

RAPID7

모의 해킹 자동화 솔루션

METASPLOIT PROFESSIONAL

Contents

- ★ 1. 모의해킹의 필요성
- 2. Metasploit 제품 소개
- 3. Metasploit 주요 기능
- 4. Metasploit 기대 효과
- 5. Metasploit 레퍼런스

취약점진단과 모의해킹의 차이



취약점 진단

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



모의해킹

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

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

- 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



Contents

1. 모의해킹의 필요성

★ 2. Metasploit 제품 소개

3. Metasploit 주요 기능

4. Metasploit 기대 효과

5. Metasploit 레퍼런스



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

익스플로잇의 신뢰성

- 20만명의 커뮤니티와 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, 커맨드 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

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

Contents

1. 모의해킹의 필요성
2. Metasploit 제품 소개
- ★ 3. Metasploit 주요 기능
4. Metasploit 기대 효과
5. Metasploit 레퍼런스

자산의 취약점 대한 안전한 공격 시뮬레이션

Exploit Database

Exploit Database

The Rapid7 Exploit Database is an archive of Metasploit modules for publicly known exploits, 0days, remote exploits, shellcode, and more for researchers and penetration testers to review. 3,000 plus modules are all available with relevant links to other technical documentation and source code. All of the modules included in the Exploit Database are also included in the Metasploit framework and utilized by our penetration testing tool, [Metasploit Pro](#).

Or, Browse [latest vulnerabilities](#) or [latest modules](#)

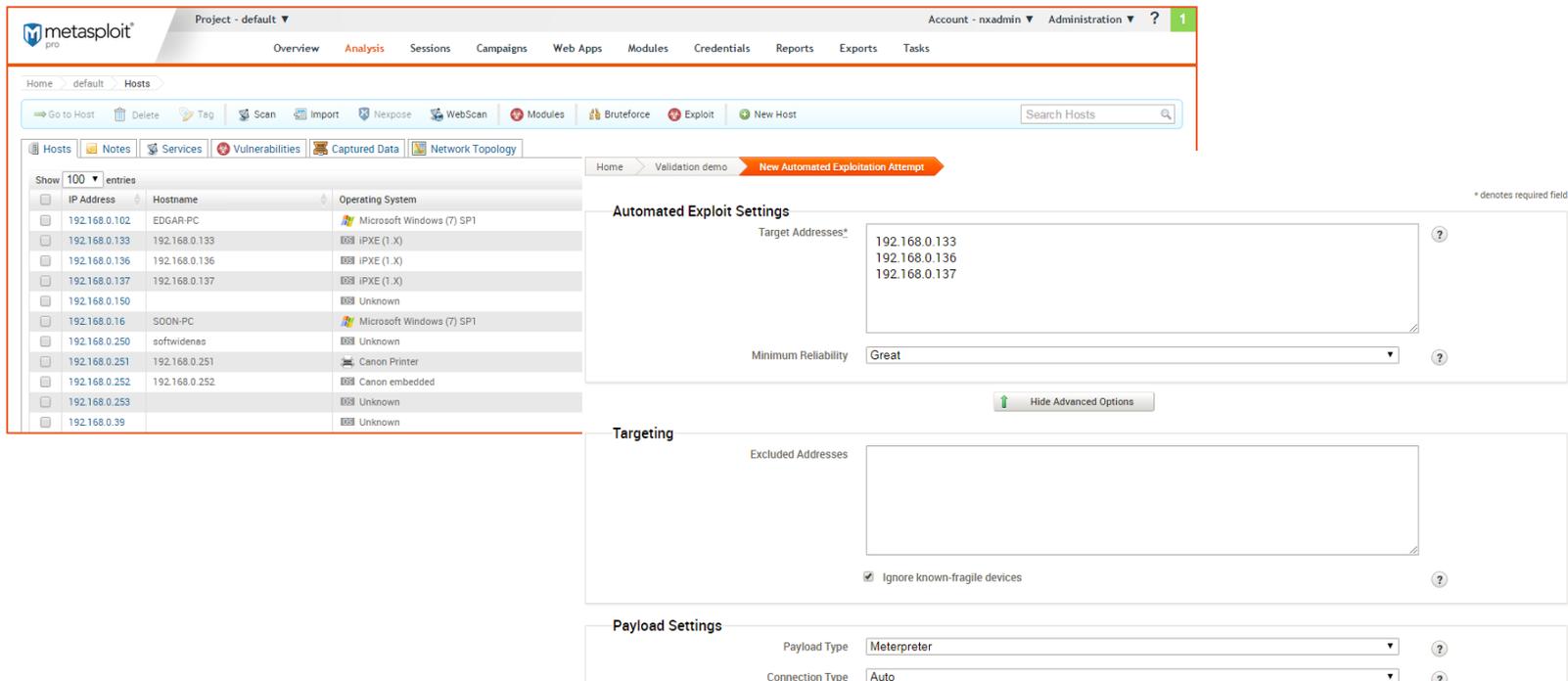
Displaying module details 1 - 10 of 3831 in total

