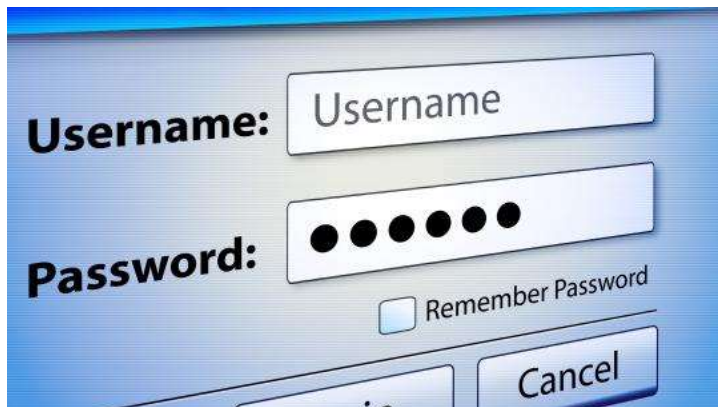


Lab 3. Password Cracking / Putty

Password Cracking

Password Cracking ?



```
c:\gsauditor> gsauditor -set:?d -binary -append -salt:6e4ca656fc53f356293c 613d9cfc0f751520ad6a28c7bef5cd4ea2179437

GSAuditor, v0.3 (Nov 26 2008), (c) EvilFingers.com
*****

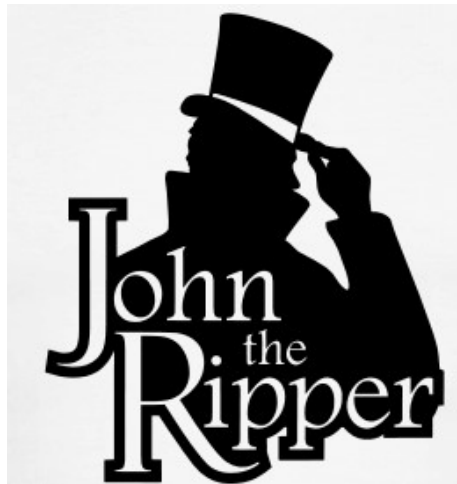
Ansi passwords will be created
Will use "0123456789" as alphabet
Starting with "0"
Ending with "99999999"
Hash to find is "613d9cfc0f751520ad6a28c7bef5cd4ea2179437"
The salt is "6e4ca656fc53f356293c" and will be appended in binary format

Press CTRL+C for current statistics (twice quick to terminate)

Password was not found. - last try was "99999999"
Seconds elapsed:18 k/s: 6172839
```

실습 사용 tool

- John the ripper
 - 간단히 암호화 된 password 를 알아낼 수 있는 tool
 - 윈도우/리눅스 버전 지원



```
C:\WINDOWS\system32\cmd.exe
John the Ripper password cracker, version 1.7.0.1
Copyright (c) 1996-2006 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john-mmx [OPTIONS] [PASSWORD-FILES]
--single                "single crack" mode
--wordlist=FILE --stdin wordlist mode, read words from FILE or stdin
--rules                enable word mangling rules for wordlist mode
--incremental[=MODE]   "incremental" mode using section MODE
--external=MODE        external mode or word filter
--stdout[=LENGTH]     just output candidate passwords [cut at LENGTH]
--restore[=NAME]       restore an interrupted session [called NAME]
--session=NAME         give a new session the NAME
--status[=NAME]        print status of a session [called NAME]
--make-charset=FILE    make a charset, FILE will be overwritten
--show                 show cracked passwords
--test                 perform a benchmark
--users=[-ILOGIN|UID[,...]] Do not load this <these> user(s) only
--groups=[-IGID[,...]]     load users [not] of this <these> group(s) only
--shells=[-ISHELL[,...]]  load users with[out] this <these> shell(s) only
--salts=[-ICOUNT]         load salts with[out] at least COUNT passwords only
--format=NAME           force ciphertext format NAME: DES/BSDI/MD5/BF/AFS/LM
--save-memory=LEVEL     enable memory saving, at LEVEL 1..3

G:\john-16\run>
```

John the ripper 설치

- <http://www.openwall.com/john/>

John the Ripper is free and Open Source software, distributed primarily in source code form. If you would rather use a commercial product tailored for your specific operating system, please consider [John the Ripper Pro](#), which is distributed primarily in the form of "native" packages for the target operating systems and in general is meant to be easier to install and use while delivering optimal performance.

