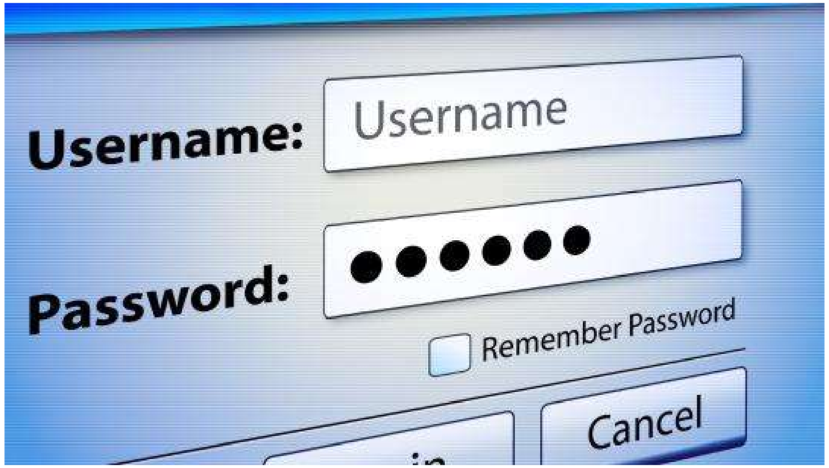
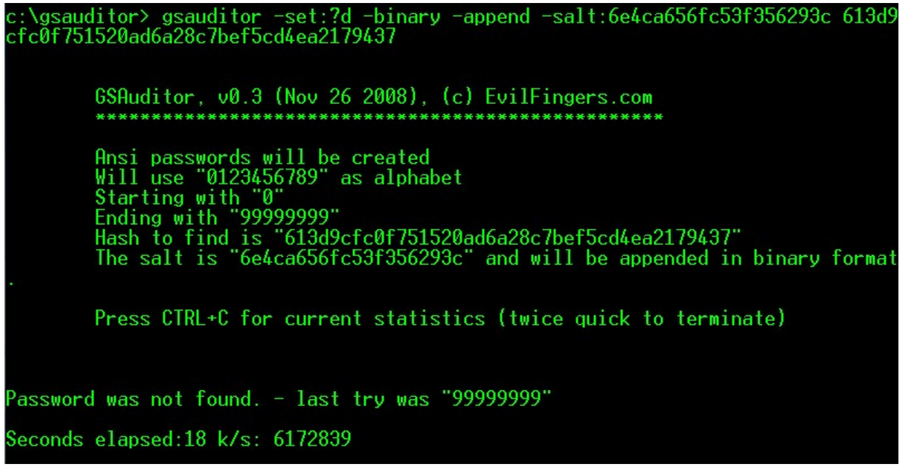
Lab 3. Password Cracking / Port Scanning

Password Cracking

Password Cracking ?

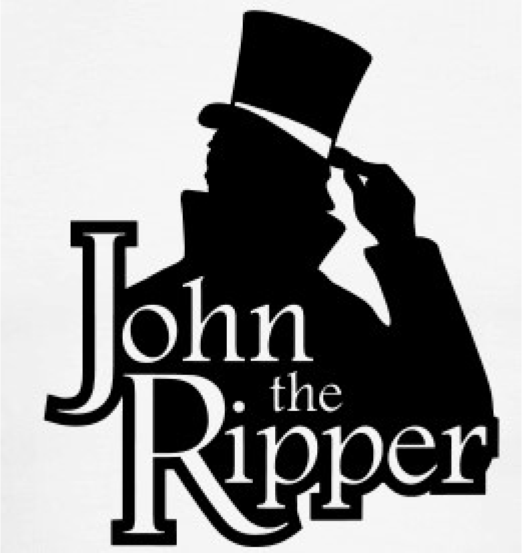


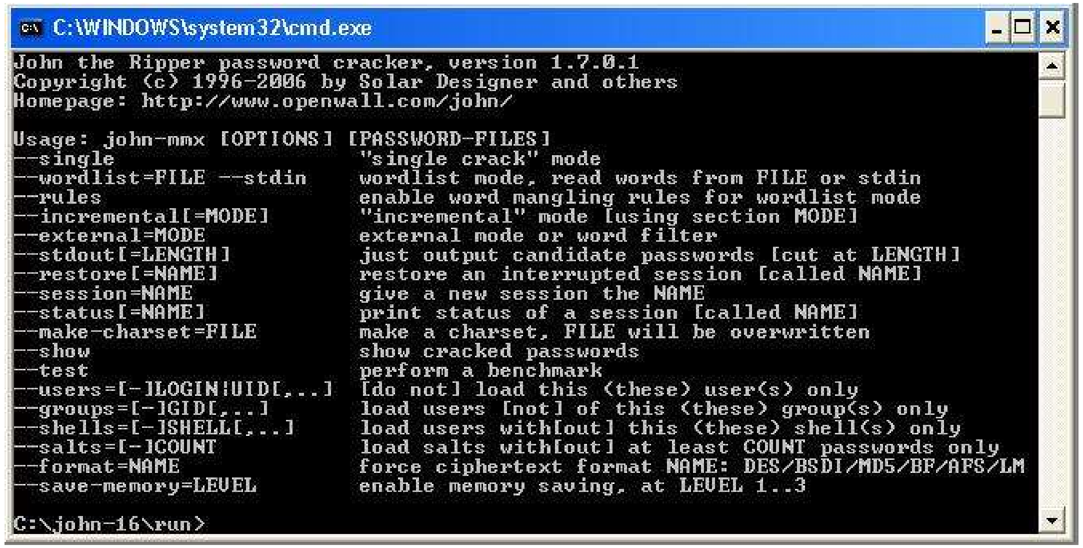


```
c:\gsauditor> gsauditor -set:?d -binary -append -salt:6e4ca656fc53f356293c 613d9
cfc0f751520ad6a28c7bef5cd4ea2179437


        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

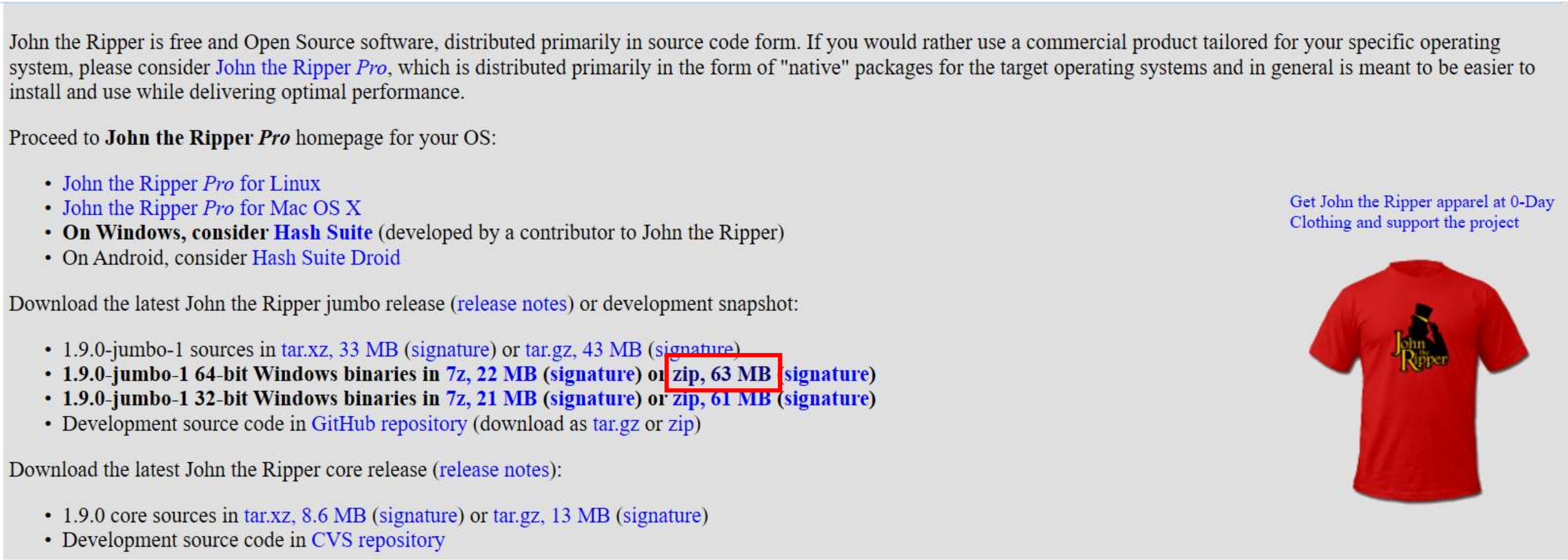




```
John the Ripper password cracker, version 1.7.0.1
Copyright (c) 1996-2006 by Solar Designer and others
Homepage: http://www.openwall.com/john/

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=[-]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
--format=NAME              force ciphertext format NAME: DES/BSDI/MD5/BF/AFS/LM
--save-memory=LEVEL        enable memory saving, at LEVEL 1..3

C:\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)

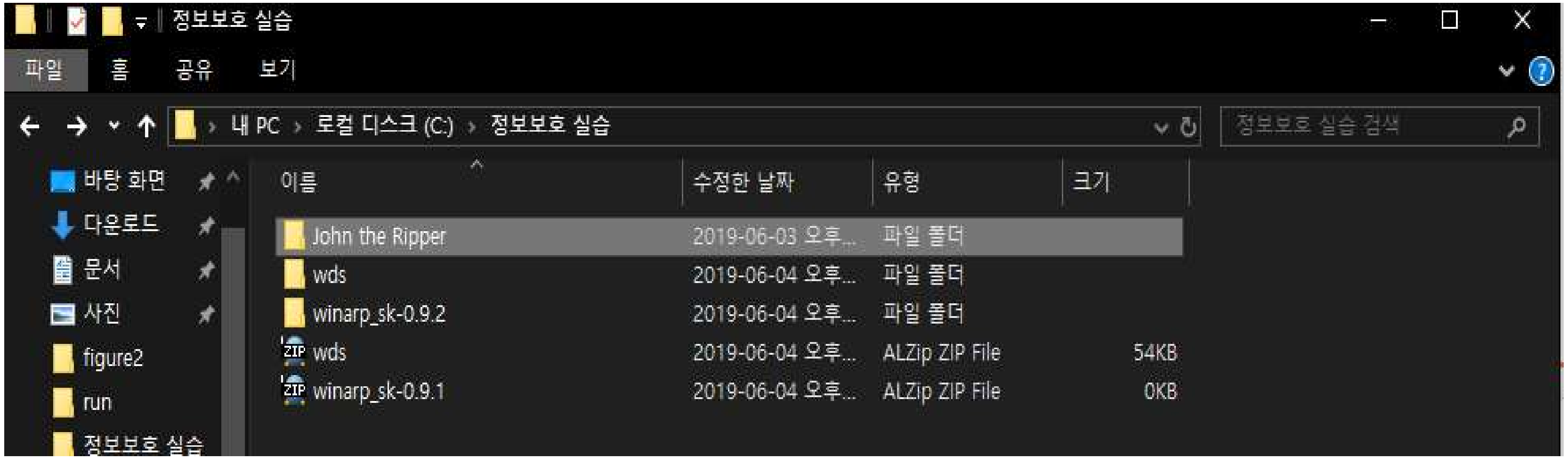
Download the latest John the Ripper core release (release notes):

- 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

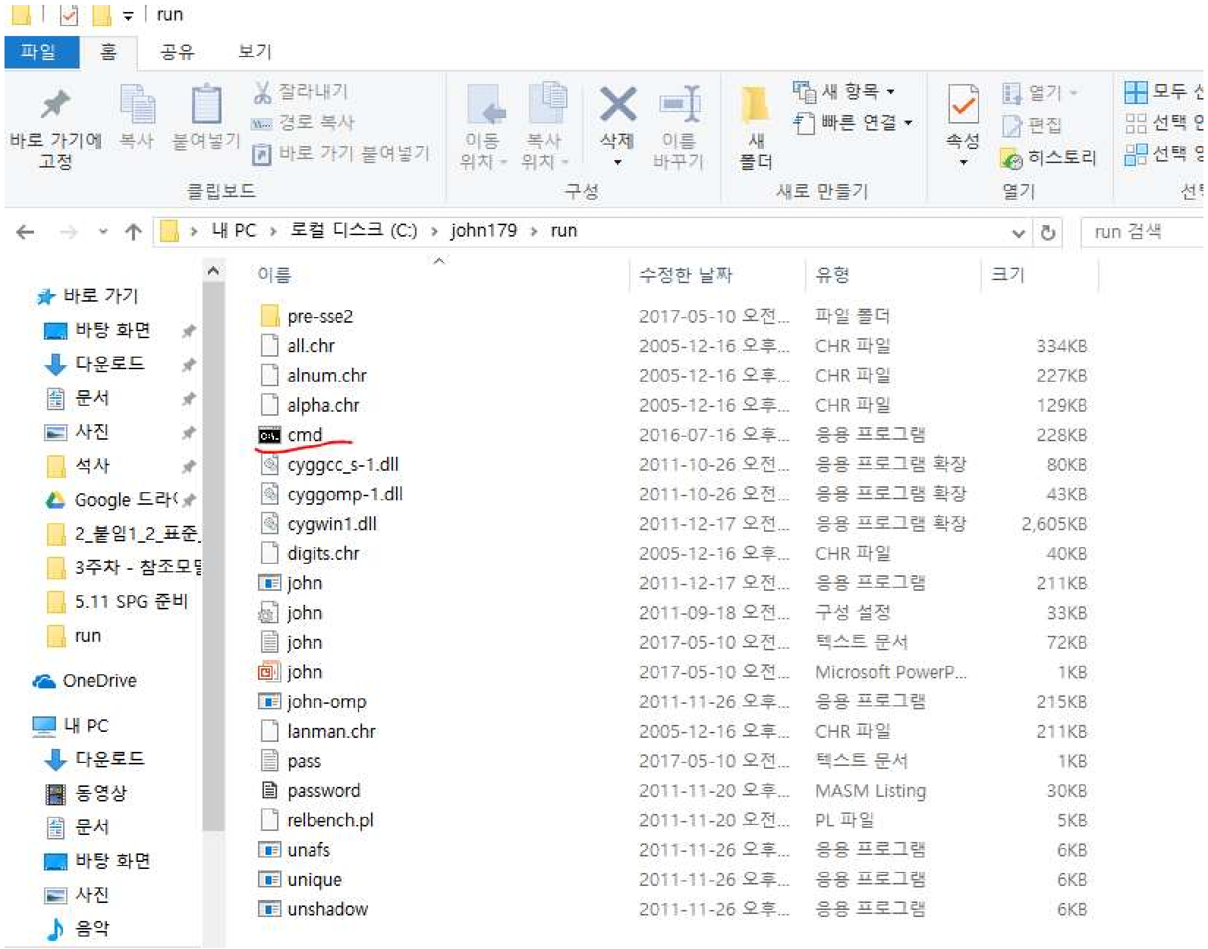
- 압축 해제



이름	수정한 날짜	유형	크기
John the Ripper	2019-06-03 오후...	파일 폴더	
wds	2019-06-04 오후...	파일 폴더	
winarp_sk-0.9.2	2019-06-04 오후...	파일 폴더	
wds	2019-06-04 오후...	ALZip ZIP File	54KB
winarp_sk-0.9.1	2019-06-04 오후...	ALZip ZIP File	0KB

