보안솔루션에 대한 우회 공격 기법 연구

손태식*, 김진원*, 박일곤*, 문종섭*, 박현미**, 김상철**

*고려대학교 정보보호대학원, **한국정보보호진흥원

A Study on the Evasion Techniques of Security Solutions

Tac-Shik Sohn*, Jin-Won Kim, Il-Gon Park, Jong-Sub Moon, Hyun-Mi Park, Sang-Cheol Kim

*GSIS, CIST, Korea Univ, **KISA

요 약

IDS, Firewall 등의 보안도구들은 보편화되어 있는 보안 솔루션이다. 시스템의 보안을 책임지는 이러한 도구들이 보안상 문제점(즉, 우회 공격 가능성)을 가지고 있다는 것은 보안에 있어 근본적인 부분이 취약성을 내포하고 있는 것과 같다. 그러므로 시스템 및 네트워크에 대한 새로운 보안 기법을 연구하기에 앞서 현재의 보안 솔루션들이 가지고 있는 우회공격과 같은 위험성을 해결하는 것 필수적이다. 따라서 본 논문에서는 일반적으로 사용되는 보안 솔루션들에 대한 우회 공격 기술 분석 및 대응 방안에 관한 연구를 수행한다.

I. 서론

정보화의 역기능과 함께 현재 심각한 사회문제로서 대두되고 있는 해킹과 같은 시스템 및 네트워크에 대한 불법적인 침해 문제의 대응방안으로서 Firewall, IDS와 같은 보안도구가 개발되었다. Firewall은 일명 "방화벽"이라 불리며 인가되지 않은 사용자에 대해서 시스템이나 네트워크에 대해서 원천적인 접근 제어를 수행하는 보안도구이며, IDS는 시스템이나 네트워크에 대하여 비정상적인 행위를 탐지해내고 관리자에게 경고를 보내주는 보안도구이다. 현재 이러한 보안도구는 다수의 기업, 기관에서 실치되어 사용되고 있으며, 실제로 2005년까지의 전 세계적 시장 규모는 약 40억 달러로서 보안 서비스를 제외한 전체 보안 도구 시장의 1/4정도를 차지한다.

하지만 이렇게 Firewall과 IDS가 일반적인 정보보호 솔루션으로서 대다수의 네트워크 및 시스템의 보안을 책임지고 있다보니 이러한 보안 도구를 우회하여 공격할 수 있는 여러 우회 기법들이 현재 문제점으로 대두되고 있다. 특히 이러한 보안도구에 대한 우회 공격은 일차적으로 해당 시스템 및 네트워크를 관리하는 관리자의 관리 부족이 근본적인 원인을 제공하고 있으며, 또한 보안도구의 잘못된 정책 실정에 의한 우회 공격, IP fragmentation과 같은 통신 프로토콜의 취약성을 이용하는 우회 공격, 침입탐지시스템의 오류 판정을 이용한 우회 공격 등이 널리 사용되고 있다.

따라서 본 논문에서는 보안도구에 대한 우회 공격 기법을 분석하고 해당 기법을 시뮬레이션하여 그 대응방안에 대하여 연구한다.

II. 우회 공격 기법

1. IDS 우회 공격 기법 개요

IDS에 대한 우회 공격은 현재 대부분의 IDS에서 사용하고 있는 스트링 패턴매칭 기법의 취약성을 이용하는 방법이 가장 일반적이며 또한 현재는 TCP/IP상의 프로토콜 특성을 이용한 fragmentation 기법이나 Covert Channel 형성의 방법 등도 사용된다. 또한 IDS의 가용 자원을 고갈시켜 IDS의 정확한 공격 판단을 어렵게 만드는 DoS 공격도 널리 사용되고 있는 실정이다.

일반적으로 IDS들은 스트링 패턴매칭 기법으로 침입을 판단하기 때문에 IDS의 룰 데이터베이스에 정의되지 않은 침입에 대해서는 탐지할 수 없게 되는 것이 이러한 취약성이 IDS 우회 기법에 널리 사용되게 된다.

2. 방화벽 우회 공격 개요

방화벽은 방화벽 시스템이 네트워크 환경에 적용되어진 이후 지금까지 해킹에 대해서 비교적 안전하게 네트워크를 보호해 왔다. 그러나 현재 나와 있는 모든 방화벽이 보안에 있어 안전하다고 할 수는 없다. 게다가 설치되어있는 방화벽 대부분이 잘못 설정되어 있거나 관리가 제 대로 이루어지지 않아서 해커들에게 무방비로 열려있다. 최적화되고 강력한 보안정책이 유지되는 방화벽은 뚫고 들어가기가 거의 불가능하다. 대부분의 해커들은 이러한 사실을 알고 있으며 이러한 방화벽의 뒤를 공격하기 위해 방화벽을 우회하거나, DoS 공격 등을 이용하여 방화벽을 무력화시킨다.