Proceed to **John the Ripper Pro** homepage for your OS:

- [John the Ripper Pro for Linux](#)
- [John the Ripper Pro for Mac OS X](#)
- **On Windows, consider Hash Suite** (developed by a contributor to John the Ripper)
- On Android, consider [Hash Suite Droid](#)

Download the latest John the Ripper jumbo release ([release notes](#)) or development snapshot:

- 1.9.0-jumbo-1 sources in [tar.xz, 33 MB \(signature\)](#) or [tar.gz, 43 MB \(signature\)](#)
- **1.9.0-jumbo-1 64-bit Windows binaries in 7z, 22 MB (signature) or zip, 63 MB (signature)**
- **1.9.0-jumbo-1 32-bit Windows binaries in 7z, 21 MB (signature) or zip, 61 MB (signature)**
- Development source code in [GitHub repository](#) (download as [tar.gz](#) or [zip](#))

Download the latest John the Ripper core release ([release notes](#)):

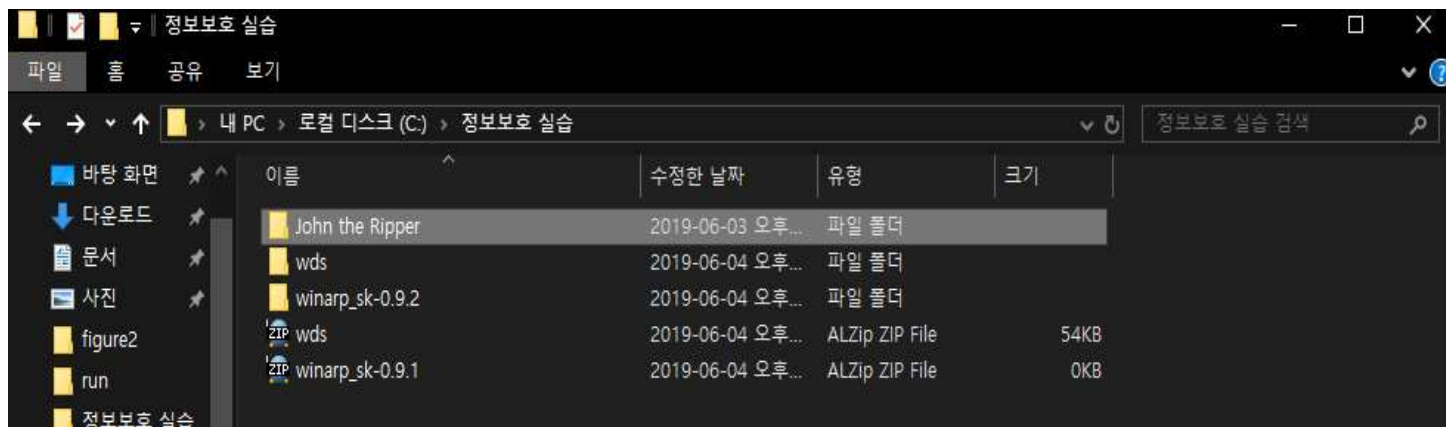
- 1.9.0 core sources in [tar.xz, 8.6 MB \(signature\)](#) or [tar.gz, 13 MB \(signature\)](#)
- Development source code in [CVS repository](#)

