

<http://ohdae.github.io/Intersect-2.5/#Intro>
<http://obscuresecurity.blogspot.co.uk/2013/03/powersploit-metasploit-shells.html>
<http://dev.kryo.se/iodine/wiki/HowtoSetup>
<http://proxychains.sourceforge.net/>
[http://man.cx/ptunnel\(8\)](http://man.cx/ptunnel(8))
<http://www.sumitgupta.net/pwnat-example/>
<https://github.com/>
<http://www.dest-unreach.org/socat/doc/README>
<https://bechtsoudis.com/webacoo/>
<http://inundator.sourceforge.net/>
<http://vinetto.sourceforge.net/>
<http://www.elithecomputerguy.com/classes/hacking/>

F. 백트랙에 메타스플로잇을 업데이트할 때의 문제 해결

메타스플로잇을 최신 버전으로 업데이트하기 위해 `msfupdate` 명령어를 입력하는데, 진행 도중에 `root` 아이디와 패스워드를 요구하는 문제가 발생한다. 이것은 기존 업데이트 서버의 이전에도 발생했으며, 제품에 대한 유료화로 인해 발생한다. 메타스플로잇 프레임워크를 업데이트하려면 현재 사이트에 올라와 있는 메타스플로잇을 다시 설치해야 한다. 그림 F-1은 `msfupdate`를 실행할 때 발생하는 메시지다(버전 4.5.0에서 상위 버전으로 업데이트가 안 되는 현상).

그림 F-1과 같은 예러가 나타나면 `p`를 눌렀을 때 `root` 계정과 `password`, `username`을 요구하며 업데이트가 되지 않는다.

```

o O
o
AAAAAAAAAAAAAAAA
PAYLOAD
**
)====(
LOOT
(
)
)====(

+-----+

[ netasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --[ 927 exploits - 499 auxiliary - 151 post
+ -- --[ 251 payloads - 28 encoders - 8 nops

msf > msfupdate
[*] exec: msfupdate

[*]
[*] Attempting to update the Metasploit Framework...
[*]

Updating '.':
Error validating server certificate for 'https://www.netasploit.com:443':
- The certificate is not issued by a trusted authority. Use the
  fingerprint to validate the certificate manually!
Certificate information:
- Hostname: www.netasploit.com
- Valid: from Fri, 05 Apr 2013 00:00:00 GMT until Sun, 05 Apr 2015 23:59:59 GMT
- Issuer: Terms of use at https://www.verisign.com/rpa (c)06, VeriSign Trust Network, VeriSign, Inc., US
- Fingerprint: ec:fc:40:64:e6:8b:58:84:27:5b:d5:aa:a3:d1:10:27:e1:0d:c3:d9
[Reject, accept (t)emporarily or accept (p)ermanently? ]

```

그림 F-1 메타스플로잇을 업데이트할 때 에러 발생

업데이트 문제를 해결하려면 다음 절차를 따르기 바란다. 결론부터 말하면 github, svn의 문제로 인해 메타스플로잇을 삭제한 후 다시 설치해줘야 한다.

먼저 그림 F-2와 같이 메타스플로잇을 삭제한다.

```

root@bt:~# apt-get remove metasploit
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libcryptfs0 libdmraid1.0.0.rc16 libdebconfclient0 ecryptfs-utils cryptsetup
  rdate bogl-bterm libdebiana-installer4 ettercap-relserfsprogs dmraid
  python-pyicu
Use 'apt-get autoremove' to remove them
The following packages will be REMOVED:
  easy-creds jboss-autopwn metasploit
0 upgraded, 0 newly installed, 3 to remove and 0 not upgraded.
After this operation, 0B of additional disk space will be used.
Do you want to continue [Y/n]? y
(Reading database ... 269221 files and directories currently installed.)
Removing easy-creds ...
Removing jboss-autopwn ...
Removing metasploit ...
/opt/metasploit/postgresql/scripts/ctl.sh : postgresql stopped
Processing triggers for desktop-file-utils ...
Processing triggers for python-gmenu ...
Rebuilding /usr/share/applications/desktop.en_US.utf8.cache...
Processing triggers for ureadahead ...
Processing triggers for python-support ...