John the ripper 사용

- John\run 폴더 내 CMD 복사

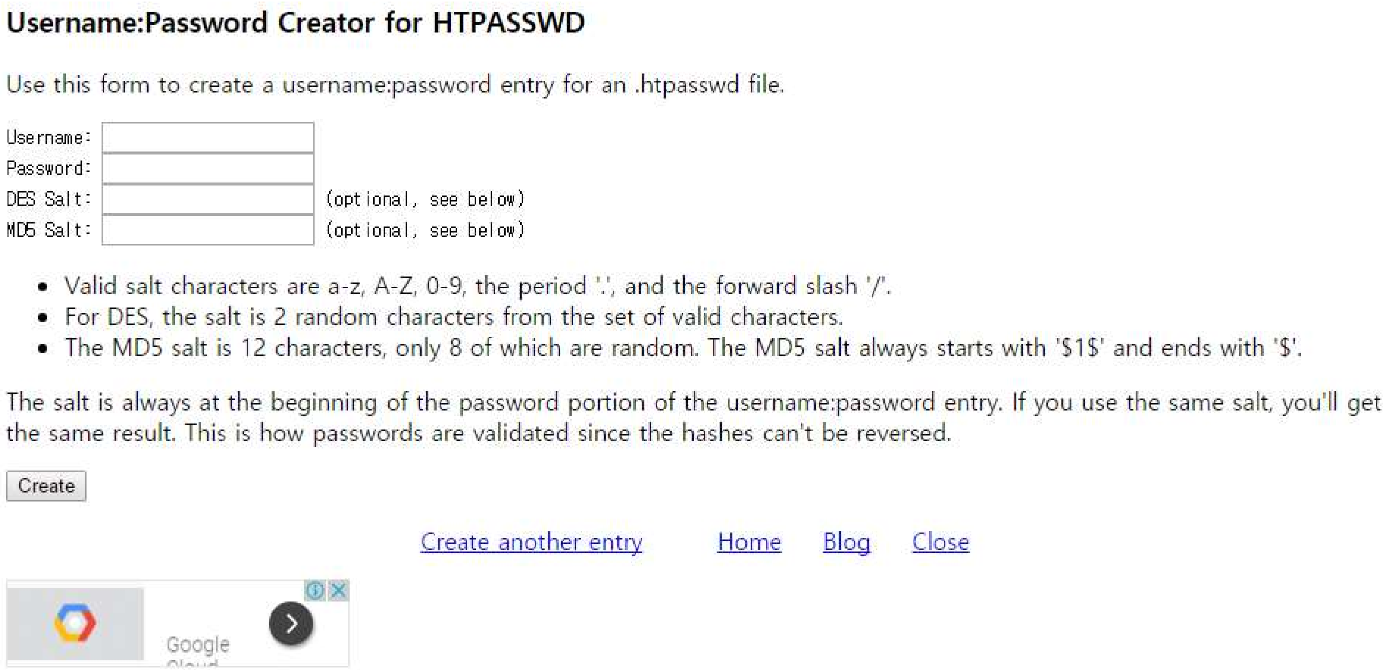


내 PC › 로컬 디스크 (C:) › john179 › run

이름	수정한 날짜	유형	크기
pre-sse2	2017-05-10 오전...	파일 폴더	
all.chr	2005-12-16 오후...	CHR 파일	334KB
alnum.chr	2005-12-16 오후...	CHR 파일	227KB
alpha.chr	2005-12-16 오후...	CHR 파일	129KB
cmd	2016-07-16 오후...	응용 프로그램	228KB
cyggcc_s-1.dll	2011-10-26 오전...	응용 프로그램 확장	80KB
cyggomp-1.dll	2011-10-26 오전...	응용 프로그램 확장	43KB
cygwin1.dll	2011-12-17 오전...	응용 프로그램 확장	2,605KB
digits.chr	2005-12-16 오후...	CHR 파일	40KB
john	2011-12-17 오전...	응용 프로그램	211KB
john	2011-09-18 오전...	구성 설정	33KB
john	2017-05-10 오전...	텍스트 문서	72KB
john	2017-05-10 오전...	Microsoft PowerP...	1KB
john-omp	2011-11-26 오후...	응용 프로그램	215KB
lanman.chr	2005-12-16 오후...	CHR 파일	211KB
pass	2017-05-10 오전...	텍스트 문서	1KB
password	2011-11-20 오후...	MASM Listing	30KB
relbench.pl	2011-11-20 오전...	PL 파일	5KB
unafs	2011-11-26 오후...	응용 프로그램	6KB
unique	2011-11-26 오후...	응용 프로그램	6KB
unshadow	2011-11-26 오후...	응용 프로그램	6KB

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:

Password:

DES Salt: (optional, see below)

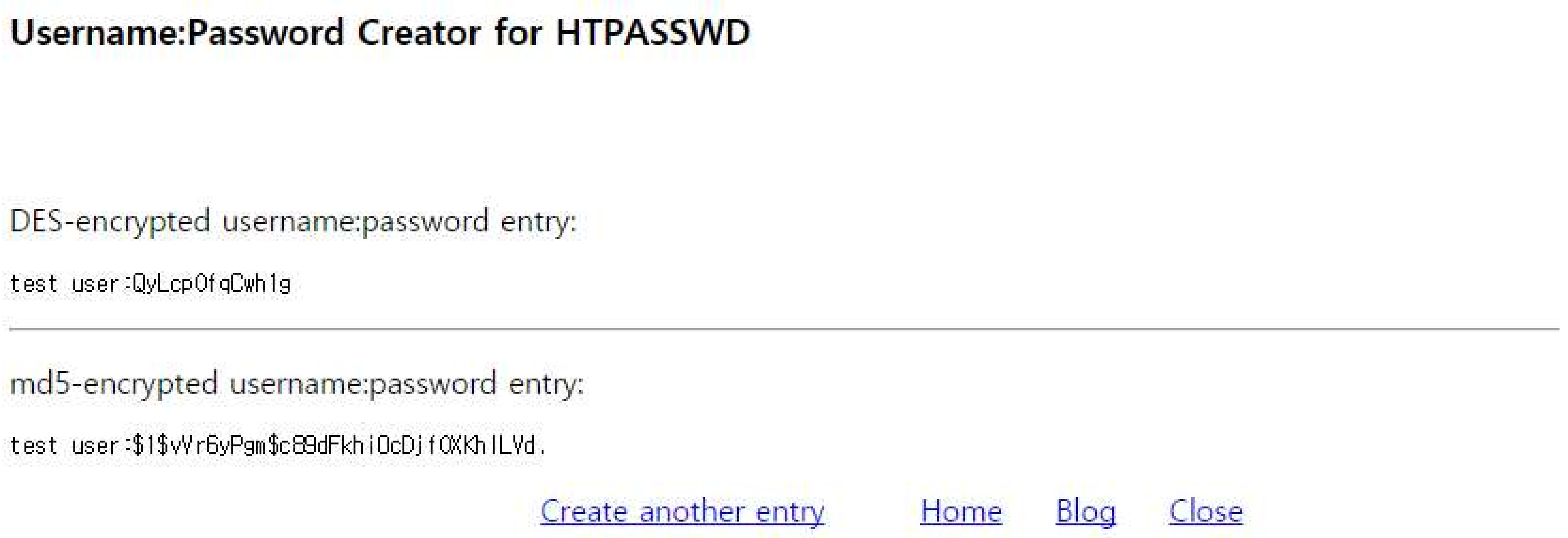
MD5 Salt: (optional, see below)

- 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.

Password 파일 생성

- sherylcanter.com/encrypt.php



Username:Password Creator for HTPASSWD

DES-encrypted username:password entry:

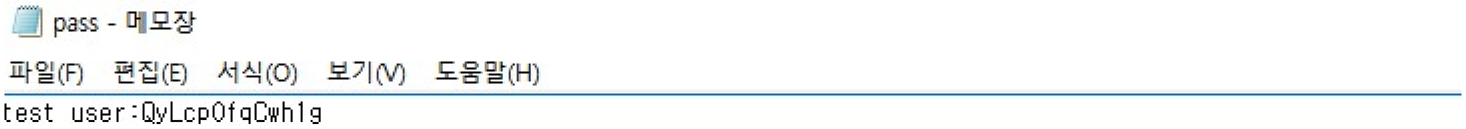
```
test user:QyLcp0fqCwh1g
```

md5-encrypted username:password entry:

```
test user:$1$vVr6yPgm$c89dFkhiOcDjf0XKhILVd.
```

Password 파일 생성

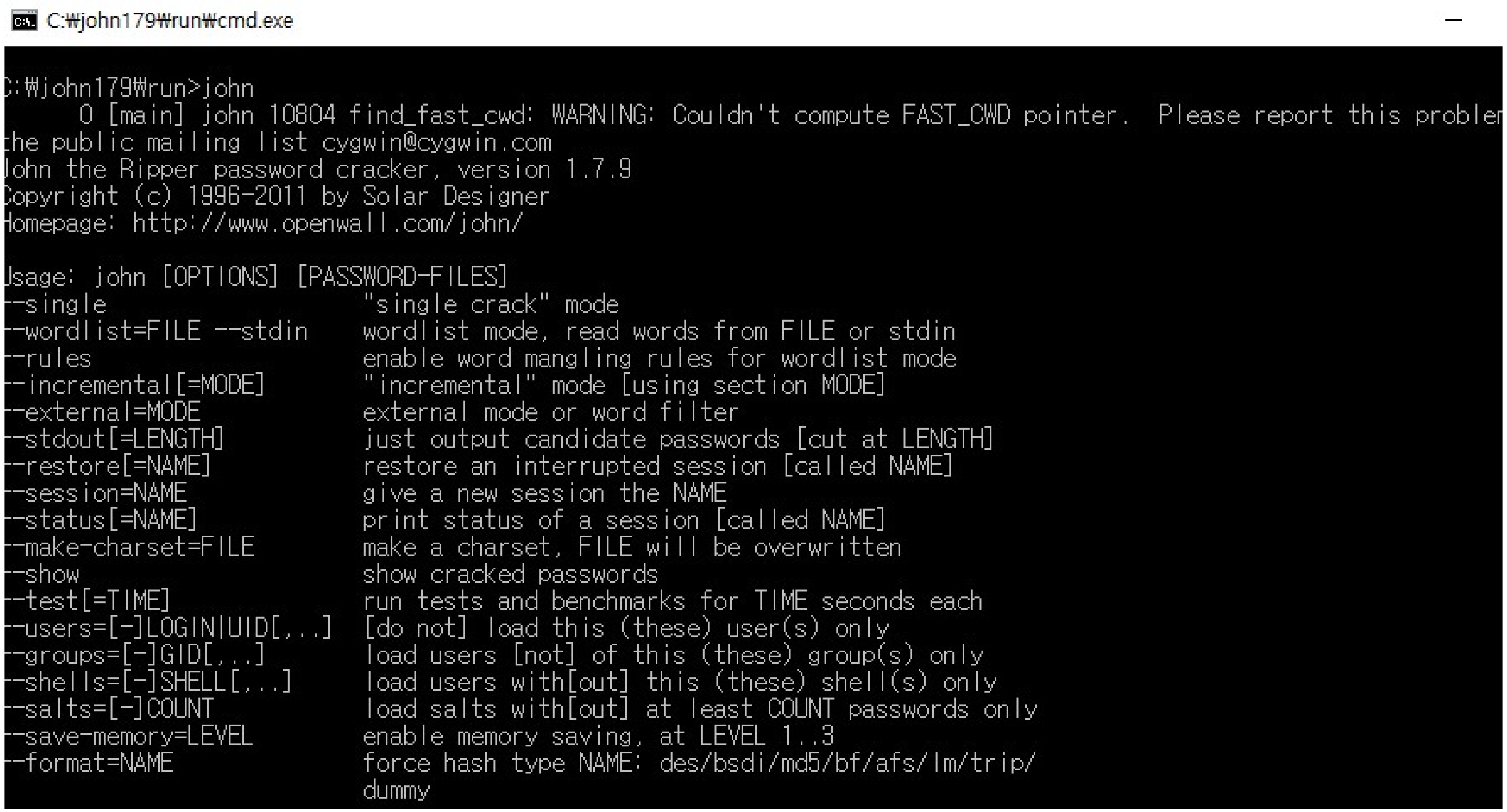
- Txt 파일로 생성 후 저장



```
test user:QyLcp0fqCwh1g
```

Password Cracking 실행

- Cmd - john

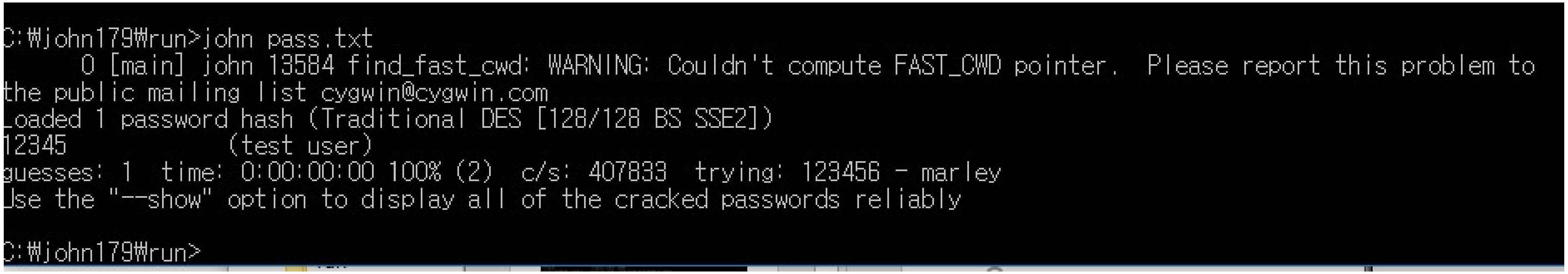


```
C:₩john179₩run>john
      0 [main] john 10804 find_fast_cwd: WARNING: Couldn't compute FAST_CWD pointer.  Please report this proble
the public mailing list cygwin@cygwin.com
John the Ripper password cracker, version 1.7.9
Copyright (c) 1996-2011 by Solar Designer
Homepage: http://www.openwall.com/john/

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

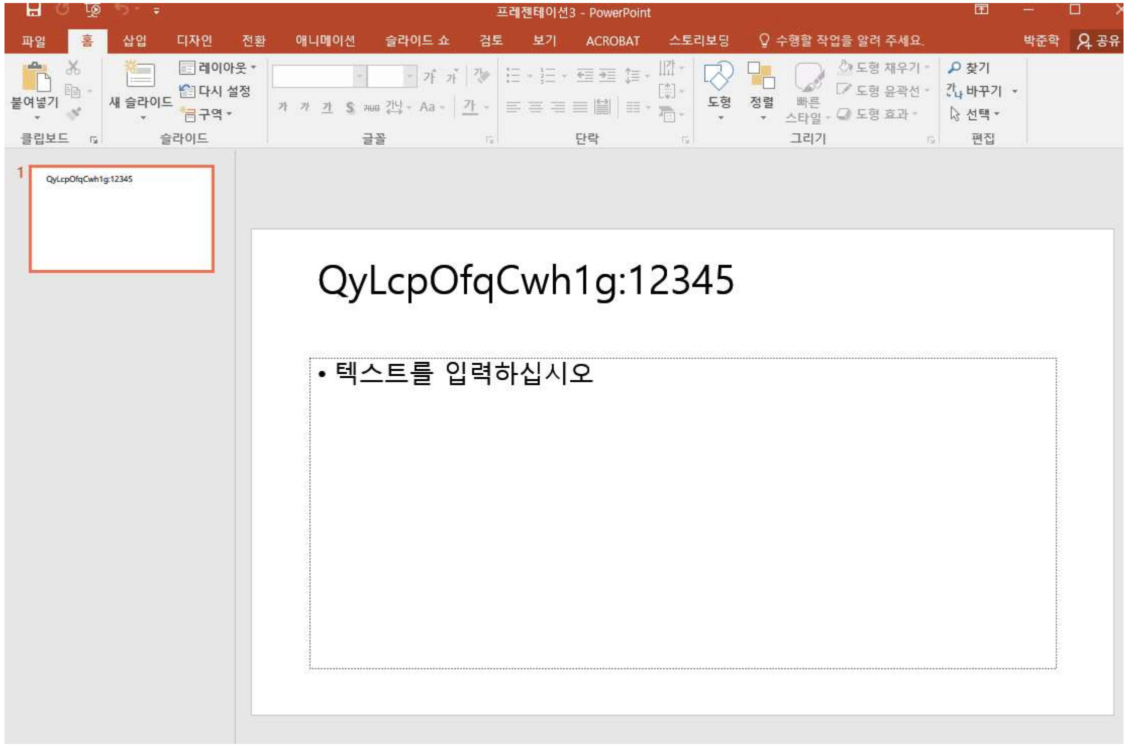
- 계정/패스워드 일치 확인