Get John the Ripper apparel at 0-Day Clothing and support the project



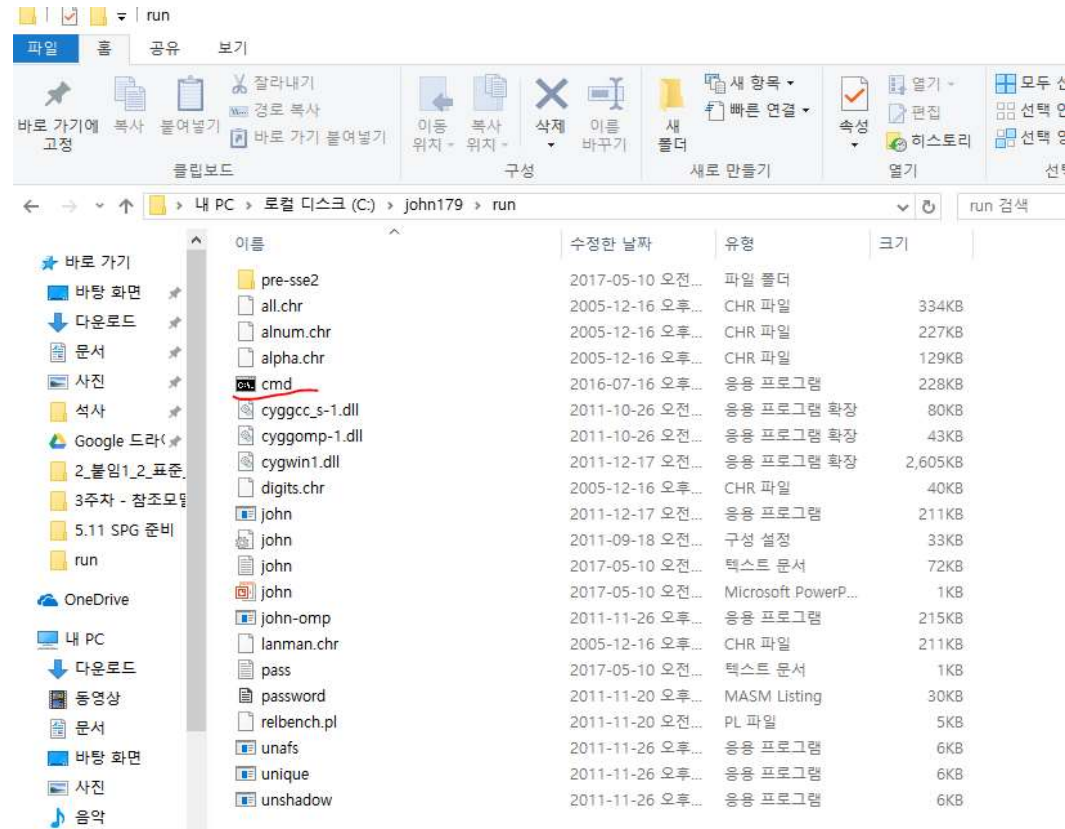
John the ripper 사용

- 압축 해제



John the ripper 사용

- JohnWrun 폴더 내 CMD 복사



Password 파일 생성

- sherylcanter.com/encrypt.php

Username:Password Creator for HTPASSWD

Use this form to create a username:password entry for an .htpasswd file.

Username:	<input type="text"/>	
Password:	<input type="password"/>	
DES Salt:	<input type="text"/>	(optional, see below)
MD5 Salt:	<input type="text"/>	(optional, see below)

- Valid salt characters are a-z, A-Z, 0-9, the period '.', and the forward slash '/'.
- For DES, the salt is 2 random characters from the set of valid characters.
- The MD5 salt is 12 characters, only 8 of which are random. The MD5 salt always starts with '\$1\$' and ends with '\$'.

The salt is always at the beginning of the password portion of the username:password entry. If you use the same salt, you'll get the same result. This is how passwords are validated since the hashes can't be reversed.

[Create another entry](#)

[Home](#)

[Blog](#)

[Close](#)



Password 파일 생성

- sherylcanter.com/encrypt.php

Username:Password Creator for HTPASSWD

DES-encrypted username:password entry:

test user :QyLcp0fqDwh1g

md5-encrypted username:password entry:

test user :\$1\$vR6yPgm\$c89dFkh i0cDj f0XKh iLVd.

[Create another entry](#)


[Home](#)

[Blog](#)

[Close](#)

Password 파일 생성

- Txt 파일로 생성 후 저장



pass - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
test user:QyLcp0fqCwhlg

Password Cracking 실행

- Cmd - john

```
C:\john179\run#cmd.exe
C:\john179\run>john
0 [main] john 10804 find_fast_cwd: WARNING: Couldn't compute FAST_CWD pointer. Please report this problem
the public mailing list cygwin@cygwin.com
John the Ripper password cracker, version 1.7.9
Copyright (c) 1996-2011 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single                "single crack" mode
--wordlist=FILE --stdin  wordlist mode, read words from FILE or stdin
--rules                 enable word mangling rules for wordlist mode
--incremental[=MODE]    "incremental" mode [using section MODE]
--external=MODE         external mode or word filter
--stdout[=LENGTH]      just output candidate passwords [cut at LENGTH]
--restore[=NAME]        restore an interrupted session [called NAME]
--session=NAME          give a new session the NAME
--status[=NAME]         print status of a session [called NAME]
--make-charset=FILE     make a charset, FILE will be overwritten
--show                  show cracked passwords
--test[=TIME]           run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]    load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..] load users with[out] this (these) shell(s) only
--salts=[-]COUNT       load salts with[out] at least COUNT passwords only
--save-memory=LEVEL     enable memory saving, at LEVEL 1..3
--format=NAME           force hash type NAME: des/bsdi/md5/bf/afs/lm/trip/
                        dummy
```

