RAPID7

취약점 진단과 모의 해킹

Nexpose / Metasploit

Rapid7 소개

세계 최고수준의 취약점 진단 기술

2000년 설립 미국 보스턴

nexpose®

2004년 Nexpose 출시
$59M 펀딩 (약 625억원)

90%+

2004 ~ 2011년까지
90%이상 연평균 성장

100여개국 5,600여 고객

보안 리서치 영역의 리더

RAPID7 LABS

Metasploit 설립자이며
Rapid7 CRO인 HD
Moore에 의해 리딩

200,000

오픈소스 컴뮤니티에
공헌하는 전 세계
20만명의 회원들

최신 위협 동향을 반영

metasploit®

세계에서
가장 많이 사용되는
모의침투테스트 툴

insightIDR

속임수기반 공격을
탐지하기 위한 가장
효과적인 솔루션

고객과 긴밀한 파트너쉽

200+

올해 12개 연합
프로그램에 참여한 200여
고객과 파트너쉽

96%+

Frontline에서
기술지원으로 97%
고객만족 평가

Gartner Market Scope for Vulnerability Assessment

Gartner **Strong Positive**

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
Beyond Security				x	
BeyondTrust/eEye Digital Security				x	
Critical Watch				x	
Digital Defense		x			
McAfee					x
nCircle				x	
Qualys					x
Rapid7					x
Saint			x		
Tenable Network Security					x
Trustwave		x			

Source: Gartner, *Market Scope for Vulnerability Assessment*, Sep. 2013

FORRESTER®

Source: *Forrester Wave for Vulnerability Management*, Q2/2010

SANS BEST OF 2014 WINNER IN Vulnerability Assessment

Vulnerability Assessment

Winner:
Rapid7

Honorable Mention:
Tenable
Qualys

https://www.sans.org/press/announcement/2015/03/30/1

SC MAGAZINE AWARDS 2014 WINNER Honored in the U.S.

SC MAGAZINE AWARDS 2015 WINNER Honored in the U.S.

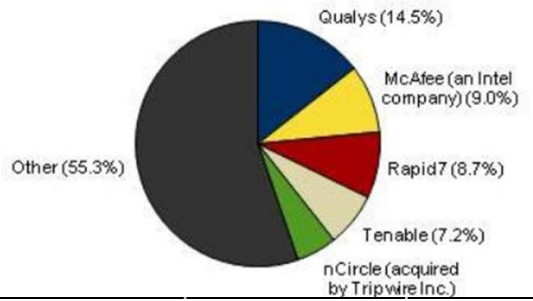
2015 SC AWARDS U.S.
Reader Trust Award
BEST VULNERABILITY MANAGEMENT SOLUTION

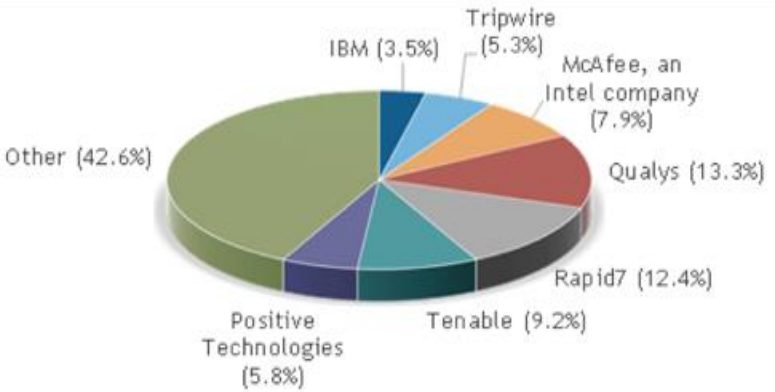
WINNER
Rapid7 for Nexpose Ultimate

Latest IDC Market Share report dated Nov 2015

Filing Information: August 2013, IDC #242465e, Volume: 1
Security Products: Market Analysis

Worldwide Device Vulnerability Assessment Revenue Share by Vendor, 2012





Source

IDC WW Device Vulnerability Management Assessement Market Share by Vendor						
	Published 8/2013	Published 8/2014	Published 11/2015	Market Share Gain	CAGR Growth%	
	2012	2013	2014			
Qualys	14.50%	14%	13.30%	-0.7%	-4%	
Rapid7	8.70%	10.90%	12.40%	1.5%	20%	
McAfee	9%	8.60%	7.90%	-0.7%	-6%	
Tenable	7.20%	7.90%	9.20%	1.3%	13%	
nCircle/TripWire	5.30%	5.90%	5.30%	-0.6%	1%	
Market Size	US$569.5M	US$628.4M	US$784.5M		17.59%	

Source: IDC, August 2014

RAPID7

Feature Comparison

Policy Compliance	McAfee MVM	Nexpose MVM	Nexpose Enterprise
CIS Benchmarks / USGCB	•	•	•
CIS Benchmarks Certified		•	•
SCAP 1.2		in certification	in certification
Policy Editor / SCAP Upload		•	•

Prioritization	McAfee MVM	Nexpose MVM	Nexpose Enterprise
CVSS Scoring / Asset Importance	•	•	•
Advanced Risk Scoring		•	•
Exploit and Exploit Kits		•	•
Validated Vulnerabilities with Rapid Metasploit®		additional fee	additional fee

Dashboards & Reporting	McAfee MVM	Nexpose MVM	Nexpose Enterprise
Dashboards	•	•	•
Pre-built Report Templates	•	•	•
Customizable Report Templates	•	•	•
SQL Query	•	•	•
Top Remediation Guidance		•	•
Department Benchmarking		•	•

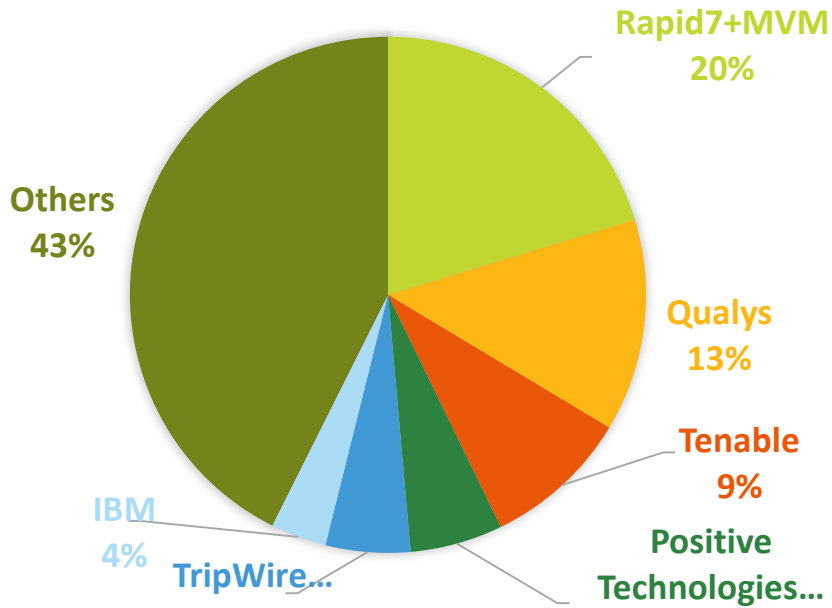
Security and IT Integrations	McAfee MVM	Nexpose MVM	Nexpose Enterprise
Open API	•	•	•
McAfee ESM (SIEM)	•	•	•
McAfee ePO	•	coming soon	coming soon
McAfee DXL		coming soon	coming soon
Third Party Integrations	10+	40+	40+

nexpose®

Intel Security's Exclusive Partner for Vulnerability Management

Licensing/Administration	McAfee MVM	Nexpose MVM	Nexpose Enterprise

BASED ON 2014 MARKETSHARE



Vulnerability Assessment	McAfee MVM	Nexpose MVM	Nexpose Enterprise
Authenticated Scanning	•	•	•
Comprehensive Coverage	•	•	•
Automatic Content Updates	•	•	•
Custom Vulnerability Checks	•	•	•
Mobile Devices (Android, iOS)	end of life*	•	•
OWASP Top 10		•	•
VMware NSX through Hypervisor		•	•

** This capability is only available when using with McAfee Asset Manager, which was recently announced end-of-life.*

Symantec CCS Vulnerability Manager 10 Administrator's Guide

Using anti-virus software on the server

Anti-virus programs may sometimes impact critical operations that are dependent on network communication, such as downloading updates and scanning. Blocking the latter may cause degraded scan accuracy.

If you are running anti-virus software on your intended host, configure the software to allow the application to receive the files and data that it needs for optimal performance in support your security goals:

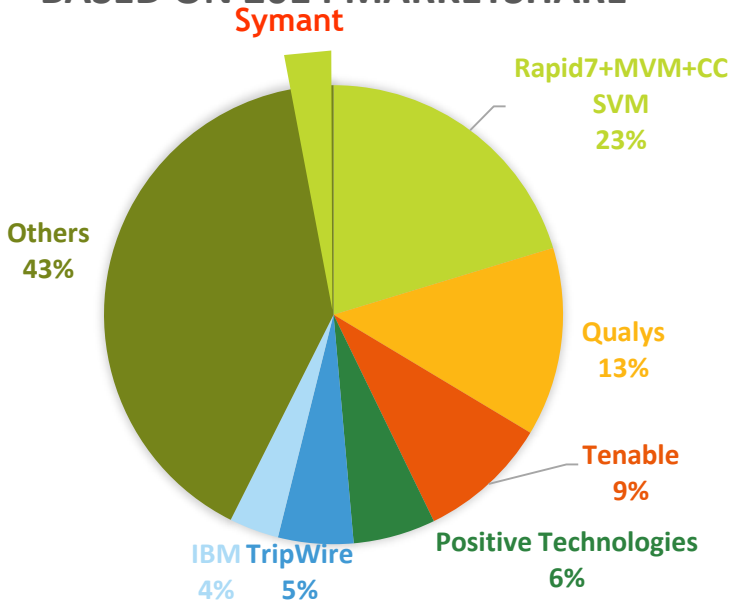
- Add the application update server, updates.rapid7.com, to a whitelist, so that the application can receive updates.
- Add the application installation directory to a whitelist to prevent the anti-virus program from deleting vulnerability- and exploit-related files in this directory that it would otherwise regard as "malicious."

Consult your anti-virus vendor for more information on configuring the software to work with the application.

Activating your license with a license file

If your Security Console does not have access to the Internet or to the updates.rapid7.com server, you can activate your license with a license file. Provided to you by the Account Management team, this file has a *.lic* extension and lists all the features and scanning capacities that are available with your license. To activate wth a license file:

BASED ON 2014 MARKETSHARE



제품 포트폴리오

보안 취약점 관리

nexpose®
appspider

숨겨진 IT 자산의 탐색 식별

취약점 보안설정, 보안통제 영역의 위험 통합 진단

위험 순위별 개선조치 자동 리포트

컴플라이언스 리포트

사용자 위험 관리

insightIDR

- 네트워크 경계, 모바일, 클라우드에 걸쳐 사용자의 비정상 행위 탐지 및 모니터링
- 침해를 당한 사용자 식별
- 보안 이벤트에 즉각적인 대응
- 차세대 SIEM

모의침투 테스트

metasploit®

- 취약점 위험 및 방어상태 검증을 위한 공격 시뮬레이션
- 자동화된 모의침투 테스트
- 피싱 노출 및 보안 의식 테스트
- 웹 어플리케이션 침투 테스트

Closed Loop 보안 진단 플랫폼

nexpose®

취약점 관리와
구성 평가

위험 평가

위험 확인

metasploit®

침투 테스트와
위협 확인

한국 고객 – 120여 중요 고객이 사용 중

9

Vulnerability

CVE vs. CCE

CVE (COMMON VULNERABILITIES & EXPOSURES)

- 공개적으로 알려진 사이버보안 영역의 취약점을 표준화하여 정의한 목록
- 글로벌 IT 밴더, 보안 제조업체, 대학 연구소, 정부 기관, 기타 보안 전문가 등 수많은 단체의 전문가들이 취약점 표준화에 참여
- 미 정부 산하 비영리 기구 MITRE에서 유지 관리 수행

CCE (COMMON CONFIGURATION ENUMERATION) – 보안 점검 항목

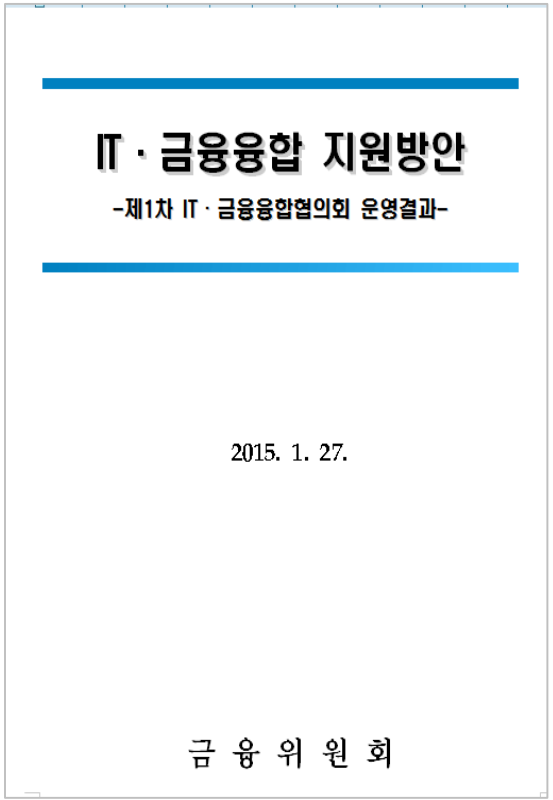
- 시스템 상의 보안상 중요한 설정 항목 및 가이드라인

ISMS 인증 심사기준 / 주요정보통신 시설 취약점 평가 지침

11.2.10	취약점 점검	정보시스템이 알려진 취약점에 노출되어 있는 지 여부를 확인하기 위하여 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치하여야 한다.	정보시스템 취약점 점검 절차를 수립하여 정기적으로 점검을 수행하고 있는가?	○ 정보시스템 취약점 점검 정책과 절차를 다음과 같은 내용을 포함하여 수립하여야 한다. - 취약점 점검 대상 (예 : 서버, 네트워크 장비 등) - 취약점 점검 주기 - 취약점 점검 담당자 및 책임자 지정 - 취약점 점검 절차 및 방법 등 ○ 정보시스템 중요도에 따라 주기적으로 다음과 같은 내용을 포함하여 취약점 점검을 실시하여야 한다. - 라우터, 스위치 등 네트워크 장비 구성, 설정 취약점 - 서버 OS, 보안 설정 취약점 - 방화벽 등 정보보호시스템 취약점 - 어플리케이션 취약점 - 웹서비스 취약점 - 스마트기기 및 모바일 서비스(모바일 앱 등) 취약점 ○ 취약점 점검 시 회사의 규모 및 보유하고 있는 정보의 중요도에 따라 모의침투테스트를 수행하는 것을 고려하여야 한다. ○ 취약점 점검 시 이력관리가 될 수 있도록 '점검일시', '점검대상', '점검방법', '점검내용 및 결과', '발견사항', ' 조치사항' 등이 포함된 보고서를 작성하여야 한다.
			발견된 취약점에 대한 조치를 수행하고 그 결과를 책임자에게 보고하고 있는가?	○ 취약점 점검 결과 발견된 취약점별로 대응방안 및 조치결과를 문서화하여야 하며 조치결과서를 작성하여 책임자에게 보고하여야 한다. - 불가피하게 조치를 할 수 없는 취약점의 경우 그 사유를 명확하게 확인하고 책임자에게 보고하여야 한다.

