(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0079047
(43) 공개일자 2010년07월08일

(51) Int. Cl.
G06Q 50/00 (2006.01) *G06F 21/00* (2006.01)
(21) 출원번호 10-2008-0137455
(22) 출원일자 2008년12월30일
심사청구일자 2008년12월30일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가1 고려대학교 내
(72) 발명자
인호
서울 용산구 이촌동 402 강촌아파트 109-1604
김도훈
서울 마포구 창전동 삼성아파트 103동 302호
이택
충청남도 아산시 권곡동 579번지
(74) 대리인
특허법인충현

전체 청구항 수 : 총 13 항

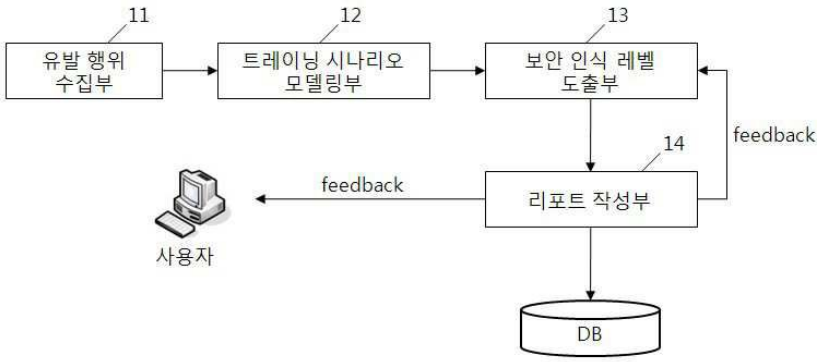
(54) 정보 보안 트레이닝 시스템 및 방법

(57) 요 약

발명은 정보 보안 트레이닝 시스템에 관한 것으로, 보다 상세하게는 정보 보안에 있어 발생할 수 있는 다양한 상황에 대해 사용자 스스로 예방하고 대처할 수 있도록 사용자를 트레이닝 시킬 수 있는 정보 보안 트레이닝 시스템에 관한 것이다.

본 명세서에서 개시하는 정보 보안 트레이닝 시스템은 사용자의 행위에 의해 유발 가능한 행위(유발 행위)들을 수집하는 유발 행위 수집부; 상기 수집된 유발 행위들에 대한 정보 보안 트레이닝에 가장 적합한 트레이닝 시나리오를 모델링하는 트레이닝 시나리오 모델링부; 상기 트레이닝의 진행 중에 관찰되는 사용자 행위가 상기 모델링된 시나리오에 부합하는지 분석하여 상기 트레이닝을 진행 중인 사용자의 보안 인식 레벨을 도출하는 보안 인식 레벨 도출부; 및 상기 도출된 보안 레벨에 기반하여 상기 사용자에게 피드백할 리포트를 작성하는 리포트 작성부를 포함하여 본 시스템 발명의 과제를 해결한다.

대 표 도 - 도1b



이 발명을 지원한 국가연구개발사업

과제고유번호	R0120080001034302008
부처명	한국과학재단
연구사업명	특정기초연구
연구과제명	사용자 취약성 연구를 위한 가상 보안 훈련장
주관기관	고려대학교 산학협력단
연구기간	2008년 05월 01일 ~2009년 02월 28일

특허청구의 범위

청구항 1

사용자의 행위에 의해 유발 가능한 행위(유발 행위)들을 수집하는 유발 행위 수집부;

상기 수집된 유발 행위들에 대한 정보 보안 트레이닝에 가장 적합한 트레이닝 시나리오를 모델링하는 트레이닝 시나리오 모델링부;

상기 트레이닝의 진행 중에 관찰되는 사용자 행위가 상기 모델링된 시나리오에 부합하는지 분석하여 상기 트레이닝을 진행 중인 사용자의 보안 인식 레벨을 도출하는 보안 인식 레벨 도출부; 및

상기 도출된 보안 레벨에 기반하여 상기 사용자에게 피드백할 리포트를 작성하는 리포트 작성부를 포함하는 정보 보안 트레이닝 시스템.

청구항 2

제 1 항에 있어서, 상기 유발 행위 수집부는

상기 유발 행위들 각각에 관찰 코드를 부여하여 분류하는 유발 행위 분류부; 및

상기 사용자의 행위의 상태들의 각 행위 상태에 행위 코드를 부여하는 코드 부여부를 포함하는 것을 특징으로 하는 정보 보안 트레이닝 시스템.

청구항 3

제 2 항에 있어서, 상기 행위 상태들은

리눅스에서 제공하는 Linux Basic Security Module(BSM Module)과 원격 터미널의 사용자 인터페이스 프로토콜(Remote Frame Buffer)을 분석하여 수집되는 것을 특징으로 하는 정보 보안 트레이닝 시스템.

청구항 4

제 2 항에 있어서, 상기 트레이닝 시나리오 모델링부는

상기 부여된 행위 코드를 기반으로, 상기 트레이닝의 진행 중에 관찰되는 사용자 행위의 패턴 분석을 위한 기준 패턴을 생성하여 상기 가장 적합한 트레이닝 시나리오를 모델링하는 것을 특징으로 하는 정보 보안 트레이닝 시스템.

청구항 5

제 4 항에 있어서, 상기 트레이닝 시나리오 모델링부는

상기 행위 상태들을 은닉 모델(hidden model)로 하는 HMM(Hidden Markov Model)을 이용하여 상기 가장 적합한 트레이닝 시나리오를 모델링하는 것을 특징으로 하는 정보 보안 트레이닝 시스템.

청구항 6

제 5 항에 있어서, 상기 보안 인식 레벨 도출부는

상기 트레이닝 진행 중에 관찰되는 사용자의 행위에 대한 관찰 패턴을 생성하는 관찰 패턴 생성부; 및

상기 관찰 패턴과 상기 기준 패턴을 비교하여 양 패턴의 합치의 정도를 근거로 상기 보안 레벨을 도출하는 패턴 비교부를 포함하는 것을 특징으로 하는 정보 보안 트레이닝 시스템.

청구항 7

(a)사용자의 행위에 의해 유발 가능한 행위(유발 행위)들을 수집하는 단계;

(b)상기 수집된 유발 행위들에 대한 정보 보안 트레이닝에 가장 적합한 트레이닝 시나리오를 모델링하는 단계;

(c)상기 트레이닝의 진행 중에 관찰되는 사용자의 행위가 상기 모델링된 시나리오에 부합하는지 분석하여 상기 트레이닝을 진행 중인 사용자의 보안 인식 레벨을 도출하는 단계; 및

(d)상기 도출된 보안 레벨에 기반하여 상기 사용자에게 피드백할 리포트를 작성하는 단계를 포함하는 정보 보안 트레이닝 방법.

