2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

가상침투를 이용한 SMTP 서버 취약성 분석 방법 연구

장정식, 김점구
남서울대학교 컴퓨터학과
e-mail:korman99@hanmail.net

A Study on the Methods of Vulnerability Analysis for SMTP Server Using Virtual Penetration Testing

Jung-Sik Jang, Jeom-Goo Kim
Dept of Computer Science, Namseoul University

요 약

스팸 전자우편과 전자우편 폭탄을 차단하기 위한 제품들은 많이 나와 있지만, 이러한 차단 제품들의 성능에 대한 신뢰성 있는 검증 자료는 많지 않으며, 검증 결과도 밴더(vendor)들의 주관이 개입될 수 있기 때문에 객관성과 공정성 면에서 부족하다고 하겠다. 이것은 차단 제품들의 성능과 잠재된 취약성을 분석하는 분석 방식의 부족과 기존의 분석 방식들의 한계성에 기인한다고 하겠다. 본 논문에서는 기존의 분석 방식들이 가지고 있는 한계점을 개선하고, 제품의 취약성 분석 과정을 자동화하여 소요되는 시간과 인적 낭비를 줄이고, 반복적으로 분석이 용이하며, 분석 결과와 관련된 취약성 정보를 제공하여 비전문가라도 취약성 분석이 용이한 SMTP 서버 보호를 위한 취약성 분석 자동화 도구를 제안한다.

1. 서 론

기존의 전화나 편지, 팩스 등이 나름대로의 편리함을 가지고 있으나, 인터넷을 이용한 전자우편(E-mail)이 주는 신속성과 정확성 그리고 음성, 영상, 텍스트 등을 포함하는 정보의 다양성으로 인하여 전자우편 서비스의 사용은 크게 늘어나고 있다.

그러나 개인 및 기업 업무의 필수요소가 된 전자우편은 한국정보보호센터 해킹 통계 자료에 의하면 전자우편 관련 침해의 90% 이상이 스팸 전자우편과 전자우편 폭탄에 의해 이루어지고 있다.

전자우편은 TCP/IP의 SMTP(simple mail transfer protocol) 프로토콜을 사용하는 SMTP 서버에 의해서 발송하게 되는데, 스팸 전자우편(spam e-mail)이나, 대량의 전자우편을 발송하는 전자우편 폭탄(e-mail bomb)에 의해서 SMTP 서버에 장애를 일으키는 등 기업의 업무 마비 및 사생활 침해의 피해뿐만 아니라 이를 처리하기 위하여 소요되는 네트워크 자원 및 시스템 자원, 인적 자원의 막대한 손실을 초래하고 있다.

현재 이에 대한 대책으로 패킷 필터링 라우터(packet filtering router), 침입차단시스템(firewall) 등의 정보보호 시스템이나, *ProcMail*, *BlackMail* 등의 스팸 전자우편 차단 프로그램을 사용하여 원하지 않는 전자우편을 차단하고 있다.

그러나 스팸 전자우편과 전자우편 폭탄을 차단하여 SMTP 서버를 보호하는 제품들의 성능이 적절하고 사용자의 요구에 맞게 운영되고 있다는 검증 자료는 많지 않으며, 검증 결과도 밴더들의 주관이 개입될 수 있기 때문에 객관성과 공정성 면에서 떨어진다고 하겠다. 이것은 차단 제품들의 성능 및 잠재된 취약성을 분석하는 분석 방식의 부족과 기존의 있는 분석 방식들의 한계성에 원인이 있다고 하겠다. 그러나 스팸 전자우편과 전자우편 폭탄에 의한 침해시 피해의 규모와 영향을 생각할 때, 정확하고 객관적인 새로운 취약성 분석 방식의 마련은 시급하다고 하겠다.

따라서 본 논문에서는 기존의 스팸 전자우편 차단 제품들의 취약성을 분석하는 방식보다도, 사용 편이성과 효용성 면에서 개선되고, 기존의 분석 방식들이 안고 있는 시간과 인적 낭비요소를 줄일 수 있으며, 취약성 분석에 있어 분석자의 주관을 최소화하여 객관성과 공정성을 갖도록 하는 SMTP 서버 보호를 위한 취약성 분석 자동화 도구를 설계하였다.