```
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

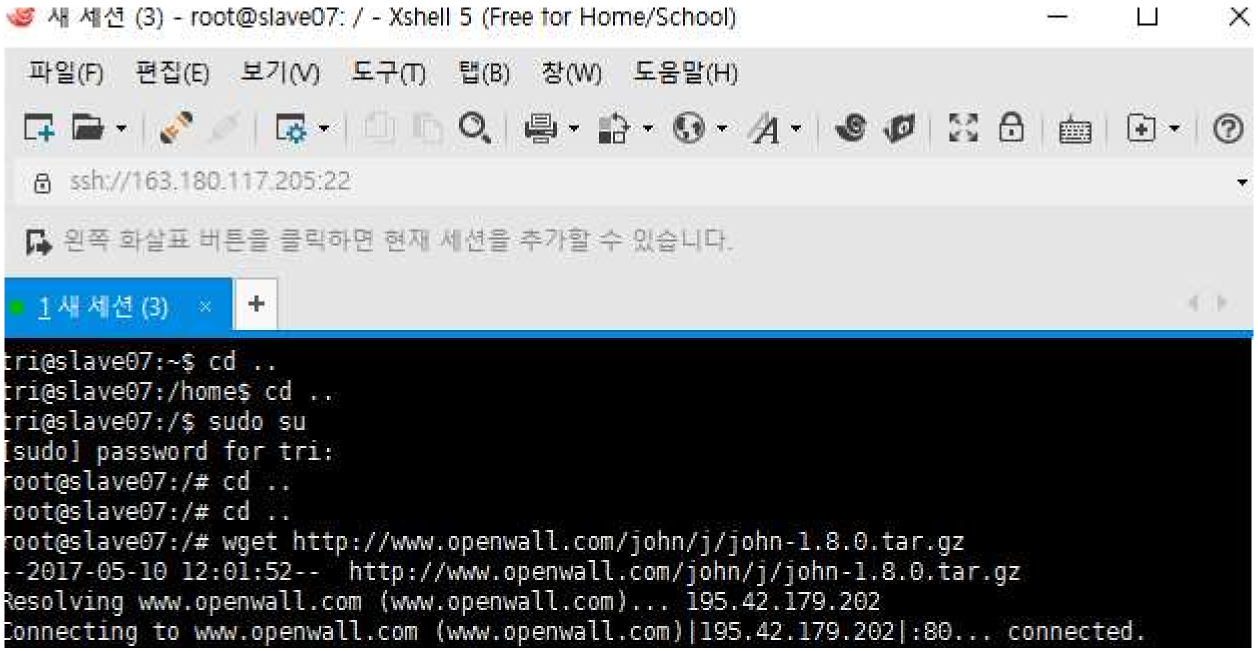


QyLcpOfqCwh1g:12345

- 텍스트를 입력하십시오

John the ripper - Linux

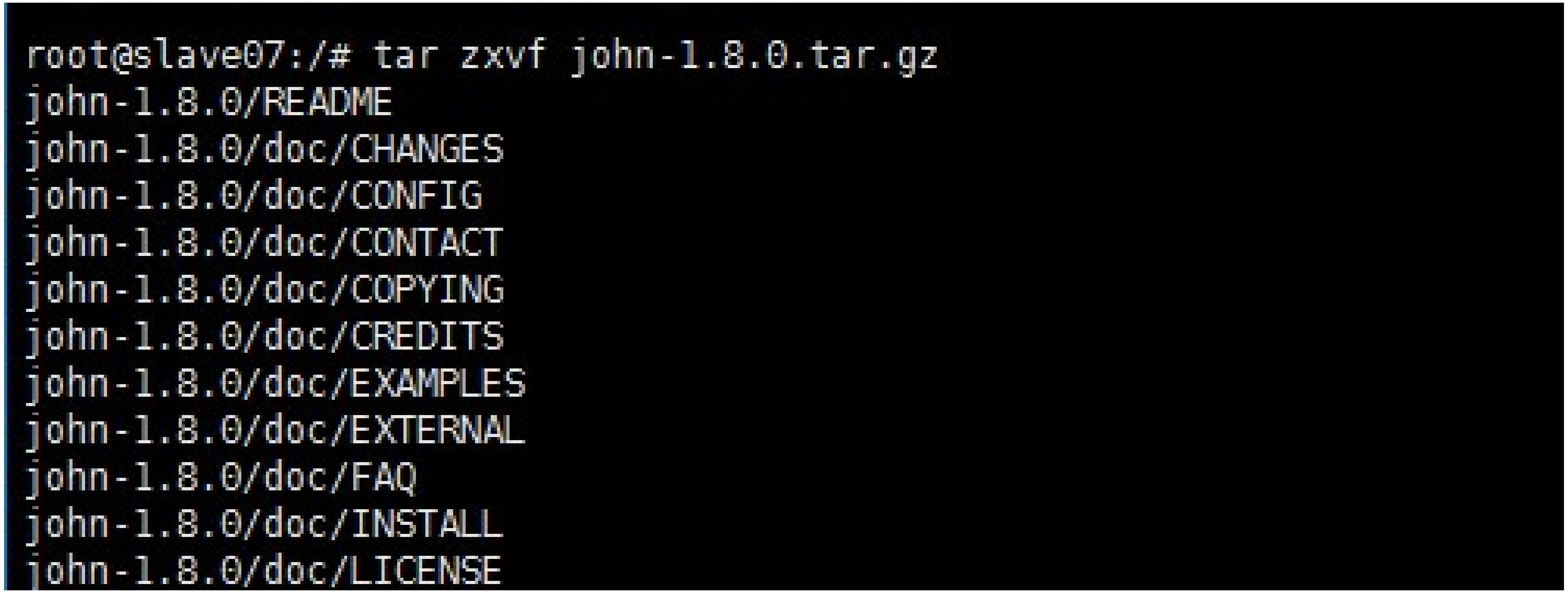
- Apt-get install john
- wget http://openwall.com/john/j/john-1.8.0.tar.gz


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

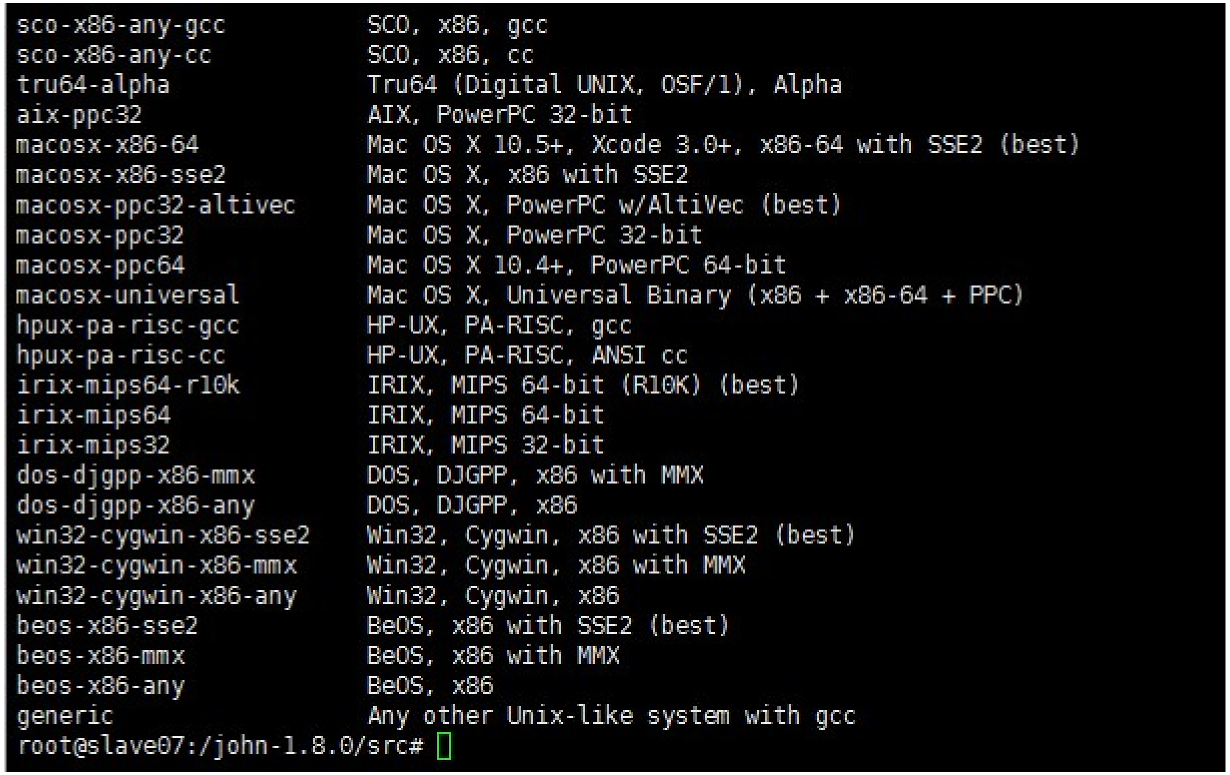


```
root@slave07:/# tar zxvf john-1.8.0.tar.gz
john-1.8.0/README
john-1.8.0/doc/CHANGES
john-1.8.0/doc/CONFIG
john-1.8.0/doc/CONTACT
john-1.8.0/doc/COPYING
john-1.8.0/doc/CREDITS
john-1.8.0/doc/EXAMPLES
john-1.8.0/doc/EXTERNAL
john-1.8.0/doc/FAQ
john-1.8.0/doc/INSTALL
john-1.8.0/doc/LICENSE
```

John the ripper - Linux

- 디렉토리 이동 후 make

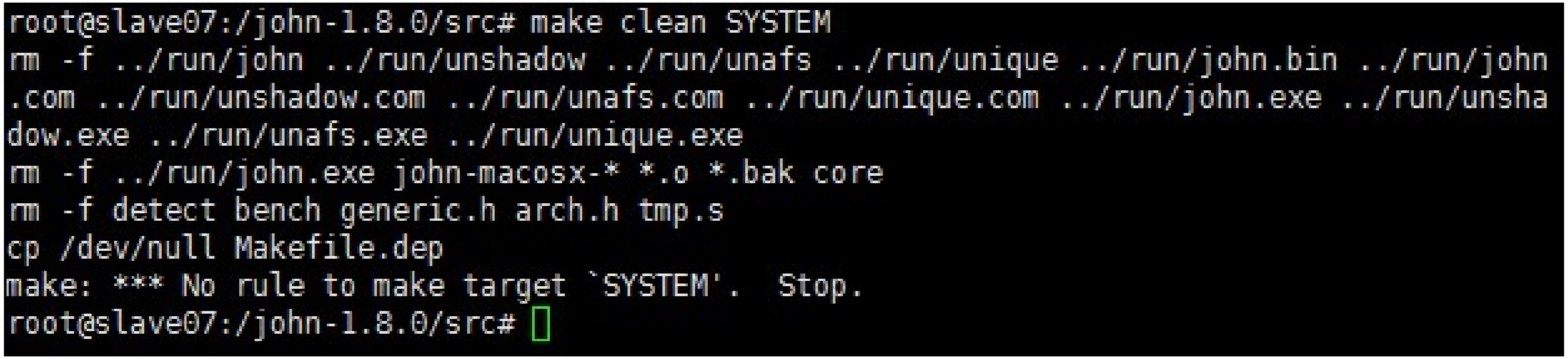
- cd john-1.8.0/src



```
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



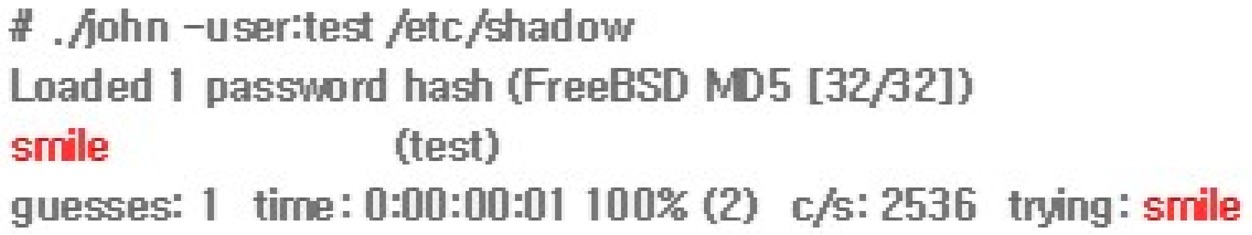
```
root@slave07:/john-1.8.0/src# make clean SYSTEM
rm -f ../run/john ../run/unshadow ../run/unafs ../run/unique ../run/john.bin ../run/john
.com ../run/unshadow.com ../run/unafs.com ../run/unique.com ../run/john.exe ../run/unsha
dow.exe ../run/unafs.exe ../run/unique.exe
rm -f ../run/john.exe john-macosx-* *.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