```

그림 F-2 메타스플로잇의 삭제

메타스플로잇을 삭제한 후에는 다음과 같은 wget 명령을 이용해 메타스플로잇 설치metasploit install 파일을 다운로드한다.

```
root@bt:~# wget http://downloads.metasploit.com/data/releases/metasploit-latest-linux-installer.run
```



```
root@bt:~# wget http://downloads.metasploit.com/data/releases/metasploit-latest-linux-installer.run
--2013-07-16 18:54:30-- http://downloads.metasploit.com/data/releases/metasploit-latest-linux-installer.run
Resolving downloads.metasploit.com [173.223.227.50]:173.223.227.50.
Connecting to downloads.metasploit.com [173.223.227.50]:80.
connected.
HTTP request sent, awaiting response... 200 OK
Length: 172903992 (165M) [text/plain]
Saving to: `metasploit-latest-linux-installer.run'

100%[=====>] 172,903,992 940K/s in 2m 39s

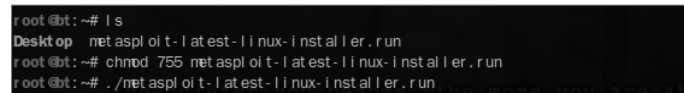
2013-07-16 18:57:11 (1.03 MB/s) - `metasploit-latest-linux-installer.run' saved
[172903992/172903992]

root@bt:~#
```

그림 F-3 메타스플로잇 최신 버전 다운로드

다운로드한 파일에 권한을 부여한 후 설치한다.

```
root@bt:~# chmod 755 metasploit-latest-linux-installer.run
root@bt:~# ./metasploit-latest-linux-installer.run
```



```
root@bt:~# ls
Desktop metasploit-latest-linux-installer.run
root@bt:~# chmod 755 metasploit-latest-linux-installer.run
root@bt:~# ./metasploit-latest-linux-installer.run
```

그림 F-4 다운로드한 파일에 권한 부여

그림 F-5와 같이 메타스플로잇 설치 화면에서 차례로 Next를 클릭해 마지막까지 설치한다.

