해킹 기법을 이용한 내부망 보안 평가 방법

서 동 일[†] · 최 병 철[††] · 손 승 원[†††] · 이 상 호[††††]

요 약

본 연구는 해킹 기법을 이용한 실질적인 내부 네트워크의 보안 수준을 평가하는 방법을 제시하였다. 제안하는 방법은 기본적인 네트워크 모델을 지대별 및 공격 경로로 분리한 후, 해킹 및 해커 수준의 분류를 바탕으로 한 해킹 시나리오 분석에 의해서 내부 네트워크를 평가하도록 구성하였다. 따라서, 본 연구는 네트워크 모델과 해킹 시나리오의 두 가지의 기준에 따라 실질적인 내부망의 보안 수준을 평가하는 방법이다. 이러한 적극적인 보안 수준 평가 방법의 목적은 실제적인 내부망의 보안 수준을 평가하여 네트워크 구축 및 유지 보수에 필요한 보안성의 강화를 추구하고자 한다. 본 논문에서는 ISL1~ISL5의 5개 등급으로 보안 수준을 분리하였으며, ISL5의 보안 수준을 가장 고수준으로 평가하였다. 본 연구에서는 ISL3용 테스트베드를 설계하고 분석하였다.

Intranet Security Evaluation Using Hacking Techniques

Dong-Il Seo[†] · Byeong-Choel Choi[††] · Sung-Won Sohn[†††] · Sang-Ho Lee[††††]

ABSTRACT

In this paper, we proposed the ISL for evaluating the security level of Intranet. This method is composed of two parts : First, Hacking Scenarios are the hacking stories by hacking/hackers levels. Second, Network Model is composed of the zone and intrusion paths. Our method is very active and practical. We divide ISL into five levels : ISL1~ISL5. Among the levels, ISL5 is the highest security level. Main purpose of this paper is to promote the security of Intranet. In this paper, we designed and analyzed the test-bed for ISL3.

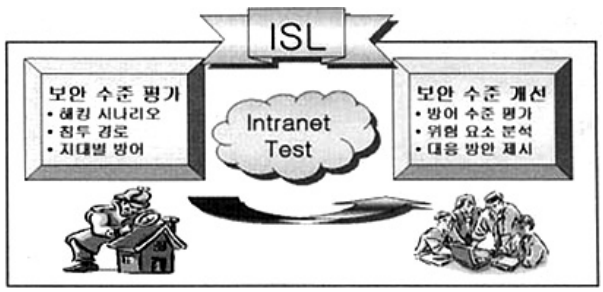
키워드 : 내부망 보안 수준(ISL : Intranet Security Levels), 해킹 수준(Hacking Levels), 네트워크 모델(Network Model), 해킹 시나리오(Hacking Scenarios)

1. 서 론

정보 산업의 발전과 더불어 정보화의 역기능의 심각성이 부각되고 있는 현 시점에서, 기업 및 기관의 해킹 사고가 증가하고 있으며, 이에 대한 근원적인 대책이 시급한 실정이다. 이를 위해서 많은 기관 및 기업에서 침해사고 대응팀을 운영하고 있지만 이것은 수동적인 대응 방안이다. 따라서, 근원적으로 내부망의 보안 수준을 평가하고 개선을 하여, 해킹 사고의 발생을 미연에 방지할 수 있는 방법이 필요하다고 판단된다[1, 8, 9]. 따라서, 네트워크 및 시스템의 보안 수준을 평가하고 이에 대한 보안 체제를 갖추는 것이 중요하며, 최근에 이러한 연구가 많이 진행되었으며, 이와 관련한 연구로는 TNI, BS7799, SSE-CMM 등이 있다[3-7].

본 연구에서는 해킹 및 해커의 수준 분류[2]에 따른 해킹 시나리오의 분석과 네트워크 테스트 모델의 제시를 통한 내부망의 보안 수준의 평가 방법을 제안하였다. 또한 평가 결과를 바탕으로 내부망의 위험 수준 분석 및 대응 방안을 제시하였다. (그림 1)은 본 연구에서 제안한 내부망 보안 수준 평가의 전체적인 개념 및 목적을 나타낸 것이다.

제 2장에서는 본 연구와 관련된 TNI, BS7799, SSE-CMM에 대해서 언급하고, 제 3장에서는 제안한 내부망 보안 수준(ISL) 평가 방법에 대한 자세한 설명을 하였다. 제 4장에서는 일반적인 테스트베드를 설계하고 분석하였으며, 제 5장에서 결론을 내렸다.



