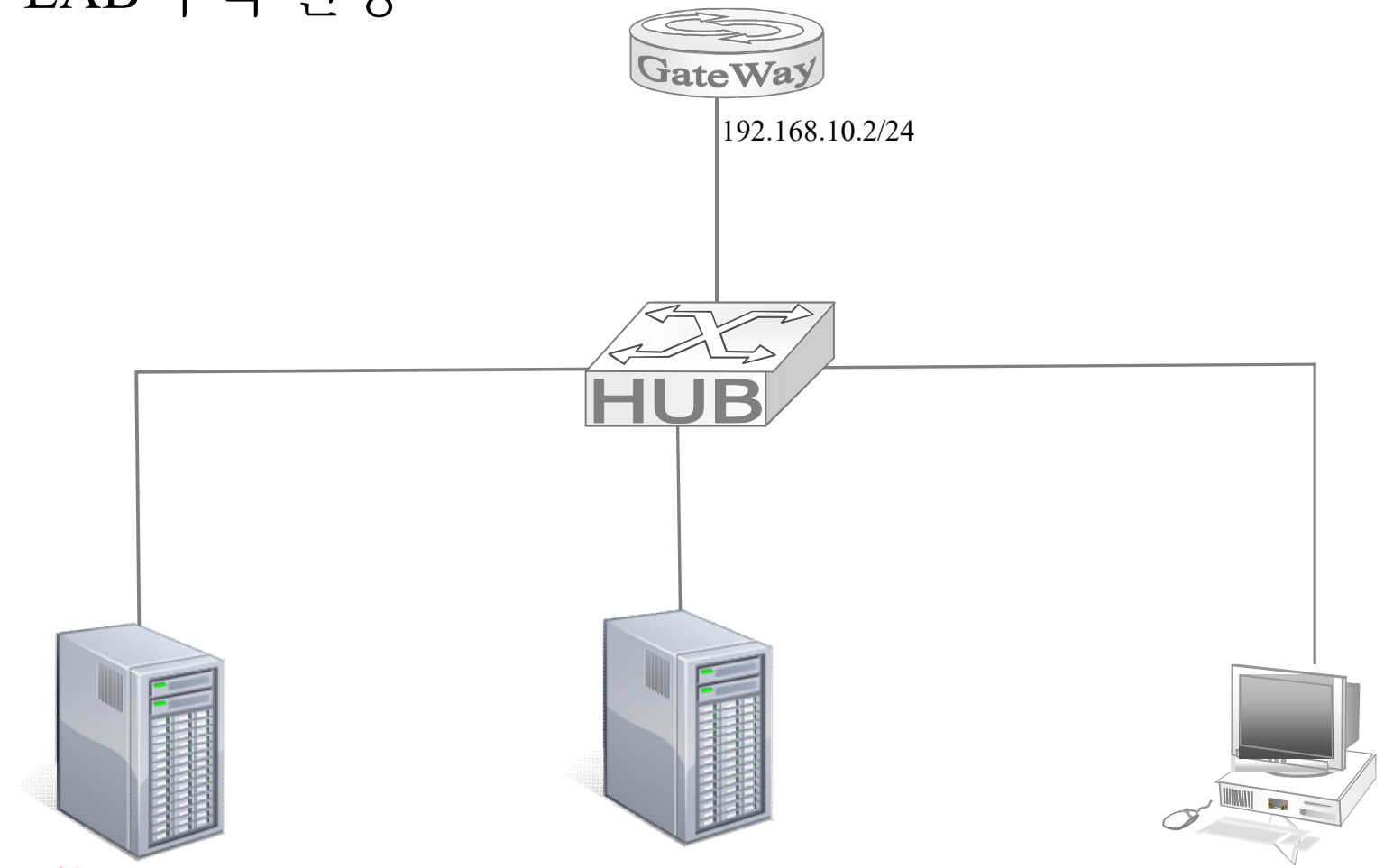
LAB 구축 환경


GateWay
192.168.10.2/24
HUB
KaliAttacker
192.168.10.10/24
Metaspolitable(target)
192.168.10.20/24
Client
192.168.10.40/24

Metaspolitable (Target)

- ID/Password : msfadmin/msfadmin

$sudo su –

#ifconfg

#cd /etc/network

#vi interfaces

auto eth0

iface eth0 inet static

address 192.168.10.20

network 192.168.10.0

netmask 255.255.255.0

gateway 192.168.10.2

broadcast 192.168.10.255

#ifdown eth0

#ifup eth0

#vi /etc/resolv.conf

nameserver 192.168.10.2

사이버 공격을 위한 준비

풋프린팅 (Foot Printing)	• 신문, 게시판 혹은 포털 검색 등을 이용 • 공격 대상의 IP 대역, DNS/Mail 서버 등의 정보를 수집
스캐닝 (Scanning)	• Ping, Port Scan, 운영체제 확인 등을 이용 • 시스템 종류, IP 주소, 서비스 등 세부적인 정보를 수집
목록화 (Listing)	• 풋프린팅, 스캐닝 방법을 통해 수집된 정보를 기반 • 라우팅 테이블, SNMP 정보 등 실용적인 정보 수집 • 시스템 취약점분석 및 공격 방법을 결정하는 지표를 작성하는 과정

