RAPID7

모의 해킹 자동화 솔루션

METASPLOIT PROFESSIONAL

INSEC security

RAPID7

Contens

INSEC security

취약점진단과 모의해킹의 차이

취약점 진단

- 체크리스트 기준으로 항목별 취약점 점검
- 위협이 있을 수 있는 취약점을 식별하고 위험의 가능성을 확인하는 수준

모의해킹

- 대상 시스템의 취약점 정보를 수집
- 취약점 정보를 바탕으로 위협 모델링
- 방법론을 구상하고 정보탈취, 정보변경, 시스템 파괴 등을 목적으로 해당 목적 달성까지 진행

중요 시스템의 정보를 탈취, 조작, 파괴 등이 가능한지를 알아내는 과정이 취약점 진단이라면,
모의해킹은 정보 탈취, 조작, 파괴 등이 실제로 일어날 수 있다는 것을 확인하고 수행하는 과정

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

RAPID7

Contens

INSEC security

Metasploit 소개

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 모듈을 선별
- Nexpose와 함께 사용하여 실제 위험 상태를 검증
- 소셜엔지니어링(피싱 기법)과 로그인 인증 검사를 통해 조직의 보안 인식과 방어 상태를 측정 관리
- Bruteforcing, VPN pivoting, social engineering 과 같은 정교한 공격에 대한 대응 훈련
- 대 내외 모의해킹 수행을 요구하는 보안 컴플라이언스에 대비한 효율적인 자동화 솔루션

Metasploit 특장점

익스플로잇의 신뢰성

- 20만명의 컴뮤니티와 본사 리서치 그룹에 의해 다양한 실제 공격 테스트 환경에서 가장 빠르고 정확하게 검증된 익스플로잇 코드 업데이트
- 라이브러리가 오픈소스이므로 다양한 환경을 위해 코드를 수정하면서 사용 가능

유연한 설치 운영 환경

- 윈도우, 레드햇, 우분투, Kali에 설치지원, 가벼운 Web UI, 컴맨드 인터페이스 지원

취약점 검증 기능

- 다양한 외부 취약점 진단 솔루션의 데이터를 이용한 위험 검증 테스트 지원
- Nexpose 와 취약점 스캔, 데이터 연결, 침투테스트 수행, 검증결과 피드백을 자동화 연동 설계

Metasploit 특장점

정교한 소셜 엔지니어링 기법

- 침투테스트 목적 이외에 임직원의 보안의식 재고 훈련 효과를 위한 정교한 피싱 기능 제공
- 한번에 5,000 명 이상의 수신인 대상으로 피싱 메일 처리 성능

풍부한 리포트

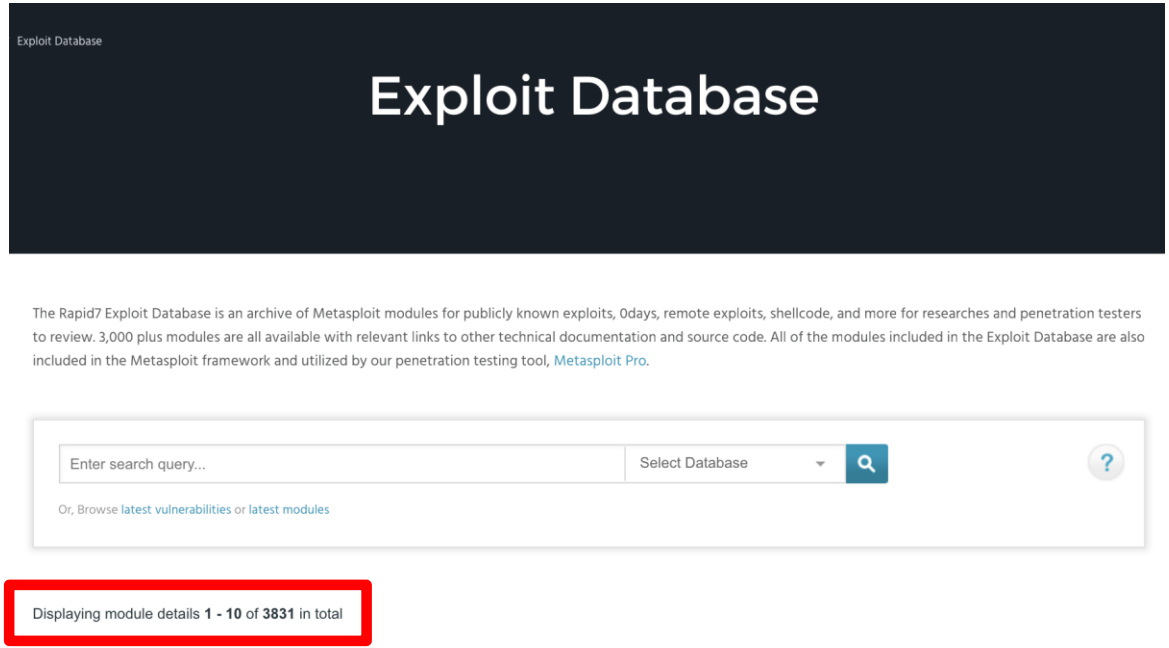
- 10가지 그래픽이 포함된 리포트 템플릿 기본 제공 및 수정 가능, 자동 리포트 생성 기능 포함
- 테스트 결과 데이터의 공유로 관리자가 원하는 외부 리포트 형식으로 출력 가능