(그림 1) 내부망 보안 수준 평가 개요 및 목적

2. 관련 연구

2.1 TNI

TNI(Trusted Network Interpretation of TCSEC)는 네트워크를 평가하기 위해서 TCSEC을 네트워크 시스템에 적

† 종신회원 : 한국전자통신연구원 선임연구원
†† 정 회 원 : 한국전자통신연구원 연구원
††† 정 회 원 : 한국전자통신연구원 책임연구원
†††† 종신회원 : 충북대학교 컴퓨터과학과 교수
논문접수 : 2001년 11월 5일, 심사완료 : 2002년 3월 18일

용한 것이며, 크게 2개의 부분으로 나눈다.

- 1부 : TCSEC으로 평가받은 시스템과의 호환성을 고려하여 네트워크 시스템 평가에 적용할 수 있도록 하였다.
- 2부 : 단일 컴퓨터나 시스템의 전체적인 구성(네트워크 구성)을 고려하여 추가적인 네트워크 보안을 고려하였다.

여기에서, 제 2부는 본 연구와 많은 연관성이 있다. 2부에서 다루는 평가기준은 기능성, 메커니즘 강도, 보증 부분이 있는데, 이 중에서 보증을 평가하기 위해 사용되는 기능시험, 주기적 침투 시험, 스트레스 시험, 프로토콜 시험 등이 본 연구의 주제와 연관성이 있다.

2.2 BS7799

BS7799는 조직의 정보 보안을 구현하고 유지하는 책임을 지는 관리자를 위해서 개발된 것으로서, 기업들간의 네트워킹의 신뢰성을 가능하도록 하였으며, BS7799도 역시 크게 두 부분으로 나눈다.

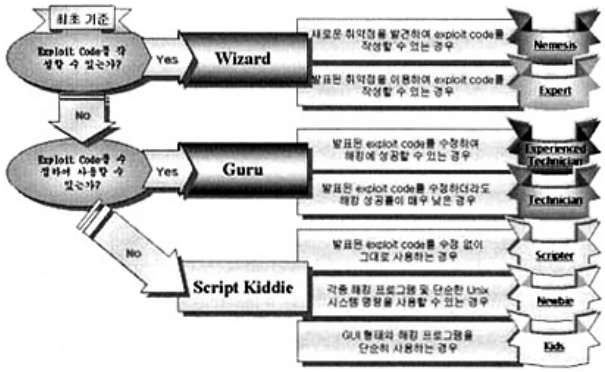
- 1부 : 표준적인 실무 지침으로 종합적인 보안 통제 목록을 제시하였다. 보안정책, 보안조직, 자산분류와 통제, 인적보안, 물리적 및 환경적 보안, 전산기 및 네트워크 관리, 시스템 접근통제, 시스템개발 및 유지보수, 업무지속성 계획 및 준수 등을 다룬다.
- 2부 : 정보관리시스템(Information Security Management System : ISMS)에 대한 표준적인 명세를 기술하며, 위험관리의 중요성을 강조하고 있다. 제 2부에서는 ISMS의 구축 단계를 언급하고 있으며, 3단계와 4단계의 위험평가수행 및 위험관리가 본 연구와 연관성을 가지고 있다.

2.3 SSE-CMM

정보시스템 일반에 대한 평가 모델중에서 CMM(Capability Maturity Model)의 하나인 SSE(Security System Engineering)-CMM이 있다. SSE-CMM은 보안 영역과 능력 부분으로 나눌 수가 있으며, 특히 보안 능력에서 공정 능력 부분의 해석이 중요하다. 공정 능력은 능력단계, 공통기능, 그리고 보편적 실무의 세 가지 기준으로 세분화된다. 본 연구와 관련이 깊은 부분은 SSE-CMM의 보안공학 공정분야로써, 보안위험평가, 취약성평가 등이 연관성이 있다.

2.4 본 연구의 적용 범위 및 의의

본 연구는 내부망 보안수준 평가를 위해 보안 대책에 대한 평가를 제외한 해킹 기법을 바탕으로 한 침투 시험에 대한 견고성을 기준으로 네트워크의 보안 수준을 평가하는 데에 초점을 맞추었다. 내부망 보안 수준(ISL)이라는 개념을 도입하고, 이에 상응하는 네트워크 모델을 설계 및 분석하여, 실질적인 해킹에 대한 보안 대책에 대한 언급을 하였다. 기존의 관련 연구에 비해서 해킹에 대한 직접적인 보안 강화 정책이 요구되는 시점에서 필요한 연구라고 판단된다.