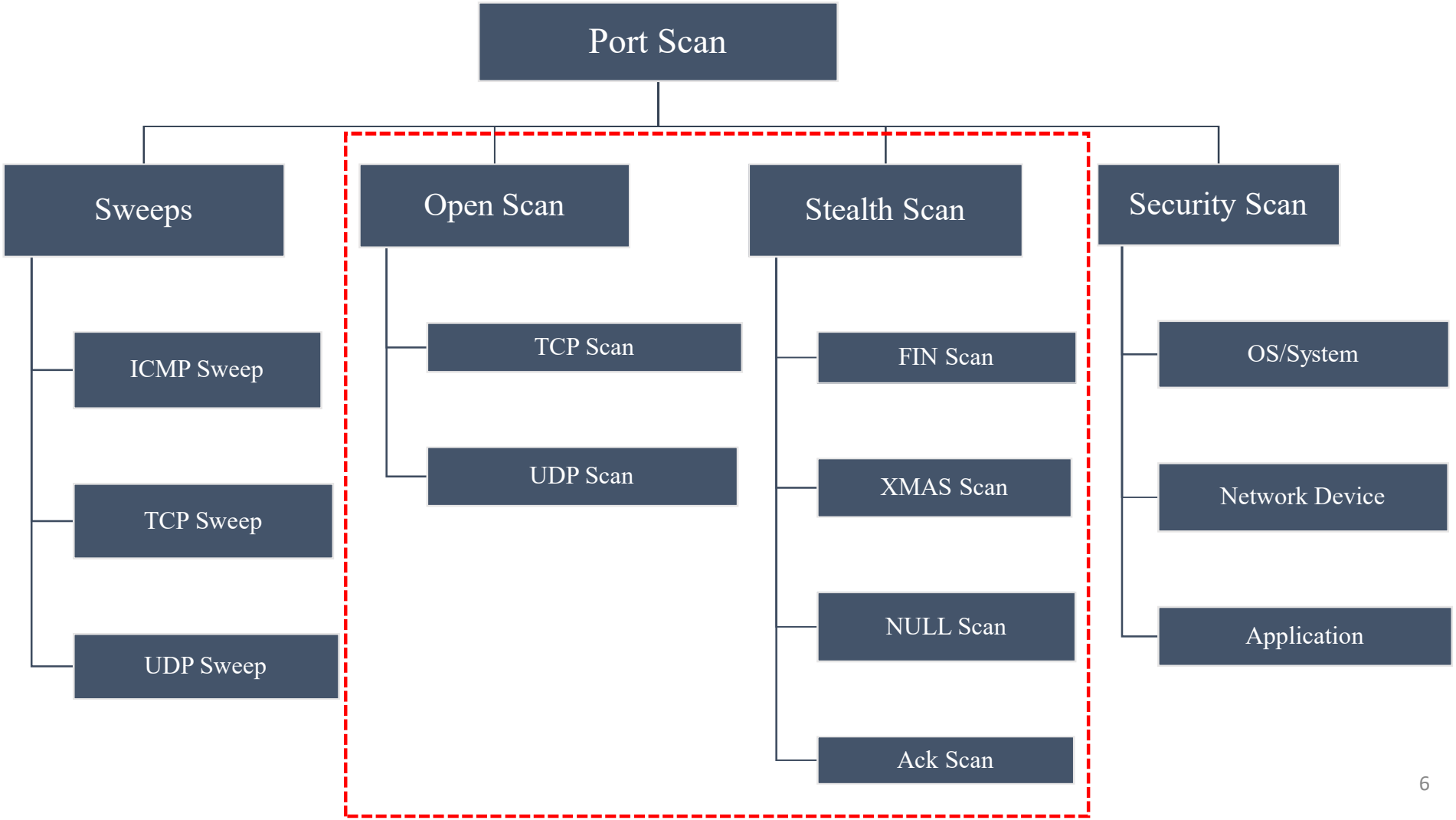
풋프린팅(Foot-printing)

- 공격자가 공격 전에 공격 대상에 대한 다양한 정보를 수집하기 널리 사용하는 방법 중 하나
- 사회공학(social engineering)기법
- 신문, 게시판 혹은 포털 검색 등을 이용
- 공격 대상이 스스로 공개한 여러가지 정보를 풋프린팅하여 공격대상의 정보(사용자 이름, 계정, 전화번호등)들을 수집

