네트워크 보안 시뮬레이터에 관한 연구

서정택[0] 윤주범 임을규 이철원
국가보안기술연구소
{seojt[0], netair, imeg, cheolee}@etri.re.kr

Study on the Simulator of Network Security

Jung-Taek Seo[0] Joo-Beom Yun Eul-Gyu Im Cheol-Won Lee
National Security Research Institute

요 약

네트워크 상의 사이버 공격에 대한 시뮬레이터 개발을 위해서는 다양한 네트워크 구성요소의 특성을 시뮬레이션 모델에 반영할 수 있어야 하며, 다양한 사이버 공격과 이를 방어하기 위한 보안대책들의 특성을 반영할 수 있어야 한다. 본 논문에서는 네트워크 상의 사이버 공격과 방어를 시뮬레이션 하기 위하여 다양한 공격과 방어기법을 표현하기 위해 공격 및 방어 DB를 설계하고, 시뮬레이션 수행시 행동을 표현할 actor를 설계하고, 이를 이용한 공격 및 방어 시나리오 DB를 설계하고, 이들을 이용한 시나리오 생성기를 설계한다. 본 논문에서 제시한 방법을 이용하여 다양한 네트워크 구조와 보안대책을 가진 네트워크에 대한 사이버 공격 및 방어 시뮬레이션이 가능하며, 이를 통하여 네트워크에 적용된 보안대책의 적절성 파악 및 사이버 공격으로 인한 네트워크의 피해 및 피해영향 파악 등으로 확장이 가능하며, 사이버 공격에 대한 적절한 보안대책을 수립하는데 도움을 줄 수 있다.

1. 서론

네트워크 보안 시뮬레이터 개발은 실세계에서 발생하는 사이버 공격과 방어에 대한 기반 연구이다. 그러나, 네트워크의 방대함, 사이버 공격과 방어의 복잡성과 다양성 등으로 인하여 아직까지 연구의 진전이 없는 상태이다. 특정 사이버 공격에 대한 네트워크 행동변화와 방어를 위한 보안시스템들의 성능을 관찰하는 방법이 가장 좋은 방법이다. 그러나, 모든 발생 가능한 공격을 시도하고, 보안시스템들의 설정을 바꾸어 가며 시험하기에는 현실적으로 많은 제약이 따른다. 이에 대한 좋은 대안으로 시뮬레이션 기법을 이용하는 방법이 있다.

사이버 공격 및 방어를 수행하고 이에 따른 네트워크 행동변화를 시뮬레이션하기 위해 본 논문에서는 대규모 네트워크에서의 공격과 이에 따른 네트워크 행동의 시뮬레이션 기반 구축을 위해 공격 및 방어 DB를 설계하고, 시뮬레이션을 위한 Actor를 설계하고, 공격 및 방어 시나리오 DB를 설계하고, DML 변환기를 이용하여 SSFNet 상에서 시뮬레이션 가능한 형태로 변환하는 각 모듈을 설계하며, 네트워크 보안 시뮬레이터 전체 구성을 제시한다.

2. 네트워크 보안 시뮬레이터

2.1 공격 및 방어 DB

공격 및 방어 DB는 정보전 시뮬레이션에서 사용되는 공격 및 방어에 대한 모형을 저장하는 DB로 공격 및 방어, 호스트, 서비스 등 세 가지로 구분하여 연구 개발한다.

1) 실세계에 사용되는 단위 공격 기술과 단위 방어 기술을 분석정리 한다. 공격자가 목표 시스템을 공격하여 관리자 권한을 획득하기 위하여 IP 주소 획득 시도, 운영체제와 서비스 정보를 얻고자 하는 스캐닝 공격, exploit code를 이용한 공격, buferoverflow 공격, Password cracking 공격 등의 다양한 단위 공격을 시도하게 되며, 관리자 권한을 획득하고 나면 다음 침입을 위하여 backdoor나 rootkit을 설치하게 되는데 이러한 기법들이 각각의 단위공격이 된다. 또한, 공격에 대한 대응방안으로 외부로부터의 접점에 침입차단시스템을 설치하여 공격에 대하여 차단하는 기법, IDS를 설치하여 공격에 대하여 탐지하는 기법 등이 단위방어가 된다.
2) 효과적인 시뮬레이션을 위하여 단위 호스트시스템에 대한 기술이 필요하다. 범용시스템, 라우터, 침입차단시스템, IDS 중에 어느 시스템인지, 호스트에 대한 정보로 동시접속 connection 수, 메모리 크기, 운영체제의 종류 및 버전, 열린 port 현황 등에 대한 정보를 기술한다.
3) 대부분의 공격이 대상 호스트의 특정 서비스를 이용하는 경우가 많다. 따라서, 호스트에 동작중인 서비스와 해당 서비스와 관련되는 취약성, 취약성을 이용한 공격기법 등에 대하여 기술한다.

2.2 Actor

시뮬레이션을 수행할 때 그들의 행동을 대변할 프로그램으로 공격 및 방어 actor를 java로 작성하여 DB에 수록한다.

Actor의 속성은 다음과 같이 설계한다.