(그림 2) 해커/해킹 기법 분류 및 레벨 정의2

3. 제안하는 방법

ISL은 내부망의 실질적인 보안 수준 평가를 위해 제안된 방법으로써, 테스트를 위한 네트워크 모델을 제시하고, 해킹 및 해커 수준 분류를 적용하여 내부망의 보안 수준을 평가하게 된다.

〈표 1〉 해킹 시나리오 분류

분 류	공격단계	공격수준		
Scenario I	1. 정보수집(시스템 취약성) 2. 불법적인 권한획득 3. Sniffer 설치 4. Backdoor 설치 5. 구체적인 피해행위 6. 침입흔적 제거	Low : Script Kiddie 수준의 공격기술 사용	Medium : Guru 수준의 공격기술 사용	High : Wizard 수준의 공격기술 사용
Scenario II	1. 정보수집(네트워크 취약성) 2. DoS 또는 DDoS 공격			
Scenario III	1. 바이러스 또는 웜 공격			

3.1 해킹 시나리오 분류

내부망의 보안 수준을 평가하기 위해서 해커 및 해킹 수준 분류를 바탕으로 하여, 테스트를 위한 해킹 시나리오를 분류하였다. 이는 제안한 평가 방법에서 테스트를 위한 공격 수준이 지침이 된다. 해킹 시나리오는 크게 3개의 부분으로 분류하고, 각각의 분류된 해킹 시나리오는 단계별로 해커/해킹 수준에 따라 공격 방법을 기술하였다. 공격수준이 높은 경우에는 새로운 취약점을 이용한 공격도 예상된다.

3.1.1 해킹 시나리오 I

일반적인 해킹 공격 기법으로 주로 시스템 취약성에 대한 정보수집, 불법적인 권한 획득, 스니퍼 설치, 백도어 설치, 구체적인 피해 행위, 침입흔적 삭제 등의 순서를 취하고 있다.

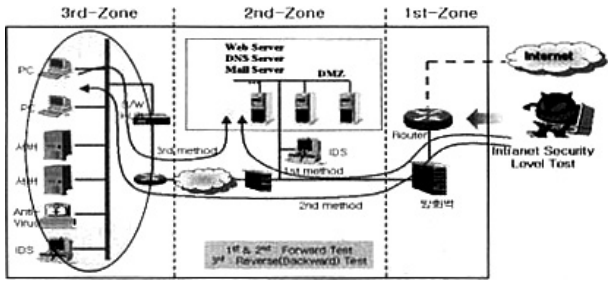
3.1.2 해킹 시나리오 II

최근에 유행했던 서비스 거부 공격(DoS)과 분산 서비스 거부 공격(DDoS)의 형태의 공격 방법으로, 다른 시스템을

해킹하기 위한 선행 작업 및 네트워크 상에서 시스템의 서비스 방해하기 위한 것이다. 이때는 주로 네트워크 취약성을 분석하고 정보를 수집한다.

3.1.3 해킹 시나리오 Ⅲ

바이러스와 인터넷 웜의 형태의 공격 방법으로, 이 방법은 인터넷 확산 속도 때문에 매우 심각하며, 신종 바이러스 및 인터넷 웜 또한 최근에 큰 문제가 되고 있다.



(그림 3) 네트워크 테스트 모델

3.2 네트워크 테스트 모델

내부망의 보안 수준을 평가하기 위한 네트워크의 구축 상태 및 테스트 모델을 제시한다. 이것은 평가 방법에 대한 전반적인 이해를 돕고 실제로 네트워크를 구축하기 위한 것이다. (그림 3)에서 네트워크는 외부망과 1지대, 2지대, 3지대의 내부망으로 구성할 수 있으며, 내부망의 방어 수준 테스트는 해킹 공격 방법에 의해서 수행하게 된다. 1지대는 라우터와 방화벽이 있으며, 2지대는 DMZ(웹, 메일, DNS 서버 등)가 있으며, 3지대는 일반 사용자의 PC 및 서버들이 존재한다. 본 연구에서는 각 지대별 보안 솔루션으로 침입탐지시스템, 침입차단시스템 및 백신 등을 사용하였다. 지대별 구분을 기준으로 침투 경로를 설정하고, 그것을 순방향 공격(Forward Attack : FA)과 역방향 공격(Backward Attack : BA)으로 구분하였다. 보안 수준이 높을수록 역방향 공격이 어렵다.

3.3 평가 방법 및 기준

네트워크 테스트 모델과 해킹 시나리오 분류를 참조하여 내부망의 보안 수준 평가가 이루어지며, 다음과 같은 평가 방법과 기준을 따른다.