2. SMTP 서버 관련 취약성

SMTP 서버의 취약성은 스팸 전자우편에 의한 취약성, 첨부파일의 바이러스에 의한 취약성, SMTP 서버 구성상의 취약성 등으로 구분할 수 있다. 그러나 취약성 중에서 침해에 가장 많이 사용되고 있는 것은 스팸 전자우편에 의한 취약성이다.

이 장에서는 SMTP 서버 관련 취약성 중에서 전자우편 서비스의 활성화에 역행하여 사회 전반에 미치는 영향이 크고 사회적으로 문제가 되고 있는 스팸 전자우편과 전자우편 폭탄의 유형에 대해서 알아본다.

2.1 스팸 전자우편

스팸 전자우편이란 사용자가 요청하지 않은 정보를 사용자의 의사와는 무관하게 전달하는 전자우편을 말하는데, 인터넷의 활성화와 함께 전자우편 사용인구가 늘어나면서 대부분의 기업들은 광고와 홍보 수단으로 사용하고 있다. 사용자의 의사와는 관계없이 전자우편을 발송하다보니 받는 전자우편의 수가 점차 많아지고 유용하지 않은 정보까지 전달되어 개인의 권리를 침해하고 있다. 이렇게 스팸 전자우편을 발송하는 사람을 스패머(spammer)라고 한다.

스팸 전자우편은 전달 유형에 따라 직접 발송 스팸 전자우편(incoming spam E-mail)과 중계 스팸 전자우편(relay spam e-mail)으로 구분한다.

가. 직접발송 스팸 전자우편

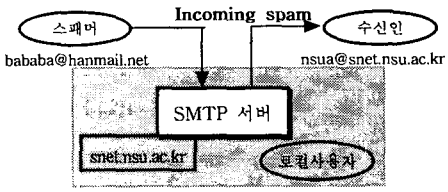
스패머에 의해서 사용자가 원하지 않는 전자우편이 사용자의 전자우편 계정이나 전자우편 서버로 직접 보내지는 스팸 전자우편을 말하는데, 많은 스팸 전자우편을 발송하기 때문에 트래픽이 증가해 회선 비용이 높아지며 서버 정지 현상이 나타날 수 있다.

(그림 1)은 스패머에 의해서 발송지 주소가 위조된 스팸 전자우편의 헤더 내용이다. (그림 1)의 ①은 전자우편 수신자가 답장을 보낼시 받게 되는 전자우편 주소를 나타내는데, 대부분 전자우편 주소는 위조되어 진다. ②는 192.168.13.23으로부터 snet.nsu.ac.kr를 통하여 nsua@snet.nsu.ac.kr로 직접 전자우편이 보내어졌음을 나타내고 ③은 조작된 발신지 주소를 나타낸다. 그리고 ④는 스팸 전자우편의 본문 내용이다.

```
① Return-Path: <bababa@hanmail.net>
② Received: from hack.com ([192.168.13.23])
      by snet.nsu.ac.kr (8.9.3/8.8.7) with SMTP id PAA04831
      for nsua@snet.nsu.ac.kr; Thu, 31 Aug 2000 15:54:08 +0900
   Date: Thu, 31 Aug 2000 15:54:08 +0900
③ From: bababa@hanmail.net
   Message-Id: <200008310654.PAA04831@snet.nsu.ac.kr>
   Subject: test haktek
   To: nsua@snet.nsu.ac.kr
   Status: R
   X-Status: N
④ I spy with my little eye...
```

(그림 1) 직접발송 스팸 전자우편의 헤더

(그림 2)는 (그림 1)의 스팸 전자우편의 헤더 내용에 따라 직접발송 스팸 전자우편의 유형을 도식화한 것이다.