RAPID7

Contens

INSEC security

자산의 취약점 대한 안전한 공격 시뮬레이션

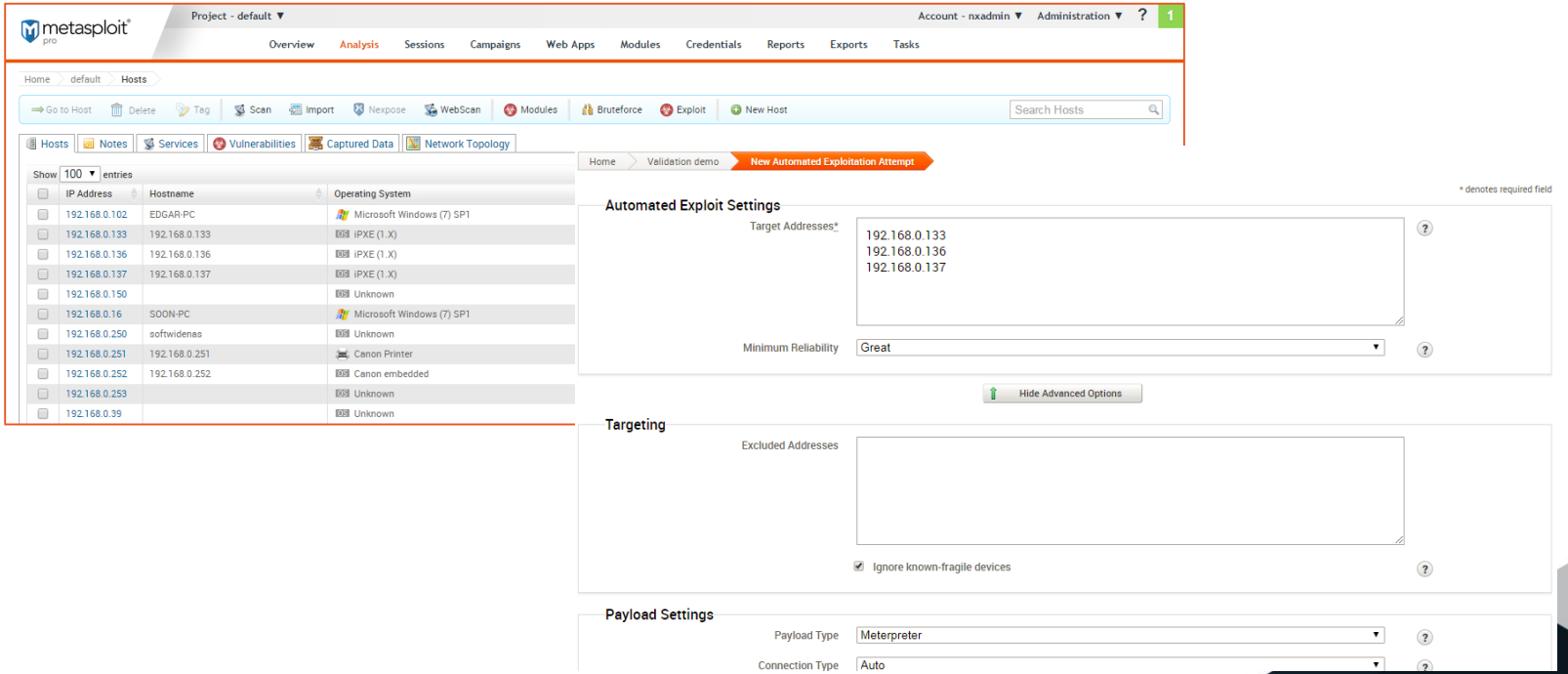


3800개 이상의
세계적으로 검증된 모듈
(2019년 3월 현재)