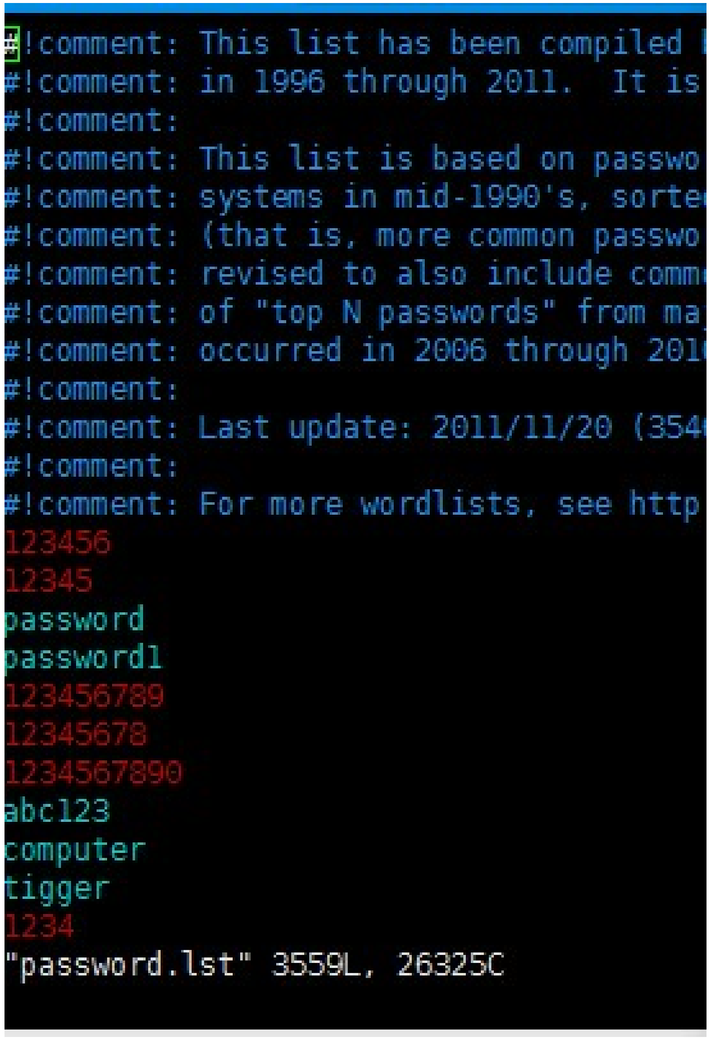
- ./john/etc/shadow 로 실행



```
# ./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

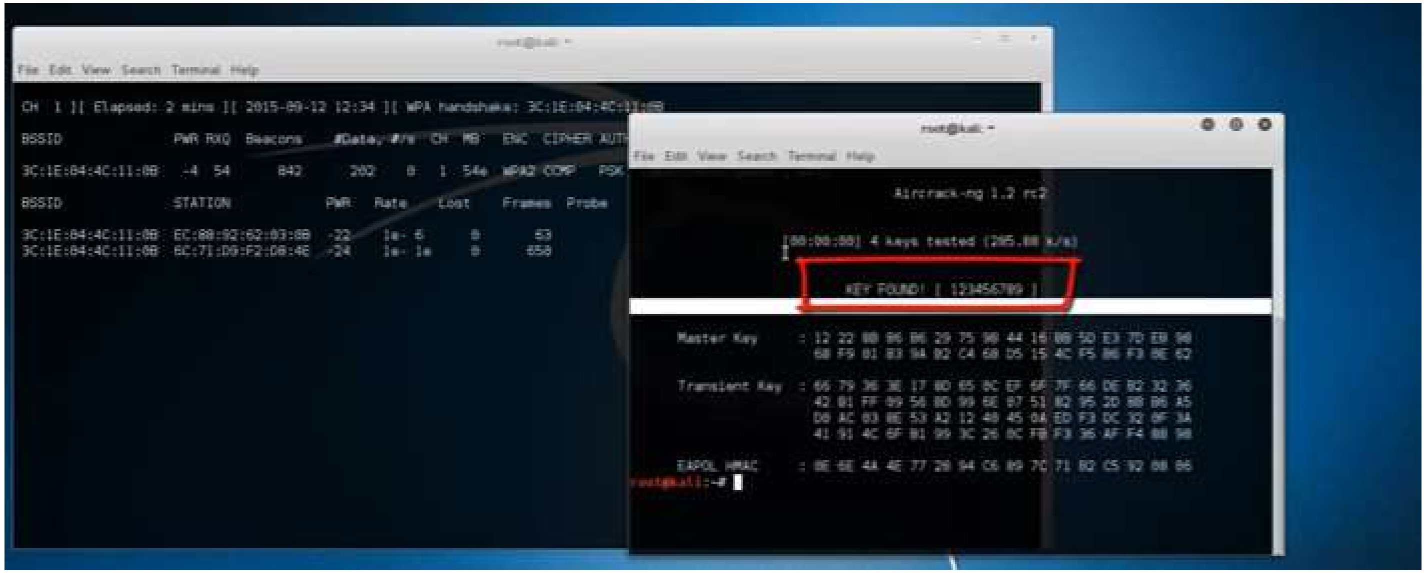
- Password.lst



```
#!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



root@kali: ~
File Edit View Search Terminal Help

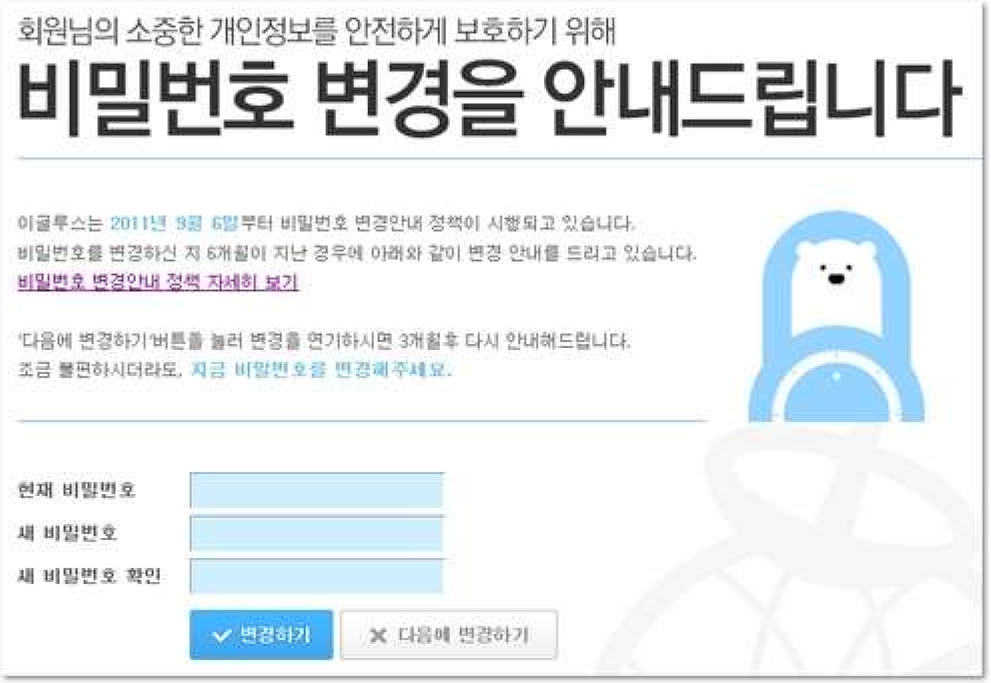
```
CH  1 ][ Elapsed: 2 mins ][ 2015-09-12 12:34 ][ WPA handshake: 3C:1E:04:4C:11:0B

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH

3C:1E:04:4C:11:0B   -4  54      842      202    0   1  54e  WPA2 CCMP   PSK

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

3C:1E:04:4C:11:0B  EC:88:92:62:03:8B  -22    1e- 6      0       63
3C:1E:04:4C:11:0B  6C:71:D9:F2:D8:4E  -24    1e- 1e     0      658
```

root@kali: ~
File Edit View Search Terminal Help

```
                          Aircrack-ng 1.2 rc2

              [00:00:00] 4 keys tested (205.00 k/s)

                      KEY FOUND! [ 123456789 ]

      Master Key     : 12 22 80 06 06 29 75 90 44 16 B0 5D E3 7D E8 90
                       68 F9 81 83 94 82 C4 68 D5 15 4C F5 86 F3 8E 62

      Transient Key  : 66 79 36 3E 17 8D 65 8C EF 6F 7F 66 DE B2 32 36
                       42 81 FF 09 56 8D 99 6E 07 51 82 95 2D 88 B6 A5
                       D8 AC 03 8E 53 A2 12 48 45 04 ED F3 DC 32 0F 3A
                       41 91 4C 6F 81 09 3C 26 8C FB F3 36 AF F4 88 98

      EAPOL HMAC     : 0E 6E 4A 4E 77 28 94 C6 89 7C 71 82 C5 92 08 86
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

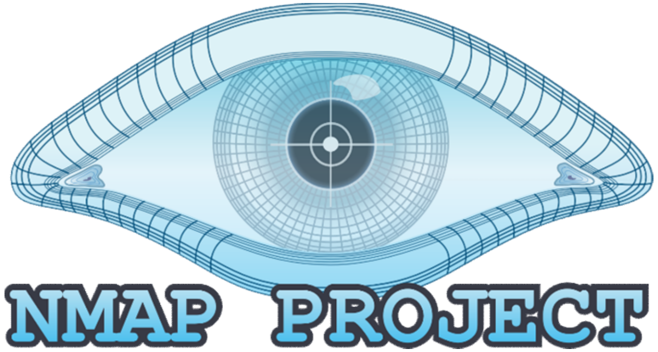
Port Scanning

Network Scanning ?

```
[root@mybox ~]# nmap -p 22 --open -sV 197.213.63.32/29
Nmap scan report for alex.peachtrees.com (197.213.63.34)
```

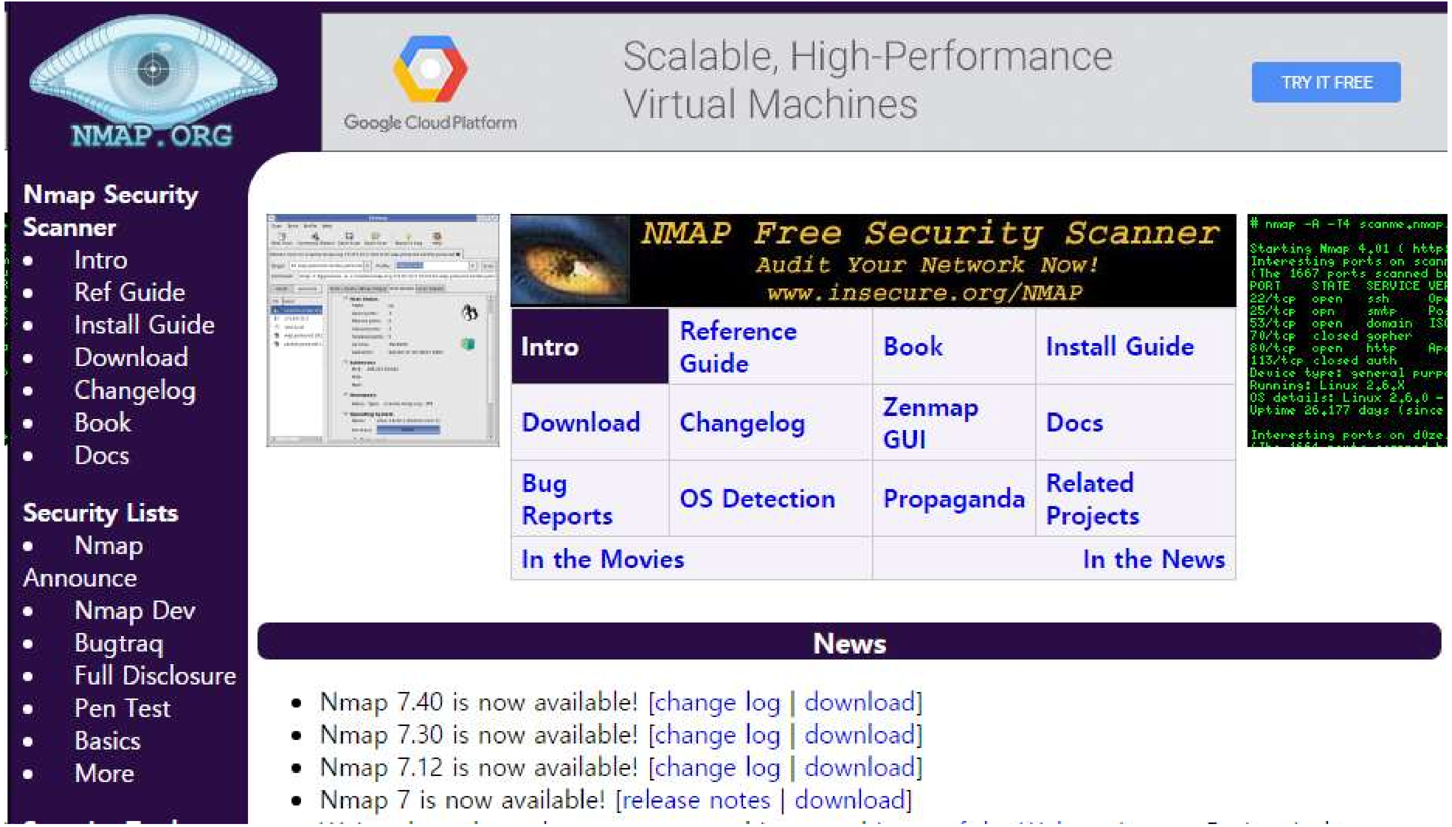
실습 사용 tool

- Nmap – network scanning tool
  - 네트워크 탐색
  - 보안 감시 가능
  - 작동중인 호스트 탐색
  - OS, 패킷 필터, 방화벽 검색 기능 제공



설치

- https://nmap.org/
- https://nmap.org/dist/nmap-7.12-setup.exe



Nmap Security Scanner

- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists

- Nmap Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

NMAP Free Security Scanner
Audit Your Network Now!
www.insecure.org/NMAP

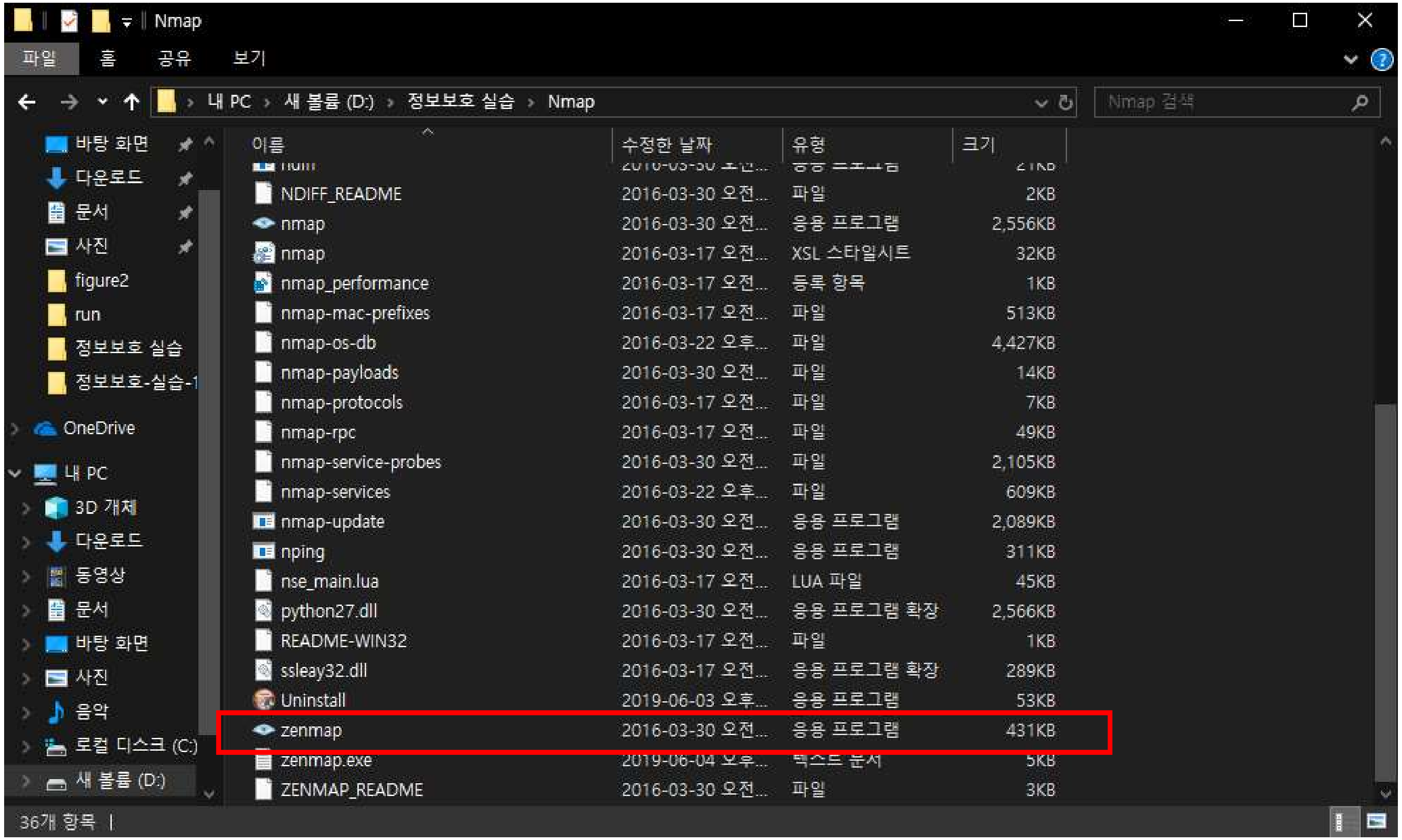
Intro	Reference Guide	Book	Install Guide
Download	Changelog	Zenmap GUI	Docs
Bug Reports	OS Detection	Propaganda	Related Projects
In the Movies			In the News

```
# nmap -A -T4 scanme.nmap.