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



The screenshot displays the Metasploit Pro web interface. The top navigation bar includes 'Project - default', 'Account - nxadmin', and 'Administration'. The main menu contains 'Overview', 'Analysis', 'Sessions', 'Campaigns', 'Web Apps', 'Modules', 'Credentials', 'Reports', 'Exports', and 'Tasks'. The breadcrumb trail is 'Home > default > Hosts'. Below the breadcrumb, there are action buttons: 'Go to Host', 'Delete', 'Tag', 'Scan', 'Import', 'Nexpose', 'WebScan', 'Modules', 'Bruteforce', 'Exploit', and 'New Host', along with a 'Search Hosts' input field.

The 'Hosts' tab is active, showing a table of 100 entries. The table has columns for 'IP Address', 'Hostname', and 'Operating System'. The data is as follows:

IP Address	Hostname	Operating System
192.168.0.102	EDGAR-PC	Microsoft Windows (7) SP1
192.168.0.133	192.168.0.133	IPXE (1.X)
192.168.0.136	192.168.0.136	IPXE (1.X)
192.168.0.137	192.168.0.137	IPXE (1.X)
192.168.0.150		Unknown
192.168.0.16	SOON-PC	Microsoft Windows (7) SP1
192.168.0.250	softwidenas	Unknown
192.168.0.251	192.168.0.251	Canon Printer
192.168.0.252	192.168.0.252	Canon embedded
192.168.0.253		Unknown
192.168.0.39		Unknown

The right-hand pane shows the 'New Automated Exploitation Attempt' configuration. It includes:

- Automated Exploit Settings:** 'Target Addresses*' is a text area containing '192.168.0.133', '192.168.0.136', and '192.168.0.137'. 'Minimum Reliability' is set to 'Great'.
- Targeting:** 'Excluded Addresses' is an empty text area. The checkbox 'Ignore known-fragile devices' is checked.
- Payload Settings:** 'Payload Type' is set to 'Meterpreter' and 'Connection Type' is set to 'Auto'.

A 'Hide Advanced Options' button is located between the 'Automated Exploit Settings' and 'Targeting' sections. A note '* denotes required field' is visible in the top right of the settings area.

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	<input type="text"/>	The printer share name to use on the target (string)
RPORT	<input type="text" value="445"/>	Set the SMB service port (integer)
SMBPIPE	<input type="text" value="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 In
[*] 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

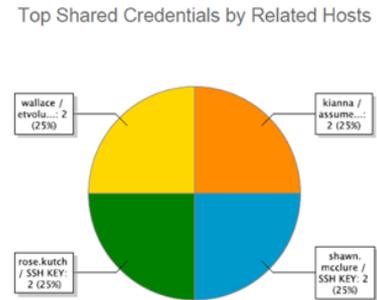
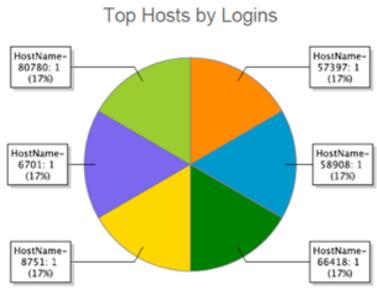
This module exploits a memory corruption vulnerability within Microsoft's HTML engine (mshtml). When parsing an HTML page containing a recursive CSS import, a C++ object is deleted and later reused. This leads to arbitrary code execution.

Module Options

OBFUSCATE	<input checked="" type="checkbox"/>	Enable JavaScript obfuscation (bool)
SRVHOST	<input type="text" value="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	<input type="text" value="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