포트스캔(Port scan)

- 실제 공격방법을 결정하거나 공격에 이용될 수 있는 네트워크 구조, 시스템이 제공하는 서비스 등의 정보를 얻기 위해 수행되는 방법
  - 공격 대상 보안 장비 사용현황
  - 우회 가능 네트워크 구조
  - 시스템 플랫폼 형태
  - 시스템 운영체제의 커널 버전의 종류
  - 제공 서비스 종류

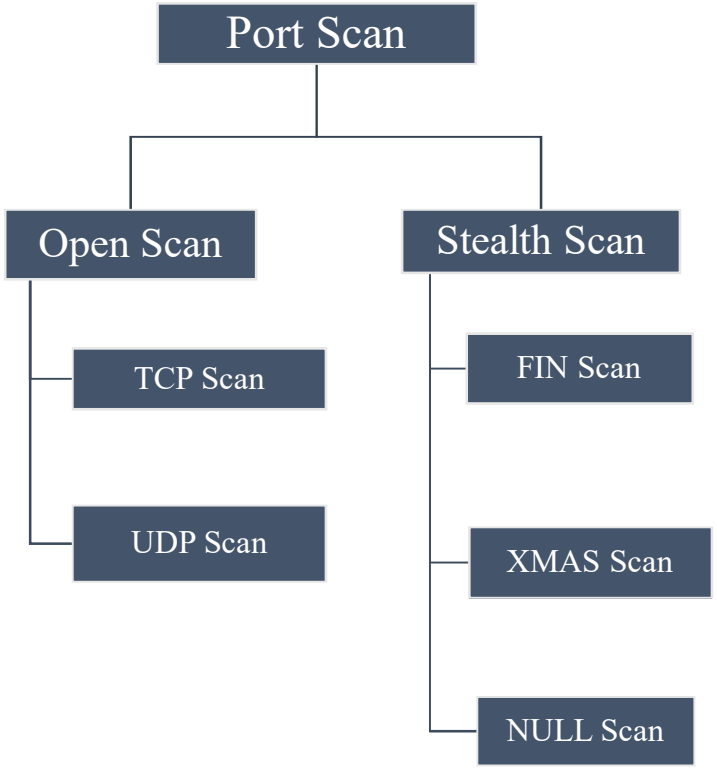
Port Scan 종류


Port Scan
Sweeps
Open Scan
Stealth Scan
Security Scan
ICMP Sweep
TCP Sweep
UDP Sweep
TCP Scan
UDP Scan
FIN Scan
XMAS Scan
NULL Scan
Ack Scan
OS/System
Network Device
Application

Nmap(Network Mapper)

- 스캔 도구
- 운영체제 종류 및 사용 서비스에 대한 정보 스캔도구

스캔 옵션	내 용
-sT	connect( ) 함수를 이용한 Open 스캔
-sS	세션을 성립시키지 않는 TCP syn 스캔
-sF	Fin 패킷을 이용한 스캔
-sN	Null 패킷을 이용한 스캔
-sX	XMas 패킷을 이용한 스캔
-sU	UDP 포트 스캔
-sA	Ack 패킷에 대한 TTL 값의 분석



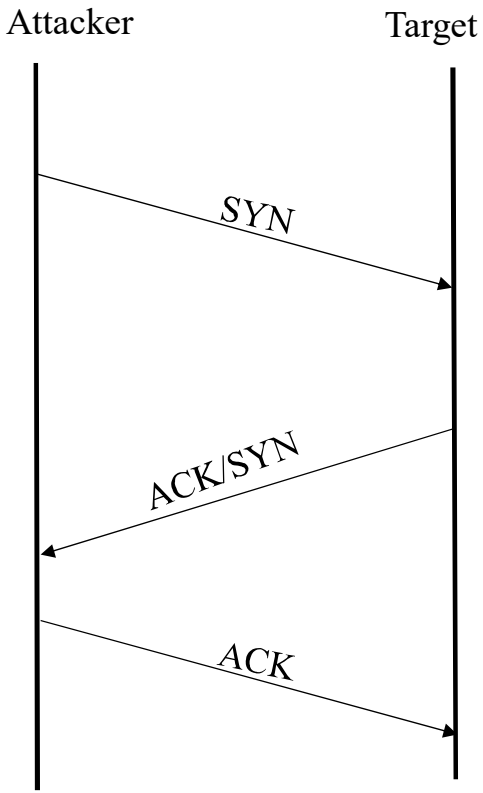
Open Scan

- 시스템 자체의 활성화 여부 확인
- 스캔하는 포트에 해당하는 서비스 활성화 여부 조사
- 포트를 스캔하여 포트가 열려 있다면 해당 시스템이 활성화로 판단
- 종류

