전산망 취약점 원격 진단시스템 개발[1)]

변경근*, 심영철*, 김상정, 김우년, 정윤종°, 신 훈, 박정현, 임휘성, 임채호
한국정보보호센터
홍익대학교*

Development of System Vulnerability Scanner Through Networks

Kyungkun Byun*, Youngchoul Shim*, Sangjeong Kim, Woonyon Kim,
Yunjong Jeong°, Jeonghyun Park, Hisung Im, Chaeho Lim
Korea Information Security Agency
Hongik University*

요 약

인터넷 등의 전산망을 통한 정보관련 서비스는 여러 가지 보안 취약점에 노출되어 해커들의 주요 공격 대상이 되고, 특히 WWW 관련 서비스는 불특정 다수를 대상으로 하기 때문에 접근 통제방식으로 어려움이 많고, 최근 많이 사용되는 방화벽이나 기타 보안도구를 이용하여 보안 수준을 높일 수가 없다. 그래서 본 논문에서는 해커들이 공격 가능한 취약점들을 분석하여 해커들의 공격을 사전 방지하고, 올바른 해킹방지 대책를 수립할 수 있는 전산망 취약점 원격 진단시스템 모델을 제시하고, 이에 대한 설계 및 구현내용을 설명한다.

1. 개요

외부의 해커들이 전산망을 통해 정보시스템을 해킹하는 것은 그 시스템이 네트워크와 연결된 부분의 취약점들을 가지고 있기 때문이다. 그러므로 정보시스템이 해킹을 막기위해 가장 우선적으로 필요한 것은 네트워크와 관련된 부분의 취약한 부분들을 막는 일이다[1].

외부와 연결된 통로를 가진 정보시스템의 취약한 네트워크 부분이란 인터넷 등 네트워크 자체의 취약성으로 인한 부분, 인터넷 접속용 서버(Server)나 데몬(Daemon)이 가진 취약부분, 네트워크 응용프로그램이 가진 취약부분, 방화벽시스템이 가진 취약부분, 사용자 계정관련 부분 등 여러 취 약한 부분(Hole)들을 고려할 수 있다. 이러한 취약한 부분들을 점검분석하는 행위를 스캔(Scan)이라고 하며 해외에서는 SATAN 이라는 대표적인 공개 소프트웨어와 ISS사의 ISS Suite가 대표적인 상용제품으로 소개되고 있으며, 해커들의 수법을 응용한 적극적인 스캔을 수행하는 것이 특징이다[2,3].

1. 이 논문은 정보통신부 국책기술과제인 "정보시스템 침해사고 방지기술개발"로 진행되고 있습니다.

이러한 기술은 해킹수법들을 응용하기 때문에 해외에서의 기술도입이 매우 어렵고 미국 등에서는 정보전(Information Warfare)의 일환으로 통제되기도 하므로 국내 자체기술로 개발하여야 한다. 이 기술은 해킹수법을 근간으로하여 실제 국내외 해커들에 대한 대응기술 등으로 활용하여야 하므로 국내 전산망 정보보호 기술력 확보에 매우 중요한 기본적인 기술의 하나가 된다[4,5,6].

본 논문은 이러한 해킹수법 기술을 바탕으로 네트워크를 통해 원격 정보 시스템의 보안취약점 들을 스캔하여 그 결과를 분석 보고하는 시스템 개발을 목표로 WWW서버 취약점 스캔, 방화벽 시스템 취약점 스캔, 인터넷에 연결된 정보시스템 전반적인 취약점을 스캔하는 시스템 구현을 설명한다. 그밖에도 홈페이지를 통해 점검서비스 요청을 받아 점검하는 온라인시큐어닥터 (Online-SecuDr)시스템의 구현과 서비스 현황도 보이고자 한다.

2. 전산망 보안취약점 분석

인터넷 등 전산망의 일반적인 보급은 사람들의 활동영역을 전세계로 확대시켰고, 특히 WWW의 등장으로 인터넷 사용자는 자신들의 홈페이지를 운영하고, 각 기업들은 자사의 홍보와 상품의 홍보를 위하여 홈페이지를 운영하는 등 인터넷의 대중화, 일반화를 촉진시켰다. 그러나 인터넷 WWW 등 전산망을 통한 정보관련 서비스는 여러 가지 보안 취약점에 노출되어 해커들의 주요 공격 대상이 되어, 경제적·사회적·국가적경쟁력 등에 상당한 손실을 가져다 주는 역기능 현상이 커져가고 있다.