Credentials Reuse Finished

Statistics Task Log

16

16/16 LOGIN ATTEMPTS

2

2/9 VALIDATED CREDENTIALS

2

2/3 VALIDATED TARGETS

4

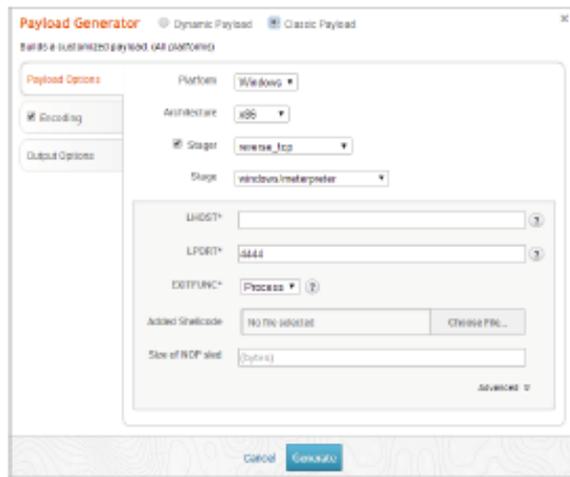
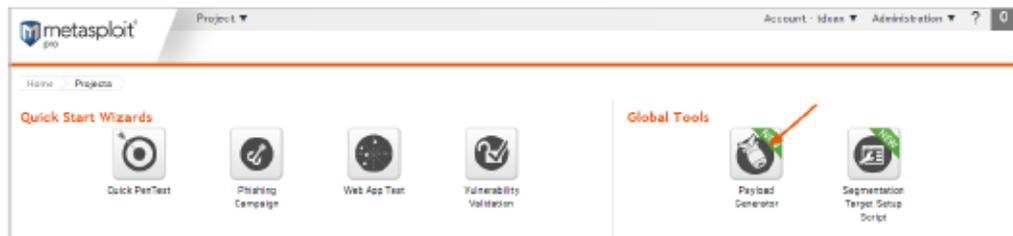
SUCCESSFUL LOGINS

HOST IP	HOST NAME	SERVICE	PUBLIC/USERNAME	PRIVATE/PASSWORD	REALM	ATTEMPTED AT	RESULT
10.20.36.51	MS-W30-SU-1	smb	administrator	e25c15074b77316d408e6b105741864a1074e69b1bde45403a680504b6b0f1e	WORKSTATION	2014-08-05 12:06:14 -0500	Successful
10.20.36.51	MS-W30-SU-1	smb	guest	ead3b433651404eeead3b433651404ee318dcfe6d16ae931b73c5987e0c089c0		2014-08-05 12:06:14 -0500	Successful
10.20.36.51	MS-W30-SU-1	ssh	guest			2014-08-05 12:06:14 -0500	Failed
10.20.36.51	MS-W30-SU-1	smb	administrator	e25c15074b77316d408e6b105741864a1074e69b1bde45403a680504b6b0f1e	WORKSTATION	2014-08-05 12:06:14 -0500	Successful
10.20.36.51	MS-W30-SU-1	smb	support_388945a0	aa83b433651404eeead3b433651404ee42b0c433ba760a156b97e4612a2c3073		2014-08-05 12:06:15 -0500	Successful
10.20.36.51	MS-W30-SU-1	smb	guest	e25c15074b77316d408e6b105741864a1074e69b1bde45403a680504b6b0f1e		2014-08-05 12:06:15 -0500	Failed
10.20.36.51	MS-W30-SU-1	smb	sahd	ead3b433651404eeead3b433651404ee318dcfe6d16ae931b73c5987e0c089c0		2014-08-05 12:06:15 -0500	Failed
10.20.36.51	MS-W30-SU-1	smb	cty_server	e25c15074b77316d408e6b105741864a1074e69b1bde45403a680504b6b0f1e	WORKSTATION	2014-08-05 12:06:15 -0500	Successful
10.20.36.51	MS-W30-SU-1	smb	support_388945a0	ead3b433651404eeead3b433651404ee42b0c433ba760a156b97e4612a2c3073		2014-08-05 12:06:15 -0500	Failed
10.20.36.51	MS-W30-SU-1	ssh	sahd			2014-08-05 12:06:15 -0500	Failed