3. 우회 공격 기법 분류

다음의 표 1은 현재 널리 사용되는 표 2의 우회공격 기법들을 사용하는 우회 공격도구들의

특성을 분류한 것이다.

[표 1] 우회 공격 도구

Tools	Description
Stick	Insertion/Evasion/DoS
Loki2	Covert Channeling
Mendax v.0.7.1	TCP DeSynchronization
Snot 0.91	Insertion/Evasion/DoS
Sidestep	Insertion/Evasion
TWWWscan v1.2	Insertion/Evasion
Babelweb v1.0	Insertion/Evasion
fragrouter	Evasion - Fragmentation
fscan 1	Insertion/Evasion
infinity-t-3	Insertion/Evasion/DoS
whisker 1.4	Insertion/Evasion
Mutate 2	Insertion/Evasion/DoS
Malice 6.1	Insertion/Evasion/DoS

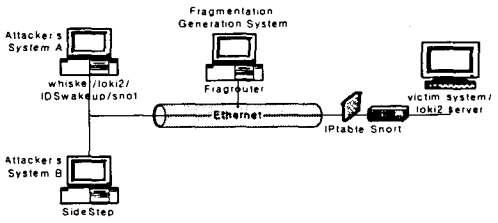
아래의 표 2는 보안도구들의 패킷 캡쳐 특성이나 TCP/IP 프로토콜 특성 보안도구 취약성, 사회공학기법 등 크게 5가지 대분류를 통하여 우회 공격 기법들을 분류한 표이다.

III. 우회 공격 시뮬레이션

우선 모든 시뮬레이션은 일반적인 인터넷 환경의 리눅스 시스템에서 실행되었다. 그림 1은 전체 시뮬레이션 구성도 이다. 그림 1의 전체 구성도와 같이 대부분의 우회 공격 도구는 리눅스가 설치된 공격 시스템(Attacker's System A)에 설치되어 역시 리눅스가 설치된 공격 대상 시스템(Victim System)을 공격하였으며, fragrouter의 시뮬레이션의 경우에는 공격 시스템 외에 fragrouter를 설치하여 특정 명령해 의해 다양한 frag 패킷들을 발생하기 위한 전용 시스템(Fragmentation Generation System)을 따로 구축하였다.

[표 2] 우회 공격 기법

대분류	특성 분류	유형에 대한 공격 기법	
Packet Filtering/Sniffering에 의한 분류	Insertion	Unicode	Long URL
			UTF encoding
		TCP/IP	FIN,RST spoofing
			Data Spoofing
	Evasion	Unicode	Method Matching
			Sessing Splicing
		Fragment	Tiny Frag
			Overlap
	DoS	Resource Exhaustion	Smurf
			Jolt3
		Abusing Reactive IDS	land
			Syn flood
TCP/IP 프로토콜 분류	Network Layer	Simple Insertion Attacks	
		MAC Address	
		IP Fragmentation	
	Transport Layer	Simple Insertion Attacks	
		TCB Creation - DeSync	
		TCP Stream Reassembly	
		TCB Teardown	
Vulnerability에 의한 분류	IDS	input data error	
		configuration error	
		Uni code parcing error	
	Firewall	exceptional handling error	
		acl control error	
		configuration error	
	Router	configuration error	
		exceptional handling error	
		acl control error	
Social Engineering 기법 분류	E-mail		
	Dumpster Diving		
	Office Snooping		
그 외 분류	Firewall		
	Backdoor		



[그림 1] 우회 도구 공격 시뮬레이션 전체 구성도

1. Covert channel 개요

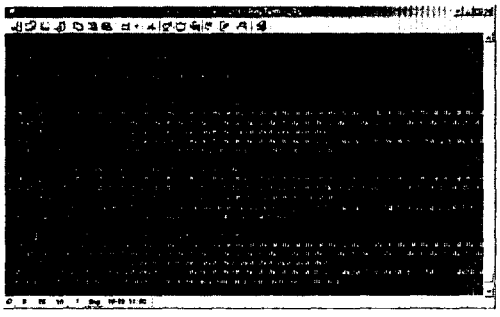
임의의 공격자가 시스템에 백도이를 실치하고 시스템 로그에 남겨진 정보를 전부 삭제했다면 그 이후로 공격자는 해당 시스템에 대한 시스템을 제어할 수 있는 악의 적인 프로그램과 통신할 수 있단 수단을 가질 수 있다. 이러한 수단은 IDS와 같은 시스템의 탐지를 회피하기 위해서 공

