Nmap을 활용한 포트 스캔

Nmap

- Nmap은 Network Mapper의 약자
- 네트워크 검색 및 보안 감사를 위한 무료 오픈 소스(라이선스) 유틸리티
- 네트워크에서 사용할 수 있는 호스트, 해당 호스트가 제공하는 서비스(애플리케이션 이름 및 버전), 실행 중인 운영체제(및 OS 버전), 사용 중인 패킷 필터/방화벽 및 기타 수십 가지 특성 파악 가능
- 포트 스캔 도구 역할로 침투 테스트의 정보 수집 단계에서 가장 많이 활용
- 스크립트를 활용하면 NFS, SMB, RPC 등의 상세한 서비스 정보들을 수집할 수 있으며, 도메인 lookup, Whois 검색, 다른 네트워크 대역 서버의 백도어 설치 여부, 취약점 여부 등 많은 작업을 수행

Nmap: the Network Mapper - Free Security Scanner

Nmap Free Security Scanner, Port Scanner, & Network Exploration Tool. Download open source software for Linux, Windows, UNIX, FreeBSD, etc.

https://nmap.org/

Nmap 옵션

옵션	설명
-p <port ranges>	지정된 포트만 검색 예) -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
-p-	모든 포트 검색 (1~65535, 포트 0은 검색되지 않음)
--exclude-ports <port ranges>	지정된 포트를 제외하고 검색 예) --exclude-ports 22; --exclude-ports 80-100;
-sS	TCP SYN 스캔으로 Stealth 스캔이라고도 불림(기본 옵션)
-sT	기본 옵션으로 TCP Connect() 스캔
-sV	열린 포트를 조사하여 서비스/버전 정보 확인
-O	운영체제 탐지 활성화
-A	운영체제 탐지, 버전 탐지, 스크립트 스캐닝 및 traceroute 사용
-T<0-5>	타이밍 템플릿 설정으로 숫자가 높을수록 빠름
-oX <file>	주어진 파일 이름에 대해 XML 형태로 결과 출력
-d	스크립트 진행 상세 내역 모니터링 가능
-dd	더욱더 상세 내역 모니터링 가능
-oX	XML 타입의 출력 스캔을 주어진 파일 이름으로 출력
--packet-trace	주고 받은 모든 패킷 표시
--script-trace	주고 받은 데이터 표시(NSE 스크립트를 지정해야 사용 가능)
-v	스캔하는 자세한 정보를 표시(더 자세한 정보는 -vv 사용)

기본 포트 설정된 것 1000개를 스캔

```
┌──(kali㉿kali)-[~] └─$ sudo nmap 192.168.81.130 [sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 03:18 EDT Nmap scan
report for 192.168.81.130 Host is up (0.0019s latency). Not shown: 977
closed tcp ports (reset) PORT STATE SERVICE 21/tcp open ftp 22/tcp open
ssh 23/tcp open telnet 25/tcp open smtp 53/tcp open domain 80/tcp open
http 111/tcp open rpcbind 139/tcp open netbios-ssn 445/tcp open microsoft-
ds 512/tcp open exec 513/tcp open login 514/tcp open shell 1099/tcp open
rmiregistry
```