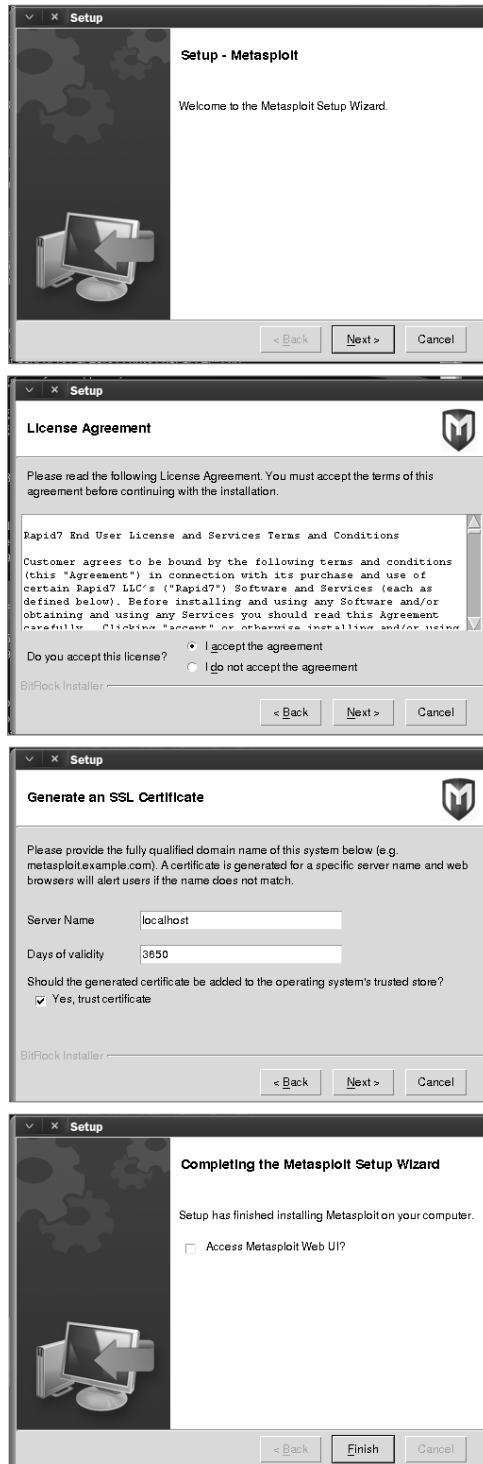


그림 F-5 메타스플로잇 설치 화면

그림 F-6처럼 Application > Internet > Firefox Web Browser를 차례로 선택한다. 파이어폭스 브라우저가 나타나면 URL 입력란에 localhost:3790을 입력하고 접속한다.

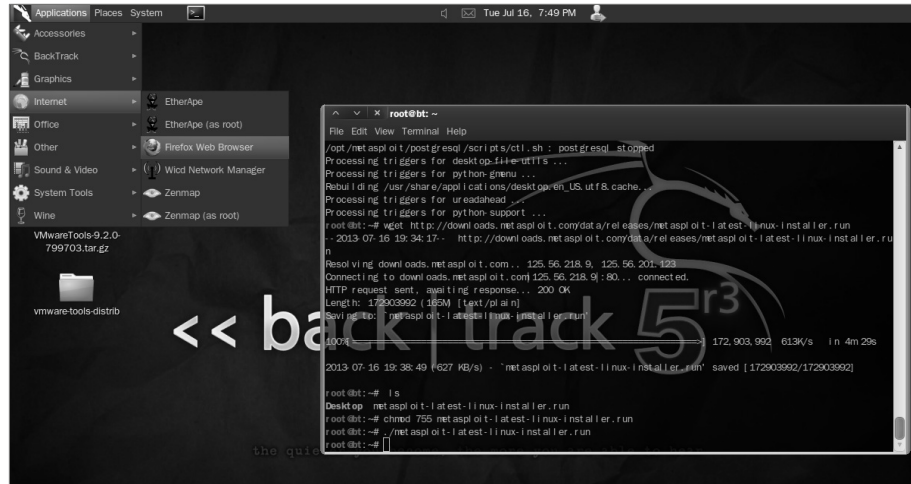


그림 F-6 웹 브라우저 실행하기

웹브라우저에 그림 F-17과 같은 설정 페이지가 나타난다. I understand the Risks를 클릭하고, 그런 후 아래쪽에 있는 Add Exception... 버튼을 클릭한다.

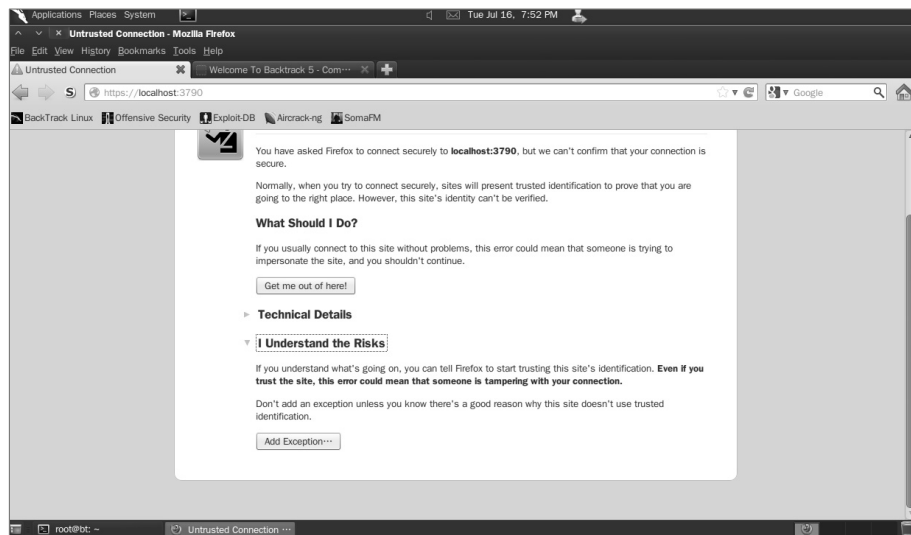


그림 F-7 URL 정보 예외 처리하기(1)

그림 F-8과 같이 기본 설정을 그대로 두고 하단에 있는 Confirm Security Exception 버튼을 클릭한다.



