3 취약성 점검 및 Scan 공격

실험 영역	취약성 점검 및 scan 공격
실험 제목	네트워크 취약점 스캔 공격
실험 요약	네트워크 스캔을 이용하여 시스템의 취약성을 점검한다.

3.1 이론

네트워크 취약점 스캔 공격은 원격지에서 다수의 시스템에 대해 시스템의 자체 버그, 시스템 구성상의 문제점 등 해킹 가능한 시스템의 보안 취약점을 알아내고자 하는 공격이며 가장 빈번하게 나타나는 공격이다.

네트워크 스캔 공격은 이미 알려진 다수의 보안 취약점을 스캐닝하는 일반적인 네트워크 스캔 공격, 특정한 보안 취약점에 대해서만 스캐닝하는 특정 취약점 스캔 공격, 스캐닝 사실을 숨기기 위한 스텔스(stealth) 스캔 공격, 네트워크 구조 스캔 공격 등이 있다.

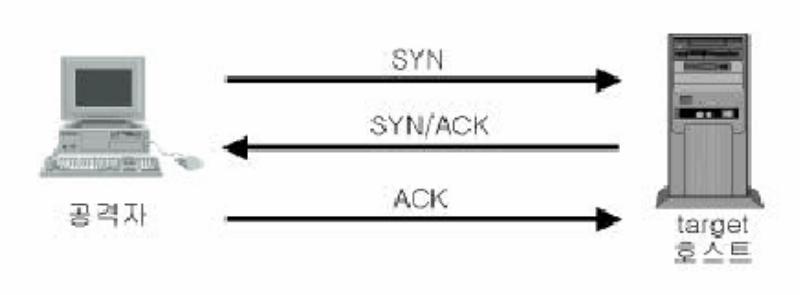
- o 다중 취약점 스캔 공격 : SAINT, sscan2k, vetescan, mscan 등
- o 특정 취약점 스캔 공격 : cgiscan, winscan, rpcscan 등
- o 은닉 스캔 도구 : nmap, stealthscan 등
- o 네트워크 구조 스캔도구 : firewalk, nmap 등

본 장에서는 스캔 공격의 가장 단순한 형태인 포트 스캔의 원리에 대하여 설명하고 스캔 공격 또는 취약성 분석 도구로 일반적으로 많이 사용되는 PC 용 도구와 Linux 용 도구를 소개한다.

3.1.1 포트 스캔

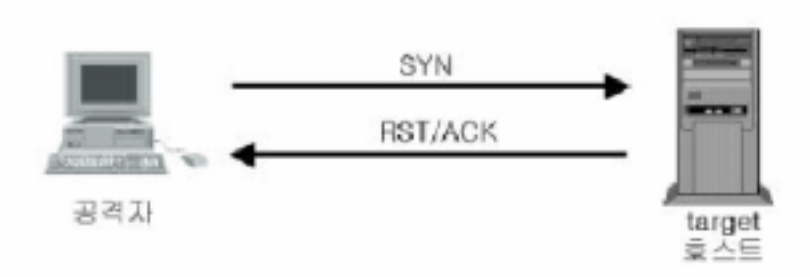
공격할 타켓 네트워크 내에서 실행되고 있는 네트워크 서비스를 식별하기 위한 효과적인 방법이 포트 스캔(port scan)이다. 포트 스캔에서 가장 간단하면서 가장 많이 사용되는 표준 TCP 접속 포트 스캔(standard TCP connection port scan)을 소개한다.

표준 TCP 접속 포트 스캔은 TCP/ IP 3- way handshake 연결을 확립한다. Target 호스트의 해당 포트가 열려 있는 경우는 다음과 같은 패킷이 전송된다.



① target 호스트로 연결을 요청하는 SYN 패킷을 보낸다.
② target 호스트의 포트가 열려 있는 경우 t arg et 호스트에서 연결 요청을 받아들이는 SYN/ACK 패킷을 보낸다.
③ ACK 패킷을 보냄으로 3 - way h andsh ake를 확립한다.