3.3.1 내부망 보안 수준 평가 방법

네트워크는 먼저 지대별 주요한 요소로 구분을 하고, 순방향 공격과 역방향 공격을 수행한다. 이때, 공격하는 형태 및 수준은 해킹 시나리오 분류를 기준으로 네트워크의 보안 수준을 시험한다. 이에 따른 네트워크 및 시스템의 보안 수준을 측정하게 된다.

3.3.2 내부망 보안 수준 평가를 위한 기준

● 네트워크 모델에 의한 기준

하위 레벨에서는 역방향 공격이 가능하며, 상위 레벨로 갈수록 일부의 순방향 공격만이 가능하다. 이것은 라우터나 방화벽의 보안 정책 및 관리자의 수준과도 관련이 있다. 3지대, 2지대, 1지대 순서로 방어 수준을 높이 평가한다. 즉, 1지대까지 방어가 가능하면 거의 완벽하다고 평가를 내린다.

● 해킹 시나리오 분류에 의한 기준

해킹 시나리오 분류에서의 공격 수준의 난이도에 따른 네트워크 테스트 배드의 보안 수준을 분류한다. Wizard 수준의 새로운 해킹 공격에 대응하려면 최소한 ISL4 이상의 수준이 되어야 한다.

3.4 내부망 보안 수준 평가

내부망 보안 수준(ISL) 평가는 해킹시나리오와 네트워크 테스트 모델을 바탕으로, 평가 방법 및 기준에 의거하여 실제적인 평가가 이루어지며, 평가를 수행한 후에는 위험요소 분석 및 대응방안을 제시함으로써 내부망의 보안 수준을 향상시킨다.

내부망 보안 수준 평가는 <표 2>와 같이 분류를 한다. 여기에서 전체 방어수준은 3 부분으로 나누었고, 각각의 명칭은 Fragile, Defensive, Excellent로 정의하였다. 이것은 5개의 ISL 등급에서 세분화되는데, 이때 사용한 명칭은 방패(shields)의 종류이다. 분류기준은 해킹 시나리오 및 네트워크 모델에서의 지대별 방어와 공격방법 또는 침투경로의 가능 여부로 평가하였다.

〈표 2〉 내부망 보안 수준

방어 수준	명칭	ISL 등급	명칭 (Shields)	분류기준(방어/공격 가능 여부)			수준 평가
				Zone (방어)	Scenario (방어)	Method (공격)	
C	Fragile	1	Buckler	1,2 : X 3 : △	L : O	FA : O BA : O	L
		2	Kite	3 : O	L<.>M : O	FA : O BA : △	L~M
B	Defensive	3	Spiked	2 : △	M : O	FA : △/O BA : X	M
		4	Tower	2 : O	M <.> H : O	FA : △ BA : X	M~H
A	Excellent	5	Gothic	1 : △/O	H : O	FA : X BA : X	H

X : 불가능, △ : 일부가능, O : 가능
FA : Forward Attack, BA : Backward Attack
L : Low, M : Medium, H : High

3.4.1 ISL1 (Buckler)

Script Kiddie에서 Kids의 해킹 수준의 공격을 방어할 수 있다. 이 단계의 방어 수준에서는 순방향 공격뿐만 아니라 역방향 공격이 가능하며, 1, 2, 3지대 모두에 대해서 공격이 가능하다. 이 경우는 먼저 시스템 자체의 보안 정책을 먼저 수립하고, 전체적인 네트워크 구성을 개선하여야 한다.

3.4.2 ISL2 (Kite)

Script Kiddie에서 Scripter의 해킹 수준의 공격을 방어할 수 있다. 이 단계의 방어 수준에서는 순방향 공격과 일부의 역방향 공격이 가능하며, 1, 2지대의 대부분과 3지대의 일부분에 대한 공격이 가능하다. 따라서, 이 단계의 네트워크

방어 수준은 일부 낮은 수준의 공격에 대해서는 방어 능력을 갖추고 있으나, DMZ의 모든 서버가 해킹이 가능한 수준이다. 이 경우에는 DMZ를 통한 정보의 손실 및 시스템의 파괴 시에 아무런 대응 능력이 없는 경우이다. DMZ 수준의 방화벽 및 서버 기반 침입탐지 시스템을 설치하여 방어 전략을 재정비하여야 할 것이다.