그림 F-8 URL 정보 예외 처리하기(2)

그림 F-9와 같은 화면이 나타난다.

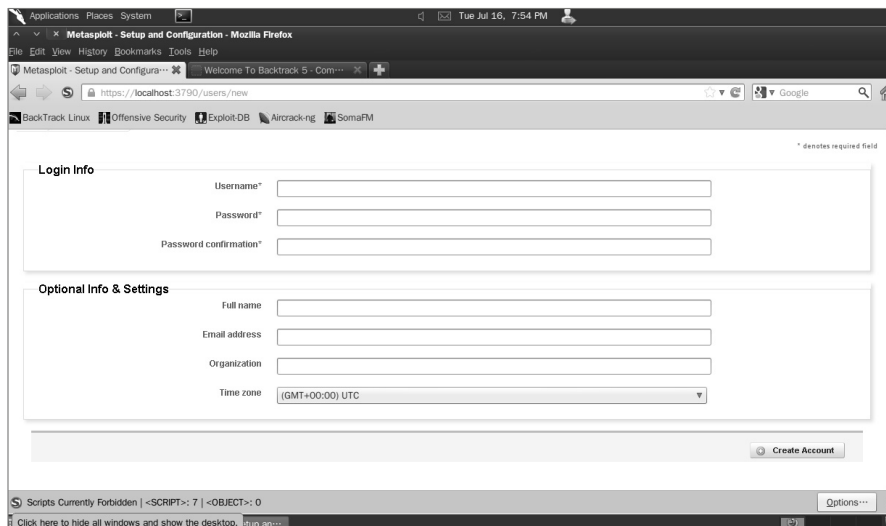


그림 F-9 계정 정보 생성

사용자 이름 username, 패스워드 password, 패스워드 확인 password confirmation 등의 정보를 입력한 후 타임 존 time zone을 설정하고 Create Account 버튼을 클릭한다.
그림 F-10과 같은 화면에서 GET PRODUCT KEY 버튼을 클릭한다.

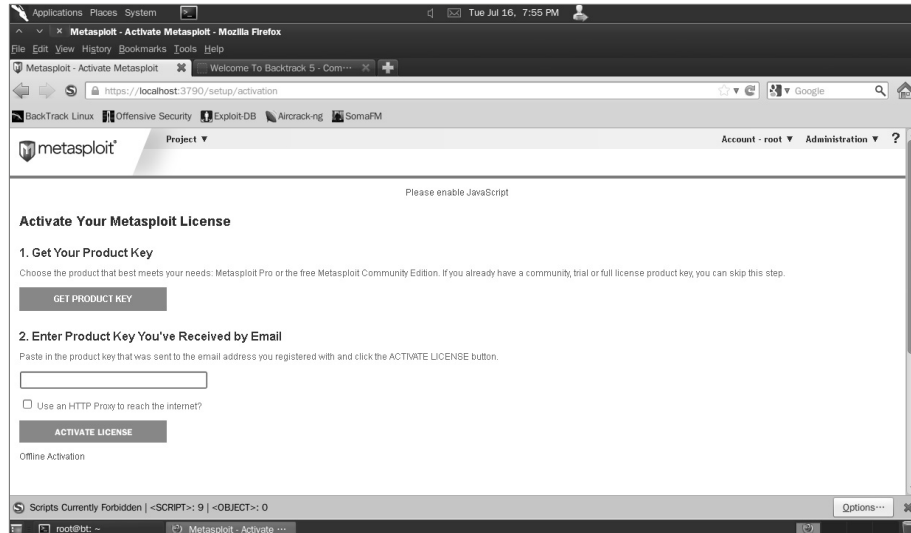


그림 F-10 제품 키 발급

그림 F-11과 같은 화면에서 GET COMMUNITY EDITION 버튼을 클릭한다.