청구항 8

제 7 항에 있어서, 상기 (a)단계는

(a1)상기 유발 행위들 각각에 관찰 코드를 부여하여 분류하는 단계; 및

(a2)상기 사용자의 행위 상태들의 각 행위 상태에 행위 코드를 부여하는 단계를 포함하는 것을 특징으로 하는 정보 보안 방법.

청구항 9

제 8 항에 있어서, 상기 (a2)단계에 의한 행위 상태들은

리눅스에서 제공하는 Linux Basic Security Module(BSM Module)과 원격 터미널의 사용자 인터페이스 프로토콜(Remote Frame Buffer)을 분석하여 수집되는 것을 특징으로 하는 정보 보안 트레이닝 방법.

청구항 10

제 8 항에 있어서, 상기 (b)단계는

상기 부여된 행위 코드를 기반으로 상기 트레이닝의 진행 중에 관찰되는 사용자 행위의 패턴 분석을 위한 기준 패턴을 생성하여 상기 가장 적합한 트레이닝 시나리오를 모델링하는 단계인 것을 특징으로 하는 정보 보안 트레이닝 방법.

청구항 11

제 10 항에 있어서, 상기 (b)단계는

상기 행위 상태들을 은닉 모델(hidden model)로 하는 HMM(Hidden Markov Model)을 이용하여 상기 가장 적합한 트레이닝 시나리오를 모델링하는 단계인 것을 특징으로 하는 정보 보안 트레이닝 방법.

청구항 12

제 11 항에 있어서, 상기 (c)단계는

(c1)상기 트레이닝 진행 중에 관찰되는 사용자의 행위에 대한 관찰 패턴을 생성하는 단계; 및

(c2)상기 관찰 패턴과 상기 기준 패턴을 비교하여 양 패턴의 합치의 정도를 근거로 상기 보안 레벨을 도출하는 단계를 포함하는 것을 특징으로 하는 정보 보안 트레이닝 방법.

청구항 13

제 7 항 내지 제 13 항의 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 정보 보안 트레이닝 시스템 및 방법에 관한 것으로, 보다 상세하게는 정보 보안에 있어 발생할 수 있는 다양한 상황에 대해 사용자 스스로 예방하고 대처할 수 있도록 사용자를 트레이닝 시킬 수 있는 정보 보안 트레이닝 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 정보 보안은 개인 또는 기업을 포함한 어느 집단의 운명을 좌우할 정도로 매우 중요한 팩터로 부각되고 있다. 정보 보안은 통상 기술적 요소에 의해서만 즉, 기술적으로 구현된 보안 알고리즘(보안 솔루션)만으로도 충분히

보장될 수 있다고 믿고 있는 경향이 강하다. 그러나 어떠한 보안 솔루션도 스스로 알아서 자체적으로 운영되는 보안 솔루션은 없으며 결정적인 긴급 상황 발생시 이의 대응에 대한 의사결정은 결국 사용자에 의해 이루어지게 된다.

[0003] 이처럼 보안성의 확보는 보안 솔루션이 아닌 사용자 자신에 의해 결정된다고 해도 과언이 아닌데, 보안 사고의 대다수는 집단 내부 또는 외부 인력에 의한 접근권한 오용에서 유발되고 있다고 보고되어 있으며, 보안성에 가장 큰 손해를 초래하는 위협들은 피싱(phishing)이나 랜섬(ransom), 산업스파이와 같은 경제적 사기 사건들로 밝혀지고 있다. 즉, 보안 솔루션에 내재하고 있는 문제에 의해 보안 사고가 발생하는 경우는 극히 드물며 집단 내부 또는 외부의 인력에 의함이 보안 사고의 다수를 차지하고 있다. 아울러 많은 해킹 공격들이 기술적으로 구현된 보안 솔루션(예를 들어 방화벽, IDS)의 방어 라인을 우회하기 위하여 사회 공학적 방법(메신저 대화 이용, 피싱 이메일 발송, 악성 사이트 접속 유도 등)을 이용하기 시작하여 정보 보안에 대한 위협은 점증하고 있다.

[0004] 이러한 보안 위협 사항들은 모두 인간 취약성(Human Vulnerability, 사용자의 정보 보안 의식의 부족을 의미하는 말)을 교묘하게 이용한 것으로, 사용자 취약성 문제 해결을 위한 유일한 대응책은 사용자로 하여금 정보 보안에 대한 심각성 내지는 중요성에 대한 인식을 제고시키는 것인데 이는 사용자에 대한 실제적이고 실용적인 교육과 트레이닝(훈련)을 통해 이루어질 수 있다. 즉 사용자들로 하여금 보안 문제의 심각성을 인식시키고 보안상의 이상 징후에 대해 스스로 예방하고 대처할 수 있는 적절한 트레이닝이 이루어져야 한다.

발명의 내용

해결 하고자하는 과제

[0005] 본 발명은 상기한 필요성에 부응하기 위해 창안된 것으로, 본 발명이 해결하고자 하는 과제는 사용자에게 정보 보안에 관하여 발생할 수 있는 다양한 상황에 대한 대처 능력을 향상시킬 수 있도록 정보 보안에 대한 일반화되고 객관화된 교육 및 트레이닝을 제공할 수 있는 정보 보안 트레이닝 시스템 및 그 방법을 제공하는 것이다.

과제 해결수단

[0006] 상기와 같은 과제를 해결하기 위해 본 명세서에서 개시하는 정보 보안 트레이닝 시스템은

[0007] 사용자의 행위에 의해 유발 가능한 행위(유발 행위)들을 수집하는 유발 행위 수집부; 상기 수집된 유발 행위들에 대한 정보 보안 트레이닝에 가장 적합한 트레이닝 시나리오를 모델링하는 트레이닝 시나리오 모델링부; 상기 트레이닝의 진행 중에 관찰되는 사용자 행위가 상기 모델링된 시나리오에 부합하는지 분석하여 상기 트레이닝을 진행 중인 사용자의 보안 인식 레벨을 도출하는 보안 인식 레벨 도출부; 및 상기 도출된 보안 레벨에 기반하여 상기 사용자에게 피드백할 리포트를 작성하는 리포트 작성부를 포함하여 본 시스템 발명의 과제를 해결한다.

