NSAT 구조 분석 및 보완 : 다양한 플랫폼에의 적용

윤희영*,곽인섭**, 강홍식***
*인제대학교 전산학과
**인제대학교 컴퓨터공학과
e-mail:*shineyhy@cs.inje.ac.kr **kinsub98@cs.inje.ac.kr,
***hskang@nice.inje.ac.kr

Structure Analysis & Supplement on NSAT : The Application of a Variety of Platforms

Hee-young Yoon*, In-Seub Kwak**, Heung-seek Kang***
*Dept of Information and Computer Engineering, Inje University
**Dept of Computer Engineering, Dae-sung University

요 약

오늘날 각종 스캐너와 같은 취약점 분석 도구들의 보급 확대로 인해 정보시설, 개인 호스트들의 침입 사례가 급증하고 있는 실정이다. 더욱이, 스캔 공격 형태 또한 나날이 그 기법이 지능화되고 있어 기존의 시스템으로는 탐지와 대응에 어려움이 가중되고 있다. 따라서 본 논문에서는 보안 도구에 사용되고 있는 스캐닝 도구 NSAT을 제시한다. NSAT의 구조를 통해 스캐닝 기술을 분석하고, 이에 기능을 보완하여 다양한 플랫폼에의 적용 방안을 제안한다..

1. 서론

지난 몇 년간 수많은 free, open source security tool이 발전되어 왔다. 이러한 툴 에서는 몇 가지 기법으로 침입을 탐지하거나 취약점을 보안하는데 이중에서 스캐닝 기법을 소개하겠다.

과거 스캐닝은 단지 침입의 한 방법으로 여겨졌으나, 최근에는 스캐닝을 통한 취약점을 분석하여 더 나은 보안을 유지하고 있다. 이러한 스캐닝 툴 에는 sscan, mscan, nmap, cops, NSAT 등이 있고, 이중에서 현재 많은 발전 가능성과 70% 이상의 점유율을 가진 스캐닝 툴 이 NSAT (Network Security Analysis Tool)이다.

이에 본 논문은 다음과 같은 구성으로 이루어진다. 스캐너의 일반적 분류에 따른 분석 및 차세대 플랫폼 형식으로 크로스 플랫폼에 대한 소개를 2장에서 하고, 3장에서는 NSAT의 구조에 따른 연구 및 취약점을 설명한다. 4장에서는 취약점을 보완하는 한 예로 다양한 플랫폼의 적용을 제시하고, 5장에서는 향후 발전 가능성 및 연구 과제를 설명하고 끝을 맺는다.

2.관련 연구

2.1 스캐너의 분류 및 기법들

1) Host scanners

host scanner는 문제의 탐지를 위해 로컬 시스템 에서 실행하는 스캐너이다.

(EX : cops, tiger, check. pl)

2) Network scanners

network scnner는 원격에서도 스캔이 가능하여 다른 시스템의 스캔을 통해 열려 있는 서비스를 찾을

수 있고 이를 이용하여 공격을 하거나, 방화벽 역할로도 사용 할 수 있는 유용한 스캐너이다.
(EX: strobe, nmap, Network Superscanner, Portsca -nner, Queso, spidermap)

3) Intrusion Scanners
Intrusion scnners는 Network scnners의 기능에 취약점 분석까지 이루어지는 스캐너이다. 일반적으로 특정 network scanner를 보완하여 만들어진다.
(EX : nessus, sara, saint)

2.2 wxwindows의 개요

NSAT의 향후 보완을 위해 wxWindows의 사용을 제시한다.

• wxWindows 는 아주 간단하고 손쉽게 크로스 플랫폼을 지원하는 프로그램을 만들기 위한 무료인 C++ 프레임워크로 현재 Windows 3.1/95/98/NT, Unix, Mac 등을 지원하며 다른 플랫폼도 지원할 예정이다.

• wxWindows은 최소한의 소스를 수정해서 다른 플랫폼에 쉽게 이식 될 수 있도록 하기 위한 C++ 라이브러리 집합이이며 GUI를 다루기 위한API(App -lication Programming Interface)뿐만 아니라 파일을 복사하거나 삭제하는 등의 운영체제의 서비스를 사용 할 수도 있도록 해준다.

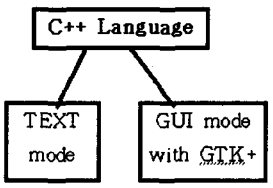
• 사용자에 의해서 재사용이 가능한 수많은 내장 함수들을 가지고 있기 때문에 프로그래머의 코딩을 크게 줄여줄 수가 있다. 문자열이나 연결 리스트, 해쉬 테이블 등과 같은 기본적인 데이터 구조도 역시 완벽하게 지원한다.