Starting Nmap 4.01 ( https
Interesting ports on scann
(The 1667 ports scanned bu
PORT    STATE  SERVICE VER
22/tcp  open   ssh     Ope
25/tcp  opn    smtp    Pos
53/tcp  open   domain  ISC
70/tcp  closed gopher
80/tcp  open   http    Apa
113/tcp closed auth
Device type: general purpo
Running: Linux 2.6.X
OS details: Linux 2.6.0 -
Uptime 26.177 days (since

Interesting ports on d0ze.
```

News

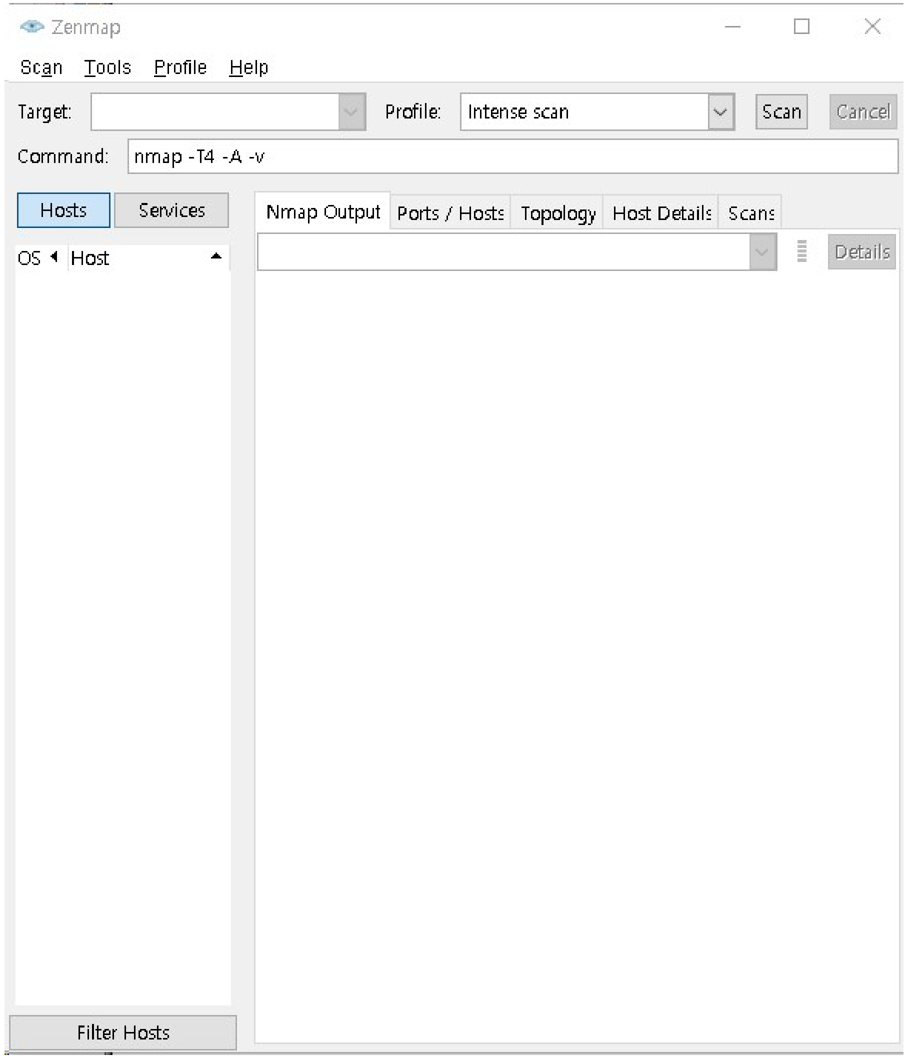
- Nmap 7.40 is now available! [change log | download]
- Nmap 7.30 is now available! [change log | download]
- Nmap 7.12 is now available! [change log | download]
- Nmap 7 is now available! [release notes | download]

설치



이름	수정한 날짜	유형	크기
ndiff	2016-03-30 오전...	응용 프로그램	21KB
NDIFF_README	2016-03-30 오전...	파일	2KB
nmap	2016-03-30 오전...	응용 프로그램	2,556KB
nmap	2016-03-17 오전...	XSL 스타일시트	32KB
nmap_performance	2016-03-17 오전...	등록 항목	1KB
nmap-mac-prefixes	2016-03-17 오전...	파일	513KB
nmap-os-db	2016-03-22 오후...	파일	4,427KB
nmap-payloads	2016-03-30 오전...	파일	14KB
nmap-protocols	2016-03-17 오전...	파일	7KB
nmap-rpc	2016-03-17 오전...	파일	49KB
nmap-service-probes	2016-03-30 오전...	파일	2,105KB
nmap-services	2016-03-22 오후...	파일	609KB
nmap-update	2016-03-30 오전...	응용 프로그램	2,089KB
nping	2016-03-30 오전...	응용 프로그램	311KB
nse_main.lua	2016-03-17 오전...	LUA 파일	45KB
python27.dll	2016-03-30 오전...	응용 프로그램 확장	2,566KB
README-WIN32	2016-03-17 오전...	파일	1KB
ssleay32.dll	2016-03-17 오전...	응용 프로그램 확장	289KB
Uninstall	2019-06-03 오후...	응용 프로그램	53KB
zenmap	2016-03-30 오전...	응용 프로그램	431KB
zenmap.exe	2019-06-04 오후...	텍스트 문서	5KB
ZENMAP_README	2016-03-30 오전...	파일	3KB

실행 화면



Target:

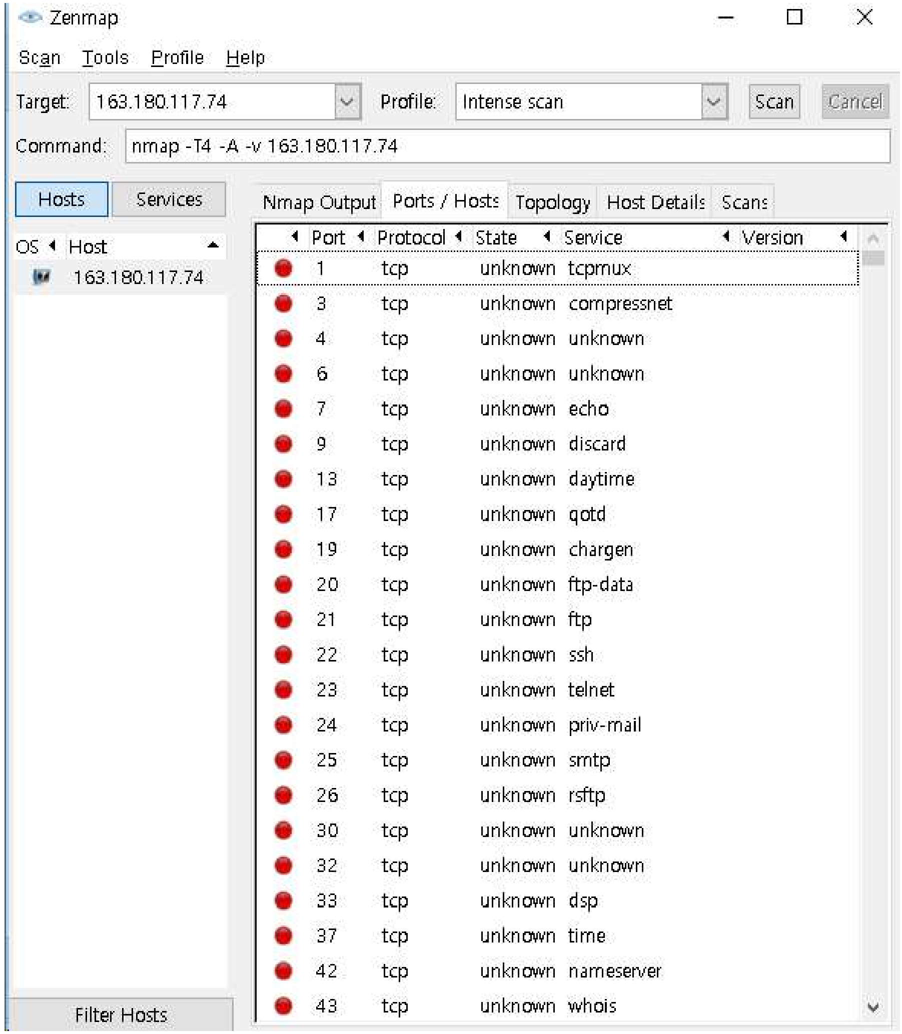
Profile: Intense scan

Command: nmap -T4 -A -v

- Target : 확인하고자 하는 도메인 혹은 IP
- Profile : 원하는 스캔 유형 선택
- Command : 명령어 (+옵션)

실행 방법

- 결과 화면



Target: 163.180.117.74

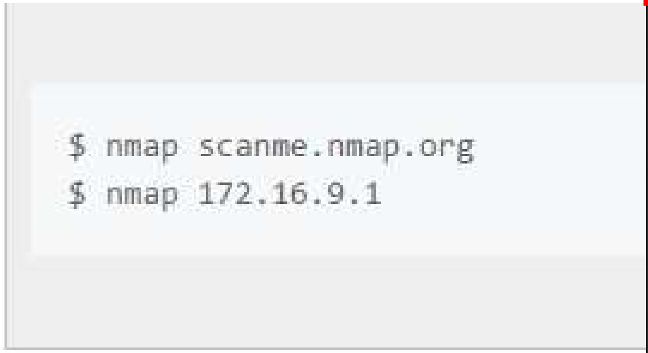
Profile: Intense scan

Command: nmap -T4 -A -v 163.180.117.74

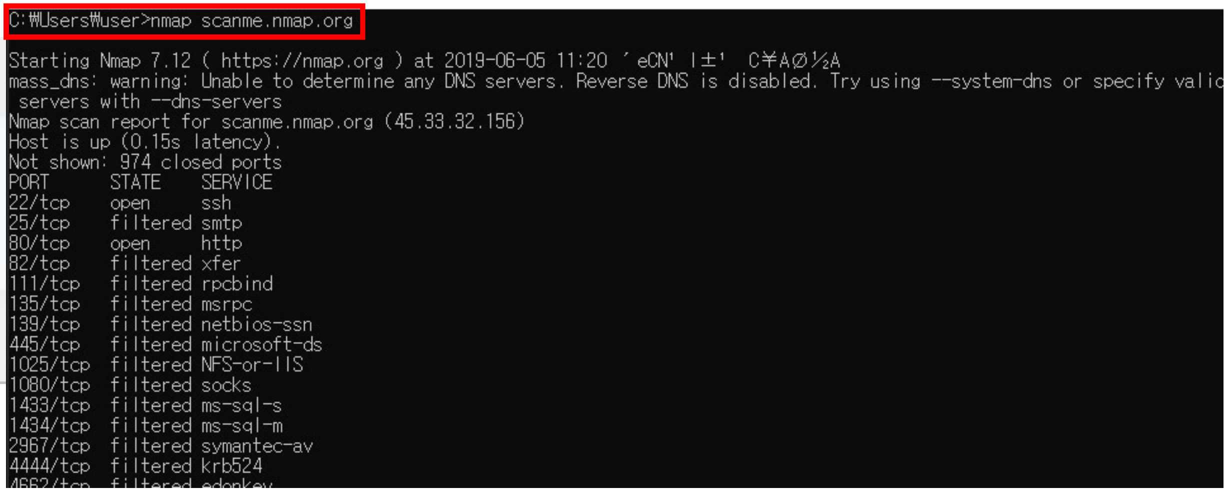
OS	Host
	163.180.117.74

	Port	Protocol	State	Service	Version
●	1	tcp	unknown	tcpmux	
●	3	tcp	unknown	compressnet	
●	4	tcp	unknown	unknown	
●	6	tcp	unknown	unknown	
●	7	tcp	unknown	echo	
●	9	tcp	unknown	discard	
●	13	tcp	unknown	daytime	
●	17	tcp	unknown	qotd	
●	19	tcp	unknown	chargen	
●	20	tcp	unknown	ftp-data	
●	21	tcp	unknown	ftp	
●	22	tcp	unknown	ssh	
●	23	tcp	unknown	telnet	
●	24	tcp	unknown	priv-mail	
●	25	tcp	unknown	smtp	
●	26	tcp	unknown	rsftp	
●	30	tcp	unknown	unknown	
●	32	tcp	unknown	unknown	
●	33	tcp	unknown	dsp	
●	37	tcp	unknown	time	
●	42	tcp	unknown	nameserver	
●	43	tcp	unknown	whois	

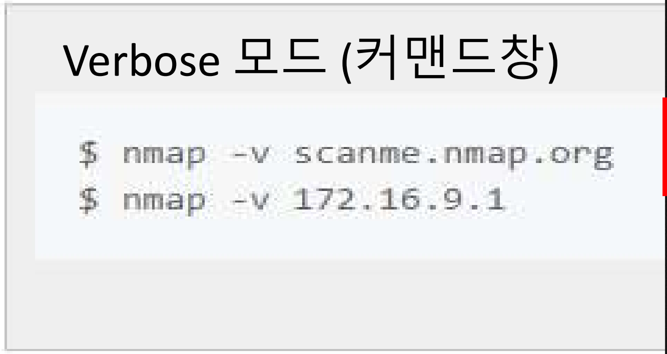
- 1. 단일 호스트 스캔
  - IP 주소 지정
  - 호스트 이름 지정



```
$ nmap scanme.nmap.org
$ nmap 172.16.9.1
```

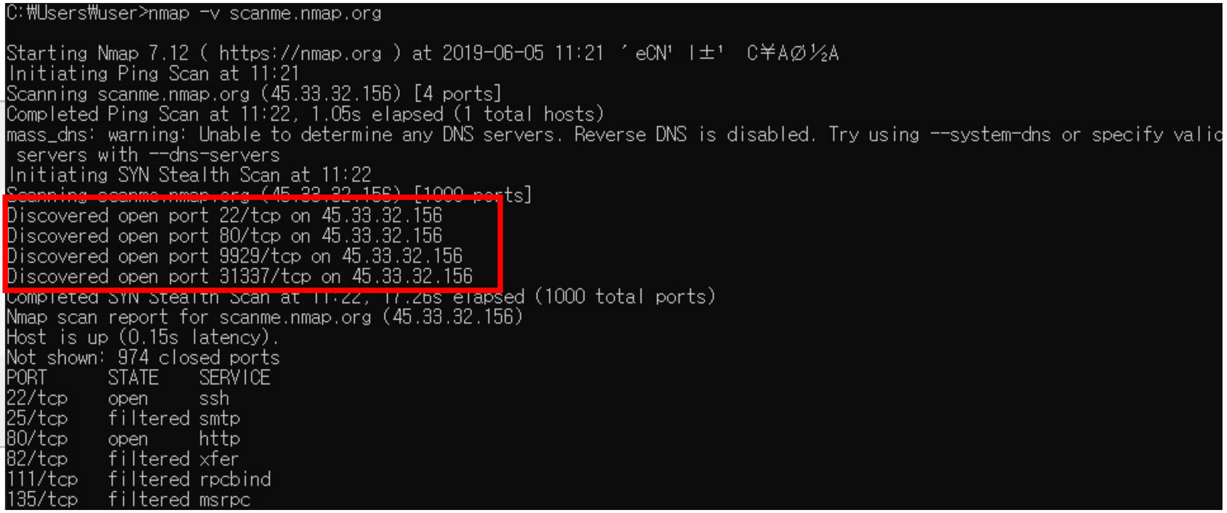