3.4.3 ISL3 (Spiked)

Guru에서 Technician의 해킹 수준의 공격을 방어할 수 있다. 이 단계에서는 순방향 공격은 가능하나, 역방향 공격은 대부분 불가능하며, 1, 2지대의 공격은 가능하나, 3지대는 대부분 불가능한 방어 수준이다. 따라서, 이 단계의 네트워크 방어 수준은 3지대는 대부분 방어가 가능하며, 2지대(DMZ)에 속한 일부 서버들이 공격의 타겟이 될 수 있는 수준이다. 이 경우에는 좀더 견고한 보안 정책을 수립함으로써 공격에 대한 방어를 수행하여야 한다.

3.4.4 ISL4 (Tower)

Guru에서 Experienced Technician의 해킹 수준의 공격을 방어할 수 있다. 이 단계에서는 순방향 공격은 가능하나, 역방향 공격은 대부분 불가능하며, 1지대는 가능하지만, 2지대는 일부 서버에만 공격이 가능하다. 물론 3지대 공격은 대부분 불가능하다. 따라서, 이 단계의 네트워크 방어 수준은 3지대는 방어가 가능하며, 2지대도 대부분 방어가 가능하다. 하지만, 1지대의 라우터 공격 및 방화벽 우회 기술을 사용할 경우 일부 공격이 가능할 수도 있다. 따라서, 이 경우에는 1지대의 방어 전략 정책을 더욱 강하게 추진할 필요가 있다.

3.4.5 ISL5 (Gothic)

Wizard에서 Expert와 Nemesis의 공격을 방어 할 수 있다. 이 단계에서는 순방향 공격 및 역방향 공격이 대부분 불가능하며, 1,2,3 지대 공격 또한 대부분 불가능하다. 따라서, 이 단계의 네트워크 방어 수준은 1,2,3 지대의 거의 모든 서버 및 네트워크 장비에 대한 보안이 되어 있기 때문에, 매우 안정된 네트워크를 구축하고 있다고 평가 할 수가 있는 수준이다. 단, 이 수준의 등급이라도, 새로운 공격에 대한 철저한 대비 전략이 갖추어져 있지 않으면, 보안 등급은 강등될 수도 있다. 따라서, 지속적인 보안 수준 강화를 위한 정책을 추진하여야 한다.

지금까지 살펴본 내부망 보안 평가에 따른 위험 요소 분석 및 이에 대한 보안 대책 및 대응 전략을 제시한다. 이것은 단순한 테스트를 위한 것이 아니라 내부망의 안전성(보안성)의 지속적인 향상을 위한 것이다. 각각의 방어 수준에 따른 위험 요소 분석 및 대응 전략은 다음과 같으며, <표 3>에 나타내었다.

3.5 ISL 분류 기준

본 연구에서 제안한 방법과 기존의 보안 평가 방법을 비교하여 <표 4>에 나타내었다. 즉, <표 4>는 ISL의 수준을

〈표 3〉 위험요소분석 및 대응전략

단 계		위험요소분석	대응전략
Fragile	ISL 1	• FA/BA 공격 모두 가능 • 1/2/3지대 모두 공격 가능 • Script Kiddie(kids) 해킹수준 방어 가능	외부 공격에 대한 방어력이 매우 약함 : 보안 도구 및 보안정책 강화
	ISL 2	• FA 공격 가능, 일부 BA 공격 가능 • 1/2지대 대부분, 3지대 일부분에 대한 공격 가능 • Script Kiddie(Scripter) 해킹 수준 방어 가능	3지대 우선 보안 강화 : Backward 공격 방어 보안 정책 강화
Defensive	ISL 3	• FA 공격가능, BA 공격 대부분 불가능 • 1/2지대 공격가능, 3지대 대부분 불가능 • Guru(Technician) 해킹 수준 방어 가능	DMZ 서버들의 취약점 보완 : IDS와 방화벽으로 보안 강화
	ISL 4	• FA 공격가능, BA공격 대부분 불가능 • 1지대 대부분, 2지대 일부 공격 가능 • Guru(Experienced Technician) 해킹 수준 방어 가능	1지대 네트워크 장비 취약성 극복 요망
Excellent	ISL 5	• FA/BA 공격 대부분 불가능 • 1/2/3지대 공격 대부분 불가 • Wizard(Expert) 해킹 수준 방어 가능	매우 안정된 보안 수준. 단, 지속적인 내부망 보안 강화

TNI와 CC로 비교한 도표이다. 여기에서 TNI의 주요 비교 대상은 제 2부이며, 제 1부는 TCSEC에서 인증되는 최소 등급을 기술한다. CC에서 TCSEC의 D급에 해당하는 EAL0는 제외하였다. 본 연구에서는 제 4장에서 ISL3 수준의 테스트 베드를 설계하고 이를 분석하였다.