[0008] 상기와 같은 과제를 해결하기 위해 본 명세서에서 개시하는 정보 보안 트레이닝 방법은

[0009] (a)사용자의 행위에 의해 유발 가능한 행위(유발 행위)들을 수집하는 단계; (b)상기 수집된 유발 행위들에 대한 정보 보안 트레이닝에 가장 적합한 트레이닝 시나리오를 모델링하는 단계; (c)상기 트레이닝의 진행 중에 관찰되는 사용자의 행위가 상기 모델링된 시나리오에 부합하는지 분석하여 상기 트레이닝을 진행 중인 사용자의 보안 인식 레벨을 도출하는 단계; 및 (d)상기 도출된 보안 레벨에 기반하여 상기 사용자에게 피드백할 리포트를 작성하는 단계를 포함하여 본 방법 발명의 과제를 해결한다.

효 과

[0010] 본 발명에 의하면, 사용자의 행위 패턴에 가장 최적인(사용자 취약성 극복에 가장 최적인) 트레이닝 시나리오(트레이닝 경로)를 모델링하여 이를 기반으로 보안 트레이닝을 실시하므로, 사용자에게 보다 자연스럽고 효과적으로 정보 보안 인식도를 제고시킬 수 있다. 보다 구체적으로는 사용자들은 보안 교육 커리큘럼을 선택하여 각자가 원하는 내용을 학습 및 실습할 수 있으며 트레이닝 효과에 대한 피드백을 받아 지속적인 보안 레벨 향상을 꾀할 수 있다.

발명의 실시를 위한 구체적인 내용

[0011] 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하고자 하는 과제의 해결 방안의 개요를 우선 제시한다.

[0012] 본 발명은 상기 필요성에 부응하기 위해 특히, 인간 취약성(Human Vulnerability)을 반영하여 정보 보안 트레이

닝 참여자(사용자)의 트레이닝 알고리즘을 제안한다. 단순히 특정 목적의 보안 실험을 위해 일시적으로 구축되는 테스트 베드가 아니라 영구적이고 지속적으로 사용가능하며, 동적으로 구성되는 다양한 트레이닝 시나리오의 생성과 경험을 통해 트레이닝 참여자들로 하여금 일반화되고 객관화된 교육 및 트레이닝(이론과 기술의 실습/실험)을 할 수 있는 트레이닝 알고리즘을 제안한다. 아울러 트레이닝에의 적극적인 참여와 신뢰성 있는 데이터의 확보를 위해 웹 환경의 훈련 참여자 리포트를 통해 효과적인 인터페이스를 제공하고자 한다.

[0013] 이하, 본 발명이 해결하고자 하는 과제의 해결 방안을 명확하게 하기 위한 발명의 구성을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명 시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다. 아울러 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.

[0014] 도 1b 내지 도 1c는 본 시스템 발명의 바람직한 구성을 설명하기 위해 제시한 도면이며, 도 2a 내지 도 2b는 본 방법 발명의 바람직한 흐름을 설명하기 위해 제시한 도면이다.

[0015] 정보 보안 트레이닝 과정은 시작과 종료가 주어지는 한정된 시간 내에서 주어진 트레이닝 미션을 달성하는 것을 목표로 한다. 사용자(트레이닝 참여자)는 트레이닝 시나리오(트레이닝 경로)를 구성하는 트레이닝의 각 진행 단계마다 행할 수 있는 행위(activity)들을 갖는데, 트레이닝 시나리오란, 도 1a에 제시된 바와 같이, 매 진행 단계에서 사용자가 행할 수 있는 행위들의 시간대별 프로세스라고 정의할 수 있다.

[0016] 도 1a를 참조하면, 트레이닝 시나리오는 N개의 단계가 존재하고 각 단계에 M개의 행위 상태가 존재하는데, 이는 이론적으로 트레이닝 시나리오의 개수가 M^N 개만큼의 경우의 수가 발생한다고 할 수 있다. 이는 사용자가 정보 보안 문제가 발생하는 실제 상황에서 보안 사고에 대한 대응에 다양한 경우의 수가 발생할 수 있음을 의미한다. 그러나 이러한 다양한 경우의 수 중에서도 사용자의 상황에 따른 최적의 트레이닝 시나리오는 존재한다. 아직 경험이 많지 않은 보안 트레이닝 참여자들은 최적의 시나리오와는 거리가 먼 불완전하고 불필요한 행위들로 구성되는 행위 프로세스를 갖는 경향이 강하다.

[0017] 따라서 본 발명에서는 주어진 트레이닝 미션 달성을 위해 사용자에게 최적인 트레이닝 시나리오를 HMM(Hidden Markov Model)을 이용해 모델링한다. 이렇게 모델링된 트레이닝 시나리오는 실제로 수행되는 트레이닝 미션에 대해 가장 바람직한 기준을 제공한다. 본 발명에 의한 이러한 HMM 기반의 정보 보안 트레이닝 시스템은 사용자가 트레이닝 중에 수행할 수 있는 행위들을 모니터링하면서 최적의 트레이닝 시나리오에 얼마나 근접하게 트레이닝을 진행 중인가를 분석한다.

[0018] 트레이닝이 종료되면 사용자가 수행한 행위를 분석하여 최적의 트레이닝 시나리오와의 격차를 분석하고 그 분석 결과를 정량적으로 점수화하여 사용자에게 피드백한다. 사용자는 피드백받은 점수를 통해 정보 보안에 요구되는 행위 목록들과의 상대적인 격차를 인지할 수 있고 최적의 트레이닝 시나리오에 비춰 어떤 트레이닝 단계들에 대해 개선이 요구되는가를 인지할 수 있다. 이러한 결과가 피드백으로 사용자에게 지속적으로 전달되면 2차, 3차의 연이은 트레이닝을 통해 사용자 취약성의 개선 효과를 볼 수 있다.

[0019] 본 발명은 유발 행위 수집부(11)에 의해 우선 유발 가능한 사용자의 행위(유발 행위)들을 수집하여 가공하는 것으로 시작된다(s11). 유발 행위 분류부(111)는 유발될 수 있는 사용자의 각 행위에 소정의 코드를 부여하여 분류한다(s211). 이때 분류의 기준은 예를 들어 아래 표 1의 대분류(관찰 코드, 관찰 가능한 정보)를 따르며, 소정의 코드란 바로 관찰 코드를 의미한다.