특히 WWW 관련 서비스는 불특정 다수를 대상으로 하기 때문에 접근 제어방식으로 안정적인 보안정책을 수립할 수 없으며, 최근 많이 사용되고 방화벽이나 기타 보안도구를 이용하여 보안 수준을 높일 수가 없다. 그러므로, 해커들이 공격 가능한 취약점들을 연구, 분석하여 보안 취약점들을 사전 점검하여 조치를 취함으로써 해커들의 공격을 사전 방지뿐아니라 올바른 해킹방지 대책를 수립할 수 있다.

2.1 방화벽(Firewall)관련 보안취약점

방화벽관련 보안취약점은 네트웍크 관련 취약성, 서비스 공격 관련 취약성, 응용 서비스 관련 취약성의 세가지로 분류(표 1참조)된다.

(표 1) 방화벽 공격방법

방화벽 취약점	해킹방법
네트워크관련 취약성	IP spoofing, 소스 포팅, 소스 라우팅 등
서비스공격관련 취약성	RPC/DNS 공격, Syslog Flooding, UDP bomb 등
응용서비스관련 취약점	Sendmail, Telnet, NFS, FTP, r*-command 등

2.2 WWW관련 보안 취약점

웹서버 보안 취약점은 웹서버 구현상의 취약점, CGI 관련 취약점, 그리고 웹서버 구성상의 취약점으로 구분할 수 있다. 웹서버 구현상의 취약점은 공개용 웹서버나 상용 웹서버의 구현상의 문제로 인하여 보안취약점이 존재하는 경우로 Windows NT/95 Website 서버, NCSA 웹서버, MS ISS 웹서버 등에 존재하고, CGI 관련 취약점은 외부의 사용자에게 호스트의 정보를 보여주는 취약점과 사용자 입력 폼을

통해서 임의의 명령을 수행할 수 있는 취약점이 존재하는 경우로 webdist.cgi, php.cgi, guestbook.cgi, nph-test-cgi 등에 존재한다. 그리고, 웹서버 구성상의 취약점은 웹서버 구성의 잘못으로 파일 접근 권한 획득, 디렉토리 내용 리스팅, 심볼릭 링크, Server Side Includes, 웹서버를 루트권한로 운영 등의 취약점을 유발할 수 있다.

2.3 인터넷관련 보안취약점

인터넷관련 보안 취약점은 NFS, Anonymous FTP, Sendmail, RPC, 서비스공격(표 2 참조)등에 의해 보안취약점이 존재할 수 있다.

(표 2) 인터넷 취약점

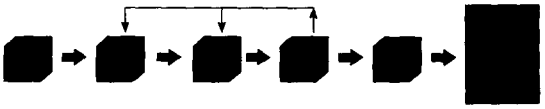
NFS	Export Checks, Portmapper export, Sun FileHandle Guess UID bug, mknod bug, write check, CD bug, access files 등
Anonymous FTP	mkdir, CD bug, site exec, writability of all files 등
SendMail	aliases, Wizard backdoor, debug mode, remote execution, identid bug, SMTP banner, syslog buffer overflow 등
RPC	rexd, wall, selection_svc, admind, boot param, X.25, SNMP, NIS, full Domain, rstat, RPC Pcnfsd, RPC/NIS updata, rpc.statd 등
Brute Force Attacks	netware FIP, cisco, telnet banner, systat/netstat 등
Denial of Service	Finger Bomb, UDP Bomb, echo service, microsoft dot dot bug ICMP redirect, nuke, DNA, open/close ports repetitively 등

3. 관련 소프트웨어 분석

위에서 논의한바와 같이 현재 사용중인 시스템에 다양한 취약성이 존재하고 있다. 이러한 취약성들을 일일이 수작업으로 점검을 한다는 것은 많은 시간과 노력을 요구한다. 따라서 이러한 노력을 줄이기 위해 다양한 시스템 보안 검검 스캐너들이 개발되어 사용되고 있다. 이들의 대표적인 제품을 보면 Dan Farmer 와 Wietse Venema가 만든 SATAN(System Adminstor Tool for Analyzing Networks), ISS에서 남들어 판매하고 있는 ISS Suite, 그리고 Pingware등이 존재한다. 이러한 제품들의 구성과 특성을 파악함으로 우리가 만들고자하는 네트워크 침입 취약성 점검시스템 개발에 참고하고자 한다.

