최근 해킹기법에 대한 분석 및 대응 방법

고 훈*

◈ 목 차 ◈

1. 서 론

최근 많은 기업들이 많은 업무들을 웹 기반으로 운영하고 있고 국가도 행정 서비스, 예를 들면 각종 증명서 발급을 웹을 통해서 서비스를 하고 있다.

이렇게 웹에 대한 관심이 증대되고 있는 가운데 최근에는 웹 해킹사고가 빈번하게 발생하고 있어 웹 서버 보안의 중요성이 강조되고 있다. 또한 웹 서버는 다른 시스템에 비해 해킹이 비교적 쉽고 해킹의 효과가 높기 때문에 초보해커들도 손쉽게 해킹을 할 수 있다는 것도 중요한 원인으로 작용하고 있다.

웹 서비스의 기능은 특성상 다른 서비스와는 달리 반드시 외부에 노출되어 있어야 하고 방화벽의 보호를 받기 어렵다. 그리고 다양한 어플리케이션들이 웹 서비스와 연동되어 있어 많은 보안 취약점들이 존재한다.

특히 웹기술들이 개발되면서 전에는 없었던 새로운 형태의 보안 취약점들이 꾸준히 생겨나고 있다.

본 논문에서는 최근 많이 발생되고 있는 웹 해킹기법들에 대한 분석 및 보안 대책을 설명하고자 한다.

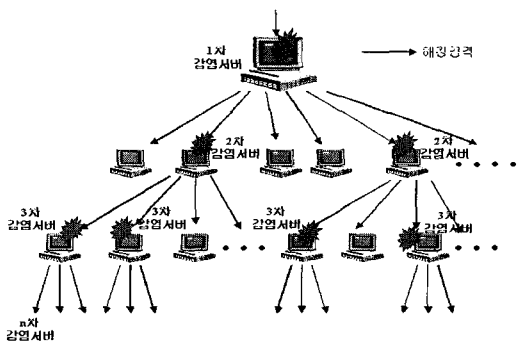
2. 최근 해킹의 경향

최근에 발생되는 해킹의 경향을 보면 다음과 같다.

- 지능화 & 자동화된 공격
- 대규모 & 분산화
- 대중화
- 범죄적인 성향

2.1 지능화 & 자동화된 공격

지능화와 자동화된 공격 기법은 광범위한 시스템 / 네트워크에 침입 및 파괴하는 하는 행위를 말한다(그림 1).



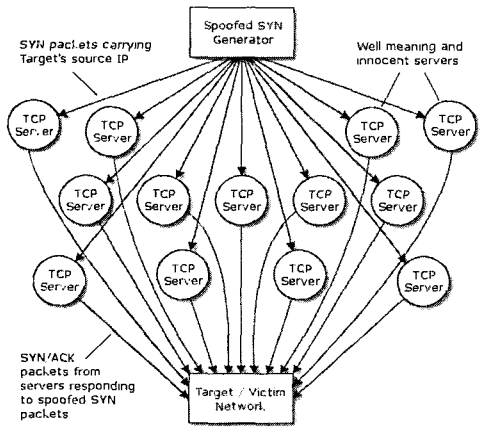
(그림 1) 지능화 & 자동화된 공격

1차 감염된 서버는 인근의 서버들을 찾아서 계속적으로 공격한다. 결국 Internet Worm의 증가를 가져온다. 이 공격에 해당되는 것으로는 VBS/Moon, SQL_Overflow, Win32/Recory.worm 등이 있다.

* 대진대학교 컴퓨터공학과

2.2 대규모 & 분산화

대규모 & 분산화 된 공격은 동시에 다수의 서버를 공격하는 기법으로 multiple scan이라고 한다. 즉 다수의 서버에서 목표 시스템 / 네트워크 공격이 가능하다. 이 공격의 예는 DDOS가 있다.