```
C:₩Users₩user>nmap scanme.nmap.org

Starting Nmap 7.12 ( https://nmap.org ) at 2019-06-05 11:20 ´eCN' ¦±'  C¥AØ½A
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valic
 servers with --dns-servers
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.15s latency).
Not shown: 974 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
82/tcp    filtered xfer
111/tcp   filtered rpcbind
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1025/tcp  filtered NFS-or-IIS
1080/tcp  filtered socks
1433/tcp  filtered ms-sql-s
1434/tcp  filtered ms-sql-m
2967/tcp  filtered symantec-av
4444/tcp  filtered krb524
4662/tcp  filtered edonkey
```



Verbose 모드 (커맨드창)

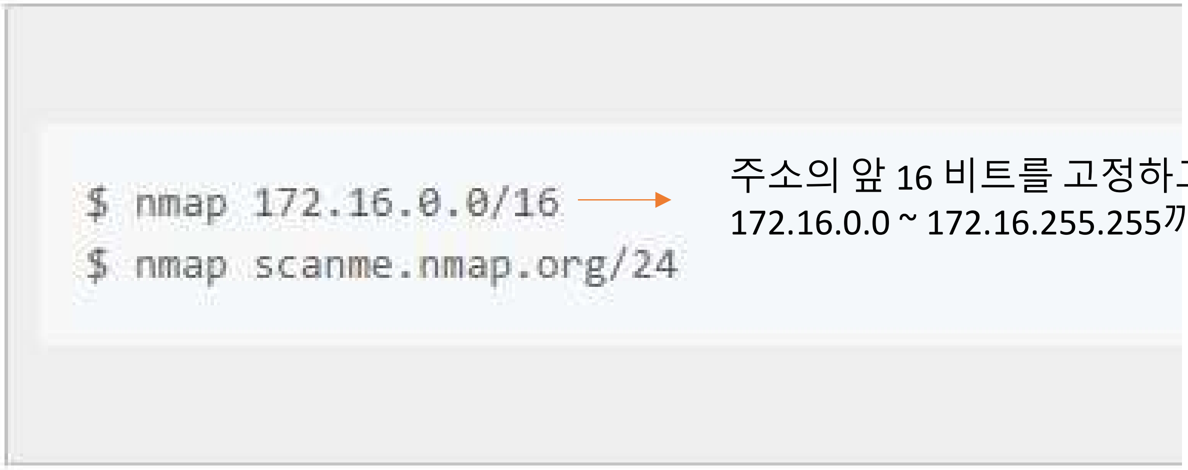
```
$ nmap -v scanme.nmap.org
$ nmap -v 172.16.9.1
```



```
C:₩Users₩user>nmap -v scanme.nmap.org

Starting Nmap 7.12 ( https://nmap.org ) at 2019-06-05 11:21 ´eCN' ¦±'  C¥AØ½A
Initiating Ping Scan at 11:21
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 11:22, 1.05s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valic
 servers with --dns-servers
Initiating SYN Stealth Scan at 11:22
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed SYN Stealth Scan at 11:22, 17.26s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.15s latency).
Not shown: 974 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
82/tcp    filtered xfer
111/tcp   filtered rpcbind
135/tcp   filtered msrpc
```

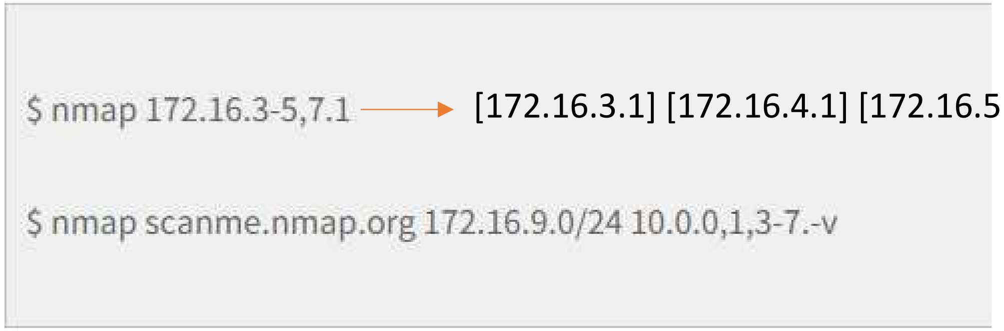
사용 방법

- 2. 다수 호스트 스캔



```
$ nmap 172.16.0.0/16
$ nmap scanme.nmap.org/24
```

주소의 앞 16 비트를 고정하고
172.16.0.0 ~ 172.16.255.255까지 스캔

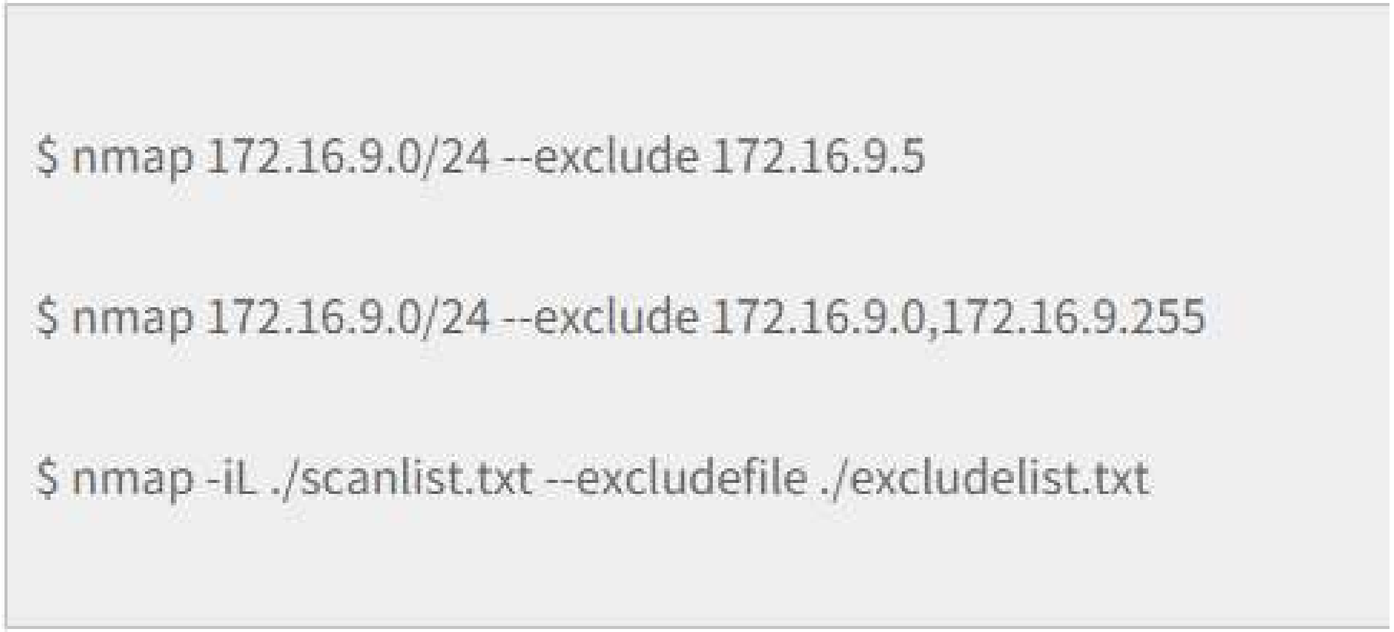


```
$ nmap 172.16.3-5,7.1

$ nmap scanme.nmap.org 172.16.9.0/24 10.0.0,1,3-7.-v
```

[172.16.3.1] [172.16.4.1] [172.16.5.1] [172.16.7.1] 스캔

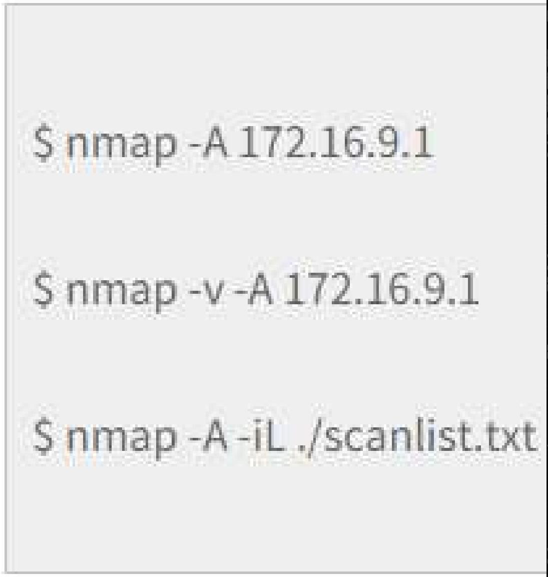
사용 방법

- 3. 특정 호스트 제외 : --exclude

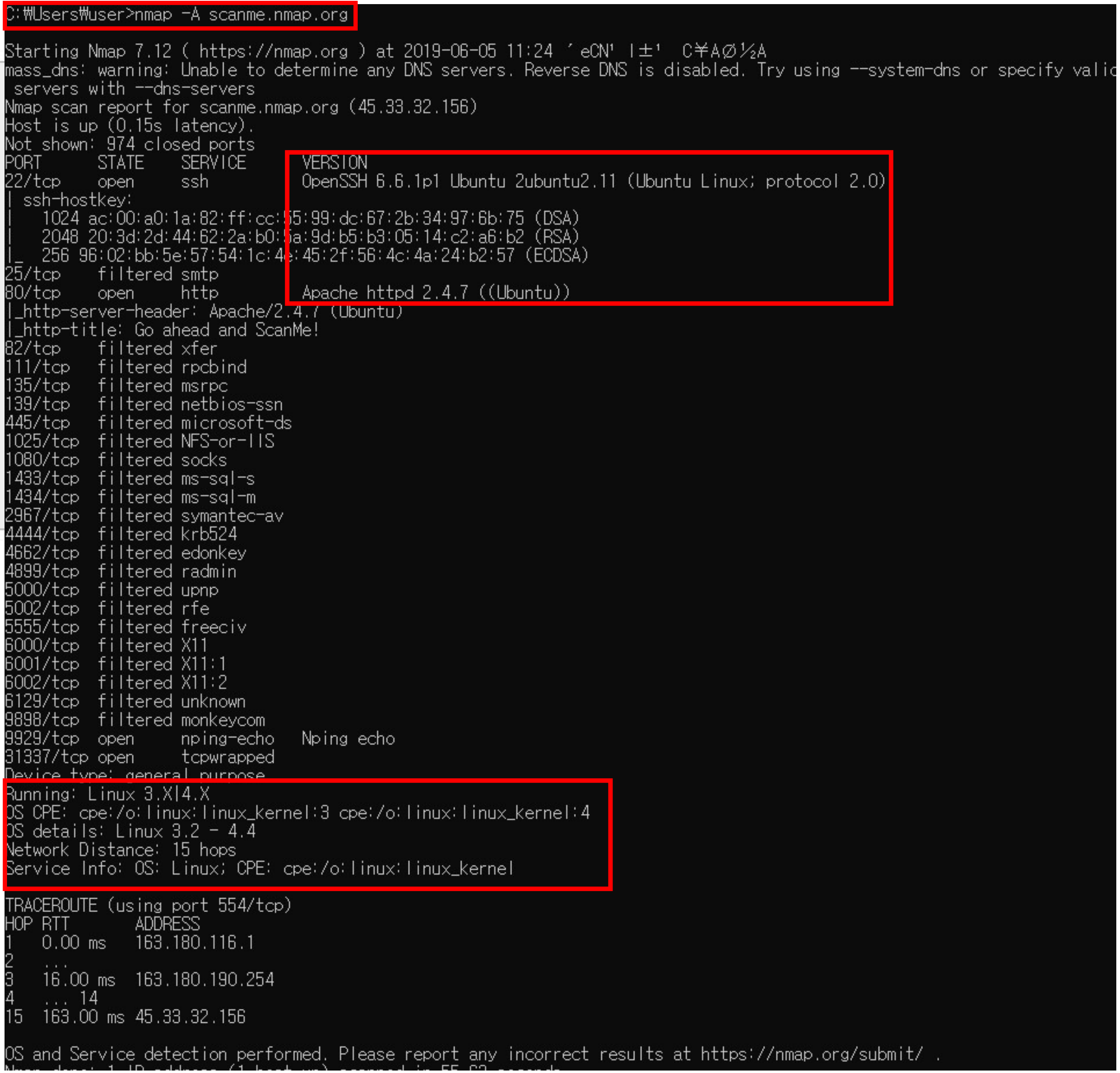


```
$ nmap 172.16.9.0/24 --exclude 172.16.9.5

$ nmap 172.16.9.0/24 --exclude 172.16.9.0,172.16.9.255

$ nmap -iL ./scanlist.txt --excludefile ./excludelist.txt
```

- 4. 운영체제, 버전 확인 기능 활성화 : -A

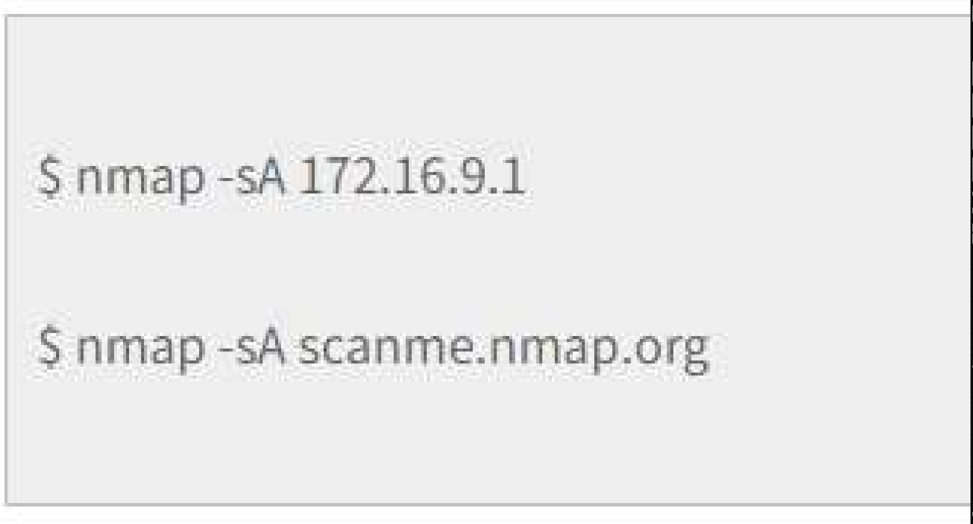


