus and OpenVAS identified this vulnerability affected the host on 10.0.0.12. Nessus ranked this vulnerability as Critical and OpenVAS ranked it as High.

CVE's was chosen to compare the results between Nessus and OpenVAS for the following reasons:

- Both scanners used different metrics to rank the vulnerabilities, which they detected. There was a need to have a common baseline for evaluation among the scanners and CVEs identifiers provided a standardized basis for evaluation. CVE Identifiers (also called "CVE names," "CVE numbers," "CVE-IDs," and "CVEs") are unique, common identifiers for publicly known information security vulnerabilities.

- Both scanners had their own databases with their own names for vulnerabilities, and it was hard to determine whether both databases were referring to the same vulnerability or different.

This comparison was performed to determine which scanner was more efficient at detecting more CVEs vulnerabilities than the other scanner. Both scanners were updated with the latest plug-ins on the same date, when the scans were performed, Nessus plug-ins count was 48,296 and OpenVAS plug-ins count was 25,563. Nessus identified 17 CVEs vulnerabilities out of all 168 vulnerabilities whereas OpenVAS identified 25 CVEs vulnerabilities out of all 173 vulnerabilities, when un-credentialed scans were performed. Similarly, Nessus was able to identified 315 CVEs vulnerabilities out of all 621 vulnerabilities whereas OpenVAS identified 314 CVEs vulnerabilities out of all 489 vulnerabilities, when credentialed scans were performed, with safe check options enabled in both the uncredentialed and credentialed scans.

Likewise, Nessus identified 15 CVEs vulnerabilities out of all 163 vulnerabilities whereas OpenVAS identified 30 CVEs vulnerabilities out of all 124 vulnerabilities when uncredentialed scans were performed. Similarly, Nessus was able to identified 318 CVEs vulnerabilities out of all 634 vulnerabilities whereas OpenVAS identified 317 CVEs vulnerabilities out of all 503 vulnerabilities, when credentialed scans were performed, with safe check options disabled in both the uncredentialed and credentialed scans.

ISSN 1512-1232

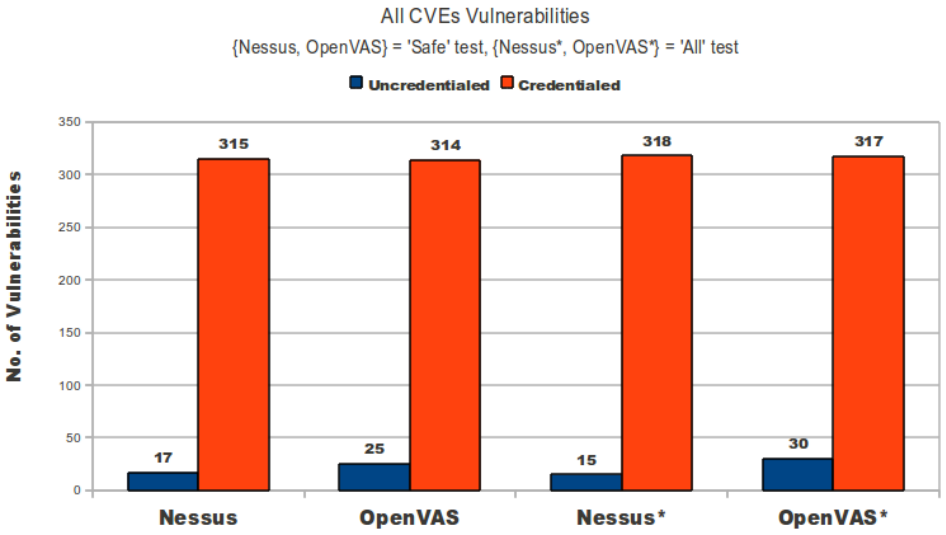

Figure 5. Nessus Vs. OpenVAS (All CVEs) Vulnerabilities

Table 1 and 2 showed the filtered results from first configuration using Uncredentialed scan and credentialed scan with safe checks option enabled.