(그림 2) 대규모 & 분산 공격

2.3 대중화

대중화란 해킹관련 정보의 취득이 쉬움을 의미한다. 인터넷 검색을 하다보면 많은 해킹 프로그램들을 손쉽게 구할 수 있고 사용하는 방법 또한 오픈 되어 있는 상황이다.

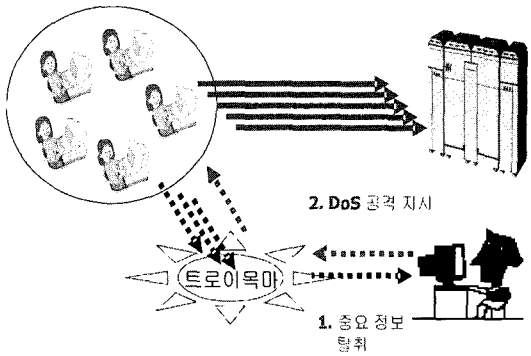
2.4 범죄적인 성향

최신 해킹의 유형을 보면 기존에 재미나 흥미 위주가 아닌 획득한 정보를 악용하는 범죄적인 성향을 띄고 있다. 즉 전자상거래 환경에서의 금전적인 이익, 기업 산업정보를 노리는 해킹, 정치적이고 무정부적인 Hackvisit 공격 등을 대표적인 예로 들 수 있다.

3. 최신 해킹 유형

최신의 해킹 유형을 보면 다음과 같다.

3.1 지능화 & 자동화된 트로이 목마

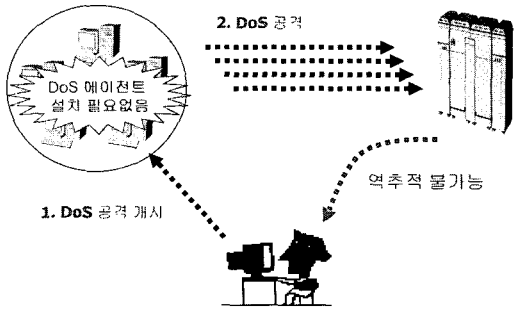


(그림 3) 트로이 목마

트로이 목마의 전파 방법을 보면 설치되는 파일 중 하나인 psexec.bat의 명령어를 이용하여 서브넷 및 다른 서브넷에 있는 시스템에 연결되어 감염된다.

트로이 목마에 감염되면 서브넷 및 다른 서브넷에 있는 시스템 감염되고, 시스템 정보 탈취 공격의 에이전트 기능 가능하게 된다.

3.2 DRDos 공격



(그림 4) DRDoS 공격

지능화된 공격 기법으로 DDos 공격이 일종의 공격 도구인 에이전트를 설치해 공격하는 것과 달리 DRDoS 공격은 별도의 에이전트를 설치할 필요없이 네트워크상의 취약성을 이용, 정상적인 서비스를 운영하고 있는 서버를 에이전트로 활용하기 때문에 해커들이 이용하기 손쉬워 점차 주요 해킹 방법으로 이용

되고 있다.

이 공격에 당하면 Dos 공격을 위한 별도의 에이전트 설치가 불필요하고 공격에 대한 방어가 어렵게 된다.

3.3 버퍼 오버플로우 공격을 이용한 기술

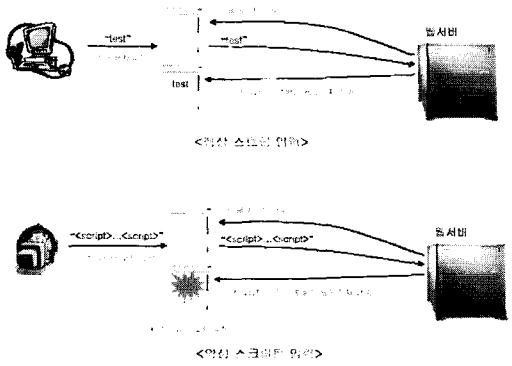
버퍼 오버플로우 공격은 프로그램에서 버퍼의 한계를 점검하지 않는 취약점을 이용하여 악의적인 코드를 입력하고 그 코드가 프로그램의 코드부분을 덮어쓰도록 해서 프로그램의 동작을 변경하거나 다운되도록 하는 공격 방법이다.

