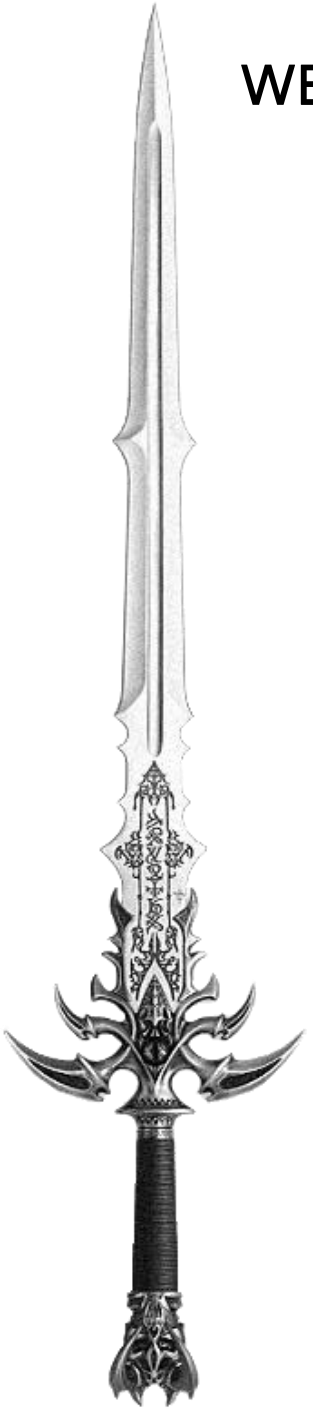
웹 모의해킹 시나리오의 완성

WEB HACKING 서버 침투 기법



Unrestricted File Upload
File download
Local File Inclusion
Remote File Inclusion
HTTP PUT Method
Command Injection
Reverse Shell
Port forwarding & Tunneling

웹 모의해킹 심화기술

OPEN SECURE LAB.

유현수 지음

현재 오픈시큐어랩 대표와 보안 카페를 운영하고 있으며 기초 해킹, 고급 해킹, 사이버 보안 실무 강의와 시나리오 침투 테스트 및 모의해킹 등의 기술 기반 컨설팅을 수행하고 있습니다.

이전에는 신한은행의 보안팀에서 취약점 분석·평가를 담당했으며 정보보호전문업체 및 금융보안원과 다수의 취약점 분석·평가 및 침해사고 대응훈련 등을 수행, 삼성 SDS 싱가폴 법인에서 삼성전자 동남아 총괄 보안에서 신규 서비스 보안성 심의 및 역내 사이버사업장 보안 담당, 시큐아이닷컴 컨설팅 사업부에서 50 개가 넘는 기관에서 보안 컨설팅을 수행했습니다.

오픈시큐어랩 카페 café.naver.com/opensecurelab
저자 블로그 n3015m.tistory.com
저자 이메일 n3oism@gmail.com

국립중앙도서관 출판예정도서목록(CIP)

웹 모의해킹 시나리오의 완성 WEB HACKING 서버 침투 기법 / 지은이: 유현수. -- [서울] : 오픈시큐어랩 BOOKS, 2017
p. ; cm

ISBN 979-11-962132-1-3 93000 : ₩18500

컴퓨터 보안[--保安]

004.61-KDC6
005.8-DDC23 CIP2017027187

웹 모의해킹 시나리오의 완성

WEB HACKING 서버 침투 기법

웹 모의해킹 심화기술

여는글

부족한게 많았던 사회 초년 시절, 첫 직장으로 정보보호전문업체에 취업해 고객사에서 고군분투 했던 기억이 새록새록 난다. 아무것도 모른다고 해도 과언이 아니었다. 고객들은 모의해킹 전문가로 많은 문제점을 찾고 해결책을 제시해 주길 바라고 있었겠지만, 늘 모르는 게 더 많아 고생했던 시간들과 밤샘하면서 연구하고 노력했던 시간들이 주마등처럼 지나간다.

어느새 정보보안 분야에서 10 년이 넘는 시간이 지나 소프트웨어 경력 기준으로 특급인력이 되었다. 마지막 회사인 제 1 금융권의 보안 담당자로 재직하며 보안관제, 보안장비 운영자 그리고 수많은 엔지니어 분들을 접했다. 정보보호전문업체와 금융결제원 및 지금의 금융보안원 등 모의해킹 프로젝트 사업을 관리하며 언제나 초급 기술자 그리고 이 업계에 첫발을 내디딘 신입 분들을 많이 접하게 되었다. 대부분 체계적인 교육을 받고 진출한 분들보다 그렇지 못한 분들이 많아 지식을 공유했던 기억이 난다. 하지만 근본적으로 열정이 있고 열심히 하고 싶은데 배울 곳이 없어 어려워하는 분들을 보았다. 간혹 준비가 덜 되었는데 현장에 내몰리면서 아우성 거리는 것 같아 안타까움도 많았다.