[0020]

관찰 코드 (Observable Codes)	**사용자가 터미널(단말)을 통해 관찰 가능한 정보(사용자에 의한 유발 행위, User Command)**
01	vi http_d.conf
02	vi /etc/passwd
03	[라인추가] nobody:x:99:99:nobody:/:/sbin/nologin
04	[라인수정] user nobody [라인수정] group nobody
05	[라인수정] DocumentRoot

06	chown 0 */bin chown 0 */conf chown 0 */logs
07	chgrp 0 */bin chgrp 0 */conf chgrp 0 */logs
08	chmod 755 */bin chmod 755 */conf chmod 755 */logs
09	chown 0 */httpd
010	chgrp 0 */httpd
011	chmod 511 */httpd
012	cd */cgi-bin
013	rm
014	[라인추가] IncludesNoexec
015	[라인수정] ScriptAlias /cgi-bin/
016	[라인추가] <Limit PUT DELETE>
017	[라인추가] order, deny, allow

[0021] <표 1>

[0022] 예를 들어 사용자가 vi http d.conf에 해당하는 행위를 유발시켰을 때, 이 행위는 관찰 코드 01로 분류됨을 의미한다. 즉, 유발 행위 분류부(111)는 사용자가 터미널(단말)을 통해 관찰 가능한 정보(User Command)를 관찰 코드(Observable Codes) ON(N은 자연수)으로 분류하는 것이다. 여기서, *는 사이에 어떤 문자가 와도 됨을 의미한다.

[0023] 다음으로 코드 부여부(112)는, 예를 들어 아래 표 2에서 볼 수 있는 바와 같이, 사용자의 행위 상태(은닉 상태, Hidden State)들을 정의하여 각 행위 상태에 대해 코드(행위 코드)를 부여한다(s212). 이때 사용자의 행위 상태들의 정의는 리눅스에서 제공하는 Linux Basic Security Module(BSM Module)과 원격 터미널의 사용자 인터페이스 프로토콜(Remote Frame Buffer)을 분석하여 이루어진다.

[0024]

행위 상태 (은닉 상태, Hidden State)		**샘플 관찰코드 시퀀스 패턴(기준 패턴 또는 최적 패턴) (Observable Pattern Sequence)**
코드	**설명**	
H1	계정 및 그룹 설정	(01,04) (02,04)
H2	웹 컨텐츠 관리	(01,05)
H3	파일 및 디렉토리 권한	(06, 07, 08, 09, 010, 011) 이 관찰코드 시퀀스는 순서가 상관없음
H4	불필요한 문서 제거	(012, 013)
H5	디렉토리 리스팅 방지	(01, 014)
H6	CGI 실행 통제	(01, 015)
H7	HTTP METHOD 통제	(01, 016)
H8	사용자 접근 권한 통제	(01, 017)

[0025] <표 2>

[0026] 트레이닝 시나리오 모델링부(12)는 상기 수집된 유발 행위들에 대한 정보 보안 트레이닝에 가장 적합한 트레이닝 시나리오를 모델링하는데, 구체적으로는 상기 부여된 행위 코드(H1, H2, …, H8)를 기반으로 상기 사용자의 정보 보안 트레이닝에 가장 적합한 트레이닝 시나리오를 모델링한다(s22). 트레이닝 시나리오 모델링부(12)는 상기 정의된 사용자 행위에 해당하는 코드(H1, H2, …, H8)에 근거하여 트레이닝 진행 시점의 행위 패턴의 분석을 위한 기준 패턴(샘플 관찰코드 시퀀스 패턴)을 생성하여 최적의 트레이닝 시나리오를 모델링한다. 생성된 기준 패턴은 패턴 DB에 저장된다.

[0027] 한편, 위에서 본 바와 같이, 관찰 코드에 근거하여 사용자의 행위 상태를 찾아내게 되는데, 트레이닝 시나리오 모델링은 이러한 행위 상태를 은닉 모델로 하는 HMM(Hidden Markov Model)을 이용하여 이루어진다.

[0028] 도 1d에는 최적의 트레이닝 시나리오를 모델링하기 위해, HMM에 적용하고자 하는 사용자의 은닉 상태 코드(행위 상태 코드)와 사용자의 관찰 코드의 천이 상태가 상태 다이어그램(state diagram)으로 표현되어 있다. 보안 트레이닝을 수행하기 위한 상태 집합(트레이닝 시나리오의 단계별 요구 행위 상태)을 S = (s1, s2, s3, …, st)라 하고, 이산적인 관측 심벌은 V = (v1, v2, v3, ..., vN)라 하자. HMM은 아래와 같은 세 가지 매개 변수 A, B, π를 갖게 된다.

[0029] Θ = (A, B, π).

[0030] 이들의 값(A, B, π, Θ)이 정해지면 HMM이 만들어진 셈이다. 즉, 트레이닝 시나리오 Θ를 추정하는 작업이 바로 HMM에 의한 트레이닝 시나리오 모델링 작업인 것이다.

[0031] (1) 상태 천이 확률

[0032] 상태 천이 확률 A = a_{ij}는 HMM이 작동하는 도중 사용자의 현재의 보안 관련 행위로부터 다음의 보안 관련 행위를 결정하는 요소이다. a_{ij}는 시간 t에 상태 si에 있다가 t+1에 sj로 이동할 확률이다. 이것을 수식으로 쓰면 아래와 같다.

[0033] $$a_{ij} = P(q_{t+1} = s_j \mid q_t = s_i), 1 \le i, j \le n \quad , \quad \sum_{j=1}^{n} a_{ij} = 1$$.

[0034] 두 번째 식의 조건은 a_{ij}가 확률이기 때문이다. n은 사용자 행위의 개수이다.

[0035] (2) 관측 심벌 확률

[0036] 관측 심벌 확률 B = $b_j(v_k)$는 HMM이 특정 행위에 도달하였을 때 그 행위에서 관측될 심벌(기호)을 결정하는 요소이다. $b_j(v_k)$는 행위 s_j에서 심벌 v_k가 관측될 확률이다. 이것을 수식으로 쓰면 다음과 같다.

[0037] $$b_j(v_k \mid q_t = s_j), 1 \le j \le n, 1 \le k \le m \quad , \quad \sum_{k=1}^{m} b_j(v_k) = 1$$.

[0038] 두 번째 식의 조건은 $b_j(v_k)$가 확률이기 때문이다. m은 심벌의 개수이다.

[0039] (3) 초기 상태 확률 π = |π_i|

[0040] π는 사용자가 보안 관련 행위를 어느 상태에서 시작할 지를 결정하는 데 쓰인다. π_i는 상태 si 에서 시작할 확률이다. 이것을 수식으로 쓰면 다음과 같다.

[0041] $$\pi_i = P(q_1 = s_i), 1 \le i \le n \quad , \quad \sum_{i=1}^{n} \pi_i = 1$$.

[0042] 두 번째 식의 조건은 π_i가 확률이기 때문에 만족되어야 한다.