- 설명 : 각 공격과 방어 기법에 대하여 설명한다.
- 특성 : 공격이나 방어 기법에 관련되는 취약성으로써 취약성 DB에 기술된 주요 특성을 기술한다.
- 분류 : 서비스거부공격, 관리자 권한 획득을 통한 정보유출 공격, 인터넷 웜 공격 등으로 분류하여 기술한다.
- 도구 : 공격이나 방어 기법에 사용되는 도구에 대한 설명이다.
- 환경 : 공격이나 방어가 이루어지기 위한 환경에 대한 기술이다.

2.3 공격 및 방어 시나리오 DB

공격 및 방어 시나리오 DB는 공격 및 방어 DB에 저장된 단위 공격 및 방어 기술의 조합으로 이루어지게 된다. 하나의 공격 시나리오의 예를 보면 다음과 같다.

1) Social Engineering 기법 및 nslookup 명령어 등을 이용하여 목표 호스트의 IP Address 정보를 획득한다.
2) Nmap 및 SuperScan 등의 도구를 이용하여 목표 시스템의 OS 정보 및 열린 포트를 검색하고, 실행중인 서비스에 대한 정보를 획득한다.
3.1) 서비스의 취약점을 이용한 공격으로 Bufferoverflow 공격, Formatstring 공격, 설정오류를 이용한 공격 등을 사용하여 관리자 권한을 획득한다.
3.2) 취약한 계정에 대한 공격으로 Bruteforce 공격, Password cracking 공격 등을 사용하여 일반사용자 계정에 대한 정보나 관리자 Password 정보를 획득한다.
4) 목표 시스템의 관리자 권한을 획득한 후, 다음의 침입을 용이하게 하기 위한 Backdoor 프로그램을 설치하거나, 침입에 대한 은닉을 위하여 Rootkit을 설치하거나, 목표 시스템 주변의 다른 시스템에 대한 공격을 위하여 sniffer 프로그램을 설치한다.

공격 시나리오 DB의 속성은 다음과 같다.

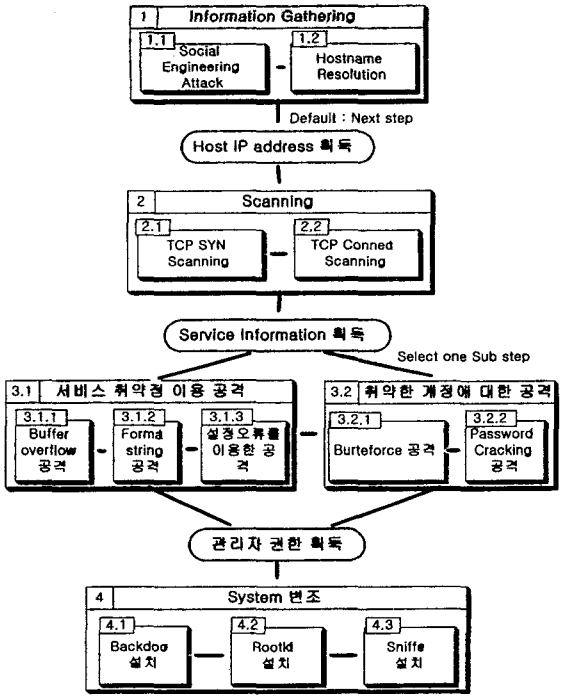
1) Step : 단위 공격의 순서이다.
2) action : 단위 공격 DB에 수록된 이름으로서 단위 공격의 종류를 구별하기 위하여 사용된다.
3) Purpose : 단위 공격 각각에 대한 공격 목적이다.
4) use : 단위 공격을 성취하기 위하여 사용되는 구체적 공격을 의미한다.
5) precondition : 단위 공격 수행 이전의 상태이다.
6) postcondition : 단위 공격 수행 이후의 상태이다.

다음 표는 앞에서 설명한 공격시나리오의 DB이다.

<표> 관리자 권한 획득 공격 시나리오 테이블

Step	Action	Purpose	Use	Precondition	Postcondition
1	Information Gathering	get Host IP address	1.1, 1,2	Start	got Host IP address
1.1	Social Engineering Attack	get Host IP address	Web page, Person	Start	got Host IP address
1.2	Hostname Resolution	get Host IP address	nslookup command	Start	got Host IP address
2	Scanning	get Service Information	2.1, 2.2	got Host IP address	got Service Information
2.1	TCP SYN Scanning	get Service Information	Nmap SuperScan	got Host IP address	got Service Information
2.2	TCP Connect Scanning	get Service Information	Nmap SuperScan	got Host IP address	got Service Information
3.1	Exploit Vulnerable Service	get Higher Privilege	3.1.1, 3.1.2, 3.1.3	got Service Information	got administrator Privilege
3.1.1	Buffer overflow Attack	get Higher Privilege	Exploit code	got Service Information	got administrator Privilege
3.1.2	Formatstring Attack	get Higher Privilege	Exploit code	got Service Information	got administrator Privilege
3.1.3	Misconfiguration Attack	get Higher Privilege	Webboard file upload exploit	got Service Information	got administrator Privilege
3.2	Vulnerable Account use Attack	get Higher Privilege	3.2.1, 3.2.2	got Service Information	got administrator Privilege
3.2.1	Bruteforce Attack	get Higher Privilege	Bruteforce Program	got Service Information	got administrator Privilege
3.2.2	Password Cracking Attack	get Higher Privilege	P/W Cracking Program	got Service Information	got administrator Privilege
4	System Disguise	Next Attack, System Occupation	4.1, 4.2, 4.3	got administrator Privilege	End
4.1	Backdoor install	Next Connection	Bo2k	got administrator Privilege	End
4.2	Rootkit install	Intrusion Hiding	t0rn, lkm	got administrator Privilege	End
4.3	Sniffer install	Psssword Capturing	Dsniff	got administrator Privilege	End