- 정보통신기반 보호법 제9조 - 주요정보통신 기반시설 취약점 평가 가이드
  - 주요 정보통신 기반 보호시설 관리기관은 **매년 취약점 분석, 평가를 실시**하여야 함(주요정보통신 기반시설 확대, 13년 209개 → 현 292개)
- 실제 ISMS 규정 내용은 CVE 취약점 진단도 포함하고 있으나 국내에서는 **CCE 분야에 한정된 보안설정 점검 항목**만 준수하도록 공공, 금융회사에 배포하고 있는 상황
- **결국, CVE 기반 취약점 진단을 강제하지 않은 결과 Heartbleed, Shellshock 와 같은 제로데이 취약점 출현 시 국내 공공, 금융회사가 즉각적이고 체계적인 대응을 못하고 있음**

전자금융거래법에 따른 금융위원회 보안점검 강화 지침



IT · 금융융합 지원방안

-제1차 IT · 금융융합협의회 운영결과-

2015. 1. 27.

금 융 위 원 회

□ **전자금융 서비스의 보안 수준에 대한 사후적 점검 강화**

① 금융회사의 **자체 보안점검 내실화** 유도

- 형식적으로 이루어졌던 신규 서비스에 대한 '취약점 분석 평가' 의 평가항목 및 평가기준을 내실화 하여 취약점 분석평가 운영을 개선

* 금융회사는 신규 서비스 출시 시 1개월 내에 금감원에 **자체 '취약점분석 평가' 실시 결과를 제출** (전자금융업법 시행령 제11조의5)

② 신종 거래구조, 신종 인증수단 등을 채택하여 보안 우려가 있는 신규 전자금융 서비스에 대해서는 **사후 검사 강화**

- 신규 서비스 출시 전 자체 보안성 심의의 충실한 수행 여부 점검 등 금감원 정기 검사 시 보안성 검사 강화

- 보안 우려가 큰 중요 IT서비스에 대해서는 금감원이 불시 기동 점검 방식의 적극적인 테마 검사 수행

- 근래 제로데이 취약점을 비롯한 미국발 주요 위험 경보에 대한 점검 현황을 상시/비상시적으로 보고하도록 지시

□ **현황**

자체 보안 점검의 내실화를 유도하는 방향으로 지침이 변경되었으나 여전히 많은 금융기업들은 기존의 CCE 기반 진단 항목만 점검하는데 목표를 두고 있는 실정

CVE 취약점 분석 솔루션 도입에 따른 향상 효과

구 분	수동 진단 [기존 방식]	자동화 진단/관리 [Nexpose]
진단주기	년 1~2회 / 일회성 서비스	수시 진단 / 관리
수행 결과 [1일 기준]	Man / Months [50대 Max.]	Man / Months [Unlimited EA] 무제한 범위 진단 수행
수행 방법	**자체 제작 스크립트(Script) 진단 수행**	**에이전트 없이 네트워크를 통한 원격 진단**
수행 범위	**샘플링(Sampling), 부분적 취약점만 진단**	**전수 조사, 거의 모든 알려진 취약점 진단**
신규 도입 / 변경	자산의 신규도입 또는 서비스 변경 시 누락 또는 취약점 장기간 존재 위험	자산의 신규도입 또는 서비스 변경 시 즉시 진단 수행
비용 / 속도	고비용 저효율 방식으로 고급 인력 참여 기피	**지속적인 비용 및 리소스 절감** **저비용, 매우 빠른 진단 속도**
보고서	**수동으로 작성 [텍스트 형태의 결과물]**	**다양한 자동화 보고서 산출**
조사 범위 / 깊이	인력을 통한 스크립트 기반 진단 수행 진단 범위 제한적 진단 속도 매우 느림	잘 알려진 모든 운영체제, 어플리케이션, 서버, 웹, DB, 유무선 네트워크, 보안 시스템 등 폭넓은 영역을 빠른 속도로 정확하게 진단

관련 뉴스 – 데일리시큐, 전자신문, 디지털타임즈 기사

“기업들, CVE 기반 취약점에 대한 대응 미비한 상태”

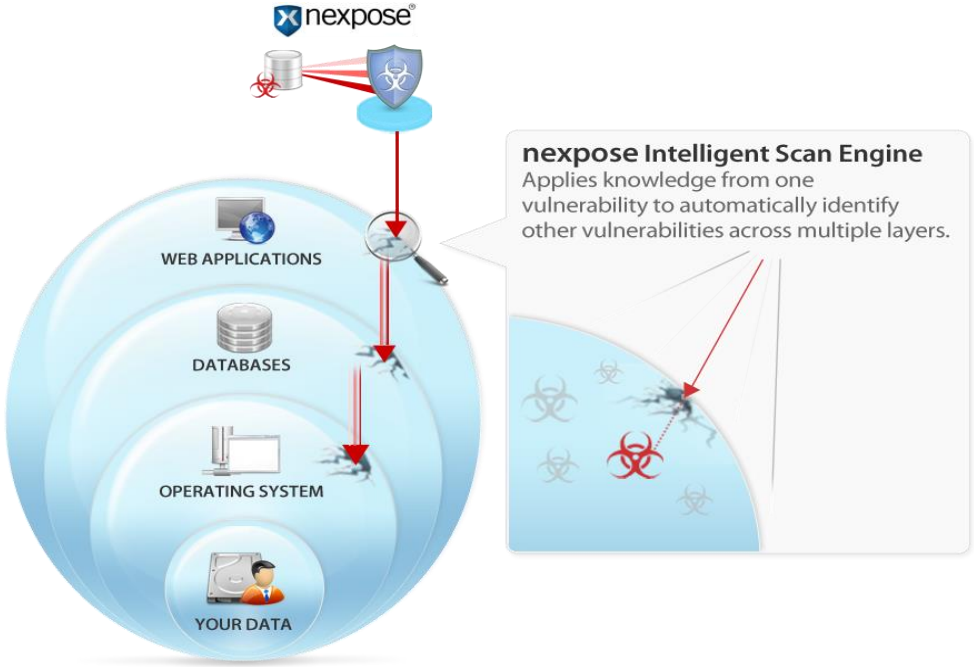
등록 : 2016-03-04 15:06 , 데일리시큐 길민권기자 , mkgil@dailysecu.com

“사이버 공격이 날로 증가하면서 기업 보안 담당자는 현 시스템에 어떤 문제가 있는지 파악하고 기업 내부 자산이 취약점에 노출됐는지 관리해야만 한다. 하지만 대부분 기업에서는 CCE 기반의 규정 준수는 하고 있지만 CVE 기반의 취약점에 대한 대응은 미비한 상태”라며 “CCE는 전자금융감독규정 및 안행부 등 시스템의 구성에 대한 점검이 주로 이루어지고 있다면, CVE는 OS 및 애플리케이션 고유의 취약점을 나타내고 있기 때문에 이를 동시에 충족할 필요가 있다”고 강조했다.


nexpose®

Nexpose: JESS 엔진을 통한 연속적 스캔영역

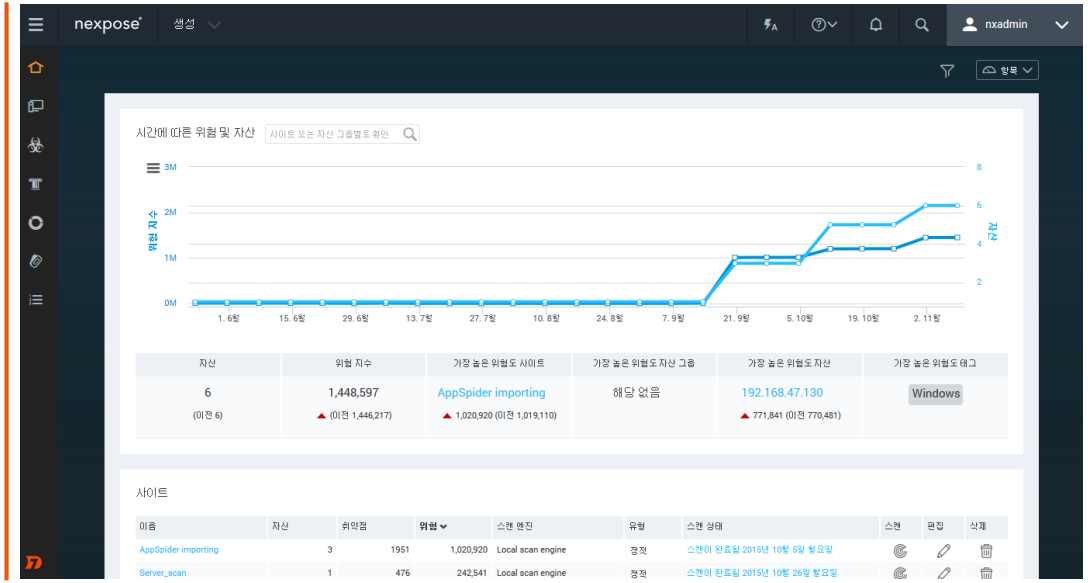
- 통합된 인공지능 스캔엔진:
  - 샌디아 국립연구소에서 NASA를 위해 개발한 인공지능 엔진 JESS(Java Expert System Shell)
  - 해커 접근 기법 구현
    다계층에 걸친 연관된 취약점들을 연속 추적하는 방식으로 정확성을 높이고 불필요한 스캔과정을 제거
  - 1% 미만의 false positive
  - 75,000개 이상의 취약점을 190,000개 이상의 체크 방법으로 진단



효율적인 통합 보안 진단

- 간단한 설정
- 통합된 스캔
  OS, 어플리케이션, 서비스,
  웹, 데이터베이스, 보안설정
- 압축된 리포트

한번의 스캔으로 전체 진단



다섯가지 위험 판단 요소로 우선순위를 결정

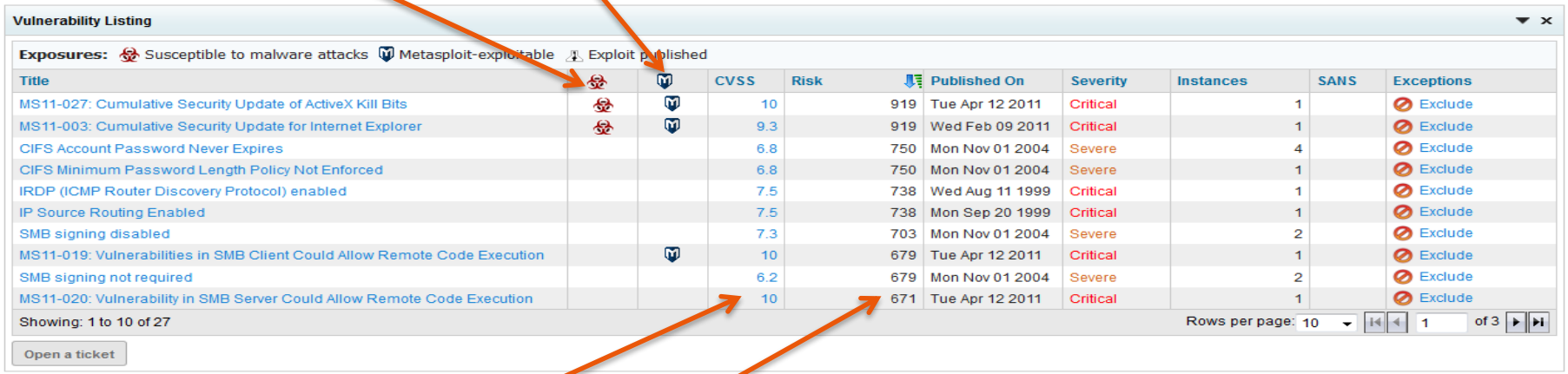
우선순위 설정을 위해 신뢰성있는 다각적 위험 정보 제공

- 준수(CVSS) or 진짜 위험?

