제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

자가 이동 기법을 이용한 공격도구의 설계

김 승 겸*, 장 성 만*, 이 극*, 권 영 미**, 이건호***
* 한남대학 컴퓨터공학과, ** 충남대학교 정보통신공학부, *** 육군본부

요 약

현재의 전쟁에서는 자국의 정보자원 및 시스템을 보호하고 적의 중요 정보자원 및 시스템에 피해를 입히거나 파괴하는 정보전이 중요한 수단이 되고 있다. 본 논문에서는 정보전에서 우위를 점하기 위하여 자가 이동기법을 이용한 공격도구를 설계한다. 자가 이동기법은 악성 프로그램이 네트워크상의 경로를 통하여 원격지 시스템으로 스스로 이동하는 기술이다.

A Design of Attacking Tool Using Self Movement Techni

Kim Seung Kyeom*, Jang Seong Man*, Lee Geuk*, Kwon Young Mi**, Lee Gun Ho***

1. 서 론

21세기에 접어들면서 국가간의 전쟁은 물리적인 파괴 및 살상보다는 상대국가의 전쟁 수행능력을 마비시킬 수 있는 정보전(Information Warfare)의 양상으로 흘러가고 있다. 미합참은 정보전이란 "정보 우위를 확보하기 위하여 적의 정보, 정보에 기반을 둔 처리, 정보체계 그리고 컴퓨터에 기반을 둔 망에 영향을 미치고, 아군측의 정보, 정보에 기반을 둔 처리, 정보체계 그리고 컴퓨터에 기반을 둔 망들을 보호하는 행위"라고 정의하고 있다[1]. 이와 같이 정보전은 아군의 정보와 시스템을 보호하는 동시에 적의 정보와 시스템에 영향을 주어서 정보 우위를 차지하는 것이다.

지금까지의 정보전의 흐름을 보면 공격적인 개념보다는 방어적인 개념에서 연구가 진행되었고 침입차단시스템, 침입탐지시스템, 침입방지시스템이 정보전에 대비하는 대표적인 보안시스템들이다. 하지만 미래의 정보전은 방어적인 개념보다는 공격적인 정보전의 형태로 나아갈 것이다. 즉, 보안시스템으로 아군의 정보와 시스템을 보호할 뿐만 아니라 적의 정보와 시스템에 영향을 줄 수 있는 가상 무기(cyber weapon)가 필요하다.

본 논문에서는 자가 이동기법을 이용한 공격도구를 설계한다. 자가 이동기법이란 해커가 직접 명령을 내려 원격지 네트워크로 악성 프로그램을 이동시키는 것과는 다르게 악성 프로그램

본 연구는 과학기술부 지역협력연구사업 (R12-2003-004-02002-0) 지원으로 수행되었음

이 스스로 원격지 네트워크로 이동 할 수 있는 기법을 말한다. 2장 관련 연구에서는 정보전에서 이용될 수 있는 해킹기술과 자가 이동기법을 분석하고, 3장 설계에서는 자가 이동코드의 구조와 흐름도에 대하여 기술하고 4장에서는 결론 및 향후 연구방향을 기술한다.

2. 관 련 연 구

2.1 해킹 기술

2.1.1 버퍼 오버플로우 취약점 이용

1996년 Bugtraq mailing list 운영자, AlephOne이 Phrack Magazine 49호 " Smashing The Stack For Fun And Profit" 이라는 문서를 저술, 발표함으로써 이에 대한 세부적인 기술이 공개되었다[3]. 버퍼 오버플로우 조건(buffer overflow condition)은 사용자 또는 프로세스가 원래 할당된 버퍼의 크기보다 더 많은 데이터를 저장함으로써 발생되는 것이다. 즉 데이터를 입력받을 때 한계값 검사(boundary check)를 하지 않음으로 해서 버퍼 오버플로우 조건을 이용하여 공격자가 상대 시스템에 피해를 주는 공격기법이다.