-p- 옵션은 전체 포트 스

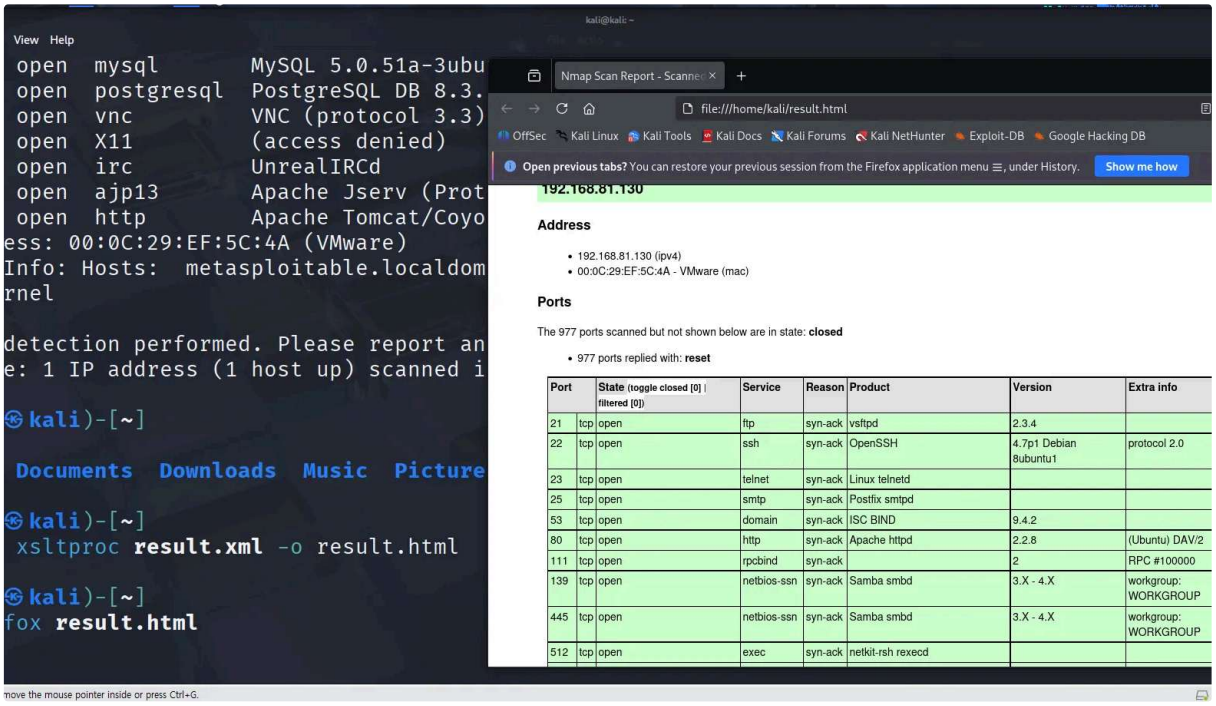
```
┌──(kali㉿kali)-[~] └─$ sudo nmap 192.168.81.130 -p- [sudo] password for kali: Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 03:29 EDT Nmap scan report for 192.168.81.130 Host is up (0.0033s latency). Not shown: 65505 closed tcp ports (reset) PORT STATE SERVICE 21/tcp open ftp 22/tcp open ssh 23/tcp open telnet 25/tcp open smtp 53/tcp open domain 80/tcp open http 111/tcp open rpcbind 139/tcp open netbios-ssn 445/tcp open microsoft-ds 512/tcp open exec 513/tcp open login
```