멀웨어 공격 위험

Exploit 공격 위험

→ 고 위험 취약점에 즉각적인 조치



Vulnerability Listing

Exposures: Susceptible to malware attacks | Metasploit-exploitable | Exploit published

Title			CVSS	Risk	Published On	Severity	Instances	SANS	Exceptions
MS11-027: Cumulative Security Update of ActiveX Kill Bits	☣	Ⓜ	10	919	Tue Apr 12 2011	Critical	1		Exclude
MS11-003: Cumulative Security Update for Internet Explorer	☣	Ⓜ	9.3	919	Wed Feb 09 2011	Critical	1		Exclude
CIFS Account Password Never Expires			6.8	750	Mon Nov 01 2004	Severe	4		Exclude
CIFS Minimum Password Length Policy Not Enforced			6.8	750	Mon Nov 01 2004	Severe	1		Exclude
IRDP (ICMP Router Discovery Protocol) enabled			7.5	738	Wed Aug 11 1999	Critical	1		Exclude
IP Source Routing Enabled			7.5	738	Mon Sep 20 1999	Critical	1		Exclude
SMB signing disabled			7.3	703	Mon Nov 01 2004	Severe	2		Exclude
MS11-019: Vulnerabilities in SMB Client Could Allow Remote Code Execution		Ⓜ	10	679	Tue Apr 12 2011	Critical	1		Exclude
SMB signing not required			6.2	679	Mon Nov 01 2004	Severe	2		Exclude
MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution			10	671	Tue Apr 12 2011	Critical	1		Exclude

Showing: 1 to 10 of 27 Rows per page: 10 1 of 3

Open a ticket

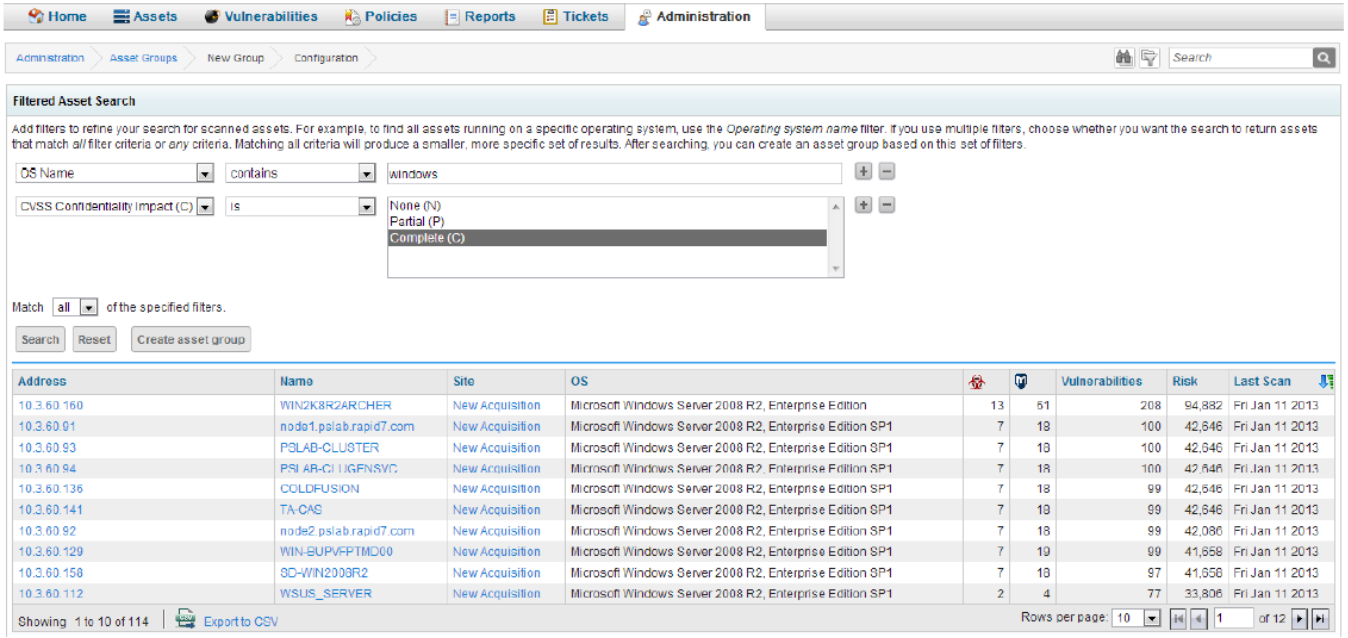
전통적 CVSS

전체 조직에 대한
취약점 별 위험점수

→ 조치순서 결정을 위한 기준

자산 정보의 분류

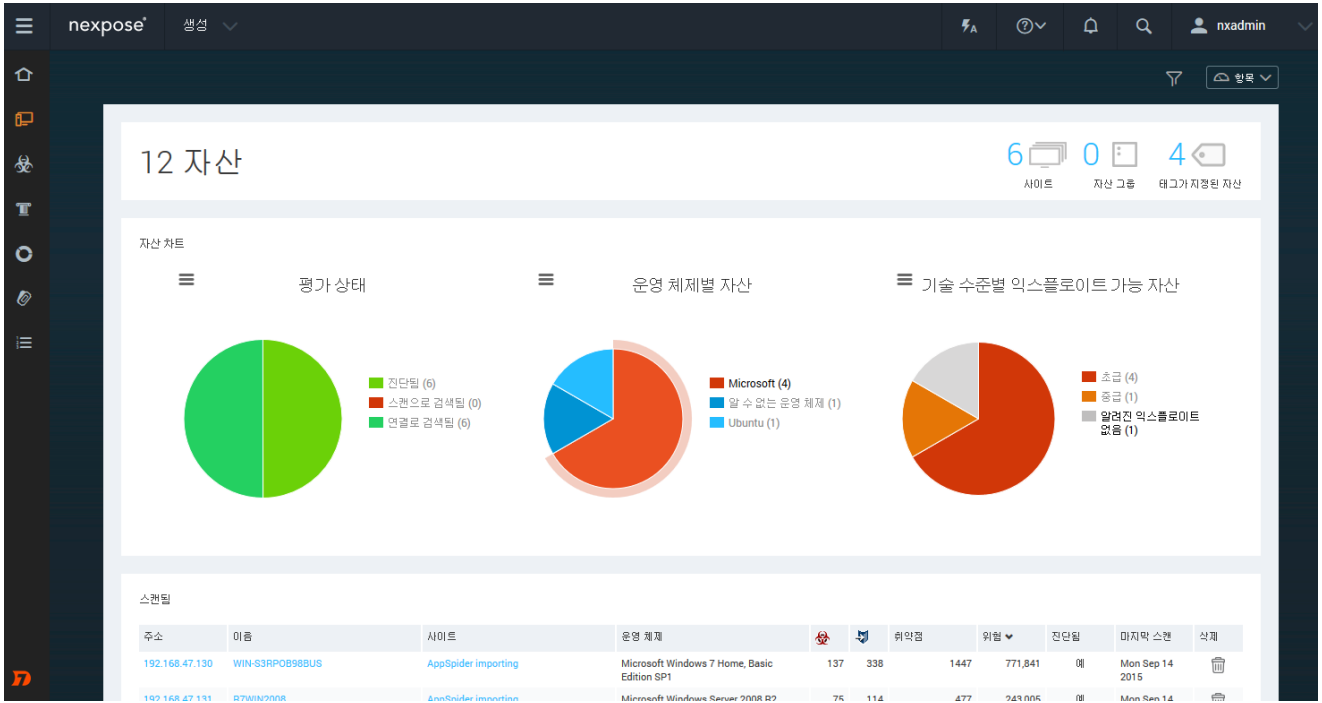
SITE, STATIC ASSET GROUP, DYNAMIC ASSET GROUP 기능으로 지속적이고 효과적으로 자산을 분류
- 가장 위험도가 높은 웹 서버들을 스캔할 때마다 어떻게 자동으로 분류하고 관리할 수 있을까?



Dynamic Asset Grouping automatically sorts assets based on new information

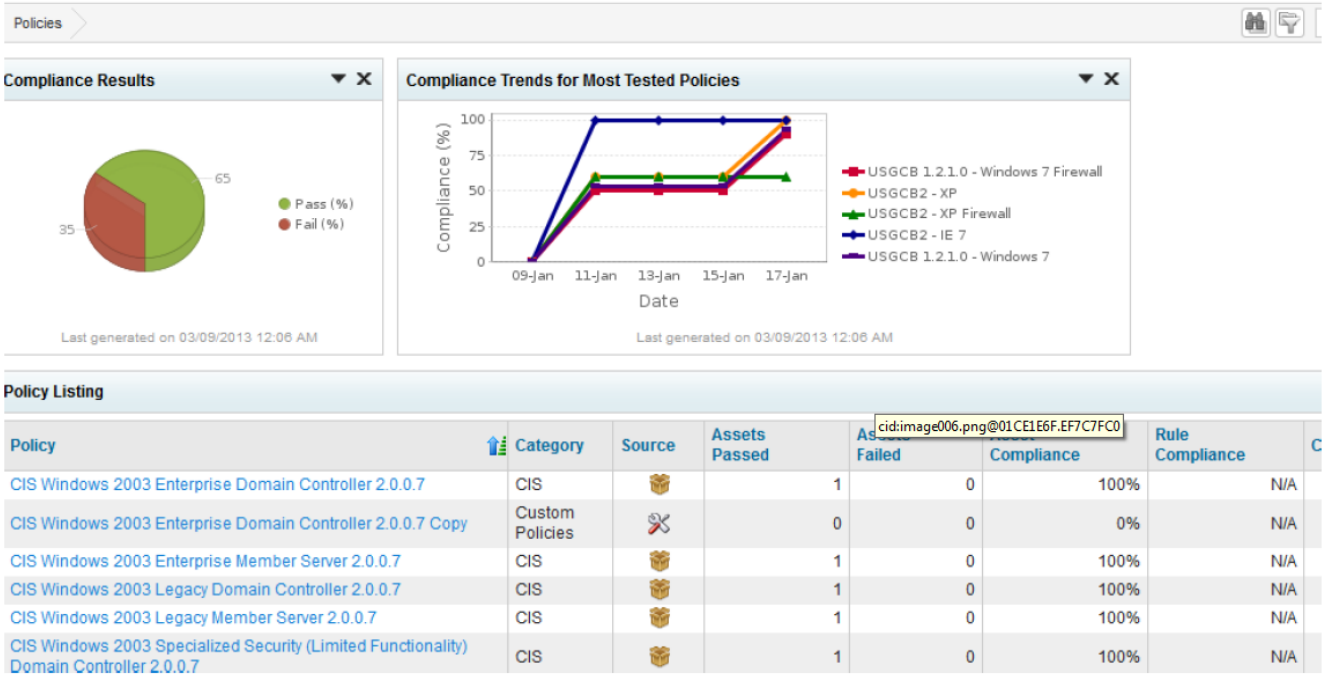
자산 정보의 분류

새롭게 발견된 자산, 취약점 진단을 완료한 자산, OS 별 분포, 공격 기술 난이도에 따른 침해가능한 자산의 분포를 한눈에 보여주는 자산 현황 대시보드



컴플라이언스를 위한 Policy 기능

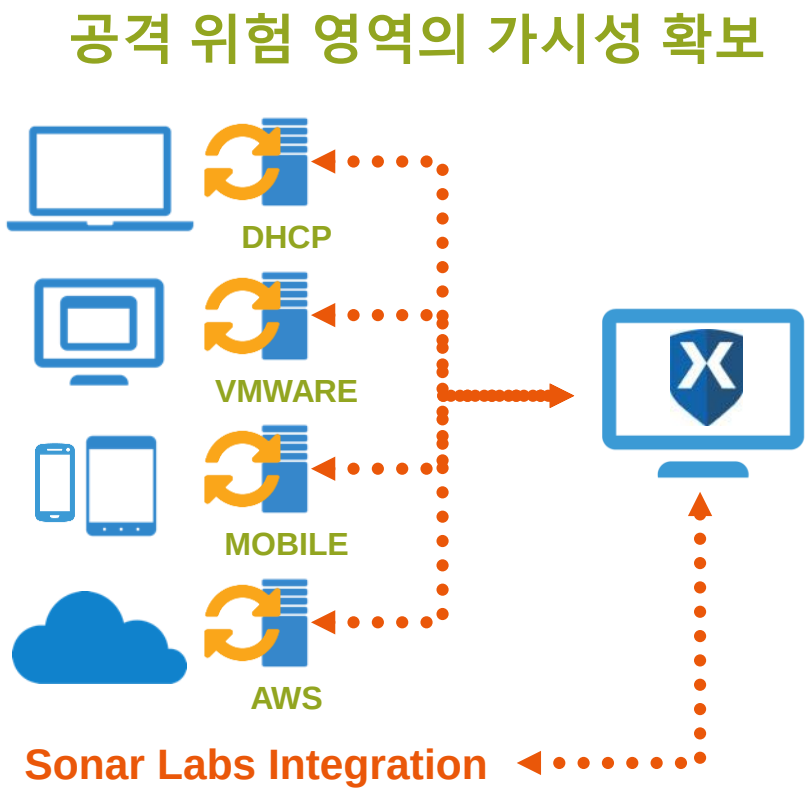
CIS, FDCC, USGCB, DISA 및 PCI, HIPAA, SOX, SCADA 등의 COMPLIANCE에 대응하는 POLICY SCAN 과 결과를 리포트로 제공



The Nexpose Configuration Policy Dashboard

적응형 진단 – 동적 자산 변화에 자동 대응

- 새로운 자산이 네트워크에 연결될 때 자동으로 식별
- 자산이 네트워크에 연결 또는 단절될 때마다 위험을 진단
- 내부 조직이 인지하지 못할 수 있는 모든 외부 자산을 자동 식별



적응형 진단 – 새로운 취약점에 자동 대응

- 새로운 취약점이 발표되는 즉시 전체 자산을 진단하여 위험에 대한 노출을 판단
- CVSS 또는 RealRisk™ 기준으로 자동 스캔 룰 설정
- 인위적인 추가 개입 필요없음

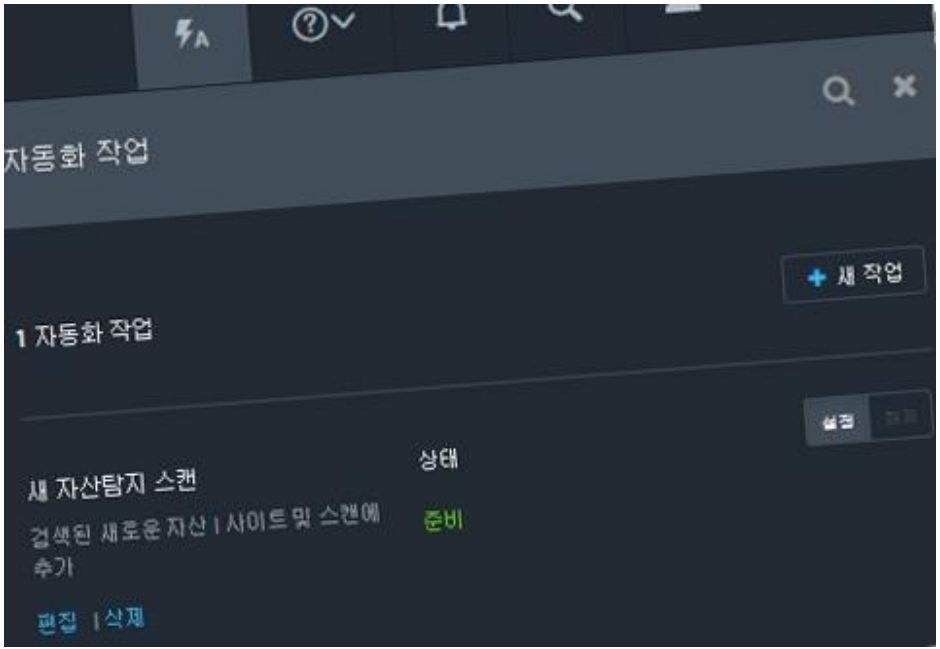
새로운 위협에 자동 대응

Zero Day

적응형 진단 - 자동화된 워크플로우

- 어떠한 설정 코드 생성 없이 맞춤형 이벤트 조건의 정의로 자동 진단 수행 설정
- 내부 업무 환경에 맞게 자산을 필터링 분류하여 정교하게 진단 행위를 정의
- 드롭다운 메뉴와 클릭선택으로 손쉬운 설정