(그림 2) 직접발송 스팸 전자우편의 유형

나. 중계 스팸 전자우편

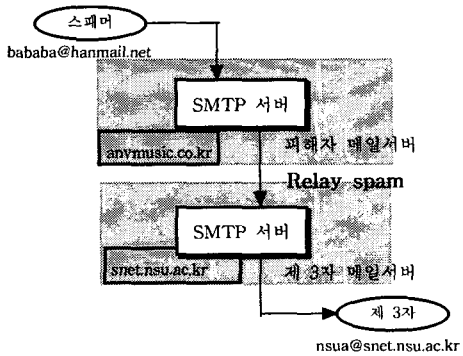
중계 스팸 전자우편은 스패머 자신의 전자우편 서버가 아닌 피해자의 전자우편 서버를 이용하여 제 3자에게 스팸 전자우편을 발송하는 유형이다. 중계된 피해자의 전자우편 서버가 스패머로 오인 받는 경우 인터넷 서비스 업체(ISP)들과 사용자로부터 전자우편 발송을 거부당할 수 있기 때문에 직접발송 스팸 전자우편 보다 피해가 심각하고 지속적이라고 하겠다.

```
① Return-Path: <bababa@hanmail.net>
② Received: from anymusic.co.kr (IDENT:root@[210.127.71.95])
      by snet.nsu.ac.kr (8.9.3/8.8.7) with ESMTP id PAA04879
      for <nsua@snet.nsu.ac.kr>;Thu, 31 Aug 2000 15:58:07 +0900
   From: bababa@hanmail.net
② Received: from hack.com ([210.95.164.1])
      by anymusic.co.kr (8.9.3/8.8.7) with SMTP id PAA14219
      for nsua@snet.nsu.ac.kr; Thu, 31 Aug 2000 15:56:48 +0900
   Date: Thu, 31 Aug 2000 15:56:48 +0900
   Message-Id: <200008310656.PAA14219@anymusic.co.kr>
   Subject: test haktek
③ To: nsua@snet.nsu.ac.kr
   Status: R
   X-Status: N
④ I spy with my little eye...
```

(그림 3) 중계 스팸 전자우편의 헤더

(그림 3)은 스패머에 의해서 발송지 주소가 위조된 중계 스팸 전자우편의 헤더 내용이다. (그림 3)의 ①은 답장을 보낼 시 받게 되는 위조된 전자우편 주소이고, ②는 210.95.164.1로부터 anymusic.co.kr로 전자우편이 보내어 지고, anymusic.co.kr에서 snet.nsu.ac.kr을 통하여 nsua@snet.nsu.ac.kr로 전자우편이 보내어졌음을 나타내고 있다. 그리고 ③은 수신자의 전자우편 주소를 나타내고, ④는 스팸 전자우편의 본문 내용이다.

(그림 4)는 (그림 3)의 스팸 전자우편의 헤더 내용에 따라 중계 스팸 전자우편의 유형을 도식화한 것이다.

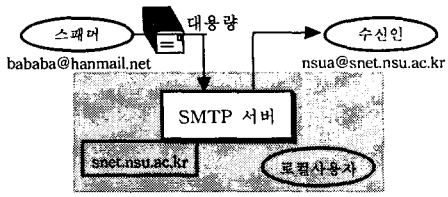


(그림 4) 중계 스팸 전자우편의 유형

2.2 전자우편 폭탄

전자우편 폭탄은 소용량의 전자우편을 동일한 사용자에게 무수히 전송하는 유형과 특정 사용자를 많은 수의 전자우편 그룹(mailing list)에 가입시켜 동시에 대량의 전자우편을 받게 하는 유형, 그리고 대용량의 전자우편을 전송하는 유형 등이 있는데, 대부분 전자우편의 헤더 내용을 위조하여 발신자의 정보를 숨기고 스패머가 지정한 횟수만큼 전자우편 발송이 가능한 'Avanche'나 'Kaboom' 등의 전자우편 폭탄 발송 프로그램을 이용하게 된다.

(그림 5)는 전자우편 폭탄의 유형을 도식화한 것으로, bababa@hanmail.net이라는 위조된 주소로부터 nsua@snet.nsu.ac.kr로 대용량의 전자우편 폭탄이 직접 발송되는 형태를 보여주고 있다.