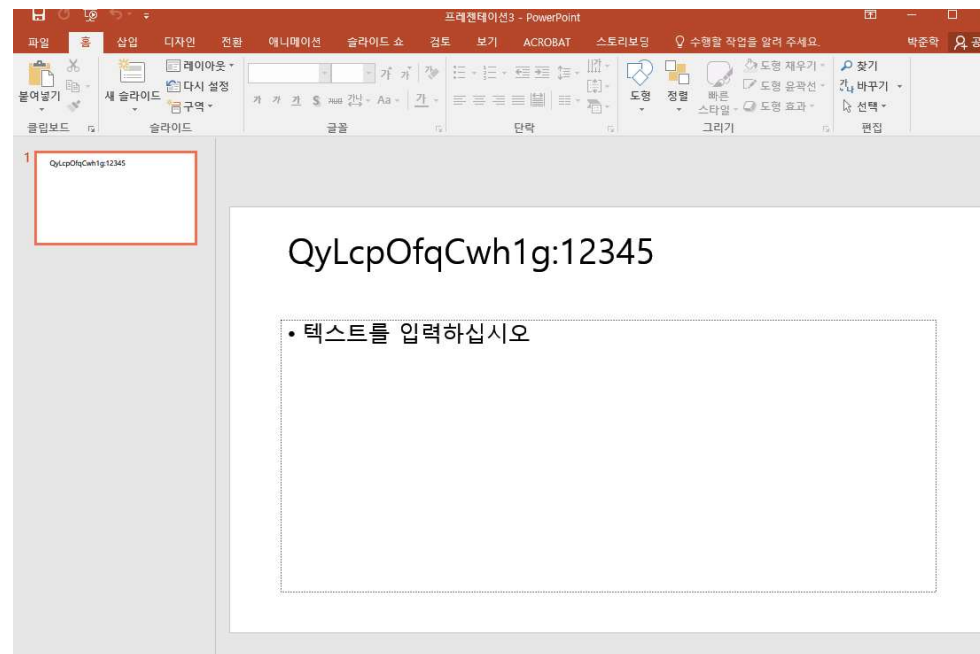
Password Cracking 실행

- Cmd – john 파일명
- 계정/패스워드 일치 확인

```
C:\john179\run>john pass.txt
0 [main] john 13584 find_fast_cwd: WARNING: Couldn't compute FAST_CWD pointer. Please report this problem to
the public mailing list cygwin@cygwin.com
Loaded 1 password hash (Traditional DES [128/128 BS SSE2])
12345 (test user)
guesses: 1 time: 0:00:00:00 100% (2) c/s: 407833 trying: 123456 - marley
Use the "--show" option to display all of the cracked passwords reliably
C:\john179\run>
```

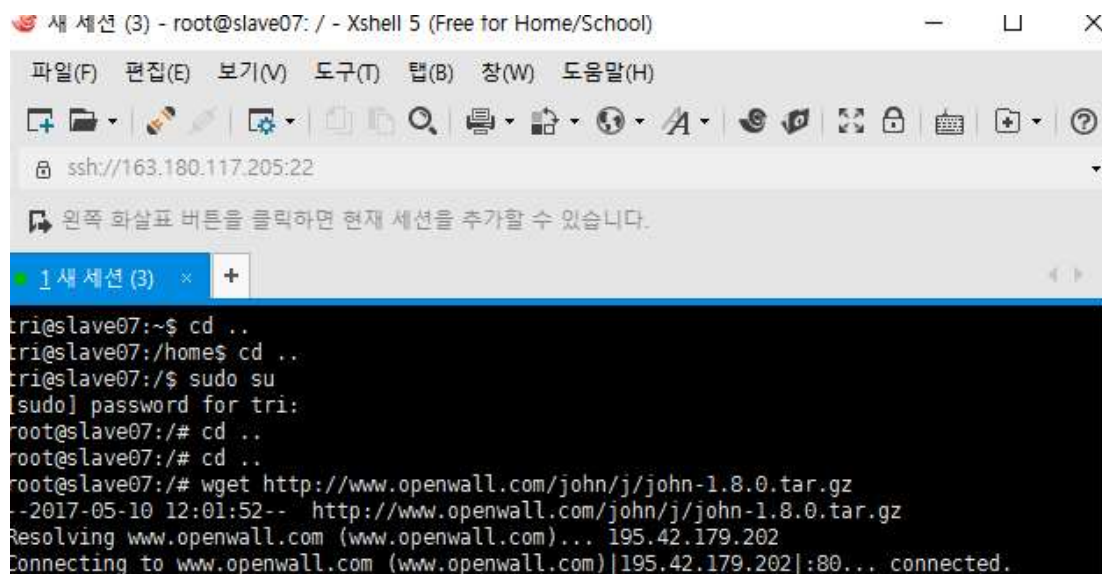
주의 사항

- 재 사용시 run 폴더에 john.pot 파일 삭제



John the ripper - Linux

- Apt-get install john
- wget <http://openwall.com/john/j/john-1.8.0.tar.gz>



The screenshot shows an Xshell terminal window with the following content:

```
새 세션 (3) - root@slave07: / - Xshell 5 (Free for Home/School)
파일(F) 편집(E) 보기(V) 도구(T) 탭(B) 창(W) 도움말(H)
ssh://163.180.117.205:22
왼쪽 화살표 버튼을 클릭하면 현재 세션을 추가할 수 있습니다.
1 새 세션 (3)
tri@slave07:~$ cd ..
tri@slave07:/home$ cd ..
tri@slave07:/$ sudo su
[sudo] password for tri:
root@slave07:/# cd ..
root@slave07:/# cd ..
root@slave07:/# wget http://www.openwall.com/john/j/john-1.8.0.tar.gz
--2017-05-10 12:01:52-- http://www.openwall.com/john/j/john-1.8.0.tar.gz
Resolving www.openwall.com (www.openwall.com)... 195.42.179.202
Connecting to www.openwall.com (www.openwall.com)|195.42.179.202|:80... connected.
```