: AUXILIARY, POST EXPLOIT, CUSTOM EXPLOIT 모듈 포함

대량의 시스템 대상 자동 모의 침투 테스트

대량의 타겟에서 발견된 취약점들을 대상으로 연속된 공격 테스트를 자동 수행



서버에 대한 공격 유형

METASPLOIT이 서버를 공격하는 클라이언트로 작동

예, MS10_061(SMB PORT 445의 취약점)을 갖고있는 WIN XP 공격

Active Sessions

Session	OS	Host	Type	Age	Description	Attack Module
Session 197		192.168.152.22 - WINXP	Meterpreter	2 minutes	NT AUTHORITY\SYSTEM @ WINXP	MS10_061_SPOOLSS

Microsoft Print Spooler Service Impersonation Vulnerability

exploit/windows/smb/ms10_061_spoolss

This module exploits the RPC service impersonation vulnerability detailed in Microsoft Bulletin MS10-061. By making a specific DCE RPC request to the StartDocPrinter procedure, an attacker can impersonate the Printer Spooler service to create a file. The working directory at the time is %SystemRoot%\system32. An attacker can specify any file name, including directory traversal or full paths. By sending WritePrinter requests, an attacker can fully control the content of the created file.

Module Options

PNAME		The printer share name to use on the target (string)
RPORT	445	Set the SMB service port (integer)
SMBPIPE	spoolss	The named pipe for the spooler service (string)

클라이언트에 대한 공격 유형

METASPLOIT이 자신에 접속하는 클라이언트를 침해하는 (웹)서버처럼 동작예, 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

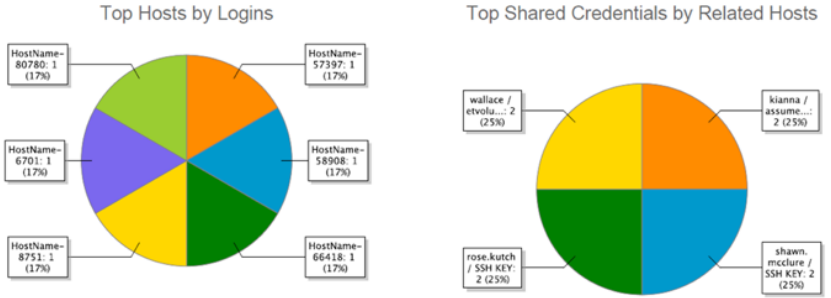
This module exploits a memory corruption vulnerability within Microsoft\'s HTML engine (mshtml). When parsing an HTML page containing a recursive CSS import, a C++ object is deleted and later reused. This leads to arbitrary code execution.

