Rate Vulnerability Reducing Measures for Home Offices Based on a Cost Effectiveness Analysis

Steinar Lieungh

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2005

The MSc programme in Information Security is run in cooperation with the Royal Institute of Technology (KTH) in Stockholm.

Institutt for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

The days when information security could be based on one firewall protecting the organization's network from the dangers of the Internet, are long gone. Today, laptops, mobile phones and home offices have made perimeter security a daunting task. As the number of possible entries to a network increases, the costs of securing the perimeters are pointing upwards. The number of security technologies available complicates the decision making. To be sure that the organization spends money wisely, it is important to perform some sort of a cost-effectiveness analysis before a purchase is made. This thesis deals with the cost-effectiveness of security measures available for home office systems. The main focus is on defining a methodology for the cost-effectiveness analysis and calculating the cost-effectiveness of security measures for three different case studies.

The result of the work carried out in this thesis is a methodology for performing a cost-effectiveness analysis on security measures for the use in home offices or similar small computer systems. The methodology has the ability to differentiate between the security needs of different organizations. By defining threat sources, their motivations, and the system vulnerabilities they might exploit, the threats against the system can be identified. Finally a cost-effectiveness analysis of different security measures has been performed using this methodology. The analysis was performed on three different case studies and the security measures were ranked after their cost-effectiveness.

Sammendrag (Abstract in Norwegian)

Stadig flere bedrifter tar i bruk hjemmekontorløsninger slik at de ansatte kan få muligheten til å jobbe hjemmefra, en eller flere dager i uken. Ved å flytte kontorene ut fra bedriften og hjem til de ansatte, vanskeliggjør man sikringen av bedriftens datasystemer og de verdiene som ligger lagret der. Man går fra å ha en kommunikasjonskanal mellom bedriftens interne nettverk og Internett, til å få flere slike kanaler. Av denne grunn må hjemmekontorene sikres på lik linje som bedriftens Internett tilkobling. I en verden hvor sikkerhet ikke står øverst på dagsorden er det viktig at man bruker bevilgningene fornuftig og investerer i løsninger som er kostnadseffektive. Denne masteroppgaven vil ta for seg kostnadseffektivitets analyse av sikkerhetsløsninger for hjemmekontor. Først og fremst vil vi utarbeide en metode for å gjennomføre en slik analyse. Deretter vil denne metoden bli brukt på tre scenarier for å finne de mest kostnadseffektive sikkerhetsløsningene.

Arbeidet gjort i denne oppgaven har ført frem til en metode for utførsel av kostnadseffektivitets analyse for sikkerhetsløsninger i hjemmekontor. Denne metoden har også den egenskapen at den kan skille mellom organisasjoner med forskjellige trusselbilder, ved at trussel agenter blir identifisert og trusselen av hver enkelt agent blir vurdert opp mot sårbarhetene i systemet. Ut i fra scenarioene som har blitt satt opp har også et utvalg sikkerhetsløsninger blitt rangert etter deres kostnadseffektivitet.

Contents

List of Figures

List of Tables

1 Introduction

1.1 Topic Covered by this Thesis

This thesis identifies different security solutions and vulnerability reducing measures available for the home office systems, and rates these based on a cost-effectiveness analysis. The methodology used for cost-effectiveness analysis, is developed as part of this thesis.

1.2 Problem Description

The use of home offices with remote access to the corporate computer system is on the increase. Today's corporations equip their employees with computers at home and an encrypted connection to the corporate network. This solution exposes the corporation to new security risks, which means more money must be spent on information security in an already tight budget.

1.3 Justification, Motivation and Benefits

As a result of an advantageous tax policy and the wish for more flexible work conditions for the employees, the use of home offices by Norwegian companies and organizations is on the rise. The arrival of high speed Internet connections has made this even more widespread. More and more corporations let their employees work at home one or several days a week. In a resent survey by Deloitte [1], Two thousand Norwegian company leaders were interviewed about their company's use of home offices. 39% of the companies asked, made use of home offices. Among the companies making use of home offices, 30% said all employees made use of home offices, while 8% of the companies employing more than 100 employees let all their employees make use of home offices. Seen from an information security point of view, the use of home offices is a real challenge. The outer bounds of the network are moved beyond the traditional perimeters of the corporate network, to the homes of the employees. The challenge is how to secure the corporate network in a way that will keep the intruders out, but at the same time let the employees in. This is most often solved by moving some of the perimeter security home to the employees. The literature is full of advises for how to secure a home office environment from the threats of the Internet [2, 3, 4, 5]. As most companies cannot afford implementing and maintaining all these security measures, the clue is how to find the right combination of security measures that provides a tolerable level of security for an affordable price. So far there has not been much literature available in this field. Blakley [6] says that companies need to get a handle on cost effectiveness of security technology. Today the vendors have no useful information available about whether the security solution bought can be cost justified in terms of preventing damage to the company. Knowing the cost-effectiveness of the different security measures available gives the corporation a great advantage when investing in home office security. Money can be saved both as a result of lower cost of investment and as a result of fewer security incidents.

1.4 Research Questions

Having in mind the security problems related to the use of home offices, the following research questions are considered relevant for this thesis:

- Which methods are the most suitable for the cost-effectiveness analysis?
- How can the cost-effectiveness analysis be adjusted to reflect different organizational needs for security?
- What is the cost effectiveness ratio of the identified vulnerability reducing measures?
- How will the cost-effectiveness ranking differ in different environments?

2 Previous Work

In this chapter we discuss previous research in the fields related to the research questions stated in Section 1.4. In Section 2.1 a short review of the literature concerning available security measures for home offices is given. Section 2.2 gives an overview of methods for cost-effectiveness analysis described in the literature. In Section 2.3, ways of making the cost-effectiveness analysis reflect the security needs of different organizations are identified.

2.1 Security Measures

Several papers and books describe security measures to be used at a home office. In [2] several aspects of host security, host hardening and building security in layers are described. Willert [3] emphasizes the importance of building security in layers. Six layers of security are defined. These layers mostly correspond with Jurancich's list of seven defensive security measures to protect the home office [4]:

- Use of Router to provide firewall and NAT type of protection from the Internet
- Configuring the router to turn off all unnecessary services
- Use of host based firewall and IDS on any system connecting to the corporate network
- Use of a standardized anti-virus product on any system connecting to the corporate network
- Establishing a standardized patching policy
- Disabling unnecessary processes on the PCs
- Use of a secure connection with authentication to the corporate network.

According to [7] defense in breadth is more important then defense in depth. This statement reflects the need for security measures covering all possible entries to the system and not many security measures covering a more limited part of the system. National Security Agency (NSA) has several guidelines for securing and hardening Windows systems. The guideline [8] describes how to harden a Windows XP system. NSA provides a security template ready to implement. NSA has also made available guidelines for hardening of Internet Explorer and Outlook Express [9, 10] respectively. National Institute of Standards and Technology (NIST) has made available a similar guideline for hardening Windows XP [5] and several security templates for different environments.

2.2 Methods for cost-effectiveness analysis

In this section different methods for cost-effectiveness analysis are reviewed. First, literature describing an overall framework for the cost-effectiveness analysis is presented. Next, literature discussing methods for measuring effectiveness and costs are presented.

In [11], Levin and McEwan discuss how to perform cost-effectiveness analysis. They state that only programs with similar goals can be compared and a common measure

of effectiveness can be used to assess them. They further state that these effectiveness data can be combined with costs in order to provide a cost-effectiveness evaluation that will enable the selection of those approaches that provide the maximum effectiveness per level of cost or that require the least cost per level of effectiveness. Levin and McEwan point out that one cannot compare alternatives with different goals. An important statement made by them is that a cost-effectiveness analysis can only state whether a given alternative has a relatively better cost-effectiveness ratio than other alternatives, but we cannot state whether its total benefits exceed its total cost. A cost-benefit analysis is supposed to do that.

When measuring the effectiveness of a security measure it is important to consider the reliability and validity of the measure. One way to do the measurement is to compare the measurement of an environment using the security measures, with an environment not using the security measures. For calculation of cost, Levin and McEwan use an approach called the ingredients model (Resource Cost Model). This approach specifies all the ingredients required, and assigns a value to each. The ingredients can be divided into Personnel and Equipment ingredients. Personnel ingredients include the roles, qualification and time commitments of the employees. Equipment ingredients include lifetime, interest rate and inflation. The cost is calculated by comparing the use of ingredients in this way, rather than in their best alternative use.

The estimates of cost and effectiveness can be combined into a ratio ordered either by the measures providing the maximum effectiveness per level of cost or the measures requiring the least cost per level of effectiveness. The cost-effectiveness ratio (CER) is computed by dividing the cost (C) of the security measure by its effectiveness (E), as described by Levin and McEwan.

$$CER = \frac{C}{E} \tag{2.1}$$

For the verification of the results, Levin and McEwan propose using a sensitivity analysis. By identifying the high and low estimates of the values used in the cost-effectiveness analysis, one can recalculate the cost-effectiveness ratio of the different measures based on the new data and see if the cost-effectiveness ranking changes.

Spilling and Ølnes [12] point out that for each security requirement one should perform a cost/benefit analysis to select the security mechanism with the best cost-effectiveness ratio. The costs of implementing a desired level of security must be justified by the potential benefits gained by the security measures. [12] also emphasizes that cost is not only the real costs, but also the indirect costs on performance and user friendliness. The cost-effectiveness analysis is based on a set of security mechanisms sorted according to the security service they can be involved in. Spilling and Ølnes outline a way to describe each security service by defining all applicable security mechanisms and their figures of merit. These include describing:

- Degree of protection
- Effect on system performance

- Effect on user friendliness
- Cost of implementation
- Cost of management.

The costs of implementing a desired level of security (as expressed in the security objectives) in a specific system must be justified by the potential benefits gained by the security measures.

A report written by Nystuen and Hagen [13] defines a method for analysing vulnerability reducing measures in the telecom sector. This report explains effectiveness in three steps:

1. The effectiveness of the whole system is a combination of the effectiveness of all subsystems and components
2. The system's effectiveness is limited to a certain period of time
3. The effectiveness of the system is often given as a number, e.g. number of attacks.

The effectiveness is the difference between consequences before and after the measure was put in place. This can be written as a formula explained by Nystuen and Hagen:

$$E = \frac{C_{EU} - C_{EM}}{C_{EM}} \tag{2.2}$$

C_{EU} - expected consequences without security measure implemented
C_{EM} - expected consequences with security measure implemented
E - Index of the performance of the measure.
The calculation of cost is based on the correlation of the costs and the expected lifetime of the security measure.

Nystuen and Hagen have divided the effectiveness index (E), by the cost to generate the cost-effectiveness factor (CE):

$$CE = \frac{E}{Cost} \tag{2.3}$$

Cost - This is the total cost of ownership of the security measure.

A sensitivity analysis can be used to test the results of the cost-effectiveness analysis. By identifying the high and low estimates of the values used in the cost-effectiveness analysis, one can recalculate the cost-effectiveness of the different measures based on the new data and see if the cost-effectiveness ranking changes.

In [14], Osborne analyses cost-effectiveness in the IT security function. He claims that the approach taken by some IT security functions is flawed in the way that they approach IT security from a technical perspective. Osborne emphasizes that IT security first and foremost is a business matter. He presents five posters for cost-effective IT security in [14]:

1. IT security is first and foremost a business matter, and secondly a technical matter
2. Always know what the organization's current IT assets are

3. Ensure that there is a formal, agreed, approved and supported IT security policy that is relevant to the organization's culture and requirements
4. Before spending any resources on protecting IT assets, ensure that the comparative risks related to those assets have been identified, by undertaking a risk assessment and analysis
5. Ensure that there is a clear and easily understood mechanism for translating the IT security policy into practice, and that there is a defined methodology for the implementation of IT security procedures and products.

Osborne defines five classes of computing assets: Hardware, software, data, people involved in computing, and documentation supporting the computing activities.

2.2.1 How to Measure Effectiveness

The effectiveness of security measures can be measured using vulnerability analysis / assessment and security testing. Several methods found in the literature are discussed next.

Vulnerability Assessment The National Defense Research Institute (RAND) has developed a methodology (the VAM methodology) for vulnerability assessment and mitigation. The methodology is performed in the following six steps as described in [15]:

1. Identify your organization's essential information functions.
2. Identify essential information systems that implement these functions.
3. Identify vulnerabilities of these systems
4. Identify security techniques to mitigate these vulnerabilities.
5. Select and apply techniques based on constraints, costs, and benefits.
6. Test for robustness and actual feasibilities under threat.

The six different steps described in [15] are explained below:

Step 1: This step is divided into four parts: The goals and the strategies of the organization are identified and prioritized - the information functions in support of these tasks are identified and categorized. The information functions are classified in three categories: essential, valuable, and expendable. The identified functions are integrated and an overall ranking is developed.

Step 2: In step two, the information systems used to perform the essential functions need to be identified and categorized. The information systems are ranked in three categories: essential, valuable, and expendable, and an overall ranking is developed.

Step 3: To identify vulnerabilities in the system, this method makes use of a Vulnerability Matrix. This matrix contains a taxonomy of attributes that lead to vulnerabilities. In this step, one should also review past experience with the critical system, to learn from what went wrong and how problems were solved. Theoretical vulnerabilities that exist in the system must also be assessed.

Step 4: The VAM methodology solves this problem by using a large matrix of general security techniques relevant to each vulnerability. If a new vulnerability is generated by the use of the proposed security technique, VAM will identify this.

Step 5: From the list in step 4, one must choose security techniques to be implemented.

Step 6: In step 6, one should test the robustness of the security measures. This is done for instance by using Red Teaming to examine for vulnerabilities.

The VAM methodology converts the risk into a scale ranging from 1 - 10, where 10 symbolizes high security risk. The method compares the risk before and after the new security measures have been put in place. This makes it possible to see the improvements of the security measures put in place in an easy way.

In [16] several approaches for performing a risk analysis are described. The book starts with a general discussion on different aspects of risk analysis and a standard methodology. Then several different approaches are discussed. The focus is on qualitative methods.

National Institute of Standards and Technology (NIST) has made available a methodology for risk assessment. This methodology is based on nine steps [17]:

Step 1 - System Characterization Information about the system is gathered. The boundary and function of the system are defined, and the criticality and sensitivity of the system and its data are stated.

Step 2 - Threat Identification The threat-sources (the person or natural disaster that is creating a threat), their eventual motivation and the threat actions they use are identified. This gives us a picture of the "enemy".

Step 3 - Vulnerability Identification A list of potential vulnerabilities is created. This can be done by performing a security test of the system, by visiting the different vendors' websites or by searching vulnerability databases.
Vulnerability / threat pairs are then identified. These are the combinations of the vulnerabilities identified, the threat sources that might exploit these vulnerabilities and the methods they may use.

Step 4 - Control Analysis The implemented and planned security measures are identified in order to see if they minimize or eliminate the probability of the exploitation of a vulnerability.

Step 5 - Likelihood Determination The probability that an incident will happen is rated.

Step 6 - Impact Analysis The impact of an incident with respect to the loss of availability, confidentiality and integrity of the system is rated.

Step 7 - Risk Determination The risk of the particular threat/vulnerability pairs is identified and the overall risk level of the IT system is identified.

Step 8 - Control Recommendations A list of recommended security measures and alternative solutions to minimize the risk is created.

Step 9 - Results Documentation Finally, the results of the risk analysis are documented.

FIRM [1] [18] is a methodology for risk management in information systems. FIRM consist of two components; SARA [2] and SPRINT [3]. SPRINT is first used to perform a "light" security evaluation of all systems in order to identify which systems are critical and need a more thorough security evaluation, and which systems only need a "light" risk evaluation. For the systems identified to have no special security needs, SPRINT is used to perform the whole security analysis. For systems that are critical and need a more thorough security analysis, SARA is used. SARA performs a more thorough and detailed analysis of the system. FIRM is only available for members of Information Security Forum, and is not therefore used in this thesis.

Security Testing NIST has made available an introduction to security and penetration testing [19]. It describes different security testing techniques and defines a framework for security testing. Some common security testing tools are also presented. The drawback of this framework is the fact that it lacks a more detailed overview of what to test during a security assessment. It does not go into more detail than, for instance, to say that one should perform a portscan.

ISECOM has made an Open Source Security Testing Methodology Manual (OSSTMM) [20]. The OSSTMM describes an efficient test of known vulnerabilities, information leaks, and deviations from law, industry standards, and best practice. This test does not check for unknown vulnerabilities. ISCOM has some requirements for a security test to become an OSSTMM test [20]. The test must be:

- Quantifiable.
- Consistent and repeatable.
- Valid beyond the "now" time frame.
- Based on the merit of the tester and analyst, not on brands.
- Thorough.
- Compliant to individual and local laws and the human right to privacy.

The OSSTMM Methodology is divided into six sections: Information security testing, process security testing, Internet technology security testing, communications security testing, wireless security testing, and physical security testing. These sections are divided into modules, which work as a guideline during the security testing. The OSSTMM methodology is under development and some parts are not yet completed.

There are literally thousands of hacker tools available on the Internet. Many of these tools can come in handy when performing a security test. The most used tools and some guidance for how to use these are described in [21, 22]. These two

[1] Fundamental Information Risk Management
[2] Simple to Apply Risk Analysis
[3] Simplified Process for Risk Identification

books describe the use of the tools and show some examples of commands to use. This can be an easy way to learn the basic usage of the tools, but for more advanced use, the manual pages of the tools give much more information. [23] describes how to perform a penetration test and proposes a toolkit needed to perform an effective penetration test. The book gives some hints on where to look for vulnerabilities and has separate chapters dedicated to Internet penetration, dial-in penetration, internal penetration and social engineering. [24] describes how to use the open source network auditing tool Nessus. This is a powerful and free tool which is frequently used in penetration and security testing.

2.2.2 How to Measure Cost

This section presents a survey of known methods of calculating cost related to IT systems.

Anderson [25] points out the lack of good measurements of information security services from which return on investment (ROI) can be calculated. Computation is difficult because of the unavailability of reliable data on different attack scenarios. [25] also points out the balance between security and cost. The question is: "How secure can we afford to be - or need to be?"

In [26], Gordon and Richardson discuss the economics of information security. They point out that today's metrics for measuring the effectiveness of investments are all based on subjective judgments and are fundamentally flawed. The article discusses the use of Return of Investment (ROI) in the information security area and the problems this may cause. For instance, how can one calculate return of investment for a firewall? The drawback is that ROI does not take into account the time value of money invested. Gordon and Richardson discuss an alternative to ROI, the use of net-present-value. The expected lifetime of a purchase is important for calculation of net-present-value. The lifetime is used when costs of purchase, maintenance and administration cost are calculated. The cost savings of the investment are also calculated. This is broken down to the cost and benefit for each year minus the cost of capital.

In [27], the authors point out that when measuring costs one has to consider both direct costs and indirect costs: Direct costs are costs related to implementation and operation of the technology. Examples of direct costs are environmental operating costs, software costs, installation and configuration costs, training costs, maintenance costs, overheads (running costs). Significant costs when implementing new technologies are the indirect costs. These costs are split into two groups: indirect human costs and indirect organizational costs. The indirect human costs consist of management time (time spent on integration of new systems), management resources, cost of ownership, employee time, employee motivation, personnel issues, employee training, management effort and dedication. Indirect organization costs are losses in productivity, business process re-engineering, covert resistance, organizational restructuring, opportunity cost and risk, strains on organizational resources.

Total cost of ownership (TCO) assesses both direct and indirect costs and benefits of IT related purchases as described in [28, 29]. TCO does not only consider the initial in-

vestments, but all the costs incurring throughout the lifecycle of an asset, such as costs of purchase, repairs, maintenance, upgrades, service and support, networking, security, user training, and software licensing.

National Institute of Health has made cost-benefit guidelines for IT-projects [30], which also include some parts that can be useful in a cost-effectiveness analysis. Especially the part describing cost calculation is interesting for this thesis. When comparing competing alternatives, all costs for the full lifecycle of the alternatives have to be included. These include: Activities and Resources, Personnel Costs, Indirect Costs, Depreciation, and Annual Costs.

Activities and Resources The costs of the resources associated with each activity performed throughout the lifespan of the IT system, should be identified.

Personnel Costs These are the costs of having people working with the IT system.

Indirect Costs These are the costs of indirect labour, indirect material costs, insurance, depreciation and more.

Depreciation Deprecation is a method to spread the cost of tangible capital assets over the assets useful life.

Annual Costs Annual costs are the estimation of all costs for each year of the system's lifecycle.

2.3 Adjustment of cost-effectiveness analysis to reflect different organizational needs for security

This section presents methods that can differentiate between organizations' need for security based on the actual threat they are facing. The results can have an overall impact on the cost-effectiveness analysis for the particular organizations.

Jones [31] has developed a method of representing threat to information systems that can be used in a wide range of scenarios. This method can be modelled and replicated in an objective manner. Jones beleives that any threat to a system is posed by a threat agent. This threat agent must have suitable access, capabilities and motivation to be effective. Jones develops a method to calculate the capabilities of these threat agents to conduct a successful attack. The threat agents are identified by looking at six different properties.

Capability The threat agents need the right skills, knowledge and methods to achieve their aims.

Inhibitors An inhibitor is a factor such as fear of capture, level of technical difficulty, cost of participation that will either prevent a threat agent to carry out a successful attack, or will minimize the impact of the attack.

Amplifiers These are factors such as peer pressure, skills, access to information that will increase the possibility of a successful attack.

Catalyst This is a factor that can make the threat agent perform the attack. This can be a newly discovered vulnerability or some other event.