(그림 5) 전자우편 폭탄의 유형

3. 기존의 취약성 분석방식과 새로운 분석모델 제안

스팸 전자우편과 전자우편 폭탄을 차단하기 위한 방법은 패킷 필터링 라우터, 침입차단시스템과 같은 정보보호 시스템을 설치하여 네트워크 상에서 차단하는 방법과 ProcMail, BlackMail 등의 전자우편 차단 프로그램을 사용하여 클라이언트 상에서 차단하는 방법 그리고 전자우편 서버 시스템 자체에서 중계 거부 설정과 전자우편 차단 리스트 등을 작성하여 차단하는 방법이 있다.

그러나 현재 이러한 스팸 전자우편 차단 제품들의 성능이 적절하고 사용자의 요구에 맞게 운영되고 있다는 검증된 자료는 많지 않다. 그리고 검증된 결과도 밴더들의 주관이 개입될 수 있기 때문에 객관성과 공정성 면에서 떨어진다고 하겠다. 이 장에서는 차단 제품들의 성능 및 잠재된 취약성을 분석하는 기존의 분석 방식과 한계점들을 알아보고 본 논문에서 제안하는 스팸 전자우편 차단 제품에 대한 취약성 분석을 자동화할 수 있는 새로운 분석 모델을 제시한다.

3.1 침투 시험 방식

침투시험 방식은 스팸 전자우편 차단 제품의 정보를 가지고 취약성 분석을 위한 시나리오를 구성하여 시나리오에 따라 직접 분석 환경을 구성해 수작업으로 취약성 분석이 이루어지는 방식이다. 즉, 침입차단시스템에서 허용 최대 메일 크기 제한이 되는지에 대한 분석은 직접적으로 허용 크기 이상의 전자우편을 만들어 직접 발송하여 제한되는지 여부만을 알 수 있게 된다.

침투시험 방식은 스팸 전자우편을 막기 위한 제품들의 반응 여부를 즉시 알 수 있으나, 허용 한계 값에 대한 분석과 그 허용 값의 증가에 따른 분석, 그리고 한계 값 이상에서 나타날 수 있는 반응에 대한 분석이 불가능하다. 또한 분석자가 직접 침투 환경을 구성해야 하기 때문에 분석에 많은 시간이 소요된다는 한계가 있다.

3.2 스팸 전자우편 발송 도구를 이용한 방식

이 방식은 스팸 전자우편 발송 도구를 이용하여 직접적으로 서버 상에 공격해 봄으로써 취약성을 분석하는 방식이다. 그러나 스팸 전자우편 발송 도구를 사용하는 것에는 문제가 있다. 대부분의 프로그램들이 대용량의 전자우편이나 많은 수의 전자우편을 발송하여 시스템에 피해를 주는 형태이기 때문에 취약성이 분석되는 부분은 수신되는 전자우편의 개수 제한 여부와 수신되는 전자우편의 파일 크기 제한 여부만이 가능하다. 그러므로 취약성이 분석되는 부분은 극히 제한적이고 분석 결과를 사용자가 모니터링하여 쉽게 분석할 수 없다는 단점이 있다. <표 1>은 현재 사용되고 있는 스팸 전자우편 발송 프로그램의 종류와 그 기능을 나타내고 있다.

<표 1> 스팸 전자우편 발송 프로그램의 종류와 기능

스팸 프로그램	헤더 위조	메일 폭탄	대량 메일링 리스트 가입	중계
AnonyMail	V	V		
Avanache v3.7	V	V	V	V
Kaboom v3.0	V	V	V	
Upyours v4.0	V	V		V
QuickFyre	V	V		
HakTek	V	V		
Voodoo	V	V		

3.3 취약성 분석 자동화 모델 제안

기존의 침투 시험 방식이나 스팸 발송용 도구에 의한 취약성 분석 방식은 분석 과정의 수작업으로 인해 시간과 인적 낭비요소가 발생할 수 있고 분석 결과에 분석자의 주관적 요소가 개입될 수 있는 여지가 있었다. 또한 분석에 대한 반응 여부만을 알 수 있는 등 분석 부분이 제한적이기 때문에 다양한 강도에 따른 취약성 분석결과를 도출할 수 없는 단점이 있다.