다음 [그림 1]에서 공격시나리오 테이블의 시나리오를 트리구조로 표현한다.



[그림 1] 관리자 권한획득 공격 시나리오 tree

2.4 공격 및 방어 시나리오 생성기

시뮬레이션을 수행하기 위하여 공격 및 방어 시나리오를 기술하기 위한 High level의 인터페이스 및 시나리오 Editor를 개발한다.

시나리오 생성을 위한 Editor에서는 다양한 공격 및 방어 시나리오를 작성하거나 공격 및 방어 시나리오를 작성 가능하도록 다양한 기능을 제공한다. 시뮬레이션에 사용할 네트워크의 구성을 지정하고, 공격 및 방어 시나리오를 구성하게 된다.

2.5 DML 변환기

시나리오 생성기에서 생성된 시나리오에 따라 시뮬레이션을 수행하기 위해 해당 actor가 실행되어야 한다. SSFNet이 JAVA로 작성되어 있으므로 모든 actor는 JAVA로 작성되어 SSFNet에서 실행된다. 또한, 시뮬레이션이 수행되면서 실행되는 actor들이 필요로 하는 값들은 사용자가 Editor를 통하여 입력하게 된다.

2.6 SSFNet 확장

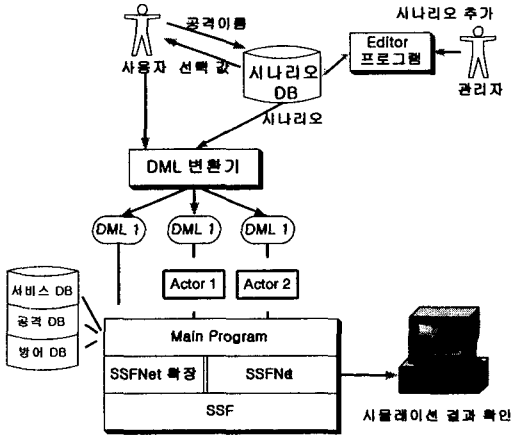
네트워크 공격 및 방어 시뮬레이션이 수행되는 SSFNet이 가지고 있는 한계점들이 있어 이에 대한 확장이 필요하다. 효과적인 네트워크 보안 시뮬레이션을 위하여 브로드캐스팅을 구현해야 하며, 호스트의 운영체제 및 서비스를 표현해야 하며, 다양한 공격에 필요한 라이브러리를 추가 구현해야 한다.

2.7 네트워크 보안 시뮬레이터 전체 구조

사용자는 시나리오 editor를 사용하여 단위공격 및 방어 actor를 기술하고, 공격 및 방어 시나리오를 작성하고, 시뮬레이션 환경을 설정한다. 환경으로는 시뮬레이션이 수행될 네트워크 구성, 공격 및 방어 actor에게 전달될 인수값 등이 된다.

시뮬레이터 main module은 시뮬레이션 환경을 입력으로 받아 DML 변환기를 통하여 DML로 변환한 후, 문법상 error가 없음을 확인한 후 시뮬레이션을 수행한다.

네트워크 보안 시뮬레이터 구조도는 다음 [그림 2]와 같다.



[그림 2] 네트워크 보안 시뮬레이터 구조도

3. 결론

본 논문에서는 실세계의 사이버공격 및 방어를 시뮬레이션 하기 위한 네트워크 보안 시뮬레이터 개발에 대한 연구내용을 제시하였다. 제시한 방법을 이용하여 다양한 사이버공격 및 방어에 대한 표현이 가능하며, 공격에 대한 파급효과를 확인할 수 있다.

또한, 네트워크에 적용된 보안대책의 적절성 파악 및 사이버공격으로 인한 네트워크의 피해 및 피해영향 파악 등으로의 확장이 가능하며, 사이버공격에 대한 적절한 보안대책을 수립하는데 많은 도움을 줄 수 있다.

참고문헌

[1] Mostow, J., Roberts, J., and Bott, J., "Integration of an Attack Simulator in an HLA Environment," Proc. IEEE Systems, Man, and Cybernetics Workshop, West Point, NY, June 2000.

[2] Donald Welch, Greg Conti, Jack Marin, "A Framework for an Information Warfare Simulation," Proc. IEEE Workshop on Information Assurance and Security, June 2001.

[3] James H. Cowie, Editor, "Scalable Simulation Framework API Reference Manual", version 1.0, Documentation draft, 1999.