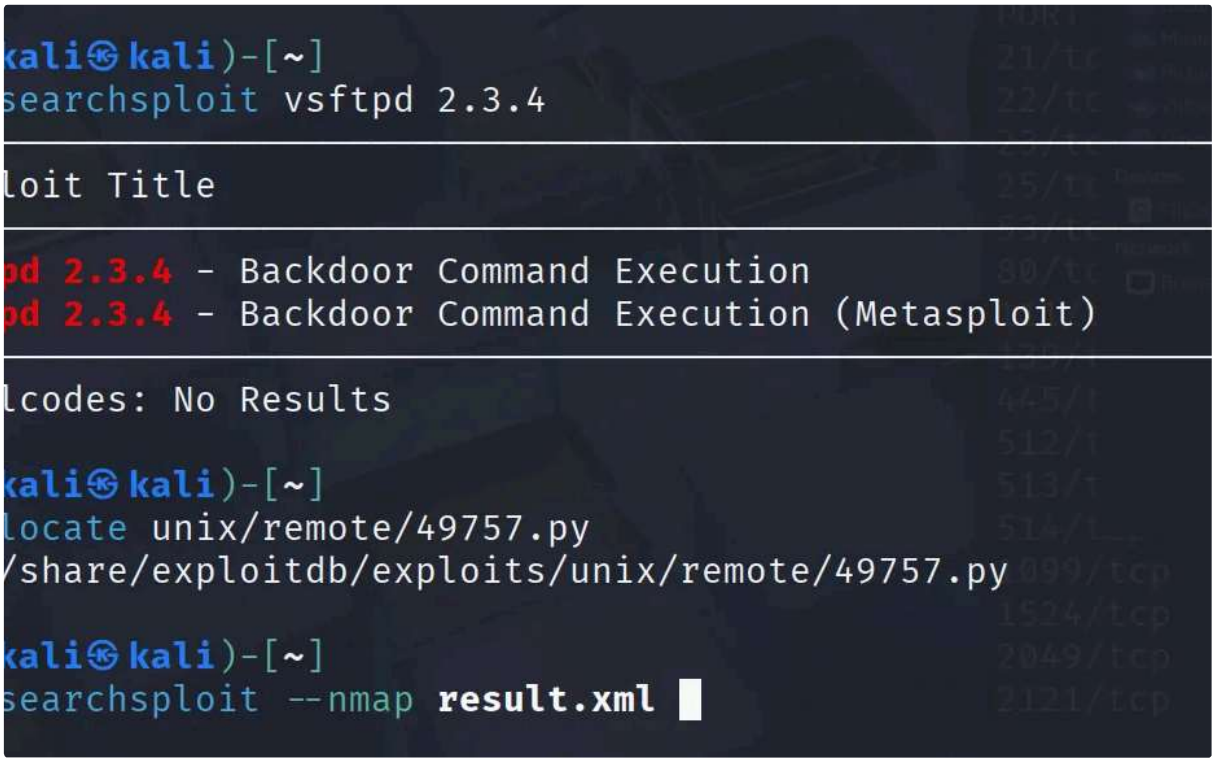
192.168.81.0/24 대역 0~254 IP 대역 전체로 포트 1-1000까지 스캔

```
┌──(kali㉿kali)-[~] └─$ sudo nmap 192.168.81.0/24 -p1-1000 Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 03:31 EDT Nmap scan report for 192.168.81.1 Host is up (0.00054s latency). Not shown: 997 filtered tcp ports (no-response) PORT STATE SERVICE 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds MAC Address: 00:50:56:C0:00:08 (VMware) Nmap scan report for 192.168.81.2 Host is up (0.00018s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 53/tcp open domain MAC Address: 00:50:56:E1:0B:79 (VMware) Nmap scan report for 192.168.81.130 Host is up (0.0021s latency). Not shown: 988 closed tcp ports (reset) PORT STATE SERVICE
```

-sV 옵션으로 버전 정보까지 포함하고, -oX 옵션으로 xml 형태로 저

```
┌──(kali㉿kali)-[~] └─$ sudo nmap -sV 192.168.81.130 -oX result.xml Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 03:56 EDT Nmap scan report for 192.168.81.130 Host is up (0.0023s latency). Not shown: 977 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 2.3.4 22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) 23/tcp open telnet Linux telnetd 25/tcp open smtp Postfix smtpd 53/tcp open domain ISC BIND 9.4.2 80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2) 111/tcp open rpcbind 2 (RPC #100000) 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 512/tcp open exec netkit-rsh rexecd 513/tcp open login 514/tcp open tcpwrapped 1099/tcp open java-rmi GNU Classpath grmiregistry 1524/tcp open bindshell Metasploitable root shell
```


View Help
open mysql MySQL 5.0.51a-3ubu
open postgresql PostgreSQL DB 8.3.
open vnc VNC (protocol 3.3)
open X11 (access denied)
open irc UnrealIRCd
open ajp13 Apache Jserv (Prot
open http Apache Tomcat/Coyo
ess: 00:0C:29:EF:5C:4A (VMware)
Info: Hosts: metasploitable.localdom
rnel
detection performed. Please report an
e: 1 IP address (1 host up) scanned i
kali)-[~]
Documents Downloads Music Picture
kali)-[~]
xsltproc result.xml -o result.html
kali)-[~]
fox result.html
Nmap Scan Report - Scanned
file:///home/kali/result.html
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Open previous tabs? You can restore your previous session from the Firefox application menu, under History.
Show me how
192.168.81.130
Address
192.168.81.130 (ipv4)
00:0C:29:EF:5C:4A - VMware (mac)
Ports
The 977 ports scanned but not shown below are in state: closed
977 ports replied with: reset
Port State (toggle closed [0] | filtered [0]) Service Reason Product Version Extra info
21 tcp open ftp syn-ack vsftpd 2.3.4
22 tcp open ssh syn-ack OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
23 tcp open telnet syn-ack Linux telnetd
25 tcp open smtp syn-ack Postfix smtpd
53 tcp open domain syn-ack ISC BIND 9.4.2
80 tcp open http syn-ack Apache httpd 2.2.8 (Ubuntu) DAV/2
111 tcp open rpcbind syn-ack 2 RPC #100000
139 tcp open netbios-ssn syn-ack Samba smbd 3.X - 4.X workgroup: WORKGROUP
445 tcp open netbios-ssn syn-ack Samba smbd 3.X - 4.X workgroup: WORKGROUP
512 tcp open exec syn-ack netkit-rsh rexecd
move the mouse pointer inside or press Ctrl+G.