[0043] 이처럼, HMM을 이용하여 트레이닝 시나리오를 모델링하기 위해 산출되어야 할 확률은 상태 천이 확률 A, 관측 심벌 확률 B, 초기 상태 확률 π이며, 각 확률이 큰 값을 가지는 방향으로 최적의 트레이닝 시나리오(트레이닝 경로) Θ가 모델링된다. 예를 들어 도 1a에서 점선 경로가 최적의 트레이닝 시나리오라 볼 수 있다. 트레이닝 시나리오 모델링에 의해 각 행위 코드에 대한 샘플 시퀀스 패턴(기준 패턴 또는 최적 패턴)이 관찰 코드의 열(column)의 형태로 상기 표 2에서와 같이 생성되며, 이 패턴은 사용자의 트레이닝 진행 중의 행위에 대해 분석되는 경우 그 분석의 결과로 나와야 할 가장 바람직한 패턴이다.

[0044] 보안 인식 레벨 도출부(13)는, 상기 모델링된 트레이닝 시나리오를 기반으로, 트레이닝 진행 중에 관찰되는 사용자 행위가 상기 모델링된 시나리오에 부합하는지 분석하여 트레이닝을 진행 중인 사용자의 보안 인식 레벨을 도출한다(s23). 이는 상기 트레이닝 시점의 사용자의 행위가 상기 모델링된 트레이닝 시나리오에 얼마나 근접하는가(근접도)를 분석하는 것으로 이루어진다.

[0045] 이를 위해 관찰 패턴 생성부(131)는 우선 상기 트레이닝 시나리오 모델 Θ = (A, B, π)을 이용하여 상기 관찰되는 행위(피 관찰행위)에 대한 관찰 패턴[O = (O1,O2, …,On)]을 아래와 같이 생성한다(s231).

[0046] (1) 피 관찰행위의 초기 상태 확률 π에 따라 피 관찰행위의 초기 상태 si을 선택한다.

[0047] (2) 초기 시간을 1(t = 1)로 한다.

[0048] (3) 관측 심벌 확률 B에 따라 상기 피 관찰행위의 관찰 코드 Ot을 생성한다.

[0049] (4) 그 상태에서 상태 천이 확률 a_{ij}에 따라 초기 상태 si에서 새로운 상태로 옮긴다.

[0050] (5)새로운 상태에서 위의 (3) 내지 (4)를 반복하여 또 다른 상태에서의 관찰 코드를 생성하고, 생성된 모든 관찰 코드를 열(column)의 형태로 구성하여 상기 피 관찰행위에 대한 관찰 패턴으로 한다.

[0051] 패턴 비교부(132)는 이렇게 생성된 관찰 패턴의 관찰 코드와 기준 패턴의 관찰 코드를 비교하여 각 관찰 코드의 합치의 정도를 근거로 사용자의 보안 레벨을 도출한다(s232).

[0052] 리포트 작성부(14)는 상기 도출된 보안 레벨에 기반하여 사용자에게 피드백할 리포트를 작성한다(s24). 작성된 리포트는 별도의 DB에 저장되며 아울러 보안 레벨 도출부(13)에 피드백하여 차후의 행위 패턴 분석에 사용되도록 한다.

[0053] 도 3a 내지 도 3e에 리포트 작성부에 의해 작성되는 리포트들의 일례가 제시되어 있다.

[0054] 도 3a의 경우는 트레이닝이 진행되기 시작할 때 리포트 작성부(14)에 의해 사용자에게 제공되는 초기 리포트 화면이다. 도 3a에서 Evaluation Part는 평가할 항목의 대분류를 위한 코드를 의미하며, 해당 코드는 수행해야 할 행동들의 집합을 의미한다. Current State of the degree of Training은 각 코드별 현재 트레이닝이 된 정도를 표현한다. Report History는 각 트레이닝(Education Session, 1st Training, 2nd Training, 3rd Training)에 대한 세부항목을 표시하며, 각 트레이닝마다 탭이 만들어진다. Education Session은 기초 지식을 체크하는 시험을 의미하며, Score는 각 문제의 정답수를 점수로 평가하는 수치를 나타낸다. Description은 각 코드별 트레이닝에 대한 평가 주제를 나타낸다.

[0055] 첫 번째 트레이닝이 끝나면 리포트 작성부(14)에 의해 도 3b와 같은 리포트 화면이 사용자에게 제공된다.

[0056] 도 3b에서 1'st Training는 첫 번째 트레이닝을 의미하는 것으로 이에 대한 세부 결과를 보여준다. # of mistakes 는 실수를 한 행동의 수를 의미하며, List of Feedback은 실수한 목록의 제목을 보여주는 창과 상세내용을 보여주는 것으로 사용자는 자신의 실수에 대해서 인식을 했다면 OK 버튼을 누름으로 받았음을 인정한다. 피드백의 결과는 다음 번째 Training에서 # of mistakes의 수의 증감으로 평가된다.

[0057] 두 번째 트레이닝이 끝나면 리포트 작성부(14)에 의해 도 3c와 같은 리포트 화면이 사용자에게 제공된다.

[0058] 1차 트레이닝에서 E01에 대한 실수가 1이였는데, 피드백을 통해서 실수가 0으로 되었다. 그래서 Final Report칸에 E01의 트레이닝이 1차에서 끝났음을 표현한다.

[0059] 두 번째 트레이닝이 끝난 후 피드백을 통해 3차 트레이닝이 종결되면, 트레이닝 리포트 작성부(14)에 의해 도 3d와 같은 리포트가 사용자에게 제공된다.

[0060] 3차 트레이닝에서는 2차 트레이닝시에 0개의 실수를 기록한 E01번이 트레이닝 목록에서 사라진다. 그리고 피드백을 통해서 E02~4번까지의 모든 실수를 줄였기 때문에 3차 트레이닝에서 모든 트레이닝이 종료되었음을 나타낸다.

[0061] 한편 모든 트레이닝 과정이 종료되면 리포트 작성부(14)에 의해 도 3e에서와 같은 최종 리포트가 사용자에게 제공된다.

[0062] 교육란을 보면 문제를 맞춘 개수를 기반으로 점수가 매겨짐을 알 수 있으며, N차 훈련 단계는 Training과 Feedback단계로 나누어지는데 Training단의 점수는 각 실수의 위험도를 기반으로 감점을 하여 점수를 매긴다. Feedback단계는 N+1 Training단계에서 실수가 얼마나 줄었는지를 기반으로 점수가 매겨지고 최종적으로 채점인이 자신의 의견을 작성할 수 있다.

[0063] 본 방법발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0064] 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 유무선 네트워크를 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가

읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0065] 이제까지 본 발명에 대하여 그 바람직한 실시예를 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다.