3.1 SATAN

SATAN 프로그램의 경우 특징을 보면 네트워크를 통하여 원격시스템의 보안 정도를 조사하는 프로그램으로 이 시스템의 구성 형태를 살펴보면 사용자와의 인터페이스 부분은 기존의 web browser를 이용하고 있으며, 몇가지의 엔진으로 시스템을 구성하고 있다. [그림 1]은 SATAN의 구조를 나타내고있다.



(그림 1) SATAN의 전체적 구조

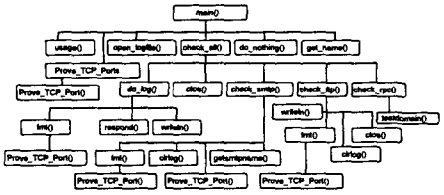
SATAN의 장단점은 표2에 설명된다.

(표 3) SATAN의 장단점

장 점	단 점
o 사용자 인터페이스가 편리하다. o 확장성이 좋다. o 결과 보고서에 취약점을 보완하는 방법 제시	o 기본 소프트웨어 환경이 필요하다. o 해커에게 악용될 소지가 있다. o 실행속도의 최적화는 크게 고려치 않음 o 설치가 복잡하다. o 많은 자원이 필요하다.(20 MB HD, 32MB MM)

3.2 ISS SAFEsuite

ISS는 공개용 ISS를 기반으로 상업용으로 개발된 것으로 먼저 공개용 ISS의 기능을 살펴보면 원격 호스트의 포트 스캔(Port Scan)을 기본적으로 하는 점검도구로 [그림 2]와 같은 구조로 구성이 되었으며, 각 모듈의 함수를 추가할 경우 더많은 수의 보안 취약점을 검점할 수 있다.



(그림 2) ISS SAFEsuit

이는 일반 사용자도 사용할수 있기 때문에 외부의 호스트 해킹의 준비작업으로 사용될 소지도 있다. 사용자 인터페이스가 스러 좋지 않아 좋은 평가는 받지 못하나 한번에 넓은 범위의 호스트들을 한꺼번에 빠른 속도로 스캔할수있다는 장점을 가지고 있다. ISS SAFEsuite는 상업용으로 만들어진 제품으로 네트워크의 보안상의 취약점을 찾아내어 그 취약점을 복구하는 방법을 제공하며, 이의 구성 요소를 보면 Web Scanner, Firewall Scanner, Intranet Scanner, System Security로 구성이 되어 있다. 최근의 자료를 보면 네트워크 보안의 허점중 절반이상이 방화벽 내부의 네트워크에서 발생하는 것으로 나타나고 있다.

[표 4]는 보안 스캐너 도구들의 주요 점검 항목에 대한 비교 분석을 나타낸다.

(표 4) 보안스캐너 도구 비교분석

주요 점검항목	PINGWARE	ISS	NETProbe	Satan
Password checking	●			
Rsh + in hosts.equiv, Rexe	●	●	●	●
YPUPDATED allows execution of commands with root privileges	●			
Rwho daemon active	●			
Spray daemon active	●			
Rstat/ Selection_svc daemon active	●	●		
Wall/Rusers/Bootparam daemon active	●	●		
Improper access control on X-servers	●	●	●	●
Tftp vulnerable	●	●	●	●
Anonymous ftp directory writable	●	●	●	●
Ftp chroot bug	●	●	●	
Real password file in FTP directory	●		●	
Http server vulnerable to stack overflow	●	●	●	
Old sendmail versions being used	●	●	●	●
Sendmail DEBUG and WIZ options	●	●	●	●
PIPE command allowed	●	●		
Easily guessable root password	●		●	
Default UNIX accounts	●	●	●	
Login accepts -f option	●	●	●	
NFS directories world readable/writable	●	●	●	●
Detects the user of mknod and uid	●	●		
Easily guessable NIS domain name	●	●	●	●
Fingered hole	●	●	●	
Telnet and SMTP banners retrieved	●	●		
Common hacking backdoor active	●		●	
Selection_svc bug	●	●		

