제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

실시간 침입자 행동양식 파악 시스템의 설계 및 구현

*서동일 ○ *최양서 **이상호

* 한국전자통신연구원 정보보호연구본부 네트워크보안연구부

** 충북대학교 전자계산학과

Design and Development of Real Time Honeypot System for Collecting the Information of Hacker Activity

*Dong-il Seo○ *Yang-seo Choi **Sang-Ho Lee

* Network Security Department, ETRI

** Department of Computer Engineering, Chung-Buk National University

bluesea@etri.re.kr, yschoi92@etri.re.kr, shlee@cnlab.cbu.ac.kr

요 약

인터넷이 생활의 한 부분이 되면서 인터넷 사용자가 급증함에 따라 각종 사이버 범죄의 발생 건수 역시 크게 증가하고 있다. 이러한 각종 사이버 범죄에 대응함에 있어서 가장 심각한 문제 중의 하나는 해커가 어떤 기술을 이용하여, 어떠한 방식으로 해킹을 진행하는지에 대한 정보가 매우 부족하다는 것이다. 현재 해커들은 해킹에 성공하기 위해 고도의 해킹 기법과 새로운 취약점을 이용하고 있는 반면, 해킹 방지를 위해 사용되고 있는 보안 강화 시스템들은 새로운 방식을 이용하는 해킹 시도를 효율적으로 방어하지 못하고 있는 것이 현실이다. 이와 같은 문제점을 해결하기 위해 제안된 것이 해커의 행동 양식에 대한 정보를 얻기 위한 침입유도 시스템(Honeypot)이다. 그러나 기존의 침입유도 시스템은 해커의 행동 양식 파악에 전문적인 기술이 필요하여 실시간 정보분석이 용이하지 못했다. 이에 본 논문에서는 해커의 행동양식을 실시간으로 파악하고 분석하는 허니넷(Honeynet) 형태의 침입자 행동양식 파악 시스템(Honeypot)을 설계하고 개발하였다.

1. 서론

인터넷은 이제 실생활에 없어서는 안될 중요한 매체가 되었다. 인터넷 사용자들은 인터넷을 통해 원하는 정보를 원하는 시간에 얻을 수 있으며, 각종 멀티미디어 서비스를 제공받을 수 있을 뿐만 아니라, 금융관련 서비스 역시 인터넷으로 수행할 수 있게 되었다.

이러한 인터넷 이용의 양적 질적 향상과 더불어 부정적인 측면도 함께 나타나고 있는데, 이는 최근 해킹 발생 건수의 증가 추이를 살펴보면 쉽게 알 수 있다[1]. 특히 인터넷이라는 개방형 네트워크로 정보통신 기반이 진화되면서 사이버 테러를 수행하는데 사용될 수 있는 각종 해킹도구를 인터넷 상에서 손쉽게 획득할 수 있는 최근 상황은 사이버 범죄의 잠재적 저변이 무서운 속도로 확대되고 있음을 암시하고 있다. 또한 인터넷에 공개된 해킹 도구들은 고도의 해킹 기술을 이용하면서도 사용방법이 매우 쉬워 초보자들 역시 쉽게 사용할 수 있다는 점에서 더욱 큰 문제가 되고 있다.

이와 같은 상황에 따라 시스템 및 네트워크 보안 기술의 확보가 시급히 요구되었고, 이를 위해 다양한 보안 솔루션들이 개발되고 있다. 그러나, 최근 발표되고 있는 각종 보안 솔루션 및 침해 대책들은 해킹에 대한 효율적인 해결책을 제시하지 못하고 있는 것이 사실이다. 이는 날로 다양해지고 고도화되고 있는 각종 해킹 기법에 대해 침입자들의 근본적인 성향과 이용 기술을 파악하지 못하고, 단기간의 미봉책만을 제시하고 있기 때문이다. 이러한 문제점을 해결하기 위해서는 해커가 사용하는 구체적인 해킹 기법들이나 행위에 대한 데이터베이스 구축을 통해 향후 발생할 수 있는 해킹 사고를 미연에 예측할 수 있어야 한다. 즉, 해커의 행동 양식 및 해킹 절차를 구체적으로 파악하고, 새로운 해킹 기법을 신속히 파악하여 그에 대한 대응책을 제시할 수 있어야 한다. 이를 위해 제안된 것이 침입유도 시스템(허니팟, Honeypot)이다.

그러나, 현재까지 개발된 허니팟 시스템들은 대부분 해커의 해킹 기법과 행동양식 파악이라는 측면을 강조하여 해커로부터 해커가 침입하려는 시스템이 침입 유도 시스템이라는 것을 감추는 측면이 소외되었던 것이 사실이다. 최근 허니넷 형태의 허니팟이 제안되면서 실제로 사용되는 시스템과 동일한 허니팟 시스템을 사용하고는 있으나, 해커의 행동양식 파악을 위해 전문가가 필요하거나, 실시간으로 분석하기 힘든 상황이었다. 따라서, 본 논문에서는 해커의 행동

양식을 실시간으로 파악하고 적용된 해킹 기법을 수집할 수 있는 허니팟 시스템을 설계하고 구현한 결과를 제시하고자 한다.

본 논문은 제 2 장에서 허니팟 시스템이란 무엇인가에 대해 알아보고, 제 3 장에서는 허니팟 시스템의 설계 및 구현 결과에 대해서 논의하며, 제 4 장에서 결론을 맺도록 한다.

2. 허니팟 시스템

2.1 정의

허니팟 시스템이라는 것은 보안 강도를 강화한다거나 해커의 침입을 방어하는 일반적인 보안 시스템과는 달리 정보를 수집하고 다른 중요 시스템을 보호하기 위해 해커를 유인하는 시스템을 의미하는 것으로 Loras R. Even 은 [2]에서 허니팟 시스템을 다음과 같이 정의하고 있다.

정의 1. 허니팟 시스템

허니팟 시스템은 시스템을 공격하거나 침입하는 해커에 대한 정보를 수집하기 위해 제작된 허위 서버들이나 시스템들이다.

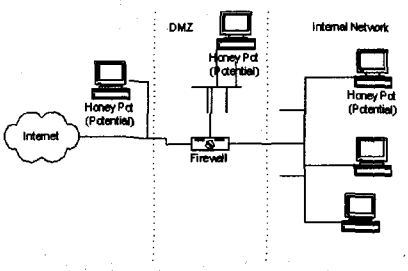
(Honey Pot Systems are decoy servers or systems setup to gather information regarding an attacker or intruder into your system.)

따라서, 허니팟 시스템이란 해커에 의해 공격 당함으로써 그 가치를 발휘하는 시스템을 의미하는 것으로 단지, 공격자의 정보를 수집하고 이를 이용하여 보안 강화에 도움이 될 수 있는 정보를 제공하는 시스템을 의미하는 것이다. 허니팟 시스템은 꿀단지를 의미하는 허니팟(honey pot)이라는 명칭에서도 알 수 있듯이 누군가를 유인하는 목적으로 사용된다.

허니팟 시스템이 적용될 수 있는 분야를 세분화 한다면 일반적으로 다음과 같이 2 가지 분야로 구분된다. 먼저, *(1)임의 네트워크에 설치되어 해커의 해킹을* 유도함으로써 사용되는 해킹 기법 및 각종 해킹 도구들에 대한 정보, 그리고 해커의 행동양식을 파악하기 위한 목적으로 사용되는 시스템과 (2)해커를 유인함으로써 같은 네트워크의 다른 중요 시스템으로의 해킹 시도 가능성을 줄이고 허니팟 시스템을 공격하는 동안 실제 중요 시스템의 보완으로 시스템을 보호하기 위해 사용되는 시스템이다.

2.2 설치 위치[2]

앞서 언급한 바와 같이 허니팟 시스템은 해커의 해킹 시도가 있어야만 그 가치를 발휘하지만, 해커의 접근이 너무 쉬운 경우에는 그로 인해 또 다른 문제를 발생시킬 수 있다. 이와 같은 현 상황에 따라 허니팟 시스템의 위치 역시 2 가지 모델이 논의되어지고 있다.



(그림 1) 허니팟 시스템의 위치

먼저, 실제로 사용되는 서버 시스템들 사이에 허니팟을 위치시키는 방법이다. 이는 허니팟 시스템의 존재여부를 감추고, 다른 실제 서버 시스템들 보다 낮은 보안 강도를 가지고 있어서, 해커의 목표가 되도록 하기 위함이다. 이런 경우, 내부 네트워크의 시스템들과 같은 위치에 설치될 수도 있으나, 대부분의 실제 서버 역시 해커로부터 접근할 수 있는 영역에 설치되어야 하기 때문에, 주로 DMZ 에 설치된다.

다음은 허니팟 시스템에서 내부 네트워크로의 접근이 불가능하도록 특정한 네트워크 상(일반적으로 외부 네트워크)에 위치시키는 것인데, 이는 해커가 허니팟 시스템을 점유한 후에 발생할 수 있는 2 차적인 해킹에 앞선 모델보다는 안전하지만, 허니팟 시스템 *만이 한 네트워크에 설치되는 경우가 실제 인터넷 환* 경에서는 거의 없기 때문에 쉽게 허니팟 시스템이 아닐까 하는 의아심을 갖을 수 있게 한다.

각각의 모델들은 나름대로의 장단점이 존재하므로, 허니팟을 설치할 위치는 해당 네트워크를 관리하는 관리자와 보안 정책에 의해 결정되어야 한다.

2.3 관련연구

허니팟 시스템은 특정 기술을 이용하는 것이 아니라 정보의 수집이라는 큰 목적을 위해 만들어진 일종의 도구이기 때문에, 일정한 형태의 같은 기술이 적용되어 구현되지는 않는다. 따라서 정형화된 관련 연구는 진행되고 있지 않다. 다만 여러 업체들에 의해 허니팟 시스템의 본래 목적을 수행하는 제품들이 다양한 형태로 개발되고 있다.

허니팟 시스템이란 해커가 접근해야만 그 목적을 달성하는 시스템이기 때문에 해커의 접근이 용이하도록 구성하게 된다. 그러나 제 2 장에서 언급한 바와 같이 해커의 접근이 너무 용이하면 비록 허니팟을 통해 얻을 수 있는 정보의 양은 많아지지만 허니팟을 통해 또 다른 해킹을 수행할 수 있는 가능성은 더욱 커지게 된다. 이러한 특성 때문에 현재 개발되고 있는 허니팟 시스템은 해커의 접근 용이성과 문제 발생 가능성 사이의 조절(tradeoff)을 통해 다양한 형태로 개발되고 있다. 즉, 해커의 접근을 용이하게 하고 많은 정보를 얻는 허니넷 형태의 허니팟 시스템과 비록 얻을 수 있는 정보는 제한되더라도 2 차적인 문제가 발생하지 않도록 구성된 시뮬레이션 형태의 허니팟 시스템 그리고 이들간의 중간 형태의 허니팟 시스템

들이 개발되고 있다.

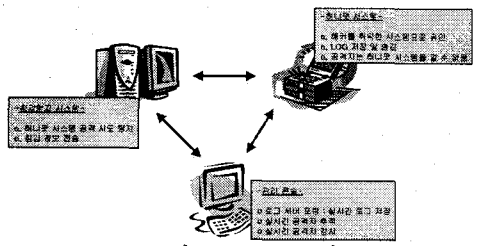
여기에는 BackOfficer Friendly(BOF), Specter[5], Homemade Honeypots[3], Deception Tool Kit[8], Mantrap[9], 허니넷(Honeynet)[10]등이 있다.

3. 시스템의 설계 및 구현

3.1. 시스템 구성

본 논문에서 개발하고자 한 허니팟 시스템은 해커의 공격 기법 및 행동양식을 실시간으로 파악하기 위한 것이다. 따라서 해커의 접근이 매우 용이한 허니넷 형태로 허니팟 시스템을 구성하고 해커의 키 입력 하나하나를 기록할 수 있는 기능을 포함시키고자 하였다. 이하 본 논문에서 개발한 시스템을 RTHS(Real Time Honeypot System)이라 칭한다.

RTHS 는 해커의 공격을 탐지하기 위한 침입탐지 시스템과 실제 허니팟 시스템, 그리고 허니팟 시스템에서 얻어지는 각종 정보를 확인할 수 있는 관리 콘솔로 이루어져 있다.

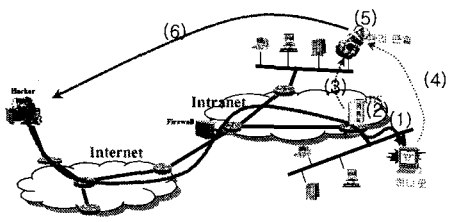


(그림 2) RTHS 구성

3.2 동작 시나리오

허니팟 시스템은 다음과 같이 동작한다.

(1) 해커에 의해 침입 발생하면,
(2) 침입 탐지 시스템에 의해 침입이 확인되고,
(3) 침입 탐지 시스템은 침입 발생 경보를 관리 콘솔 내의 로그 서버로 전송한다.
(4) 허니팟 시스템은 지속적으로 시스템 로그를 확인하고, 변경이 있는 경우, 그 내용을 관리 콘솔 내의 로그 서버로 전송하며, 해커에 의해 입력되는 각종 명령 역시 로그 서버로 전송한다.
(5) 침입탐지 시스템 및 허니팟 시스템으로부터 얻은 정보를 분석하여 보고 자료를 작성하고, 이를 실시간으로 확인 가능하도록 저장하며,
(6) 분석된 정보를 이용하여 해커의 시스템 정보를 수집하고 가능한 범위 내에서 추적을 시도한다.



(그림 3) RTHS 동작 시나리오

3.3 주요 블록 기능

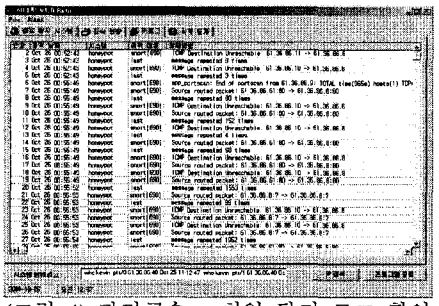
o 침입탐지 시스템

본 허니팟 시스템 구현에 있어서 가장 기본적인 모듈인 침입 탐지 모듈은 무료로 배포되고 있는 snort 를 사용하였다. Snort 를 사용함에 있어서 snort 에서 발생하는 각종 로그들은 콘솔에 포함되어 있는 로그 서버로 전송하도록 구성하였다.

o 관리 콘솔

관리 콘솔은 Visual Basic 을 이용하여 윈도우 운영체제 하에서 GUI 를 이용하여 확인하도록 구현하였으며, 침입 탐지 로그, 접속 현황, 키 로그, 침입 통계의 4 부분으로 구성하였다.

침입 탐지 로그 확인을 위해 snort 에서 발생하는 침입 탐지 로그를 관리 콘솔의 로그 서버에 저장하고, 이를 확인할 수 있도록 구성하였다.



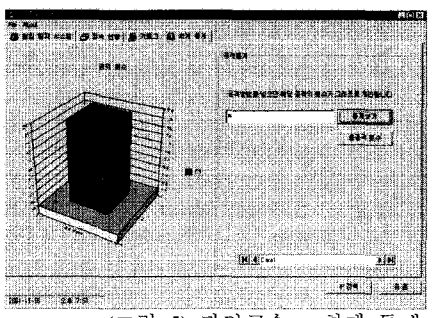
(그림 4) 관리콘솔 – 침입 탐지 로그 확인

접속 현황에서는 현재 허니팟 시스템에 접속해 있는 공격자의 ID 와 접속을 시도한 위치, 그리고 접속 시간 등을 확인할 수 있다.

키 로그는 누가 언제 어떤 명령 및 옵션을 수행했는지를 확인할 수 있도록 구성되었다.

회계 통계는 허니팟 시스템에 시도된 해킹 수법별 시도 횟수 통계자료를 확인할 수 있도록 구성하였다.

로그 서버는 MS 사의 Access DB 를 이용하여 구성하였으며, 허니팟 시스템과는 UDP 2345 포트를 이용하여 통신하도록 구성하였다. UDP 를 이용한 이유는 지속적인 연결을 유지해야 하는 TCP 에 비해 해커에 의해 확인될 확률이 매우 낮고, 로그 발생시 신속히 송신할 수 있기 때문이다.



(그림 5) 관리콘솔 – 회계 통계

관리 콘솔에서 해커의 시스템에 대한 간단한 역추적이 가능하도록 개발하였다. 관리콘솔 화면의 우측 하단에 위치한 "IP 검색" 버튼을 클릭하는 경우, 해커의 IP 주소를 이용하여 해당 IP 주소의 관리자와 위치에 대한 정보를 얻을 수 있다.

o 허니팟 시스템

허니팟 시스템은 RedHat Linux 7.1 운영체제를 이용하는 Intel Pentium3 CPU 가 탑재된 시스템에 설치하였다. RedHat Linux 7.1 은 추가적인 보안 강도 강화를 위한 패치없이 일반 배포판을 그대로 설치하였으며, 옵션 변경을 수행하지 않았다. 물론 침입 탐지와 로그 전송을 위해 침입탐지 시스템(snort)과 로그 전송 모듈은 추가 설치하였다.

허니팟 시스템에서 발생하는 각종 로그들을 수집하여 로그 서버로 전송하는 모듈로서, 침입탐지 시스템의 침입 로그기록뿐만 아니라, 허니팟 시스템 자체에서 생성되는 시스템 로그를 수집하여 전송한다. 앞서 언급한 바와 같이 관리 콘솔과의 통신은 UDP 2345 포트를 사용하도록 구현하였다.

로그 전송 모듈은 단순히 시스템의 syslogd 에 의해 발생하는 로그 기록 뿐만 아니라, 접속자 현황을 확인하기 위해, wtmp, utmp 로그 기록 역시 로그 서버로 전송하며, 해커에 의해 입력되는 명령에 대한 기록 역시 로그 서버로 전송한다.

본 시스템의 구현에 있어서 해커의 행동 양식 파악을 위한 보다 정확한 동장 상태를 확인하고자 2 가지 추가적인 작업을 진행하였다.

먼저, 해커의 명령을 옵션까지 확인하기 위한 작업이다. 해커의 명령을 확인하기 위해서 각 사용자의 홈 디렉토리에 존재하는 history 파일을 참조하려고 했으나, 이는 오직 명령부분 만이 기록될 뿐만 아니라, 정상적인 로그인이 아닌 경우, 즉 해킹에 의해 쉘이 실행되는 경우에는 명령 기록을 추출할 수 없었다. 이에, 본 구현에서는 리눅스 시스템에서 일반적으로 사용하는 기본 쉘인 bash 의 소스코드를 변형하여 해커에 의해 수행되는 모든 명령 및 옵션을 확인할 수 있도록 구성하였다.

또 다른 추가적인 작업은, 해커가 허니팟 시스템에 접속하여 시스템을 장악하더라도, 본 시스템이 허니팟 시스템임을 알 수 없도록 하기 위해 허니팟의 일부로 사용되는 각종 모듈들이 ps 명령을 통해 확인되지 않도록 ps 의 소스 코드를 수정하였다.

4. 결론

허니팟은 해커가 사용하는 해킹기법 및 해커의 행동양식에 대한 정보를 수집하여 경제적인 손실이 발생하기 이전에 새로운 해킹 기법을 방어할 수 있는 대응책을 마련할 수 있도록 하기 위한 침입유도 시스템이다. 본 논문에서는 해커의 해킹 기법과 행동양식을 실시간으로 파악하기 위한 허니넷 형태의 허니팟 시스템 RTHS(Real Time Honeypot System)를 개발하고 이를 논하였다.

본 논문에서 개발한 RTHS 는 해커의 행동을 파악하기 위한 실제 허니팟과 침입탐지시스템, 허니팟 시스템 전체를 관리하는 관리 콘솔로 구성되어 있으며, 관리콘솔에는 허니팟 시스템과 침입탐지 시스템에서 발생하는 로그를 관리하는 로그 서버가 포함되어 있다. 또한 허니팟 시스템이 해커에게 발각되지 않게 하기 위해 일반 ps 명령으로 확인할 수 없도록 수정하였으며, 해커에 의해 입력되는 명령의 옵션을 확인하기 위해 bash 를 수정하였다.

향후에는 응용 프로그램 수준에서 변경시킨 ps 와 bash 등을 커널 수준에서 처리할 수 있도록 하여야 할 것이다.

참고 문헌

[1] Lance Spitzner, Honeypots – Definitions and Value of Honeypots, Honeynet Project (http://project.honeynet.org), 2002

[2] Loras R. Even, What is a Honeypot? – Honey Pot Systems Explained, 2000

[3] Honeynet Project, Know Your Enemy: Honeynets - What a Honeynet is, its value, how it works, and risk/issues involved, http://project.honeynet.org/papers-/honeynet, 2000.

[4] NFR Homepage, http://www.nfr.com/products/bof/

[5] Specter Corp., Specter Manual, 2002, http://www.specter.ch/introduction50.shtml

[6] SANS Institute. http://www.sans.org/

[7] Security focus. http://www.securityfocus.com

[8] Fred Cohen, Deception Toolkit, http://www.all.net/dtk

[9] http://www.recourse.com/product/ManTrap/

[10] Honeynet Project, Know Your Enemy : Honeynets – What a Honeynet is, its value, how it works, and risk/issues involved, http://project.honeynet.org, 2002

[11] Lance Spitzner, To Build A Honeypot, Honeynet Project, 2000

[12] 유닉스 로그분석을 통한 침입자추적 및 로그관리 Part 1/2, 한국 정보보호 진흥원, 2001

[13] Lance Spitzner, Watching Your Logs, Honeynet Project, 2000, http://www.enteract.com/~lspitz/swatc- h.html