[0066] 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 균등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면의 간단한 설명

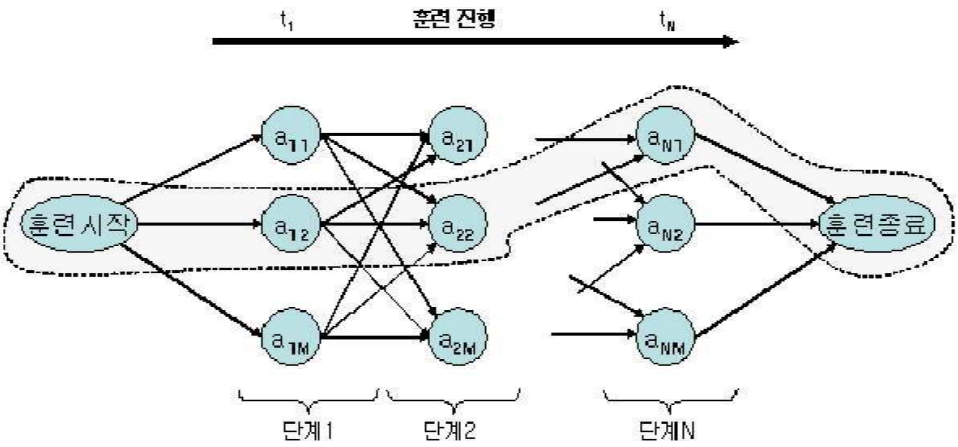
[0067] 도 1a 내지 도 1d는 본 시스템 발명의 바람직한 구성 및 본 방법 발명에 관한 관련 사항을 설명하기 위해 제시한 도면이다.

[0068] 도 2a와 도 2b는 본 방법 발명의 흐름을 제시한 도면이다.

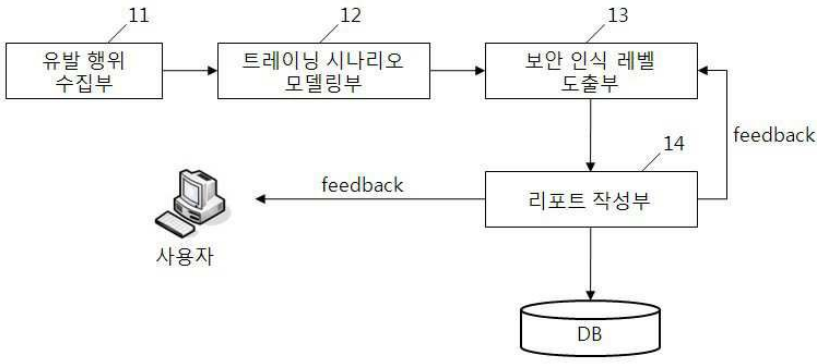
[0069] 도 3a 내지 도 3e는 리포트 작성부에 의해 작성되는 리포트들의 일례를 제시한 도면이다.

도면

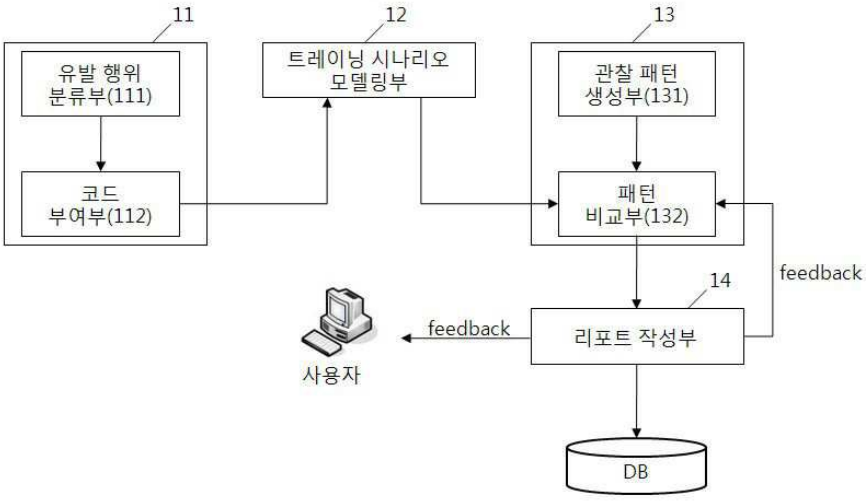
도면1a



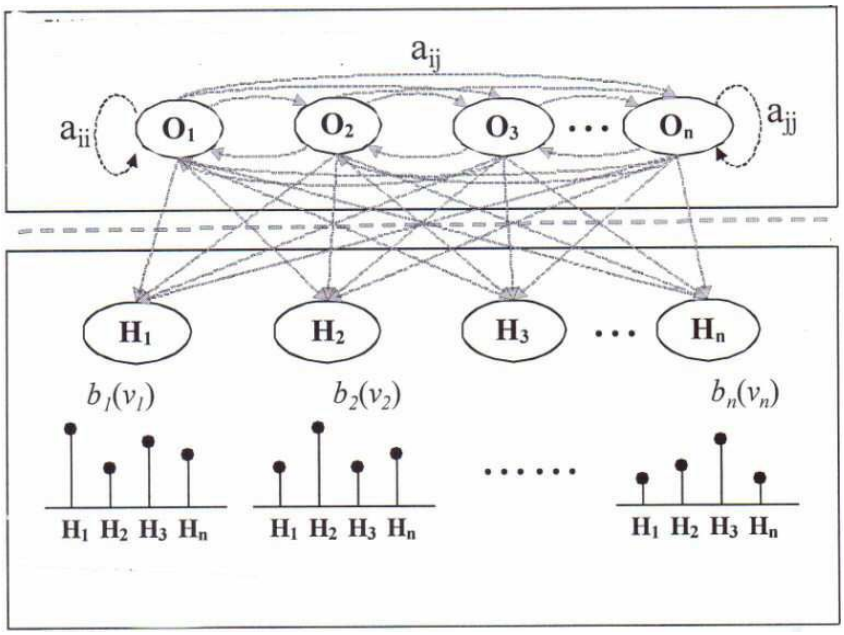
도면1b



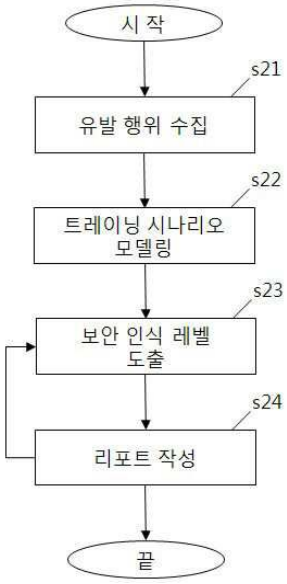
도면1c


11
12
13
유발 행위
분류부(111)
코드
부여부(112)
트레이닝 시나리오
모델링부
관찰 패턴
생성부(131)
패턴
비교부(132)
14
feedback
feedback
리포트 작성부
사용자
DB