3.4 Cross site Scripting(XSS)

XSS 취약점은 웹 어플리케이션이 사용자 입력으로 받은 악성 코드를 필터링 하지 않고 그대로 동적으로 생성된 웹페이지에 포함하여 사용자에게 재전송하는 것이다.

공격자는 XSS 취약점이 존재하는 웹사이트를 이용하여 자신이 만든 악의적인 스크립트를 일반 사용자의 컴퓨터에 전달/실행시킬 수 있는데, 이러한 공격 방법을 통해 사용자 쿠키를 훔쳐서 해당 사용자권한으로 로그인하거나 브라우징을 제어할 수 있다.

공격자는 XSS 취약점이 존재하는 웹 페이지의 사용자 입력으로 "test"와 같이 정상적인 스트림을 입력하는 것이 아니라 <script>로 시작하는 악성 스크립트 코드를 입력한다. 그러면 웹 서버는 공격자가 입력한 악성 스크립트 코드가 포함된 웹페이지를 생성해서 클라이언트에게 되돌려준다. 이 웹페이지에 포함된 스크립트 코드는 클라이언트 측 브라우저에서 실행된다.



(그림 5) XSS

공격자는 웹메일이나 게시판 등을 이용하여 리턴되는 웹페이지를 공격 목표가 되는 일반 사용자에게 전달한다. 공격자는 웹메일에 악성 스크립트 코드를 포함하여 전달하거나 게시판에 악성스크립트 코드가 포함된 글을 포스팅 한 후, 그 글을 읽도록 한다. 일반 사용자가 공격자로부터 수신한 웹메일을 여는 순간 혹은 공격자가 포스팅 한 게시물을 읽는 순간, 해당 웹페이지에 포함된 스크립트 코드가 진행된다.

3.5 SQL Injection

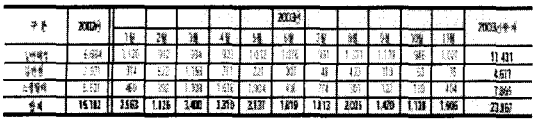
최근 웹프로그램은 자료의 효율적인 저장 및 검색을 위해 DBMS를 필수적으로 사용하고 있다. 주로 PHP, JSP, ASP 등의 스크립트 언어를 이용하여 DBMS와 연동하는데, 이러한 웹어플리케이션에서 클라이언트의 잘못된 입력값을 검증하지 않아 비정상적인 SQL 쿼리가 발생할 수 있다.

이러한 비정상적인 쿼리는 사용자 인증을 우회하거나 데이터베이스에 저장된 데이터를 노출시킬 수 있다. 공격자는 SQL Injection 취약점을 이용하여 아이디와 암호를 몰라도 웹기반 인증을 통과할 수 있고, 데이터베이스에 저장된 데이터를 열람해 볼 수 있다.

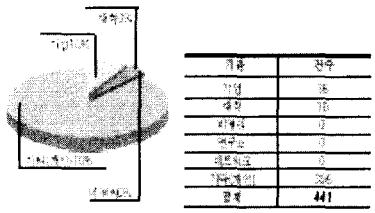
4. 해킹사고 발생현황

2003년 11월까지의 CERTCC-KR 신고접수 특징은 일반해킹, 웜, 스팸릴레이 관련사고 모두 증가하였다. 특히 스팸릴레이 관련사고가 많이 증가하였으며 이에 서버 관리자들에게 스팸릴레이 이용 여부에 대한 확인이 필요하다.