John the ripper - Linux

- 압축 해제

```
root@slave07:/# tar zxvf john-1.8.0.tar.gz
john-1.8.0/README
john-1.8.0/doc/CHANGES
john-1.8.0/doc/CONFIG
john-1.8.0/doc/CONTACT
john-1.8.0/doc/COPYING
john-1.8.0/doc/CREDITS
john-1.8.0/doc/EXAMPLES
john-1.8.0/doc/EXTERNAL
john-1.8.0/doc/FAQ
john-1.8.0/doc/INSTALL
john-1.8.0/doc/LICENSE
```

John the ripper - Linux

- 디렉토리 이동 후 make
- cd john-1.8.0/src

```
sco-x86-any-gcc      SCO, x86, gcc
sco-x86-any-cc      SCO, x86, cc
tru64-alpha         Tru64 (Digital UNIX, OSF/1), Alpha
aix-ppc32           AIX, PowerPC 32-bit
macosx-x86-64       Mac OS X 10.5+, Xcode 3.0+, x86-64 with SSE2 (best)
macosx-x86-sse2     Mac OS X, x86 with SSE2
macosx-ppc32-altivec Mac OS X, PowerPC w/AltiVec (best)
macosx-ppc32        Mac OS X, PowerPC 32-bit
macosx-ppc64        Mac OS X 10.4+, PowerPC 64-bit
macosx-universal    Mac OS X, Universal Binary (x86 + x86-64 + PPC)
hpux-pa-risc-gcc    HP-UX, PA-RISC, gcc
hpux-pa-risc-cc     HP-UX, PA-RISC, ANSI cc
irix-mips64-r10k    IRIX, MIPS 64-bit (R10K) (best)
irix-mips64         IRIX, MIPS 64-bit
irix-mips32         IRIX, MIPS 32-bit
dos-djgpp-x86-mmx   DOS, DJGPP, x86 with MMX
dos-djgpp-x86-any   DOS, DJGPP, x86
win32-cygwin-x86-sse2 Win32, Cygwin, x86 with SSE2 (best)
win32-cygwin-x86-mmx Win32, Cygwin, x86 with MMX
win32-cygwin-x86-any Win32, Cygwin, x86
beos-x86-sse2       BeOS, x86 with SSE2 (best)
beos-x86-mmx        BeOS, x86 with MMX
beos-x86-any        BeOS, x86
generic             Any other Unix-like system with gcc
root@slave07:/john-1.8.0/src#
```


John the ripper - Linux

- Make clean SYSTEM 입력
 - 현재 리눅스 서버 시스템이 무엇인지 알려줌

```
root@slave07:/john-1.8.0/src# make clean SYSTEM
rm -f ../run/john ../run/unshadow ../run/unafs ../run/unique ../run/john.bin ../run/john
.com ../run/unshadow.com ../run/unafs.com ../run/unique.com ../run/john.exe ../run/unsha
dow.exe ../run/unafs.exe ../run/unique.exe
rm -f ../run/john.exe john-macosx-* *.o *.bak core
rm -f detect bench generic.h arch.h tmp.s
cp /dev/null Makefile.dep
make: *** No rule to make target `SYSTEM'. Stop.
root@slave07:/john-1.8.0/src#
```

John the ripper - Linux

- Make clean generic 입력
 - 서버 시스템 조사 후 맞게 설정
- Run 디렉토리로 이동
- ./john/etc/shadow 로 실행

```
# ./john -user:test /etc/shadow
Loaded 1 password hash (FreeBSD MD5 [32/32])
smile          (test)
guesses: 1  time: 0:00:00:01 100% (2)  c/s: 2536  trying: smile
```