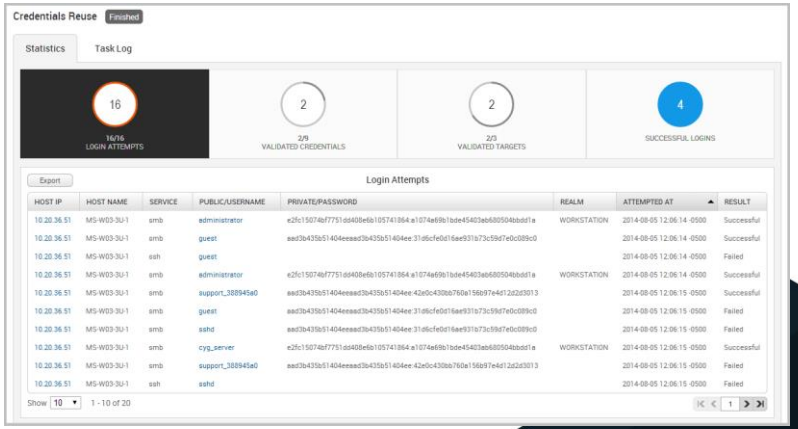
Module Options

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 탈취된 인증 정보를 활용한 공격에 대비

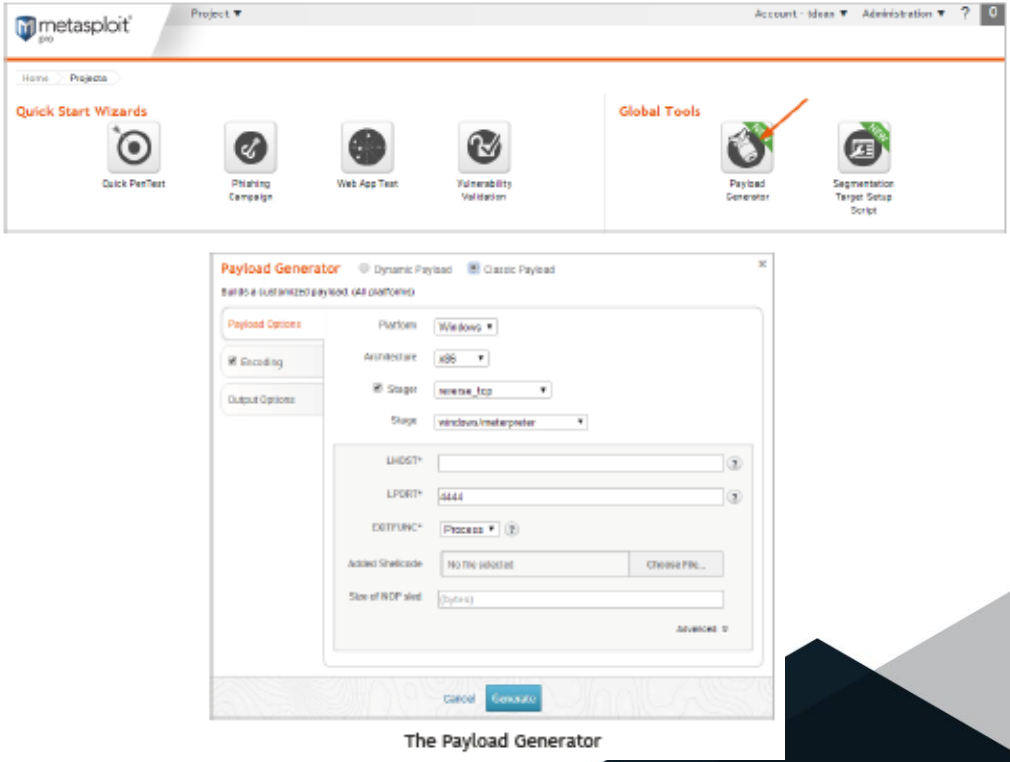
- 취약점 EXPLOIT 이외에 시스템 계정 침투 공격이 새로운 위협으로 부상
- 다양한 BRUTE FORCE 테스트 기능
- 타겟 시스템에서 획득한 기존 계정 정보 수집 및 재사용
- 사용자가 정의한 계정 리스트로 신속한 인증 침투 테스트 수행
- 계정 인증 침투 테스트 결과 리포트 생성





안티바이러스를 우회하는 고급 Payload 생성

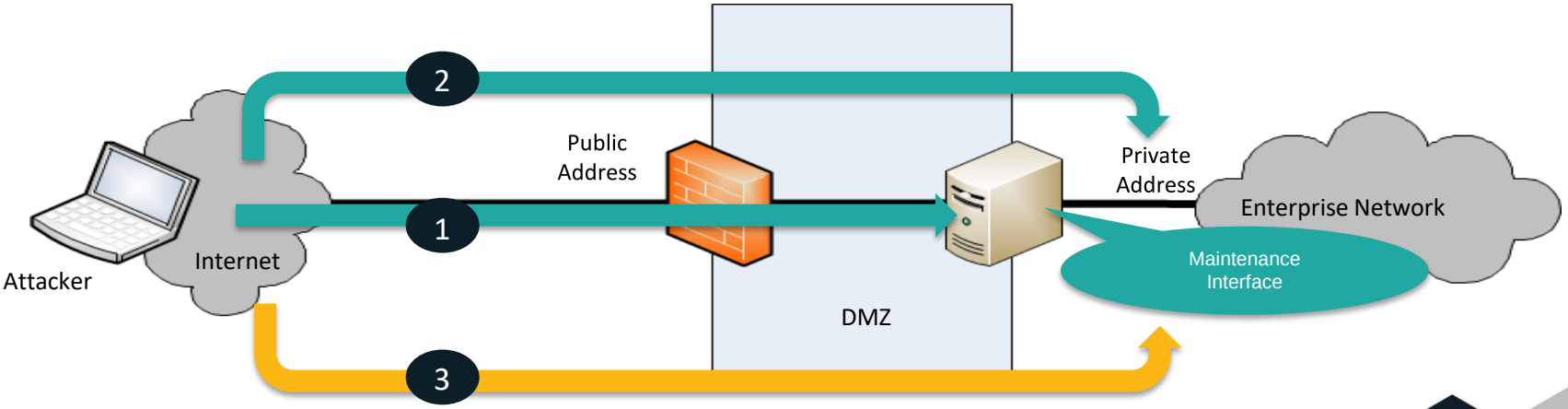
- DYNAMIC PAYLOAD 생성 기능으로 기존 대부분의 안티바이러스 및 IPS 등을 우회 침투
- 손쉬운 마법사 메뉴로 간단히 생성
- 피싱 등의 기법을 활용하여 내부 침투 테스트 수행
- 전통적인 기본 PAYLOAD 생성도 지원