Motivation These are factors that motivate the threat agent to perform the attack. This can be personal gain, crime, political, to mention a few.

Access To perform an attack, the threat agent must have physical or electronic access to the system.

National Institute of Standards and Technology (NIST) makes use of a similar approach in its risk analysis [17]. During the threat identification, the potential adversaries are identified, along with their motives using a similar approach as explained by Jones. However this approach is not so comprehensive as the one described in [31]. The threat identification is divided into three parts. First, the threat sources are identified. The threat source can be either natural, environmental or human. Once all the threat sources are in place, their motivations are identified. Motivations can be such things as challenge, destruction of information, revenge, competitive advantage, and so on. Threat actions are then identified, which assumes determining the type of attack methods the threat sources are capable of using. A few examples can be system penetration, social engineering, fraud and theft, system sabotage, and denial of service. The threat sources are used later on in the risk assessment by matching vulnerabilities found in the system with threat sources capable of exploiting these vulnerabilities.

3 A Methodology for Cost-effectiveness Analysis

The aim of this thesis is to provide a methodology for calculation of cost-effectiveness of security measures for the use in home offices. A search through the existing literature shows that most literature available is aimed at the educational and health sector. Literature describing methodologies for calculation of cost-effectiveness in the information security field are scares. This thesis provides new knowledge in the following areas:

- Providing methodology for performing a cost-effectiveness analysis for different security solutions for small IT-systems, like a home office environment.
- Finding a method for detecting how the cost-effectiveness analysis can be adjusted to reflect different organizational needs for security.
- Performing a cost-effectiveness analysis for different security measures for a home office and rating the results based on this analysis.
- Performing the cost-effectiveness analysis on different case studies to see how the cost-effectiveness of different security measures change based on the security needs of the organization.

The methodology of cost-effectiveness analysis suitable for use in home office systems is as follows:

3.1 The Methodology

The methodology chosen for the cost-effectiveness analysis is built around a framework provided by Nystuen and Hagen [13]. The cost-effectiveness analysis is performed in eight steps.

1. Identify different home office security threats and countermeasures
2. Risk assessment
3. Apply vulnerability reducing measures
4. Risk assessment of the improved system
5. Calculate effectiveness
6. Calculate costs
7. Calculate cost-effectiveness
8. Sensitivity analysis

In step one, we identify different home office security measures. The vulnerability assessments in step two and step five are carried out with the help of a qualitative vulnerability analysis approach described in [17]. The vulnerability assessment in step two describes the level of security of the unsecured standard system, while the vulnerability assessment in step four assesses the system vulnerability after security measures have been added. Step four is repeated for all sets of pre-defined vulnerability reducing measures applied in step three. In step five we compare the results of the old and the new

security assessments and calculate the effectiveness of each set of security measures. In step six the cost of the different security measures is calculated by means of the formula given in [13]. The results of the cost calculation and the effectiveness calculation are used in step seven to determine the cost-effectiveness of each set of security measures. In step eight a sensitivity analysis is carried out in order to take care of uncertain numbers, which can influence the final ranking. This is done by using the upper and lower bounds of uncertain costs or effects to find the minimum and maximum cost-effectiveness ratio for that particular security measure. This can then be used to see if the uncertain values influence the overall ranking.

For the vulnerability assessment to represent the real state of the home office system, it is based on the results of security testing, the search through vulnerability databases and the information found in the literature.

3.2 Risk Assessment

The risk assessment to be used in this thesis is based on the methodology described by National Institute of Standards and Technology (NIST) [17]. This methodology provides several advantages. It can be scaled down and used on small systems. The risk assessment is based on knowledge of the threat sources and their capabilities, which makes the risk determination more accurate. Several ways of vulnerability identification is supported, including security testing and the use of vulnerability databases. The risk assessment is divided into nine steps: System Characterization, Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendations, and Results Documentation. This methodology may be used for both qualitative and quantitative assessments, but in this case the assessment is qualitative, due to the lack of accurate statistics and numbers for attack frequencies, attack costs etc.

Step 1 - System Characterization This step gives an overview of the system assessed.

Step 2 - Threat Identification This step is used to identify threat sources that can exploit system vulnerabilities. The thesis only considers human threat sources, not environmental and natural threat sources. Next, the motivation of the threat sources and the threat actions has to be identified.

Step 3 - Vulnerability Identification During this step the vulnerabilities of the system are identified. This is done by using vulnerability databases and by performing security testing.

Step 4 - Control Analysis The implemented and planned security measures are identified in order to see if they minimize or eliminate the probability of the exploitation of a vulnerability.

Step 5 - Likelihood Determination The likelihood for security incident to happen is rated by using the likelihood definition described by NIST [17].

Table 1: NIST - Likelihood Definition [17]

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised

Step 6 - Impact Analysis The impact analysis determines the impact on availability, confidentiality, and integrity resulting from a successful attack. The impact definition by NIST [17] is used.

Table 2: NIST - Magnitude of Impact Definitions [17]

Magnitude of impact	Impact Definition
High	Exercise of vulnerability (1)may result in the highly costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Step 7 - Risk Determination The risk calculation is based on a scale where high likelihood gives a score of 1.0, medium likelihood gives a score of 0.5 and low likelihood gives a score of 0.1. High impact gives a score of 100, medium impact gives a score of 50 and low impact gives a score of 10. These numbers are then multiplied with each other to represent the risk level. The scale for the risk level is: High (>50 - 100), medium (>10 - 50) and low (1 - 10).

Step 8 - Control Recommendations This step is not used in this thesis, as the results of the risk assessment are going to be used to calculate the effectiveness of the security measures already implemented and not be used as a base to secure the system even more.

Step 9 - Results Documentation This step is not used in this thesis, as the results of the risk assessment are going to be used to calculate the effectiveness of the security measures already implemented.

3.2.1 Vulnerability / Attack Groups

The vulnerabilities / attack groups considered during the risk assessment are the ones defined by Cheswick and Bellovin [32] and commented by Howard [33] during his analysis of taxonomies of computer and network attacks. The list of categories given below is found in [33].

- Stealing passwords - Methods used to obtain other users' passwords
- Social engineering - talking one's way into information that one should not have
- Bugs and backdoors - taking advantage of systems that do not meet their specifications, or replace software with compromised versions.
- Authentication failures - defeating of mechanisms used for authentication
- Protocol failures - protocols themselves are improperly designed or implemented

- Information leakage - using system such as finger or DNS to obtain information that is necessary to administrators and the proper operation of the network, but could also be used by attackers
- Denial of Service - efforts to prevent users from being able to use their systems.

The social engineering attack group is outside the scope of this thesis and is therefore not considered. Stealing Passwords and Protocol Failures are not considered either. No relevant protocol failures were found. The stealing password attack is considered to be a bit of Social engineering and a bit of information leakage. For instance, password traversing on an unencrypted connection can be intercepted, which is considered as information leakage.

3.3 Security Testing

The methodology used for these tests are based on the OSSTMM v2.1 [20]. Even though the OSSTMM is still under development, and some sections are not completed, this is a thorough methodology for security testing. The OSSTMM is easy to use and it defines clearly how to perform the security testing, what methods to be used, and how to organize the results. The OSSTMM is claimed to be consistent, quantifiable, repeatable and valid beyond the "now" time frame. No other security testing methodologies examined as part of this thesis have all of these properties. Because of the rather small size of the system being tested, only parts of this methodology are used. The tests performed on the home office system uses the relevant modules of section C of [20]: The modules used are System Services Identification, Vulnerability Research and Verification, Routing, and Containment Measures Testing. A more thorough examination of the security test is presented below:

System Services Identification The main objective of this module is to identify open, closed or filtered ports, active services, service types, service application type and patch level, OS type and patch level. Several tests should be performed in order to obtain this information.

Vulnerability Research and Verification The main objective of this module is to find vulnerable applications or services running on the system, patch level of the system and applications, and possible denial of service vulnerabilities. Ideally one uses at least two different vulnerability scanners to perform the vulnerability scan in order to reduce the occurrence of false positives and false negatives. Vulnerability scanners are expensive, so an alternative approach is to verify the results manually to eliminate false positives. By comparing the results from the vulnerability scan with results obtained by means of other tools during the security scan, and by checking out all vulnerabilities found with vulnerability databases, to see if the vulnerability detected may occur on that platform with that particular configuration, most false positives may be removed. False negatives may be more difficult to find. Comparing the vulnerability scan with the other scans performed during the security test may reveal false negatives. Tools may employ different scanning techniques and this may give different results. The use of vulnerability databases may also reveal vulnerabilities not discovered during security testing.

Routing The primary objective of this module is to find router type, services and system

information, map the ACL implemented and a list of packets that may enter.

Containment Measures Testing No tests have been found to perform an evaluation of the containment measures. This is done theoretically instead, using vulnerability databases and virus databases.

3.4 Calculation of Effectiveness

When measuring the effectiveness of a security measure it is important to consider the reliability and validity of the measurement. Levin and McEvan [11] suggest that one way to do this is to compare the measurement of an environment using the security measures with an environment not using the security measures. Nystuen and Hagen [13] present a formula to calculate effectiveness based on measurements before and after a security measure is applied. For the use in this cost-effectiveness analysis this formula has been slightly changed. Instead of comparing the consequences of a successful attack before and after a security measure is added, this formula compares the risk of a successful attack before and after the security measures are added.

$$E = \frac{C_{EU} - C_{EM}}{C_{EM}} \tag{3.1}$$

C_{EU} - expected risk of a successful attack without the security measure implemented
C_{EM} - expected risk of a successful attack with the security measure implemented
E - Index of the performance of the measure

The effectiveness is calculated based on the results of the risk assessment.

3.5 Cost Calculation

The cost calculation is performed using the method described in [30] for the use in cost-benefit and cost-effectiveness analysis. The method suites this purpose well. It makes use of all costs incurring throughout the lifecycle of an asset. The calculation considers personnel costs, indirect costs, depreciation, and annual costs. Future cost is expressed in present values.

Personnel Cost For the calculation of personnel costs, one can use income statistics for the organization. The income statistics of the past few years can also be used to calculate the average salary increase per year.

Indirect Cost The indirect costs are explained by NIH [30] to be costs such as indirect labour, indirect material, fixed costs such as depreciation, taxes, utilities, and insurance. Indirect labour costs may be the employee trying to solve a problem under the guidance of the helpdesk or on his own.

Depreciation NIH [30] defines depreciation as the reduction of the estimated value of a capital asset and as a method used to spread the cost of tangible capital assets over an asset's useful life. Usually this is only done with items with a value greater than $5000, approx NOK 30 000.

Annual Cost The annual cost of the home office for the expected lifetime of the system is calculated. The annual cost consists of Implementation costs, maintenance costs, software costs, hardware costs, support costs, and user training costs. The

Implementation costs are calculated using the number of man-hours needed to implement the security measure and multiplying it with the salary costs. The maintenance costs, support costs and user training are calculated using the number of man-hours needed each year and multiplying it with the salary costs. The average salary increase per year is taken into account. The costs are summarized for each year and the present value of the expenses is calculated using the formula described in [30]:

$$P = F\frac{1}{(1+I)^n} \tag{3.2}$$

where P = Present Value, F = Future Value, I = Interest Rate, and n = number of years. This formula transforms future NOK values into present NOK values, which gives us a common unit of measurement to compare the alternatives.

3.6 Calculation of Cost-effectiveness

For the calculation of the cost-effectiveness of the security measures we use the formula described by Levin and McEwan [11]. The cost-effectiveness ratio (CER) is computed by dividing the cost (C) of the security measure and its effectiveness (E).

$$CER = \frac{C}{E} \tag{3.3}$$

3.7 Sensitivity Analysis

A sensitivity analysis [11, 13] can be used to test the results of the cost-effectiveness analysis. By identifying the high and low estimates of the values used in the cost-effectiveness analysis, one can recalculate the cost-effectiveness of the different measures based on the new data and see if the cost-effectiveness ranking changes.

4 Experimental Work

4.1 Introduction

The main goal of this experiment is to show how a cost-effectiveness analysis can be performed for a home office system, and how this methodology makes distinctions between different organizations with different security needs.

4.2 Methods to be used for cost-effectiveness analysis

During this work, several methods were considered, but in the end the methodology of choice was built around a framework provided by Nystuen and Hagen [13].

1. Identify different home office security threats and counter measures
2. Risk assessment
3. Apply vulnerability reducing measures
4. Risk assessment of improved system
5. Calculate effectiveness
6. Calculate costs
7. Calculate cost-effectiveness
8. Sensitivity analysis

Identify different home office security threats and counter measures This part of the methodology was based on the results of a literature study.

Risk assessment The risk assessment was based on [17]. This methodology suits this purpose well. The assessment was first performed on an unsecured system, and later on a secured system, as explained later. The methodology is based on the identity of the attacker and his / her capabilities. When the threats are identified, possible vulnerabilities that can be used in an attack are also identified. This approach also assigns values to the impact and the likelihood level, which makes it easy to implement the methodology in the spreadsheet for calculation of cost-effectiveness ratio. There are several ways to find the vulnerabilities. We choose two methodologies. The first was to perform a security test, as described below, and the second was to search vulnerability databases Securityfocus [34], Microsoft Security Bulletins [35] and Symantec Security Response [36]. The search of vulnerability databases helps finding known vulnerabilities, which might not be detected by the security testing, and to verify the findings of the security testing. The security testing on the other hand gives a good overview of the state of the system, and information on what the attacker really sees when attacking the system, which is very useful when securing the system. In the risk assessment the attacks, which the system can be exposed to, had to be identified. For this we used a list of attack categories defined by Cheswick and Bellovin [32, 33]. These risk categories include

all attack types, but at the same time they do not overlap. The security tests were performed using the Open Source Security Testing Methodology Manual v2.1 [20]. This is quite a thorough methodology for security testing, although still under development. The methodology is designed for security testing in several types of information systems and networks. Only a fraction of this is relevant for the system being tested here. For that reason we only used the relevant modules of section C: "Internet Technology Security". The modules used were System Services Identification, Vulnerability Research and Verification, Routing and Containment Measures Testing.

Apply vulnerability reducing measures After the security assessment of the unsecured system was carried out, the security measures were added.

Risk assessment of improved system The risk assessment of the improved system was just a repetition of the risk assessment carried out for the unsecured system.

Calculating effectiveness The calculation of effectiveness was done using the formula by Nystuen and Hagen [13]:

$$E = \frac{C_{EU} - C_{EM}}{C_{EM}} \tag{4.1}$$

C_{EU} - expected risk of the system without the security measure implemented
C_{EM} - expected risk of the system with the security measure implemented
E - Index of the performance of the measure

Calculate costs The calculation of cost was done using guidelines made by National Institute of Health (NIH) [30], for the use in cost-benefit analysis of IT-projects. The annual cost of the home office for the expected lifetime of the system was calculated. The annual cost consists of Implementation costs, maintenance costs, software costs, hardware costs, support costs, and user training. The Implementation costs were calculated using the number of man-hours needed to implement the security measure and multiplying it with the salary costs. The maintenance costs, support costs and user training were calculated using the number of man-hours needed each year and multiplying it with the salary costs. The average salary increase per year was taken into account; this was the average salary increase for the previous four years. The costs were summarized for each year and the present value of the expenses is calculated using the formula:

$$P = F\frac{1}{(1+I)^n} \tag{4.2}$$

where P = Present Value, F = Future Value, I = Interest Rate, and n = number of years. The interest rate used was the average interest rate over an eight years period. This formula transforms future NOK values into present NOK values which gives us a common unit of measurement to compare the alternatives.

Calculate cost-effectiveness For the calculating of the cost-effectiveness of the security measures we used the formula described by Levin and McEwan [11]. The cost-effectiveness ratio (CER) is computed by dividing the cost (C) of the security measure and its effectiveness (E).

$$CER = \frac{C}{E} \tag{4.3}$$

The output of this formula is then ranged according to its cost-effectiveness ratio.

Sensitivity analysis A sensitivity analysis was to be performed on the experimental data. Due to time limitation this was not performed in this thesis.

4.3 Case Studies

To answer the research questions set up in Section 1.4, we made use of three different case studies representing different environments and threat level.

Case 1 - Bank The example bank has 10 000 employees situated around the country. This is a huge bank according to Norwegian standards. It is estimated that the bank has 500 users of home offices.

Case 2 - County Council This represents a county council with 600 employees. The employees works within the areas of education, health care, renovation, administration, IT, welfare, etc. 20 employees are using home offices.

Case 3 - Mid-size Business This is a business with 2500 employees where about 100 use home offices. Their main area of business is as a power supplier and security services.

4.4 Experimental Design

4.4.1 Home Office Solutions to Be Tested

A basically unsecured system and ten systems using different security mechanisms have been tested. Because of the great amount of security measures available and the difficulty of drawing a line between what are the security measures of the home office and what are the security measures of the corporate network, some limitations had to be introduced. The security measures that were tested were only those that were physically installed on the home office computer. This thesis did not compare different algorithms for secure communication or different authentication schemes. The vulnerability tests only tested a basic Windows XP Professional system. No extra software, except of security software was added. In a real life situation this would not very likely be the case. The security measures tested were software patching using Windows update, software hardening, Internet Connection Firewall (Windows firewall), Zone Alarm Pro Firewall, Norman Antivirus, VPN using Windows' L2TP over IPSec client and VPN, NAT, ACL using D-Link DI-804HV Router. These seven security measures were set together in different configurations and tested to find the most effective configuration.

The first home office solution to be tested were a basic solution with no extra security measures added, except of those already present by default in the operating system. The unsecured system was compared with different secured systems in order to measure the effectiveness of different home office solutions considered in this experiment.

Unsecured System This was a system running Windows XP Professional Service Pack 1. The system ran the standard out-of-the-box configuration. No security mechanisms, not turned on by default, were used. No patches released after the release date of Service Pack 1 were added.

Ten different home office solutions were tested and compared against the unsecured system. A short summary of these is given below:

Solution 1 This solution was based on the out-of-the-box configuration of Windows XP Pro. Service Pack 1. No further updates had been installed. Norman antivirus v5.8 had been installed and was up-to-date. The Windows XP L2TP over IPSec client was activated.

Solution 2 This solution was based on the out-of-the-box configuration of Windows XP Pro. Service Pack 1. No further updates had been installed. Norman antivirus v5.8 had been installed and was up-to-date. The Windows Internet Connection Firewall (ICF) was enabled with its default configuration in place. The Windows XP L2TP over IPSec client was activated.

Solution 3 This solution was based on the out-of-the-box configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman antivirus v5.8 had been installed and was up-to-date. The Windows XP L2TP over IPSec client was activated.

Solution 4 This solution was based on the out-of-the-box configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman antivirus v5.8 had been installed and was up-to-date. The Windows Firewall was enabled with its default configuration in place. The Windows XP L2TP over IPSec client was activated.

Solution 5 This solution was based on the out-of-the-box configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman antivirus v5.8 had been installed and was up-to-date. The Windows XP L2TP over IPSec client was activated. Zone Alarm Pro firewall was installed.

Solution 6 This solution was based on a hardened configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman antivirus v5.8 had been installed and was up-to-date. The Windows Firewall was enabled. The Windows XP L2TP over IPSec client was activated.

Solution 7 This solution was based on a hardened configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman antivirus v5.8 had been installed and was up-to-date. Zone Alarm Pro firewall was installed. The Windows XP L2TP over IPSec client was activated.

Solution 8 This solution was based on the out-of-the-box configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman antivirus v5.8 had been installed and was up-to-date. The Windows Firewall was enabled with its default configuration in place. A broadband router with NAT, ACL and IPSec was used.

Solution 9 This solution was based on the out-of-the-box configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman antivirus v5.8 had been installed and was up-to-date. Zone Alarm Pro firewall was installed. A broadband router with NAT, ACL and IPSec was used.

Solution 10 This solution was based on a hardened configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman antivirus v5.8 had been installed and was up-to-date. Zone Alarm Pro firewall was installed. A hardened broadband router with NAT, ACL and IPSec was used.

4.5 Test Environment

4.5.1 Network Properties

The test network was set up in two different ways depending on whether the broadband router was used or not. The network topology is illustrated in the Figure 1. In Network Scenario 1, the home office makes use of a broadband router to connect to the Internet while in Network Scenario 2 the home office computer is connected directly to the Internet.

4.5.2 Hardware

The hardware used during the security test is described below:

Two Dell OptiPlex GX1: One acted as a file server, the other acted as the home office workstation

- Intel Pentium III 450 MHz
- 128 MB SDRAM
- 30 GB IDE hard drive
- CD-ROM
- Network Interface Card

Toshiba Equium 3300M

- Intel Pentium III 667 MHz
- 512 MB RAM
- 10 GB IDE hard drive
- CD-ROM
- 2 x Network Interface Card

This computer acted as an enterprise firewall, protecting the internal network of the organization.

Dell Dimension XPS B800

- Intel Pentium III 800 MHz
- 384 MB RDRAM
- 40 GB 7200 RPM IDE hard drive
- DVD/CD-ROM
- Network Interface Card

This was the computer of the attacker.

D-Link DI-804HV Router - This was the home office router

CNet 5-port switch 10/100 Mbit/s - This switch represents the Internet, connection the different networks and computer together.