뭐든지 접해보는게 가장 큰 공부라는 것에 동의하지만, 현실을 견디지 못하고 또는 다양한 이유로 몇 달도 안 돼 이직해 버리는 엔지니어들을 보았다. 열심히 노력해서 실력자로 성장한 엔지니어를 만날 땐 부럽기도 했었다. 본의 아니게 숱한 사람을 만나게 되면서 뭔가 도움을 줄 수 있는 활동을 했으면 하는 나름의 목표를 마음에 품게 되었다.

책을 쓰고 지식을 공유한다는 건 한없이 행복하지만, 언제나 필자가 아는게 전부가 아니기 때문에 두려운 마음이 앞선다. 용기를 내어 조심스럽게 처음 전문업체에서 시작했던 모의해킹 분야부터 첫 서적 출간에 도전한다. 본 서적은 대부분 인터넷에 공개되어 있는 내용이지만, 필자의 경험을 최대한 가미하고 사례별 핵심과 노하우를 접목시켜 실무에 유용한 내용으로 재구성하였다. 이 서적이 모의해킹 전문가를 꿈꾸는 독자에게 조금이라도 도움이 된다면 저자의 보람이 될 것이다.

아쉽게도 출판은 쉽지가 않았다. 이곳저곳 문을 두드려 봤지만, 초급자용 웹 해킹 서적으로 평가하여 시장성이 없다고 고배를 마셨다. 하지만, 주변 지인의 조언과 여러 상황을 고려하여 출판 분야에 전문성은 없지만 출판업을 등록하여 출간을 하게 되었다.

전문 에디터, 디자이너는 없지만 원고부터 책 디자인 구성까지 모두 저자 혼자 감당하고 해결해야하니 유수한 출판 업체의 인쇄물에 비해 품질은 뒤떨어지나 내용면에선 알차게 구성했다고 단언하고 싶다.

본 서적의 부족한 면과 개선사항 등 다양한 의견을 저자에게 개진해 준다면 기쁜 마음으로 더욱 발전하는 밑거름으로 삼을 것이다.

마지막으로 책 출간까지 많은 격려와 도움을 준 가족과 오픈시큐어랩 카페 회원 및 수강생들 그리고 도움주신 이전 직장의 지인들께 감사를 드린다.

2017 년 10 월
오픈시큐어랩 대표
유현수

보안윤리

정보보안 분야를 다루면서 빼놓을 수 없는게 보안윤리이다. 해킹 기술은 양날의 검처럼 어떻게 쓰이는지에 따라서 화이트 해커가 될 수 있고 크래커인 범죄자가 될 수 있다.

정보통신윤리위원회가 2000 년 6 월 15 일에 발표한 "네티즌 윤리강령"을 통해서 인터넷을 이용하는 사람들의 기본 정신과 행동 강령을 정했다. 해당 내용을 제고하면서 보안 발전에 기여하는 전문인력으로 성장하기를 바란다.

네티즌 행동 강령

- 우리는 타인의 인권과 사생활을 존중하며 보호한다.
- 우리는 건전한 정보를 제공하고 올바르게 사용한다.
- 우리는 불건전한 정보를 배격하며 유포하지 않는다.
- 우리는 **타인의 정보를 보호하며 자신의 정보도 철저히 관리한다.**
- 우리는 비속어나 욕설 사용을 자제하고 바른 언어를 사용한다.
- 우리는 실명으로 활동하며 자신의 ID 로 행한 행동에 책임을 진다.
- 우리는 **바이러스 유포, 해킹 등 불법적인 행동을 하지 않는다.**
- 우리는 타인의 지적 재산권을 보호하고 존중한다.
- 우리는 사이버 공간에 대한 자율적 감시와 비판 활동에 적극 참여한다.
- 우리는 네티즌 윤리 강령 실천을 통하여 건전한 네티즌 문화를 조성한다

목차

Chapter 1

취약점 개요 및 실습 환경 구축

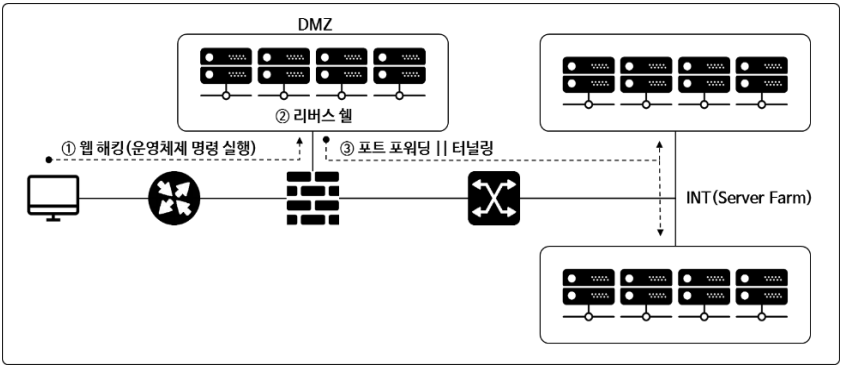
웹 해킹 공격에서 서버 침투에 가장 필수적인 운영체제 명령 실행은 현실적으로 가장 많이 발생하는 웹쉘WebShell을 이용한 공격이 대부분이라고 할 수 있다. 이 장에서는 서버 침투에 필요한 웹쉘과 학습에 필요한 실습 환경 구축 방법을 설명한다.