사자는 네트워크를 통해 백도어 프로그램과 통신을 제공하는 방안의 기반이 된다. 이러한 통신 과정을 숨기는 방법을 은닉 채널(Covert Channel)이라고 한다. 은닉 채널은 데이터를 숨길 때에 필수적인 것이다. 수학적으로 데이터를 암호화하는 것은 상대가 내용을 이해할 수 없도록 하는 것이지만 은닉 채널은 상대가 처음부터 해당 데이터를 발견하지 못하도록 만드는 것이다. 공격자들은 데이터를 숨기는 것과 암호화하는 것을 같이 이용 한다.

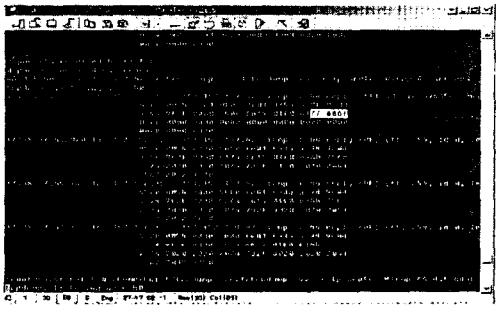
2. Covert Channel - Loki2

Loki2를 이용한 ICMP Coverchannel을 통한 IDS 및 방화벽 우회 공격의 수행에 대해서 "ps", "who" 등의 명령을 사용하여 IDS가 설치된 시스템에 대해서 테스트 해 보았다.(그림 2참조) 우선 Loki2 서버는 보안도구로 보호되는 대상 시스템에 설치되어 있어야 하며 이러한 Loki2 서버에 대해 외부의 클라이언트가 특정 명령을 내리게 되면 Loki2 서버는 클라이언트의 요구에 따른 명령 실행 결과를 보여주게 된다. 이러한 공격은 ICMP 패킷의 페이로드 부분에 포함되므로 일반적인 IDS나 방화벽으로는 탐지가 어렵다.

역시 테스트에 사용된 snort 1.8.7과 IPTable 1.2.5에서는 Loki2의 우회 공격을 탐지하지 못하였다. 이러한 결과는 피해시스템에서 공격 명령어를(본 시뮬레이션의 경우 "who") 포함하고 있는 icmp의 tcp 덤프를 통해서 확인할 수 있다.(그림 3참조)



[그림 2] loki2 테스트 화면 - who



[그림 3] victim 시스템에서의 icmp 패킷 덤프 화면

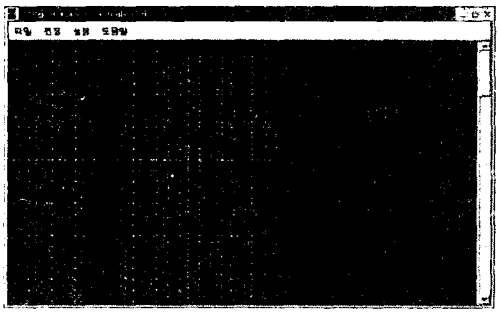
3. fragment 공격 개요

IP fragmentation은 물리적인 네트워크 인터페이스의 MTU에 맞게 패킷을 다중 데이터그램으로 나누어준다. 전형적으로 TCP는 mtu를 알고 있으며 IP 레벨에서 분할이 필요한 패킷은 보내지는 않는다. 스니퍼와 IDS를 혼란스럽게 만들기 위해 이것을 이용할 수 있다. fragmentation과 연관된 몇몇 잠재적인 공격들이 있다. 한 개의 패킷에 TCP헤더의 처음 8바이트, 나머지 데이터들은 32바이트 패킷들에 나누어 보낼 수 있다. 이것은 네트워크 분석 도구를 속일 수 있는 많은 능력들을 제공한다. 첫째로 스니퍼/IDS는 fragment의 재조합하는 능력이 있어야 할 것이다. 둘째로 분할된 TCP헤더들을 처리 할 수 있는 능력이 있어야 할 것이다. 이 간단한 기술은 패킷들을 대부분의 데이터링크 레벨 네트워크 모니터들을 통과하기에 충분하다는 것이 판명되었다.