〈표 4〉 ISL vs. TNI/CC

방어수준	ISL 등급	TNI 등급		CC등급
		제 2부	제 1부	
Fragile	1	Minimum	C1 이상	EAL 1
	2			EAL 2
Defensive	3	Fair	C2 이상	EAL 3
	4			EAL 4
Excellent	5	Good	B2 이상	EAL 5~7

4. 테스트베드 설계 및 분석

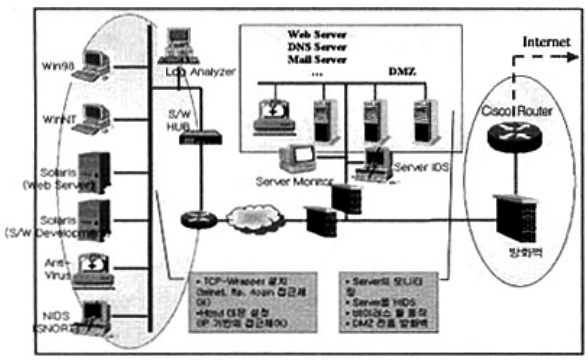
본문에서 제안한 네트워크 테스트 모델인 (그림 3)을 바탕으로 (그림 4)와 같은 테스트 베드를 설계하고 그 보안 수준을 분석하였다. 본 연구에서 구성된 네트워크의 수준을 분석한 결과 ISL3 수준으로 판정되었다. 이의 보안 수준을 한 단계 상승을 위해서는 다음의 사항을 더 고려하여야 한다.

- 시스템 취약성 완전 패치
- 네트워크 취약성 극복을 위한 대응 방안
- 새로운 해킹 및 바이러스 공격 대항

4.1 네트워크 구성

1지대는 라우터와 방화벽이 존재한다. 내부망(DMZ와 로컬 네트워크를 포함)으로 들어가는 패킷과 내부망에서 외부망으

로 나오는 패킷을 필터링한다. 2지대는 DMZ로써 각종 서버(DNS, 메일, 웹, ftp 서버 등)들이 존재한다. 이것은 서비스가 목적이기 때문에 개방된 형태이다. 하지만, 인증(ID와 패스워드)과 접근제어를 통한 보안 설정을 한다. 또한, 서버의 트래픽 및 로그를 모니터링 할 수 있고, 서버용 침입탐지시스템도 작동중이다. DMZ로의 역방향 공격을 방어하기 위한 방화벽이 설치되어 있다. 또한, DMZ로 들어가는 바이러스를 제거하는 바이러스 월이 설치된다. 3지대는 일반 PC와 웹서버 및 S/W 개발용 서버가 존재한다. 여기에는, 각 PC마다 바이러스 점검 및 제거 툴이 설치되어 있다. 또한, 로그를 분석할 수 있는 로그 분석 시스템과 네트워크 기반 IDS가 설치되어 있다. 내부 사용자와 외부 사용자의 서버 접근을 제



(그림 4) 테스트 베드 설계

한하기 위해서 tcp-wrapper가 설치되어 있어서, inetd 방식(telnet, ftp, rlogin 등)으로 동작하는 데몬들을 IP 기반으로 접근제어를 하였다. 웹 서버의 경우는 인증된 IP만을 디렉토리에 접근할 수 있도록 httpd의 데몬 환경설정을 하였다.

4.2 공격 실험

본 연구에서는 1지대에서 2지대로의 접근을 위해서 방화벽에 인증된 웹 서버를 통하여 일단 공격을 시도하고 웹 서버에서 다른 시스템으로 공격을 시도하였다. 일단 2지대의 접근 후 3지대로의 공격에서는 3지대의 방화벽의 패킷 통과 정책에 따라서 좀 다르겠지만 테스트베드의 방화벽 정책은 외부에서의 모든 패킷을 막고 있으며, 내부에서 외부로의 접근은 허용하고 있기 때문에 우회공격을 통한 2지대에서 3지대로의 공격은 대부분 불가능하였다. 또한, 침입탐지시스템(IDS)의 우회공격을 시도하여 공격 대상 시스템의 정보를 분석하는 방법을 사용하였다. 이때 사용한 것이 Phrack 57호의 Line-noise Section에 실린 "SeolMa" 소스를 사용하여 테스트하였다.