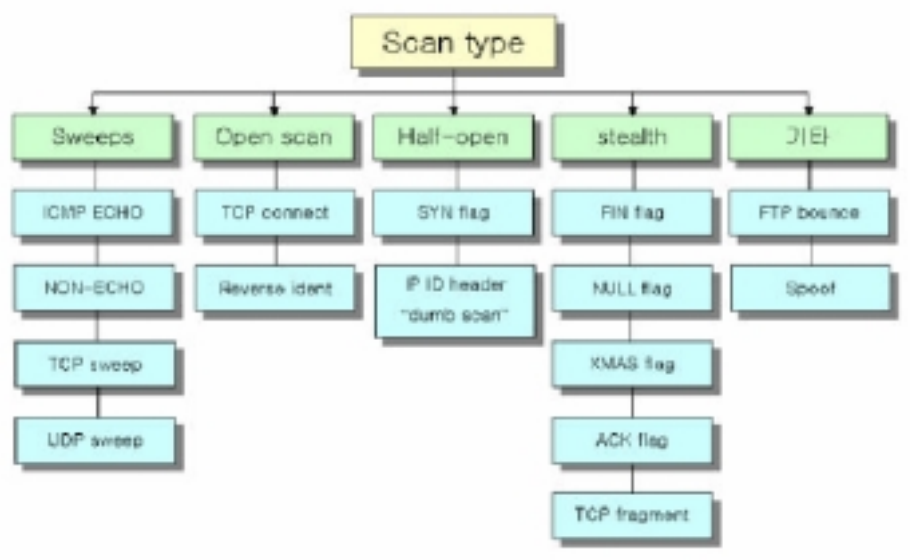
Target 호스트의 해당 포트가 닫혀 있는 경우에는 다음과 같이 패킷이 전송된다.



① targ et 호스트로 연결을 요청하는 SYN 패킷을 보낸다.
② target 호스트의 포트가 닫혀 있는 경우 연결 요청을 받아들이지 못하므로 t arg et 호스트로부터 RST/ ACK 패킷을 받는다.

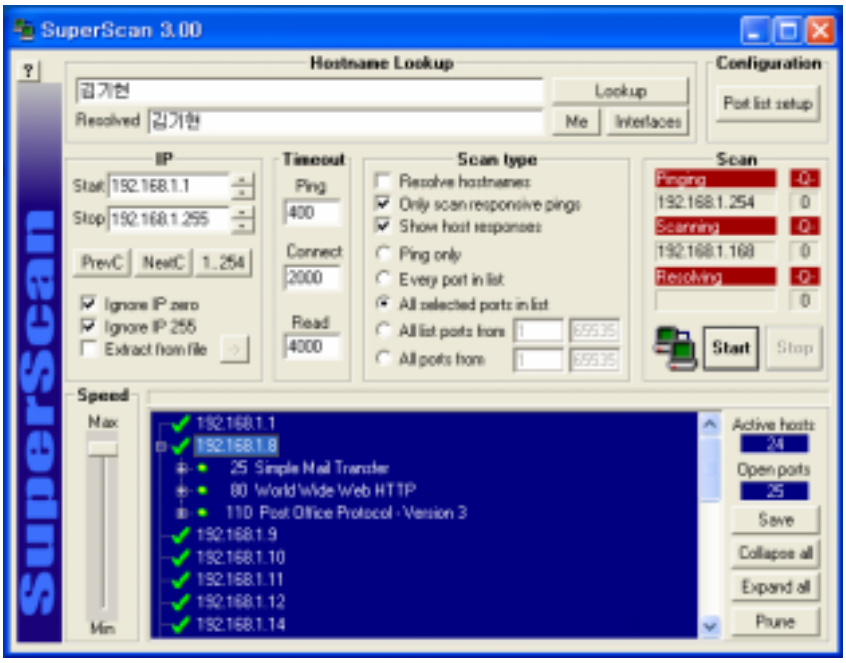
이러한 방법에 의해 접근 가능한 TCP 네트워크 서비스를 식별하는 것은 아주 신뢰할 수 있는 정확한 결과를 얻을 수 있고 특정 시스템에서 권한 없이도 가능하나 쉽게 로깅되며 탐지될 수 있는 가장 원시적인 scanning 유형이다.

이에 쉽게 탐지될 수 있는 단점을 보완하기 위하여 다양한 스캔 방법이 나오고 있다. 해커에 의해 이용되는 포트 scanning 기술은 다음과 같이 몇 개의 그룹으로 분류할 수 있다.



이러한 각각의 scanning 기법은 target 네트워크를 원격으로 조사하기 위해, 열려 있거나 닫혀진 또는 필터링 되는 포트들을 식별하기 위해 사용되나 target 호스트와 네트워크에서 적용하는 네트워크 topology 나 보안 메커니즘 등과 같은 환경에 영향을 받는다. 또한 IDS 나 firewall 과 같은 보안 도구들을 우회하기 위해 패킷의 플래그를 교묘하게 설정하는 등의 방법은 target 네트워크 환경에 따라 성공하기도 하며 경우에 따라서는 실패한다.

아래 그림은 인터넷 상에서 공개 도구로 소개되고 있는 windows 용 scan 도구를 사용한 예이다.