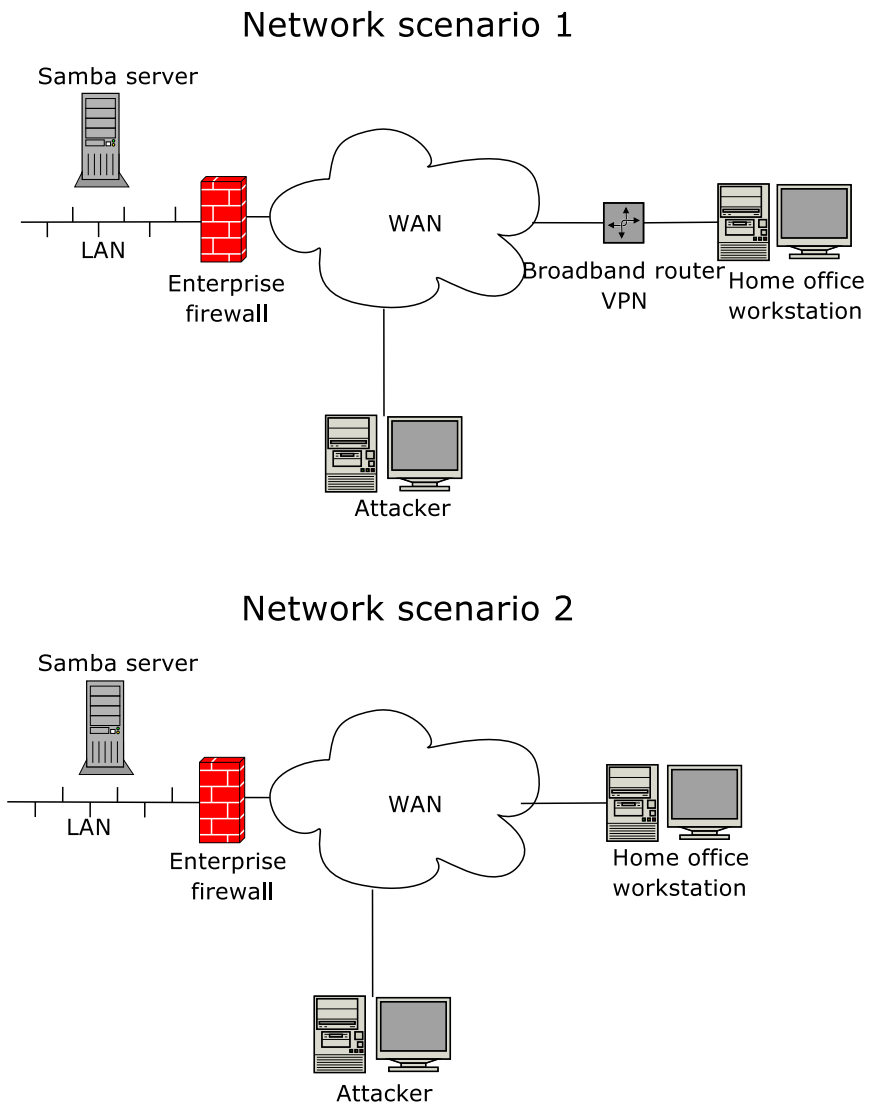

Figure 1: Network Scenarios

4.5.3 Software

In this section, different pieces of software used on the test system are described. The software is listed according to the computer it was installed on. For a better view of where each computer was situated in the test system, see Figure 1.

Attacker's computer This computer ran dual boot Windows XP Pro SP2 / SuSE Linux 9.2. A short description of the penetration tools used is given below

- Firewall tester 0.9 (Ftester) [37] is an open source tool designed for testing firewall filtering policies and IDS capabilities. Ftester consists of a packet injector and a packet sniffer which are placed on each side of the firewall. A configuration file containing the tests to be performed is written, and used by the packet injector when sending packets towards the firewall. Firewall Tester is supported by ISECOM; it is compliant with the OSSTMM requirements.
- Nessus 2.2.4 [38] is an open source vulnerability scanner. Nessus uses a client/server architecture where the server performs the scans and the client is used to configure the server and to analyse the results. Plugins are used to test the system for weaknesses. One can choose what class of plugins to run to make it reflect the system being tested. Nessus is able to recognize services running on any port, even though they do not run on the standard Internet Assigned Numbers Authority (IANA) port number. Nessus uses plugins which not only scan for vulnerabilities but also try to exploit these and report if it was successful in exploiting the weakness.
- Nmap 3.70 [39] is probably the most popular network scanner. It offers several different scanning techniques, including UDP scans, TCP connect scan, half open scan, bounce back attack, ping sweep, FIN scan, ACK sweep, XMAS tree scan, SYN sweep, IP protocol scan and NULL scan. Other features are OS detection and TCP/IP fingerprinting, which come in handy during enumeration of a system.
- Hping2 [40] can do typical ping echo request / echo reply, but also similar tests using any IP packets, Including ICMP, UDP, TCP and Raw-IP protocols. Hping2 can be used to map networks, test firewall rules, port scanning and identify OS remotely.
- Enum [41] is a tool using null session to obtain information about users, groups, shares and system information.
- Winfingerprint 0.6.1 [42] is a Windows enumeration scanner which is capable of performing SMB, TCP, UDP, ICMP, RPC and SNMP scans. Winfingerprint can also enumerate OS, users, groups, SIDs, password policies, services, service packs and hotfixes, NetBIOS shares, transports, sessions, disks, security event logs, time of day, active directory and WMI APIs.
- Amap 4.8 [43] is used to identify applications even though they do not run on their default port. Amap uses a different technique from the one used by Nmap. These two programs are therefore used together for a more reliable identification of services.

Enterprise Firewall This computer was running Astaro Security Linux v5.022.

Home Office Computer The home office computer ran Windows XP Pro. During the testing several different configurations were used and extra software was added, as described later. The software used (not necessarily used at the same time) are listed below.

- Norman Antivirus v5.8
- Windows XP L2TP over IPSec client
- ZoneAlarm Pro firewall (5.5.062.011)
- Internet Connection Firewall (ICF) (SP1)
- Windows Firewall (SP2)

Samba Server This computer was running Fedora Core 3 Linux with a Samba 3 server.

4.5.4 Configuration Details

The way different security measures were configured during the test is described below.

Antivirus Norman Antivirus was set to automatically update once a day.

Broadband Router This was a NAT router with the ability to set up an ACL rule set. The rule set was set to deny all inbound connections from the Internet. While all connections from the LAN are allowed. IPSec configuration: IPSEC, IKE - DH group MODP768, 3DES, SHA1, Lifetime 1000 Kbyte. IPSEC – DH group MODP768, 3DES, SHA1, Lifetime 1000Kbytes

Internet Connection Firewall Default configuration was used.

Patched System The system that was considered up-to-date in this thesis consists of Windows XP Professional Service Pack 2 and the following patches:

1. Windows Malicious Software Removal Tool - March 2005 (KB890830)
2. Update for Windows XP (KB887742)
3. Security Update for Windows XP (KB885250)
4. Security Update for Windows XP (KB873333)
5. Security Update for Windows XP (KB888113)
6. Cumulative Security Update for Internet Explorer for Windows XP (KB867282)
7. Security Update for Windows XP (KB891781)
8. Security Update for Windows Messenger (KB887472)
9. Security Update for Windows XP (KB890047)
10. Security Update for Windows XP (KB888302)
11. Security Update for Windows XP (KB885835)
12. Windows Update website Security Update for Windows XP (KB890175)
13. Security Update for Windows XP (KB885836)

14. Critical Update for Windows XP (KB886185)
15. Security Update for Windows XP (KB873339)
16. 816093: Security Update Microsoft Virtual Machine (Microsoft VM)

A fully updated system in these experiments was a system having the latest patches as of 18th of March 2005.

L2TP over IPSec The Windows XP L2TP over IPSec client was configured to use Microsoft CHAP Version 2 and a preshared key for authentication.

Host Hardening The hardening of Windows XP was based on a Template provided by NIST (Downloadable from [5]). This template includes modified account policy settings, modified local policy settings, modified event log setting, managing restricted groups, managing system services, modified register security settings, and modified file system security setting. This template was designed for the use in home offices and suited the test system's needs for security. It would be a rather long and detailed process to explain all the changes made to the home office system during the hardening process. For more details about the hardening process see [5].

The hardening of Internet Explorer followed the NIST guidelines [5]. The following changes were done under tools -> Internet Options -> Security -> Internet Zone -> Custom Level.

- ActiveX controls and plugins: Disable Script ActiveX controls marked safe for scripting.
- Scripting: Disable Active scripting
- Scripting: Disable scripting of Java applets

The following changes were done under tools -> Internet Options -> Advanced.

- Security: Enable "check for server certificate revocation".
- Security: Enable "Empty Temporary Internet Files folder when browser is closed"

The following changes were done under tools -> Internet Options -> Privacy -> Advanced.

- Enable "Override automatic cookie handling"
- Select Prompt on "Third-party Cookies"

The hardening of Outlook Express followed the NIST guidelines [5]. The following changes were done under tools -> Options.

- Send tab: Change the mail sending format from HTML to plain text
- Security tab: Set the security zone to Restricted sites zone under virus protection.

The router was also hardened by enabling statefullness and disabling WAN ping.

Personal Firewall Zone Alarm Pro firewall was installed. Two Security zones were defined: Internet Zone and Trusted Zone. Internet Zone Security was set to High (Stealth Mode), while Trusted Zone Security was set to Medium. The trusted zone served for the VPN connection to the office. Program Control was set to High. Internet Explorer, Outlook Express, Norman Antivirus and Windows Update were allowed to enter the Internet. Inbound and outbound mailsafe protection was on. Cookie control and mobile code control were turned off.

4.5.5 Security Testing

The methodology used for this testing is based on the OSSTMM v2.1 [20]. The modules used were System Services Identification, Vulnerability Research and Verification, Routing and Containment Measures Testing. Several tools were used during the testing. These tools were Nmap, Nessus, Enum, Ftester, Winfingerprint, Hping2 and Amap. Vulnerability databases, Securityfocus [34], Microsoft security bulletin [35] and Symantec Security Response [36] were used to identify weaknesses and vulnerabilities of the system. A more thorough examination of the security test is presented below:

System Services Identification The main objective of this module is to identify open, closed or filtered ports, active services, service types, service application type and patch level, OS type, and patch level. Several tests should be performed in order to obtain this information. The tools used were Nmap, Hping2, Amap, Enum, Winfingerprint. Nmap and Hping2 performed TCP Connect(), TCP Syn scan, Source Port Scan, UDP Scan, ACK Scan, FIN Scan, Null Scan, and XMAS scan. More information about these scans is provided in Section 4.5.6. Nmap was also used to perform OS detection and fingerprinting. Amap is a tool that was used to detect the service running on different ports. It uses a different approach than Nmap and was therefore used to verify the results. Amap uses the logs obtained by Nmap scans to check the service fingerprints to identify the services running. Services running on non-standard ports are also identified. Other tools used are Winfingerprint and Enum, which both are tools used for enumeration of a computer system. Enumeration is the process of identifying a system's running services and its known weaknesses [21]. Scan options used with Winfingerprint were: Domain, win32 OS version, user, patch level, Null IPC$ Sessions, services, Mac Address, Netbios shares, Disks, Sessions, Date and time, groups, event log, print host rpc bindings, show error, traceroute host. Scan options used with Enum were: -U get userlist, -M get machine list, -N get namelist dump, -S get sharelist, -P get password policy information, -G get group and member list.

Vulnerability Research and Verification The main objective of this module is to find vulnerable applications or services running on the system, patch level of the system and applications, and possible denial of service vulnerabilities. The tool used for this purpose was Nessus [38]. Ideally one uses at least two different vulnerability scanners to perform the vulnerability scan in order to reduce the occurrence of false positives and false negatives. Due to limited resources and the limited availability of free vulnerability scanners, in this thesis only Nessus was used. The results were verified manually to eliminate false positives. By comparing the results from the vulnerability scan with results obtained by means of other tools during the security

scan, and by checking out all vulnerabilities found with vulnerability databases, to see if the vulnerabilities detected may occur on that platform with that particular configuration, most false positives may be removed. False negatives may be more difficult to find. Comparing the vulnerability scan with the other scans performed during the security test may reveal false negatives. The tools used employ different scanning techniques and this may give different results. The use of vulnerability databases may also reveal vulnerabilities not discovered during security testing.

The configuration of Nessus used in this thesis was as follows. No system tested had patches newer than 18th of March 2005, which was considered as up-to-date in this experiment. For this reason Nessus had not been updated and no new plug-ins have been added after that date. The plugin groups used in this experiment were: Service Detection, Denial of Service, Windows: Microsoft Bulletins, Windows, Misc, General, RPC, backdoors, firewalls, SMTP problems, Remote Access, useless services, Windows: User management, Settings. Plugin groups not considering vulnerabilities relevant to the Windows platform were filtered out. For the port scanning Nessus used several scanners: Scan for LaBrea tarpitted hosts, SYN Scan, Nessus TCP scan, Netstat scanner. All ports 0 - 65535 are scanned.

The vulnerability databases used for identifying vulnerabilities were Securityfocus [34], Microsoft Security Bulletins [35] and Symantec Security Response [36].

Routing The primary objective of this module is to find router type, services and system information, map the ACL implemented and a list of packets that may enter. Two tools were used for this purpose: ftester and nmap. Ftester was used to map the ACL settings and to check for packets that may enter. The scan consists of several different tests: SYN stealth scan, source port scan, RST scan, UDP scan, ACK scan, FIN scan, NULL scan and XMAS scan. Nmap was used to find router type, services and system information. For more information about the scan types, see Section 4.5.6.

Containment Measures Testing No tests have been found to perform an evaluation of the containment measures. This was done theoretically instead, using vulnerability databases and virus databases.

4.5.6 Scan Methods

A description of various scan methods is given in [44]. These scan methods were used during the security testing. Nmap, Hping2 and ftester were used to carry out the scans. All scans were performed on ports 0 - 65535. They were used during the testing of the system service identification module and the routing module.

TCP Connect() This scan opens a connection to every port defined in the scan. If the port is listening the connect() is successful.

TCP SYN Scan This scan does not open a full TCP connection. It sends a SYN packet and waits for response. If we receive an SYN|ACK packet, the port is listening and the connection is closed with a RST packet; if we receive a RST packet, the port is not listening.

Source-Port Scan During this scan, the source port number used in the scan is set. Some naive firewalls have exceptions in their rule sets that let DNS (53) and FTP-DATA (20) to get through and establish a connection. This scan takes advantage of this.

RST Scan A RST scan sends RST packets to the host. If the host exists, no response is received. If a ICMP "host unreachable" message is received the host does not exist. This is known as inverse mapping [45].

UDP Scan This scan determines which UDP ports are open by sending 0 bytes UDP packets to the port on the target machine. If the ICMP "port unreachable" message is received the port is closed. If an UDP response is received the port is open, and if nothing is received at all, the state shown by Nmap is open|filtered, which means the port is open or the communication is filtered.

ACK Scan This scan can be used to determine if a firewall is statefull or only a packet filtering firewall. If the firewall returns a RST packet, the scanned port is unfiltered. If it returns an ICMP unreachable packet or nothing at all the port is filtered.

FIN Scan Closed ports are required to answer the FIN packet with a RST packet while open and filtered ports drop the packet. MS Windows does not follow the standard and drops FIN packets in either way. This causes closed ports to seem open when performing a FIN scan.

Null Scan Closed ports are required to answer the packet with a RST packet while open and filtered ports drop the packet. Null scans use no flags. MS Windows does not follow the standard and drops the packets in either way. This causes closed ports to seem open when performing a Null scan.

XMAS Tree Scan Closed ports are required to answer the packet with a RST packet while open and filtered ports drop the packet. XMAS Tree scan uses the FIN, URG and PUSH flag. MS Windows does not follow the standard and drops the packets in either way. This causes closed ports to seem open when performing a XMAS Tree scan.

4.5.7 Cost Calculation

The cost calculation was performed using the methods described in [30] for the use in cost-benefit and cost-effectiveness analysis. This calculation considers personnel costs, indirect costs, depreciation, and annual costs. Future cost is expressed in present values.

The cost calculation was based on several assumptions. The number of man-hours needed to implement, maintain and support the use of each security measure is very difficult to predict. The numbers used in this thesis were based on the use of centralized administration of the antivirus software, firewall policy administration, patch administration (not in the case of the country council), and MS Windows configurations and policies, such as operating system hardening policies, firewall (MS Windows firewall) policies and VPN client configuration. We assumed that the configuration tools needed were already in use by the organization for use on the internal network. Therefore no extra training and server investments are needed.

Personnel Costs For the calculation of personnel costs, we used income statistics for Norway provided by Statistisk Sentralbyrå [46]. The income statistics of 2003 shows that the average monthly income for an employee in the ICT sector was 34 991 NOK. Presumably the numbers are before tax deduction (this is not stated in the statistics), and reflects what the employee must be paid in salary and not what the employees make after income tax is paid. We assumed that it is 22 workdays per month and that it is 8 hours workday. This gives a salary of NOK 199 per hour before tax deduction. Average salary increases per year between 1999 and 2003 was 5,8 percent. This number was used in this thesis to represent the expected salary increase per year.

Indirect Cost Indirect costs are explained by NIH [30] to be costs such as indirect labour, indirect material, fixed costs such as depreciation, taxes, utilities, and insurance. Indirect labour costs may be the employee trying to solve a problem under the guidance of the helpdesk or on his own. None of these costs were considered in this cost-effectiveness analysis, because of the uncertainty surrounding the real costs and relatively small amount of money involved.

Depreciation Depreciation was not considered in this thesis as the investments in hardware are minimal and it would have no value for sale later on. NIH [30] defines depreciation as the reduction of the estimated value of a capital asset and as a method used to spread the cost of tangible capital assets over an asset's useful life. Usually this is only done with items with a value greater than $5000, approx NOK 30 000. The equipment used in this thesis is nowhere near that value and depreciation is therefore not considered.

Annual Cost The annual cost of the home office for the expected lifetime of the system was calculated. The annual cost consists of Implementation costs, maintenance costs, software costs, hardware costs, support costs, and user training costs. The Implementation costs were calculated using the number of man-hours needed to implement the security measure and multiplying it with the salary costs. The maintenance costs, support costs and user training were calculated using the number of man-hours needed each year and multiplying it with the salary costs. The average salary increase of 5,8 percent per year was taken into account. The costs were summarized for each year and the present value of the expenses was calculated using the formula described in [30]:

$$P = F\frac{1}{(1+I)^n} \tag{4.4}$$

where P = Present Value, F = Future Value, I = Interest Rate, and n = number of years. The interest rate to be used was the average interest rate between 1995 and 2003 which was 4,44 percent in Norway [47]. This formula transforms future NOK values into present NOK values, which gives us a common unit of measurement to compare the alternatives.

Bank The bank has 500 home offices to implement, maintain and support. The lifetime of the home office investment was set to four years. The salary was set to NOK 199 per man-hour. A salary increase of 5,8% was part of the calculation. The antivirus and firewall prices were calculated as an average of prices collected from

eTrust, Trend Micro, McAfee, Kaspersky and Symantec. Only prices available on their web sites were used. The prices for renewal of licenses are 30% off the original price. Prices were collected on 20.05.2005. The initial cost of the antivirus software was estimated to NOK 194 per license, while the cost of upgrading the antivirus software was estimated to NOK 135 per license per year. The initial cost of the personal firewall / antivirus software package was estimated to NOK 281 per license, while the cost of upgrading the personal firewall / antivirus software package was estimated to NOK 196 per license per year. The cost of a broadband router was estimated to NOK 490 per router. Antivirus, firewall and operation system management are performed remotely using the secure VPN connection. Table 3 shows the estimated number of hours used for implementation, maintenance and support each year. Work on implementation is only the first year.

Table 3: Bank - Workload in Hours

Security Measure	Implementation	Maintenance	Support
Solution 1	35	100	100
Solution 2	60	125	100
Solution 3	85	150	100
Solution 4	110	175	100
Solution 5	85	160	110
Solution 6	235	215	100
Solution 7	210	200	110
Solution 8	150	175	100
Solution 9	125	160	110
Solution 10	250	200	110

County Council The county council has 25 home offices to implement, maintain and support. The lifetime of the home office investment was set to six years. The salary was set to NOK 199 per man-hour. A salary increase of 5,8% was part of the calculation. The antivirus and firewall prices were calculated as an average of prices collected from eTrust, Trend Micro, McAfee, Kaspersky and Symantec. Only prices available on their web sites were used. The prices for renewal of licenses are 30% off the original price. Prices were collected on 20.05.2005. The initial cost of the antivirus software was estimated to NOK 212 per license, while the cost of upgrading the antivirus software was estimated to NOK 149 per license per year. The initial cost of the personal firewall / antivirus software package was estimated to NOK 296 per license, while the cost of upgrading the personal firewall / antivirus software package was estimated to NOK 207 per license per year. The cost of a broadband router was estimated to NOK 630 per router. Antivirus, firewall and operation system management are performed remotely using the secure VPN connection. Table 4 shows the estimated number of hours used for implementation, maintenance and support each year. Work on implementation is only the first year.

Table 4: County Council - Workload in Hours

Security Measure	Implementation	Maintenance	Support
Solution 1	50	50	50
Solution 2	75	75	50
Solution 3	50	50	50
Solution 4	75	75	50
Solution 5	50	55	55
Solution 6	150	100	50
Solution 7	125	80	55
Solution 8	75	75	50
Solution 9	50	55	55
Solution 10	125	80	55

Mid-size Business The mid-size business has 100 home offices to implement, maintain and support. The lifetime of the home office investment was set to five years. The salary was set to NOK 199 per man-hour. A salary increase of 5,8% was part of the calculation. The antivirus and firewall prices were calculated as an average of prices collected from eTrust, Trend Micro, McAfee, Kaspersky and Symantec. Only prices available on their web sites were used. The prices for renewal of licenses are 30% off the original price. Prices were collected on 20.05.2005. The initial cost of the antivirus software was estimated to NOK 198 per license, while the cost of upgrading the antivirus software was estimated to NOK 139 per license per year. The initial cost of the personal firewall / antivirus software package was estimated to NOK 286 per license, while the cost of upgrading the personal firewall / antivirus software package was estimated to NOK 200 per license per year. The cost of a broadband router was estimated to NOK 560 per router. Antivirus, firewall and operation system management are performed remotely using the secure VPN connection. Table 5 shows the estimated number of hours used for implementation, maintenance and support each year. Work on implementation is only the first year.