• 대상 플랫폼이 지원하는 컨트롤이나, 대화상자 등을 사용하며 다른 플랫폼에서는 wxWindows가 그 플랫폼에 맞는 컨트롤을 생성하여 사용한다. 예를 들어서, win32플랫폼에서는 리스트 컨트롤이 사용되지만, GTK에서는 다른 것과 비슷한 기능을 하는 일반적인 리스트 컨트롤이 사용된다.

3. NSAT의 구조 분석

3.1 NSAT의 개발 환경

환경: Console (Text Based), X11 Applications
License: GNU General Public License (GPL)
기본언어: English
운영체제: BSD, Linux, SunOS/Solaris (POSIX계열)
Programming Language: C++, GTK



[그림1] NSAT의 기본 구조

[그림1] 에서와 같이 NSAT은 text 환경에서만 사용 가능한 것이 아니라, GTK로 이루어진 GUI환경에서도 실행 가능하다.

3.2 특징

현재 가장 많이 사용되고 있는 Network scanner가 NMAP이다. 그러나 NSAT은 NMAP과 비교할 때 여러 가지 장점이 있다.

NSAT은 원격 네트워크로 50개 이상의 각종 서비스를 탐지하고 버전 및 보안상의 문제점을 확인한다. 또한 다른 Scanner와의 차이점은 빠른 시간 내에 스캔하고 어떤 서비스가 스캔되었는지 언제든지 확인 할 수 있도록 로그 파일을 남기는 것이다.

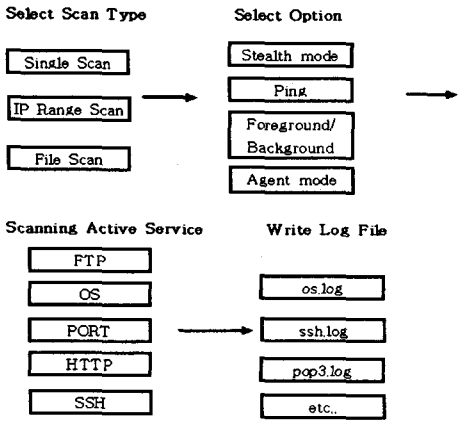
3.3 NSAT의 주요 기능 및 서비스

◎기능
-stealth mode, ping에 따른 스캔 on/off, virtual host scan, background에서 실행 가능,etc.

◎스캔 가능한 서비스
-FTP, OS, PORT, HTTP, POP2, POP3, SSH, SNMP, FINGER SMTP, XWIN, IMAP, etc ..

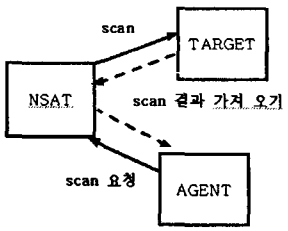
3.4 실행 과정 및 실행 창

다음 [그림 2]는 스캔 타입을 선택해서 스캔된 서비스를 로그 파일에 남기기까지의 과정이다.

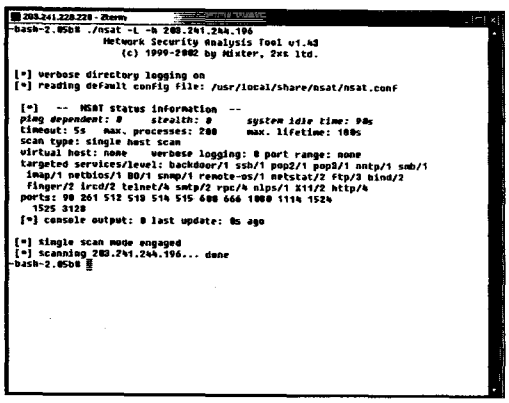


[그림2] scanning 과정

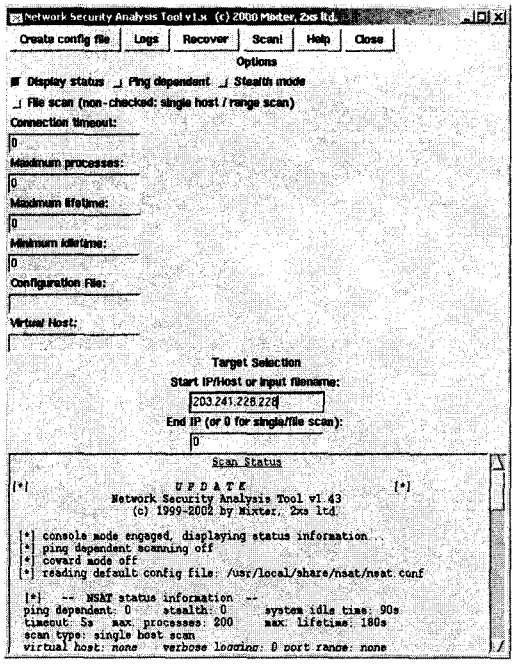
위와 같은 과정으로 NSAT은 실행 되며 이 중에서 Agent mode 구조는 아래 [그림3]과 같다



