Auditing Albaha University Network Security using in-house Developed Penetration Tool

M E Alzahrani

Department of Computer Science/Engineering, College of Computer Science & IT, Albaha University, Saudi Arabia
meid@bu.edu.sa

Abstract. Network security becomes very important aspect in any enterprise/organization computer network. If important information of the organization can be accessed by anyone it may be used against the organization for further own interest. Thus, network security comes into it roles. One of important aspect of security management is security audit. Security performance of Albaha university network is relatively low (in term of the total controls outlined in the ISO 27002 security control framework). This paper proposes network security audit tool to address issues in Albaha University network. The proposed penetration tool uses Nessus and Metasploit tool to find out the vulnerability of a site. A regular self-audit using in-house developed tool will increase the overall security and performance of Albaha university network. Important results of the penetration test are discussed.

1. Introduction
Network security management becomes a main concern of enterprise network recently. One of its main aims is to prevent unauthorized person accessing their classified information to be used against the organization for further own interest. The bigger the network size the more vulnerable the network from information stealing. The possibility that unauthorized personnel to access classified information should made to as minimum as possible. Thus, the network security should be prioritized and reinforced. It is the only way to guarantee smooth and productive operations.

Human interactions directly or indirectly cause network attacks. Employees themselves pose the biggest threat to enterprise. As an example, employees unintentionally install piracy software that is infected with viruses, worms or Trojans. Or, users may forget to secure their PCs, leaving them open as an easy target to potential attackers. Other users or employees may give sensitive information to outsiders, or even play a role in an important part of an attack.

User may extract classified information from the company’s servers or storage devices by gaining physical access to those network devices. The gaining access to network resources from outside enterprise premise is done through a common way network security is compromised, the Internet. Nevertheless, many cases of attacks launched from internal network. Therefore, a security policy should include internal and external threats.

Penetration testing using commercially available automated tool scan help avoid such faults, however the analysis of several popular testing tools reveals significant drawbacks in the performance. Identifying the input vectors of a web application and checking the results of an attack are important parts of penetration testing. Then vulnerability assessments are necessary for discovering potential threats throughout the environment. In general, the scope of a normal vulnerability assessment
arrangement is not necessary to be full exploitation of systems and services. Systems are typically enumerated and evaluated for vulnerabilities, and testing can often be done with or without authentication. Most vulnerability management and scanning solutions provide actionable reports that detail mitigation strategies such as applying missing patches, or correcting insecure system configurations.

According to the internal security audit conducted by a vendor on 7 September 2014, Albiha University network still having the following problems, in term of security: IT Department needs more skilled resources, single engineer cannot handle day to day operations
- Security requirements and business criticality for ALBAHA need to be defined and communicated
- More procedures and processes required to be applied for ensuring compliance to ISO27001
- More technical investment is required for Managing and Monitoring performance and capacity
- Incident management need more security controls
- Business continuity or disaster recovery plans need to be planned and tested
- There is no plans to conduct periodic vulnerability assessments or penetrations tests

This work attempts to improve the security of the university network, by developing a penetration test tool and use the tool to conduct self-assessment periodically.

2. Related Work

Works by [1-5], discuss steps and techniques commonly used to penetrates a system as follows.
1. Reconnaissance, which is a preparatory phase used to gather more information about the target.
2. Scanning, which is the pre-attack phase to find the basic information.
3. Gaining access, the first penetration phase, used to find holes in the system and get access to highly detailed information.
4. Maintaining access, in which the intruders establish control on an ownership level, leaving part of their presence in the system so as to gain at will access.
5. Clearing their tracks, in which the intruders hide traces of their activity by removing evidence from the system logs.

The methodology is used to gather information, scan for vulnerabilities and initiate penetration mechanisms (such as sniffing, password guessing, backdooring and flooding).

Mukhopadhyay et al. [6] surveyed existing available web penetration tools and introduced a penetration test architecture using Nessus and metasploit tool to perform vulnerabilities scan of a website.

In their survey, they identified a tool to discovery all the known vulnerabilities. They report the increase of number of web applications vulnerabilities. Research work in [7] concluded that existing approaches are based on the Tainted Mode vulnerability model that cannot handle inter-module vulnerabilities.

In another paper two important steps of penetration testing are identifying; the IVs of a web application and determining whether an attempted attack was successful. This paper proposed a new approach to penetration testing that improves both of these steps. The approach incorporates a conservative static analysis of the web application that identifies IVs directly from the application’s code. The approach improves the response analysis by leveraging automated dynamic analyses that accurately detect when an attack has succeeded. The proposed steps’ performance is compared against two state-of-the-art penetration testing tools and found the result is satisfactory [8].

3. Proposed Method

The architecture of the proposed method is shown in Figure 1. The proposed method consists of four main steps. In the first steps (information gathering), we use automated scanning to gain information related to the target application. This information is later used to launch the attack in the second steps
(Attack generation). We combine the recognised information and domain knowledge on possible vulnerabilities, to generate attacks. Combination of existing commercial as well as open-source tools are utilized to automate the attacks generation. In the third step (the response analysis), we do the checking whether an attack has succeeded. If so, the information about the attack is logged into a file. The final step is the visualization of the final result of the penetration testing process. The report contains details of the discovered vulnerabilities and corresponding attacks. Based on this information, we can recommend to the system/network manager steps or actions to eliminate the vulnerabilities and improve the security of their network [9].