Table 5: Mid-Size Business - Workload in Hours

Security Measure	Implementation	Maintenance	Support
Solution 1	20	60	60
Solution 2	30	80	60
Solution 3	30	90	60
Solution 4	40	110	60
Solution 5	30	100	70
Solution 6	100	140	60
Solution 7	90	130	70
Solution 8	80	130	60
Solution 9	70	120	70
Solution 10	130	150	70

5 Results

In this chapter we present the results of the thesis in the same order as of the research questions stated in Section 1.4.

5.1 Most Suitable Methods for Cost-effectiveness Analysis

Several methods were considered when answering research question one. In the end the methods used in the methodology for cost-effectiveness analysis, described in Chapter 3, were chosen. This methodology is built around a framework of eight steps as described in Section 3.1. We have not identified any reliability or validity issues surrounding the use of this framework. To perform each of the eight steps leading to the finalization of the cost-effectiveness analysis, several other methods have to be used.

- The risk assessment is conducted using a risk assessment method [17], see Section 3.2, developed and recommended by National Institute of Standards and Technology (NIST). We have tried to make the risk assessment results as reliable as possible by using security testing and vulnerability database searches as part of the risk assessment. Still one has to use subjective opinions when doing a risk assessment, because of the lack of attack statistics of similar systems. As long as the probability of an attack cannot be estimated using statistics, some level of subjective opinion has to be used. The impact assessment of an attack may also be a bit subjective, even though we try to base the results on available information of system vulnerabilities.
- The security testing is performed using the Open Source Security Testing Methodology Manual [20], see Section 3.3. This is a peer-reviewed security testing methodology that is claimed to be repeatable and valid beyond the "now" time frame. For the parts of the home office system not easily testable with the OSSTMM, mostly browser and e-mail client vulnerabilities, a vulnerability database search is performed to identify known vulnerabilities.
- The cost calculation is performed using the method described in [30], see Section 3.5. The method makes use of all costs incurring throughout the lifecycle of an asset, such as costs of purchase, maintenance, upgrades, support, user training, and software licensing. The cost calculation method is based on the cost calculation section of the cost-benefit analysis guide for NIH IT projects.

The results of the cost and effectiveness calculations are used to calculate the cost effectiveness ratio of each security measure considered. A formula presented by [13] is used to calculate the effectiveness from the results of the risk assessment, see Section 3.4. The output of this formula is together with the output of the cost calculation used to calculate the cost-effectiveness ratio of the security measures. For this calculation a formula presented by [11] is used, see Section 3.6.

The methodology presented in this thesis consists of several well tested methods with no known reliability or validity issues. The effectiveness and the cost-effectiveness cal-

culations are based on methods recommended for cost-effectiveness analysis by several sources [11, 13]. We consider this methodology to have good reliability and validity.

The methodology has been tested out on three case studies with success. The results of these tests are presented in Section 5.3.

5.2 Adjustment of cost-effectiveness analysis to reflect different organizational needs of security

Research question two was answered using the threat identification method provided in step 2 of the risk assessment methodology in [17]. When performing the threat identification, all threat sources that make up any level of threat against the organization are identified. The next step is to identify the threat source's motivation for attacking the system. Finally the threat actions are identified. When the threat identification is performed, we have a good overview of potential security threats, their motivations and the probable attack methods used by the threat sources to achieve their goals. The results are used in the risk assessment.

This method is just as accurate as the available statistics and information about possible threats. The more information one can base the threat identification on, the more accurate the results become. It is important to spend some time doing research on former incidents and possible threat sources before finalizing the threat identification.

Threat identification was performed as a part of the risk assessment performed in this thesis. As the results in Section 5.3 show the three organizations described in the case studies all had different threat sources to worry about. The threat sources identified for the bank were the hacker, the computer criminal, the malicious code writer, and the industrial espionage agent. The threat sources identified for the county council were the hacker, the computer criminal, and the malicious code writer, while the threat sources identified for the mid-size business were the hacker, the computer criminal, the malicious code writer, the industrial espionage agent, and the terrorist.

A short description of these threat sources is given next:

- The hacker might be very knowledgeable but with insufficient resources compared with industrial espionage agents and computer criminals. His motives are a combination of proving his skills and the challenge. Some hackers might only attack with automatic tools and if the security of the home office is poor, a hacker may perform a random attack to exploit a security weakness in the home office system. The curiosity of the hacker might lead him to try to enter the organization's internal computer system from the home office system. Others might like the challenge of getting past advance security barriers such as the security barriers provided by a bank. Well secured systems are popular targets for hackers trying to achieve recognition in the hacker subcultures. These hackers might try to use the home office computer as a backdoor into these computer systems.
- The computer criminal enters the system as part of a larger criminal act. The reason can be to use system resources to share illegal material, delete information, alter in-

formation, or steal information. The attacker can be paid to do this or demand money as part of a blackmailing process. The computer criminal has more resources available to his disposal then the hacker. He can be part of organized crime. A computer criminal may try to blackmail the organization by stealing or altering information, take control over vital infrastructure or by threatening to do so. The home office might provide an entrance to the computer system.

- The malicious code writers are the people writing worms, viruses and other malicious code. Some might be hackers writing code for their own use, but the greatest threat are the people writing new viruses every time a new vulnerability is discovered. They are not aiming at a particular organization, but at the whole Internet community. Creation of some viruses might be economically motivated, like those used to send SPAM from the infected computers. Other viruses install backdoor programs or are used to launch Distributed Denial of Service attacks.
- The industrial espionage is performed to get the upper edge over the competitors. The attackers are highly funded and try to get a hand on secret/sensitive information in a way that is difficult to detect. Most likely nothing is deleted or altered. Files are copied and the attacker leaves without a trace. The motive is purely economical. The threat source might be a competing bank or it might be someone trying to get sensitive information about one or several of the bank's customers. In the case of the mid-size business it can be a competitor looking for information that can give him the upper edge in the competition or it can be another nation state looking for information on the power supply infrastructure in Norway.
- A terrorist is a person or a group of people who use violence or threats of violence to reach their goal [48]. Groups might train their own cyber warriors to fight out a battle in a foreign country not accessible otherwise. The aim is massive destruction or blackmail. The terrorist threat to the mid-size business is present due to its involvement in power production. A terrorist taking control over a hydroelectric power plant or the power supply infrastructure can be very damaging. A terrorist might find the home office system to be the easiest way to enter the organization's computer system.

5.3 Cost-effectiveness Ratio of the Different Vulnerability Reducing Measures

A cost-effectiveness analysis was performed on three case studies using the methodology described in Chapter 3. The results of the cost-effectiveness analysis are presented below, one case at the time.

5.3.1 Case 1 - Bank

Results of Threat Identification Four threat sources relevant for this case were identified: the hacker, the computer criminal, the malicious code writer, and the industrial espionage agent. Their motivation and their threat actions are described in Table 6. Table 6 is based on a table of human threats defined by [17].

Table 6: Bank - Human Threats

Threat-Source	Motivation	Threat Actions
Hacker	Challenge Ego Rebellion Revenge	Hacking Unauthorized system access System intrusion
Computer Criminal	Computer resources Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	Computer Crime Fraudulent act (e.g replay, impersonation, interception) Information bribery System intrusion Blackmail
Malicious Code Writer	Destruction System Access Monetary Gain	Denial of Service System attack
Industrial espionage agent	Competitive Advantage	Information theft Unauthorized system access System penetration

Results of Risk Assessment The results of the risk assessment are presented in Table 7. The risk of a successful attack is rated for each threat source present in one of the vulnerability groups described in Section 3.2.1. The results are based on the likelihood of such attacks and the impact these attacks may have on the availability, confidentiality, and integrity of the system. To make the risk assessment more reliable it was based on the results of a security test performed in combination with a vulnerability database search as explained in Section 4.5.5. The results of the security testing are found in Appendix A. The results are based on the risk rating of the threat source that is found to make up the greatest risk to the system. The numbers present in the column "Total Score" are used in the calculation of the effectiveness of the security measure.

Table 7: Bank - Risk scale: High (>200 - 400); Medium (>40 - 200); Low (1 - 40)

System	Bugs And Buckdoor	Authentication Failure	Information leakage	Denial of Service	Total Score
Unsecured	HIGH	HIGH	MEDIUM	MEDIUM	300
Solution 1	HIGH	HIGH	LOW	LOW	215
Solution 2	MEDIUM	MEDIUM	LOW	LOW	106
Solution 3	HIGH	MEDIUM	LOW	LOW	160
Solution 4	MEDIUM	MEDIUM	LOW	LOW	106
Solution 5	LOW	LOW	LOW	LOW	26
Solution 6	MEDIUM	MEDIUM	LOW	LOW	52
Solution 7	LOW	LOW	LOW	LOW	12
Solution 8	MEDIUM	MEDIUM	LOW	LOW	106
Solution 9	LOW	LOW	LOW	LOW	26
Solution 10	LOW	LOW	LOW	LOW	12

The results show that solution 1 scores HIGH on the risk scale. Solutions 2,3,4,6,8 score MEDIUM on the risk scale and Solutions 5,7,9,10 score LOW on the risk scale.

Results of Cost Calculation The results of the cost calculation are shown in Table 8. The most interesting is the "Present Value", which is used in the cost-effectiveness calculation later on. This is the total cost of the security measure transformed into present value giving us a common unit of measurement to compare the alternatives.

Table 8: Bank - Cost Calculations (NOK)

Security Measure	Implement-ation Cost	Mainten-ance Cost	Soft-ware Cost	Hard-ware Cost	Support Cost	Total	Present Value
Solution 1	6965	86797	299500	0	86797	480059	432848
Solution 2	11940	108496	299500	0	86797	506733	457041
Solution 3	7960	130195	299500	0	86797	524452	472660
Solution 4	12935	151894	299500	0	86797	551126	496853
Solution 5	7960	138875	434500	0	95476	676811	610224
Solution 6	37810	186613	299500	0	86797	610720	551758
Solution 7	32835	173594	434500	0	95476	736405	665129
Solution 8	20895	151894	299500	245000	86797	804086	739059
Solution 9	15920	138875	434500	245000	95476	929771	852430
Solution 10	40795	173594	434500	245000	95476	989365	907335

Results of Cost-effectiveness Ratio Calculation The numbers obtained in the cost and the effectiveness calculation are used to calculate the cost-effectiveness ratio as shown in Table 9.

Table 9: Bank - Cost-effectiveness calculation

System	Effectiveness	Cost	Cost-effectiveness Ratio
Solution 1	0,276595745	432848	1564914
Solution 2	0,923076923	457041	495128
Solution 3	0,875	472660	540183
Solution 4	0,923076923	496853	538257
Solution 5	10,53846154	610224	57904
Solution 6	8,375	551758	65881
Solution 7	24	665129	27714
Solution 8	0,923076923	739059	800647
Solution 9	10,53846154	852430	80888
Solution 10	24	907335	37806

Results of Cost-effectiveness Analysis The results of the cost-effectiveness analysis has been ranked in Table 10.

Table 10: Bank - Ranking of Cost-effectiveness

Number	System
1	Solution 7
2	Solution 10
3	Solution 5
4	Solution 6
5	Solution 9
6	Solution 2
7	Solution 4
8	Solution 3
9	Solution 8
10	Solution 1

The results show that Solution 7 has the best overall cost-effectiveness ratio of the security measures used in this case study. A closer look at the results shows us that the four security measures scoring LOW on the risk scale are also the security measures with the best cost effectiveness ratio.

5.3.2 Case 2 - County Council

Results of Threat Identification Three threat sources relevant for this case were identified: the hacker, the computer criminal and the malicious code writer. Their motivation and their threat actions are described in Table 11. Table 11 is based on a table of human threats defined by [17].

Table 11: County Council - Human Threats

Threat-Source	Motivation	Threat Actions
Hacker	Challenge Ego Rebellion Revenge	Hacking Unauthorized system access System intrusion
Computer Criminal	Computer resources Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	Computer Crime Fraudulent act (e.g replay, impersonation, interception) Information bribery System intrusion Blackmail
Malicious Code Writer	Destruction System Access Monetary Gain	Denial of Service System attack

Results of Risk Assessment The results of the risk assessment are presented in Table 12. The risk of a successful attack is rated for each threat source present in one of the vulnerability groups described in Section 3.2.1. The results are based on the likelihood of such attacks and the impact these attacks may have on the availability, confidentiality, and integrity of the system. To make the risk assessment more reliable it was based on the results of a security test performed in combination with a vulnerability database search as explained in Section 4.5.5. The results of the security testing are found in Appendix A. The results are based on the risk rating of the threat source that is found to make up the greatest risk to the system. The numbers present in the column "Total Score" are used in the calculation of the effectiveness of the security measure.

Table 12: County Council - Risk scale: High (>200 - 400); Medium (>40 - 200); Low (1 - 40)

System	Bugs And Buckdoor	Authentication Failure	Information leakage	Denial of Service	Total Score
Unsecured	HIGH	HIGH	MEDIUM	MEDIUM	300
Solution 1	MEDIUM	MEDIUM	LOW	LOW	115
Solution 2	MEDIUM	LOW	LOW	LOW	66
Solution 3	MEDIUM	LOW	LOW	LOW	70
Solution 4	MEDIUM	LOW	LOW	LOW	66
Solution 5	LOW	LOW	LOW	LOW	26
Solution 6	MEDIUM	LOW	LOW	LOW	32
Solution 7	LOW	LOW	LOW	LOW	12
Solution 8	MEDIUM	LOW	LOW	LOW	66
Solution 9	LOW	LOW	LOW	LOW	26
Solution 10	LOW	LOW	LOW	LOW	12

The results show that no security measure scores HIGH on the risk scale. Solution 1,2,3,4,8 score MEDIUM on the risk scale and Solution 5,6,7,9,10 score LOW on the risk scale.

Results of Cost Calculation The results of the cost calculation are shown in Table 13. The most interesting is the "Present Value", which is used in the cost-effectiveness calculation later on. This is the total cost of the security measure transformed into present value giving us a common unit of measurement to compare the alternatives.

Table 13: County Council - Cost Calculations (NOK)

Security Measure	Implement-ation Cost	Mainten-ance Cost	Soft-ware Cost	Hard-ware Cost	Support Cost	Total	Present Value
Solution 1	9950	69056	23925	0	69056	171987	148396
Solution 2	14925	103584	23925	0	69056	211490	182688
Solution 3	9950	69056	23925	0	69056	171987	148396
Solution 4	14925	103584	23925	0	69056	211490	182688
Solution 5	9950	75961	33275	0	75961	195148	168323
Solution 6	29850	138111	23925	0	69056	260943	226506
Solution 7	24875	110489	33275	0	75961	244601	212142
Solution 8	14925	103584	23925	15750	69056	227240	197768
Solution 9	9950	75961	33275	15750	75961	210898	183404
Solution 10	24875	110489	33275	15750	75961	260351	227222

Results of Cost-effectiveness Ratio Calculation The numbers obtained in the cost and the effectiveness calculation are used to calculate the cost-effectiveness ratio as shown in Table 14.

Table 14: County Council - Cost-effectiveness calculation

System	Effectiveness	Cost	Cost-effectiveness
Solution 1	0,276595745	148396	536510
Solution 2	3,545454545	182688	51527
Solution 3	3,285714286	148396	45164
Solution 4	3,545454545	182688	51527
Solution 5	10,53846154	168323	15972
Solution 6	8,375	226506	27045
Solution 7	24	212142	8839
Solution 8	3,545454545	197768	55781
Solution 9	10,53846154	183404	17403
Solution 10	24	227222	9468

Results of Cost-effectiveness Analysis The results of the cost-effectiveness analysis have been ranked in Table 15.

Table 15: County Council - Ranking of Cost-effectiveness

Number	System
1	Solution 7
2	Solution 10
3	Solution 5
4	Solution 9
5	Solution 6
6	Solution 3
7	Solution 2
7	Solution 4
8	Solution 8
10	Solution 1

The results show that Solution 7 has the best overall cost-effectiveness ratio of the security measures used in this case study. A closer look at the results shows us that the four security measures scoring LOW on the risk scale are also the security measures with the best cost effectiveness ratio.

5.3.3 Case 3 - Mid-size Business

Results of Threat Identification Five threat sources relevant for this case were identified: the hacker, the computer criminal, the malicious code writer, the industrial espionage agent and the terrorist. Their motivation and their threat actions are described in Table 16. Table 16 is based on a table of human threats defined by [17].

Table 16: Mid-size Business - Human Threats

Threat-Source	Motivation	Threat Actions
Hacker	Challenge Ego Rebellion Revenge	Hacking Unauthorized system access System intrusion
Computer Criminal	Computer resources Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	Computer Crime Fraudulent act (e.g replay, impersonation, interception) Information bribery System intrusion Blackmail
Malicious Code Writer	Destruction System Access Monetary Gain	Denial of Service System attack
Industrial espionage agent	Competitive Advantage	Information theft Unauthorized system access System penetration
Terrorist	Destruction Blackmail Exploitation Revenge	Information warfare System penetration System tampering

Results of Risk Assessment The results of the risk assessment are presented in Table 17. The risk of a successful attack is rated for each threat source present in one of the vulnerability groups described in Section 3.2.1. The results are based on the likelihood of such attacks and the impact these attacks may have on the availability, confidentiality, and integrity of the system. To make the risk assessment more reliable it was based on the results of a security test performed in combination with a vulnerability database search as explained in Section 4.5.5. The results of the security testing are found in Appendix A. The results are based on the risk rating of the threat source that is found to make up the greatest risk to the system. The numbers present in the column "Total Score" are used in the calculation of the effectiveness of the security measure.

Table 17: Mid-size Business - Risk scale: High (>200 - 400); Medium (>40 - 200); Low (1 - 40)

System	Bugs And Buckdoor	Authentication Failure	Information leakage	Denial of Service	Total Score
Unsecured	HIGH	HIGH	MEDIUM	MEDIUM	300
Solution 1	MEDIUM	MEDIUM	LOW	LOW	115
Solution 2	MEDIUM	MEDIUM	LOW	LOW	81
Solution 3	MEDIUM	MEDIUM	LOW	LOW	110
Solution 4	MEDIUM	MEDIUM	LOW	LOW	106
Solution 5	LOW	LOW	LOW	LOW	26
Solution 6	MEDIUM	MEDIUM	LOW	LOW	52
Solution 7	LOW	LOW	LOW	LOW	12
Solution 8	MEDIUM	MEDIUM	LOW	LOW	106
Solution 9	LOW	LOW	LOW	LOW	26
Solution 10	LOW	LOW	LOW	LOW	12

The results show that no security measures score HIGH on the risk scale. Solution 1,2,3,4,6,8 score MEDIUM on the risk scale and Solution 5,7,9,10 score LOW on the risk scale.

Results of Cost Calculation The results of the cost calculation are shown in Table 8. The most interesting is the "Present Value", which is used in the cost-effectiveness calculation later on. This is the total cost of the security measure transformed into present value giving us a common unit of measurement to compare the alternatives.

Table 18: Mid-Size Business - Cost Calculations (NOK)

Security Measure	Implement-ation Cost	Mainten-ance Cost	Soft-ware Cost	Hard-ware Cost	Support Cost	Total	Present Value
Solution 1	3980	82867	89300	0	82867	259014	223027
Solution 2	5970	110489	89300	0	82867	288626	248554
Solution 3	5970	124300	89300	0	82867	302437	260365
Solution 4	7960	151922	89300	0	82867	332049	285893
Solution 5	5970	138111	128600	0	96678	369359	318097
Solution 6	19900	193355	89300	0	82867	385422	332759
Solution 7	17910	179544	128600	0	96678	422732	364963
Solution 8	15920	179544	89300	56000	82867	423631	370756
Solution 9	13930	165734	128600	56000	96678	460941	402960
Solution 10	25870	207167	128600	56000	96678	514314	449826

Results of Cost-effectiveness Ratio Calculation The numbers obtained in the cost and the effectiveness calculation are used to calculate the cost-effectiveness ratio as shown in Table 19.

Table 19: Mid-size Business - Cost-effectiveness calculation

System	Effectiveness	Cost	Cost-effectiveness
Solution 1	0,276595745	223027	806327
Solution 2	1,830188679	248554	135808
Solution 3	1,727272727	260365	150738
Solution 4	1,830188679	285893	156210
Solution 5	10,53846154	318097	30184
Solution 6	8,375	332759	39732
Solution 7	24	364963	15207
Solution 8	1,830188679	370756	202578
Solution 9	10,53846154	402960	38237
Solution 10	24	449826	18743

Results of Cost-effectiveness Analysis The results of the cost-effectiveness analysis have been ranked in Table 20.

Table 20: Mid-size Business - Ranking Cost-effectiveness

Number	System
1	Solution 7
2	Solution 10
3	Solution 5
4	Solution 9
5	Solution 6
6	Solution 2
7	Solution 3
8	Solution 4
9	Solution 8
10	Solution 1

The results shows that Solution 7 has the best overall cost-effectiveness ratio of the security measures used in this case study. A closer look at the results show us that the four security measures scoring LOW on the risk scale are also the security measures with the best cost effectiveness ratio.