이벤트로 자동 시작되는 스캔



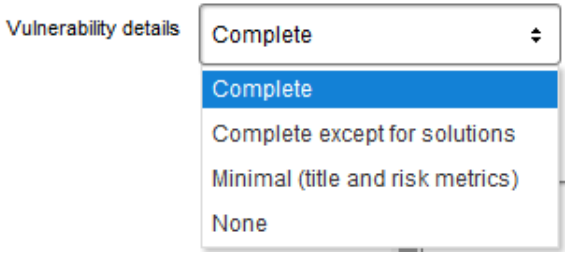
보고서 – 취약점 결과정보를 분류하여 산출

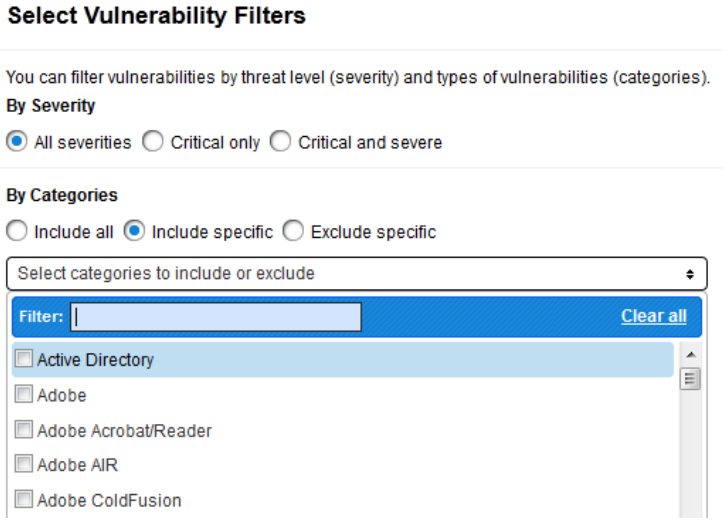
호스트 필터: IP, SITE, STATIC GROUP, DYNAMIC GROUP

취약점 필터: 150 개의 카테고리 및 심각도에 따른 분류

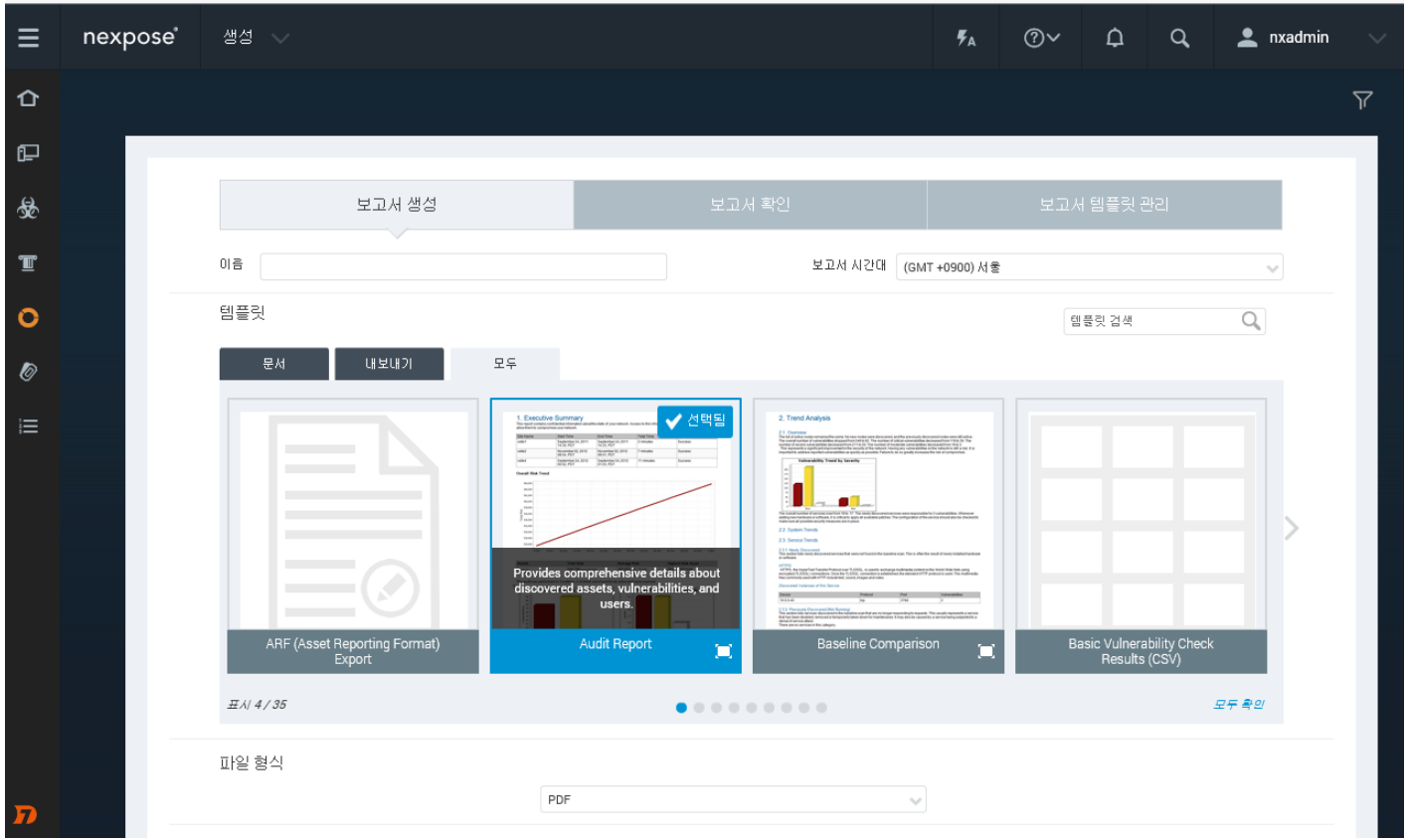
취약점 세부정보: 리포트 대상에 따라 4가지의 분류 옵션

예> 위험수준이 높은 웹 서버들로부터 발견된 심각도가 CRITICAL인 모든 웹 관련 취약점만 추출해서 리포트를 생성





보고서 – Wizard 형태로 취약점 결과를 편리하게 추출



보고서 – 해결 조치 방법 제시 (Remediation Plan Report)

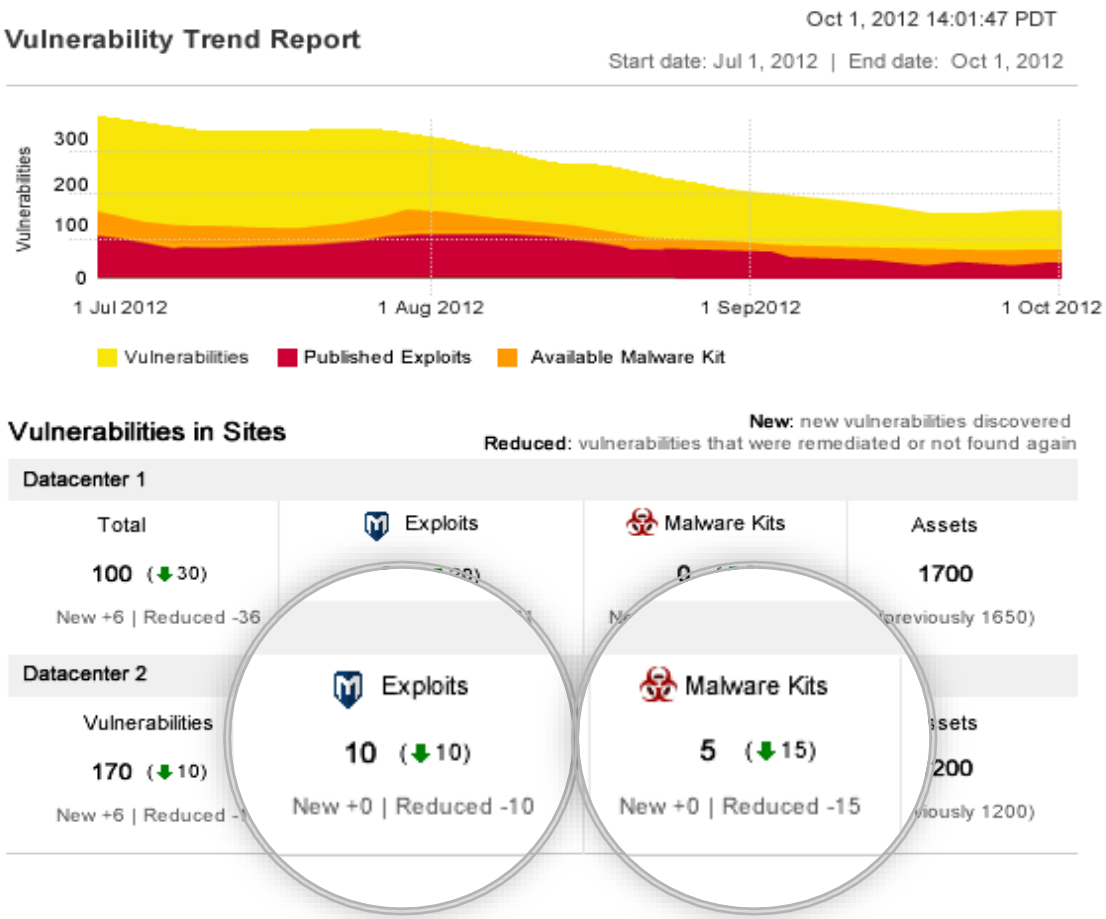
패치와 구성 변경에 대한 순서 및 단계별 조치를 제공

Set the password expiration
Estimated time: 30 minutes

Microsoft Windows 2000 Professional, Microsoft Windows XP Professional
If the account is not used, delete or disable the account. If the account is a built-in system account such as the IUSR_ or IWAM_ accounts, enable the "User cannot change password" option to stop this vulnerability from being reported (Microsoft best practices dictate that built-in system accounts NOT be allowed to change their own passwords). Otherwise, ensure that the password expires by disabling the "Password never expires" option.

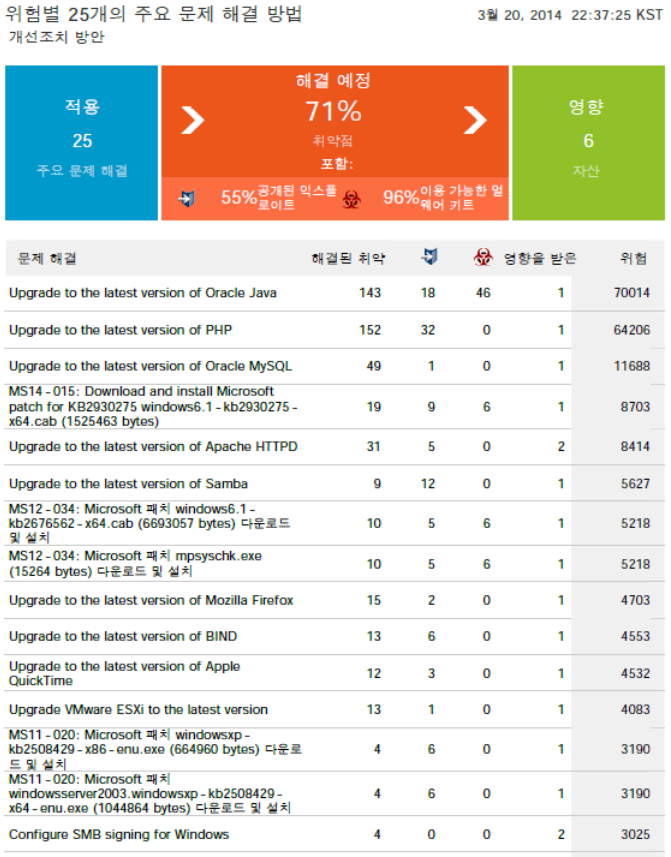
1. Right click on "My Computer"
2. Select "Manage"
3. Open the "Local Users and Groups" folder
4. Open the "Users" folder
5. Double-click on the desired user
6. Uncheck "Password never expires"

보고서 – 시간에 따른 취약점 변화 (Trend Report)



보고서 – 최우선 이행조치와 기대효과 (Top Remediation Report)

- 높은 위험에 대한 가시성 확대
  - 주요 취약점의 치료방법 효율화
  - 한정된 자원에 집중
  - 취약점 분류에 따라 전문가를 효율적으로 배치



위험별 25개의 주요 문제 해결 방법
개선조치 방안

3월 20, 2014 22:37:25 KST

적용
25
주요 문제 해결

해결 예정
71%
취약점
포함:
55% 공개된 익스플로이트
96% 이용 가능한 멀웨어 키트

영향
6
자산

문제 해결	해결된 취약			영향을 받은	위험
Upgrade to the latest version of Oracle Java	143	18	46	1	70014
Upgrade to the latest version of PHP	152	32	0	1	64206
Upgrade to the latest version of Oracle MySQL	49	1	0	1	11688
MS14 - 015: Download and install Microsoft patch for KB2930275 windows6.1 - kb2930275 - x64.cab (1525463 bytes)	19	9	6	1	8703
Upgrade to the latest version of Apache HTTPD	31	5	0	2	8414
Upgrade to the latest version of Samba	9	12	0	1	5627
MS12 - 034: Microsoft 패치 windows6.1 - kb2676562 - x64.cab (6693057 bytes) 다운로드 및 설치	10	5	6	1	5218
MS12 - 034: Microsoft 패치 mpsyschk.exe (15264 bytes) 다운로드 및 설치	10	5	6	1	5218
Upgrade to the latest version of Mozilla Firefox	15	2	0	1	4703
Upgrade to the latest version of BIND	13	6	0	1	4553
Upgrade to the latest version of Apple QuickTime	12	3	0	1	4532
Upgrade VMware ESXi to the latest version	13	1	0	1	4083
MS11 - 020: Microsoft 패치 windowsxp - kb2508429 - x86 - enu.exe (664960 bytes) 다운로드 및 설치	4	6	0	1	3190
MS11 - 020: Microsoft 패치 windowsserver2003.windowsxp - kb2508429 - x64 - enu.exe (1044864 bytes) 다운로드 및 설치	4	6	0	1	3190
Configure SMB signing for Windows	4	0	0	2	3025