차단 제품의 취약성 분석은 무엇보다도 분석자의 편견을 배제하는 공정성(impartiality)과 주관적 요소를 최소화하는 객관성(objectivity)이 필요하다.

따라서 본 논문에서는 스팸 전자우편과 전자우편 폭탄을 막는 제품들에 대한 취약성 분석을 자동화할 수 있는 분석 모델을 통하여 분석자에게는 취약성 분석의 공정성과 객관성을 갖게 하고 취약성 분석에 따른 시간과 인적 낭비를 최소화하며, 사용자에게는 신뢰성을 줄 수 있는 새로운 분석 모델을 제안한다.

4. 제안된 취약성 분석 자동화 도구 설계

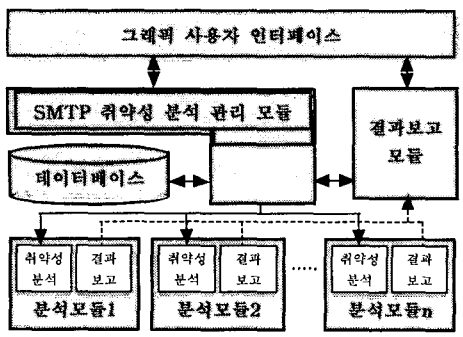
본 논문에서 제안하는 취약성 분석 자동화 도구는 취약성 분석 자동화 모델에 따라 취약성 분석의 효율성과 신뢰성, 객관성을 갖도록 설계됐고 기존의 분석 방식들이 가지고 있는 한계점을 개선하고, 취약성 분석 과정을 자동화함으로써 소요되는 시간과 인적 낭비를 최소화하였으며, 반복적으로 분석이 용이하며 상세한 분석 결과를 통하여 전문 지식 정도에 관계없이 분석이 용이하도록 설계하였다. 제안된 취약성 분석 자동화 도구는 다음과 같은 사항을 만족하도록 설계하였다.

- 스팸 전자우편이나 전자우편 폭탄에 의해 발생할 수 있는 SMTP 서버 관련 취약성을 점검한다.
- 그래픽 사용자 인터페이스(graphic user interface, GUI)를 제공하여 설정 기능을 단순화시켜 사용자 편이성을 제공한다.
- 분석 항목별로 취약성 관련 정보와 함께 통합적이고 상세한 분석 결과를 제공하여 분석의 용이성과 정확성을 제공한다.
- 새로운 SMTP 서버 관련 취약성 항목 추가시 기존 프로그램에 쉽게 결합하도록 하여 확장성 있는 소프트웨어 구조를 갖게 한다.

4.1 취약성 분석 자동화 도구의 구조

취약성 분석 자동화 도구는 제어 기능에 따라 5가지 모듈로 구성된다. 기본 구성 요소로는 그래픽 사용자 인터페이스, 취약성 분석 관리 모듈, 결과보고 모듈, 분석 모듈, 데이터베이스 등으로 구성되어 있다.

(그림 6)은 취약성 분석 도구의 기본 구조를 나타내고 있다. 분석을 위한 기본 환경과 분석 대상을 설정하고, 취약성이 분석되는 동안에 실행 현황의 표시와 분석 결과를 제공하는 그래픽 사용자 인터페이스, 설정된 환경에 따라 분석 대상에 대해 분석 모듈들의 실행과 분석 결과를 데이터베이스에 저장하고 관리하는 SMTP 취약성 분석 관리 모듈, 분석결과를 사용자에게 전달하는 결과보고 모듈, 각 취약성 항목에 따라 취약성을 점검하는 분석 모듈, 기본 환경 정보와 분석 결과를 저장하는 데이터베이스 등으로 구성된다.