kali)-[~]
searchsploit vsftpd 2.3.4
loit Title
pd 2.3.4 - Backdoor Command Execution
pd 2.3.4 - Backdoor Command Execution (Metasploit)
lcodes: No Results
kali)-[~]
locate unix/remote/49757.py
/share/exploitdb/exploits/unix/remote/49757.py
kali)-[~]
searchsploit --nmap result.xml

```
┌──(kali㉿kali)-[~] └─$ cd /usr/share/nmap/scripts ┌──(kali㉿kali)-[/usr/share/nmap/scripts] └─$ ls -al | more total 5040 drwxr-xr-x 2 root root 32768 May 29 15:13 . drwxr-xr-x 4 root root 4096 May 29 15:13 .. -rw-r--r-- 1 root root 3901 May 15 11:37 acarsd-info.nse -rw-r--r-- 1 root root 8749 May 15 11:37 address-info.nse -rw-r--r-- 1 root root 3345 May 15 11:37 afp-brute.nse -rw-r--r-- 1 root root 6463 May 15 11:37 afp-ls.nse -rw-r--r-- 1 root root 7001 May 15 11:37 afp-path-vuln.nse -rw-r--r-- 1 root root 5600 May 15 11:37 afp-serverinfo.nse -rw-r--r-- 1 root root 2621 May 15 11:37 afp-showmount.nse -rw-r--r-- 1 root root 2262 May 15 11:37 ajp-auth.nse -rw-r--r-- 1 root root 2983 May 15 11:37 ajp-brute.nse -rw-r--r-- 1 root root 1329 May 15 11:37 ajp-headers.nse -rw-r--r-- 1 root root 2590 May 15 11:37 ajp-methods.nse -rw-r--r-- 1 root root 3051 May 15 11:37 ajp-request.nse -rw-r--r-- 1 root root 6719 May 15 11:37 allseeingeye-info.nse -rw-r--r-- 1 root root 1678 May 15 11:37 amqp-info.nse -rw-r--r-- 1 root root 15024 May 15 11:37 asn-query.nse
```

전체 vuln 스크립트 사례

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts] └─$ sudo nmap -sV --script=vuln
192.168.81.130 Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 20:47
EDT Pre-scan script results: | broadcast-avahi-dos: | Discovered hosts: |
224.0.0.251 | After NULL UDP avahi packet DoS (CVE-2011-1002). Not shown:
977 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp
vsftpd 2.3.4 | vulners: | vsftpd 2.3.4: | PACKETSTORM:162145 10.0
https://vulners.com/packetstorm/PACKETSTORM:162145 *EXPLOIT* | EDB-
ID:49757 10.0 https://vulners.com/exploitdb/EDB-ID:49757 *EXPLOIT* | CVE-
2011-2523 10.0 https://vulners.com/cve/CVE-2011-2523 |_ 1337DAY-ID-36095
9.8 https://vulners.com/zdt/1337DAY-ID-36095 *EXPLOIT* | ftp-vsftpd-
backdoor: | VULNERABLE: | vsFTPd version 2.3.4 backdoor | State:
VULNERABLE (Exploitable) | IDs: BID:48539 CVE:CVE-2011-2523 | vsFTPd
version 2.3.4 backdoor, this was reported on 2011-07-04. | Disclosure
date: 2011-07-03 | Exploit results: | Shell command: id | Results:
uid=0(root) gid=0(root) | References: |
https://github.com/rapid7/metasploit-
framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb |
https://www.securityfocus.com/bid/48539 | https://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2011-2523 |_
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-
backdoored.html 22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol
2.0) .....
```