위 그림에서와 같이 scan 할 IP 를 설정하고 start 버튼을 누르면 자동으로 target 을

스캔한다. 현재 동작 중인 시스템의 IP 와 열려진 포트를 볼 수 있다.

3.1.2 mscan vs. sscan

sscan 은 지난 '98 년 6 월 mscan 을 개발하여 전세계를 떠들썩하게 한 johann sebastian bach 가 개발한 보안 취약점 스캐닝 도구로 '99 년 1 월에 버전 0.1 을 발표하였다. sscan 은 mscan 의 명성(?)으로 인해 발표된지 얼마되지 않아서 많은 공개 사이트에서 소개되고 있으며 미국 CERT 팀에서도 그 위험성을 경고하고 있다.

sscan 은 '98 년에 개발된 mscan 에 비해 네트워크 보안 취약점 점검 기능이 매우 강력해져 최근에 발표되고 있는 많은 수의 보안 취약점들을 점검한다. 또한 유닉스 시스템 뿐만 아니라 윈도우즈 95/98, 윈도우즈 NT 시스템의 보안 취약점도 점검하여 지난 '98 년에 윈도우즈 시스템에 많은 위협을 가하였던 백오리피스에 대해서도 진단을 한다.

sscan 자체가 취약점을 공격하지는 않지만 취약점을 공격할 수 있는 명령어들의 모음인 공격 스크립트를 수행하도록 설정할 수도 있다.

따라서 sscan 취약점 스캐닝과 함께 공격 목표 시스템에 대하여 보안 취약점을 이용한 공격이 가능하게 된다. sscan 과 함께 보급된 문서에는 sscan 에 의해 알려진 취약점을 이용하여 공격하는 방법과 자기 복제가 가능한 예제 스크립트를 소개하고 있다.

sscan 의 점검항목을 mscan 과 비교하면 다음과 같다.

점검 항목		mscan	sscan	비고
운영체제 버전 확인		○	○	
네트워크 포트 스캐닝		○	○	
QPOP root 버퍼 오버플로우		○	○	
IMAP root 버퍼 오버플로우		○	○	
Sendmail EXPN			○	
solaris x86 listen/nlps_serv 원격 root 버퍼 오버플로우			○	
리눅스 mSQL 2.0 원격 스택 오버플로우			○	
리눅스 bind/iquery 버퍼 오버플로우			○	
취약한 CGI 점검	/cgi-bin/phf	○	○	
	/cgi-bin/Count.cgi		○	
	/cgi-bin/test-cgi	○	○	
	/cgi-bin/php.cgi		○	
	/cgi-bin/handler	○	○	
	/cgi-bin/webgais		○	
	/cgi-bin/websendmail		○	
	/cgi-bin/webdist.cgi		○	
	/cgi-bin/faxsurvery		○	
	/cgi-bin/htmlscript		○	
	/cgi-bin/pfdisplay.cgi		○	
	/cgi-bin/perl.exe		○	

/cgi-bin/wwwboard.pl		○	
윈도우즈 시스템의 백오리피스(31337 포트 점검)		○	
NFS 취약점 - export 목록 - 모든 사용자에 읽기/쓰기 가능 여부	○	○	
리눅스 mountd 원격 버퍼 오버플로우		○	
Statd 버퍼 오버플로우	○	○	
solaris NIS 서비스(rpc.nisd) 원격 오버플로우		○	
solaris nlockmgr 원격 오버플로우		○	
X11 점검 - X 출력 화면 덤프, 스니핑 가능성	○	○	
Wingate 동작 유무		○	
FINGER 점검 - 사용자 확인(default : root, guest) - 한번도 로그인하지 않은 사용자 확인		○	
스크립트 모듈 수행		○	
Named	○		
IRIX default 계정 유무	○		

mscan 에 비해 기능이 막강해진데 반해 사용방법은 대단히 단순해졌으며, 점검 결과 도 시스템의 취약점을 쉽게 파악할 수 있도록 잘 정리되어 있다.

sscan 을 얻을 수 있는 사이트는 국내에도 여러 곳이 있고 대표적인 사이트는 다음과 같다.

http://www.hwa-security.net

본 실습에서는 /TainingToolkit/Scan/sscan2k-pre6.HWA.tar.gz 을 Linux 환경의 PC 다운받아 아래와 같이 수행하면된다.

① 압축을 푼다.

```
# gzip -d sscan2k-pre6.HWA.tar.gz
```

② tar 를 푼다.

```
# tar xvf sscan2k-pre6.HWA.tar
```

③ 컴파일 한다.

```
# make
```

④ 환경을 설정한다.

```
# sscanconfig
```

⑤ sccan 을 실행한다.

```
# sscan (-o hostname | -s) (-c configfile)
Options:
    -c <config> : specify an alternate config file.
    -o <host>   : specify a single host to scan.
    -e <script> : use this script in addition to default.
    -m : skip all hardcoded checks and just use script file.
    -s : accept host's to scan from stdin.
```

다음은 sscan 의 다양한 사용예를 나타내고 있다.

- o 다수 호스트를 스캐닝하는 경우

  ./sscan domainname.co.kr/24

  설명 : C 클래스로 가정하고 해당 도메인에 ping 을 보내 찾아진 모든 호스트를 스캐닝한다.

- o DNS 영역을 스캐닝하는 경우

  ./tools/z0ne -o domain.com | ./sscan -s > outputfile

  설명 : -s 플래그는 IP 주소를 표준입력에서 받겠다는 의미이고, z0ne 등과 같은 IP 수집 프로그램 등과 함께 사용할 수 있다.

- o 단일 호스트를 스캐닝하는 경우

  ./sscan -vo www.victim.com

  설명 : 특정한 하나의 호스트의 보안 취약점을 점검하여 자세히 출력한다.

다음은 ssan 의 실행예를 나타내고 있다.

```
# ./sscan www.civtim.com/24
- - - - - - - - - - - - - - - - - - - - - - - - - - -<[ * report for host xxx.xxx.xxx.97 *
<[ tcp port: 80 (http) ] > <[ tcp port: 23 (telnet) ] >
<[ tcp port: 143 (imap) ] > <[ tcp port: 110 (pop -3) ] >
<[ tcp port: 111 (sunrpc) ] > <[ tcp port: 79 (finger) ] >
<[ tcp port: 25 (smtp) ] > <[ tcp port: 21 (ftp) ] >
<[ tcp port: 22 (unknown) ] > <[ tcp port: 1114 (unknown) ] >
- -<[ *OS*: xxx.xxx.xxx.97: os detected: solaris 2.x
-<[ *FINGER*: xxx.xxx.xxx.97: root: account exists.
-<[ *FINGER*: xxx.xxx.xxx.97: guest: account exists.
```

```
--<[ *VULN*: xxx.xxx.xxx.97: /cgi-bin/test-cgi here.
--<[ *VULN*: xxx.xxx.xxx.97: solaris running statd (automountd remote?) ^Q
--<[ *VULN*: xxx.xxx.xxx.97: solaris running nlockmgr.. remote overflow? ^M
----------<[ * scan of xxx.xxx.xxx.97 completed *
----------<[ * report for host xxx.xxx.xxx.252 *
<[ tcp port: 80 (http) ] > <[ tcp port: 143 (imap) ] >
<[ tcp port: 110 (pop-3) ] > <[ tcp port: 111 (sunrpc) ] >
<[ tcp port: 79 (finger) ] > <[ tcp port: 53 (domain) ] >
<[ tcp port: 2766 (unknown) ] > <[ tcp port: 25 (smtp) ] >
<[ tcp port: 21 (ftp) ] >
--<[ *OS*: xxx.xxx.xxx.252: os detected: solaris 2.x
-<[ *NFS exp0rt*: xxx.xxx.xxx.252: to: everyone! =) dir: /export/home/thanawat ] >-
-<[ *NFS exp0rt*: xxx.xxx.xxx.252: to: netscape2.mfec.co.th dir: / ] >-

.....
```

sscan 은 보안 취약점 점검과 함께 공격 목표 시스템에 대하여 예측할 수 없는 공격 스크립트에 의한 공격이 가능하게 된다. 이 스크립트 언어는 동일한 보안 취약점이 발견되는 시스템에서는 자기 복제를 무한히 하고 시스템의 파괴 행위 등을 수행할 수 있는 인터넷 웜과 같은 성격을 띌 수도 있다.

3.2 실험

본 실험에서는 csan 도구를 이용하여 실습 서버의 취약성을 분석한다. Windows 환경의 PC 인 경우 ftp 를 이용하여 실습 서버로 접속하고 아래 파일을 다운받아 superscan 을 설치한다.

- /root/Question/Q03/superscan.exe

Linx 환경의 PC 인 경우 ftp 를 이용하여 실습 서버에 접속하고 아래 파일을 다운받고 root 로 권한에서 이 프로그램을 실행시켜야 한다.

- /root/Question/Q03/ sscan2k-pre6.HWA.tar.gz

가. Windows 용 scan 도구인 superscan 을 설치하고 실습 서버를 스캔하시오.

나. Linux 용 scan 도구인 sscan 을 설치하고 실험 서버를 scan 하시오.