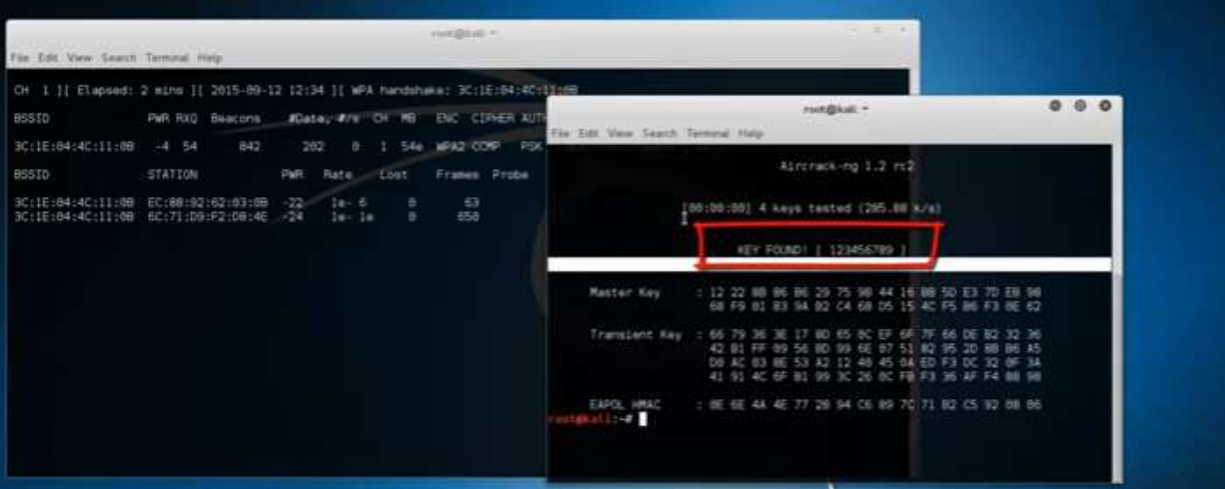
John the ripper - Linux

- Password.lst

```
#!comment: This list has been compiled  
#!comment: in 1996 through 2011. It is  
#!comment:  
#!comment: This list is based on passwo  
#!comment: systems in mid-1990's, sorte  
#!comment: (that is, more common passwo  
#!comment: revised to also include comm  
#!comment: of "top N passwords" from ma  
#!comment: occurred in 2006 through 201  
#!comment:  
#!comment: Last update: 2011/11/20 (354  
#!comment:  
#!comment: For more wordlists, see http  
123456  
12345  
password  
password1  
123456789  
12345678  
1234567890  
abc123  
computer  
tigger  
1234  
"password.lst" 3559L, 26325C
```

응용 시나리오

- Aircrack-ng 를 이용한 Wifi password 탈취
 - <https://cpuu.postype.com/post/55291/>
 - <http://itmir.tistory.com/387>
 - <https://www.youtube.com/watch?v=4DjyEnPH2bY>



```
File Edit View Search Terminal Help
root@kali: ~
CH 1 | Elapsed: 2 mins | 2015-09-12 12:34 | [ WPA handshake: 3C:1E:04:4C:11:0B ]
BSSID PWR RXQ Beacons #Data: #fr CH HB ENC CIPHER AUTH
3C:1E:04:4C:11:0B -4 54 842 202 0 1 54e WPA2 CCMP PSK
BSSID STATION PWR Rate Cost Frames Probe
3C:1E:04:4C:11:0B EC:88:92:02:03:0B -22 1e-6 0 0 0
3C:1E:04:4C:11:0B BC:71:D9:F2:08:4E -24 1e-1a 0 0 0

Aircrack-ng 1.2 rc2
[00:00:00] 4 keys tested (295.88 k/s)
KEY FOUND! ( 123456789 )

Master Key : 12 22 88 96 86 25 75 98 44 16 88 50 E3 70 EB 98
68 F9 81 83 94 82 C4 68 05 15 4C F5 86 F3 8E 62

Transient Key : 66 79 36 3E 17 80 65 9C EF 6F 7F 66 DE B2 32 36
42 81 FF 09 56 8D 99 6E 07 51 82 95 2D 88 86 A5
D9 AC 03 8E 53 A2 12 48 45 0A ED F3 DC 32 0F 3A
41 91 4C 6F 81 99 3C 26 0C F8 F3 36 AF F4 88 98

EAPOL HMAC : 8E 6E 4A 4E 77 28 94 C6 89 7C 71 82 C5 92 88 66
root@kali:~#
```

추가 정보

- 암호를 어렵게 만들어야 하는 이유
 - 숫자 + 영문 + 특수문자 : 12시간이 지나도 뚫지 못함

회원님의 소중한 개인정보를 안전하게 보호하기 위해
비밀번호 변경을 안내드립니다

이글루스는 2011년 9월 6일부터 비밀번호 변경안내 정책이 시행되고 있습니다.
비밀번호를 변경하신 지 6개월이 지난 경우에 아래와 같이 변경 안내를 드리고 있습니다.
[비밀번호 변경안내 정책 자세히 보기](#)

*다음에 변경하기 버튼을 눌러 변경을 연기하시면 3개월후 다시 안내해드립니다.
조금 불편하시더라도, **지금 비밀번호를 변경해주세요.**

현재 비밀번호

새 비밀번호

새 비밀번호 확인



Putty

Putty란?