The Payload Generator

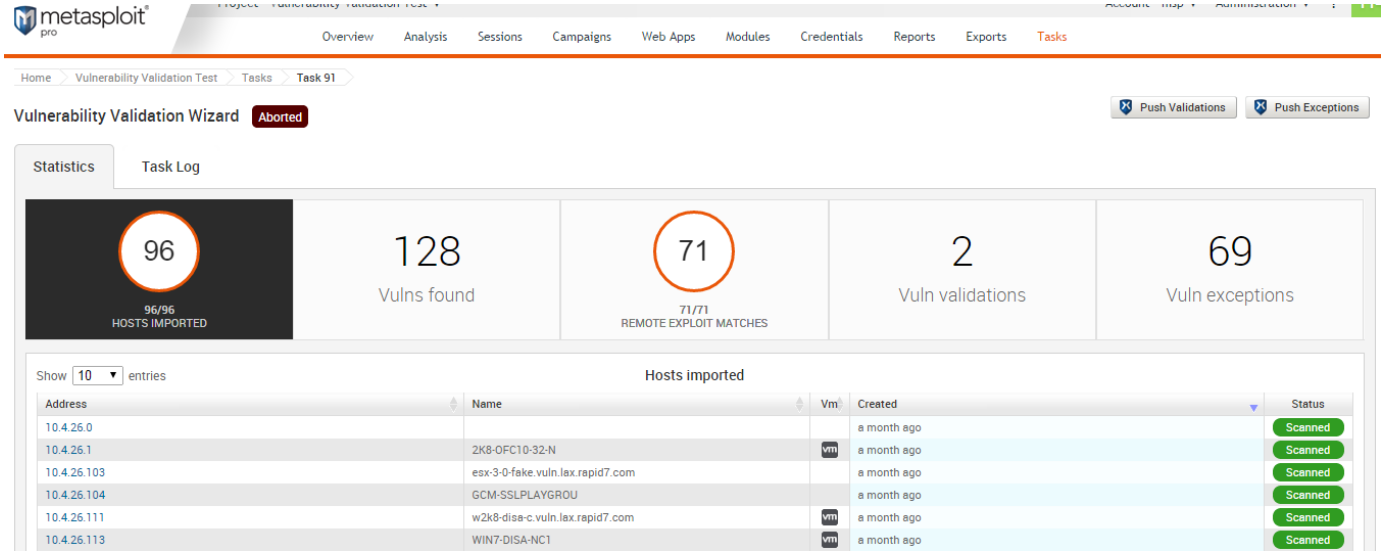
VPN Pivot 공격기법 제공

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



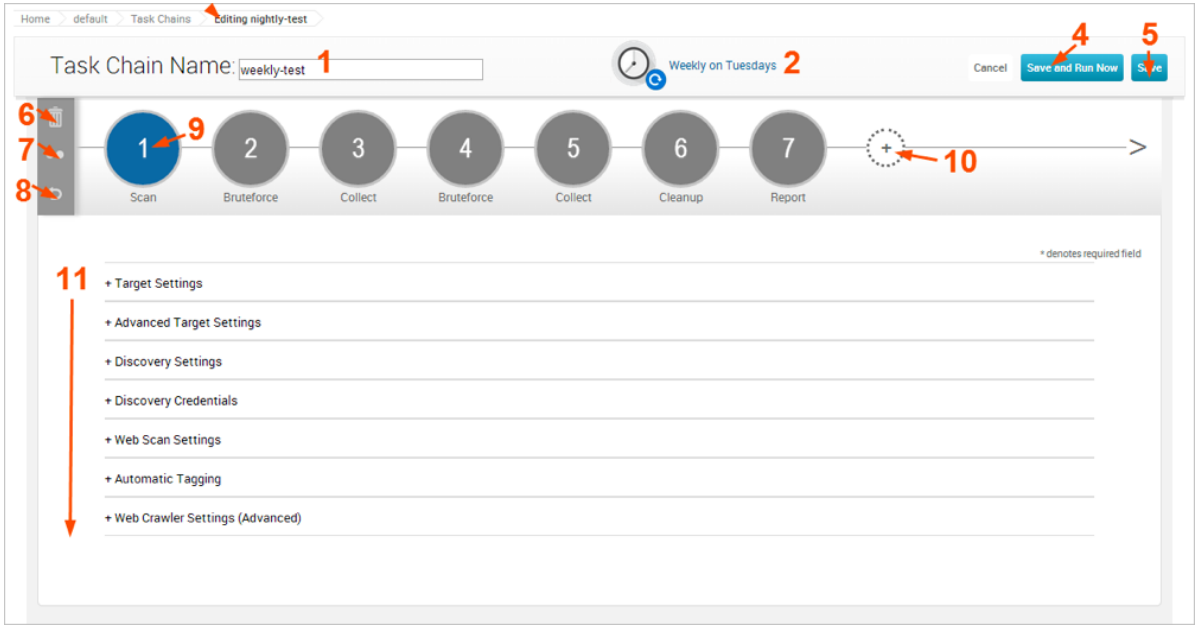
취약점의 실제 공격 위험을 검증 – Nexpose 와 동적인 연동

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



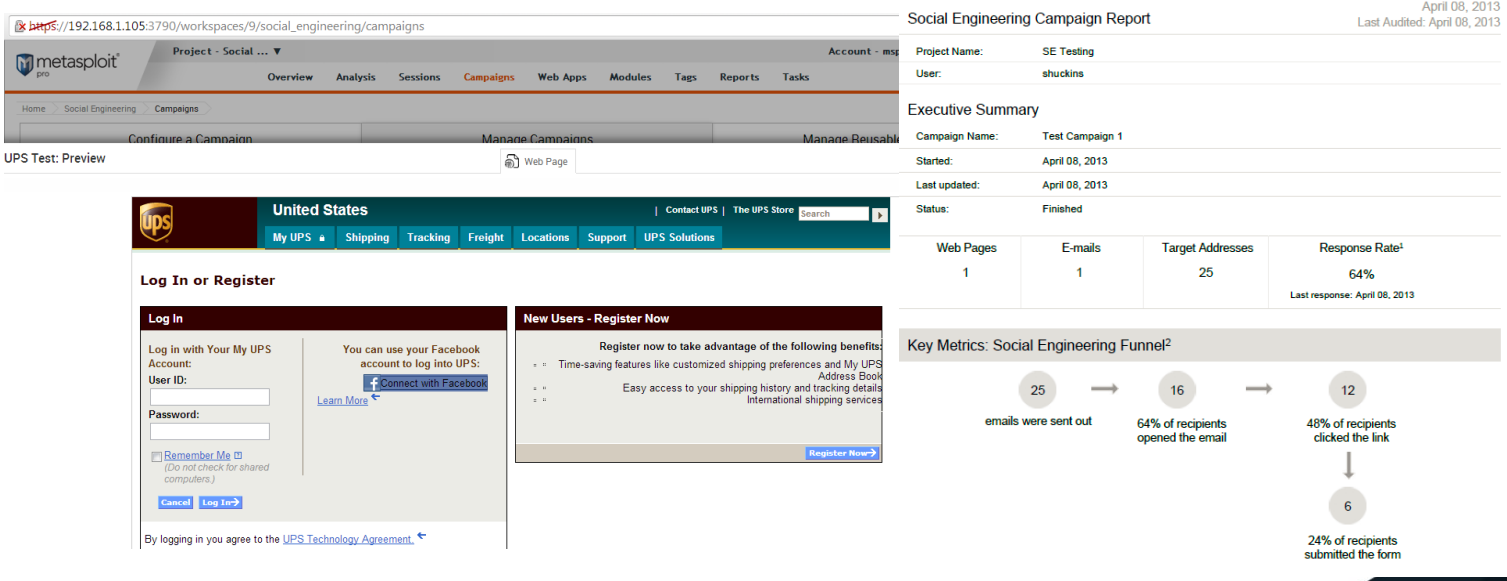
Task Chains

- 개별 테스트 작업들을 정의하고 연속적으로 배치하여 워크플로우를 만드는 기능
- 워크플로우를 스케줄링하여 자동으로 수행 후 결과 보고서 생성



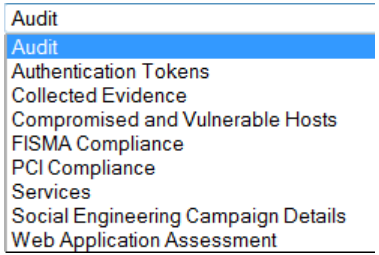
사회공학 테스트(Social Engineering)

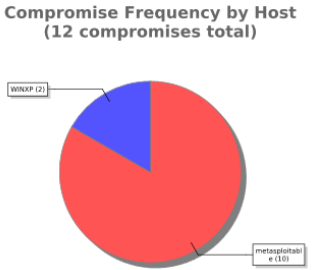
- 피싱 이메일과 사이트를 쉽게 생성