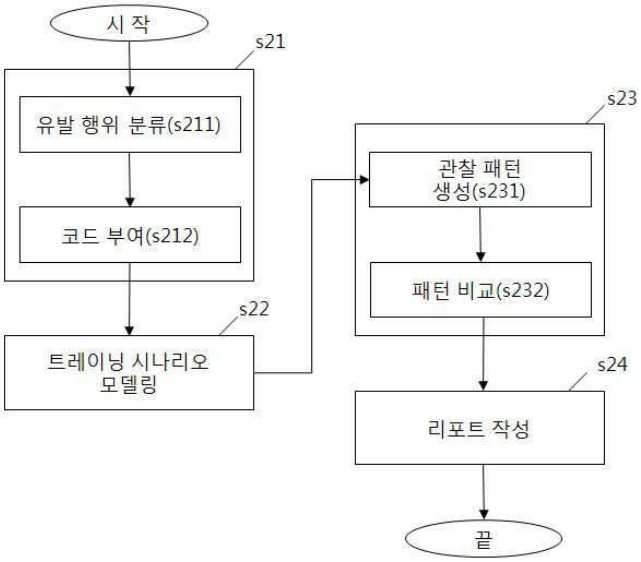
도면1d


a_{ij}
a_{ii}
O_1
O_2
O_3
O_n
a_{jj}
H_1
H_2
H_3
H_n
$b_1(v_1)$
$b_2(v_2)$
$b_n(v_n)$
H_1 H_2 H_3 H_n
H_1 H_2 H_3 H_n
H_1 H_2 H_3 H_n

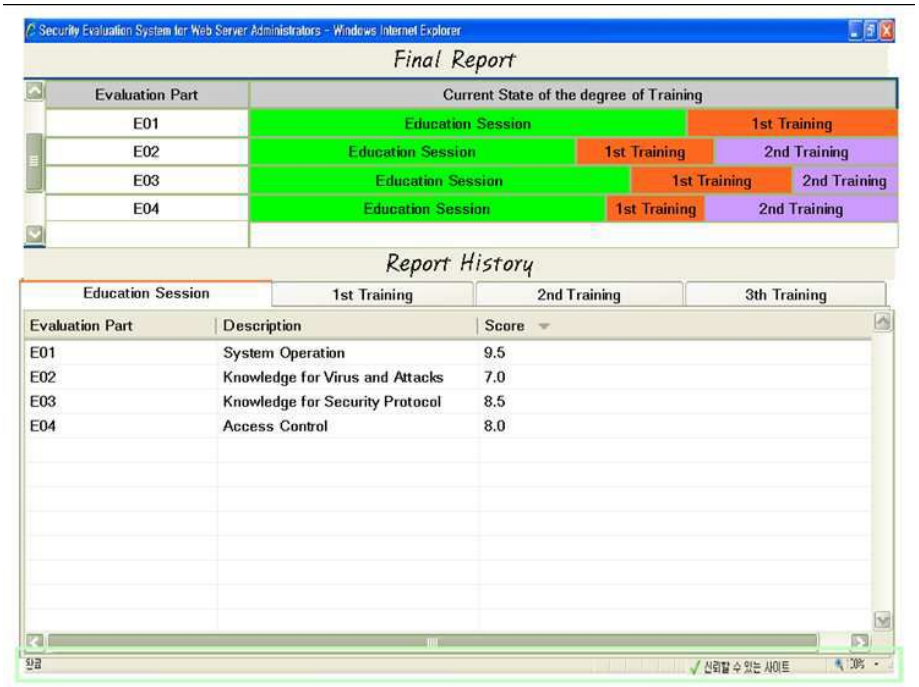
도면2a


시 작
s21
유발 행위 수집
s22
트레이닝 시나리오 모델링
s23
보안 인식 레벨 도출
s24
리포트 작성
끝

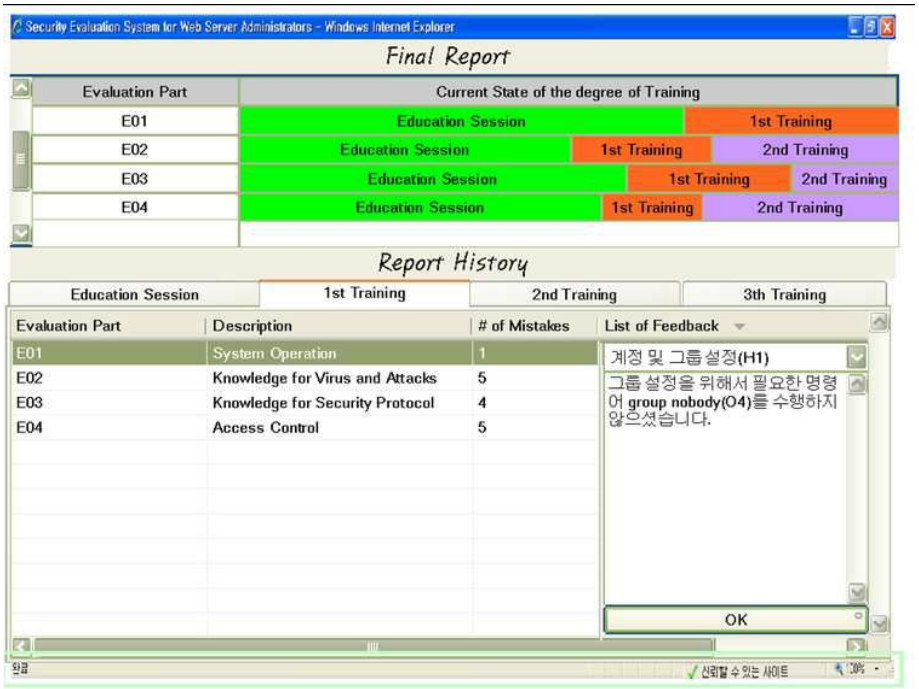
도면2b


시 작
s21
유발 행위 분류(s211)
코드 부여(s212)
s22
트레이닝 시나리오 모델링
s23
관찰 패턴 생성(s231)
패턴 비교(s232)
s24
리포트 작성
끝