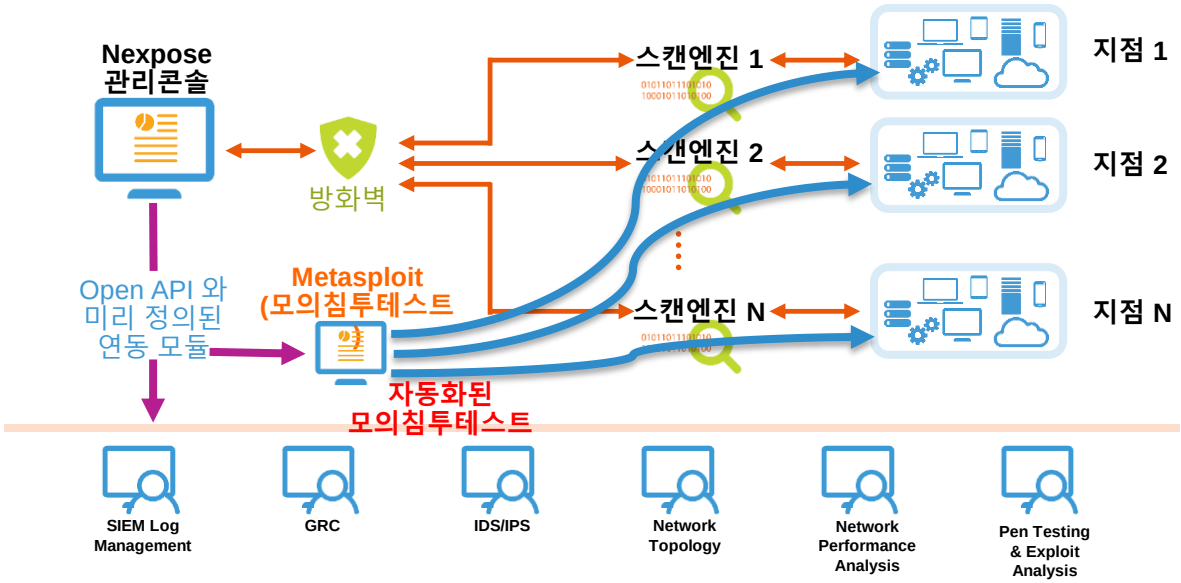
취약점 위험 관리의 기대효과

가시성 확대	위험의 우선순위 관리	자동화
- 시스템 및 네트워크의 취약점 파악 - “양호” 상태의 변경 원인 파악 (예: 구성) - 목표 지수를 이용하여 인지, 행동, 의무 수행	- 방어에 필요한 데이터 산출 - 단순한 취약점만이 아닌, 이용가능성에 따른 치료방법의 우선순위 설정 - 위험 해결을 위한 수치화가 가능한 대책 마련	- 평가와 치료 주기의 자동화 - 데이터 정확성 증가를 위한 지속적인 평가 가능 - 업무연관 IT위험의 영향 산출
위협 대비	**효율성 증가**	**업무 생산성 증대**

유연하게 확장 가능한 아키텍쳐

- 다중 설치 옵션
- 에이전트 없는 스캔
- 스캔 엔진의 확장 설치
- OpenAPI™- 타제품과 연동

취약점 진단관리 구성 아키텍쳐



한글화 지원 – UI, 보고서, 도움말, 매뉴얼

Audit Report

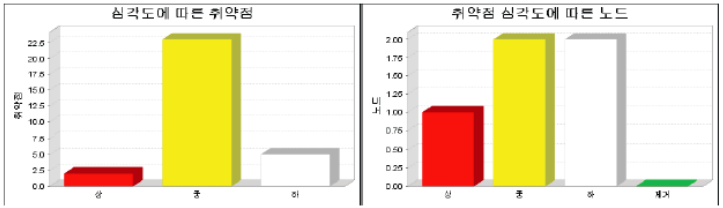
1. 개요

이 보고서는 Nexpose이 Rapid7 LLC에서 수행한 보안 감사에 대한 내용입니다. 이 보고서는 귀하의 네트워크 상태에 대한 기밀 정보를 포함합니다. 권한 없는 사용자가 이러한 정보에 액세스하는 경우, 네트워크 문제가 발생할 수 있습니다.

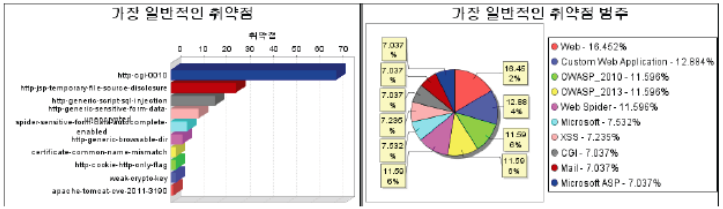
사이트 이름	시작 시간	종료 시간	전체 시간	상태
Web_Svr	February 14, 2014 21:35, PST	February 14, 2014 22:01, PST	25 분	성공

전체 자산 추세를 표시할 수 있는 충분한 이력 데이터가 없습니다.

2개의 시스템에 대한 감사가 수행되었으며 이 중 2개의 시스템이 액티브 상태이고 검색된 것으로 나타났습니다.



검색하는 동안 30개의 취약점이 발견되었습니다. 이 중, 심각도가 상인 취약점은 2개입니다. 심각도가 상인 취약점이 발견되면 즉시 조치를 취해야 합니다. 이러한 취약점은 해커에 의해 악용되기 쉬우며 영향을 받은 시스템이 조작될 수도 있습니다. 심각도가 중인 취약점은 23개입니다. 심각도가 중인 취약점의 경우 상대적으로 악용하기 쉽지 않고 해당 시스템에 액세스하기 어려울 수도 있습니다. 심각도가 하인 취약점이 5개 발견되었습니다. 하지만 차후에 귀하의 네트워크를 공격하는 데 이용될 수 있는 정보를 공격자에게 제공할 수 있습니다. 이러한 취약점은 다른 취약점만큼 시급하지 않지만 적시에 해결되어야 합니다.
심각도가 상인 취약점이 발견되었으며 보안 위협이 가장 높은 시스템은 1개입니다. 2개의 시스템에서 심각도가 중인 취약점이 발견되었습니다. 2개의 시스템에서 심각도가 하인 취약점이 발견되었습니다. 모든 시스템에서 취약점이 발견되었습니다.



http - cgi - 0010 취약점은 71번 발생한 가장 일반적인 취약점입니다. 취약점이 166개 발생한 Web 범주는 가장 일반적인 취약점 범주입니다.

위험별 25개의 주요 문제 해결 방법

개선조치 방안

3월 20, 2014 22:37:25 KST

적용 25 주요 문제 해결

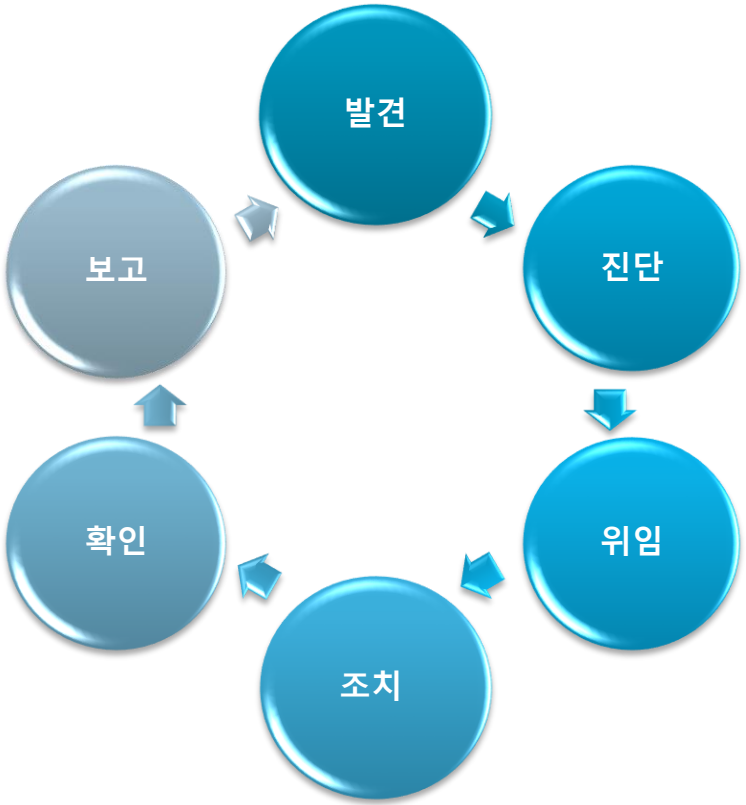
해결 예정 71% 취약점 포함: 55% 공개된 익스플로이트 96% 이용 가능한 멀웨어 키트

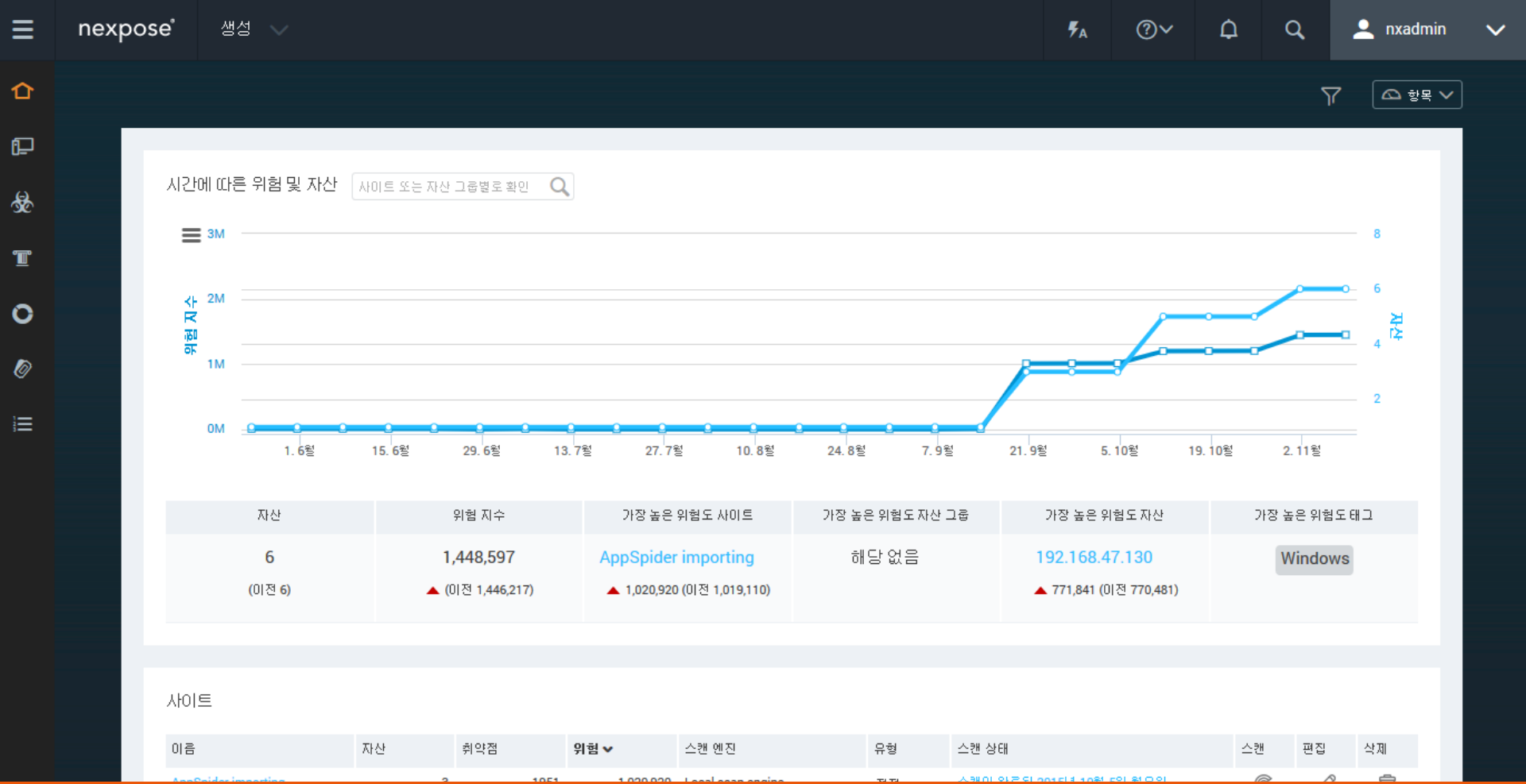
영향 6 자산

문제 해결	해결된 취약			영향을 받은	위험
Upgrade to the latest version of Oracle Java	143	18	46	1	70014
Upgrade to the latest version of PHP	152	32	0	1	64206
Upgrade to the latest version of Oracle MySQL	49	1	0	1	11688
MS14 - 015: Download and install Microsoft patch for KB2930275 windows6.1 - kb2930275 - x64.cab (1525463 bytes)	19	9	6	1	8703
Upgrade to the latest version of Apache HTTPD	31	5	0	2	8414
Upgrade to the latest version of Samba	9	12	0	1	5627
MS12 - 034: Microsoft 패치 windows6.1 - kb2676562 - x64.cab (6693057 bytes) 다운로드 및 설치	10	5	6	1	5218
MS12 - 034: Microsoft 패치 mpsyschk.exe (15264 bytes) 다운로드 및 설치	10	5	6	1	5218
Upgrade to the latest version of Mozilla Firefox	15	2	0	1	4703
Upgrade to the latest version of BIND	13	6	0	1	4553
Upgrade to the latest version of Apple QuickTime	12	3	0	1	4532
Upgrade VMware ESXi to the latest version	13	1	0	1	4083
MS11 - 020: Microsoft 패치 windowsxp - kb2508429 - x86 - enu.exe (664960 bytes) 다운로드 및 설치	4	6	0	1	3190
MS11 - 020: Microsoft 패치 windowsserver2003.windowsxp - kb2508429 - x64 - enu.exe (1044864 bytes) 다운로드 및 설치	4	6	0	1	3190
Configure SMB signing for Windows	4	0	0	2	3025

취약점 관리 프로세스

- 발견 - IT 자산을 식별하고 분류
- 진단 - 취약점 스캔 수행
- 위임 - 고위험 순으로 취약점 조치 권고 전달
- 조치 - 패치, 업그래이드, 대체 방안 등 조치 이행
- 확인 - 취약점 제거 이행 검증을 위한 스캔
- 보고 - 책임자에 위험 진단 처리 결과 보고