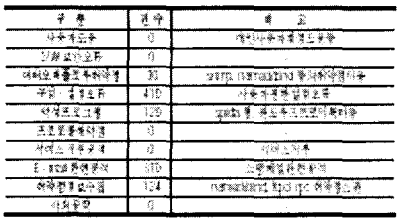
또 하나의 특징은 Windows NT/2000/XP 계열의 피해가 타 운영체제에 비해 보다 높게 나타났다. 이것은 일반 사용자들의 타 운영체제에 비하여 보안 취약점이 많이 내재된 윈도우 운영체제를 많이 사용하는 것을 뜻한다. 해커들이 보안이 강화된 유닉스 등의 서버보다는 보안이 취약한 윈도우를 주 공격대상으로 삼



(그림 6) 2003년 해킹사고



(그림 7) 기관별 해킹 피해



(그림 8) 공격수법에 따른 해킹

고 있으므로 윈도우 운영체제에 대한 사용자들의 취약점 패치와 윈도우 보안 업데이트 및 개인 방화벽 설치가 필요하다.

(그림 6)(그림 7)(그림 8)은 2003년에 발생된 해킹 통계 및 공격수법에 따른 해킹 피해를 보여 주고 있다.

5. 해킹사고 분석 및 보안대책

5.1 Cross site Scripting(XSS)

XSS 취약점을 제거하기 위해서는 웹서버에서 사용자의 입력을 철저하게 필터링 해야 한다. 즉 사용자 입력으로 사용 가능한 문자들을 정해놓고, 그 문자들을 제외한 나머지 모든 문자들을 필터링 하게 한다. 그리고 게시판의 경우 되도록이면 HTML 방식 이외의 사용자 입력이 불가능하도록 설정한다.

XSS 공격으로 인한 피해를 최소화하기 위해서, 사용자가 이용할 수 있는 기능들 및 몇 개의 영역으로 나누어서 영역 경계를 넘는 경우 재인증을 요구하게 한다. 그리고 웹 취약점 스캐너와 매뉴얼한 취약점 점검방법을 이용해서 웹 사이트의 취약점을 주기적으로 점검하도록 한다.

사용자 입장에서는 XSS 공격을 예방하기 위한 가장 확실한 방법은 웹서비스 이용시 XSS 공격에 대해 스스로 주의를 기울이는 것이다. 의심이 가는 메일이나 게시판의 글은 절대 열지 않도록 하고, 메일에 포함된 URL은 직접 클릭하지 않도록 한다. 웹사이트 방문시 링크를 직접 클릭하지 말고 반드시 본인이 직접 URL을 입력하도록 하는 것이 안전하다.

5.2 SQL Injection

SQL Injection에 대한 가장 훌륭한 해결책은 포괄적인 입력 검증을 수행하는 것이다. 모든 스크립트에 존재하는 모든 파라미터들을 점검하여 사용자의 입력값이 SQL Injection을 발생시키지 않도록 수정한다. 그리고 SQL 서버의 에러 메시지를 사용자에게 보여주지 않도록 설정하고 웹어플리케이션이 사용하는 데이터베이스 유저의 권한을 제한시키고 데이터베이스 서버에 대한 보안 설정을 수행한다.

5.3 버퍼 오버플로우

버퍼오버플로우 취약점으로부터 웹서버를 보호하기 위해서는 항상 최신의 버그 리포터에 주위를 기울이고 즉각적인 패키를 수행하는 것이 중요하다. 직접 개발한 어플리케이션에 대해서는 사용자 입력을 받는 코드 부분을 점검하고, 반드시 모든 외부 입력에 대해 적절한 한계 체크를 수행하도록 한다. 버퍼오버플로우 공격이 아니더라도 매우 큰 입력은 서비스 거부나 동작 문제를 일으킬 수 있기 때문에 이 점에 대한 점검도 같이 수행한다.

5.4 파일 업로드

파일 업로드는 주로 게시판의 파일첨부 기능을 통

해 이루어진다. 게시판의 파일 첨부 기능을 통해 웹서버에 파일을 업로드한 후에 그 파일을 요청하는 것이다. 따라서 게시판에 cgi, asp, jsp, php, php3와 같은 확장자를 갖는 파일이 업로드 되지 않도록 주의해야 한다. 좀 더 확실한 대응 방법은 doc, hwp, txt 파일을 제외한 모든 파일의 업로드를 막는 것이다. 그리고 꼭 필요한 기능이 아니라면 게시판의 파일 업로드 기능을 제거해야 한다.

5.5 불필요하게 노출된 파일의 이용

불필요한 파일들은 반드시 백업 및 삭제를 해야 한다. 디폴트로 설치된 샘플 파일들은 필요여부를 검토한 후에 웹서버에게 모두 삭제하도록 한다. 어플리케이션의 소스 코드나 중요 설정 파일, 임의로 접근이 불가능해야 하는 특정 웹페이지가 외부에 노출되지 않는지 혹은 그 백업 파일이 웹서버에 존재하지는 않는지 모든 웹 디렉토리를 점검하도록 한다.

6. 결론

지금까지 해킹 기법이 대응 방안 등에 대해서 살펴보았다. 그러나 앞으로는 더 지능적이고 교묘한 방법이 계속적으로 개발되어 사용되어질 것이다. 스파이웨어를 탐지하기 위해 사용되는 백신이나 안티 스파이웨어를 솔로션 등을 우회하기 위한 기술인 고성능 스파이웨어를 통한 정보유출, 무선랜의 활성화에 따라 무선랜 프로토콜 아키텍처의 취약점을 이용한 무선랜 해킹, 해커들이나 해커 그룹간 공조를 통해 역추적을 위한 경로파악을 어렵게 하는 방안 등이 개발될 것이다. 일반 사용자들은 이들로부터 안전하기 위해서 지속적인 보안패치, 취약점 분석 자료를 이용하여 취약점 제거 설정 및 운영 지침을 준수하고, 메일 및 P2P 자료 공유시 악성 코드를 항시 검사해야 하며 범국민적인 보안의식 고취를 위한 홍보 및 위로부터의 정보보호 중요성을 인식하고 내부자의 정보보호 교육 강화 노력이 필요하다. 마지막으로 기술적인 한계에도 불구하고 보안을 유지하는 유일한 방법은 정보보안 과정을 만드는 것이며, 정보보안은 보안 제품만으로는 해결할 수 없다는 원칙을 인식해야 한다.

참고문헌

[1] 인터넷 보안기술 및 시장동향, ETRI 주간기술동향, 2003. 4.

[2] 정보보호 기술개념과 동향, 전자부품연구원, 2003. 2.

[3] 전자신문, http://www.etimesi.com

[4] 정보보호진흥원, "월간 정보보호 뉴스"

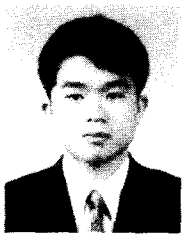
[5] Big Picture: IT Security Products and Services Forecast and Analysis, IDC, 2002. 12.

[6] Worldwide Security Software Forecast, 62003~2007, IDC, 2003. 3.

[7] Security Appliance: The Primary Platform for Delivering Security Software, IDC, 2003. 1.

[8] http://www.certcc.or.kr/right11.htm

◐ 저 자 소 개 ◑



고 훈

1992. 3~1998. 2 호원대학교 전자계산학과 학사
1998. 3~2000. 2 숭실대학교 컴퓨터학과 통신연구실 석사
2000. 3~2002. 2 숭실대학교 컴퓨터학과 통신연구실 박사수료
2000. 5~2002. 7 (주) 지오나스 선임연구원
2003. 1~2003. 12 한국정보보호학회 편집위원
2002. 9~현재 대진대학교 컴퓨터공학과 초빙교수
관심분야 : 정보보안, 보안프로토콜, 인터넷보안, 네트워크 보안