5.4 The difference in cost-effectiveness ranking in different environments

The three case studies used in this thesis represents organizations of different size, field of operation, and need of security. In research question four we want to explore any differences this may give on the experimental results. Several differences exist in the data used for the cost-effectiveness calculation. For instance the bank has 500 home office

systems, an expected lifetime of the investment of four years, and four identified threat sources. The county council has 25 home office systems, an expected lifetime of the investments of six years, and three identified threat sources. The mid-sized business has 100 home office systems, an expected lifetime of investments of five years, and five identified threat sources. The total costs of the investments also differ a lot. In Table 21 we have compared the results of the cost-effectiveness analysis performed on the three case studies.

Table 21: Ranking Cost-effectiveness

Number	Bank	County Concil	Mid-size Business
1	Solution 7	Solution 7	Solution 7
2	Solution 10	Solution 10	Solution 10
3	Solution 5	Solution 5	Solution 5
4	Solution 6	Solution 9	Solution 9
5	Solution 9	Solution 6	Solution 6
6	Solution 2	Solution 3	Solution 2
7	Solution 4	Solution 2	Solution 3
8	Solution 3	Solution 4	Solution 4
9	Solution 8	Solution 8	Solution 8
10	Solution 1	Solution 1	Solution 1

There are only minor differences between the results of the cost-effectiveness analysis of the different case studies. The same three security measures have the best cost-effectiveness ratio in all three cases. Further down the list there are some differences between the case studies. Because no sensitivity analysis were performed due to limited available time, there are some uncertainties surrounding the ranking.

6 Conclusion

Information security is just as much a business matter as a technical matter. The economics and the effectiveness of the investments have to be considered before investments are being made. One way of doing this is by performing a cost-effectiveness analysis of the security measures considered. This thesis had the main focus on home office security. We have looked at different methods for calculation of cost, effectiveness and cost-effectiveness ratio. As a result of this work, a methodology for performing cost-effectiveness analysis on home office systems has been developed. This methodology consists of several well tested methods with no known reliability or validity issues. The methodology is adaptable, and the fact that different organizations face different levels of threat from different threat sources, is accounted for. The level of threat faced by the organization is identified by looking at possible threat sources and their motivation and actions. This can be used to identify which threats we are up against and how to protect our systems.

The methodology was tested in an experiment, using three different case studies representing organizations of different size, field of operation, and security needs. We chose to use bank, mid-size business, and county council as case studies. A total of five different threat sources were identified as part of this thesis. The threat sources identified for the bank were the hacker, the computer criminal, the malicious code writer, and the industrial espionage agent. The threat sources identified for the county council were the hacker, the computer criminal, and the malicious code writer, while the threat sources identified for the mid-size business were the hacker, the computer criminal, the malicious code writer, the industrial espionage agent, and the terrorist. A risk assessment was performed based on the information on threat sources, their motivation and their threat actions, in addition to results of system security testing and vulnerability database searches. Based on the results of the risk assessment the effectiveness of the results was calculated. The cost-effectiveness ratio was then computed by dividing the cost of the security measure and its effectiveness.

The results of the experiment were ranked by their cost-effectiveness ratio. One security measure had the relatively best cost-effectiveness ratio in all case studies considered. This security measure was based on a combination of host hardening, security patching, antivirus software, commercial host firewall and a L2TP over IPSec software client used for encrypted communication.

When comparing the results of the three different case studies only minor differences in the cost-effectiveness ratio ranking were discovered.

7 Further Work

In this thesis we have focused on a methodology for cost-effectiveness analysis for home office systems. Still the methodology has the potential for use in other areas of information security. Further work can be done to prove the methodology's usability on bigger and more complex computer systems. During the work on this thesis, we were not able to identify any freely available methodologies for cost-effectiveness analysis, in the field of information security. To prove this methodology's usability in larger systems, or to improve the methodology in a way that makes it useable in such systems, will certainly be useful for the information security community.

During the earlier stages of this thesis the VAM methodology was tested as part of the cost-effectiveness analysis methodology. This did not work out due to the rather small size of the home office systems. For cost-effectiveness analysis of security measures in larger systems it will be interesting to see how the VAM methodology performs. The potential benefits of this methodology are its ease of use and ability to identify new vulnerabilities generated by the use of a proposed security technique.

Bibliography

[1] DA, D. A. August 2004. Svært populært med hjemmekontor. "http://www.deloitte.com/dtt/press_release/0,1014,sid%253D6959%2526cid%%253D56103,00.html". Norwegian Only.

[2] Northcutt, S., Zeltser, L., Winters, S., Frederick, K. K., & Ritchey, R. W. July 2003. Inside network perimeter security. volume First Edition. New Riders.

[3] Willert, J. Oktober 2001. Best computer practice for home, home office, small business and telecommuters. http://www.sans.org/rr/papers/26/616.pdf.

[4] Jurancich, P. P. 2003. Setting up a secure home office network. http://www.giac.org/practical/GSEC/Perry_Jurancich_GSEC.pdf.

[5] Souppaya, M., Johnson, P. M., Kent, K., & Harris, A. June 2004. Nist special publication 800-68 - guidance for securing microsoft windows xp systems for it professionals: A nist security configuration checklist. http://csrc.nist.gov/itsec/download_WinXP.html.

[6] Blakley, B. April 2002. Security insights. *Sciencedirect*. "http://www.sciencedirect.com/".

[7] Gregg Shudel, B. J. W. Adversary work factor as a metric for information assurance.

[8] Bickel, R., Cook, M., Haney, J., & Kerr, M. December 2003. Guide to securing microsoft windows xp. "http://www.nsa.gov/snac/downloads_winxp.cfm?MenuID=scg10.3.1.1".

[9] Doernberg, C. July 2002. Guide to securing internet explorer 5.5 using group policy. "http://www.nsa.gov/snac/downloads_ms_ie.cfm?MenuID=scg10.3.1.4". Version 1.0.

[10] Pitsenbarger, T. & Bartock, P. November 2003. Outlook e-mail security in the midst of malicious code attacks. "http://www.nsa.gov/snac/downloads_docs.cfm?MenuID=scg10.3.1". Version 3.0.

[11] Levin, H. M. & McEwan, P. J. 2001. *Cost-effectiveness analysis: Methods and applications*. SAGE Publications, 2nd edition edition.

[12] Spilling, P. & Ølnes, J. June 1995. Race common functional specification h 211 security of service management. http://citeseer.ist.psu.edu/329942.html.

[13] Nystuen, K. O. & Hagen, J. M. 2000. Metode for analyse av såbarhetsreduserende tiltak innen telekommunikasjon: problematisering og teoretisk tilnærming. "http://rapporter.ffi.no/rapporter/98/06261.pdf". Norwegian only.

[14] Osborne, K. June 1998. Auditing the it security function. *Sciencedirect*. "http://www.sciencedirect.com/".

[15] Anton, P. S., Anderson, R. H., Mesic, R., & Scheiern, M. 2003. *Finding and Fixing Vulnerabilities in Information Systems - The Vulnerability Assessment and Mitigation Methodology*. RAND National Defense Research Institute, "http://www.rand.org/publications/MR/MR1601/MR1601.pdf".

[16] Peltier, T. R. 2001. *Information Security Risk Analysis*. Auerbach.

[17] Stoneburner, G., Goguen, A., & Feringa, A. July 2002. Special publication 800-30 - risk management guide for information technology systems. "http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf". NIST - Computer Security Division.

[18] (ISF), I. S. F. Firm - fundamental information risk management.

[19] Division, N. C. S. October 2003. Nist special publication 800-42 - guideline on network security testing. http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf.

[20] SECURITY, I. I. F. & Herzog, O. M. P. Aucust 2003. Osstmm 2.1. open-source security testing methodology manual. http://isecom.securenetltd.com/osstmm.en.2.1.pdf.

[21] Stuart McClure, J. S. & Kurtz, G. 2003. *Hacking Exposed: Network Security Secrets and Solutions*. McGraw-Hill/Osborne, fourth edition edition.

[22] Shema, M. & Johnson, B. C. 2004. *Anti-Hacker Toolkit*. McGraw-Hill/Osborne, second edition edition.

[23] T.J. Klevinsky, S. L. & Gupta, A. June 2002. *Hack I.T. - Security Through Penetration Testing*. Addison-Wesley.

[24] Deraison, R., Meer, H., Temmingh, R., van der Walt, C., Alder, R., Alderson, J., Johnston, A., & Theall, G. A. 2004. *Nessus Network Auditing*. Jay Beale's Open Source Security Series. Syngress Publishing.

[25] Anderson, J. M. June 2003. Why we need a new definition of information security. *Sciencedirect*. "http://www.sciencedirect.com/".

[26] Gordon, L. A. & Richardson, R. March 2004. The new economics of information security. *InformationWeek*, 982, 53–56.

[27] Remenyi, D., Money, A., & Sherwood-Smith, M. 2003. *The effective measurement and management of IT costs and benefits*. Butterworth-Heinemann, 2nd edition edition.

[28] M.H. Aziz, Ong Con Nie, J. C. M. Y. & Wei, L. C. September 2003. Tco reduction. *APCC 2003. The 9th Asia-Pacific Conference on Communications*, Volume 3, 1147 – 1151.

[29] Wikipedia. http://en.wikipedia.org/wiki/Total_cost_of_ownership. Total Cost of Ovnership. Visited April 2005.

[30] Office of The Deputy Chief Information Officer, N. I. o. H. N. May 1999. Cost-benefit analysis guide for nih it projects. "http://irm.cit.nih.gov/itmra/cbaguide.html#2.5". (Visited March 2005).

[31] Jones, A. 2003. Identification of a method for the calculation of threat in an information environment. *Information Warfare Journal*. QinetiQ Trusted Information Management.

[32] Cheswick, W. R. & Bellovin, S. M. 1994. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley Publishing Company.

[33] Howard, D. J. D. 1997 April. An analysis of security incidents on the internet 1989-1995. "http://www.cert.org/research/JHThesis/Start.html". Chapter 6 - A Taxonomy of Computer and Network Attacks.

[34] Securityfocus. "http://www.securityfocus.com/bid".

[35] Microsoft security bulletins. "http://www.microsoft.com/technet/security/current.aspx".

[36] Symantec security response. "http://securityresponse.symantec.com/avcenter/vinfodb.html".

[37] Firewall tester. "http://ftester.sourceforge.net/ftester.html". Tool for testing firewall filtering policies.

[38] Nessus open source vulnerability scanner project. "http://www.nessus.org". Vulnerability Scanner.

[39] Nmap. "http://www.insecure.org". Tool for network exploration and security auditing.

[40] Hping2. "http://www.hping.org/". TCP/IP packet assembler/analyzer.

[41] Enum. "http://www.bindview.com/Services/RAZOR/Utilities/Windows/enum_readme.c%fm". Enumeration tool.

[42] Winfingerprint. "http://winfingerprint.sourceforge.net/". Win32 Host/Network Enumeration Scanner.

[43] Thc-amap. "http://thc.org/". Application protocol detection tool.

[44] Fyodor. Nmap network security scanner man page. http://www.insecure.org/nmap/data/nmap_manpage.html.

[45] Northcutt, S. 1999. Intelligence gathering techniques. "http://www.microsoft.com/technet/security/topics/networksecurity/intel%.mspx". Chapter 8 from Network Intrusion Detection: An Analyst's Handbook, published by New Riders Publishing. Visited April 2005.

[46] Statistisk sentralbyrå. "http://www.ssb.no/emner/06/05/lonnikt/". Income Statistics for the ICT-sector. Norwegian only. Visited March 2005.

[47] Statistisk sentralbyrå. "http://www.ssb.no/aarbok/tab/t-101310-526.html". Statistics on Interest Rates 1995 - 2004. Norwegian only. Visited April 2005.

[48] AS, J. C. F. Caplex. "http://www.caplex.net/web/artikkel/artdetalj.asp?art_id=9337422". Encyclopedia: Definition of a terrorist. Norwegian Only. Visited May 2005.

A Security Test Results

UNSECURED SYSTEM

This is a system running Windows XP Professional Service Pack 1. The system is running the standard out-of-the-box configuration. No security mechanisms, not turned on by default, are used. No patches released after the release date of Service Pack 1 are added.

Workstation Information Template

IP address	Domain name	Operating System
192.168.1.171	NAGASAKI	Windows XP SP1

Port	Protocol	Service	Service Details
80	TCP	http	
135	TCP	Msrpc	Netbios session
139	TCP	Netbios-ssn	SMB server running on this port
445	TCP	Microsoft-ds	CIFS server running on this port
1025	TCP	Msrpc	Netbios session, DCE service running
5000	TCP	http / upnp	NMAP and amap does not agree. Nessus: Microsoft UPnP TCP Helper running
7102	TCP	Unknown	
123	UDP	Ntp	Open \ filtered - Network Time Protocol Server listening at this port
135	UDP	ms-location-service	Open
137	UDP	netbios-ns	Open
138	UDP	Netbios-dgm	Open \ filtered
445	UDP	Microsoft-ds	Open \ filtered
500	UDP	Isakmp	Open \ filtered
1027	UDP	ms-location-service	Open
1028	UDP	Ms-lsa	Open \ filtered

1041	UDP	ms-location-service	Open
1900	UDP	UPnP	Open \ filtered
13846	UDP	Unknown	Open \ filtered
39051	UDP	Unknown	Open \ filtered

Banner(s)

Port	Protocol	Banner
135	TCP	Microsoft Windows msrpc
137	UDP	Microsoft Windows NT netbios-ssn (host: DELL-XP workgroup: NAGASAKI)
445	TCP	Microsoft Windows XP microsoft-ds
1025	TCP	Microsoft Windows msrpc / DCE service running
5000	TCP	Microsoft Windows UPnP / Microsoft UPnP TCP Helper running

TCP Sequencing

TCP Secuence Prediction
Random positive increments
TCP ISN Seq. Numbers
IPID Sequence Generation
Incremental (non-random – possible to predict next value)
Uptime: Unknown

Concerns and Vulnerabilities

Concern or Vulnerability
Vulnerability in Task Scheduler Could Allow Code Execution (MS04-022)
Example
Remote code execution because of an unchecked buffer. If a user is logged on with administrator privileges, an attacker can take full control over the affected system. The worms/Trojan horses Bloodhound.exploit.11 and Bloodhound.exploit.12 exploit this vulnerability. (Symantec)
Solution
Install security update for Windows XP (KB841873)

Concern or Vulnerability
TCP 135 – Several vulnerabilities in RPC/DCOM (MS04-012)
Example
MS Windows RPC service crashes trying to dereference a null pointer when it receives a certain malformed request. (Nessus) These vulnerabilities can cause denial of service for the RPC/DCOM service or an attacker exploiting the vulnerability may take full control over the system. W32.Bobax.C worm, Several of the W32.Kibuv.Worm, several of the W32.Spybot.Worm, several of the W32.HLLW.Gaobot.gen, W32.Randex worm , several of the W32.Kobot worm, W32.Explet.A@mm, Backdoor.IRC.Whisper.B, W32.Dopbot, W32.Bropia.N, several versions of the W32.Kelvir worm, W32.Donk worm, W32.Mugly worm exploit DCOM RPC vulnerability using TCP port 135. (Symantec)
Solution
Block access to TCP port 135

Concern or Vulnerability
TCP 135
Example
Distributed Computing Environment services running on the remote host can be enumerated by connecting to port 135 and doing the appropriate queries. (Nessus)
Solution
Filter incoming traffic to this port

Concern or Vulnerability
Microsoft-ds TCP 445 – Multivulnerabilities (MS04-011)
Example

1. LSAS Vulnerability: Buffer overrun vulnerability. Can allow remote code execution on the remote system. The attacker can take complete control of the system. Several variants of W32.sasser Worm, several variants of W32.Korgo worm, Hacktool.LsassSba, several versions of the W32.bobax worm, W32.Huayu worm, W32.Multex worm, several versions of Trojan.Netdepix, W32.Aizu worm, Bloodhound.Exploit.8, W32.Waltz worm, W32.Cycle worm, several of the W32.Kibuv.Worm, W32.Janx worm, W32.Linkbot.H worm, several versions of the W32.Mytob@ worm, W32.Spybot.Worm, W32.HLLW.Gaobot.gen worm, W32.Randex worm, W32.Kobot worm, W32.Explet.A@mm worm, Trojan.Otinet, Backdoor.Sdbot.AA, Backdoor.IRC.Whisper.B, W32.Bropia.N, several versions of the W32.Kelvir worm, W32.Donk worm, W32.Mugly worm exploits this vulnerability. (Symantec) 2. Winlogon vulnerability: Buffer overrun vulnerability in the Windows logon process for users belonging to a Domain. Attackers can remotely execute code and take complete control over the system. The attacker needs permission to user objects in the Domain to exploit this vulnerability. 3. Metafile vulnerability: Vulnerability in the rendering of WMF and EMF image formats. An attacker can set up a website which is used to exploit this vulnerability. The attacker can obtain the same privileges as the user. 4. Help and support centre vulnerability: An attacker can exploit this vulnerability by setting up a malicious website or send out malicious emails, containing a malicious HCP URL. The attacker can take complete control over the system. 5. Negotiate SSP vulnerability: Buffer overrun vulnerability that can allow remote code execution. An attacker can take complete control over the system, but in most cases the result will be a denial of service. 6. ASN.1 “Double free” vulnerability: Remote code execution vulnerability. The attacker may take complete control over the system, but is most likely to create a denial of service situation.
Solution
1. Use Firewall, Security Update for Windows XP (KB835732) 2. Security Update for Windows XP (KB835732) 3. Read E-mail in plain text, Security Update for Windows XP (KB835732) 4. Use IE 6.0 or later, OE 6.0 or later, Security Update for Windows XP (KB835732) 5. Security Update for Windows XP (KB835732) 6. Security Update for Windows XP (KB835732)

Concern or Vulnerability
Microsoft-ds TCP 445 – ASN.1 Vulnerability could allow code execution (MS04-007)
Example
A buffer overflow vulnerability in Microsoft ASN.1 library. An attacker can execute code with system privileges and take complete control over the system. Hacktool.Asni exploits this vulnerability.
Solution
Security Update for Windows XP (KB828028)

Concern or Vulnerability
Microsoft-ds TCP 445 – Named Pipe Vulnerability (MS05-007)
Example
An attacker can remotely read the user names of users, which have an open connection to an available shared resource
Solution
Use Firewall, disabling the computer browser service, Security update for Windows XP (KB888302)

Concern or Vulnerability
Microsoft-ds TCP 445 – The host security identifier can be obtained remotely
Example
An attacker can use this to obtain a list of local users on this host. (Nessus)
Solution
Filter the ports 137-139 and 445

Concern or Vulnerability
Microsoft-ds TCP 445 – NULL sessions
Example
By logging in providing null user name and null password one can get a guest account.
Solution
Use Firewall

Concern or Vulnerability
TCP 1025
Example
Distributed Computing Environment service running on the host. Can be enumerated by connecting to port 135. (Nessus)
Solution
Filter incoming traffic to this port

Concern or Vulnerability
TCP 5000 – Microsoft UPnP TCP helper
Example
Should be disabled
Solution
Disable service

Concern or Vulnerability
UDP 135 – Buffer overrun in messenger service could allow code execution (MS03-043)
Example
Buffer overrun in messenger service could allow code execution. The attacker can run code with local system privileges. The attacker can take complete control over the system. W32.HLLW.Gaobot.gen worm, W32.Randex, W32.Spybot.Worm, W32.Kibuv, W32.Bropia.N, W32.Welchia Worm, W32.Mugly worm exploits this vulnerability.
Solution
Block NetBIOS ports 135-137 and UDP broadcast packets with a firewall, disable messenger service, Security Update for Windows XP (KB828035)

Concern or Vulnerability
NTP UDP 123
Example
Network Time Protocol Server is listening on this port
Solution

Concern or Vulnerability
Isakmp UDP 500
Example
Solution

Concern or Vulnerability
Netbios-ns UDP 137
Example
An attacker can find the netbios name of the computer
Solution
Filter incoming traffic to this port

Concern or Vulnerability
UDP 1027
Example
Distributed Computing Environment service running on the host. Can be enumerated by connecting to port 135. (Nessus)
Solution
Filter incoming traffic to this port

Vulnerabilities not discovered by the security testing.