Table 1: Nessus's Uncredentialed Scan with safe checks enabled

Target Hosts	Critical	High	Medium	Low
10.0.0.10	0	0	3	2
10.0.0.12	2	0	1	0
10.0.0.13	1	0	3	0
10.0.0.14	2	2	7	1

Table 2: Nessus's Credentialed Scan with safe checks enabled

Target Hosts	Critical	High	Medium	Low
10.0.0.10	0	0	3	2
10.0.0.12	14	109	27	1
10.0.0.13	2	1	3	1
10.0.0.14	15	63	80	7

Results in table 1 and 2 showed that credentialed scan were more effective at identify vulnerabilities as compared to un-credentialed scan. Credential scan showed that the target host on 10.0.0.12 and 10.0.0.14 were highly vulnerable as both host had 14 and 15 critical risk factors respectively. The benefits of credentialed scan over un-credentialed scan were that credentialed scan was able to find localized vulnerabilities, and verify settings and configuration.

5.0. CONCLUSION

The success of any penetration test depends on the applied methodology. In order to perform a successful penetration test, the introduced methodology should make use of different security tools e.g. Nmap, Nessus, OpenVAS and Metasploit Framework were examined. The selection of the tools was based on its versatility, usability and effectiveness. With all the tools in hand, each stage of the methodology was adapted in a systematic and methodological procedure. The selected tools were divided into three categories. The Intelligence gathering phase covered the tools, which

ISSN 1512-1232

assisted in network profiling, network scanning and operating system and services fingerprinting. Nmap was identified as one of the best tool, to be used during this phase. The Scanning and Vulnerability Assessment phase covered the tools, which allowed the exploration of network and system vulnerabilities. Nessus and OpenVAS were two such tools emphasized in this paper. With over 48,000 and 25,500 plugins respectively, they were the best tools to be used during scanning and vulnerability assessment phase. In conclusion, tools and methodology, if properly utilized, can prove their usefulness for understanding the weaknesses of the network or systems and how they might be exploited. Penetration testing is not an alternative to other security measures. In fact, it should be used to complement the Defense in Depth principle. In today's world of information security, where threats and vulnerabilities are changing and evolving, penetration testing tools and methods used to combat against such threats and vulnerabilities should also change and evolve along with technological advancement.

References

[1]. Ali, S. and Herivato, T.(2011) - BackTrack 4: Assuring Security by Penetration Testing. Packt Publishing.

[2]. Barrett, N.(2003) - Penetration testing and social engineering hacking the weakest link. Information Security Technical Report, 8(4), pp 56–64.

[3]. Kudrass, T.(2006) Integrated university information systems. In: ManolopoulosY, Filipe J, Constantopoulos P & Cordeiro J(Eds.) Proceedings of Eighth International Conference on Enterprise Information Systems, Information System Analysis and Specification, pp 208-214.

[4]. Ogeto, V.M.K(2004) A survey of Computer-Based Information Systems Security Implemented by Large Private Manufacturing Companies in Kenya", Unpublished MBA Thesis. University of Nairobi.

[5]. Luo, X. and Warkentin, M.(2004) Assessment of Information Security spending and costs of failure‘‘, Mississippi State University.

[6]. McCumber, J(2005) - Assessing and Managing Security Risk in IT Systems: A Structured Methodology. New York, NY: Auerbach Publications.

[7]. Lui, V.(2007) - Penetration testing: The white hat hacker‖. Available on http://www.issa.org/Library/Journals/2007/July/Lui7 2007. Accessed on 13th March 2016, 6:15 pm.

[8]. Northcutt, S., Shenk, J., Shackleford, D., Rosenberg, T., Siles, R. and Mancini, S.(2006) Penetration Testing: Assessing Your Overall Security Before Attackers Do‘, SANS Institute

[9]. Saindane, M.(2008) - Penetration testing - a systematic approach, available at http://www.infosecwriters.com/text_resources/pdf/PenTest_MSaindane.pdf, 2008. Accessed on 18th Febuary 2016.

[10]. Kurtz, G. and Prosise, C.(2000) Penetration Testing Exposed -Part 3 Audits, Assessments & Tests. September. Information Security Magazine. Available on: http://www.infosecuritymag.com/articles/september00/features3.shtml Accessed on (18 March 2016).

[11]. Melmeg, A.(2007) Penetration testing Available at: http://www.giac.org/cissppap ers/197.pdf (Accessed on 18 March 2016).

Article received: 2018-05-03