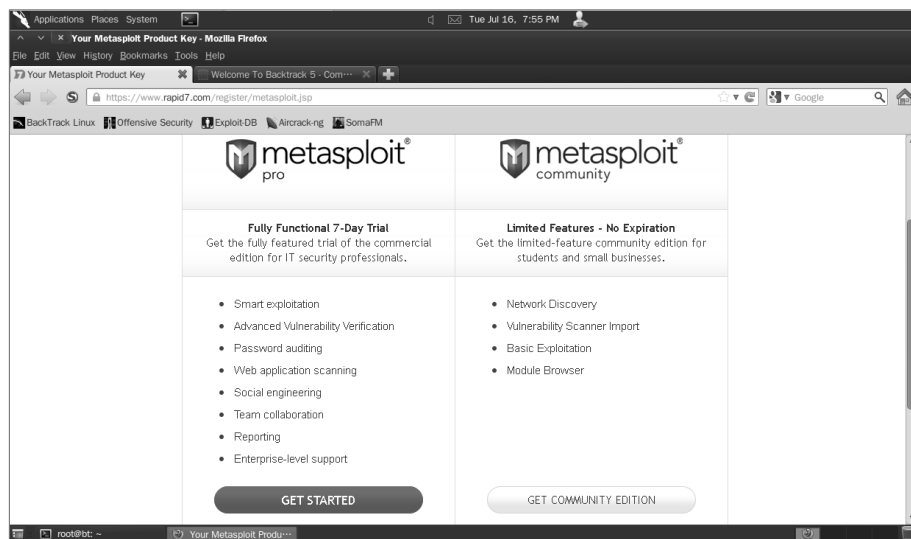


그림 F-11 Community 버전 다운로드

그림 F-12와 같은 화면에서 * 표시가 있는 부분을 입력하면 이메일로 제품 키 Product Key를 수신할 수 있고, 받은 제품 키를 Active Your Metasploit License 창에 두 번 입력한 후 Active License를 클릭한다.

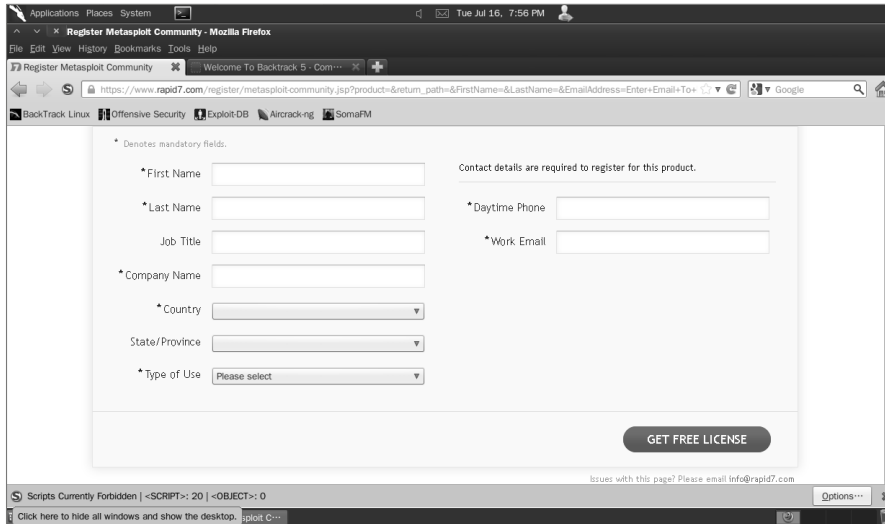


그림 F-12 Community 버전 라이선스 받기

‘Activation Successful’이라는 알림과 함께 그림 F-13과 같은 새로운 화면이 나타난다. 브라우저 상단의 메뉴에서 Tools > Add-ons를 클릭한다.