Concern or Vulnerability
The system can be compromised exploiting an unchecked buffer in the Windows shell (MS02-072)
Example
The attacker can create an malicious .MP3 or .WMA file and host it on a website or windows share. The vulnerability will be invoked if the user hover his mouse pointer over the file icon. This can mount a buffer overrun attack. The code will run with user privilege.
Solution
Windows XP Security Patch: Unchecked Buffer in Windows Shell Could Enable System Compromise

Concern or Vulnerability
Remote code execution due to flaw in Windows script engine (MS03-008)
Example
An attacker can construct a web page that will execute code with user privileges when visited by the user.
Solution
Turn off active scripting in Internet Explorer JScript 5.6 Security Patch for Windows 2000 and XP (814078)

Concern or Vulnerability
Flaw in Microsoft VM Could Enable System Compromise (MS03-011)
Example
An attacker can create a malicious java applet. It would exploit the vulnerability when the user visits the website. Will only get user privileges. This vulnerability is exploited by the Trojan horse Trojan.ByteVerify. (Symantec)
Solution
Patch available

Concern or Vulnerability
Flaw in Windows Media Player Skins Downloading could allow Code Execution (MS03-017)
Example
A flaw in the way Windows Media Player handles skin files, which gives the attacker an opportunity to place a malicious file on the system. The file will be run with user privileges. An attacker can make a malicious website that exploit this vulnerability
Solution
Windows Media Security Patch: Flaw in Windows Media Player Skins Downloading could allow Code Execution

Concern or Vulnerability
Buffer Overrun In HTML Converter Could Allow Code Execution (MS03-023)
Example
A buffer overrun vulnerability in the HTML converter that can be exploited by an attacker by making a malicious web site or a HTML e-mail. This can make arbitrary code run with user privileges.
Solution
Windows XP Security Patch: Buffer Overrun In HTML Converter Could Allow Code Execution

Concern or Vulnerability
Unchecked Buffer in DirectX Could Enable System Compromise (MS03-030)
Example
By exploiting this vulnerability an attacker can run arbitrary code with user privileges on the system. The attacker can make a malicious web site or a HTML e-mail which will exploit the vulnerability if the user visits it.
Solution
Windows XP Security Patch: Unchecked Buffer in DirectX Could Enable System Compromise

Concern or Vulnerability
Flaw in NetBIOS Could Lead to Information Disclosure (MS03-034)
Example
An attacker can retrieve arbitrary or random data from the memory of the computer by sending NetBT Name Service queries to the system.
Solution
Security Update for Windows XP (KB824105)

Concern or Vulnerability
Vulnerability in Authenticode Verification Could Allow Remote Code Execution (MS03-041)
Example
An attacker can make a malicious web site. An ActiveX control can be installed without user approval under certain low memory situation. The attacker can obtain user privileges.
Solution
Security Update for Microsoft Windows XP: KB823182

Concern or Vulnerability
Buffer Overrun in Windows Help and Support Centre Could Lead to System Compromise (MS03-044)
Example
Due to an unchecked buffer in the HCP protocol an attacker can construct an URL, on a web page or in an e-mail, that can execute the code of choice in the local security context. An attacker can then read and launch files on the system.
Solution
Security Update for Microsoft Windows XP: KB825119

Concern or Vulnerability
Buffer Overrun in the Workstation Service Could Allow Code Execution (MS03-049)
Example
A vulnerability in the workstation service can allow remote code execution on the system. An attacker can gain system privileges on the system. This vulnerability is exploited by several worms and Trojans: Hacktool.WKRShell, W32.Randex, several of the W32.Gaobot.(X) worms, several of the W32.Spybot.(X) worms, W32.Bropia.N, several of the W32.Kelvir.(X) worms, several of the W32.Welchia.(X).Worm, several variants of the W32.Mugly.B@ worm. (Symantec)
Solution
Block inbound UDP ports 138, 139, 445 and TCP ports 138, 139, 445 Security Update for Microsoft Windows XP: KB828035

Concern or Vulnerability
Vulnerability in Help and Support Center Could Allow Remote Code Execution (MS04-015)
Example
An attacker can construct a malicious HCP URL on a web site or in an e-mail. If the remote code execution succeeds the attacker will get the same privileges as the user.
Solution
Security Update for Windows XP (KB840374)

Concern or Vulnerability
Vulnerability in HTML Help Could Allow Code Execution (MS04-023)
Example
An attacker can exploit these vulnerabilities by making a user visit a malicious web site. He will then gain user privileges
Solution
Security Update for Windows XP (KB840315)

Concern or Vulnerability
Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (MS04-028)
Example
A buffer overrun in JPEG processing can allow remote code execution. An attacker can gain the privileges of the user of the system. Several Trojan horses and backdoors exploit this vulnerability: severak variants of Backdoor.Roxe, several variants of Trojan.Ducky, Bloodhound.Exploit.13, Trojan.Moo, Hacktool.JPEGDownload, Hacktool.JPEGShell, W32.Yanz.B@mm. (Symantec)
Solution
Security Update for Windows XP (KB833987)

Concern or Vulnerability
Security Update for Microsoft Windows (MS04-032), Window Management Vulnerability, Virtual DOS Machine Vulnerability, Graphics Rendering Engine Vulnerability, Windows Kernel Vulnerability
Example
Window Management Vulnerability: This vulnerability will let a logged on user take complete control over the system. Vulnerability can only be exploited locally. Virtual DOS Machine Vulnerability: Logged in users can take complete control over the system. Vulnerability can only be exploited locally Graphics Rendering Engine Vulnerability: A special crafted WMF or EMF file could allow remote execution on a system if the user views a folder, mail or web site that contain the file. The attacker can take complete control over the system. This vulnerability is exploited by Bloodhound.Exploit.17, W32.Scard and Backdoor.Emcommander Windows Kernel Vulnerability: An attacker can locally run a program that will cause a denial of service attack on the workstation. The system will automatically restart.

Solution
Security Update for Windows XP (KB840987)

Concern or Vulnerability
Vulnerability in Compressed (zipped) Folders Could Allow Remote Code Execution (MS04-034)
Example
An unchecked buffer can be exploited by an attacker creating a malicious zipfile. A user can visit a website containing this file or receive it by e-mail. If the user opens the file an attacker can take complete control over the system
Solution
Security Update for Windows XP (KB873376)

Concern or Vulnerability
Vulnerability in Windows Shell Could Allow Remote Code Execution (MS04-037)
Example
Shell Vulnerability: Remote code execution which could be exploited by an attacker by setting up a malicious web site. The attacker can take complete control over the system. Program Group Converter Vulnerability: Remote code execution when user open a malicious attachment or link, which can give an attacker complete control over the system. This vulnerability is exploited by Bloodhound.Exploit.15
Solution
Security Update for Windows XP (KB841356)

Concern or Vulnerability
Vulnerability in WordPad Could Allow Code Execution (MS04-041)
Example
Remote code execution vulnerability when opening malicious crafted .wri.rtf.doc files in WordPad. The attacker can obtain the same privileges as the user of the system.
Solution
Security Update for Windows XP (KB885836)

Concern or Vulnerability
Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege (MS04-044)
Example
Windows Kernel Vulnerability and LSASS Vulnerability could allow a logged in user to take full control over the system.
Solution
Security Update for Windows XP (KB885835)

Concern or Vulnerability
Vulnerability in HTML Help Could Allow Code Execution (MS05-001)
Example
An attacker can use a web site to exploit this remote code execution and information disclosure vulnerability. If the user visit the web page and the attack is successful the attacker can take complete control over the system. This vulnerability is exploited by several Trojans: Bloodhound.Exploit.21, several of the Trojan.Phel.A, Trojan.Phel.B and Trojan.Magise
Solution
Security Update for Windows XP (KB890175)

Concern or Vulnerability
Vulnerability in PNG Processing Could Allow Remote Code Execution (MS05-009)
Example
Several PNG Processing vulnerabilities exist in Windows Mediaplayer, Windows Messenger and MSN Messenger which can cause remote code execution. The attacker can get the privileges of the user on the system. This vulnerability is exploited by Bloodhound.Exploit.24
Solution
Update Windows Media Player, Windows Messenger and MSN Messenger.

Concern or Vulnerability
Vulnerability in OLE and COM Could Allow Remote Code Execution (MS05-012)
Example
COM Structured Storage Vulnerability: Privilage evelation vulnerability that can make the logged in user take full control of the system. Input Validation Vulnerability: A malicious document containing can be published on a website or by e-mail. User interaction is required to exploit the vulnerability which can execute code remotly and give the attacker complete control of the system.
Solution
Security Update for Windows XP (KB873333)

Concern or Vulnerability
Vulnerability in the DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (MS05-013)
Example
A vulnerability exist that can allow information disclosure and remote code execution. This can happen by visiting a malicious web site. The attacker can gain complete control over the system.
Solution
Security Update for Windows XP (KB891781)

Concern or Vulnerability
Vulnerability in Hyperlink Object Library Could Allow Remote Code Execution (MS05-015)
Example
An unchecked buffer while handling hyperlinks can be used to execute code remotely. If a user clicks on a malicious hyperlink in an e-mail or a website the malicious code can get executed and the attacker will get the privileges of the user on the system.
Solution
Security Update for Windows XP (KB888113)

Containment Measures Review Template

IP Address	Domain Name
192.168.1.171	NAGASAKI
Desktop Anti-virus / Anti-Trojan Mechanisms	
None	
Response to SAP 27 and 42.zip	
None	

Desktop Mail Client Types
Outlook Express 6.0 SP1
Desktop Mail Client Vulnerabilites (www.microsoft.com/technet/security/current.aspx)
• MHTML URL Handler vulnerability (MS03-014): Allows an attacker to run code on the user's machine. For the attack to work, Windows has to open a specially constructed MHTML URL from an web site or included in a HTML e-mail message. • Malformed header vulnerability (MS04-018): An attacker can send special crafted e-mail messages, which will make Outlook Express fail, causing a denial of service situation. • MHTML URL Processing Vulnerability (MS04-013): A remote code execution vulnerability that can give an attacker complete control over the computer. Outlook Express processes special crafted MHTML URLs that will allow the attackers HTML code to be run in the Local Machines Security Zone in Internet Explorer. • Unchecked buffer in Windows help facility (MS02-055). The attacker can run code with the user privilege of the user of the system. Can be exploited by e-mail or website.

Desktop Browser Client Type
Internet Explorer 6.0 SP1
Desktop Browser Client Vulnerabilities (www.microsoft.com/technet/security/current.aspx)
• XMLHTTP vulnerability (MS02-008). An attacker can read from a data source on the user's system. The vulnerability is exploited from a website and the attacker has to know the full path to the file he wants to read. • A certificate validation flaw can enable identity spoofing (MS02-050).

Equipment	
Equipment Used	Switch
Servers, Number and Types	Astaro Security Linux v5 firewall, Fedora core 3 Samba server 3.0.x
Workstations, Number and Type	2x, Windows XP Professional SP1 and Suse Linux 9.2
Software used	Nessus 2.2.4, Nmap 3.70, Hping2, Enum, Winfingerprint, amap 4.8
Host names used	DELL-XP
Network Topology	
Anti-virus Capabilities	None
Network Protection Facilities Used	None
Remote Access Facilities Used	None
Routers Used	None
Physical Access Control Technology Used	None

SOLUTION 1

This solution is based on a out-of-the-box configuration of Windows XP Pro. Service Pack 1 no further updates have been installed. Norman anti virus v5.8 has been installed and is up-to-date. The Windows XP IPSec over L2TP client is activated.

Workstation Information Template

IP address	Domain name	Operating System
192.168.1.171	NAGASAKI	Windows XP SP1

Port	Protocol	Service	Service Details
135	TCP	Msrpc	Netbios session
139	TCP	Netbios-ssn	SMB server running on this port
445	TCP	Microsoft-ds	CIFS server running on this port
1025	TCP	Msrpc	Netbios session, DCE service running
2868	TCP	Unknown	
5000	TCP	http / upnp	NMAP and amap does not agree. Nessus: Microsoft UPnP TCP Helper running
11230	TCP	Unknown	
123	UDP	Ntp	Open \ filtered - Network Time Protocol Server listening at this port

135	UDP	ms-location-service	Open
137	UDP	netbios-ns	Open
138	UDP	Netbios-dgm	Open \ filtered
445	UDP	Microsoft-ds	Open \ filtered
500	UDP	Isakmp	Open \ filtered
1026	UDP	Unknown	Open
1030	UDP	Iad1	Open \ filtered
1041	UDP	ms-location-service	Open \ filtered
1121	UDP	Unknown	Open \ filtered
1701	UDP	L2TP	Open \ filtered
1900	UDP	UPnP	Open \ filtered
9127	UDP	Unknown	Open \ filtered
25195	UDP	Unknown	Open \ filtered

Banner(s)

Port	Protocol	Banner
135	TCP	Microsoft Windows msrpc / netbios-session
139	TCP	Netbios-session
445	TCP	Microsoft Windows XP microsoft-ds
1025	TCP	Microsoft Windows msrpc / netbios-session
5000	TCP	Microsoft Windows UpnP / http
135	UDP	Ms-location-service
137	UDP	Microsoft Windows NT netbios-ssn (host: DELL-XP workgroup: NAGASAKI)
1026	UDP	Ms-location-service

Concerns and Vulnerabilities

Concern or Vulnerability
Vulnerability in Task Scheduler Could Allow Code Execution (MS04-022)
Example
Remote code execution because of an unchecked buffer. If a user is logged on with administrator privileges, an attacker can take full control over the affected system. The worms/Trojan horses Bloodhound.exploit.11 and Bloodhound.exploit.12 exploit this vulnerability. (Symantec)
Solution
Install security update for Windows XP (KB841873)

Concern or Vulnerability
TCP 135 – Several vulnerabilities in RPC/DCOM (MS04-012)
Example
MS Windows RPC service crashes trying to dereference a null pointer when it receives a certain malformed request. (Nessus) These vulnerabilities can cause denial of service for the RPC/DCOM service or an attacker exploiting the vulnerability may take full control over the system. W32.Bobax.C worm, Several of the W32.Kibuv.Worm, several of the W32.Spybot.Worm, several of the W32.HLLW.Gaobot.gen, W32.Randex worm , several of the W32.Kobot worm, W32.Explet.A@mm, Backdoor.IRC.Whisper.B, W32.Dopbot, W32.Bropia.N, several versions of the W32.Kelvir worm, W32.Donk worm, W32.Mugly worm exploit DCOM RPC vulnerability using TCP port 135. (Symantec)
Solution
Block access to TCP port 135

Concern or Vulnerability
TCP 135
Example
Distributed Computing Environment services running on the remote host can be enumerated by connecting to port 135 and doing the appropriate queries. (Nessus)
Solution
Filter incoming traffic to this port

Concern or Vulnerability
Microsoft-ds TCP 445 – Multivulnerabilities (MS04-011)
Example
7. LSAS Vulnerability: Buffer overrun vulnerability. Can allow remote code execution on the remote system. The attacker can take complete control over the system. Several variants of W32.sasser Worm, several variants of W32.Korgo worm, Hacktool.LsassSba, several versions of the W32.bobax worm, W32.Huayu worm, W32.Multex worm, several versions of Trojan.Netdepix, W32.Aizu worm, Bloodhound.Exploit.8, W32.Waltz worm, W32.Cycle worm, several of the W32.Kibuv.Worm, W32.Janx worm, W32.Linkbot.H worm, several versions of the W32.Mytob@ worm, W32.Spybot.Worm, W32.HLLW.Gaobot.gen worm, W32.Randex worm, W32.Kobot worm, W32.Explet.A@mm worm, Trojan.Otinet, Backdoor.Sdbot.AA, Backdoor.IRC.Whisper.B, W32.Bropia.N, several versions of the W32.Kelvir worm, W32.Donk worm, W32.Mugly worm exploits this vulnerability. (Symantec) 8. Winlogon vulnerability: Buffer overrun vulnerability in the Windows logon process for users belonging to a Domain. Attackers can remotely execute code and take complete control over the system. The attacker needs permission to user objects in the Domain to exploit this vulnerability. 9. Metafile vulnerability: Vulnerability in the rendering of WMF and EMF image formats. An attacker can set up a website which is used to exploit this vulnerability. The attacker can obtain the same privileges as the user. 10. Help and support centre vulnerability: An attacker can exploit this vulnerability by setting up a malicious website or send out malicious emails, containing a malicious HCP URL. The attacker can take complete control over the system. 11. Negotiate SSP vulnerability: Buffer overrun vulnerability that can allow remote code execution. An attacker can take complete control over the system, but in most cases the result will be denial of service. 12. ASN.1 “Double free” vulnerability: Remote code execution vulnerability. The attacker may take complete control over the system, but is most likely to create a denial of service situation.
Solution

7. Use Firewall, Security Update for Windows XP (KB835732) 8. Security Update for Windows XP (KB835732) 9. Read E-mail in plain text, Security Update for Windows XP (KB835732) 10. Use IE 6.0 or later, OE 6.0 or later, Security Update for Windows XP (KB835732) 11. Security Update for Windows XP (KB835732) 12. Security Update for Windows XP (KB835732)

Concern or Vulnerability
Microsoft-ds TCP 445 – ASN.1 Vulnerability could allow code execution (MS04-007)
Example
A buffer overflow vulnerability in Microsoft ASN.1 library. An attacker can execute code with system privileges and take complete control over the system. Hacktool.Asni exploits this vulnerability.
Solution
Security Update for Windows XP (KB828028)

Concern or Vulnerability
Microsoft-ds TCP 445 – Named Pipe Vulnerability (MS05-007)
Example
An attacker can remotely read the user names of users who have an open connection to an available shared resource
Solution
Use Firewall, disabling the computer browser service, Security update for Windows XP (KB888302)

Concern or Vulnerability
Microsoft-ds TCP 445 – The host security identifier can be obtained remotely
Example
An attacker can use this to obtain a list of local users on this host. (Nessus)
Solution
Filter the ports 137-139 and 445

Concern or Vulnerability
Microsoft-ds TCP 445 – NULL sessions
Example
By logging in providing null user name and null password one can get a guest account.
Solution
Use Firewall

Concern or Vulnerability
TCP 1025
Example
Distributed Computing Environment service running on the host. Can be enumerated by connecting to port 135. (Nessus)
Solution
Filter incoming traffic to this port

Concern or Vulnerability
TCP 5000 – Microsoft UPnP TCP helper
Example
Should be disabled
Solution
Disable service

Concern or Vulnerability
UDP 135 – Buffer overrun in messenger service could allow code execution (MS03-043)
Example
Buffer overrun in messenger service could allow code execution. The attacker can run code with local system privileges. The attacker can take complete control over the system. W32.HLLW.Gaobot.gen worm, W32.Randex, W32.Spybot.Worm, W32.Kibuv, W32.Bropia.N, W32.Welchia Worm, W32.Mugly worm exploits this vulnerability.
Solution
Block NetBIOS ports 135-137 and UDP broadcast packets with a firewall, disable messenger service, Security Update for Windows XP (KB828035)

Concern or Vulnerability
NTP UDP 123
Example
Network Time Protocol Server is listening on this port
Solution

Concern or Vulnerability
Isakmp UDP 500
Example
Solution

Concern or Vulnerability
Netbios-ns UDP 137
Example
An attacker can find the netbios name of the computer
Solution
Filter incoming traffic to this port

Concern or Vulnerability
UDP 1027
Example
Distributed Computing Environment service running on the host. Can be enumerated by connecting to port 135. (Nessus)
Solution
Filter incoming traffic to this port

Vulnerabilities not discovered by the security testing.

Concern or Vulnerability
System can be compromised exploiting an unchecked buffer in the Windows shell (MS02-072)
Example
The attacker can create an malicious .MP3 or .WMA file and host it on a website or windows share. The vulnerability will be invoked if the user hover his mouse pointer over the file icon. This can mount a buffer overrun attack. The code will run with user privileges.
Solution
Windows XP Security Patch: Unchecked Buffer in Windows Shell Could Enable System Compromise

Concern or Vulnerability
Remote code execution due to flaw in Windows script engine (MS03-008)
Example
An attacker can construct a web page that will execute code with user privileges when visited by the user.
Solution
Turn off active scripting in Internet Explorer JScript 5.6 Security Patch for Windows 2000 and XP (814078)

Concern or Vulnerability
Flaw in Microsoft VM Could Enable System Compromise (MS03-011)
Example
An attacker can create a malicious java applet. It would exploit the vulnerability when the user visits the website. Will only get user privileges. This vulnerability is exploited by the Trojan horse Trojan.ByteVerify. (Symantec)
Solution
Patch available

Concern or Vulnerability
Flaw in Windows Media Player Skins Downloading could allow Code Execution (MS03-017)
Example
A flaw in the way Windows Media Player handles skin files, which gives the attacker an opportunity to place a malicious file on the system. The file will be run with user privileges. An attacker can make a malicious website that exploit this vulnerability
Solution
Windows Media Security Patch: Flaw in Windows Media Player Skins Downloading could allow Code Execution

Concern or Vulnerability
Buffer Overrun In HTML Converter Could Allow Code Execution (MS03-023)
Example
A buffer overrun vulnerability in the HTML converter that can be exploited by an attacker by making a malicious web site or a HTML e-mail. This can make arbitrary code run with user privileges.
Solution
Windows XP Security Patch: Buffer Overrun In HTML Converter Could Allow Code Execution

Concern or Vulnerability
Unchecked Buffer in DirectX Could Enable System Compromise (MS03-030)
Example
By exploiting this vulnerability an attacker can run arbitrary code with user privileges on the system. The attacker can make a malicious web site or a HTML e-mail which will exploit the vulnerability if the user visits it.
Solution
Windows XP Security Patch: Unchecked Buffer in DirectX Could Enable System Compromise

Concern or Vulnerability
Flaw in NetBIOS Could Lead to Information Disclosure (MS03-034)
Example
An attacker can retrieve arbitrary or random data from the memory of the computer by sending NetBT Name Service queries to the system.
Solution
Security Update for Windows XP (KB824105)

Concern or Vulnerability
Vulnerability in Authenticode Verification Could Allow Remote Code Execution (MS03-041)
Example
An attacker can make a malicious web site. An ActiveX control can be installed without user approval under certain low memory situation. The attacker can obtain user privileges.
Solution
Security Update for Microsoft Windows XP: KB823182

Concern or Vulnerability
Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (MS03-044)
Example
Due to an unchecked buffer in the HCP protocol an attacker can construct an URL, on a web page or in an e-mail, that can execute the code of choice in the local security context. An attacker can then read and launch files on the system.
Solution
Security Update for Microsoft Windows XP: KB825119