시나리오 1의 경우에서는 일단 nessus, nmap, hunt 등을 사용하여 시스템의 취약점을 분석한 후 해당 취약점을 이용한 해킹 공격을 시도하였다. 시나리오 2의 경우는 DoS 또는 DDoS 형태의 공격을 시도하였다. 일반 시스템뿐만 아니라 NIDS에 대해서도 실시하였으며 이때 사용한 것이

〈표 5〉 공격 실험 분석

공 격 방 법	세부 공격 방법	분 류	평 가 결 과
시스템/서비스 설정 문제	Password Cracking	S1 / Z2,3 / M1,2	공격 불가능
	환경변수 이용	S1 / Z2,3 / M1,2	공격 불가능
	SUID 설정 이용	S1 / Z2,3 / M1,2	공격 불가능
	FTP, HTTP 설정 문제	S1 / Z2,3 / M1,2	Z2에 일부 공격 가능
프로그래밍 오류	CGI, PHP 등 취약점	S1 / Z2,3 / M1,2	일부 공격 가능
	버퍼 오버플로우	S1 / Z2,3 / M1,2	공격 불가능
	힙 오버플로우	S1 / Z2,3 / M1,2	공격 불가능
	Race Condition	S1 / Z2,3 / M1,2	공격 불가능
	Format String 공격	S1 / Z2,3 / M1,2	Z2에 일부 공격 가능
프로토콜 취약점	Packet Sniffing	S1 / Z2,3 / M1,2	Z2에 일부 공격 가능
	IP Spoofing	S1 / Z2,3 / M1,2	공격 불가능
	ARP Spoofing	S1 / Z2,3 / M1,2	공격 불가능
정 보 수 집	보안 스캐너 사용	S1,2 / Z2,3 / M1,2	Z2에 일부 공격 가능
	시스템 명령 사용	S1 / Z2,3 / M1,2	Z2에 일부 공격 가능
	서비스 명령 사용	S1,2 / Z2,3 / M1,2	Z2에 일부 공격 가능
	Finger Printing	S1 / Z2,3 / M1,2	공격 불가능
서비스 거부공격	NIDS용 DoS	S2 / Z2,3 / M1,2	일부 공격 가능
	SYN Flooding	S2 / Z2,3 / M1,2	일부 공격 가능
	Ping Flooding	S2 / Z2,3 / M1,2	일부 공격 가능
	일반 DDoS	S2 / Z2,3 / M1,2	일부 공격 가능
악성코드(Virus/Worm/Backdoor)	트로이잔 프로그램 사용	S3 / Z2,3 / M1,2	Z2에 일부 공격 가능
	파일 바이러스	S3 / Z2,3 / M1,2	공격 불가능
	Backdoor 프로그램	S1 / Z2,3 / M1,2	Z2에 일부 공격 가능
로그 삭제	단순 로그 삭제	S1 / Z2,3 / M1,2	공격 불가능
	모든 로그 삭제	S1 / Z2,3 / M1,2	공격 불가능
	자신의 흔적 로그만 제거	S1 / Z2,3 / M1,2	Z2에 일부 공격 가능
기 타	F/W 우회공격	Z1,2,3 / M1,2,3	Z1, Z2에 일부 공격 가능
	IDS 우회공격	Z2,3 / M1,2,3	Z2, Z3에 일부 공격 가능

< S : Scenario / Z : Zone / M : Method >

RealAttack의 "Mearong"을 사용하였다. 시나리오 3의 경우에서는 E-mail을 통하여 바이러스 혹은 웜의 형태의 전파를 시도하였다. 이때 대부분의 바이러스 혹은 웜은 바이러스 제거 툴에 의해서 실시간으로 점검되어 제거가 되었다.

이에 대한 실험 결과는 <표 5>에 나타내었으며, 다음절의 보안 수준 분석에서 ISL의 보안 등급을 분석하였다.