2.1.2 네트워크 프로토콜의 취약점 이용

인터넷 통신 방식의 근간을 이루는 것은 TCP/IP 프로토콜이며, 인터넷의 최초 구성 이유가 정보의 공유에서 출발 되었듯이 본 프로토콜 또한 이러한 특성에 맞게 개방적인 구조를 이루고 있다[4]. 따라서 이러한 개방적인 구조를 이용하여 해킹하는 방법은 매우 다양하며, 대표적으로 IP 스푸핑(Spoofing) 공격, SYN 플러딩(Flooding) 공격, 분산 서비스거부(DDoS) 공격 등이 있다.

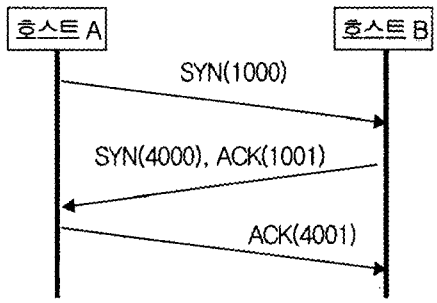
가. IP 스푸핑 공격

IP 스푸핑은 IP를 속이는 행위를 말하는데 IP 자체의 보안 취약성을 악용한 것이다. 패킷을 판단할 때에는 단지 IP 주소만 가지고 판단의 근거를 가지기 때문에, 수신자는 패킷이 어디서 왔는지 명확하게 알 수 있는 길이 없다.

통신을 하고 있는 세션을 가로채는 TCP 세션 하이재킹(TCP Session Hijacking) 같은 기술은 위의 대표적인 공격이라고 볼 수 있다. TCP 세션 하이재킹을 성공적으로 하기 위해서는 TCP의 순서(SEQ) 번호를 유추해야 하는 어려움이 따르지만, 이것은 초당 250,000번, 즉 4Microsecond마다 한 번씩 증가되도록 되어 있어 어느 정도 추측이 가능하도록 되어 있다[5].

나. SYN 플러딩 공격

SYN 플러딩 공격은 TCP 프로토콜의 취약점을 이용하여 시스템의 자원을 고갈시키는 공격방법이다. 이 방법은 시스템을 파괴하지는 않지만 목표로 하는 포트를 마비시켜 해당 서비스가 제공되지 못하게 한다. 또한 소스 주소를 속이기 때문에 공격자를 추적하기가 매우 어렵다.



(그림 2-1) TCP의 연결과정

(그림 2-1)은 호스트 A가 호스트 B로 TCP 연결을 맺는 일반적인 모습이다. 호스트 A는 호스트 B에 연결을 하기 위해 SYN 패킷을 보낸다. 그러면 B는 요청받은 포트에 기다리고 있는 서비스가 있다면 연결을 받아들이기 위한 초기화 과정을 거치게 된다. 이때 시스템 자원이 할당이 된다. 이 연결은 SYN_RECV 상태가 되고

호스트 B는 SYN/ACK 패킷을 호스트 A로 보내게 된다. 그리고 호스트 A가 마지막으로 ACK 패킷을 보내게 되면 연결이 이루어지고 상태가 성립이 된다.

이 연결과정 중에서 SYN/ACK 패킷을 보내고 다시 ACK 패킷을 받을 때까지 운영체제는 제한된 자원을 사용하게 된다. 이 부분에서 SYN 플러딩 공격이 이루어진다. SYN 플러딩 공격을 할 때 공격자는 존재하지 않는 호스트의 주소로 소스 주소를 변경하여 목표 시스템에 SYN 패킷을 보낸다. 목표 시스템에서는 위조된 소스 주소로 SYN/ACK를 보내고 ACK를 기다리게 된다. 위조된 소스 주소가 존재한다면 그 호스트는 SYN 패킷을 보내지 않았기 때문에 RESET 패킷을 보내게 되어 연결을 위해 대기 중이던 자원이 해제 된다. 하지만 존재하지 않는 주소로 SYN/ACK 패킷을 보내게 되면 연결 대기시간이 초과될 때 까지 ACK 패킷을 기다리게 된다. 공격자가 이 시간 안에 주기적으로 백로그 큐(연결 대기 중인 큐)가 찰 만큼의 SYN 패킷을 보낸다면 공격 받는 호스트는 해당 포트에 더 이상 연결을 받아들일 수 없는 상태가 된다 [6].