Concern or Vulnerability
Buffer Overrun in the Workstation Service Could Allow Code Execution (MS03-049)
Example
A vulnerability in the workstation service can allow remote code execution on the system. An attacker can gain system privileges on the system. This vulnerability is exploited by several worms and Trojans: Hacktool.WKRShell, W32.Randex, several of the W32.Gaobot.(X) worms, several of the W32.Spybot.(X) worms, W32.Bropia.N, several of the W32.Kelvir.(X) worms, several of the W32.Welchia.(X).Worm, several variants of the W32.Mugly.B@ worm. (Symantec)
Solution
Block inbound UDP ports 138, 139, 445 and TCP ports 138, 139, 445 Security Update for Microsoft Windows XP: KB828035

Concern or Vulnerability
Vulnerability in Help and Support Center Could Allow Remote Code Execution (MS04-015)
Example
An attacker can construct a malicious HCP URL on a web site or in an e-mail. If the remote code execution succeeds the attacker will get the same privileges as the user.
Solution
Security Update for Windows XP (KB840374)

Concern or Vulnerability
Vulnerability in HTML Help Could Allow Code Execution (MS04-023)
Example
An attacker can exploit these vulnerabilities by making a user visit a malicious web site. He will then gain user privileges
Solution
Security Update for Windows XP (KB840315)

Concern or Vulnerability
Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (MS04-028)
Example
A buffer overrun in JPEG processing can allow remote code execution. An attacker can gain the privileges of the user on the system. Several Trojan horses and backdoors exploit this vulnerability: severak variants of Backdoor.Roxe, several variants of Trojan.Ducky, Bloodhound.Exploit.13, Trojan.Moo, Hacktool.JPEGDownload, Hacktool.JPEGShell, W32.Yanz.B@mm. (Symantec)
Solution
Security Update for Windows XP (KB833987)

Concern or Vulnerability
Security Update for Microsoft Windows (MS04-032), Window Management Vulnerability, Virtual DOS Machine Vulnerability, Graphics Rendering Engine Vulnerability, Windows Kernel Vulnerability
Example
Window Management Vulnerability: This vulnerability will let a logged on user take complete control over the system. Vulnerability can only be exploited locally. Virtual DOS Machine Vulnerability: Logged in users can take complete control over the system. Vulnerability can only be exploited locally Graphics Rendering Engine Vulnerability: A special crafted WMF or EMF file could allow remot execution on a system if the user views a folder, mail or web site that contain the file. The attacker can take complete control over the system. This vulnerability is exploited by Bloodhound.Exploit.17, W32.Scard and Backdoor.Emcommander Windows Kernel Vulnerability: An attacker can locally run a program that will cause a denial of service attack on the workstation. The system will automatically restart.
Solution
Security Update for Windows XP (KB840987)

Concern or Vulnerability
Vulnerability in Compressed (zipped) Folders Could Allow Remote Code Execution (MS04-034)
Example
An unchecked buffer can be exploited by an attacker creating a malicious zipfile. A user can visit a website containing this file or receive it by e-mail. If the user try to open the file an attacker can take complete control over the system
Solution
Security Update for Windows XP (KB873376)

Concern or Vulnerability
Vulnerability in Windows Shell Could Allow Remote Code Execution (MS04-037)
Example
Shell Vulnerability: Remote code execution which could be exploited by an attacker by setting up a malicious web site. The attacker can take complete control over the system. Program Group Converter Vulnerability: Remote code execution when user open a malicious attachment or link, which can give an attacker complete control over the system. This vulnerability is exploited by Bloodhound.Exploit.15
Solution
Security Update for Windows XP (KB841356)

Concern or Vulnerability
Vulnerability in WordPad Could Allow Code Execution (MS04-041)
Example
Remote code execution vulnerability when opening malicious crafted .wri.rtf.doc files in WordPad. The attacker can obtain the same privileges as the user of the system.
Solution
Security Update for Windows XP (KB885836)

Concern or Vulnerability
Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege (MS04-044)
Example
Windows Kernel Vulnerability and LSASS Vulnerability could allow a logged in user to take full control over the system.
Solution
Security Update for Windows XP (KB885835)

Concern or Vulnerability
Vulnerability in HTML Help Could Allow Code Execution (MS05-001)
Example
An attacker can use a web site to exploit this remote code execution and information disclosure vulnerability. If the user visits the web page and the attack is successful the attacker can take complete control over the system. This vulnerability is exploited by several Trojans: Bloodhound.Exploit.21, several of the Trojan.Phel.A, Trojan.Phel.B and Trojan.Magise
Solution
Security Update for Windows XP (KB890175)

Concern or Vulnerability
Vulnerability in PNG Processing Could Allow Remote Code Execution (MS05-009)
Example
Several PNG Processing vulnerabilities exist in Windows Mediaplayer, Windows Messenger and MSN Messenger which can cause remote code execution. The attacker can get the privileges of the user on the system. This vulnerability is exploited by Bloodhound.Exploit.24
Solution
Update Windows Media Player, Windows Messenger and MSN Messenger.

Concern or Vulnerability
Vulnerability in OLE and COM Could Allow Remote Code Execution (MS05-012)
Example
COM Structured Storage Vulnerability: Privilage evelation vulnerability that can make the logged in user take full control of the system. Input Validation Vulnerability: A malicious document containing can be published on a website or by e-mail. User interaction is required to exploit the vulnerability which can execute code remotly and give the attacker complete control of the system.
Solution
Security Update for Windows XP (KB873333)

Concern or Vulnerability
Vulnerability in the DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (MS05-013)
Example
A vulnerability exists that can allow information disclosure and remote code execution. This can happen by visiting a malicious web site. The attacker can gain complete control over the system.
Solution
Security Update for Windows XP (KB891781)

Concern or Vulnerability
Vulnerability in Hyperlink Object Library Could Allow Remote Code Execution (MS05-015)
Example
An unchecked buffer while handling hyperlinks can be used to execute code remotely. If a user click on a malicious hyperlink in an e-mail or a website the malicious code can get executed and the attacker will get the privileges of the user on the system.
Solution
Security Update for Windows XP (KB888113)

Containment Measures Review Template

IP Address	Domain Name
192.168.1.171	NAGASAKI
Desktop Anti-virus / Anti-Trojan Mechanisms	
Norman Antivius	
Response to SAP 27 and 42.zip	
None	

Desktop Mail Client Types
Outlook Express 6.0 SP1
Desktop Mail Client Vulnerabilites (www.microsoft.com/technet/security/current.aspx)
• MHTML URL Handler vulnerability (MS03-014): Allows an attacker to run code on the user's machine. For the attack to work, Windows has to open a specially constructed MHTML URL from a web site or included in a HTML e-mail message. • Malformed header vulnerability (MS04-018): An attacker can send special crafted e-mail messages which will make Outlook Express fail, causing a denial of service situation. • MHTML URL Processing Vulnerability (MS04-013): A remote code execution vulnerability that can give an attacker complete control over the computer. Outlook Express processes special crafted MHTML URLs that will allow the attackers HTML code to be run in the Local Machines Security Zone in Internet Explorer. • Unchecked buffer in Windows help facility (MS02-055). The attacker can run code with the user privilege of the user of the system. Can be exploited by e-mail or website.

Desktop Browser Client Type
Internet Explorer 6.0 SP1
Desktop Browser Client Vulnerabilities (www.microsoft.com/technet/security/current.aspx)
• XMLHTTP vulnerability (MS02-008). An attacker can read from a data source on the user's system. The vulnerability is exploited from a website and the attacker has to know the full path to the file he wants to read. • A certificate validation flaw can enable identity spoofing (MS02-050).

Equipment	
Equipment Used	Switch
Servers, Number and Types	Astaro Security Linux v5 firewall, Fedora core 3 Samba server 3.0.x
Workstations, Number and Type	2x, Windows XP Professional SP1 and Suse Linux 9.2
Software used	Nessus 2.2.4, Nmap 3.70, Hping2, Enum, Winfingerprint, amap 4.8, Norman anti virus v5.8, WinXP IPSEC client
Host names used	DELL-XP
Network Topology	
Anti-virus Capabilities	Norman Antivirus v5.8
Network Protection Facilities Used	None
Remote Access Facilities Used	None
Routers Used	None
Physical Access Control Technology Used	None

SOLUTION 2

This solution is based on a out-of-the-box configuration of Windows XP Pro. Service Pack 1. No further updates have been installed. Norman anti virus v5.8 has been installed and is up-to-date. The Windows Internet Connection Firewall (ICF) has been enabled, with its default configuration in place. The Windows XP IPSec over L2TP client is activated.

Workstation Information Template

IP Address	Domain name
192.168.1.171	

This test didn't give much information. One host where found to be alive. Operation system and services running are unknown. When running Fin, XMAS and NULL scans with Nmap, all ports are reported open. If this is a windows computer, it will respond this way if the ports are open or not.

Port	Protocol	Service	Service Details
2950	TCP	Unknown	Closed
12307	TCP	Unknown	Open
ALL	TCP		Filtered
	UDP		459 ports closed – the rest open\filtered

Vulnerabilities not discovered by the security testing.

Concern or Vulnerability
System can be compromised exploiting an unchecked buffer in the Windows shell (MS02-072)
Example
The attacker can create an malicious .MP3 or .WMA file and host it on a website or windows share. The vulnerability will be invoked if the user hover his mouse pointer over the file icon. This can mount a buffer overrun attack. The code will run with user privilege.
Solution
Windows XP Security Patch: Unchecked Buffer in Windows Shell Could Enable System Compromise

Concern or Vulnerability
Remote code execution due to flaw in Windows script engine (MS03-008)
Example
An attacker can construct a web page that will execute code with user privileges when visited by the user.
Solution
Turn off active scripting in Internet Explorer JScript 5.6 Security Patch for Windows 2000 and XP (814078)

Concern or Vulnerability
Flaw in Microsoft VM Could Enable System Compromise (MS03-011)
Example
An attacker can create a malicious java applet. It would exploit the vulnerability when the user visits the website. Will only get user privileges. This vulnerability is exploited by the Trojan horse Trojan.ByteVerify. (Symantec)
Solution
Patch available

Concern or Vulnerability
Flaw in Windows Media Player Skins Downloading could allow Code Execution (MS03-017)
Example
A flaw in the way Windows Media Player handles skin files, which gives the attacker an opportunity to place a malicious file on the system. The file will be run with user privileges. An attacker can make a malicious website that exploit this vulnerability
Solution
Windows Media Security Patch: Flaw in Windows Media Player Skins Downloading could allow Code Execution

Concern or Vulnerability
Buffer Overrun In HTML Converter Could Allow Code Execution (MS03-023)
Example
A buffer overrun vulnerability in the HTML converter that can be exploited by an attacker by making a malicious web site or a HTML e-mail. This can make arbitrary code run with user privileges.
Solution
Windows XP Security Patch: Buffer Overrun In HTML Converter Could Allow Code Execution

Concern or Vulnerability
Unchecked Buffer in DirectX Could Enable System Compromise (MS03-030)
Example
By exploiting this vulnerability an attacker can run arbitrary code with user privileges on the system. The attacker can make a malicious web site or a HTML e-mail which will exploit the vulnerability if the user visits it.
Solution
Windows XP Security Patch: Unchecked Buffer in DirectX Could Enable System Compromise

Concern or Vulnerability
Flaw in NetBIOS Could Lead to Information Disclosure (MS03-034)
Example
An attacker can retrieve arbitrary or random data from the memory of the computer by sending NetBT Name Service queries to the system.
Solution
Security Update for Windows XP (KB824105)

Concern or Vulnerability
Vulnerability in Authenticode Verification Could Allow Remote Code Execution (MS03-041)
Example
An attacker can make a malicious web site. An ActiveX control can be installed without user approval under certain low memory situation. The attacker can obtain user privileges.
Solution
Security Update for Microsoft Windows XP: KB823182

Concern or Vulnerability
Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (MS03-044)
Example
Due to an unchecked buffer in the HCP protocol an attacker can construct an URL, on a web page or in an e-mail, that can execute the code of choice in the local security context. An attacker can then read and launch files on the system.
Solution
Security Update for Microsoft Windows XP: KB825119

Concern or Vulnerability
Buffer Overrun in the Workstation Service Could Allow Code Execution (MS03-049)
Example
A vulnerability in the workstation service can allow remote code execution on the system. An attacker can gain system privileges on the system. This vulnerability is exploited by several worms and Trojans: Hacktool.WKRShell, W32.Randex, several of the W32.Gaobot.(X) worms, several of the W32.Spybot.(X) worms, W32.Bropia.N, several of the W32.Kelvir.(X) worms, several of the W32.Welchia.(X).Worm, several variants of the W32.Mugly.B@ worm. (Symantec)
Solution
Block inbound UDP ports 138, 139, 445 and TCP ports 138, 139, 445 Security Update for Microsoft Windows XP: KB828035

Concern or Vulnerability
Vulnerability in Help and Support Center Could Allow Remote Code Execution (MS04-015)
Example
An attacker can construct a malicious HCP URL on a web site or in an e-mail. If the remote code execution succeeds the attacker will get the same privileges as the user.
Solution
Security Update for Windows XP (KB840374)

Concern or Vulnerability
Vulnerability in HTML Help Could Allow Code Execution (MS04-023)
Example
An attacker can exploit these vulnerabilities by making a user visit a malicious web site. He will then gain user privileges
Solution
Security Update for Windows XP (KB840315)

Concern or Vulnerability
Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (MS04-028)
Example
A buffer overrun in JPEG processing can allow remote code execution. An attacker can gain the privileges of the user on the system. Several Trojan horses and backdoors exploit this vulnerability: severak variants of Backdoor.Roxe, several variants of Trojan.Ducky, Bloodhound.Exploit.13, Trojan.Moo, Hacktool.JPEGDownload, Hacktool.JPEGShell, W32.Yanz.B@mm. (Symantec)
Solution
Security Update for Windows XP (KB833987)

Concern or Vulnerability
Security Update for Microsoft Windows (MS04-032), Window Management Vulnerability, Virtual DOS Machine Vulnerability, Graphics Rendering Engine Vulnerability, Windows Kernel Vulnerability
Example
Window Management Vulnerability: This vulnerability will let a logged on user take complete control over the system. Vulnerability can only be exploited locally. Virtual DOS Machine Vulnerability: Logged in users can take complete control over the system. Vulnerability can only be exploited locally Graphics Rendering Engine Vulnerability: A special crafted WMF or EMF file could allow remote execution on a system if the user views a folder, mail or web site that contain the file. The attacker can take complete control over the system. This vulnerability is exploited by Bloodhound.Exploit.17, W32.Scard and Backdoor.Emcommander Windows Kernel Vulnerability: An attacker can locally run a program that will cause a denial of service attack on the workstation. The system will automatically restart.
Solution
Security Update for Windows XP (KB840987)

Concern or Vulnerability
Vulnerability in Compressed (zipped) Folders Could Allow Remote Code Execution (MS04-034)
Example
An unchecked buffer can be exploited by an attacker creating a malicious zipfile. A user can visit a website containing this file or receive it by e-mail. If the user try to open the file an attacker can take complete control over the system
Solution
Security Update for Windows XP (KB873376)

Concern or Vulnerability
Vulnerability in Windows Shell Could Allow Remote Code Execution (MS04-037)
Example
Shell Vulnerability: Remote code execution which could be exploited by an attacker by setting up a malicious web site. The attacker can take complete control over the system. Program Group Converter Vulnerability: Remote code execution when user opens a malicious attachment or link, which can give an attacker complete control over the system. This vulnerability is exploited by Bloodhound.Exploit.15
Solution
Security Update for Windows XP (KB841356)

Concern or Vulnerability
Vulnerability in WordPad Could Allow Code Execution (MS04-041)
Example
Remote code execution vulnerability when opening malicious crafted .wri.rtf.doc files in WordPad. The attacker can obtain the same privileges as the user of the system.
Solution
Security Update for Windows XP (KB885836)

Concern or Vulnerability
Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege (MS04-044)
Example
Windows Kernel Vulnerability and LSASS Vulnerability could allow a logged in user to take full control over the system.
Solution
Security Update for Windows XP (KB885835)

Concern or Vulnerability
Vulnerability in HTML Help Could Allow Code Execution (MS05-001)
Example
An attacker can use a web site to exploit this remote code execution and information disclosure vulnerability. If the user visit the web page and the attack is successful the attacker can take complete control over the system. This vulnerability is exploited by several Trojans: Bloodhound.Exploit.21, several of the Trojan.Phel.A, Trojan.Phel.B and Trojan.Magise
Solution
Security Update for Windows XP (KB890175)

Concern or Vulnerability
Vulnerability in PNG Processing Could Allow Remote Code Execution (MS05-009)
Example
Several PNG Processing vulnerabilities exist in Windows Mediaplayer, Windows Messenger and MSN Messenger which can cause remote code execution. The attacker can get the privileges of the user on the system. This vulnerability is exploited by Bloodhound.Exploit.24
Solution
Update Windows Media Player, Windows Messenger and MSN Messenger.

Concern or Vulnerability
Vulnerability in OLE and COM Could Allow Remote Code Execution (MS05-012)
Example
COM Structured Storage Vulnerability: Privilege elevation vulnerability that can make the logged in user take full control of the system. Input Validation Vulnerability: A malicious document containing can be published on a website or by e-mail. User interaction is required to exploit the vulnerability which can execute code remotely and give the attacker complete control of the system.
Solution
Security Update for Windows XP (KB873333)

Concern or Vulnerability
Vulnerability in the DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (MS05-013)
Example
A vulnerability exist that can allow information disclosure and remote code execution. This can happen by visiting a malicious web site. The attacker can gain complete control over the system.
Solution
Security Update for Windows XP (KB891781)

Concern or Vulnerability
Vulnerability in Hyperlink Object Library Could Allow Remote Code Execution (MS05-015)
Example
An unchecked buffer while handling hyperlinks can be used to execute code remotely. If a user click on a malicious hyperlink in an e-mail or a website the malicious code can get executed and the attacker will get the privileges of the user on the system.
Solution
Security Update for Windows XP (KB888113)

Containment Measures Review Template

IP Address	Domain Name
192.168.1.171	NAGASAKI
Desktop Anti-virus / Anti-Trojan Mechanisms	
Norman Antivirus	
Response to SAP 27 and 42.zip	
None	

Desktop Mail Client Types
Outlook Express 6.0 SP1
Desktop Mail Client Vulnerabilites (www.microsoft.com/technet/security/current.aspx)
• MHTML URL Handler vulnerability (MS03-014): Allows an attacker to run code on the users machine. For the attack to work Windows have to open a specially constructed MHTML URL from an web site or included in a HTML e-mail message. • Malformed header vulnerability (MS04-018): An attacker can send special crafted e-mail messages which will make Outlook Express fail, causing a denial of service situation. • MHTML URL Processing Vulnerability (MS04-013): A remote code execution vulnerability that can give an attacker complete control over the computer. Outlook Express processes special crafted MHTML URLs that will allow the attackers HTML code to be run in the Local Machines Security Zone in Internet Explorer. • Unchecked buffer in Windows help facility (MS02-055). The attacker can run code with the user privilege of the user of the system. Can be exploited by e-mail or website.

Desktop Browser Client Type
Internet Explorer 6.0 SP1
Desktop Browser Client Vulnerabilities (www.microsoft.com/technet/security/current.aspx)
• XMLHTTP vulnerability (MS02-008). An attacker can read from a data source on the user's system. The vulnerability is exploited from a website and the attacker has to know the full path to the file he wants to read. • A certificate validation flaw can enable identity spoofing (MS02-050).

Equipment	
Equipment Used	Switch
Servers, Number and Types	Astaro Security Linux v5 firewall, Fedora core 3 Samba server 3.0.x
Workstations, Number and Type	2x, Windows XP Professional SP1 and Suse Linux 9.2
Software used	Norman Anti-virus v5.8, Win XP IPsec client, WinXP firewall, Nessus 2.2.4, Nmap 3.70, Hping2, Enum, Winfingerprint, amap 4.8
Host names used	DELL-XP
Network Topology	
Anti-virus Capabilities	Norman Anti-virus v5.8
Network Protection Facilities Used	ICF (Windows Firewall)
Remote Access Facilities Used	None
Routers Used	None
Physical Access Control Technology Used	None

SOLUTION 3

This solution is based on a out-of-the-box configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman anti virus v5.8 has been installed and is up-to-date. The Windows XP IPSec over L2TP client is activated.