- Raw TCP, SSH, Telnet, Rlogin 등의 방법으로 IP를 이용하여 원격접속 할 수 있는 프로그램.

Putty

- **Rlogin** : 명령은 TCP 포트 513를 통해 통신 사용자가 네트워크를 통해 다른 호스트에 로그인할 수 있도록 유닉스와 같은 컴퓨터 운영 체제를 위한 소프트웨어 유틸리티이다.
- **TCP** : 근거리 통신망이나 인트라넷, 인터넷에 연결된 컴퓨터에서 실행되는 프로그램 간에 일련의 옥텟을 안정적으로, 순서대로, 에러 없이 교환할 수 있게 한다.
- **텔넷(TELNET)** : 인터넷이나 로컬 영역 네트워크 연결에 쓰이는 네트워크 프로토콜이다. 텔넷의 보안 문제 때문에 사용률이 감소하여, 원격 제어를 위해 SSH로 대체되기도 하였다.
- **SSH(Secure Shell)** : 네트워크 상의 다른 컴퓨터에 로그인하거나 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해 주는 응용 프로그램 또는 그 프로토콜을 가리킨다. 기존의 rsh, rlogin, 텔넷 등을 대체하기 위해 설계되었으며, 강력한 인증 방법 및 안전하지 못한 네트워크에서 안전하게 통신을 할 수 있는 기능을 제공한다.

Putty 설치

- <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

Package files

You probably want one of these. They include versions of all the PuTTY utilities.

(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

MSI ('Windows Installer')

32-bit: [putty-0.71-installer.msi](#) [\(or by FTP\)](#) [\(signature\)](#)

64-bit: [putty-64bit-0.71-installer.msi](#) [\(or by FTP\)](#) [\(signature\)](#)

Unix source archive

.tar.gz: [putty-0.71.tar.gz](#) [\(or by FTP\)](#) [\(signature\)](#)

Alternative binary files

The installer packages above will provide versions of all of these (except PuTTYtel), but you can download standalone binaries one by one if you prefer.

(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

putty.exe (the SSH and Telnet client itself)

32-bit: [putty.exe](#) [\(or by FTP\)](#) [\(signature\)](#)

64-bit: [putty.exe](#) [\(or by FTP\)](#) [\(signature\)](#)

pscp.exe (an SCP client, i.e. command-line secure file copy)

32-bit: [pscp.exe](#) [\(or by FTP\)](#) [\(signature\)](#)

64-bit: [pscp.exe](#) [\(or by FTP\)](#) [\(signature\)](#)

psftp.exe (an SFTP client, i.e. general file transfer sessions much like FTP)

32-bit: [psftp.exe](#) [\(or by FTP\)](#) [\(signature\)](#)

64-bit: [psftp.exe](#) [\(or by FTP\)](#) [\(signature\)](#)

HTTP

SuperScan 3.00

Hostname Lookup: 163.180.116.60
Resolved: SEC30CDA7B71AD9

IP: Start 163.180.116.1, Stop 163.180.116.254

Timeout: Ping 400, Connect 2000, Read 4000

Scan type: Resolve hostnames, Only scan responsive pings, Show host responses, Ping only, Every port in list, All selected ports in list, All list ports from 1 to 65535, All ports from 1 to 65535

Scan results:

Service	Port	Count
Pinging	-Q-	0
163.180.116.254	0	0
Scanning	-Q-	0
163.180.116.252	0	0
Resolving	-Q-	0

Speed: Max, Min

Active hosts: 107, Open ports: 36

Scan results list:

- 163.180.116.40
- 163.180.116.44
- 163.180.116.53
- 163.180.116.55
- 163.180.116.60 # 80 WorldWide Web HTTP
- 163.180.116.61
- 163.180.116.65
- 163.180.116.66