다. 분산 서비스거부 공격

분산 서비스 거부 공격 공격은 기존의 서비스 거부공격 공격에 분산 처리 개념이 도입되고 모든 공격이 자동화되어 있다. 널리 유포된 분산 서비스 거부 공격 도구를 이용하면 웬만한 해킹 기술을 가진 공격자라도 쉽게 적용할 수 있는 일종의 인터넷 테러리즘이라고 볼 수 있다[7]. 즉 공격자들은 우선 스니퍼(sniffer)나 네트워크 스캐너 등의 도구를 이용하여 인터넷상의 취약한 호스트를 탐색하여 이를 침해한 다음, 이렇게 침해된 수백 수천 대의 호스트에 온라인으로 공격 도구를 설치한다. 이런 모든 과정은 자동화되어 있어 단 몇 십 분이면 완료될 수 있다. 이제 공격자의 컴퓨터에서 단 한 줄의 명령어만 보내면 수백 수천대의 호스트가 공격대상인 컴퓨터에 일정시간 동안 지속적으로 의미 없는 패킷 스트림을 보냄으로서 그 서버를 다운시키거나 네트워크 대역폭을 포화시켜 일반 사용자가 그 서버에 접근하지 못하도록 하는 것이다.

분산 서비스 거부 공격 공격의 특징은 대부분의 공격이 자동화된 도구를 이용하여 쉽고 짧은 시간에 수행할 수 있다는 점과 높은 대역폭을 갖는 중간 매개 사이트들을 공격자원으로 활용하여 분산 공격 네트워크를 구성하는 협동 공격이라는 점이다. 따라서 일차적인 피해자는 직접적으로 공격당한 목표 호스트이지만 자신도 모르게 마스터나 데몬으로 이용당하는 중간 매개 사이트들도 이차적인 피해자가 되는 셈이다.

통상 공격자는 높은 대역폭을 갖는 데몬들을 선택하여 공격의 효율을 높인다. 예를 들면, 100대의 데몬이 이용되고 각 데몬들이 1Mbps의 속도로 패킷 스트림을 보낸다면 목표 호스트는 100Mbps로 들어오는 패킷을 처리해야 하므로 이들을 처리하지 못하여 느려지거나 시스템 다운이 발생할 것이다.

2.2 자가 이동기법

자가 이동기법은 악성 프로그램이 한 컴퓨터에서 네트워크상의 경로를 통하여 원격지 컴퓨터로 스스로 이동하는 것이다. 자가 이동기법을 이용한 공격도구는 원격지의 컴퓨터 시스템이 제공하는 서비스의 취약점을 이용하여 자신의 프로그램의 복제본을 이동시킨다. 이동된 프로그램은 원격지 컴퓨터에서 컴파일 하여 실행된 후에 위의 과정을 되풀이하게 된다. 기존의 해킹기술에 네트웍상의 경로를 따라서 스스로 이동할 수 있는 자가 이동기법이 첨가된다면 강력한 사이버 테러 무기가 될 것이다.

2.2.1 자가 이동을 이용한 공격도구의 특성

자가 이동기법을 이용한 공격도구는 네트워크 상의 경로를 따라서 원격지 컴퓨터로 스스로 이동하기 때문에 다음과 같은 특성을 가져야 한다.