새롭게 설계된 직관적 인터페이스

nexpose 생성 nxadmin

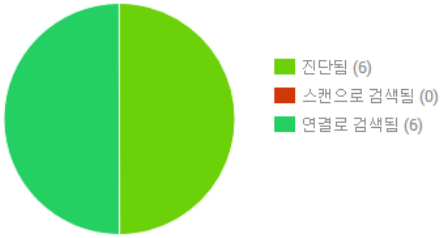
항목

12 자산

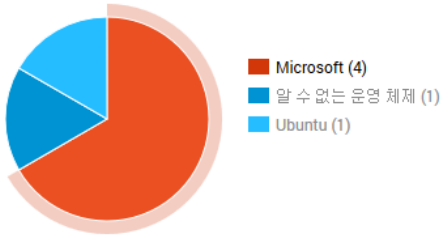
6 사이트 | 0 자산 그룹 | 4 태그가 지정된 자산

자산 차트

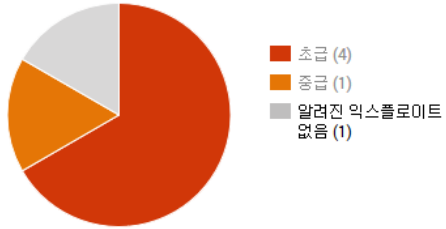
평가 상태



운영 체제별 자산



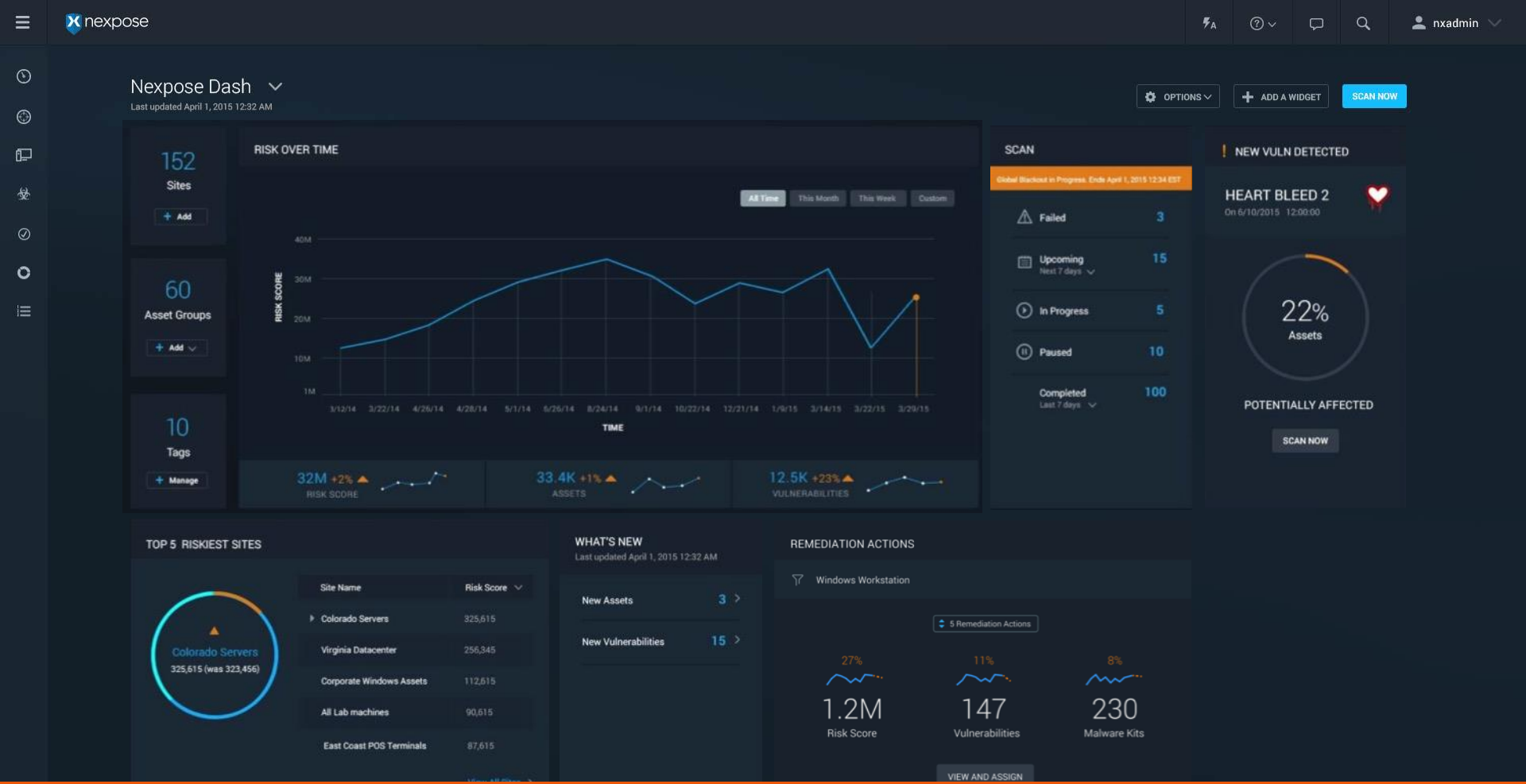
기술 수준별 익스플로이트 가능 자산



스캔됨

주소	이름	사이트	운영 체제			취약점	위험	진단됨	마지막 스캔	삭제
192.168.47.130	WIN-S3RPOB98BUS	AppSpider importing	Microsoft Windows 7 Home, Basic Edition SP1	137	338	1447	771,841	예	Mon Sep 14 2015	

아시아 지역 언어 : 한국어, 일본어, 간체 중국어



InsightVM powered by Insight Platform

왜 Rapid7의 Nexpose를 선택합니까?

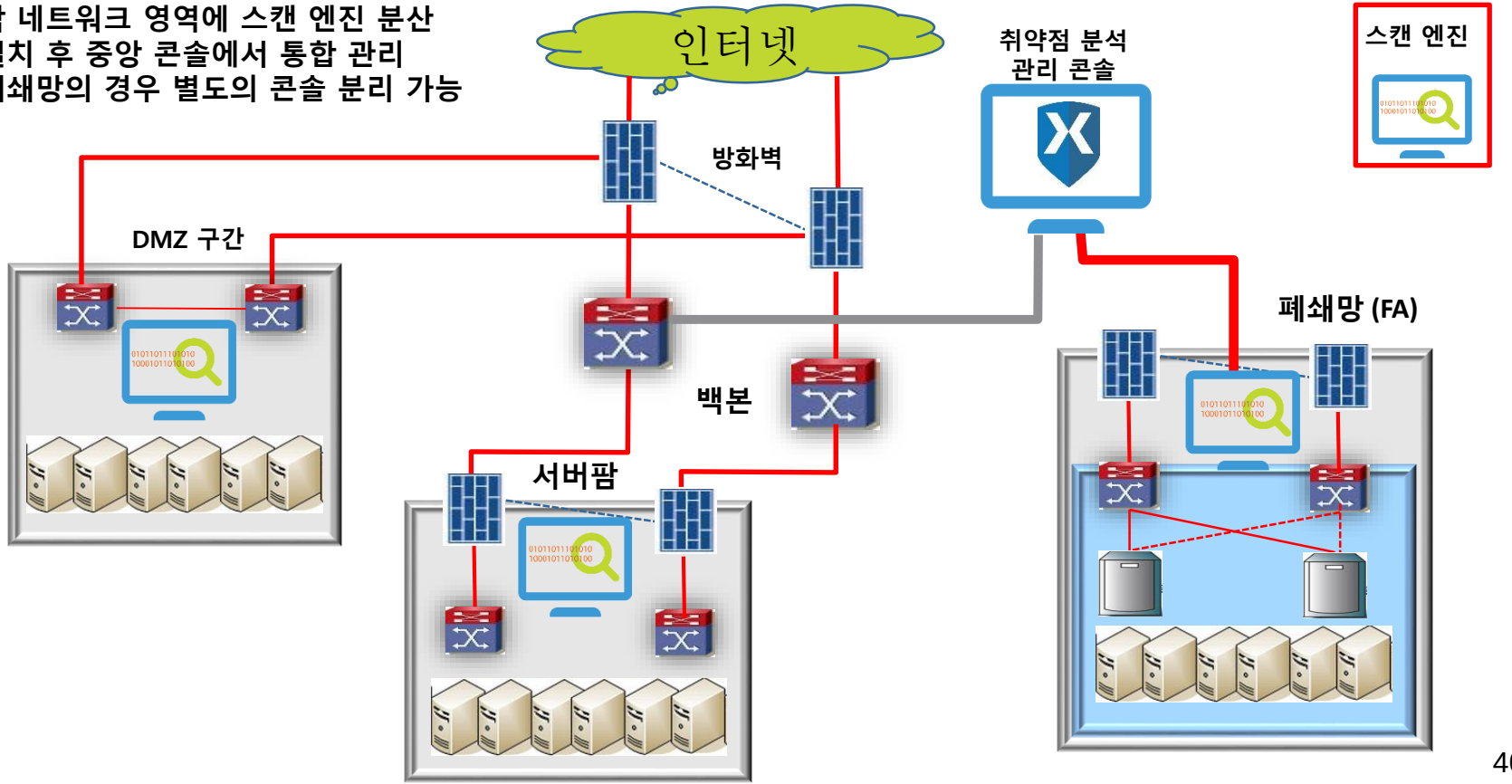
- 높은 스캔 정확도
- 동적 자산 자동식별 (DHCP, Vmware, AWS, Mobile)
- 동적 자산그룹 자동 업데이트 (DAGs)
- 순환 연결형 취약점 검증 (with Metasploit Pro)
- RealRisk™ and RealContext™ (실제위협 반영)
- 최우선 해결조치 보고서
- 적응형 보안 (자산의 변경, 새로운 위협에 자동대응)
- 풍부한 Open API 제공으로 유연한 연동 확장

도입 사례 - 금융권

구축 운용 지표	H 카드 社(2013년 도입)	I 은행 社 (2013 도입)
점검 자산 규모	1500 IP	3,000 IP
점검 대상 서버	Windows, Unix, Linux, 어플리케이션, 웹서버, DB	Windows, Unix, Linux, 어플리케이션, 웹서버, DB
점검 주기	평균 2 개월	수시, 평균 1-2 개월
주요 취약점 관리 포인트	• CVE 기반 고위험 취약점 상시 진단 후 제거 • 제로데이 취약점에 대한 신속한 진단 및 조치 • 모의침투테스트 툴로 실제 공격성공 여부 검증	• 스캔의 정확성이 뛰어난 솔루션 선택 • 제로데이 취약점에 대한 신속한 진단 및 조치 • 시스템 변경, 서비스 오픈 전 안전성 진단
도입 효과	• 전체 자산 취약점을 한번에 자동 진단 • 전사적 서버 고위험 취약점의 상시 진단 및 제거 • ISMS 등 컴플라이언스 및 감사에 대응	• 내부 보안침해 예방을 위한 근본적 해결책 • 고위험 및 제로데이 취약점의 신속한 제거로 보안 위협 사전 제거 • ISMS 등 컴플라이언스에 대응
운용 프로세스	• 서버 변경 시 취약점 진단 수행 • 서버 담당자를 위해 상세한 취약점 근거와 조치방안 제공 • 진단 운영자는 재점검을 수행하여 실제 취약점 조치 여부를 확인 • 지속적인 취약점 관리 사이클에 따라 운용	• 진단 운영팀이 정기적인 전체 취약점 진단 • 실제 공격가능한 고위험 취약점을 우선 조치 • 진단 운영자는 재점검을 수행하여 실제 취약점 조치 여부를 확인 • 시간에 따른 취약점 변화 보고서 제출 • 지속적인 취약점 관리 사이클에 따라 운용

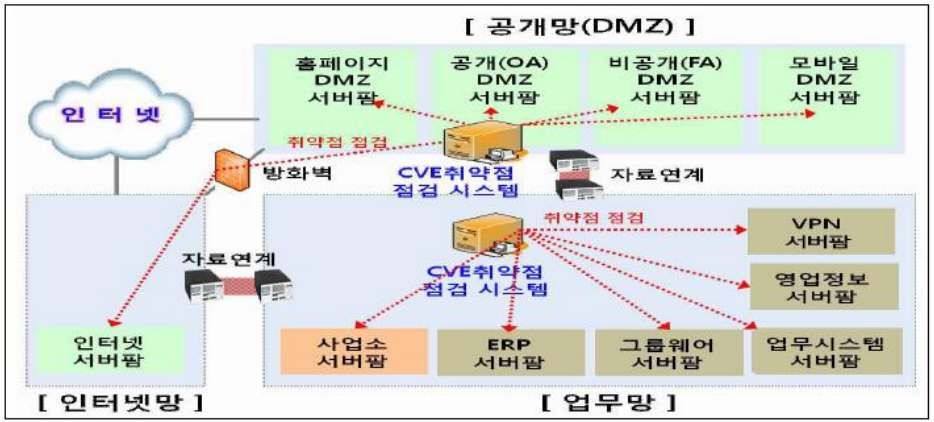
도입 사례 – 폐쇄망

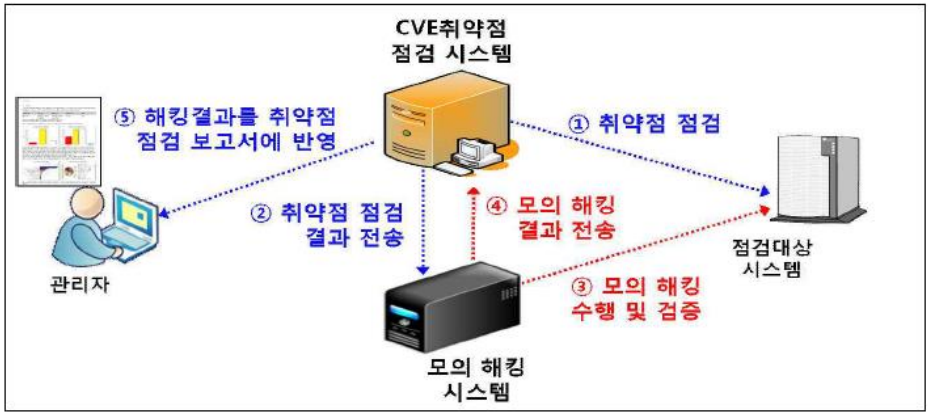
- 각 네트워크 영역에 스캔 엔진 분산 설치 후 중앙 콘솔에서 통합 관리
- 폐쇄망의 경우 별도의 콘솔 분리 가능



도입 사례 – Nexpose과 Metasploit 연동

- 공개망 및 업무망 전체에 대한 자동 진단을 위한 간단한 구축
- 한번의 스캔 명령으로 전체 자산에 대한 원격 진단
- 스케줄링에 의한 자동 진단 편의성 제공
- 모의해킹 시뮬레이션 시스템과 동적 연동으로 자동화된 위험 검증 체계 구축





도입 사례 구성도 – 삼성전자 (AWS + On-Premise)

- 원격 관리 : 수원 본사
- 관리 콘솔 : 미국
- 스캔 엔진 : 분산 설치
  미국, 독일, 싱가폴, 중국 등

- 보안 조치 및 조직 간 업무 협조의 근거로 데이타 활용
  예) 삼성전자 vs 삼성페이

Rapid7 국제인증 – Nexpose

Common Criteria – Certified EAL 3+

Certification Report

EAL 3+ Evaluation of Rapid7™ Nexpose™ Vulnerability Management and Penetration Testing System V5.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-148-CR
Version:	1.0
Date:	22 May 2012
Pagination:	i to iii, 1 to 9

CVE Number Authority

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

CVE Numbering Authorities

Participating CNAs | Documentation for CNAs | Requesting CVE IDs from CNAs | Become a CNA

CVE Numbering Authorities (CNAs) are organizations that are authorized to assign CVEs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities. These CVEs are provided to researchers, vulnerability disclosers, and information technology vendors.

