Nmap 명령어 정리

Nmap이란?

- nmap은 네트워크 보안을 위한 유틸리티 도구로, 대규모 네트워크를 고속으로 스캔하는 Port Scanning 도구이다.
    - 네트워크에 어떤 호스트가 살아있는지, 어떤 포트를 사용하는지, 운영체제가 뭔지 등 네트워크의 수 많은 특징을 점검할 수 있다.
        - 특히나 방화벽이 오픈되어 있는지의 여부를 확인할 수 있다.

사용법

- nmap <옵션> 호스트
    - -sT : TCP Open Scan
    - -sS : TCP half open Scan (TCP SYN Scan) (세션을 성립하지 않는다. (스텔스 스캔))
    - -sF : TCP FIN Scan (FIN 패킷을 이용한 스캔)
    - -sN : TCP NULL Scan (NULL 패킷을 이용한 스캔)
    - -sX : TCP Xmas Scan (FIN, PSH, URG 패킷을 이용한 스캔)
    - -sP : ping을 이용한 스캔
    - -sA : : ACK 패킷에 대한 TTL 값을 분석한다. (방화벽 규칙 상태 확인 시 사용한다.)
    - -sW : 윈도우 스캔은 ACK 스캔과 같은데, 특정 장치에 대해 열린 혹은 닫힌 포트를 구별한다.
    - -sI : Idel 스캔으로 가장 은밀한 스캔이며, 느리고 복잡하다.
    - -sL : 목록 스캔 (서버가 살아있는지 죽었는지 확인하는 가장 좋은 방법이다.)
    - -sU : UDP Port Scan
    - -O : 대상 호스트의 운영체제 판별
    - -o : 스캔 결과를 텍스트 파일로 저장
    - -F : Fast Scan

- -sV : service version
- -p : 포트 선택
- -h : nmap의 옵션들을 확인한다.
- -v : 출력을 자세하게 한다.
- -w : -v보다 더 자세하게 출력을 한다.
- -oN <File명> : 일반 형식으로 파일을 출력한다.
- -oX <File명> : XML 파일 형식으로 출력한다.
- -PS : TCP SYN 패킷을 보낸다. (SYN → SYN, ACK → RST)
- -PA : TCP ACK 패킷을 보낸다. (위의 -PS와 비슷하지만, 방화벽을 우회하기 위해 ACK를 보낸다.)
- -PU : UDP Ping, 빈 UDP 패킷을 해당 포트에 보낸다. (TCP 필터링을 피해간다.)
- -PO : IP Protocol Ping, ICMP, IGMP, IP 패킷을 이용한 스캔이다.
- -PR : ARP 스캔

ex) 호스트의 특정 포트가 열려있는지 확인하는 방법

```
nmap -PN 111.222.333.444 -p 8000    # nmap -PN <IP> -p <PORT>
```

ex) 네트워크 전체를 스캔

```
nmap 192.168.1.*/16
```

ex) 해당 호스트의 정보를 조금 더 자세하게 보여준다.

```
nmap -v 192.168.1.*
```

ex) 192.168.1.*가 살아있는지 스캔한다.

```
nmap -sp 192.168.1.*
```

ex) 192.168..1.200의 1번부터 20000번까지 RPC 포트를 찾는다.

```
nmap -sR -p 1-20000 192.168.1.200
```