4.3 보안 수준 분석

테스트 베드의 지대별, 해킹 시나리오별, 침투 경로 및 방법에 대한 공격 가능성을 분석해 본다. 본 연구에서 구축한 테스트 베드는 1지대는 고수준의 해킹 기법에 의해서만 공격당할 수 있다. 라우팅 테이블 변경 및 방화벽 우회 공격 같은 일부 공격에 대해서만 취약점을 가지고 있다. 2지대의 DMZ는 각종 보안 툴 및 감시 시스템이 동작하며, 인증 및 접근제어를 통해서 외부 공격자의 공격에 대처하여 공격하기가 힘들지만 고수준의 해킹을 통해서 접근 가능하다. 3지대는 바이러스 제거 툴과 침입탐지시스템 및 로그 분석기가 존재하기 때문에 공격이 쉽지 않다. 또한, 일반 PC는 공유폴더가 모두 패치되어 있기 때문에 접근이 불가능하며, 바이러스의 공격 또한 불가능하다. 해킹 시나리오에서 시나리오 Ⅰ의 시스템 취약점을 이용하는 경우는 고수준으로 일부 네트워크 장비 및 서버에 공격이 가능한 수준이다. 시나리오 Ⅱ의 네트워크 취약점을 이용하는 공격의 경우도 일부 네트워크 장비 및 서버에 공격이 가능한 수준이다. 시나리오 Ⅲ의 바이러스 및 인터넷 웜을 이용한 공격은 바이러스 월 및 PC용 바이러스 점검 및 제거 툴이 동작하기 때문에 공격을 할 수 없다. 3가지의 침투경로 공격방법에서 1차 순방향 공격은 일부 가능하나, 2차 순방향 공격 및 3차의 역방향 공격은 대부분 불가능하다. 하지만, 새로운 해킹 공격 및 바이러스 공격에 대해서는 보안성을 유지하지 못하는 수준이다. 즉, ISL3 수준으로 판단된다.

5. 결 론

본 연구에서는 내부 네트워크의 보안 수준을 강화하기 위하여 해킹 기법을 이용하는 방법을 제시하였다. 제안한 ISL에 의한 내부망의 보안 수준의 평가와 관련 연구로는 TNI, BS7799, SSE-CMM 등이 있으며, 본 연구에서 제안하는 방법은 해킹에 대한 내부망의 실질적인 보안수준을 평가하고, 내부망의 보안 수준을 개선하고자 함에 그 목적이 있다. 제안한 방법에서는 내부 네트워크를 지대별 및 공격 경로별로 구분하고, 해킹 시나리오에 따른 공격 수준을 적용하여 내부망의 보안 수준을 평가하였다. 제안된 방법 ISL은 ISL1~ISL5의 5개 등급으로 구분하였으며, ISL5가 내부망 보안 수준에서 가장 보안성이 높음을 의미한다. 본 연구에서 구성한 테스트베드는 ISL3으로 분석되었으며, ISL4 이상의 수준을 위해서는 보안 장비, 정책 그리고 관리자의 수준 향상이 요구된다.

참 고 문 헌

[1] 사이버테러기술분석팀, "정보화역기능 기술분석 및 대응방안 연구", *ETRI* 2000.
[2] 최양서, 서동일, 손승원, "해커/해킹기법 분류 및 레벨 정의", *ETRI주간기술동향, 01-32호*, 2001.
[3] NCSC, "TNI of the TCSEC," *Tech. Rept.NCSC-TG-005, NCSC*, July, 1987.
[4] http : //www.c-cure.org.
[5] http : //www.ismlab.co.kr.
[6] Carnegie Mellon University, "SSE- CMM Ver. 2.0," *CMU*, April, 1999.
[7] http : //www.kisa.or.kr.
[8] 사이버테러기술분석팀, "차세대 해킹기술 및 네트워크 안전성 분석 연구", *ETRI* 2001.
[9] 서동일, 윤이중, 조현숙, "사이버테러 기술 및 대응방안의 현황 분석", Telecommunications Review, 제10권 제5호, 2000.

서 동 일

e-mail : bluesea@etri.re.kr
1989년 경북대학교 전자공학과 학사
1994년 포항공과대학교 정보통신학과 석사
2000년~현재 충북대학교 전산학과 박사과정
1994년~현재 한국전자통신연구원 선임연구원(팀장)
관심분야 네트워크 보안, 해킹, 인터넷정보보호

최 병 철

e-mail : corea@etri.re.kr
1999년 서울시립대학교 제어계측공학과 학사
2001년 서울시립대학교 전자전기공학부 석사
2001년~현재 한국전자통신연구원 연구원
관심분야 : 네트워크 보안, 워터마킹, 컴퓨터비젼

손 승 원

e-mail : swsohn@etri.re.kr
1984년 경북대학교 전자공학과 학사
1994년 연세대학교 전자공학 석사
1999년 충북대학교 컴퓨터공학과 박사
1991년~현재 한국전자통신연구원 책임연구원(부장)
관심분야 : 네트워크 보안, 라우팅 알고리즘, 생체인식기술

이 상 호

e-mail : shlee@cnlab.cbu.ac.kr
1976년 숭실대학교 전자계산학과(공학사)
1971년 숭실대학교 전자계산학과(공학석사)
1989년 숭실대학교 전자계산학과(공학박사)
1979년~1979년 한국전력전자계산소
1981년~현재 충북대학교 컴퓨터과학과, 교수
관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture