情 報 保 護 學 會 誌
第19卷 第1號, 2009. 2

가상화 기술을 도입한 정보보호 교육 방안

신 원*, 조 성 목*

요 약

최근 가상화 기술은 하드웨어의 추상화, 통합된 시스템 관리, 유지관리 비용의 절감 등 다양한 장점과 가능성으로 주목받는 기술로 각광받고 있으며, 가상화 기술을 도입한 다양한 제품과 기술이 개발되어 정보통신의 여러 분야에 적용되고 있다. 본 고에서는 해킹 또는 악성 코드를 다루기 위해 별도의 격리된 환경이 필수적인 정보보호 교육에 있어 가상화 기술의 적용을 위한 방안을 여러 측면에서 살펴보고, 이에 대한 장단점과 정보보호 교육의 특성을 잘 반영할 수 있는 고려사항에 대해 논의한다.

Ⅰ. 서 론

정보시스템에 대한 요구가 다양해지고 증가하면서 이에 따른 도입 및 운영 비용과 정보시스템의 규모가 기하급수적으로 늘어나고 있다. 이러한 비용과 규모의 증가는 정보통신 기술의 효율성에 대한 관심을 증진시켰고, 결과적으로 이를 해결하기 위한 다방면의 검토가 이루어지고 있으며, 이와 관련한 새로운 기술들이 등장하게 되었다. 그 중 가상화 기술은 이러한 정보시스템의 효율성을 높이기 위한 주요기술로써 각광받고 있다.

가상화 기술은 유휴 자원 및 서버 가동률의 확대, 기업의 운영 및 관리 비용 절감, 시스템 복잡성 감소 등의 장점으로 수많은 기업에서 도입을 진행 또는 검토하고 있으며, 이러한 기업의 요구를 만족하기 위해 새로운 개념을 도입한 가상화 기술과 가상화 제품들이 시장에 속속 등장하고 있다. 이러한 추세에 따라 가상화 시장은 매년 60% 이상의 고성장세를 보이고 있으며, 다양한 기업들의 참여에 의해 시장 규모가 증가하고 있는 추세이다. 기존 VMware, Microsoft 등 전문 가상화 소프트웨어 기업들은 물론 Intel, AMD 등 프로세서 제작업체와 XenSource와 같은 오픈소스 소프트웨어 업체들이 경쟁을 벌이고 있다.

또한, 가상화 기술은 기존의 물리적 장비와 달리 여러 사용자가 하나의 호스트 자원을 논리적인 자원으로 할당받아 사용할 수 있다는 특징을 가지고 있기 때문에 자원의 사용량이 상대적으로 많은 기업 또는 조직의 비용 절감, 친환경 IT정책 차원에서 가상화 기술의 보급 및 이용이 확대되고 있다. 또한, 가상화는 서버는 물론 데스크톱, 스토리지, 네트워크에 이르기까지 IT 솔루션 전반에 걸쳐 확대 적용될 것으로 보인다.

본 고에서는 기업 환경에 앞다투어 적용하고 있는 가상화 기술을 정보보호 교육에 도입하는 방안에 대하여 연구한다. 정보보호 교육은 해킹과 악성코드를 직접 다루는 고유의 특성 상 일반적인 컴퓨팅 환경에 직접 적용하기 힘든 특성을 가지고 있으며, 이를 이용한 교육 방법도 다른 컴퓨팅 환경과는 판이하게 다른 실정이다. 따라서, 가상화 기술을 이용한 구체적인 정보보호 교육 사례를 살펴보고, 정보보호 교육의 특성을 잘 반영할 수 있는 방안 모색을 목표로 한다. 본 고의 구성은 다음과 같다. 2장에서 가상화 기술에 대하여 살펴보고, 3장에서 가상화 기술을 도입한 정보보호 교육을 사례를 통하여 살펴본다. 4장에서는 가상화 기술의 정보보호 교육 적용 시 고려사항을 살펴보고, 5장에서 마지막 결론을 맺는다.

Ⅱ. 가상화 기술

2.1 가상화 기술의 개념

컴퓨팅 분야에서 가상화(Virtualization)란 물리적으

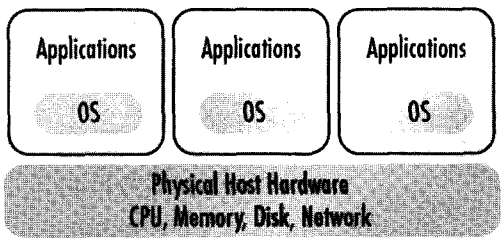
* 동명대학교 정보보호학과 (shinweon@tu.ac.kr, smcho@tu.ac.kr)

로 다른 시스템을 논리적으로 통합하거나 하나의 시스템을 논리적으로 분할해 자원을 효율적으로 사용하게 하는 기술로 정의할 수 있다[1]. 즉, 가상화는 컴퓨터 자원을 추상화한다는 의미이며 자원을 다루는 어플리케이션이나 사용자에게는 복잡한 물리적인 속성을 숨기고 논리적인 자원을 보여주는 기술을 의미한다. 여기서 가상화는 Workload 재분배를 통하여 시스템 운용의 효율성을 제공하고 하드웨어의 추상화로 운영체제와 어플리케이션을 쉽게 이전할 수 있게 하며 소프트웨어 배포의 편의성을 제공하는 등 다양한 장점을 가진다. 또한, 어플리케이션 가상화, 데스크탑 가상화 등 기존의 서버 가상화 뿐만 아니라 다양한 영역에서 가상화 기술이 적용되고 있으며, 많은 기업들이 비용절감을 위한 방안으로 가상화에 대해 지대한 관심을 가지고 있다.

2.2 가상화 소프트웨어

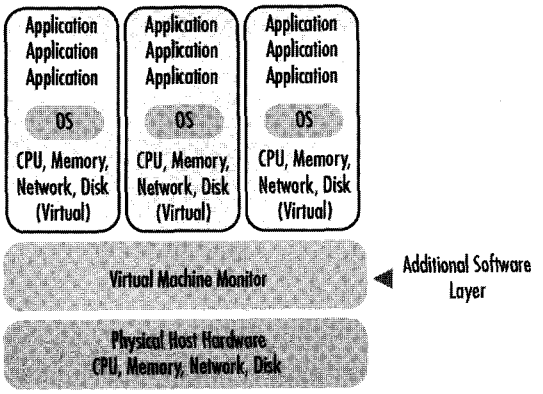
가상화 기술의 적용은 하드웨어 자원에서 어플리케이션에 이르는 다양한 분야에 적용할 수 있다. 일반적으로 서버와 스토리지의 물리적 개수를 줄이고, 각종 자원을 가상적으로 묶어 풀(Pool)을 형성하면 자원을 동적으로 추가, 삭제, 변경할 수 있고 어플리케이션에 할당 및 반환될 수 있는 시스템을 구축하여 운영할 수 있다. 그 중 서버 가상화 기술은 자원의 가상화, 플랫폼기반 가상화, 프로세서 기반 가상화(또는 Hypervisor 기반 가상화), OS기반 가상화 등으로 분류할 수 있다[2][3].

서버 가상화의 경우 가상 머신(Virtual Machine)이라는 특수한 중간 계층을 두고, 하나의 물리 서버를 복수의 가상 서버로 분할하는 방식으로 운영체제 상에서 하드웨어를 에뮬레이션하는데, 일반적으로 IBM PC의 Intel x86 을 에뮬레이션한다. 여기서, 물리적인 컴퓨터의 운영체제를 "호스트 운영체제(Host OS)", 가상 컴퓨터의 운영체제를 "게스트 운영체제(Guest OS)"로 정의한다. 특히 가상 머신은 Windows, Linux 등의 호스트 운영체제 위에서 동작하는 다수의 운영체제, 즉 다수의 게스트 운영체제를 설치할 수 있다. [그림 1]은 일반적인 컴퓨터의 동작을 개념적으로 그린 것이다.



〔그림 1〕 일반적인 컴퓨터의 동작

[그림 2]는 가상화 기술이 도입되어 가상 머신 계층(Virtual Machine Layer)이 추가된 컴퓨터의 동작을 개념적으로 보여준다.



〔그림 2〕 가상 머신 계층이 포함된 컴퓨터의 동작

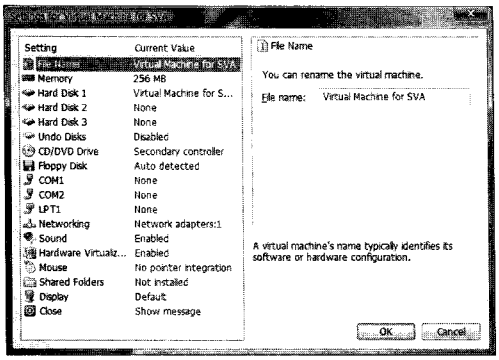
여기서, 가상 머신 모니터(VMM, Virtual Machine Monitor)는 가상화 기술의 핵심으로 물리적인 컴퓨터 환경에서 동작하는 소프트웨어로 제작된 가상 머신 계층을 말한다. 가상 머신 모니터는 호스트 운영체제 상에서 동작하는 게스트 운영체제가 가상 머신 계층을 통하여 호스트 운영체제의 중앙처리장치(CPU), 하드디스크

〔표 1〕 대표적인 가상화 제품

제품	제작사	Host OS	Guest OS	License
Virtual PC[4]	Microsoft	OS X, Windows	Linux, OS/2, Windows	Free
Virtual Server[5]	Microsoft	Windows	Linux, Windows	Free
VMware Workstation[6]	VMware	Linux, Windows	FreeBSD, Linux, Netware, Solaris, Windows	상용
VMware Server[7]	VMware	Linux, Windows	FreeBSD, Linux, Netware, Solaris, Windows	Free
Xen[8]	XenSource	NetBSD, Linux, Solaris	xBSD, Linux, Solaris, Windows	GPL

(HDD) 등의 서버 자원을 사용하도록 해준다. 따라서, [그림 2]와 같은 동작에 의해 하나의 물리적인 컴퓨터 상에서 다수의 가상 컴퓨터의 동작이 가능하다. 현재 서버 가상화는 구현 방식에 따라 소프트웨어 구현을 통한 가상화 기능 또는 하드웨어 제작업체의 지원을 통한 하드웨어 가상화 기능을 갖춘 VMware, Microsofot, XenSource 등 다양한 회사의 가상화 제품들이 출시되고 있는데, 이를 정리하면 [표 1]과 같다.

[그림 3]은 Microsoft 사에서 인터넷을 통하여 무료로 제공하고 있는 Virtual PC의 설정화면으로, PC에서 사용가능한 Windows 운영체제에 최적화되어 있으나, Linux도 설치가 가능하다.



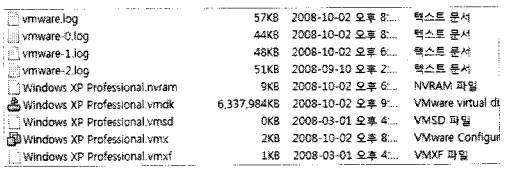
〔그림 3〕 Microsoft 사의 Virtual PC 설정 화면

2.3 가상화 환경 구성을 위한 준비

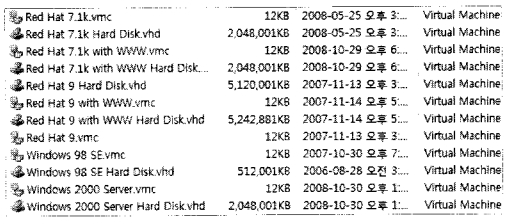
가상화 환경을 구성하기 위하여 준비해야 하는 하드웨어와 소프트웨어 구성은 다음과 같다.

하드웨어는 서버급이면 좋으나 일반 PC도 사용 가능하다. 그러나, 가능한 고속의 CPU와 고용량의 메모리가 필요하며, 가상 이미지를 저장할 대용량의 하드디스크 및 백업 장비도 필요하므로 구비하는 것이 좋다. 네트워크 연결을 위한 NIC(Network Interface Card)는 1개라도 무방하나 2개 이상이면 더욱 효율적으로 사용할 수 있다. 소프트웨어로는 가상화 소프트웨어가 필수적인데, 공개 소프트웨어인 MS Virtual PC, VMware Player 등이 있으며 상용 소프트웨어로 VMware Workstation이 출시되어 있으므로 상황에 맞게 사용하도록 한다. 호스트 운영체제는 Windows 계열과 Linux 계열을 하드웨어 구성에 맞도록 설치하여야 하는데, 보편적으로 많이 사용되는 Windows 계열이면 무난하다. 단, MS Virtual PC의 경우는 Windows 만 지원하므로 이를 고려하여 구성한다. 게스트 운영체제를 설치하기 위하여 각종 운영체제가 필요한데, Windows 환경의 경우 Microsoft Windows 2000/2003 Server, Windows XP, MS SQL Server 등이 필요하며, Linux 환경의 경우 Redhat Linux, Fedora 등이 필요하다.

게스트 운영체제의 설치에서 가상 머신 이미지 파일을 생성하는 것 이외에는 일반 컴퓨터에 운영체제를 설치하는 것과 동일한 과정을 거치는데, 하나의 물리적 컴퓨터 내에 여러 대의 가상 컴퓨터 설치가 가능하고 가상 컴퓨터 1대는 물리 컴퓨터 1개의 (가상 머신 이미지) 파일에 대응한다. 즉, 하나의 호스트 운영체제 위에 다수의 게스트 운영체제의 동작이 가능한데, 그 개수는 메모리 크기와 HDD 크기에 비례한다. [그림 4]는 VMware를 통하여 설치된 가상 머신 이미지 파일(*.vmdk)이고, [그림 5]는 Virtual PC를 통하여 설치된 가상 머신 이미지 파일(*.vhd)이다. [그림 4]와 [그림 5]에서 보이는 바와 같이 각각의 게스트 운영체제가 호스트 운영체제에서는 각각의 파일로 존재함을 확인할 수 있다.



〔그림 4〕 VMware의 가상 머신 이미지 파일



〔그림 5〕 Virtual PC의 가상 머신 이미지 파일

여기서, 가상 머신 이미지 파일을 복사 또는 배포하여 다른 호스트 운영체제에서 동작시키면 각각의 게스트 운영체제의 동일한 동작을 보장할 수 있다. 또한, 실제로는 물리적 컴퓨터가 한 대라 할지라도 외부에서 볼 때는 게스트 운영체제는 물리적으로 여러 대의 개별 컴퓨터인 것과 동일한 효과를 얻을 수도 있다. 특히, 게스

트 운영체제마다 독립적인 하드웨어 및 환경 설정과 어플리케이션 설치가 가능하므로 개별 운영체제로 운영할 수 있다. 즉, 게스트 운영체제에서 동작하는 어플리케이션을 하나의 물리적인 컴퓨터에서 동작시키는 것처럼 속임으로써 어플리케이션 동작에 대한 일관성을 보장하는 것이다. 심지어 물리적인 컴퓨터와 동일한 동작이 가능함으로써 악성코드 및 바이러스도 감염될 수 있다.

Ⅲ. 가상화 기술을 도입한 정보보호 교육

본 장에서는 정보보호 교육에 가상화 기술을 도입하여 2008년에 직접 강의를 진행한 동명대학교 정보보호학과 사례를 중심으로 살펴본다.

3.1 사례 1 : 시스템 프로그래밍

동명대학교 정보보호학과에서 2008년 2학기에 개설된 "시스템 프로그래밍" 교과목은 Linux 시스템의 구조에 대해 이해하고 시스템의 호출과 라이브러리 함수의 사용법을 익혀 시스템 프로그래밍에 필요한 기술과 지식 배양을 목표로 한다. 이를 가상화 기술을 도입하여 운영하는 과정은 다음과 같다.

환경 구성 및 준비

○ 교수용 PC
- 호스트 운영체제 : Windows XP
- 가상화 소프트웨어 : VMware Workstation
- IP주소 : 210.x.y.90

○ 가상 서버
- 게스트 운영체제 : Redhat Fedora Core 5
- IP주소 : 210.x.y.91

○ 실습용 PC 40대
- 운영체제(멀티부팅 가능) : Windows XP, Redhat Fedora Core 5
- IP주소 : 210.x.y.50~89

"시스템 프로그래밍" 강의진행

○담당 교수

절차 1. 교수용 PC의 호스트 운영체제에서 빔프로젝트를 통하여 PowerPoint 자료를 활용하여 판서 등과 함께 강의를 진행한다.

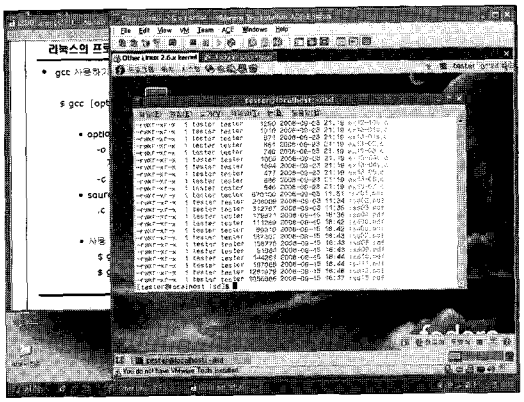
절차 2. VMware Workstation을 실행하여 게스트 운영체제인 Redhat Fedora 부팅 후 각종 실습을 함께 진행한다.

절차 4. 담당 교수는 재부팅 없이 호스트 운영체제인 Windows와 게스트 운영체제 Fedora를 번갈아 가면서 강의 진행이 가능하다.

○ 학생

절차 3. 실습용 PC를 켠 후 선택가능한 멀티 부팅 화면에서 Redhat Fedora를 선택하여 부팅한 후 담당 교수의 지도에 따라 실습을 진행한다.

[그림 6]은 "시스템 프로그래밍" 강의 진행 중 한 화면으로, 왼쪽 뒤쪽에 진행되는 강의 내용이 보여지고 앞쪽에 Fedora가 실행되어 있음을 확인할 수 있다.



[그림 6] "시스템 프로그래밍" 강의 화면

3.2 사례 2 : 해킹 및 악성코드 대응

동명대학교 정보보호학과에서 2008년 2학기에 개설된 "해킹 및 악성코드 대응" 교과목은 컴퓨터 시스템의 공격과 침입에 대한 보다 적극적인 대응을 위하여 각종 플랫폼과 프로토콜의 기본 동작, 다양한 해킹 기법 및 도구에 대한 분석과 대응 방안, 바이러스, 웜, 트로이목마와 같은 악성 코드의 원리와 치료 기법 등에 관련한 이론과 기술 습득을 목표로 한다. 이를 가상화 기술을 도입하여 운영하는 과정은 다음과 같다.

환경 구성 및 준비

○ 교수용 PC
- 호스트 운영체제 : Windows XP
- IP주소 : 210.x.y.90

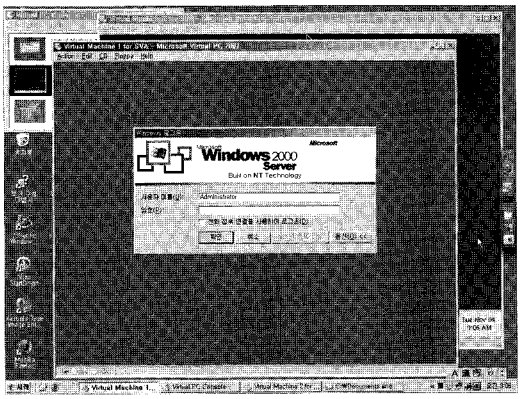
○ 물리 서버
• 호스트 운영체제 : Windows 2003 Server Standard
• 가상화 소프트웨어 : Microsoft Virtual PC 2007
• IP주소 : 210.x.y.91, 210.x.y.92
○ Victim1 : Windows 가상 서버
• 게스트 운영체제 : Windows 2000 Server
• IP주소 : 210.x.y.93
○ Victim2 : Linux 가상 서버
• 게스트 운영체제 : Redhat Linux 9.0
• IP주소 : 210.x.y.94
○ 실습용 PC 40대
• 운영체제 : Windows XP
• 가상화 소프트웨어 : Microsoft Virtual PC 2007
• IP주소 : 210.x.y.50~89

"해킹 및 악성코드 대응" 강의진행
○ 담당 교수
절차 1. 교수용 PC에서 PowerPoint 자료를 이용하여 판서 등을 이용하여 강의를 진행한다.
절차 3. 물리 서버를 부팅한 후 호스트 운영체제 상에서 가상화 소프트웨어를 실행하여 게스트 운영체제 Victim1 (210.x.y.93), Victim2 (210.x.y.94)를 각각 실행한다.

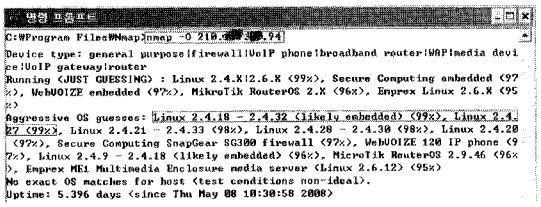
○ 학생
절차 2. 실습용 PC에서 PowerPoint 자료를 이용하여 실습을 진행한다.
절차 4. 담당 교수의 지도하에 Victim1 (210.x.y.93), Victim2 (210.x.y.94)를 대상으로 스캐닝하거나 악성프로그램, 공격 코드 등을 직접 실행한다.

[그림 7]은 담당 교수가 물리 서버에서 Victim1 Windows 가상 서버(앞쪽)와 Victim2 Linux 가상 서버(오른쪽 뒤쪽)를 실행한 화면이다. 각각은 서로 간섭없이 독립적으로 동작하며 별도의 구성을 가진다. 즉, 외부에서 네트워크를 통하여 보면 물리 서버, Victim1, Victim2의 3개의 물리 서버가 존재하는 것으로 보인다.

[그림 8]은 네트워크 스캐너인 nmap[9]을 이용하여 Victim2를 스캐닝하여 운영체제를 추측한 결과이다. 2.4.x 버전의 커널을 가진 Linux 서버임을 확인할 수 있는데, 실제로는 Linux 가상 서버지만 nmap은 실제 동작하는 물리적인 Linux 서버로 판단한다.



〔그림 7〕 "해킹 및 악성코드 대응"에서 Victim 실행 화면



〔그림 8〕 "해킹 및 악성코드 대응"에서 Victim2에 대한 스캐닝 수행 화면

3.3 사례 3 : 시스템 취약성 분석

동명대학교 정보보호학과에서 2008년 1학기에 개설된 "시스템 취약성 분석" 교과목은 다양한 취약성 정보, 분석 도구, 데이터베이스, 지식 등을 활용하여 불법적인 사용자의 접근을 허용할 수 있는 위협, 정상적인 서비스를 방해하는 위협, 중요한 데이터의 유출, 변조, 삭제에 대한 위협 등이 정보시스템에 존재하고 있는지에 대한 점검과 점검 후 보안 수준의 분석과 대응 능력을 배양하는 것을 목표로 한다. 이를 가상화 기술을 도입하여 운영하는 과정은 다음과 같다.

환경 구성 및 준비
○ 교수용 PC
• 호스트 운영체제 : Windows XP
• IP주소 : 192.168.28.9
○ 물리 서버
• 호스트 운영체제 : Windows 2003 Server Standard
• 가상화 소프트웨어 : Microsoft Virtual PC 2007

- IP주소 : 192.168.28.2, 192.168.28.3

○ Victim1 : Windows 가상 서버

- 게스트 운영체제 : Windows 2000 Server
- IP주소 : 192.168.28.4

○ Victim2 : Linux 가상 서버

- 게스트 운영체제 : Redhat Linux 9.0
- IP주소 : 192.168.28.5

○ 실습용 PC 40대

- 운영체제 : Windows XP
- 가상화 소프트웨어 : Microsoft Virtual PC 2007
- IP주소 : 192.168.28.10~49

"시스템 취약성 분석" 강의진행

○ 담당 교수

절차 1. 교수용 PC에서 PowerPoint 자료를 이용하여 판서 등을 이용하여 강의를 진행한다.

절차 3. 물리 서버를 부팅한 후 호스트 운영체제 상에서 가상화 소프트웨어를 실행하여 게스트 운영체제 Victim1 (192.168.28.4), Victim2 (192.168.28.5)를 각각 실행한다.

절차 5. Victim1 (192.168.28.4), Victim2 (192.168.28.5)의 가상 머신 이미지 파일을 학생들에게 배포한다.

○ 학생

절차 2. 실습용 PC에서 PowerPoint 자료를 이용하여 실습을 진행한다.

절차 4. 담당 교수의 지도 하에 Victim 1, Victim 2를 대상으로 스캐닝하거나 악성프로그램, 공격 코드 등을 직접 실행한다.

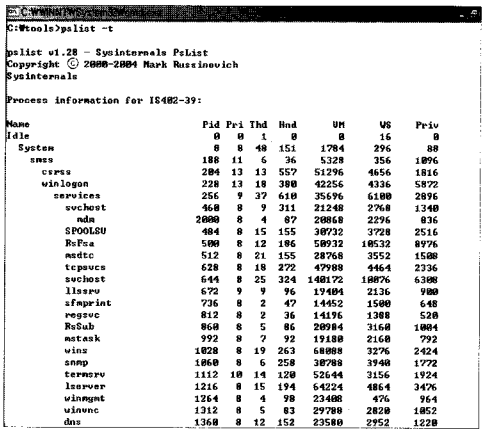
절차 6. 다운로드받은 Victim1 (192.168.28.4), Victim2 (192.168.28.5)의 가상 머신 이미지 파일을 실행하여 적절한 환경 설정 후 취약성 분석을 각각 수행하고 결과를 제출한다.

[그림 9]는 공개 침투 테스트 도구인 MSF(Metaploit Framework)[10]를 이용하여 Victim1의 취약점을 이용하여 공격한 실행 화면이다. Victim1은 Windows 가상 서버이지만 물리 서버와 마찬가지로 취약점에 따른 공격이 가능함을 알 수 있다.

[그림 10]은 각종 공격 후 Victim1의 가상 이미지 파일을 배포한 후 이를 다운로드받은 학생이 자신의 PC에서 Victim1을 실행하여 현재 동작 중인 프로세스를

〔그림 9〕 "시스템취약성 분석"에서 공격 실행 화면

분석하는 화면이다. 물리 서버에서 동작한 것과 동일한 동작이 가능하다. 단, 가상 서버 실행을 위한 설정 변경 시 IP주소 등의 시스템 관련 구성값은 다를 수 있다.



```
C:\tools>pslist -t

pslist v1.28 - Sysinternals PsList
Copyright (C) 2000-2004 Mark Russinovich
Sysinternals

Process information for IS482-39:

Name                Pid Pri Thd  Hnd      VM      WS    Priv
Idle                  0   0   1    0      16      16       0
  System              8   8  48  151    1784     296      88
    smss            188  11   6   36    5328     356    1096
      csrss         204  13  13  557   51296    4656    1816
      winlogon      228  13  18  390   42256    4336    5872
        services    256   9  37  610   35696    6180    2896
          svchost   468   8   9  311   21248    2760    1340
            ndm    2080   8   4   87   20068    2296     836
          SPOOLSV   484   8  15  155   30732    3728    2516
          RsPxa     500   8  12  196   58932   18532    8976
          msdtc     512   8  21  155   28768    3552    1588
          tcpsvcs   628   8  18  272   47988    4464    2336
          svchost   644   8  25  324  148172   18876    6388
          llssrv    672   9   9   96   19404    2136     980
          sfmprint  736   8   2   47   14452    1500     648
          regsvc    812   8   2   36   14196    1388     520
          RsSub     860   8   5   86   20984    3168    1004
          mstask    992   8   7   92   19188    2160     792
          wins     1028   8  19  263   68088    3276    2424
          snmp     1060   8   6  258   38788    3940    1772
          termsrv  1112  10  14  120   52644    3156    1924
            lsarver 1216  8  15  194   64224    4864    3476
          winmgmt  1264   8   4   98   23408     476     964
          winvnc   1312   8   5   83   29788    2820    1052
          dns      1360   8  12  152   23580    2952    1228
```

〔그림 10〕 "시스템취약성 분석"에서 Victim1의 실행 프로세스 분석 화면

3.4 정보보호 교육 적용시 장단점

가상화 기술을 실제 정보보호 교육에 적용함에 있어 장점과 단점을 살펴보면 다음과 같다.

정보보호 교육 적용시 장점

○ 가상화 기술은 새로운 응용 방법을 제시함으로써 다양한 활용이 가능하고 시스템 구성이 편리하다.

- 물리적인 시스템 및 네트워크 환경과 독립적으로 구성된 별도의 격리된 구성이 가능하다.
- 가상 이미지 파일을 복사하는 것만으로 새로운 시

스템 생성이 가능하다.

○ 실제 시스템 공격을 대체함으로써 물리 시스템 백업 및 복구 등의 부작용을 최소화할 수 있으며, 관리의 용이성으로 인하여 효율성이 증가한다.

• x86 기반의 다양한 시스템 구성 가능한데, 대표적으로 Windows, Linux, Solaris, Mac OS 등을 게스트 운영체제로 설치하여 운영할 수 있다.

• 실제 시스템 공격을 통한 희생자 시스템 설치 및 복구가 필요 없고, 백업 파일 복구 만으로 원상 복구가 가능하다.

정보보호 교육 적용시 단점

○ 실제 시스템에 비하여 상대적으로 느리므로 시스템 속도 등 성능을 중요시하는 실습 등에는 부적당하다.

• 일반적으로 가상 환경은 소프트웨어로 구현되어 별도의 계층 구조를 가지므로 물리 시스템에 비교하여 성능 문제를 야기할 수 있다.

• 많은 클라이언트 접속시 소프트웨어 처리로 인해 오버헤드가 발생할 수 있다.

○ 가상 환경은 물리 환경을 흉내(Emulate)내는 것이지 동일한 환경은 아니므로 시스템 특성을 따르는 분야에는 부작용이 발생할 가능성이 있다.

• 가상화 소프트웨어 개발 회사에 따른 드라이버 인식 및 호환성 문제가 발생할 수 있다.

• 특정 시스템 문제로 인하여 물리 환경과 다른 문제를 발생시킬 수 있다.

○ VMware, Virtual PC 등 가상화 소프트웨어 간의 상호 호환성이 결여되어 있다.

• 각각의 장점을 내세우는 가상화 소프트웨어 개발 회사 간의 가상 이미지 파일(*.vmdk, *.vhd 등)에 대한 호환성이 부족하다.

• 호환성 부족으로 인하여 가상화 소프트웨어를 변경해야 하는 경우 가상 환경을 새로 설치해야 하는 문제가 발생한다.

지금까지 사례를 중심으로 정보보호 교육 적용 방법과 장단점을 살펴보았는데, 정보보호 교육 적용시 다음을 고려하여야 한다.

첫째, 정보보호 교육의 특성상 악성코드나 해킹 기술들을 다루기 위한 별도의 격리된 가상 환경을 구성한다.

• 악성코등 감염 등의 부작용을 최소화하기 위하여 물리적인 네트워크와는 다른 구성을 가진 가상 네트워크를 구성한다.

• 가상 환경 상에서 해킹 도구 및 악성코드들이 물리 환경에서와 거의 동일하게 동작하므로 시스템 재설치가 필요없다.