Workstation Information Template

IP address	Domain name	Operating System
192.168.1.171	NAGASAKI	Windows XP SP2

Port	Protocol	Service	Service Details
135	TCP	Msrpc	Netbios session
139	TCP	Netbios-ssn	Netbios session / SMB server running on this port
445	TCP	Microsoft-ds	A CIFS server running on this port
2868	TCP	Unknown	
2869	TCP	http	
123	UDP	Ntp	Open \ filtered - Network Time Protocol Server listening
137	UDP	Netbios-ns	Open \ filtered
138	UDP	Netbios-dgm	Open \ filtered
445	UDP	Microsoft-ds	Open \ filtered
500	UDP	Isakmp	Open \ filtered

1030	UDP	Iad1	Open \ filtered
1121	UDP	Unknown	Open \ filtered
1701	UDP	L2TP	Open \ filtered
1900	UDP	UpnP	Open \ filtered
4500	UDP	Sae-urn	Open \ filtered

Banner(s)

Port	Protocol	Banner
135	TCP	Microsoft Windows msrpc
139	TCP	Netbios-session
445	TCP	Microsoft Windows XP microsoft-ds
137	UDP	Microsoft Windows NT netbios-ssn (Host: DELL-XP workgroup: NAGASAKI)

TCP Sequencing

TCP Secuence Prediction
Truly Random
TCP ISN Seq. Numbers
IPID Sequence Generation
Incremental - Non random IPIDs
Uptime
Unknown

Concern or Vulnerability
Microsoft-ds TCP 445 – NULL sessions
Example
By logging in providing null user name and null password one can get a guest account.
Solution
Use Firewall

Concern or Vulnerability
Netbios-ns UDP 137
Example
An attacker can find the netbios name of the computer
Solution
Filter incoming traffic to this port

Concern or Vulnerability
General ICMP
Example
The host answer ICMP times tamp requests. Can be used to defeat time based authentication protocols
Solution
Filter incoming ICMP 13 and outgoing ICMP

Containment Measures Review Template

IP Address	Domain Name
192.168.1.171	NAGASAKI
Desktop Anti-virus / Anti-Trojan Mechanisms	
Norman Anti-virus v5.8	
Response to SAP 27 and 42.zip	
Desktop Mail Client Types	
Outlook Express 6 [xpsp_sp2_rtm.040803-2158]	
Desktop Mail Client Vulnerabilities	
Desktop Browser Client Type	
Internet Explorer Version 6.0.2900.2180.xpsp_sp2_rtm.040803-2158	
Desktop Browser Client Vulnerabilities	

Equipment	
Equipment Used	Switch
Servers, Number and Types	Astaro Security Linux v5 firewall, Fedora core 3 Samba server 3.0.x
Workstations, Number and Type	2x, Windows XP Professional SP2 and Suse Linux 9.2
Software used	Norman Anti-virus v5.8, Win XP IPsec client, Nessus 2.2.4, Nmap 3.70, Hping2, Enum, Winfingerprint, amap 4.8
Host names used	DELL-XP
Network Topology	
Anti-virus Capabilities	Norman Anti-virus v5.8
Network Protection Facilities Used	None
Remote Access Facilities Used	None
Routers Used	None
Physical Access Control Technology Used	None

SOLUTION 4

This solution is based on a out-of-the-box configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman anti virus v5.8 has been installed and is up-to-date. The Windows Firewall has been enabled with its default configuration in place. The Windows XP IPSec over L2TP client is activated.

Workstation Information Template

IP Address	Domain name
192.168.1.171	

This test didn't give much information. One host where found to be alive. Operation system and services running are unknown. All ports are filtered, except from when running Fin, XMAS and NULL scan with Nmap, then all ports are reported open. If this is a windows computer, it will respond this way if the ports are open or not. When running UDP scan, Nmap reports all ports as open\filtered.

Containment Measures Review Template

IP Address	Domain Name
192.168.1.171	Unknown
Desktop Anti-virus / Anti-Trojan Mechanisms	
Norman Anti-virus v5.8	
Response to SAP 27 and 42.zip	
Desktop Mail Client Types	
Outlook Express 6 [xpsp_sp2_rtm.040803-2158]	
Desktop Mail Client Vulnerabilities	
Desktop Browser Client Type	
Internet Explorer Version 6.0.2900.2180.xpsp_sp2_rtm.040803-2158	
Desktop Browser Client Vulnerabilities	

Equipment	
Equipment Used	Switch
Servers, Number and Types	Astaro Security Linux v5 firewall, Fedora core 3 Samba server 3.0.x
Workstations, Number and Type	2x, Windows XP Professional SP2 and Suse Linux 9.2
Software used	Norman Anti-virus v5.8, Win XP IPsec client, Windows firewall, Nessus 2.2.4, Nmap 3.70, Hping2, Enum, Winfingerprint, amap 4.8
Host names used	DELL-XP
Network Topology	
Anti-virus Capabilities	Norman Anti-virus v5.8
Network Protection Facilities Used	ICF (Windows Firewall)
Remote Access Facilities Used	None
Routers Used	None
Physical Access Control Technology Used	None

SOLUTION 5

This solution is based on the out-of-the-box configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman antivirus v5.8 has been installed and is up-to-date. The Windows XP IPSec over L2TP client is activated. Zone Alarm Pro firewall is installed.

Workstation Information Template

IP address	Domain name
192.168.1.171	

Port	Protocol	Service	Service Details
2868	TCP	Unknown	
ALL	UDP		Open \ filtered

When running FIN, XMAS and NULL scan with Nmap, than all ports are reported open. If this is a windows computer it will respond this way if the ports are open or not.

TCP Sequencing

TCP Secuence Prediction
Unknown
TCP ISN Seq. Numbers
Unknown
IPID Sequence Generation
Unknown
Uptime
Unknown

Containment Measures Review Template

IP Address	Domain Name
192.168.1.171	
Desktop Anti-virus / Anti-Trojan Mechanisms	
Norman antivirus v5.8, ZoneAlarm Pro firewall (5.5.062.011)	
Response to SAP 27 and 42.zip	

Desktop Mail Client Types
Outlook Express 6 [xpsp_sp2_rtm.040803-2158]
Desktop Mail Client Vulnerabilities
Desktop Browser Client Type
Internet Explorer Version 6.0.2900.2180.xpsp_sp2_rtm.040803-2158
Desktop Browser Client Vulnerabilities

Equipment	
Equipment Used	Switch
Servers, Number and Types	Astaro Security Linux v5 firewall, Fedora core 3 Samba server 3.0.x
Workstations, Number and Type	2x, Windows XP Professional SP2 and Suse Linux 9.2
Software used	Norman Anti-virus v5.8, Win XP IPsec client, ZoneAlarm Pro firewall (5.5.062.011), Nessus 2.2.4, Nmap 3.70, Hping2, Enum, Winfingerprint, amap 4.8
Host names used	DELL-XP
Network Topology	
Anti-virus Capabilities	Norman Anti-virus v5.8
Network Protection Facilities Used	ZoneAlarm Pro firewall (5.5.062.011)
Remote Access Facilities Used	None
Routers Used	None
Physical Access Control Technology Used	None

SOLUTION 6

This solution is based on a hardened configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman antivirus v5.8 has been installed and is up-to-date. The Windows Firewall is enabled. The Windows XP IPSec over L2TP client is activated.

Workstation Information Template

IP Address	Operating System
192.168.1.171	

Port	Protocol	Service	Service Details
139	TCP	Netbios-ssn	Closed
445	TCP	Microsoft-ds	Closed
12108	TCP	Unknown	Closed
Remaining	TCP		Filtered
ALL	UDP		Open/filtered

TCP Sequencing

TCP Secuence Prediction
Unknown
TCP ISN Seq. Numbers
IPID Sequence Generation
Unknown
Uptime
Unknown

Containment Measures Review Template

IP Address	Domain Name
192.168.1.171	
Desktop Anti-virus / Anti-Trojan Mechanisms	
Norman Anti virus v5.8	
Response to SAP 27 and 42.zip	

Desktop Mail Client Types
Outlook Express 6 [xpsp_sp2_rtm.040803-2158]
Desktop Mail Client Vulnerabilities
Desktop Browser Client Type
Internet Explorer Version 6.0.2900.2180.xpsp_sp2_rtm.040803-2158
Desktop Browser Client Vulnerabilities

Equipment	
Equipment Used	Switch
Servers, Number and Types	Astaro Security Linux v5 firewall, Fedora core 3 Samba server 3.0.x
Workstations, Number and Type	2x, Windows XP Professional SP2 and Suse Linux 9.2
Software used	Norman Anti-virus v5.8, Windows Firewall , Win XP IPsec client, Nessus 2.2.4, Nmap 3.70, Hping2, Enum, Winfingerprint, amap 4.8
Host names used	DELL-XP
Network Topology	
Anti-virus Capabilities	Norman Anti-virus v5.8
Network Protection Facilities Used	Windows Firewall
Remote Access Facilities Used	None
Routers Used	None
Physical Access Control Technology Used	None

SOLUTION 7

This solution is based on a hardened configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman anti virus v5.8 has been installed and is up-to-date. Zone Alarm Pro firewall is installed. The Windows XP IPSec over L2TP client is activated.

Workstation Information Template

IP Address	Operating System
192.168.1.171	

Port	Protocol	Service	Service Details
2868	TCP	Unknown	

TCP Sequencing

TCP Secuence Prediction
Unknown
TCP ISN Seq. Numbers
IPID Sequence Generation
Unknown
Uptime
Unknown

Containment Measures Review Template

IP Address	Domain Name
192.168.1.171	
Desktop Anti-virus / Anti-Trojan Mechanisms	
Norman Anti virus v5.8, ZoneAlarm Pro firewall (5.5.062.011)	
Response to SAP 27 and 42.zip	

Desktop Mail Client Types
Outlook Express 6 [xpsp_sp2_rtm.040803-2158]
Desktop Mail Client Vulnerabilities
Desktop Browser Client Type
Internet Explorer Version 6.0.2900.2180.xpsp_sp2_rtm.040803-2158
Desktop Browser Client Vulnerabilities

Equipment	
Equipment Used	Switch
Servers, Number and Types	Astaro Security Linux v5 firewall, Fedora core 3 Samba server 3.0.x
Workstations, Number and Type	2x, Windows XP Professional SP2 and Suse Linux 9.2
Software used	Norman Anti-virus v5.8, ZoneAlarm Pro firewall (5.5.062.011), Win XP IPsec client, Nessus 2.2.4, Nmap 3.70, Hping2, Enum, Winfingerprint, amap 4.8
Host names used	DELL-XP
Network Topology	
Anti-virus Capabilities	Norman Anti-virus v5.8
Network Protection Facilities Used	ZoneAlarm Pro firewall (5.5.062.011)
Remote Access Facilities Used	None
Routers Used	None
Physical Access Control Technology Used	None

SOLUTION 8

This solution is based on the out-of-the-box configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman anti virus v5.8 has been installed and is up-to-date. The Windows Firewall has been enabled with its default configuration in place. A broadband router with NAT and ACL and IPSec is used.

Workstation Information Template

IP Address	Domain name
192.168.0.137	

This test didn't give much information. One host where found to be alive. Operation system and services running are unknown. All ports are filtered, except from when running Fin, XMAS and NULL scan with Nmap, then all ports are reported open. If this is a windows computer, it will respond this way if the ports are open or not. When running UDP scan, Nmap reports all ports as open\filtered

Firewall Analysis Template

Fingerprinting

This test is to determine the success of various packet response fingerprinting methods through the firewall

Method	Result
Nmap –O	Running: FastComm embedded, DEC TOPS-20 OS details: FastComm FRAD (Frame Relay Access Device) F9200-DS-DNI – Ver.4.2.3A, DEC TOPS-20 Monitor 7(102540)-1,TD-1
Nmap –O	D-Link

Stealth

This determines the viability of SYN stealth scanning through the firewall for enumeration

Result
TCP 1040, 34104, 37958 – 38050

Source port control

This test measures the use of scanning with specific source ports through the firewall for enumeration

Protocol	Source	Results
TCP	20	Open ports:1040, 57782 – 57872
TCP	21	Open ports:1040, 58734 – 58820
TCP	22	Open ports:1040, 59654 – 59743
TCP	23	Open ports:1040, 60600 – 60691
TCP	53	Open ports:1040, 34138 – 34224
TCP	80	Open ports:1040, 35072 – 35167
TCP	110	Open ports:1040, 36021 - 36107
TCP	143	Open ports:1040, 36879 – 36940
TCP	443	Open ports:1040, 37829 – 37887

Overlap

This test measures the ability of the firewall to handle overlapped fragments such as that used in the TEARDROP attack

Protocol	Results

Fragments

This test measures the ability of the firewall to handle tiny fragmented packets.

IP	Result

SYN flood

This test the firewall's ability to manage an ongoing series of SYN packets coming in

IP	Result

RST flag

This test exacts the firewall's response to packets with RST flag set.

IP	Result
192.168.1.5	1040, 34104, 39096 – 39128

UDP

This tests the firewall's management of standard UDP packets.

IP	Result
192.168.1.5	1040, 42400 – 42477

ACK

This test is to discover the firewall's ability to screen enumeration techniques using ACK packets.

IP	Result
192.168.1.5	1040, 43359 – 43417

FIN

This test is to discover the firewall's ability to screen enumeration techniques using FIN packets

IP	Result
192.168.1.5	1040, 50126 – 50207

NULL

This test is to discover the firewall's ability to screen enumeration techniques using NULL packets

IP	Result
192.168.1.5	1040, 53495 – 53581

WIN

This test is to discover the firewall's ability to screen enumeration techniques using WIN packets

IP	Result

XMAS

This test is to discover the firewall's ability to screen enumeration techniques using packets with all flags set.

IP	Result
192.168.1.5	1040, 56848 - 56942

Containment Measures Review Template

IP Address	Domain Name
192.168.1.171	Unknown
Desktop Anti-virus / Anti-Trojan Mechanisms	
Norman Anti-virus v5.8	
Response to SAP 27 and 42.zip	

Desktop Mail Client Types
Outlook Express 6 [xpsp_sp2_rtm.040803-2158]
Desktop Mail Client Vulnerabilities
Desktop Browser Client Type
Internet Explorer Version 6.0.2900.2180.xpsp_sp2_rtm.040803-2158
Desktop Browser Client Vulnerabilities

Equipment	
Equipment Used	Switch
Servers, Number and Types	Astaro Security Linux v5 firewall, Fedora core 3 Samba server 3.0.x
Workstations, Number and Type	2x, Windows XP Professional SP2 and Suse Linux 9.2
Software used	Norman Anti-virus v5.8, Win XP IPsec client, Windows firewall, Nessus 2.2.4, Nmap 3.70, Hping2, Enum, Winfingerprint, amap 4.8, ftester 0,9
Host names used	DELL-XP
Network Topology	
Anti-virus Capabilities	Norman Anti-virus v5.8
Network Protection Facilities Used	Windows Firewall, Router
Remote Access Facilities Used	None
Routers Used	None
Physical Access Control Technology Used	None

SOLUTION 9

This solution is based on the out-of-the-box configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman antivirus v5.8 has been installed and is up-to-date. Zone Alarm Pro firewall is installed. A broadband router with NAT and ACL and IPSec is used.

Workstation Information Template

IP address	Domain name
192.168.0.137	

Port	Protocol	Service	Service Details
ALL	UDP		Open \ filtered

When running FIN, XMAS and NULL scan with Nmap, than all ports are reported open. If this is a windows computer, it will respond this way if the ports are open or not. When running UDP scan, Nmap reports all ports as open\filtered. I was not able to identify TCP sequence predictability, TCP ISN sequence numbers predictability or IPID sequence generation predictability.

TCP Sequencing

TCP Secuence Prediction
Unknown
TCP ISN Seq. Numbers
Unknown
IPID Sequence Generation
Unknown
Uptime
Unknown

Firewall Analysis Template

Fingerprinting

This test is to determine the success of various packet response fingerprinting methods through the firewall

Method	Result
Nmap –O	Running: FastComm embedded, DEC TOPS-20 OS details: FastComm FRAD (Frame Relay Access Device) F9200-DS-DNI – Ver.4.2.3A, DEC TOPS-20 Monitor 7(102540)-1,TD-1
Nmap –O	D-Link

Stealth

This determines the viability of SYN stealth scanning through the firewall for enumeration

Result
TCP 1040, 34104, 37958 – 38050

Source port control

This test measures the use of scanning with specific source ports through the firewall for enumeration

Protocol	Source	Results
TCP	20	Open ports:1040, 57782 – 57872
TCP	21	Open ports:1040, 58734 – 58820
TCP	22	Open ports:1040, 59654 – 59743
TCP	23	Open ports:1040, 60600 – 60691
TCP	53	Open ports:1040, 34138 – 34224
TCP	80	Open ports:1040, 35072 – 35167
TCP	110	Open ports:1040, 36021 - 36107
TCP	143	Open ports:1040, 36879 – 36940
TCP	443	Open ports:1040, 37829 – 37887

Overlap

This test measures the ability of the firewall to handle overlapped fragments such as that used in the TEARDROP attack

Protocol	Results

Fragments

This test measures the ability of the firewall to handle tiny fragmented packets.

IP	Result

SYN flood

This test the firewall's ability to manage an ongoing series of SYN packets coming in

IP	Result

RST flag

This test exacts the firewall's response to packets with RST flag set.

IP	Result
192.168.1.5	1040, 34104, 39096 – 39128

UDP

This tests the firewall's management of standard UDP packets.

IP	Result
192.168.1.5	1040, 42400 – 42477

ACK

This test is to discover the firewall's ability to screen enumeration techniques using ACK packets.

IP	Result
192.168.1.5	1040, 43359 – 43417

FIN

This test is to discover the firewall's ability to screen enumeration techniques using FIN packets

IP	Result
192.168.1.5	1040, 50126 – 50207

NULL

This test is to discover the firewall's ability to screen enumeration techniques using NULL packets

IP	Result
192.168.1.5	1040, 53495 – 53581

WIN

This test is to discover the firewall's ability to screen enumeration techniques using WIN packets

IP	Result

XMAS

This test is to discover the firewall's ability to screen enumeration techniques using packets with all flags set.

IP	Result
192.168.1.5	1040, 56848 - 56942

Containment Measures Review Template

IP Address	Domain Name
192.168.1.171	
Desktop Anti-virus / Anti-Trojan Mechanisms	
Norman antivirus v5.8, ZoneAlarm Pro firewall (5.5.062.011)	
Response to SAP 27 and 42.zip	

Desktop Mail Client Types
Outlook Express 6 [xpsp_sp2_rtm.040803-2158]
Desktop Mail Client Vulnerabilities

Desktop Browser Client Type
Internet Explorer Version 6.0.2900.2180.xpsp_sp2_rtm.040803-2158
Desktop Browser Client Vulnerabilities

Equipment	
Equipment Used	Switch
Servers, Number and Types	Astaro Security Linux v5 firewall, Fedora core 3 Samba server 3.0.x
Workstations, Number and Type	2x, Windows XP Professional SP2 and Suse Linux 9.2
Software used	Norman Anti-virus v5.8, Win XP IPsec client, Nessus 2.2.4, Nmap 3.70, Hping2, Enum, Winfingerprint, amap 4.8, Ftester 0,9
Host names used	DELL-XP
Network Topology	
Anti-virus Capabilities	Norman Anti-virus v5.8
Network Protection Facilities Used	ZoneAlarm Pro firewall (5.5.062.011), Router
Remote Access Facilities Used	None
Routers Used	None
Physical Access Control Technology Used	None

SOLUTION 10

This solution is based on a hardened configuration of Windows XP Pro. Service Pack 2 with the newest updates installed. Norman anti virus v5.8 has been installed and is up-to-date. Zone Alarm Pro firewall is installed. A hardened broadband router with NAT and ACL and IPSec is used.

Workstation Information Template

IP Address	Operating System
192.168.0.137	

Port	Protocol	Service	Service Details

TCP Sequencing

TCP Secuence Prediction
Unknown
TCP ISN Seq. Numbers
IPID Sequence Generation
Unknown
Uptime
Unknown

Firewall Analysis Template

Fingerprinting

This test is to determine the success of various packet response fingerprinting methods through the firewall

Method	Result
Nmap –O	Running: FastComm embedded, DEC TOPS-20 OS details: FastComm FRAD (Frame Relay Access Device) F9200-DS-DNI – Ver.4.2.3A, DEC TOPS-20 Monitor 7(102540)-1,TD-1
Nmap –O	D-Link

Stealth

This determines the viability of SYN stealth scanning through the firewall for enumeration

Result

Source port control

This test measures the use of scanning with specific source ports through the firewall for enumeration

Protocol	Source	Results
TCP	53	1040, 48625 – 48715

Overlap

This test measures the ability of the firewall to handle overlapped fragments such as that used in the TEARDROP attack

Protocol	Results

Fragments

This test measures the ability of the firewall to handle tiny fragmented packets.

IP	Result

SYN flood

This test the firewall's ability to manage an ongoing series of SYN packets coming in

IP	Result

RST flag

This test exacts the firewall's response to packets with RST flag set.

IP	Result

UDP

This tests the firewall's management of standard UDP packets.

IP	Result

ACK

This test is to discover the firewall's ability to screen enumeration techniques using ACK packets.

IP	Result

FIN

This test is to discover the firewall's ability to screen enumeration techniques using FIN packets

IP	Result

NULL

This test is to discover the firewall's ability to screen enumeration techniques using NULL packets

IP	Result

WIN

This test is to discover the firewall's ability to screen enumeration techniques using WIN packets

IP	Result

XMAS

This test is to discover the firewall's ability to screen enumeration techniques using packets with all flags set.

IP	Result

Containment Measures Review Template

IP Address	Domain Name
192.168.1.171	
Desktop Anti-virus / Anti-Trojan Mechanisms	
Norman Anti virus v5.8, ZoneAlarm Pro firewall (5.5.062.011)	
Response to SAP 27 and 42.zip	
Desktop Mail Client Types	
Outlook Express 6 [xpsp_sp2_rtm.040803-2158]	
Desktop Mail Client Vulnerabilities	
Desktop Browser Client Type	
Internet Explorer Version 6.0.2900.2180.xpsp_sp2_rtm.040803-2158	
Desktop Browser Client Vulnerabilities	

Equipment	
Equipment Used	Switch
Servers, Number and Types	Astaro Security Linux v5 firewall, Fedora core 3 Samba server 3.0.x
Workstations, Number and Type	2x, Windows XP Professional SP2 and Suse Linux 9.2
Software used	Norman Anti-virus v5.8, ZoneAlarm Pro firewall (5.5.062.011), Win XP IPsec client, Nessus 2.2.4, Nmap 3.70, Hping2, Enum, Winfingerprint, amap 4.8, Ftester 0,9
Host names used	DELL-XP
Network Topology	
Anti-virus Capabilities	Norman Anti-virus v5.8
Network Protection Facilities Used	ZoneAlarm Pro firewall (5.5.062.011), Router
Remote Access Facilities Used	None
Routers Used	None
Physical Access Control Technology Used	None