- 몇 명의 사용자가 열어보고, 정보입력 후 제출 행위까지 했는지 통계를 보여줌

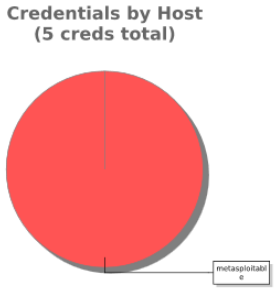


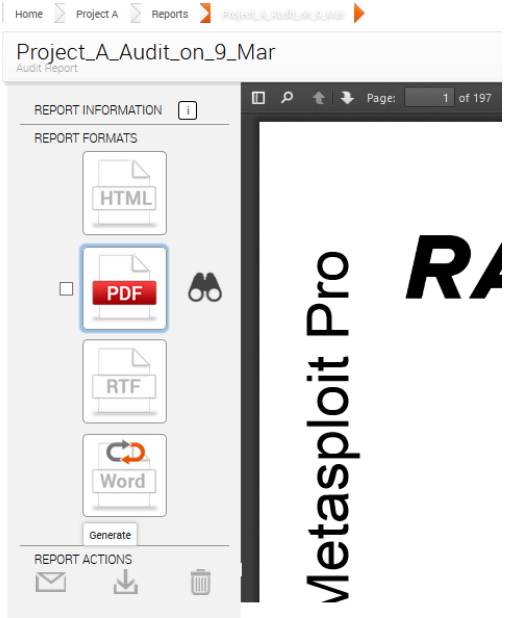
리포팅

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









RAPID7

Contens

INSEC security

취약점 위험 관리의 기대효과

모의 침투 테스트

- 실제 공격자 관점에서 전체 IT자산의 보안 문제 검증
- 기존의 모의 침투테스트 비용 및 시간 대폭 절감

자동 모의해킹 수행

취약점 별 실제 위험 검증

- 실제 위험의 정확한 판별로 순위별 개선 조치 업무 제시
- Nexpose 연동을 통해, 취약점 결과 기반으로 모의침투 수행

해결조치 우선순위 결정

사용자들의 보안의식 관리

- 사용자들 대상, 모의 피싱 테스트로 보안의식 평가
- 전반적인 위험 관리에 대한 실질적 교육 효과

침해사고 사전 예방 효과

RAPID7

Contens

INSEC security

한국 고객

공공기관

NSR 국가보안기술연구소 National Security Research Institute

Defense Security Support Command Since 2018 군사안보지원사령부

대한민국 국방부 Ministry of National Defense

KISA 한국인터넷진흥원 Korea Internet & Security Agency

cbist 충북과학기술혁신원 Chungbuk Innovation Institute of Science & Technology

Incheon Airport 인천국제공항공사

일반기업

LG전자

SEOUL 서울반도체㈜

SAMSUNG 삼성전자

천재교육

롯데정보통신

NCSOFT

HYUNDAI

충청대학교 CHUNG CHEONG UNIV.

THANK YOU

INSEC security

본　　사 : 서울특별시 금천구 가산디지털1로 19 대륭테크노타운 18차 406호
Email : insec@insec.co.kr TEL : 02-863-5687 www.insec.co.kr

RAPID7