(그림 6) 취약성 분석 자동화 도구의 기본 구조

4.2 취약성 분석 자동화 도구의 제어 모듈 기능

가. 그래픽 사용자 인터페이스

그래픽 사용자 인터페이스를 통하여 취약성을 분석하기 위한 대상과 취약성 분석 항목을 지정하게 된다. 그리고 SMTP 취약성 분석 관리 모듈로부터 현재 실행 현황과 분석 결과를 받아서 사용자에게 알린다.

나. 분석 대상 관리 모듈

분석대상 관리 모듈은 분석 대상에 대한 정보 관리와 전달 기능의 두 가지 기능을 갖는데, 추후 반복하여 분석이 용이하도록 분석 대상의 IP 주소를 저장하고 GUI로부터 입력된 분석 대상

정보를 SMTP 취약성 분석 관리 모듈에 보낸다. 취약성 분석 관리 모듈은 분석 대상 정보를 가지고 취약성을 분석하게 된다.

다. 분석 항목 관리 모듈

분석 항목 관리 모듈은 분석대상의 정보, 분석대상 취약성, 그리고 각 취약성에 관련된 세부적인 정보들을 관리한다. 분석 대상에 대한 세부 분석 항목들의 설정이 가능하다. 또한 분석자로부터 설정된 분석 항목의 설정값을 SMTP 취약성 분석 관리 모듈에 전달한다.

라. SMTP 취약성 분석 관리 모듈

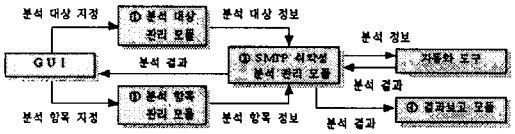
SMTP 취약성 분석 관리 모듈은 분석대상 정보와 분석 항목 정보의 내용에 따라서 취약성을 분석하는데, 설정된 분석 항목별로 각각의 분석 모듈을 실행시키며, 취약성 분석 모듈로부터 분석된 결과를 받아서 데이터베이스에 저장한다. 또한 현재 분석 현황을 GUI를 통하여 사용자에게 알리고, 사용자가 분석의 실행을 중지하고자 할 경우 원하는 임의의 시점에서 중지가 가능하도록 한다.

마. 분석결과 보고 모듈

분석결과 보고 모듈은 분석 모듈로부터 전달받은 취약성 분석 결과를 사용자에게 보여주는 기능을 제공한다. 또한 데이터베이스에 저장된 취약성 정보와 함께 분석 결과를 항목 별로 상세하게 나타내어 사용자에게 분석 결과에 대해 신뢰성을 갖게 하고 취약성 파악을 용이하게 한다.

4.3 취약성 분석 자동화 도구의 기능 흐름

(그림 7)은 사용자가 취약성 분석을 실행하여 분석 결과를 받을 시점까지의 4단계로 구성되는 기능 흐름도이다.



(그림 7) 취약성 분석 자동화 도구의 기능 흐름도

단계 1 : 사용자는 GUI를 통하여 분석 대상 관리 모듈에 분석 대상을 지정하게 되고 분석 대상에 대한 정보는 SMTP 취약성 분석 관리 모듈에 전달된다.

단계 2 : 지정된 분석 대상에 대해서 분석하고자 하는 항목을 분석 항목 관리 모듈에 지정하고 분석 항목 정보는 SMTP 취약성 분석 관리 모듈에 전달된다.

단계 3 : SMTP 취약성 분석 관리 모듈은 분석 대상 정보와 분석 항목 정보를 전달받아 입력된 내용에 따라 분석을 실행시킨다. 분석 결과는 결과보고 모듈에 전달되어 사용자에게 제공된다.

단계 4 : 결과보고 모듈을 통해서 관련 취약성 정보와 함께 분석 결과를 사용자에게 제공한다. 분석 대상 정보와 분석 항목 정보, 분석 결과는 추후 재실행이 용이하도록 데이터베이스에 저장된다.