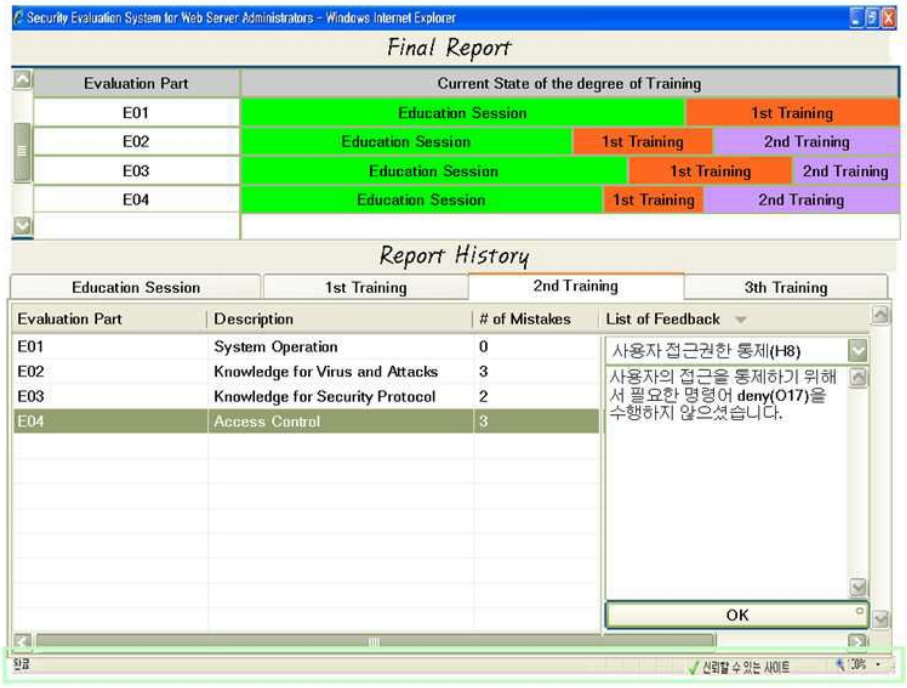
도면3a


Security Evaluation System for Web Server Administrators - Windows Internet Explorer
Final Report
Evaluation Part
Current State of the degree of Training
E01
Education Session
1st Training
E02
Education Session
1st Training
2nd Training
E03
Education Session
1st Training
2nd Training
E04
Education Session
1st Training
2nd Training
Report History
Education Session
1st Training
2nd Training
3th Training
Evaluation Part
Description
Score
E01
System Operation
9.5
E02
Knowledge for Virus and Attacks
7.0
E03
Knowledge for Security Protocol
8.5
E04
Access Control
8.0

도면3b


Security Evaluation System for Web Server Administrators - Windows Internet Explorer
Final Report
Evaluation Part
Current State of the degree of Training
E01
Education Session
1st Training
E02
Education Session
1st Training
2nd Training
E03
Education Session
1st Training
2nd Training
E04
Education Session
1st Training
2nd Training
Report History
Education Session
1st Training
2nd Training
3th Training
Evaluation Part
Description
# of Mistakes
List of Feedback
E01
System Operation
1
계정 및 그룹설정(H1)
그룹 설정을 위해서 필요한 명령어 group nobody(O4)를 수행하지 않으셨습니다.
E02
Knowledge for Virus and Attacks
5
E03
Knowledge for Security Protocol
4
E04
Access Control
5
OK

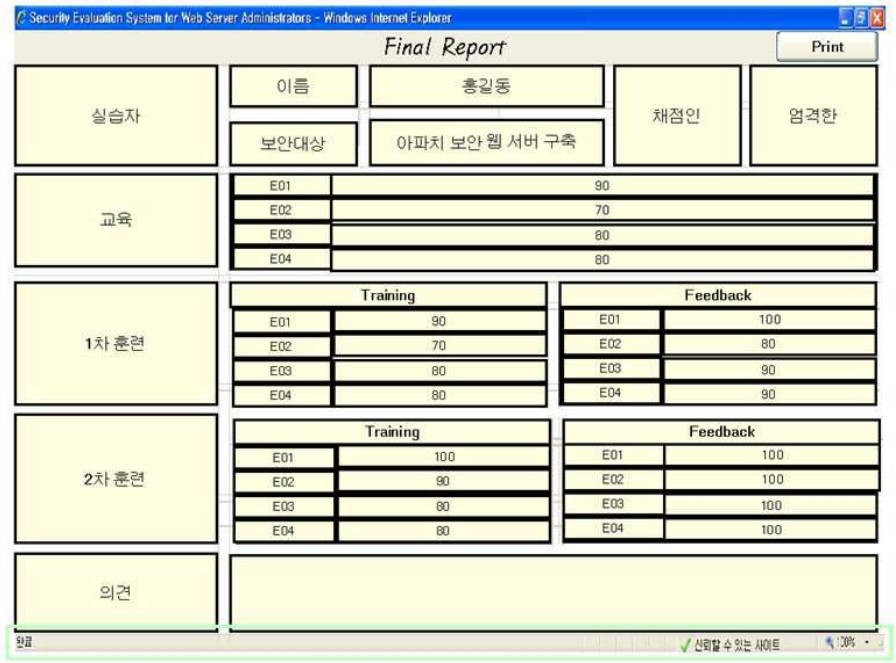
도면3c


Security Evaluation System for Web Server Administrators - Windows Internet Explorer
Final Report
Evaluation Part
Current State of the degree of Training
E01
Education Session
1st Training
E02
Education Session
1st Training
2nd Training
E03
Education Session
1st Training
2nd Training
E04
Education Session
1st Training
2nd Training
Report History
Education Session
1st Training
2nd Training
3th Training
Evaluation Part
Description
# of Mistakes
List of Feedback
E01
System Operation
0
E02
Knowledge for Virus and Attacks
3
E03
Knowledge for Security Protocol
2
E04
Access Control
3
사용자 접근권한 통제(H8)
사용자의 접근을 통제하기 위해서 필요한 명령어 deny(O17)을 수행하지 않으셨습니다.
OK

도면3d


Security Evaluation System for Web Server Administrators - Windows Internet Explorer
Final Report
Evaluation Part
Current State of the degree of Training
E01
Education Session
1st Training
E02
Education Session
1st Training
2nd Training
E03
Education Session
1st Training
2nd Training
E04
Education Session
1st Training
2nd Training
Report History
Education Session
1st Training
2nd Training
3th Training
Evaluation Part
Description
# of Mistakes
List of Feedback
E02
Knowledge for Virus and Attacks
0
E03
Knowledge for Security Protocol
0
E04
Access Control
0
OK

도면3e


Security Evaluation System for Web Server Administrators - Windows Internet Explorer
Final Report
Print
실습자
이름
홍길동
보안대상
아파치 보안 웹 서버 구축
채점인
엄격한
교육
E01 90
E02 70
E03 80
E04 80
1차 훈련
Training
E01 90
E02 70
E03 80
E04 80
Feedback
E01 100
E02 80
E03 90
E04 90
2차 훈련
Training
E01 100
E02 90
E03 80
E04 80
Feedback
E01 100
E02 100
E03 100
E04 100
의견
완료
신뢰할 수 있는 사이트