4. 시스템 모델 및 설계

인터넷과 인트라넷을 통한 침입은 방화벽의 취약점이나 웹서버의 취약점을 통하여 이루어진다. 정보 시스템은 인터넷과 인트라넷에 연결되어 있으므로 이들이 지닌 취약점에 의하여 침해당할 수 있다. 정보 시스템 취약점 점검 시스템은 웹서버, 방화벽, 그리고 인트라넷에 대한 취약점을 점검한다. 이들의 취약점을 점검하는 방법에 따라서 로컬 네트워크인 인트라넷에서 수행되는 점검과 인터넷을 통하여 외부 인트라넷에 접근하여 점검하는 방식이 있다.

본 절에서는 웹서버 취약점 점검, 방화벽 취약점 점검, 인트라넷 취약점 점검 모듈로 이루어지는 정보 시스템 취약점 점검 시스템의 시스템 모델과 구조에 대하여 설명하고, 각각의 모듈의 점검 절차에 대하여 설명한다. 그리고, 정보 시스템 취약점 점검 시스템은 인트라넷 내부에서 뿐만 아니라 인터넷을 통하여 원격 네트워크에 접근하여 점검할 수 있다. 이러한 시스템인 온라인 시큐어 닥터의 구조와 동작 모

델에 대하여 설명한다.

4.1 시스템 모델

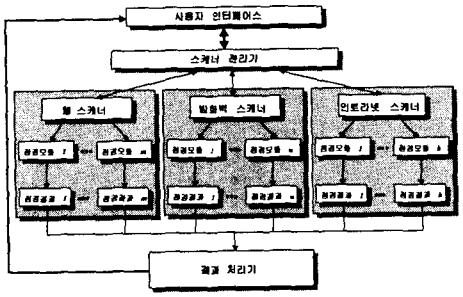
정보 시스템 취약점 점검 시스템은 인터넷과 인트라넷을 통하여 사용자의 점검 사항에 대하여 취약점을 점검하고, 점검의 최종결과를 사용자에게 전달한다. [그림 3]은 정보 시스템 취약점 점검 시스템의 구조로서, 사용자 인터페이스, 스캐너 관리기, 스캐너, 그리고 결과 처리기의 4가지 부분으로 구성된다.

사용자 인터페이스는 점검 항목, 점검 호스트등의 점검을 위한 자료로서 사용되는 데이터를 받아들여 스캐너 관리기에게 전달하며, 수행중인 점검 사항이나 중간 결과를 사용자에게 표시한다. 그리고, 사용자의 점검 중지 이벤트를 받아들여 관리자로 전달한다.

스캐너 관리기는 사용자의 선택사항에 따라서 적절한 취약점 점검 스캐너를 선택하고, 사용자가 선택한 데이터를 바탕으로 필요한 점검 모듈들을 선택한다. 그리고, 시스템의 현재 진행 사항들을 수집하여 사용자에게 전달하며, 사용자의 중지 이벤트에 대해서 적절한 점검 모듈이나 전체 점검을 중지 시키는 역할을 한다.

취약점 점검 스캐너는 점검 항목에 따라서 인트라넷 취약점을 점검하는 모듈, 웹서버 취약점을 점검하는 모듈, 그리고 방화벽 취약점을 점검하는 모듈로 구성된다. 각각의 스캐너는 점검하고자 하는 항목별로 각각의 점검 모듈을 구성하고 있으며, 스캐너 관리기에 의해 하나의 프로세서가 생성된다. 각각의 점검 모듈은 점검을 위해서 적절한 메시지를 생성하여 네트웍을 통하여 전달하게 되고, 돌아오는 결과값을 분석하여 결과를 생성한다.

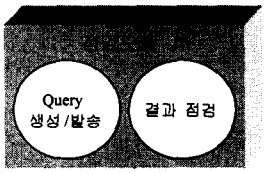
결과 처리기는 각각의 점검 모듈에 의해서 생성된 각각의 결과를 수집하여, 요약 보고서와 최종 점검 보고서를 작성한다. 보고서의 내용은 점검 대상 시스템의 이름, 도메인 이름, IP 주소, 점검 시간, 취약점 목록, 취약점에 대한 관련 권고 문서 정보등이 포함되며, 보고서는 사용자 인터페이스에 의하여 표시되거나, 인터넷을 통한 취약점 점검인 경우는 점검 요청자에게 전달하게 된다.