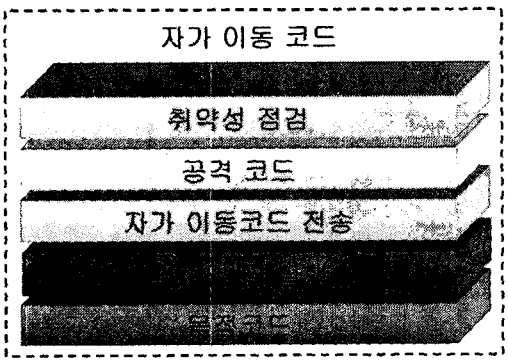
가. 단일 프로그램
나. 원격지 시스템의 취약성 판별
다. 자가 이동코드 전송
라. 데몬 프로그램으로 실행

위와 같은 자가 이동기법의 특성을 이용하여 3장에서 공격도구를 설계한다.

3. 설 계

3.1 자가이동코드 구조

본 논문에서는 정보전에 이용될 수 있는 해킹 기술에 자가 이동기법을 적용한 공격도구를 설계하며, 자가이동코드의 구조는 그림(3-1)과 같다.



(그림 3-1) 자가이동코드 구조

가. 취약성 점검

공격도구는 자가 이동을 하기에 앞서 원격지 시스템에서 제공하는 서비스가 취약성이 있는지를 판별한다.

나. 자가 이동을 위한 공격코드

원격지 시스템에서 제공하는 서비스의 취약성이 발견되면 원격지 시스템에 공격코드를 실행하여 원격지 시스템의 쉘을 획득한다. 공격코드에는 원격지 시스템의 취약성의 종류에 따른 해킹기술이 포함되어진다. 예를 들면, 버퍼 오버플로우 공격기술을 이용하여 /bin/bash 또는 /bin/sh를 획득한다.

다. 자가 이동코드 전송

원격지 시스템의 쉘을 획득한 후에 자신의 복제본을 이동시키기 위하여 소켓 API를 이용하여 원격지 시스템과 연결을 맺고 자신의 복제본을 이동시킨다.

라. 컴파일 및 실행

원격지 시스템으로 이동된 공격도구의 복제본은 원격지 시스템의 환경에 맞게 재컴파일되고 실행되어진다. 원격지 시스템에서 실행되는 공격도구는 데몬 프로그램으로 실행이 된다. 데몬은 백그라운드로 실행되어 있다가 네트워크를 통해 들어오는 요청에 대해 서비스를 하는 프로그램이다[8]. 공격도구는 원격지 시스템에 이동된 후에 계속해서 다른 원격지 시스템으로 이동하기 위해서 데몬 프로그램으로 실행되어야 하며 관리자에게 발각되지 않게 하기 위해서 프로그램명을 통상적으로 서버 프로그램에서 자주 쓰이는 데몬 프로그램 이름으로 실행되게 한다. 예를 들면 "httpd", "proftpd", "telnetd"와 같이 자주 쓰이는 데몬 프로그램 이름으로 한다.

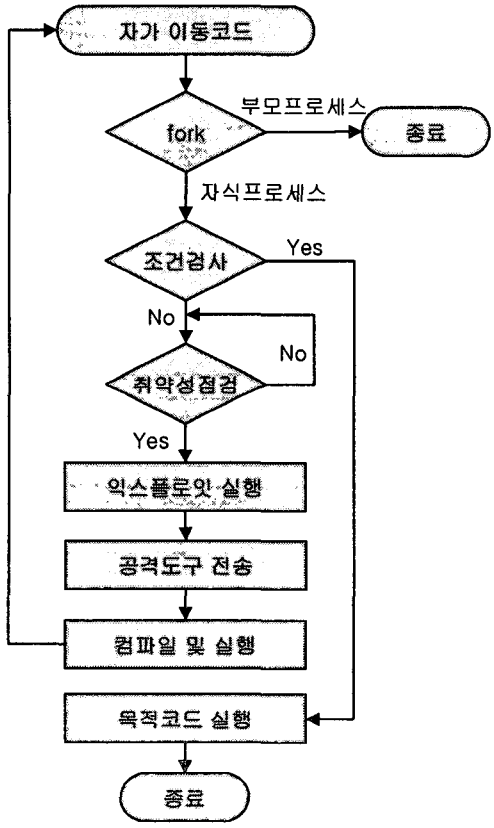
라. 목적 코드

공격도구의 목적은 네트워크 상에서 자가 이동을 하는 것뿐만 아니라 원격지 컴퓨터 시스템의 정보를 알아내거나 시스템에 심각한 피해를 입히거나 제 2의 공격거점으로 삼는 것이다. 이를 위해서 원격지 컴퓨터 시스템에 피해를 입힐 수 있는 목적코드가 공격도구에 포함되어야 한

다.