```
$ nmap -A 172.16.9.1

$ nmap -v -A 172.16.9.1

$ nmap -A -iL ./scanlist.txt
```

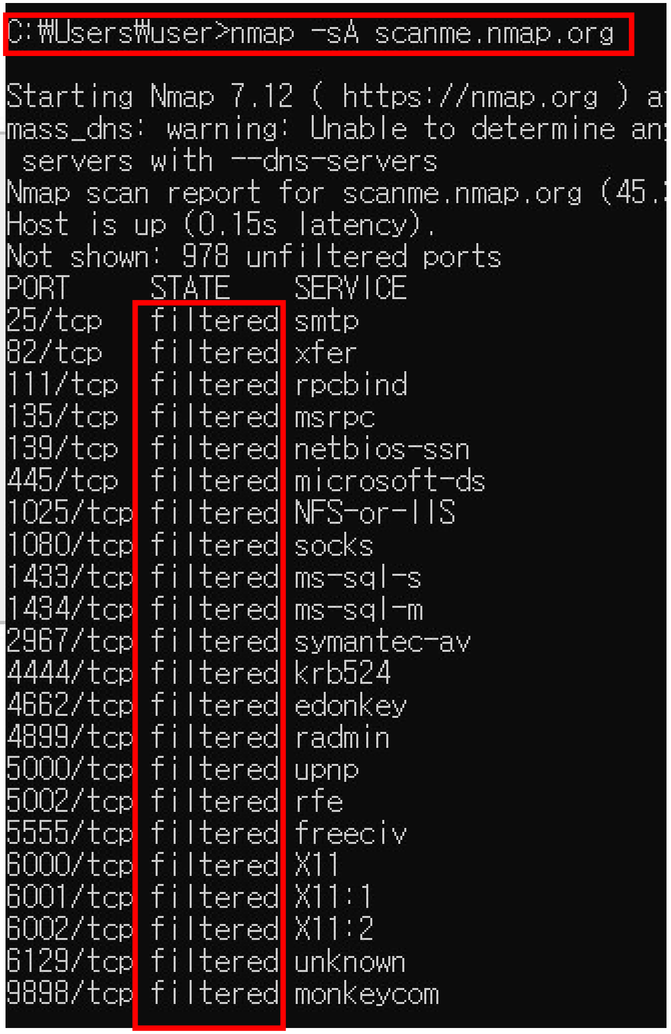


```
C:₩Users₩user>nmap -A scanme.nmap.org

Starting Nmap 7.12 ( https://nmap.org ) at 2019-06-05 11:24 ´eCN¹ Ì±¹  C¥AØ½A
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify vali
 servers with --dns-servers
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.15s latency).
Not shown: 974 closed ports
PORT      STATE    SERVICE       VERSION
22/tcp    open     ssh           OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_  256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
25/tcp    filtered smtp
80/tcp    open     http          Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
82/tcp    filtered xfer
111/tcp   filtered rpcbind
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1025/tcp  filtered NFS-or-IIS
1080/tcp  filtered socks
1433/tcp  filtered ms-sql-s
1434/tcp  filtered ms-sql-m
2967/tcp  filtered symantec-av
4444/tcp  filtered krb524
4662/tcp  filtered edonkey
4899/tcp  filtered radmin
5000/tcp  filtered upnp
5002/tcp  filtered rfe
5555/tcp  filtered freeciv
6000/tcp  filtered X11
6001/tcp  filtered X11:1
6002/tcp  filtered X11:2
6129/tcp  filtered unknown
9898/tcp  filtered monkeycom
9929/tcp  open     nping-echo    Nping echo
31337/tcp open     tcpwrapped
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.4
Network Distance: 15 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 554/tcp)
HOP RTT       ADDRESS
1   0.00 ms   163.180.116.1
2   ...
3   16.00 ms  163.180.190.254
4   ... 14
15  163.00 ms 45.33.32.156

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.62 seconds
```

- 5. 방화벽 보호 여부 확인 : -sA



```
$ nmap -sA 172.16.9.1

$ nmap -sA scanme.nmap.org
```

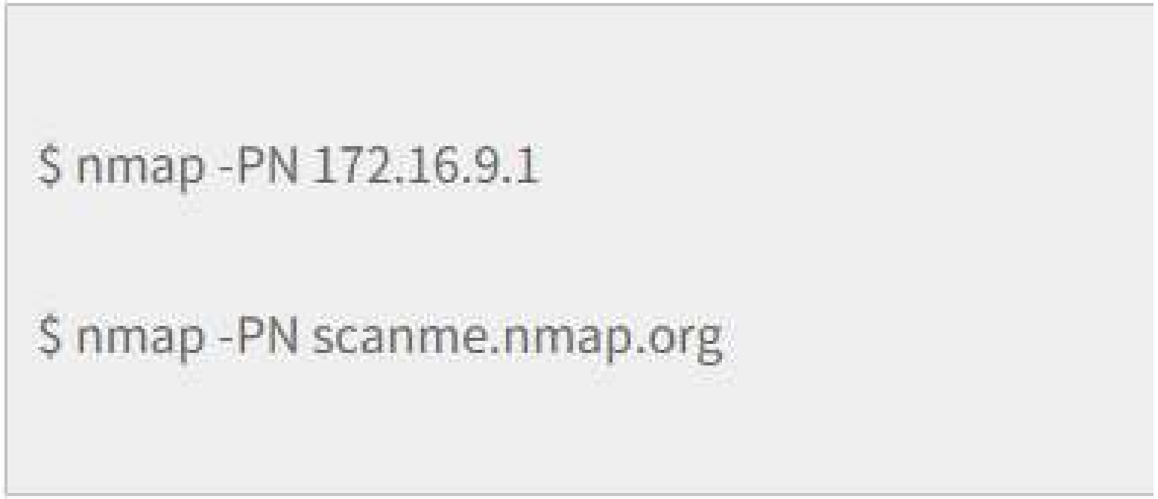


```
C:₩Users₩user>nmap -sA scanme.nmap.org

Starting Nmap 7.12 ( https://nmap.org ) a
mass_dns: warning: Unable to determine an
 servers with --dns-servers
Nmap scan report for scanme.nmap.org (45.
Host is up (0.15s latency).
Not shown: 978 unfiltered ports
PORT      STATE    SERVICE
25/tcp    filtered smtp
82/tcp    filtered xfer
111/tcp   filtered rpcbind
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1025/tcp  filtered NFS-or-IIS
1080/tcp  filtered socks
1433/tcp  filtered ms-sql-s
1434/tcp  filtered ms-sql-m
2967/tcp  filtered symantec-av
4444/tcp  filtered krb524
4662/tcp  filtered edonkey
4899/tcp  filtered radmin
5000/tcp  filtered upnp
5002/tcp  filtered rfe
5555/tcp  filtered freeciv
6000/tcp  filtered X11
6001/tcp  filtered X11:1
6002/tcp  filtered X11:2
6129/tcp  filtered unknown
9898/tcp  filtered monkeycom
```

- filtered : 방화벽에 의해 필터링 되어 open/close 를 알 수 없는 상태

사용 방법

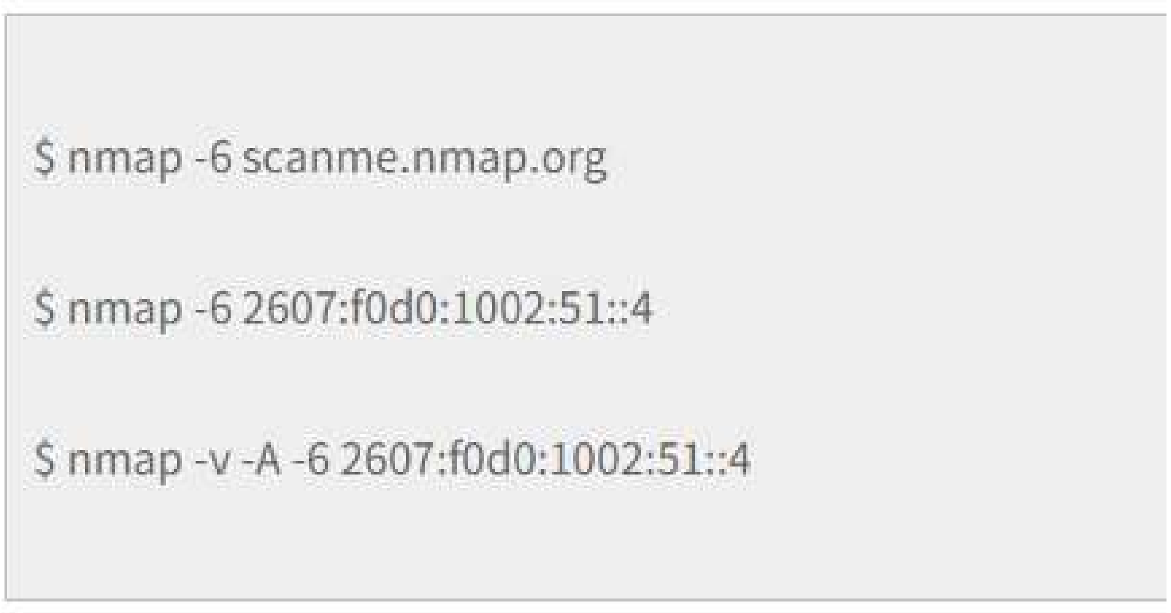
- 6. 핑 테스트를 건너뛴다.(시간과 은닉의 장점을 추구): -PN



```
$ nmap -PN 172.16.9.1

$ nmap -PN scanme.nmap.org
```

사용 방법

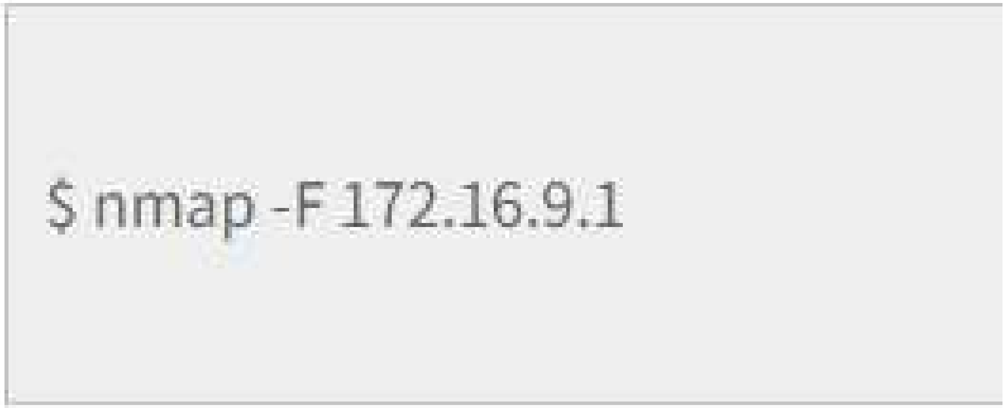
- 7. ipv6 호스트 스캔 : -6



```
$ nmap -6 scanme.nmap.org

$ nmap -6 2607:f0d0:1002:51::4

$ nmap -v -A -6 2607:f0d0:1002:51::4
```

사용 방법

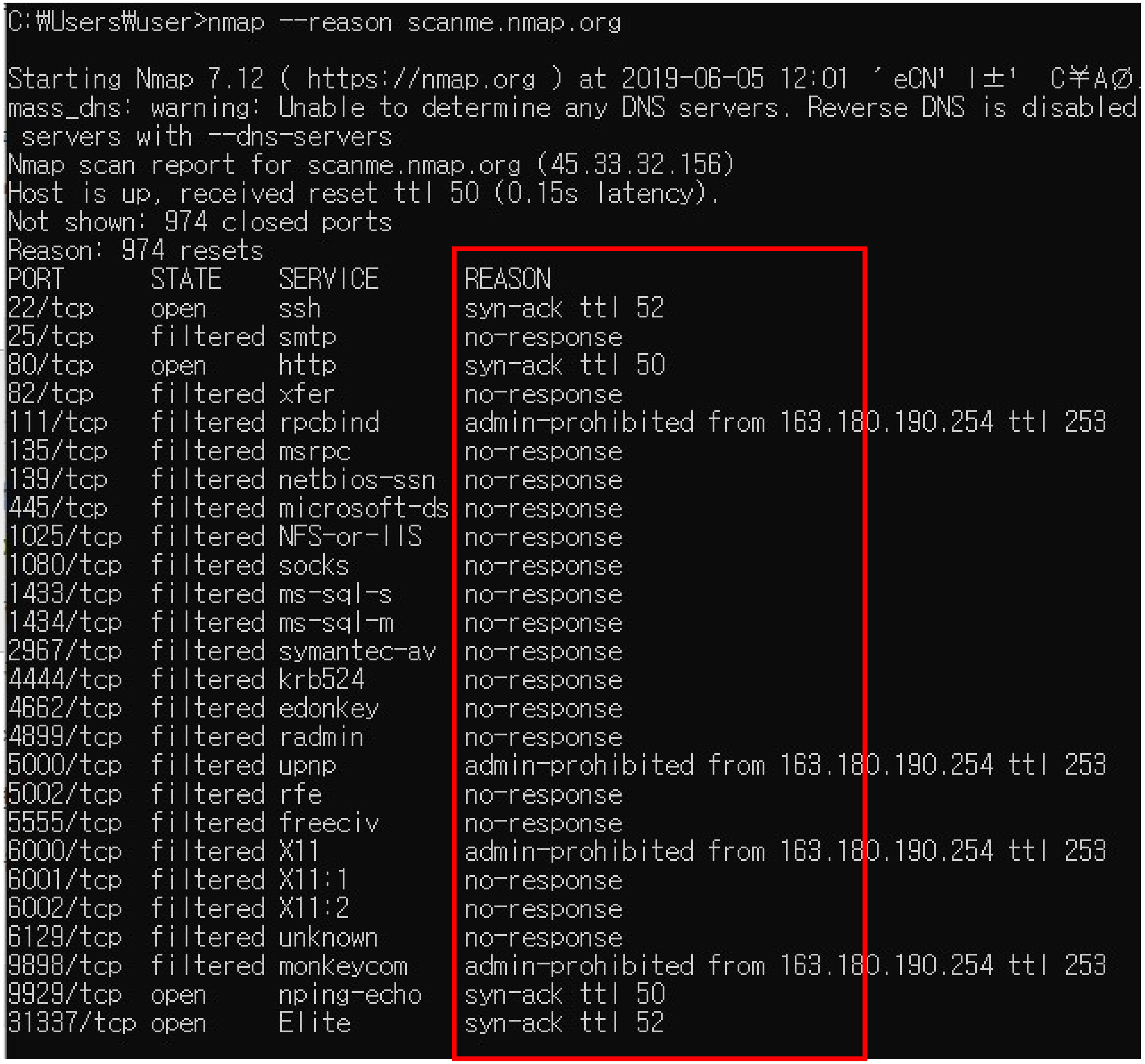
- 8. 빠른 스캔 : -F
  - 탐색 포트 수 1000 -> 100개