(그림 3) 취약점 점검 시스템 구조

세가지 스캐너는 유사한 동작 모델을 가진다. 세가지 모두 점검을 위한 질의를 생성하고, 질의를 점검을 원하는 호스트에 전달하여, 돌아오는 결과값을 분석하는 과정을 거친다. [그림 4(a)]는 취약점 점검 모듈로서 각각의 모듈은 질의 생성기와 결과 점검기가 있어서 질의에 대한 응답을 분석하는 부분으로 되어 있다. [그림 4(b)]는 스캐너의 점검 모듈의 동작 절차이다. 스캐너 점검 모듈들은 점검하기 위한 질

의를 생성하고, 이 질의를 점검 대상 호스트에 보낸다. 점검 대상 호스트로부터 응답이 있을때까지 기다린다. 응답이 오면, 이 응답을 분석하여 점검 대상 호스트의 상태를 결정한다.

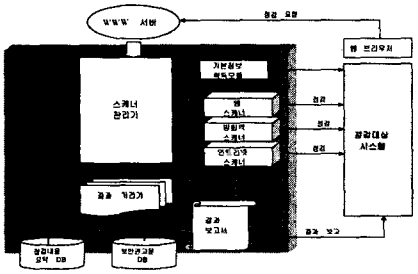



```
int checking_module(char *host)
{
        make Query message;
        write Query message to network port(80, 8080);
        waite for replying message;
        read replying message;
        analyze replying message;
        return result of checing;
}
```

(그림 4) (a) 점검 모듈 구조, (b) 취약점 점검 모듈 점검 절차

4.2 인터넷을 통한 정보 시스템 보안 취약점 점검

인터넷을 통한 정보 시스템 보안 취약점 점검 시스템은 온라인 시큐어 닥터라고 한다. 온라인 시큐어 닥터는 인터넷을 통하여 원격지 네트워크에 접근해서 보안 취약성을 점검하는 시스템이다. 점검 부분은 웹서버 보안 스캐너, 방화벽 보안 스캐너, 인트라넷 보안 스캐너를 포함한다. [그림 5]는 온라인 시큐어 닥터의 구조를 나타낸 것이다. 웹 브라우저를 통하여 점검 신청을 하면, 점검을 위한 정보가 온라인 시큐어 닥터가 설치된 웹 서버로 전달된다. 웹서버는 CGI 처리 모듈을 통하여 전달된 정보를 인증 과정을 통하여 값이 참이 될 때만 실제 점검 모듈을 실행시킨다. 온라인 시큐어 닥터의 관리기는 이 정보를 이용하여 점검을 위한 스캐너들과 스캐너의 점검 모듈들을 선택한다. 점검 모듈은 인터넷을 통하여 점검 대상 호스트에 접속하여 호스트를 점검하고, 점검 결과를 생성한다. 생성된 점검 결과를 이용하여 결과 처리기는 점검 내용 요약 DB와 보안 권고문 DB를 이용하여 점검 결과와 함께 권고 사항을 함께 엮은 보고서를 작성한다. 작성된 보고서는 네트웍을 통하여 점검을 요청했던 요청자에게 전자메일을 이용하여 전달된다.



(그림 5) 온라인 시큐어 닥터 구조

온라인 시큐어 닥터에서 중요한 것은 웹서버의 CGI 처리 모듈과 사용자 인증 모듈이다. CGI 처리 모듈은 서버로 전달된 정보의 인증과정을 통하여 인증된 정보만을 스캐너 관리기를 통하여 실제 점검을 수행하도록 한다. 사용자 인증 모듈은 CGI 처리 모듈로부터 받은 정보 중에서 IP 주소와 기계 이름을