실습 환경 구축의 예시 그림은 지면의 제약으로 편집된 그림을 사용한다.

1.1. 서버 침투 개요

서버 침투는 웹 해킹 Web Hacking 을 통해서 서버에 침투가 가능한 공격으로 웹 애플리케이션의 취약점을 이용하여 운영체제의 접근권한 획득 및 내부망 침투가 가능한 공격 기법을 총칭해서 표현한 의미이다.

일반적인 웹 서비스 환경의 인프라 구성도를 이용하여 서버 침투에 필요한 공격 기법 및 절차를 알아보면 다음과 같이 3 단계로 구분할 수 있다.



웹 해킹을 통해 서버에 침투가 가능한 공격 기술을 단계별로 알아보면, ①운영체제 명령 실행이 가능한 웹 해킹 기법, ②대화형 운영체제의 명령 실행이 가능한 리버스 쉘 Reverse Shell 기법, ③방화벽 등 보안장비를 우회하여 내부의 서비스에 접속이 가능한 포트 포워딩 Port Forwarding 및 터널링 Tunneling 기법 등이다. 이러한 기술을 이용하여 내부망까지 침투가 가능하다.

본 서적은 각 단계별로 필요한 공격 기법을 순서대로 학습할 수 있도록 구성하였다.

공격 기법	설명
Track1 웹 해킹	공개용 웹 서비스의 취약점을 통해 운영체제 명령 실행
Track2 리버스 쉘	웹 서버의 대화형 Interactive 쉘 획득
Track3 포트 포워딩 & 터널링	방화벽 및 보안장비의 네트워크 접근 통제 우회
Track4 웹쉘 탐지	웹쉘 탐지 솔루션 소개 및 활용방안

세부 내용을 학습하기 전에 트랙 Track 별로 간략하게 요약하면 다음과 같은 내용으로 구성되어 있다.

Track1. 웹 서버 접근권한 획득

웹 해킹을 통해서 운영체제 명령 실행이 가능한 대표적인 취약점으로 파일 업로드 Unrestricted File Upload 와 운영체제 명령 실행 OS Command Injection 이 있다. 이 외에도 운영체제 명령 실행이 가능한 취약점은 다양하지만 본 서적에서는 아래의 취약점 위주로 기술되어 있다.

취약점	취약점 설명
파일 업로드	악성 웹 애플리케이션을 업로드 하여 웹 서버 조작
불필요한 METHOD	PUT METHOD 를 이용한 파일 업로드
DB 관리자	phpMyAdmin 등을 이용한 파일 업로드
WAS 관리자	Tomcat Application Manager 를 이용한 파일 업로드
불필요한 서비스	외부에 공개된 FTP 서비스를 이용한 파일 업로드
File Include Inclusion	악성 파일 삽입이 가능한 취약점
운영체제 명령 실행	시스템 명령 실행이 가능한 취약점

운영체제 명령 실행을 제외한 대부분의 취약점은 명령 실행 기능이 포함된 악의적인 파일을 업로드하는 방식으로 공격이 진행된다.

Track1 에서는 웹 서버 탈취에 필수적인 운영체제 명령 실행이 구현된 웹쉘 파일을 이용한 공격기법으로 파일 업로드 취약점의 다양한 사례를 실습하면서 취약점의 원리를 이해 할 수 있도록 구성되어 있다.

Track2. 웹 서버의 쉘 획득 기법

웹쉘을 이용한 운영체제 명령 실행은 비대화형 Non-Interactive 으로 대화형 Interactive 쉘 획득이 가능한 리버스 쉘 Reverse Shell 의 다양한 기법을 학습한다. 비대화형 및 대화형 쉘의 차이점은 Track2 에서 알아본다.

Track3. 주변 및 내부 서버 침투 기법

리버스 쉘 기법을 이용하여 웹 서버를 장악 하여도, 방화벽 등 보안장비의 접근 통제로 주변 서버 및 내부망 침투에는 제약이 있다. 방화벽을 우회하여 내부망 침투에 필요한 포트 포워딩 Port Forwarding 및 터널링 Tunneling 기법에 대해서 모의해킹 프로젝트에서 활용성이 높은 기법 위주로 학습한다.

Track4. 웹쉘(WebShell) 탐지 기법

웹 서버 침투 및 장악에 가장 많이 사용되는 웹쉘의 피해를 최소화 하기 위해서 신속한 탐지가 매우 중요하다고 할 수 있다. Track4 에서는 침해사고 분석 및 컨설팅 등에서 용이하게 웹쉘을 탐지할 수 있는 방법으로 Grep 등의 리눅스 기본 명령어와 오픈소스 웹쉘 스캐너 Scanner 를 활용한 탐지 기법을 학습한다.

모의해킹 컨설팅에서는 장악한 시스템에 각종 해킹 툴 설치 및 시스템 설정 변경은 장애 가능성이 있어 가급적 지양하고 있다. 본 서적의 모든 학습은 서버의 설정 변경을 최소화하는 범위 내에서 구현이 가능한 기술 위주로 구성되어 있다.