```
$ nmap -F 172.16.9.1
```

- 9. 포트 상태 원인 탐색 : --reason

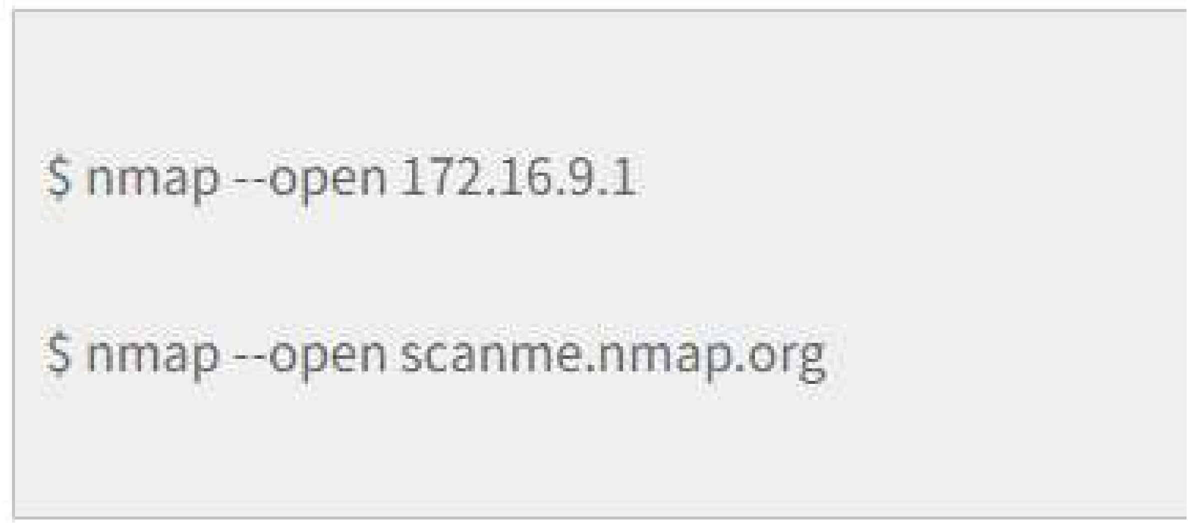
```
$ nmap --reason 172.16.9.1

$ nmap --reason scanme.nmap.org
```



```
C:\Users\user>nmap --reason scanme.nmap.org

Starting Nmap 7.12 ( https://nmap.org ) at 2019-06-05 12:01 ´eCN' |±¹  C¥AØ.
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled
 servers with --dns-servers
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received reset ttl 50 (0.15s latency).
Not shown: 974 closed ports
Reason: 974 resets
PORT      STATE    SERVICE        REASON
22/tcp    open     ssh            syn-ack ttl 52
25/tcp    filtered smtp           no-response
80/tcp    open     http           syn-ack ttl 50
82/tcp    filtered xfer           no-response
111/tcp   filtered rpcbind        admin-prohibited from 163.180.190.254 ttl 253
135/tcp   filtered msrpc          no-response
139/tcp   filtered netbios-ssn    no-response
445/tcp   filtered microsoft-ds   no-response
1025/tcp  filtered NFS-or-IIS     no-response
1080/tcp  filtered socks          no-response
1433/tcp  filtered ms-sql-s       no-response
1434/tcp  filtered ms-sql-m       no-response
2967/tcp  filtered symantec-av    no-response
4444/tcp  filtered krb524         no-response
4662/tcp  filtered edonkey        no-response
4899/tcp  filtered radmin         no-response
5000/tcp  filtered upnp           admin-prohibited from 163.180.190.254 ttl 253
5002/tcp  filtered rfe            no-response
5555/tcp  filtered freeciv        no-response
6000/tcp  filtered X11            admin-prohibited from 163.180.190.254 ttl 253
6001/tcp  filtered X11:1          no-response
6002/tcp  filtered X11:2          no-response
6129/tcp  filtered unknown        no-response
9898/tcp  filtered monkeycom      admin-prohibited from 163.180.190.254 ttl 253
9929/tcp  open     nping-echo     syn-ack ttl 50
31337/tcp open     Elite          syn-ack ttl 52
```

사용 방법

- 10. open 상태 포트만 보이기 : --open



```
$ nmap --open 172.16.9.1

$ nmap --open scanme.nmap.org
```

사용 방법

- 11. open 상태 포트만 보이기 : --packet-trace
  - nmap –packet-trace IP

- 12. 네트워크 인터페이스와 라우트 정보 확인 : -iflist
  - nmap –iflist

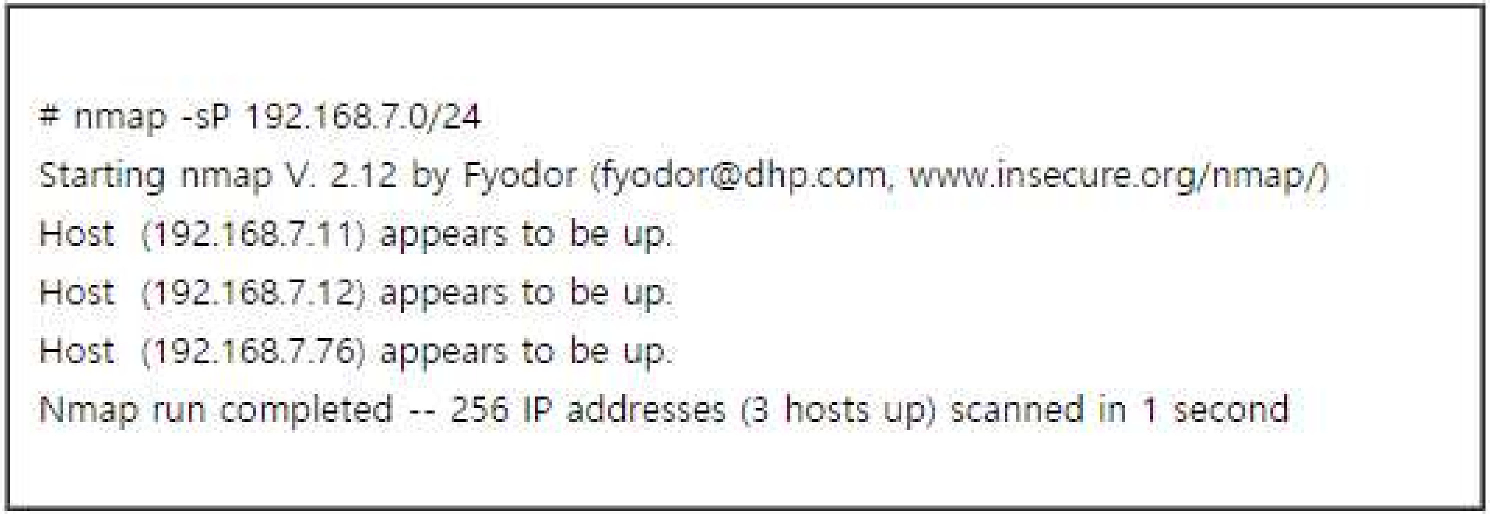
- 13. 특정 포트 스캔 : -p(포트)
  - nmap –p80 IP
  - nmap –p80,100 IP
  - nmap –p80-100 IP
  - nmap –p”*” IP

사용 방법

- 14. 포트 스캔 속도 지정 : -T(0~5)
  - 0(저속) – 5(고속)
  - nmap –T5 IP
- 15. 운영체제 탐지 기능 활성화 : -O
  - nmap –O IP
  - nmap –O –osscan-guess IP
- Etc…
  - http://sisiblog.tistory.com/21

사용 방법

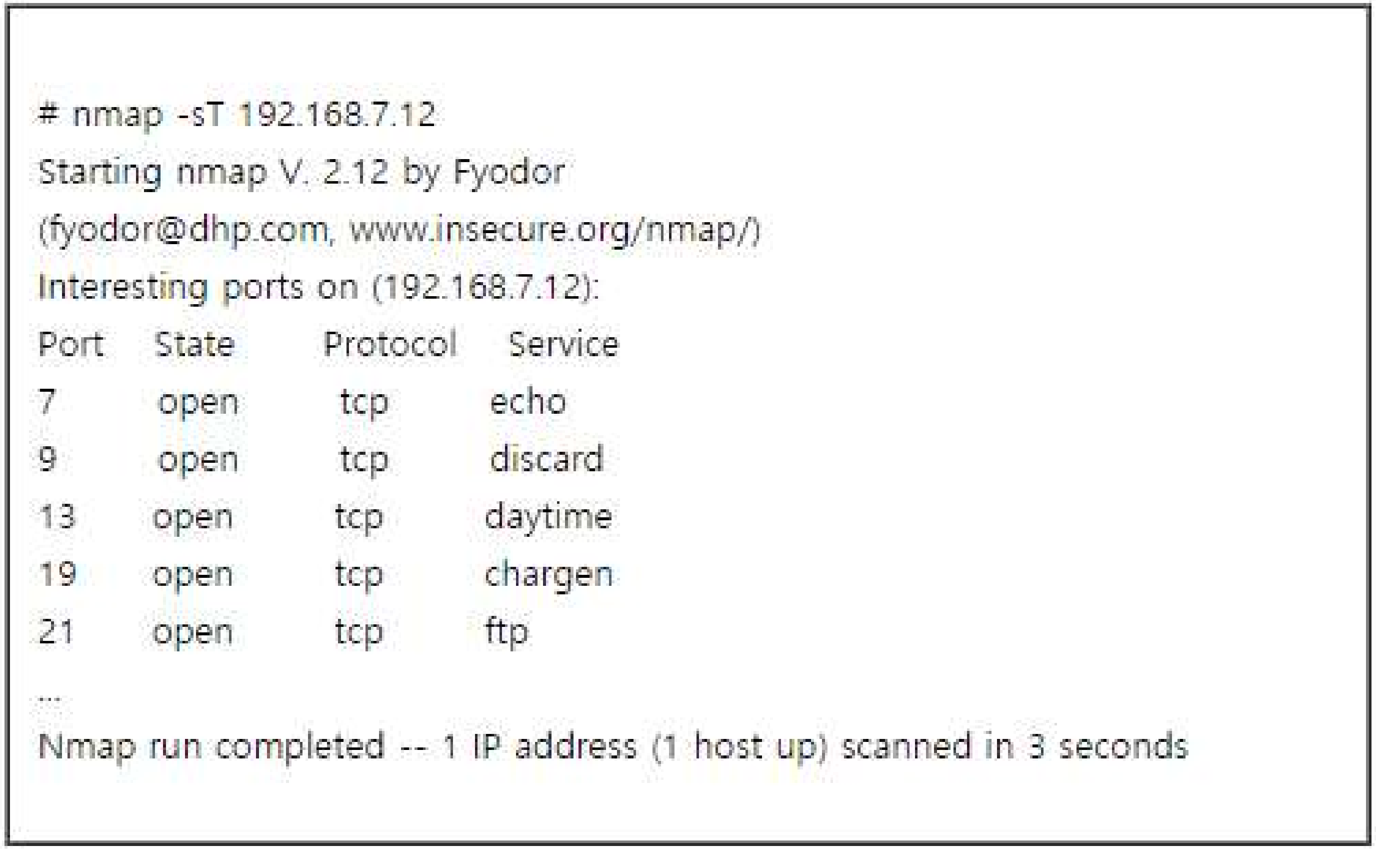
- Ping sweeping : -sP



```
# nmap -sP 192.168.7.0/24
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Host  (192.168.7.11) appears to be up.
Host  (192.168.7.12) appears to be up.
Host  (192.168.7.76) appears to be up.
Nmap run completed -- 256 IP addresses (3 hosts up) scanned in 1 second
```

사용 방법

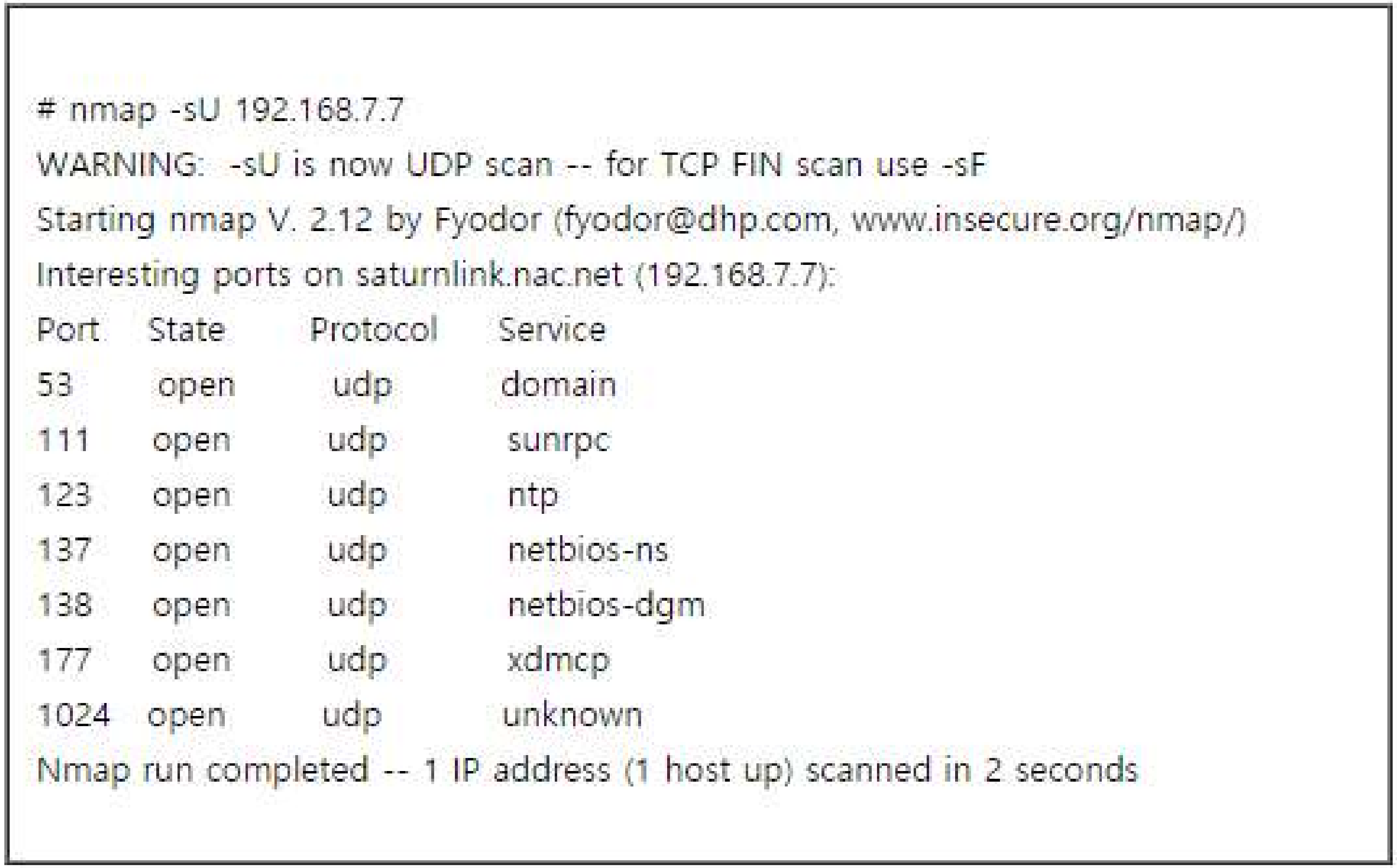
- Port scanning : -sT (TCP)



```
# nmap -sT 192.168.7.12
Starting nmap V. 2.12 by Fyodor
(fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on (192.168.7.12):
Port    State       Protocol    Service
7        open        tcp         echo
9        open        tcp         discard
13      open        tcp         daytime
19      open        tcp         chargen
21      open        tcp         ftp
...
Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds
```

사용 방법

- Port scanning : -sU (UDP)



```
# nmap -sU 192.168.7.7
WARNING:  -sU is now UDP scan -- for TCP FIN scan use -sF
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on saturnlink.nac.net (192.168.7.7):
Port    State       Protocol     Service
53       open        udp         domain
111     open        udp          sunrpc
123     open        udp          ntp
137     open        udp          netbios-ns
138     open        udp          netbios-dgm
177     open        udp          xdmcp
1024   open        udp          unknown
Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```