Vulnerability Researchers

- Larry Cashdollar
- Rapid 7
- Talos


metasploit®

실제 환경의 보안 테스트 및 위험 확인

외부 공격자와 같은 공격 방법을 사용하여 조직의 다양한 네트워크 방어체계에 대한 통합 검증 테스트

- 테스트 자산에 안전한 **공격 시뮬레이션**
- 세계에서 가장 많은 품질이 **검증된 취약점 공격 모듈**을 선별
- Nexpose와 함께 사용하여 **실제 위험 상태를 검증**
- **소셜엔지니어링**(피싱 기법)과 **로그인 인증 검사**를 통해 조직의 **보안 인식**과 방어 상태를 측정 관리
- Bruteforcing, VPN pivoting, social engineering 과 같은 **정교한 공격에 대한 대응 훈련**

Metasploit 의 주요 이정표

2003 - 2009

HD Moore
Metasploit 설계,
Pen Testing
오픈소스 프로젝트

April 2010

Metasploit Express
출시

October 2011

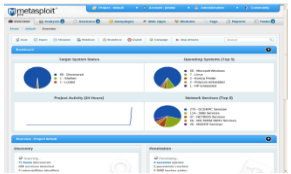
Metasploit
Community 출시

October 2009

Rapid7 Metasploit
인수

October 2010

Metasploit Pro 출시



December 2011

2011년 1백만 회
Metasploit Editions
다운로드

- HD Moore – Rapid7의 CRO 이며 Chief Architect
- 세계에서 가장 많이 사용되는 #1 침투테스트 솔루션
- 200,000 이상의 사용자와 참여회원
- 공신력을 기반으로 가장 광범위하고 품질이 증명된 Exploit 제공
- Security Community를 활성화

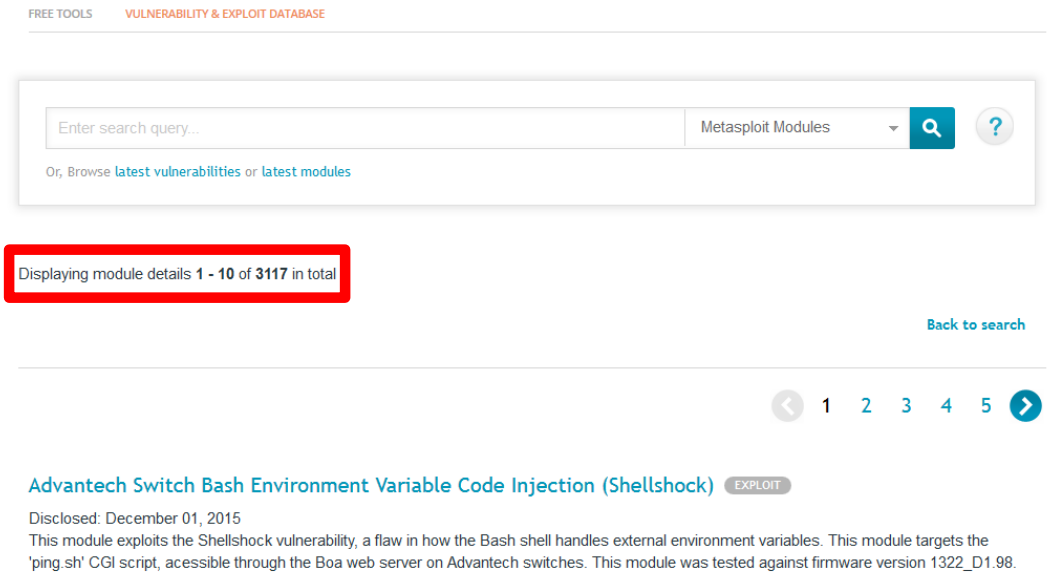
Metasploit Pro Workflow

모의 침투테스트의 필요성

- 발견된 취약점의 위험을 검증
- 보안 통제장치들의 실제 효력을 시험
- 사용자들의 보안 인식을 향상
- 패스워드 정책의 검증 테스트 및 감사
- 침해 공격 가능한 시스템 검출
- 침해 공격 상황의 영향 분석
- PCI 와 같은 컴플라이언스 요구

검색한 자산에 대한 안전한 공격 시뮬레이션

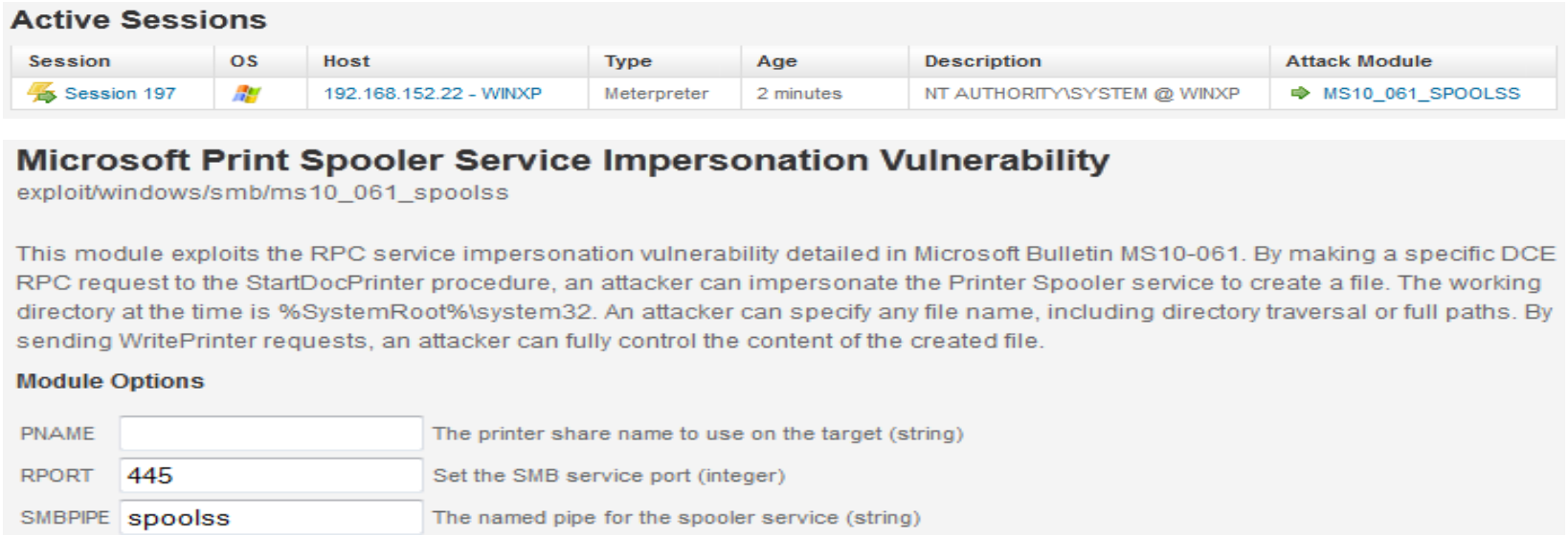
3100 개 이상의 세계적으로 검증된 모듈 (DEC 2015)



- Auxiliary, Post exploit, Custom exploit 모듈 포함

서버에 대한 공격 유형

METASPLOIT이 서버를 공격하는 클라이언트로 작동
예, MS10_061(SMB PORT 445의 취약점)을 갖고있는 WIN XP 공격



클라이언트에 대한 공격 유형

METASPLOIT이 자신에 접속하는 클라이언트를 침해하는 (웹)서버처럼 동작
예, IE에 내포된 취약점으로 공격받는 WIN7 사례

```
[*] [2012.04.19-13:46:20] 192.168.152.132:49261 Sending windows/browser/ms11_003_ie_css_import CSS
[*] [2012.04.19-13:46:20] Sending stage (752128 bytes) to 192.168.152.132
[*] [2012.04.19-13:46:25] Session ID 2 (192.168.152.10:1024 -> 192.168.152.132:49262) processing Ini
[*] Current server process: iexplore.exe (2532)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 3784
[+] Successfully migrated to process
```

Internet Explorer CSS Recursive Import Use After Free

exploit/windows/browser/ms11_003_ie_css_import

This module exploits a memory corruption vulnerability within Microsoft\'s HTML engine (mshtml). When parsing an HTML page containing a recursive CSS import, a C++ object is deleted and later reused. This leads to arbitrary code execution.

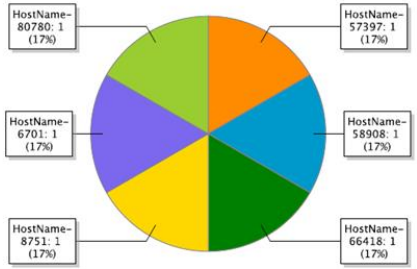
Module Options

OBFUSCATE	☑	Enable JavaScript obfuscation (bool)
SRVHOST	0.0.0.0	The local host to listen on. This must be an address on the local machine or 0.0.0.0 (address)
SRVPORT	8080	The local port to listen on. (port)

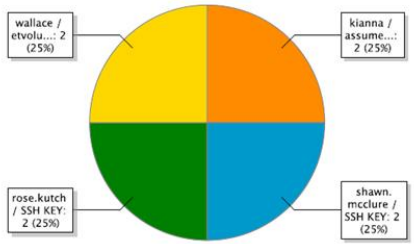
새롭게 부각되는 계정 인증 공격에 대비

- 취약점 EXPLOIT 이외에 시스템 계정 인증 침투 공격이 새로운 위협으로 부상
- 인증 정보 관리 기능 추가
- 신속한 계정 인증 검사 기능
- 기존 계정 정보를 효과적으로 재사용
- 계정 침투 테스트 전용 리포트 생성

Top Hosts by Logins



Top Shared Credentials by Related Hosts



Credential Details

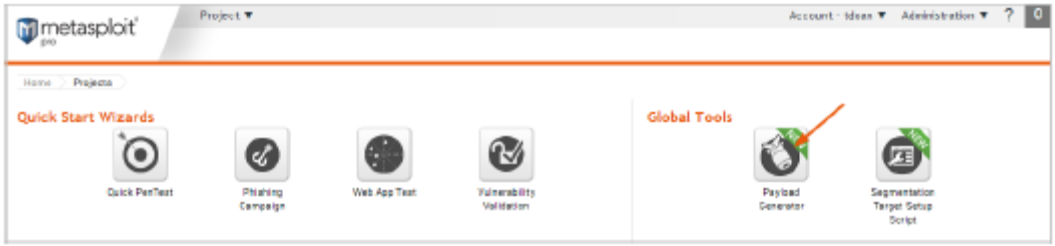
All credentials in the selected workspace are described here, divided by type.

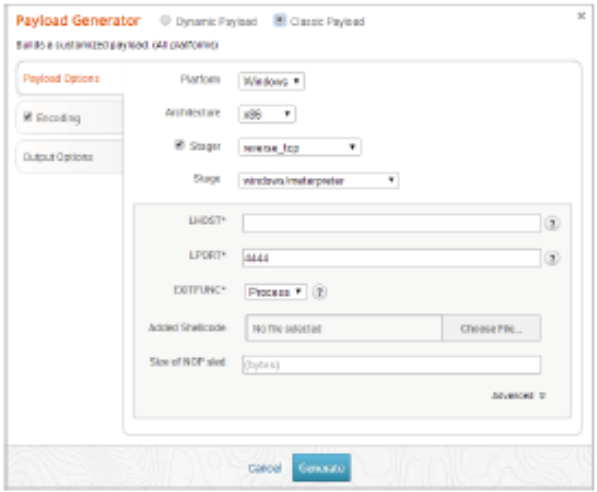
Plaintext Passwords

Public	Private	Realm Type	Realm Value	Origin	Hosts	Services
ralph	nequeametnatus	Active Directory Domain	lynchortiz	Service	1	1
shannon	estautaliquam	Oracle System Identifier	langworth	Service	1	1
osbaldo	etestaliquid	PostgreSQL Database	prosacco	Session	1	1
amalia.langosh	voluptasetquasi	DB2 Database	braun	Service	1	1
bella	enimblanditiiset	PostgreSQL Database	wintheiser	Service	1	1

안티바이러스를 우회하는 고급 Payload 생성

- DYNAMIC PAYLOAD 생성 기능으로 기존 대부분의 안티바이러스 및 IPS 등을 우회 침투
- 손쉬운 마법사 메뉴로 간단히 생성
- 피싱 등의 기법을 활용하여 내부 침투 테스트 수행
- 전통적인 기본 PAYLOAD 생성도 지원