둘째, 가상 머신 이미지 파일 배포만으로 복잡한 설치와 구성의 필요없이 동일한 시스템 및 운영 환경을 구축할 수 있다.

• 가상 머신 이미지 파일을 복사하여 부팅하면 동일한 가상 컴퓨터가 하나 더 생성되므로 최초 이미지 파일을 잘 관리한다.

• 운영체제와 어플리케이션 설치 및 시스템 구성이 복잡한 경우, 하나의 가상 머신을 구성하고 이미지 파일을 복사하면 별도의 설치나 구성없이 동일한 시스템 구성이 가능하다.

셋째, 물리 시스템과 가상 시스템을 적절하게 병행하여 사용하는 경우, 강의 내용에 따라 정보보호 교육의 특성을 잘 반영할 수 있는 실습 도구로 활용할 수 있다.

• 웹 서버, 데이터베이스 서버와 같이 시스템 의존적인 구성이나 성능을 중심으로 하는 환경은 물리 서버로 운영한다.

• 실습을 위하여 공격가능한 취약한 희생자 서버 또는 동일한 환경 구성이 필요하여 배포를 하여야 하는 경우는 가상 서버로 운영한다. 또한, 가상 서버를 악성코드 수집 또는 네트워크 해킹 증거 수집을 위한 Honeypot 용도로도 운영할 수 있다.

Ⅳ. 결 론

가상화 기술은 서버 자원을 효율적으로 사용하기 위하여 많은 기업들이 도입하고 있으며, 최근 운영 비용 절감 및 친환경 IT정책 차원에서도 서버 가상화 기술의 보급 및 이용이 확대되고 있다. 특히 IDC는 x86 서버 시장이 급팽창하고 있으며, 가상 서버의 수가 2005년부터 2010년까지 연평균 40%의 성장률을 보일 것으로 예측하였다[11]. 따라서 가상화 기술은 지속적으로 성장하고 있으며 다양한 가능성을 가진 기술로 인정받고 있다.

본 고에서는 다른 교육과는 달리 해킹과 악성코드를 직접 다루는 정보보호 교육의 특성을 잘 반영할 수 있는 가상화 기술을 이용한 구체적인 정보보호 교육 사례를 살펴보았고, 가상화 기술을 적용한 정보보호 교육의 장단점 및 고려사항을 논의하였다. 가상화 기술을 도입

한 정보보호 교육 방안은 향후 가상화 기술의 발전 방향과 정보보호 교육 특성에 따라 다양하게 활용될 수 있을 것으로 사료되며, 응용분야의 지속적인 연구가 필요할 것으로 판단된다.

참고문헌

[1] 탁정수, "가상화 기술현황과 공공기관 적용 시사점", 정보사회진흥원 정보사회 현안분석 II, 2007.

[2] 한국과학기술정보연구원, "*IT 자원 가상화 기술*", 2005.

[3] Chris Wolf, Erick M. Halter, "*Virtualization From the Desktop to the Enterprise*", Apress, 2005.

[4] Microsoft Virtual PC, http://www.microsoft.com/windows/products/winfamily/virtualpc/default.mspx.

[5] Microsoft Virtual Server, http://www.microsoft.com/windowsserversystem/virtualserver/.

[6] VMware Workstation, http://www.vmware.com/products/ws/.

[7] VMware Server, http://www.vmware.com/products/server/.

[8] Xen, http://www.xen.org/.

[9] Nmap, http://nmap.org/.

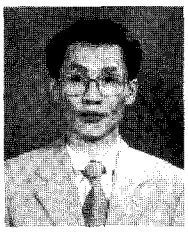
[10] The Metasploit Project, http://www.metasploit.com/.

[11] IDC, "*Virtualization and Multicore Innovations Disrupting the Worldwide Server Market*", 2007.

〈著者紹介〉

신 원 (Shin, Weon)

1996년 2월: 부경대학교 전자계산학과 졸업
1998년 2월: 부경대학교 전자계산학과 석사
2001년 8월: 부경대학교 전자계산학과 박사
2002년 3월~ 2005년 1월: (주)안철수연구소 선임연구원
2005년 3월 ~현재: 동명대학교 정보보호학과 조교수
<관심분야> 악성코드 확산, 컴퓨터 포렌식, 소프트웨어 보안, 암호학 응용



조 성 목 (Cho, Sung-Mok)

1988년 2월: 경북대학교 전자공학과 졸업
1990년 2월: 경북대학교 전자공학과 석사
1995년 2월: 경북대학교 전자공학과 박사
2006년 3월~현재: 동명대학교 정보보호학과 부교수
<관심분야> 서버시스템보안, 무선랜보안