4. Fragmentation - fragruter

본 시뮬레이션에서는 임의의 크기로 fragment 패킷을 생성하는 fragrouter를 사용하여 테스트하였다. fragrouter 프로그램을 이용한 공격은 첫번째로 공격자가 fragrouter에서 공격자의 패킷을 입력으로 받도록 공격자 자신의 기본 라우터를 fragrouter로 설정한다. 두 번째는 fragrouter의 기본 라우터를 침입하고자 하는 공격대상 시스템이 포함되어 있는 네트워크상의 라우터로 설정한다. 세번째는 fragrouter가 공격자의 패킷을 입력받아 단지 단편화만을 수행했기 때문에 공격대상자의 응답은 fragrouter를 거치지 않고 직접적으로 공격자에게 전달된다.

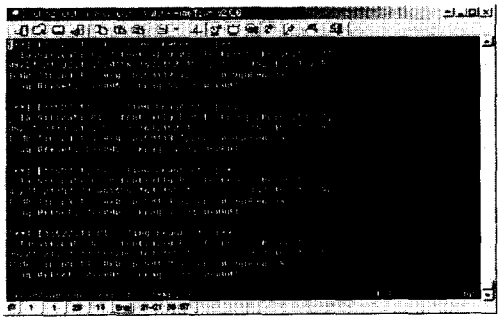
다음의 그림 4는 fragrouter의 일반적인 단편화 옵션을 사용한 공격 패킷 생성에 관련된 그림이며, 이러한 공격에 대한 IDS의 탐지는 다음의 그림 5에서 알 수 있다.



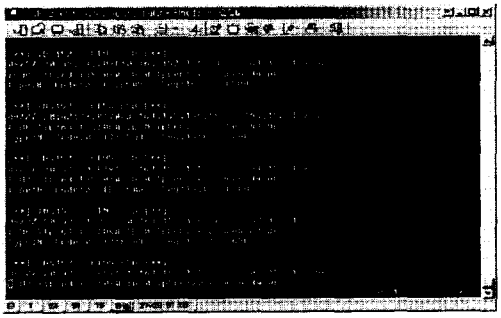
[그림 4] Fragrouter 패킷 생성

현재 테스트된 snort 1.8.7에서는 fragrouter의 F1~5의 단편화 옵션에 대한 공격을 탐지하는 것을 알 수 있지만 그 외 TCP 3WH와 함께 이루

어지는 단편화 공격에 대해서는 아직까지 정확하게 탐지하지 못하는 것을 알 수 있었다. (그림6참고)



[그림 5] fragrouter의 -F옵션을 사용



[그림 6] Snort 탐지 화면

또한 같은 Snort에서도 개발 버전에 따라 fragment 패킷을 처리하는 방식이 다음의 표 3과 같이 차이를 가지고 있었다.

[표 3] snort 버전별 defragmentation 기능 비교

	Snort ver 1.7	Snort ver 1.8
발표 시점	2000년	2001년 07월
defragmentation	minfrag, defrag	frag2
defrag rule	X	O
기타	구현미비	패킷 버퍼링 기능

IV. 탐지 방안

본 논문에서의 우회 공격 기법에 대한 시뮬레이션 결과 일반적으로 널리 알려진 DoS 도구들이나 웹서버 인코딩 룰을 이용하는 방법 등에 대해서는 공개 IDS로서 사용되는 snort를 통해서도 쉽게 탐지가 됨을 알 수 있었다. 하지만 그 외 변형된 fragment를 이용하는 방법이나 은닉채널 등을 이용하는 방법은 현재의 룰 매칭 IDS로는 탐지가 어렵다. 따라서 본 논문에서는 패턴 매칭 기법의 우회 공격 탐지 방안 및 신경망 기반의 탐지 방안을 제안한다.

1. 패턴 매칭 기반

패턴 매칭 기반의 탐지 방안은 널리 사용되는 도구들이나 공격 기법에 의한 우회 공격의 경우에 그 도구나 기법의 특성을 바탕으로한 탐지룰을 만들어 대처하는 것이다. 이러한 방안의 예시는 FTP의 "cd ~root" 와 같은 공격에 대해서 아래와 같이 변형된 룰을 사용함으로써 대처할 수 있음을 알수 있다.

Current Snort rule

alert tcp SEXTERNAL_NET any -> SHOME_NET 21 (msg:"FTP-cwd~root"; flags:PA; content:"cwd ~root"; nocase;)

Rule for evaded content:

alert tcp SEXTERNAL_NET any -> SHOME_NET 21 (msg:"FTP-cwd~root"; flags:PA; content:"c|FF F1|wd ~|FF F1|ro|FF F1|ot"; nocase;)

2. 신경망 기반

은닉채널 생성이나 fragment와 같은 공격의 경우 아래와 같이 일반적인 패킷의 경우(정상 행위)를 학습하여 패킷 페이로드를 통한 은닉 채널 형성(비정상 행위), 비정상적인 패킷 분할과 같은 경우를 탐지하는 신경망를 사용하는 방안을 제시할 수 있다.

은닉 채널 공격의 학습 데이터

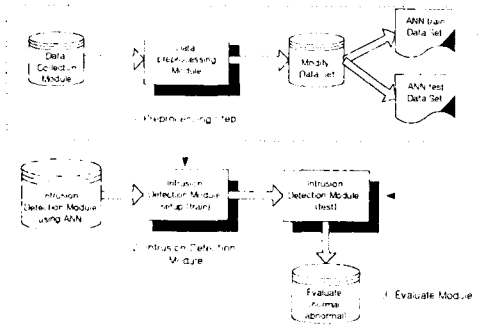
정상 ICMP 패킷
- Ping 프로그램을 사용한 정상 패킷 생성

비정상 우회 공격 패킷
- Loki2를 이용한 우회 공격 패킷 생성
- 여러 쉘 명령이 포함된 Loki2 생성 ICMP 패킷

fragmentation 공격의 학습 데이터

정상
-ICMP request 패킷

비정상 패킷
-Fragrouter를 이용한 비정상 ping fragment 패킷
-frag1:비정상적으로 분할된 tiny fragment 공격
-frag3:tiny fragment + 순서가 변경된 패킷 사용
-frag4:tiny fragment + teardrop 공격
-frag5:tiny fragment + 순서 변경 패킷 + teardrop 공격



[그림 7] 신경망 탐지 구성도

V. 결론 및 향후 연구 방향

현재 사용되는 대부분의 우회 도구 공격 기법들은 대부분이 IDS에 초점을 두고 있지만, IDS에 우회를 목적으로 하는 도구일지라도 사용되는 우회 기법의 특성상 패킷 필터링에 기반한 보안 도구인 경우에 IDS, FW 등의 구분은 큰 의미가 없다. 또한 TCP/IP 프로토콜의 디자인 특성을 이용한 Covert Channel 우회 기법은 어떤 보안 도구를 사용하여 대비한다라도 생성되는 Covert Channel의 특성을 파악하지 못한다면 우회 공격에 대해 특별한 대응 방안을 마련하기 어렵다.

따라서 일반적으로 알려진 기법에 대해서는 snort 탐지룰과 같은 패턴 매칭 기법을 사용하며 그 외 은닉 채널등 그 공격 특성에 있어 비정상 패턴을 찾아내기 어려운 기법은 정상행위 학습을 통한 신경망 기법을 적용하는 것이 필요하다.

향후에는 우회 기법에 대한 탐지룰 작성과 신경망 기법 적용에 대한 보다 깊은 연구가 필요하다.

참고문헌

[1] Thomas H.Ptacek, Timothy N.Newsham "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection", January 1998,

[2] Fred Cohen, 50 ways to defeat your intrusion Detection System http://all.net/

[3] Haken Kvarnstrom, "A Survey of commercial tools for intrusion detection, http://www.ce.chalmers.se/staff/hkv/IDS_Survey-99.pdf

[4] Coretez Giovanni, "Passive Mapping: An offensive use of IDS", http://www.eurocompton.net/stick/papers/OffensiveUseofIDS.pdf

[5] Insecure.org. "Top 50 Security Tools". August 19, 2000 URL: http://www.insecure.com/tools.html

[6] Goldsmith, David and Schiffman, Michal. "Firewalking: A Traceroute-Like Analysis of IP Packet Responses to Determine Gateway Access Control Lists". October 1998. URL: http://www.packetfactory.net/firewalk/firewalk-final.html

[7] Graham, Robert. "FAQ: Firewalls: What an I seeing?". January 15, 2000.

[8] Greg Hoglund, Jon Gary. "Multiple Levels of De-synchronization and other concerns with testing an IDS system". August, 2000. http://online.securityfocus.com/infocus/1204

[9] IDS Evasion Techniques and Tactics, Kevin Timm, May 7, 2002, http://online.securityfocus.com/infocus/1577

[10] IDS Evasion with Unicode, Eric Hacker, Jan. 3, 2001,