이용하여 생성한 IP 주소와 CGI 환경 변수를 이용하여 구한 현재 접속중인 기계의 원격 IP주소등 이 세가지 IP 주소를 비교하여 참인 경우만이 올바른 점검 대상 기계인 경우이다. 따라서, 사용자 인증 모듈을 사용함으로써 다른 기계를 해킹할 목적으로 특정 기계를 대상으로 삼고 온라인 시큐어 닥터를 악용하는 것을 막아준다. 다음 [그림 6]은 사용자 인증 모듈의 처리 과정 이다.

```
// 입력 매개 변수, 호스트 IP 주소, 호스트 이름
// CGI 환경 변수를 이용하여 구한 현재 접속중인 기계의 원격 IP
get host_IP from hostname;
        :
if(host_IP == 사용자 IP == CGI 처리 모듈에서 구한 IP)
        return TRUE;
else
        return FALSE;
```

(그림 6) 사용자 인증 모듈의 실행 과정

5. 구현 및 시험

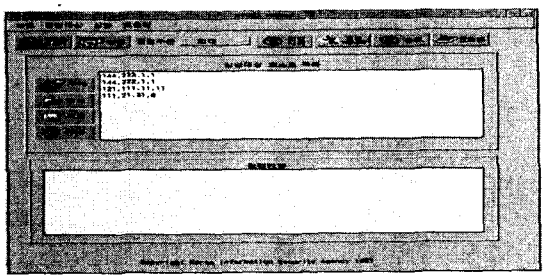
정보시스템 취약점 원격 진단분석시스템은 WWW 서버 취약점 스캔, 방화벽시스템 취약점 스캔, 정보시스템의 전반적인 스캔을 목적으로 한 인터넷 스캔 등 크게 3개 모듈의 스캔 부분으로 나누어지고 이를 통합한 인터페이스와 결과 분석 및 보고모듈로 나누어져 구현하였다. WWW 서버 취약점 스캔, 방화벽 시스템 취약점 스캔, 정보시스템의 전반적인 스캔을 목적으로 한 인터넷 스캔은 Sun의 Solaris 2.5.1 운영체제에서 WWW인터페이스로 개발되였고, 특히 정보시스템의 전반적인 스캔을 목적으로 한 인터넷 스캔모듈은 현재 일반사용자를 대상으로 점검서비스를 수행중에 있다.

5.1 WWW 서버/방화벽 취약점 스캐너

방화벽 취약점 스캐너에서는 IP Source Routing, RIP(Routing Information Protocol) attack, Sequence number Prediction, TCP Port Stealth Scanning, echo, chargen etc. attack, Syslog Flood, Source Porting에 대한 취약점 검검하고, WWW서버 취약점 점검스캐너에서는 현재 점검 할 수 있는 항목은 test-cgi, nph-test-cgi, campus.cgi, websendmail, webgais, aglimpse, NCSA1.4/1.5a, Apache1.0.2/1.1.1, phf, php-password, finger, php-overflow, count.cgi, Apache/1.2b8, SGI's /cgi-bin/handler, guestbook.cgi, wrap, webdist, jj, Apache/1.1.3, view-source.cgi, Stronghold v1.3.2 등이고 앞으로 더 추가할 계획이다.

5.2 사용자 인터페이스

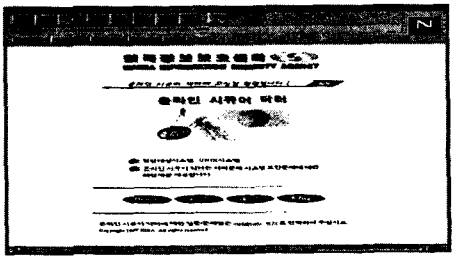
정보시스템 취약점 원격 진단분석시스템의 사용자 인터페이스([그림 7]참조)는 WWW, 방화벽 및 인트라넷 스캐너를 수행할 수 있도록 구성되어 있고, 점검현황 표시화면, 점검환경 설정 화면, 점검 수준 설정 화면, 점검내용 편집 화면 등으로 구성되어 있다.



(그림 7) 사용자 인터페이스 화면

5.3 인터넷 스캐너

정보시스템의 전반적인 스캔을 목적으로 한 인터넷 스캐너는 현재 일반 사용자를 대상으로 네트워크 점검 서비스를 수행하고 있는데, 주요기능으로는 온라인 보안취약점 점검 기능, 서비스에 대한 새소식 제공기능, 서비스에 대한 요구사항 제안기능, 이용법, 의문사항 등을 제공하는 FAQ기능을 가지고 있다([그림 8]참조). 주요 점검 항목은 NFS, Anonymous FTP, SendMail, RPC, Brute Force Attacks, Denial ofService관련 보안취약점 40여가지를 점검하고 있고, '97년 말까지 60여가지를 개발할 예정이다. 또한 '97년 10월까지 55개기관에 99회서비스를 제공했고, 총 294가지의 보안취약점이 점검되었다.