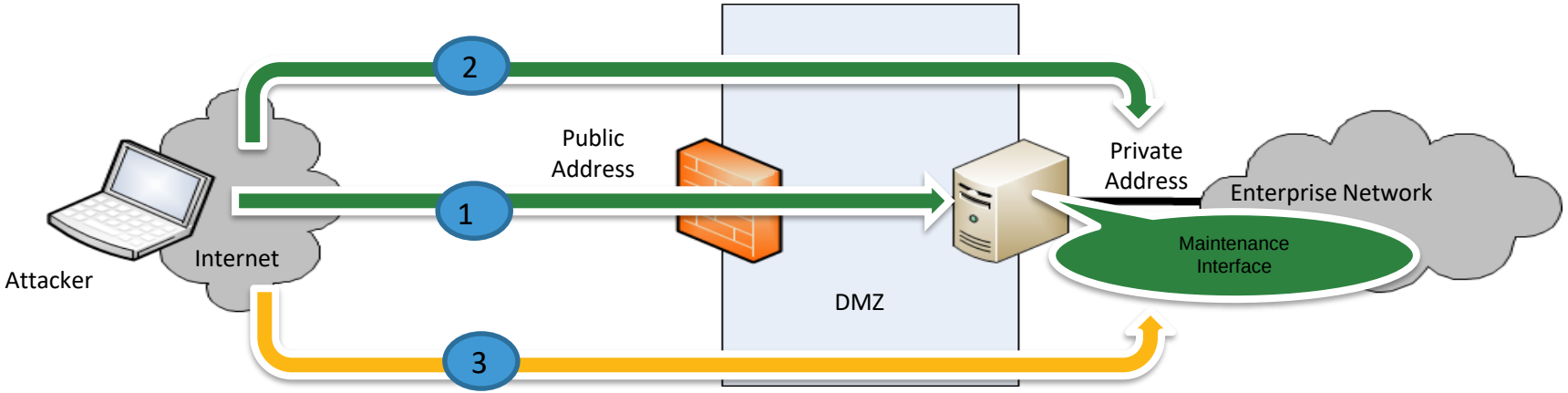




The Payload Generator

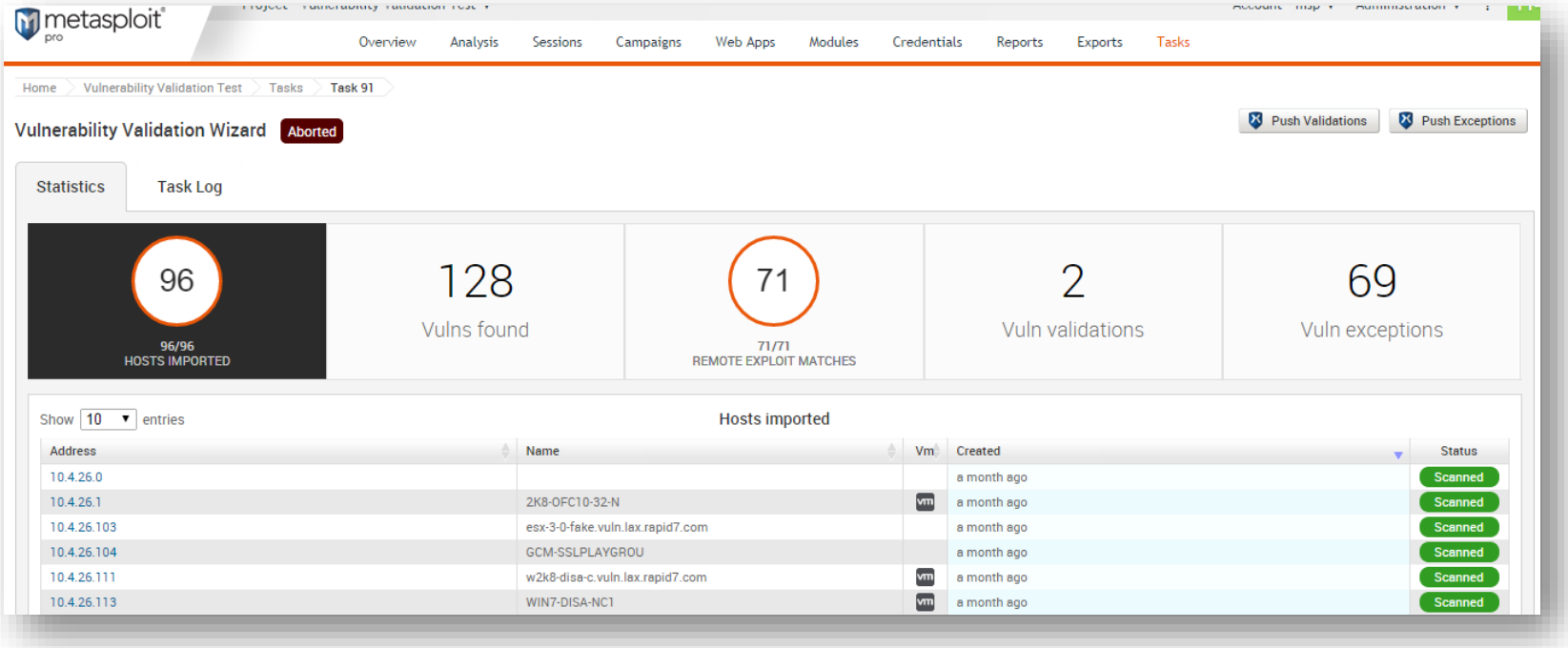
VPN Pivot 공격기법 제공

1. 원격 타겟시스템 연결을 위한 기법으로 METERPRETER 원격 전달
2. VPN PIVOT 생성
3. VPN PIVOT은 공격 시스템 위에 원격 타겟 시스템과 직접 연결할 수 있는 인터페이스를 생성



취약점의 실제 위험성 검증

취약점들을 제거 조치하기 위해 실제 해킹 검증 후 우선순위 설정
예외대상 취약점 항목과 실제 공격 성공한 취약점 항목을 NEXPOSE에 연결 표시



웹 어플리케이션 감사

OWASP TOP 10 진단

취약점에 해당하는 URL, PARAMETER와 취약점 근거를 보여줌

Show 10 entries

Risk	Category	Name	Path	Confidence	Method	Parameter	Proof
High	SQLi	SQL Injection	http://192.168.152.13/mutillidae/index.php	75	GET	password	xecuting query: You have an...
High	SQLi	SQL Injection	http://192.168.152.13/mutillidae/index.php	75	GET	username	xecuting query: You have an...
High	SQLi	SQL Injection	http://192.168.152.13/mutillidae/index.php	75	GET	username	xecuting query: You have an...
High	SQLi	SQL Injection	http://192.168.152.13/mutillidae/index.php	75	POST	ToolID	xecuting query: You have an...
High	SQLi	SQL Injection	http://192.168.152.13/mutillidae/index.php	75	POST	author	xecuting query: You have an...
High	SQLi	SQL Injection	http://192.168.152.13/mutillidae/index.php	75	POST	blog_entry	xecuting query: You have an...
High	SQLi	SQL Injection (blind)	http://192.168.152.13/mutillidae/index.php	55	POST	author	Boolean manipulation.
High	SSN-disclosure	Found Social Security Number	http://192.168.152.13/twiki/bin/view/TWiki/RegularExpression	100	GET	path	123-45-6789
Low	CSRF	Business-logic-relevant form without anti-CSRF token	http://192.168.152.13/mutillidae/index.php	75	GET	path	<form action="./index.php?p...
Low	CSRF	Business-logic-relevant form without anti-CSRF token	http://192.168.152.13/phpMyAdmin/test/theme.php	75	GET	path	<form method="post" action=...

Showing 11 to 20 of 44 entries

First Previous 1 2 3 4 5 Next Last

웹 모의침투 공격

웹 취약점(XSS, SQLI, ETC) 모의 공격 수행

Vuln Info: OWASP Top 10 #209 (XSS)

URL: http://192.168.152.13/mutillidae/index.php

Host: 192.168.152.13

Category: XSS

Name: Cross-Site Scripting

Risk: Low (3)

Confidence: 100

Description:

A cross-site scripting vulnerability has been identified. This may allow the attacker to run javascript in the context of the web application's domain

Vulnerable Method: GET

Vulnerable Parameter: password

Proof:

```
o use near '"--><xssmsfpro/>
```

Replay Vulnerability

page

user-info.php

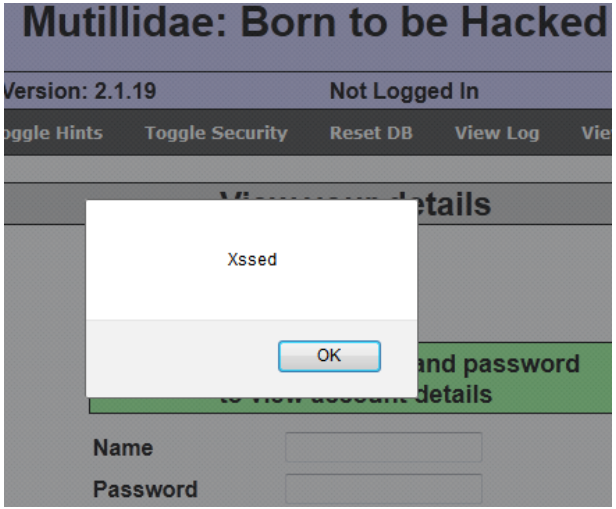
username

password

```
"--><script>alert("Xssed")</script>
```

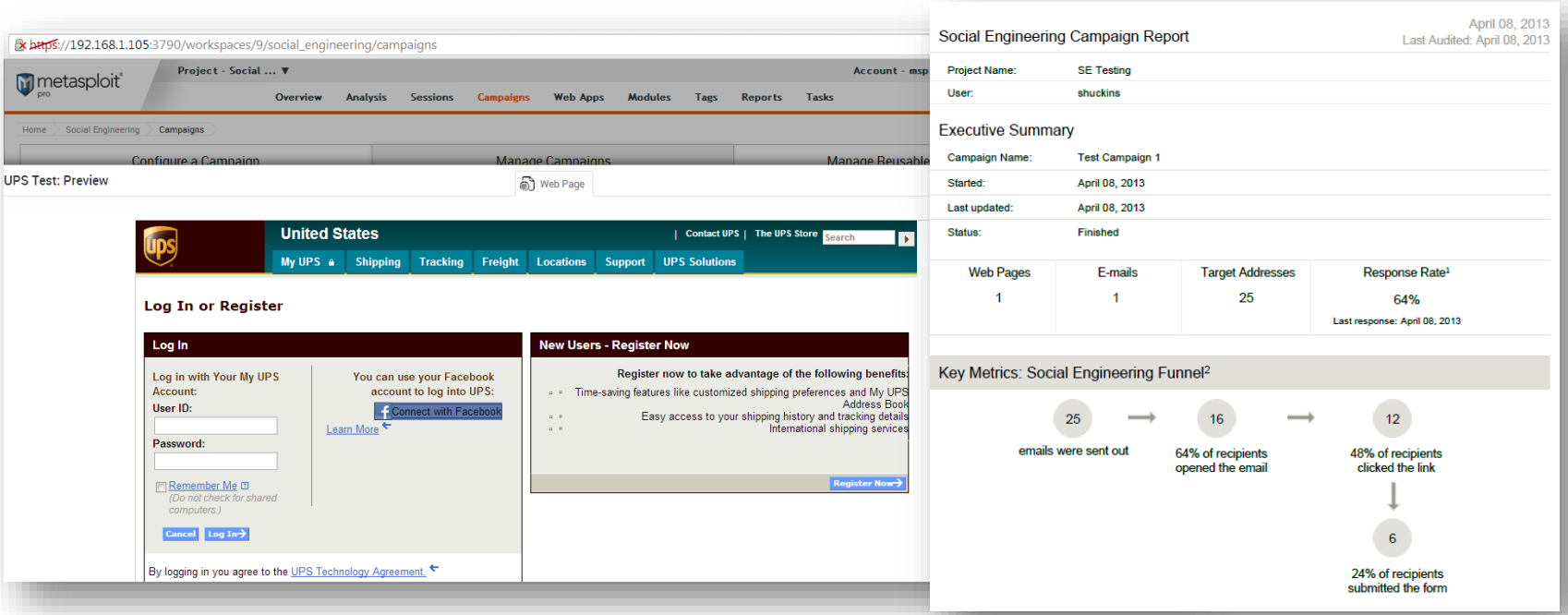
user-info-php-submit-button

View Account Details



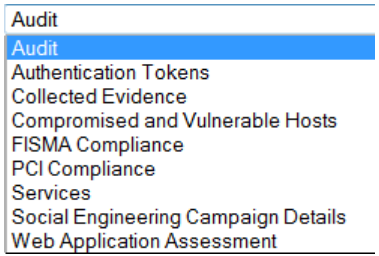
사회공학 테스트(Social Engineering)

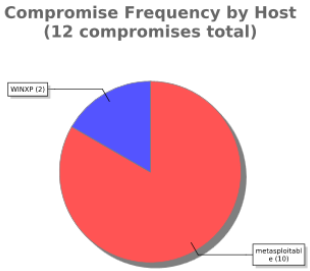
피싱 이메일과 사이트를 쉽게 생성
몇 명의 사용자가 열어보고, 정보입력 후 제출 행위까지 했는지 통계를 보여줌

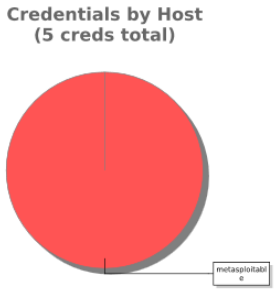


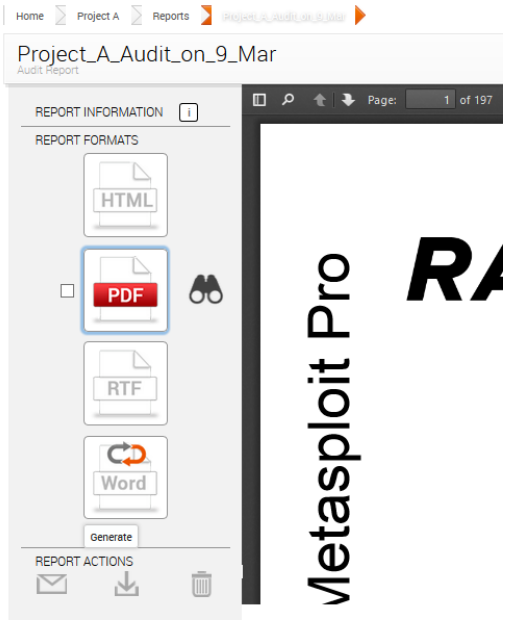
리포팅

기본 9 종류의 리포트 형식 제공
사용자 정의 리포트 : 고객사 로고 및 새로운 템플릿 작성 가능









핵심 요약

편의성

- 모의 침투 테스트를 잘 모르는 사람도 Metasploit을 통해 손쉽게 수행할 수 있음

효율성

- 수많은 취약점들 중에서 실제 위험성을 쉽게 검증하고 해당하는 공격 유형을 자동으로 적용함
- 기존의 수동 기반 선택적 침투 테스트가 아닌 자동 전수 테스트를 수행
- 다른 수동 명령 툴에 비해 최소 45% 빠른 테스트 수행 효과

다각적인 침투 테스트 기능

- 서버 대상 공격, 클라이언트 대상 공격, 웹 공격, 사회공학 공격 등
- 내부 기타 보안 장치들의 실효성 검증, 클라이언트의 잠재적 위협 검증
- 조직의 임직원들의 보안 의식 제고를 위한 효과적 수단

취약점 통합 분석과 위험 관리 절차

Rapid7 기술 파트너 에코시스템

Rapid7은

75 이상의

파트너들과
플랫폼 연동 제휴

RAPID7

DATA COLLABORATION PARTNERS

- Two-way data sharing
- ‘Single pane of glass’
- Enhanced platform value

DATA WORKFLOW PARTNERS

- IT security integration
- Streamlines correction
- Improves IT efficiencies

DATA INGESTION PARTNERS

- Enhances analytics
- Enables detection
- Simplifies investigations

감사합니다

Contact Information

㈜파인앤애플시스템즈 신동호 부장
Phone : 070-7010-5902
Mobile : 010-6855-9776
E-Mail : dhshin@pineandapple.com