Show 10 1 - 10 of 20

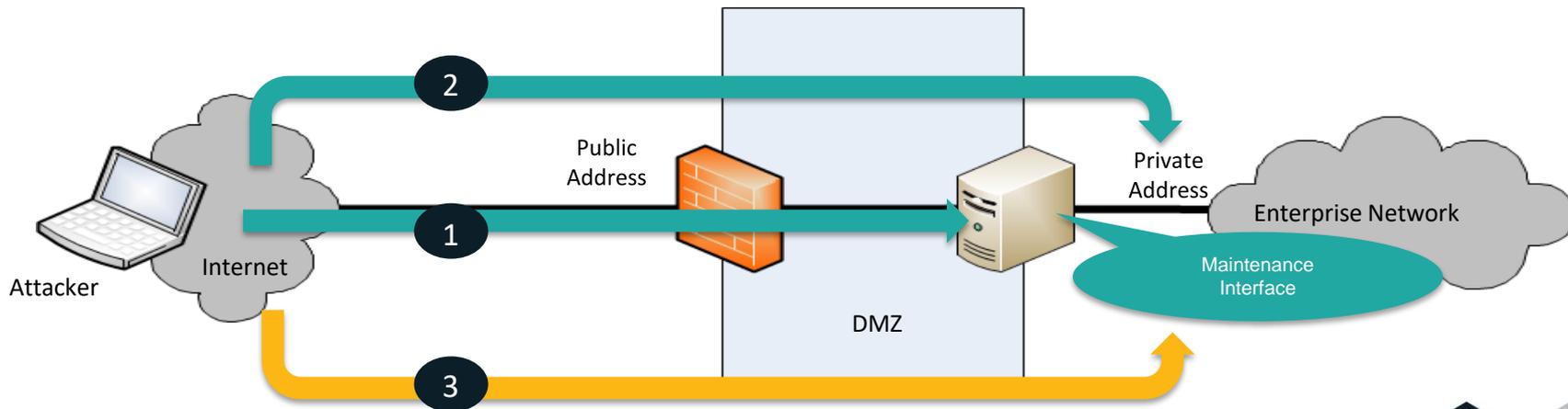
안티바이러스를 우회하는 고급 Payload 생성

- 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

- 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

metasploit^{pro}

Overview Analysis Sessions Campaigns Web Apps Modules Credentials Reports Exports Tasks

Home > Vulnerability Validation Test > Tasks > Task 91

Vulnerability Validation Wizard **Aborted** Push Validations Push Exceptions

Statistics Task Log

96 96/96 HOSTS IMPORTED	128 Vulns found	71 71/71 REMOTE EXPLOIT MATCHES	2 Vuln validations	69 Vuln exceptions
-------------------------------	--------------------	---------------------------------------	-----------------------	-----------------------

Show 10 entries

Address	Name	Vm	Created	Status
10.4.26.0			a month ago	Scanned
10.4.26.1	2K8-0FC10-32-N	vm	a month ago	Scanned
10.4.26.103	esx-3-0-fake.vuln.lax.rapid7.com		a month ago	Scanned
10.4.26.104	GCM-SSLPLAYGROU		a month ago	Scanned
10.4.26.111	w2k8-dise-c.vuln.lax.rapid7.com	vm	a month ago	Scanned
10.4.26.113	WIN7-DISA-NC1	vm	a month ago	Scanned

Task Chains

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

Home > default > Task Chains > editing nightly-test

Task Chain Name: weekly-test 1

Weekly on Tuesdays 2

Cancel Save and Run Now 4 Save 5

6 7 8

1 2 3 4 5 6 7 + 10

Scan Bruteforce Collect Bruteforce Collect Cleanup Report

11 + Target Settings

+ Advanced Target Settings

+ Discovery Settings

+ Discovery Credentials

+ Web Scan Settings

+ Automatic Tagging

+ Web Crawler Settings (Advanced)

* denotes required field

사회공학 테스트(Social Engineering)

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

UPS Test: Preview

Social Engineering Campaign Report

April 08, 2013

Last Audited: April 08, 2013

Project Name: SE Testing
User: shuckins

Executive Summary

Campaign Name: Test Campaign 1

Started: April 08, 2013

Last updated: April 08, 2013

Status: Finished

Web Pages	E-mails	Target Addresses	Response Rate ¹
1	1	25	64%

Last response: April 08, 2013

Key Metrics: Social Engineering Funnel²



United States | Contact UPS | The UPS Store

My UPS | Shipping | Tracking | Freight | Locations | Support | UPS Solutions

Log In or Register

Log In

Log in with Your My UPS Account:

User ID:

Password:

Remember Me (Do not check for shared computers.)

[Cancel](#) [Log In](#)

By logging in you agree to the [UPS Technology Agreement](#).

New Users - Register Now

Register now to take advantage of the following benefits:

- Time-saving features like customized shipping preferences and My UPS Address Book
- Easy access to your shipping history and tracking details
- International shipping services

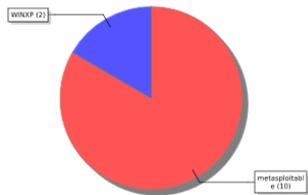
[Register Now](#)

리포트

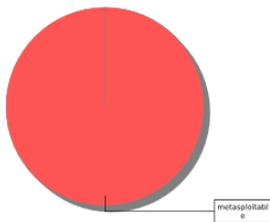
- 기본 9 종류의 리포트 형식 제공
- 사용자 정의 리포트 : 고객사 로고 및 새로운 템플릿 작성 가능

Audit
Audit
Authentication Tokens
Collected Evidence
Compromised and Vulnerable Hosts
FISMA Compliance
PCI Compliance
Services
Social Engineering Campaign Details
Web Application Assessment

Compromise Frequency by Host
(12 compromises total)



Credentials by Host
(5 creds total)



Contents

1. 모의해킹의 필요성
2. Metasploit 제품 소개
3. Metasploit 주요 기능
- ★ 4. Metasploit 기대 효과
5. Metasploit 레퍼런스

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

Contents

1. 보안 동향
2. Metasploit 제품 소개
3. Metasploit 주요 기능
4. Metasploit 기대 효과
- ★ 5. Metasploit 레퍼런스

공공기관



일반기업



서울반도체|주|



THANK YOU