[그림3] Agent mode 구조



[그림4] 실제 text 상에서의 실행 창



[그림5] 실제 GUI환경에서의 실행 창

4. 취약점 보완

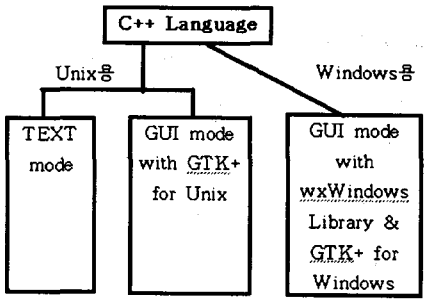
NSAT은 차기 Network scanner임에도 불구하고 몇 가지 해결해야할 문제들이 있다. NSAT은 GUI환경이 미흡하고, log파일의 기록도 단순하다. 그 중에서 주요 취약점이 POSIX 기반에서만 실행된다는 것이다.

현재 많은 스캔 툴 이 단 기종의 스캔만 가능하다는 문제점을 가지고 있고 NSAT도 예외는 아니다. 그러나 NSAT은 C++과 GTK+기반의 툴 이라는 점에서 발전 가능성이 있다.

NSAT의 취약점을 보완하기 위한 방안으로 wx-Windows 라이브러리 사용을 제안한다

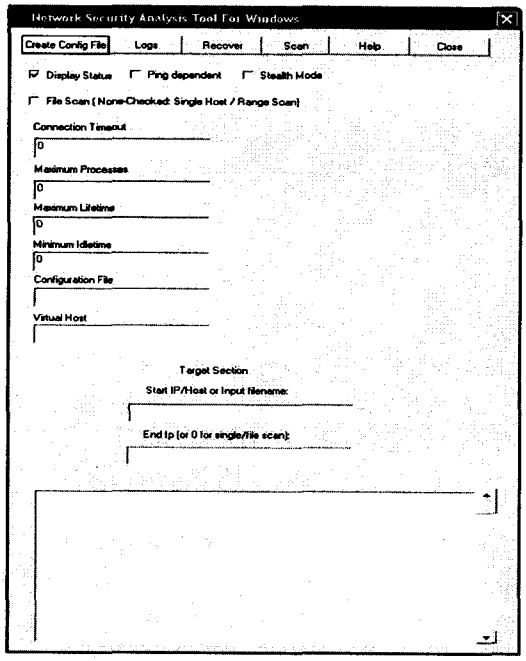
wxWindows라이브러리를 이용할 경우 C++을 기반으로 windows용 gtk+를 이용하여 크로스 플랫폼을 지원하는 프로그램이 가능하다.

현재 NSAT은 C++기반의 Unix를 위한 text mode 모듈과 GUI mode 모듈로 구성되어 있다. 이에 wxWindows 라이브러리를 이용한 Windows용 GUI 모듈을 추가하여 새로운 형태의 툴 을 설계하였다. 아래 [그림6]은 추가 보완된 모듈 형태이다.



[그림6] wxWindows를 이용한 모듈의 구조 설계

아래는 간단히 wxWindows를 이용하여 Windows용 GUI를 구현한 것이다



[그림7] Windows용 GUI 창

5. 향후 NSAT의 활용 방안

앞서 말했듯이 NSAT은 NMAP과 비교하여도 손색이 없는 프로그램이다. 현재 NMAP은 NESSUS라는 Intrusion scanner의 핵심 기반으로 이용되고 있다. 이처럼 NSAT 또한 취약점 스캔 도구로써 충분히 활용 가치가 있다고 본다. 앞서 제시한 툴은 단순히 Windows 플랫폼에의 적용의 한 예로 보였으나, NSAT은 다양한 플랫폼에의 적용 시도도 가능하다. 이에 더 많은 스캔 가능한 서비스를 추가한다면 현재 Intrusion scanner의 최강인 NESSUS를 능가하는 스캔 도구가 될 수 있을 것이다.

참고문헌

[1] Security PLUS for Unix / PLUS 저
영진.com , 2000

[2] Beginning GTK+ / GNOME programming / Peter Wrigt
Brimingham : Wrox Press , 2000.

[3] (초보자를 위한)리눅스 GTK+ 프로그래밍 : 21일 완성 / Donna Martin...[등저] ; 김진구 ; 윤상필 ; 이충환 공역

[4] (GTK+를 이용한)X 윈도우 프로그래밍 / Havoc Pennington ; 장성재

[5] http://www.badnom.com/

[6] http://www.certcc.or.kr/

[7] http://www.gtk.org/

[8] http://www.nessus.org/

[9] http://sourceforge.net/projects/nsat