4.4 취약성 분석 자동화 도구의 분석 항목

분석 모듈은 각각의 분석 모듈에 따라 취약성 분석을 실행하고 분석 결과를 결과보고 모듈에 전달한다. 취약성 분석 항목별로 그 취약성을 분석하는 분석 모듈이 존재하며, 스팸 전자우편과 전자우편 폭탄에 의한 취약성 항목들을 갖는다. 분석 항목은 다음과 같다.

가. 신분 확인

사용자 ID와 패스워드를 통해서 시스템에 접근을 시도하는 사용자의 신분을 식별(identification)하고 인증(authentication)하는지 여부를 분석하는 항목이다.

나. 허용 최대 메일 크기 제한

전자우편 폭탄에 의한 SMTP 서버 취약성을 분석하는 항목으로, SMTP 서버로 허용된 크기 이상의 전자우편이 수신되었을 때 스팸 전자우편 차단 제품에 의한 제한 여부를 분석한다.

다. 첨부 파일 크기 제한

대용량의 파일을 첨부하여 SMTP 서버에 장애를 일으키는 것에 대한 취약성을 분석하는 항목으로 수신된 전자우편의 첨부 파일의 크기가 허용된 크기 이상일 때 제한되는지를 분석한다.

라. 특정 호스트의 전자우편 송수신 개수 제한

전자우편 폭탄에 대한 취약성 분석 항목으로 관리자로부터 설정된 특정 호스트에서 송수신 되는 전자우편이 제한된 개수와 시간이 초과되었을 때 통제되는지를 분석하는 항목이다.

마. 특정 전자우편 주소의 필터링

스패머로 지정된 특정 주소에서 송수신 되는 전자우편의 차단 여부를 분석하는 항목으로 관리자에 의해서 필터링 리스트에 설정된 전자우편 주소로부터 수신되는 전자우편이 필터링 되는지 여부를 분석하게 된다.

바. 중계 제한.

중계 제한 항목은 중계에 의한 취약성을 분석하는 항목으로 중계하고자 하는 전자우편이 수신되었을 때 스팸 전자우편 차단 제품에 의해서 중계가 통제되는지 여부를 분석한다.

5. 결론 및 향후 연구 과제

본 논문에서는 스팸 전자우편과 전자우편 폭탄을 차단하는 제품들의 성능과 잠재된 취약성을 분석할 수 있는 취약성 분석 자동화 도구를 제안하였다.

본 논문에서 제안된 취약성 분석 자동화 도구가 기존의 분석 방식에서 개선된 점은 분석 작업을 자동화하여 인적, 시간적 낭비요소를 줄일 수 있고 새로운 취약성 분석 항목의 추가를 가능하게 하여 확장성과 분석의 다양성을 갖게 했으며, 관련 취약성 정보와 세분화된 분석 결과를 제공하여 취약성 분석이 용이하다는 것이다.

본 연구 결과로 벤더들에게는 제품의 성능 및 취약성 분석시 효율성과 객관성의 이점을 제공하며, 사용자에게는 전자우편 사용의 안전성과 신뢰감을 줄 것으로 기대된다.

향후에는 취약성 분석에서 직접 적용할 수 있도록 취약성 분석 자동화 도구의 개발에 관한 연구가 필요하다고 하겠다.

<참고 문헌>

[1] Reto E. Haeni, "Firewall Penetration Testing", 1998
[2] Tim Bass, Lt. Col. Grenn Watt, "A simple framework for filtering queued SMTP mail(Cyberwar countermeasures)"
[3] Jeam-Goo Kim, Young-cheol Lee, Jae-Kwang Lee, "An Implementation of Vulnerability Evaluation System for Network Security on CC", PDPTA '2000, Vol II, pp1091-1095, June. 2000
[4] W. Richard Stevens, "TCP/IP Illustrated Volum 1", Addison-Wesley, 1997
[5] 조영남, 전문석, "침입차단시스템에서 안전한 메일시스템 설계 및 구현", 한국정보과학회 가을 학술발표논문집(III) Vol. 26, No. 2, 1999
[6] 한국정보보호센터, "정보시스템 침해사고 방지기술 개발에 관한 연구", 1999