3.2 공격도구 흐름

자가 이동기법을 이용한 공격도구의 흐름도는 아래 그림(3-2)와 같다.



(그림 3-2) 공격도구 흐름도

① 자가 이동코드는 데몬 프로그램으로 실행되기 위하여 fork 함수를 통하여 프로세스를 부모 프로세스와 자식 프로세스로 분기한다. 부모 프로세스는 바로 종료하게 되고 커널이 자식 프로세스를 관리하게 되어 데몬 프로그램의 형식을 갖추게 된다.

② 공격도구는 현재 이동되어진 시스템이 목적 시스템인지 검사하게 된다. 목적 시스템이 맞거나 공격도구의 자가 이동 횟수나 이동 시간이 일정 수준에 이르게 되면 자가 이동을 멈추게 되고 목적 코드를 수행하게 된다. 목적 코드에는 목적 시스템에 직접적으로 피해를 줄 수 있는 공격 코드와 수많은 자가 이동의 시도에도 목적 시스템으로 직접 이동 할 수 없을 경우에는 목적 시스템에 분산 서비스 공격을 수행할 수 있는 공격 코드가 있다.

③ 조건검사를 하여 조건에 부합되지 않은 경우에는 자가 이동을 계속하기 위하여 랜덤으로 지정된 IP 주소를 통하여 원격지 시스템에 취약성 점검을 시도하고 취약성이 있다면 익스플로잇을 실행하여 자가 이동코드의 복제본을 전송한다.

④ 이동된 자가 이동코드는 컴파일과 실행과정을 거치고 ①②③의 과정을 반복한다.

4. 결론 및 향후 연구방향

본 논문에서는 자가 이동기법을 이용하여 공격도구를 설계하였다. 공격도구는 원격지 시스템의 보안 관리자에게 탐지 가능성을 낮추기 위하여 데몬 프로그램으로 실행된다. 그 후에 공격도구는 네트워크 경로를 통하여 원격지 시스템의 취약성을 이용하여 스스로 이동하게 된다. 이동된 공격도구는 미리 정의된 조건검사에 부합될 경우에는 목적코드를 실행하여 목적 시스템에 피해를 준다. 하지만 조건에 맞지 않을 경우에는 다른 원격지 시스템으로 이동을 반복하게 된다. 향후 연구방향으로는 원격지 시스템으로의 자가 이동을 위하여 원격지 시스템에서 제공하는 서비스들에 대한 취약성 연구와 취약성에 따른 해킹기법의 연구 및 적용이 필요하다.

참고문헌

[1] 박상서, 이진석, 박춘식. "정보전 개념과 대응 기술", 정보과학회지, pp. 8-19, 2000.

[2] 박성서, 박춘식, "정보전 개념과 주요 동향", 정보처리학회지, pp. 47-57, 2003.

[3] 조기준.김훈희 역, 해킹과 방어 완전 실무. 구민사, 2001

[4] 서동일, 윤이중, 조현숙, "정보전 대비 실시간 감지 및 경보 네트워크 구축방안", 정보과학회지, pp. 36-44, 2000.

[5] 황석훈 역, 네트워크 이론과 해킹 기법. 혜지원, 2003

[6] http://www.kisa.or.kr/Critical_Information_Infrastructure/data/m_01_04_tech_data_20030705_YJ_web_hacking.pdf

[7] http://www.securitymap.net/sdm/docs/attack/TopologyDOS.pdf

[8] http://www.wowlinux.com/information/freshmanview.html?id=84&view=1