**NMAP**

NMAP is port scan tools. The basic process is send SYN Packet to target server. Some nmap option is required root privileges so it must run the root user or sudo.

Nmap has variable options and you can combined it. Basically, nmap is work port based. That is mean might be result isn’t match the real service. The Web Service default port is TCP 80. But if changed the other port like TCP 21, nmap is show TCP 21 is opend and service FTP. -sV option is solve this problem. That option is need more time for scan but the you can see the more correctly output.

Frequently used nmap options

\*이하 공부 내용을 모두 영어로 적기에는 무리가 있어 우선 한글로 정리함. 추후 영어 공부하면서 다시 수정 예정\*

자주 사용되는 옵션 중에서도 공격에 있어서 실질적으로 유용하다고 판단되는 것을 위주로 작성하였다.

-sS : 기본 동작의 경우 Threeway-Handshake를 모두 수행하기에 target server에 access log가 남게 된다. 그러나 이 옵션을 사용하면 Stealth Scan 즉, TCP half-open scan을 수행하기 때문에 처음 SYN 패킷을 전송한 후 SYN/ACK 응답이 돌아왔을 경우 RST 패킷을 전송하여 Session이 성립되기 이전에 연결을 해제한다. 따라서 TCP Session이 성립되지 않았기에 target server에도 log가 남지 않게 되어 Stealth scan이라고 불린다.

-sN : TCP Null Scan으로 모든 flag를 unset으로 지정함으로써 해당 port가 closed일 경우 RST/ACK 패킷이 돌아오는 것을 이용한 스캔

-sF, -sX : -sF의 경우 TCP FIN Scan, -sX의 경우 XMAS Scan으로 XMAS는 FIN, URG, PSH Flag를 set 하여 port status를 확인한다. Scan 방식의 경우 TCP Null Scan과 같은 mechanism으로 동작한다.

--scanflags <flags>를 통해 직접 사용할 flag를 지정할 수도 있다.

-sA : ACK flag를 set하여 패킷을 전송한다. 주로 방화벽의 규칙을 찾아내기 위해 사용하는 옵션이기에 port의 open, closed와 같은 status는 이를 통해 알 수가 없다.

-D RND:<num> : nmap을 이용하여 scan을 진행하면 같은 주소로부터 반복적인 TCP 접근이 이루어지기에 의심을 받기 쉬워진다. 따라서 이 옵션을 사용하면 num에서 지정한 수 만큼의 random한 IP를 생성하여 총 num+자신의 IP 주소로 패킷을 보내게 된다. 여기서 생성되는 Random IP의 경우 대역도 모두 다르게 생성된다.

-v : 흔히 있는 verbose 옵션이다.

-p : Scan할 port를 지정할 수 있다. 지정하지 않을 경우 기본적으로 1000개의 port를 target으로 한다. 근데 실제로 지정하지 않고 해보면 8000번 대의 port도 scan이 되는데 이를 보면 순차적으로 1000개가 아닌 것 같기도… 이 부분은 추후에 알아봐야 할 것 같다.

-T <0-5> : scan의 속도를 지정할 수 있다. 높게 지정할 수록 더 빠르게 scan을 진행하며 기본적으로 5의 속도로 진행된다. 이 옵션의 경우 IDS와 같은 장비로부터 탐지를 회피하기 위해 사용한다. 빠른 시간내에 반복적인 패킷이 들어오면 의심되기 때문이다. 혹은 느린 회선을 target으로 할때도 마찬가지다.

-g : source port를 지정할 수 있다. 이를 지정하지 않고 nmap을 실행하면 well known port가 아닌 randomized port 하나가 선정되어 해당 포트를 통해 스캔을 시도한다. 이러한 경우도 port scan으로 의심되기에 좋기 때문에 -g option을 통해 특정 service의 포트를 이용해 마치 service인 마냥 속일 수 있다.

-oA <basename> : nmap의 scan result를 .nmap, .gnmap, .xml 총 세 가지의 형식으로 저장한다. filename의 경우 basename을 사용한다.