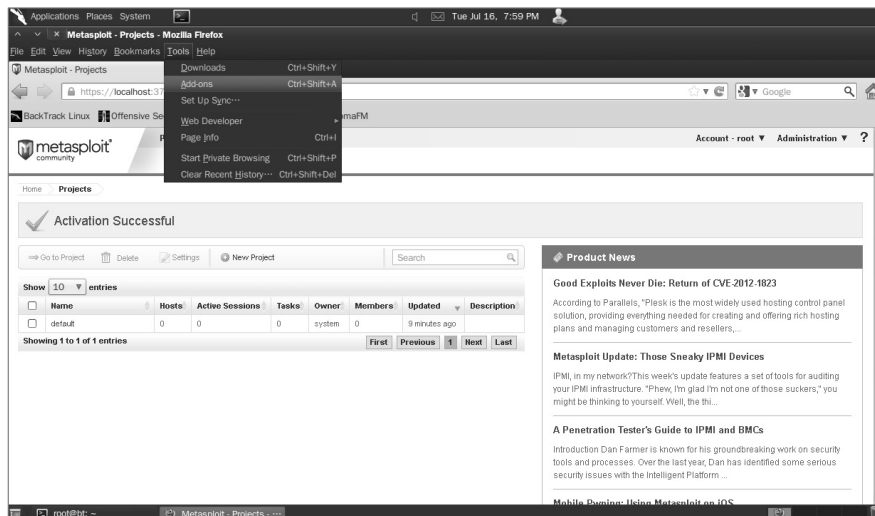


그림 F-13 브라우저 상단의 애드온 클릭

그림 F-14와 같은 화면이 나타나면 NoScript 2.3 부분의 오른쪽에 있는 Enable 버튼을 클릭한다.

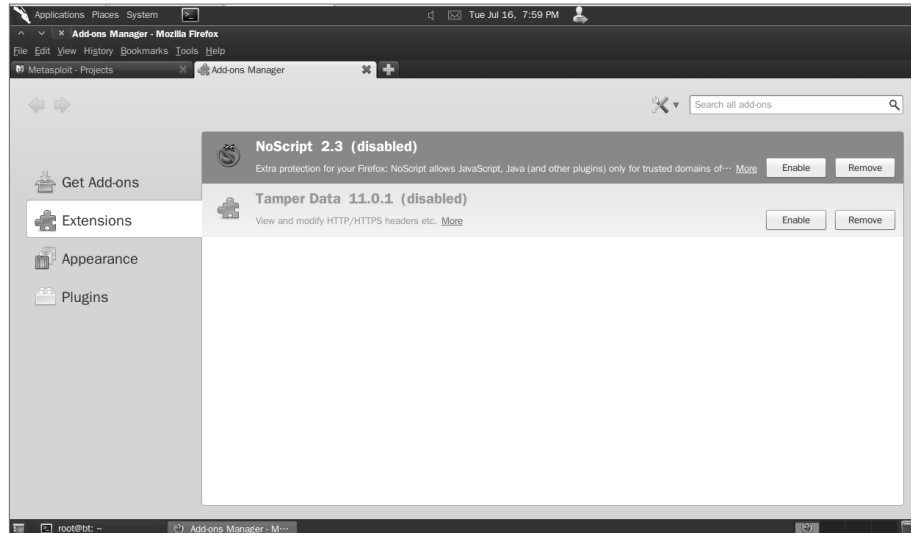


그림 F-14 브라우저 상단의 애드온 클릭 후의 화면

브라우저 창 종료 후 그림 F-15와 같이 콘솔 창에 msfconsole을 입력한다.

```
root @bt:~# msfconsole
```



그림 F-15 msfupdate 진행

이제 v4.6.2-1로 업데이트됐다. 그림 F-15의 하단처럼 msfupdate를 입력해 보자.

```
root@bt:~# msfupdate
```

그림 F-16과 같이 정상적으로 업데이트가 진행되는 것을 볼 수 있다. 이후에는 msfupdate를 입력하면 최신 업데이트 모듈과 공격 코드를 쉽게 유지할 수 있다.



그림 F-16 msfupdate의 진행 확인

G. SET 업데이트 문제 해결

백트랙을 기본 설치로 운영을 할 때에는 SET 패키지를 업그레이드할 경우 에러가 발생한다. 이런 문제를 해결하는 방법에는 저장소 주소를 수정해 업데이트하거나 신규로 다운로드해 설치하는 두 가지 방식이 있다.

저장소 주소의 수정

다음과 같이 se-toolkit.postinst 파일을 수정한 후 apt-get update, apt-get upgrade를 실행하면 자동으로 업데이트가 진행된다.

```
root@bt:~# vi /var/lib/dpkg/info/se-toolkit.postinst
```