(그림 8) 온라인 시큐어닥터 초기 화면

6. 결론 및 향후방향

본 논문을 통하여 정보시스템이 인터넷 등 전산망과 연결되어 생길 수 있는 취약점들을 분석하여 보았고, 이러한 취약점들을 스캔하여 이를 사전에 예방하려는 소프트웨어들에 대하여 살펴보았으며 이를 토대로 해킹 수법들을 응용한 스캔 소프트웨어에 대한 모델을 보이고 설계, 구현하였다. 이 소프트웨어는 WWW 서버 취약점 스캔, 방화벽시스템 취약점 스캔, 정보시스템의 전반적인 스캔을 목적으로 한 인터넷 스캔 등 크게 3개 모듈의 스캔 부분으로 나누어지고 이를 통합한 인터페이스와 결과 분석 및 보고 모듈로 나누어져 구현하였다.

이는 해외 주요 상용 스캐너를 목표로 개발하였으나 독자적인 해킹 수법 시험 분석을 통하여 개발되어 국내 관련 기술력 확보에 큰 의의가 있으며 단순한 해킹대응 기술력확보 차원이 아닌 시스템의 하나로서 부가가치적 제품화도 개대할 수 있는 가능성을 확보한 것도 또하나의 의의라고 볼 수 있다. 향후 기존의 해외 상용제품의 기능을 크게 앞지른 시스템 개발을 추진하고자 하며 보다 안정성있는 시스템 통합과 상용화를 위한 기술이전을 꾀하고자 한다.

참고문헌

[1] 한국정보보호센터, 정보시스템 해킹 현황 및 대응, 1996. 11

[2] 한국정보보호센터, 정보보호현황, 1996. 10

[3] KUS, PLUS, "인터넷 침입 수법과 대응 방안", NETSEC-KR96 특강 자료집, 1996

[4] 임채호 외, 관리자를 위한 인터네트 보안지침서 Version 1.4, 시스템공학연구소, 1995.

[5] 이재우 외, 정보화 역기능 현황 및 분석, 한국전산원, 1995.

[6] 임채호, "해킹 수법 현황 및 방지 대책", '96 정보보호심포지움 1996.

[7] RAND, "Emerging Challenge: Security and Safety in Cyberspace", IEEE Technology and Society Magazine, Vol.14 No.4., 1996.

[8] Marcus J. Ranum,"A Taxonomy of Internet Attacks : What You Can Expect," IWI, 1995.

[9] Simson Garfinkel and Gene Spafford, Practical Internet and UNIX Security, O'Reilly & Association, 1996.

[10] D. Farmer and E. Spafford, "The COPS Security Checker System," USENIX Conference Proceedings, Anaheim, CA, 1990.

[11] David R. Safford, Douglas Lee Schales, and David K. Hess, "The TAMU security packages: An ongoing response to internet intruders in an academic environment," In dward Dehart, editor, Proceedings of the Security IV Conference, pp. 91-118, Berkeley, CA, USENIX, 1993.

[12] D. V. Klein, "Foiling the Cracker: A Survey of, and Improvements to, Password Security", EKKUUG Summer 90, pp.147-154, London, July 1990,

[13] Gene H. Kim and Eugene H. Spafford," Experiences with tripwire: Using integrity checkers for intrusion detection," In Systems Administration, Networking and Security Conference III, Usenix, April 1994.

[14] Hans Husman ,"Introduction to Denial of Service", Feb 9, 1997

[15] ftp://ftp.win.tue.nl/pub/security/satan-1.0.tar.Z

[16] ftp://ftp.iss.net/pub/iss/

[17] ftp://ftp.cert-kr.or.kr/pub/KUS

[18] http://www.iss.net/prod/

[19] ftp://sunsite.docic.ac.uk/computing/Systems/sun/sunflash/1994/1000-1099/

[20] http://cs.swu.ac.kr

[21] CERT-Advisory Series, CERT.

[22] http://8lgm.org, 8lgm Security Advisories.