PuTTY Configuration

Category: Session, Terminal, Window, Connection

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 163.180.116.60, Port: 80

Connection type: Raw, Telnet, Rlogin, SSH, Serial

Load, save or delete a stored session

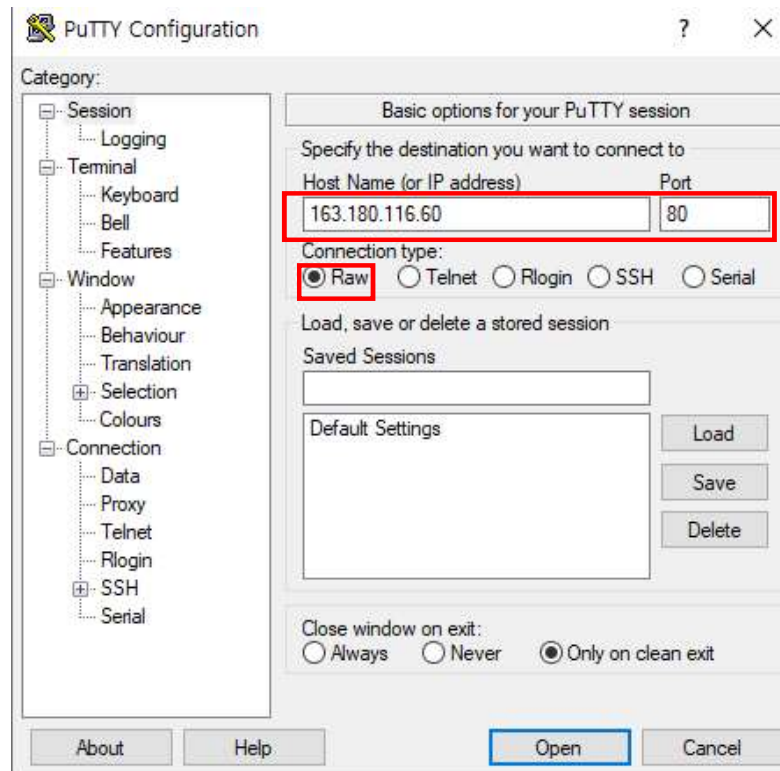
Saved Sessions: [Empty list]

Default Settings: [Empty text box]

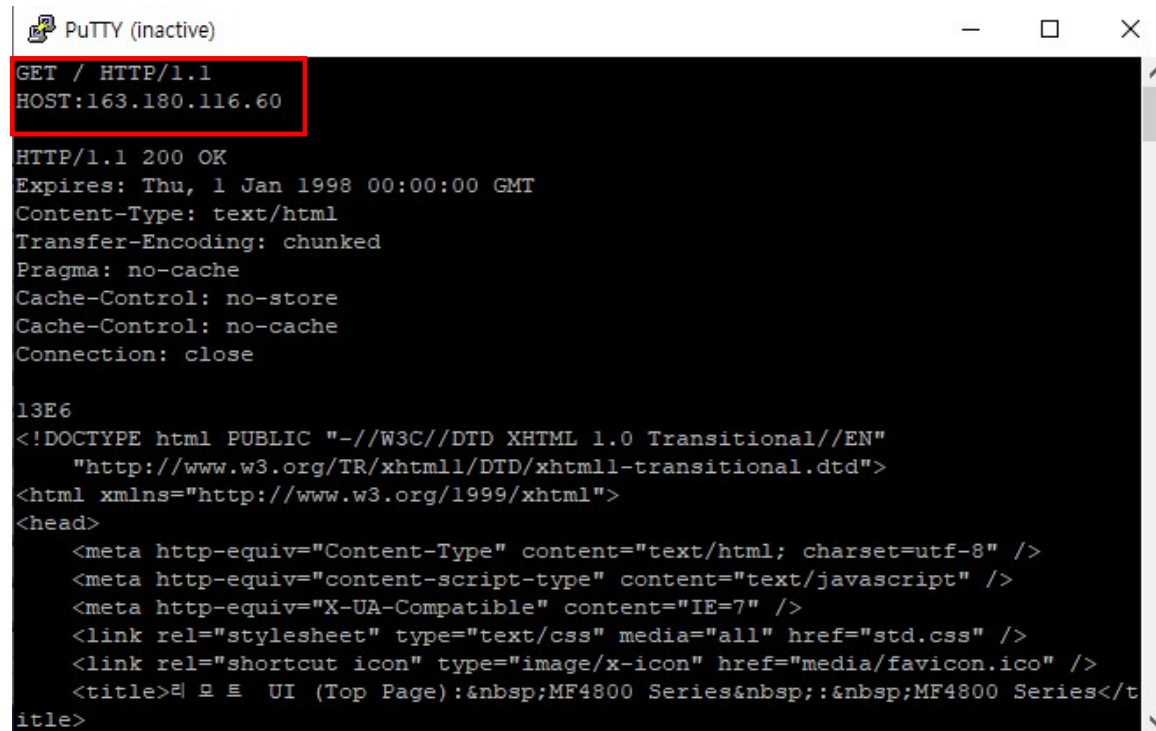
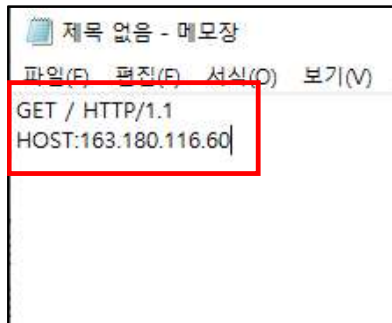
Close window on exit: Always, Never, Only on clean exit

Buttons: About, Help, Open, Cancel

HTTP



HTTP



SMTP