**Figure 1.** The proposed penetration test architecture (Adapted from [6])

### 3.1. Implementation of the Pentest Tool

The main three techniques in performing penetration test are: ports scanning, gaining access, and maintaining the access. In this work, the scanning is done by using Nessus tool. Having done a vulnerability analysis using Nessus, a list of vulnerability is obtained. The list is used as a basis to launch the attacks using Metasploit tool. The ability to correlate information gained by different types of requests is equally important. Thus, the penetration test tool has to be based on consistent and standard procedure to provide integrated support for detecting a maximum number of vulnerabilities with a minimal false positive number. The visualization module is developed using JavaScript.

### 3.2. Nature of audit

Following the guidelines setup by ISO27001, the study will include physical inspection, policy study, and a detailed assessment of security measures. The tasks on each element above however limited to data gathering (read-only, no changes), and if active testing is to be performed in the process of data gathering such as probing the university’s network, the task is restricted to non-destructive.

Security measures are not limited to investment on tools or devices for protecting the university’s assets. A good security planning allocates human resource aspect such as team building, clear set of responsibilities, staff training are some of the examples. Indirectly from this study, this aspect of security is included in the study’s scope.

While external test is mainly focused on collection of data in broad and general sense, internal (onsite) audit is revolving around collecting specific and presumably accurate data. The internal auditing is limited to assessing security measures on university’s selected data center -- a center that housed all important servers. The main tasks at this stage are divided into three elements, review of security policy, interview of key personnel, and the actual internal pen-test; and typically these tasks were accomplished for over a maximum period of two days.
The first step is to study and review security policy and other related documentations. This task is essential as the policy provides management decisions in regard to security and upon which the auditor can check and verify security practices. Other localized inside information such as network topologies, security management team, physical infrastructure and monitoring measures are often provided by the university.

Interview session guided by prepared checklists with IT Center staff is carried out just after the review of security policy. Typically, this task proceeds concurrently whereby each member of audit team will correspond face-to-face with respective IT Center technical staff. The checklist is service or device specific, and the questionnaires were customized from the standard practices stated in ISO27001 handbook of computer security. Some samples of the questions were extracted from SAN’s GIAC program for Security Auditing (Track 5). The questions are of both objective where the answer is of either true/false or yes/no, and when there is question that requires subjective answer a scale from 1 – 10 is used to rate the likeliness of the respondent answer.

The final task of the onsite audit is the actual internal pen-test normally performed once internal information gathering tasks are completed (policy study and interview). The main aim of this task is to test and verify whether the guidelines set forth in the policy have been properly enforced. Common tasks performed at this stage include inspections of filtering devices (routers, firewalls, IDSs) configurations, running through a set of test on Operating Systems (OS) patches, testing on particular services or applications offered by the university, running tools to assess security vulnerability on internal network. Some of these tasks can be accomplished via the usage of automatic tools, while other may requires manual intervention assisted by the IT Center staff. Depending on the university policy in regard to internal pen-test – deploying foreign tools on internal network could be against the university security policy, hence the usage of automated tools is only materialized upon the approval by IT Center management.

4. Results
On average Albaha University has an overall performance of up to 30% of the total controls outlined in the ISO 27002 security control framework (see Figure 2).

![Figure 2. Overall performance of Albaha University in terms of ISO/IEC 27002 (Security controls) strengths and conformities.](image)

Overall Vulnerability Assessment Results for Windows based servers and Linux/Unix based servers are shown in Figure 3a and Figure 3b, respectively.
Among the critical vulnerabilities, include:
- Microsoft Windows Administrator Default Password Detection.
- OpenSSL Heartbeat Information Disclosure (Heartbleed).
- The remote host is running Microsoft Windows XP. Support for this operating system by Microsoft ended April 8th, 2014.

5. Conclusion
The proposed penetration tool successfully provided a report on overall network security and performance according to the ISO/IEC 27002 (Security controls) strengths and conformities. The tool helps Albaha University IT Center staff in performing regular self-assessment of their security.

As a future work it is to consider combining Nessus and other metasploit as a holistic penetration tool that can accurately discover more vulnerabilities of a site.

Acknowledgment
The author would like to thank Albaha University for the research funding under research contract number 70/1438.

References
[1] Stiawan D, Idris MY, Abdullah AH, Aljaber F and Budiarto R 2017 Cyber-attack penetration test and vulnerability analysis Int. J. Online Eng. 13(1) pp 125-32.
[2] Kim W, Jeong OR, Kim C and So J 2011 The dark side of the Internet: Attacks, costs and responses Inf. Syst. 36(3) pp 675-705.
[3] Richard B and Integralis A 2001 Hacking Techniques: The tools that hackers use, and how they are evolving to become more sophisticated Comput. Fraud Secur. pp 9-12.
[4] Hansman S and Hunt R 2005 A taxonomy of network and computer attacks, Computers Security Comput. Secur. 24 pp 31-43.
[5] Zhijie L, Chongjun W and Shifu C 2008 Correlating multi-step attack and constructing attack scenarios based on attack pattern modeling Int. Conf. Inf. Secur. Assur. pp 214-9.
[6] Mukhopadhyay I, Goswami S and Mandal E 2014 Web penetration testing using nessus and metasploit tool IOSR J. Comput. Eng. 16(3) ver IV pp 126-9
[7] Petukhov A and Kozlov D 2008 Detecting security vulnerabilities in web applications using dynamic analysis with penetration testing (Moscow: Moscow State University).
[8] Halfond WGJ, Choudhary SR and Orso A 2011 Improving penetration testing through static and dynamic Analysis Softw. Test. Verif. Reliab. 21(3) pp 195-214
[9] Halfond WG, Choudhary SR and Orso A 2009 Penetration Testing with Improved Input Vector identification IEEE ICST pp 346-55.