  - TCP Open Scan

  - UDP Open Scan

TCP Full Open Scan

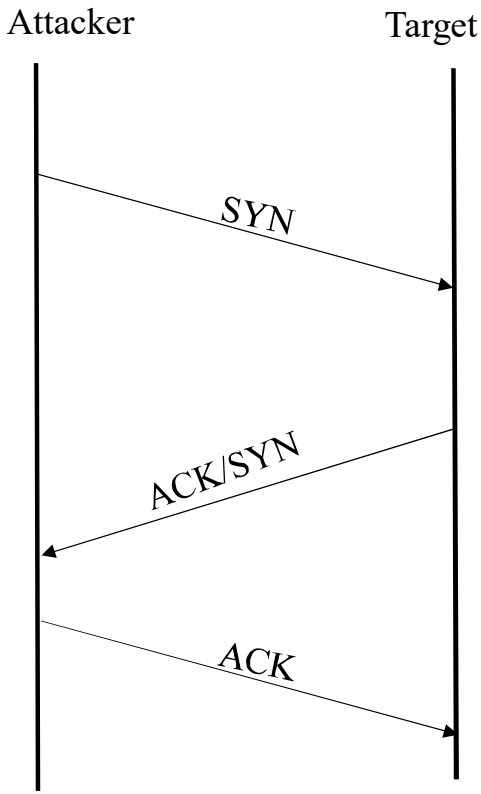


<<열린 포트인 경우 >>

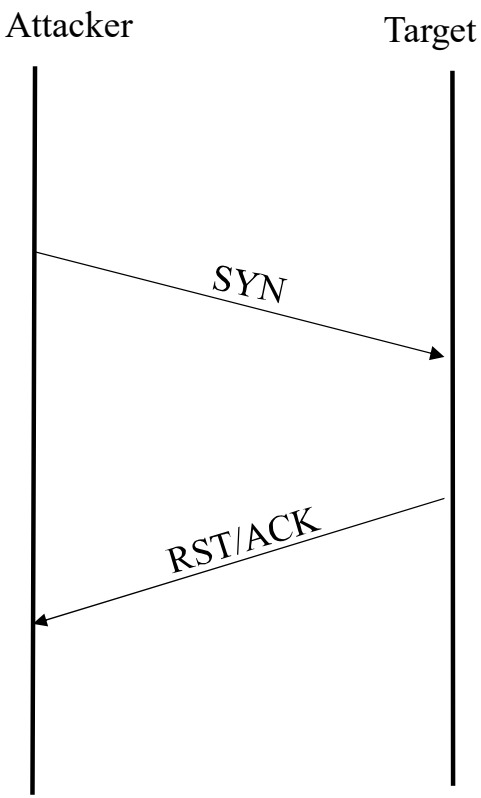
$nmap –sT [대상IP]

- 포트가 열려 있는 경우 SYN/ACK 패킷 수신
- SYN/ACK에 ACK 패킷을 전송함으로써 연결을 완료
- 스캔하고자 하는 포트에 접속을 시도해 완전한 TCP 연결을 맺어 신뢰서 있는 결과 얻음
- 속도가 느리고 로그를 남기므로 탐지가 가능하다는 단점을 가짐

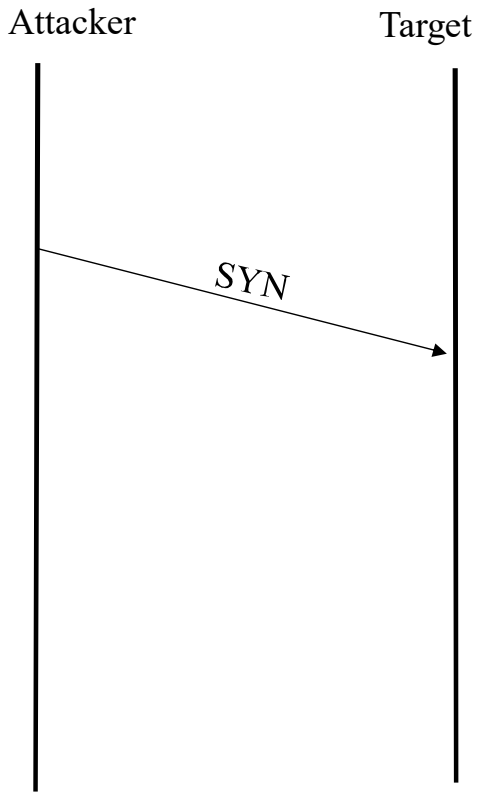
TCP Full Open Scan



<<열린 포트인 경우 >>



<<닫힌 포트인 경우 >>

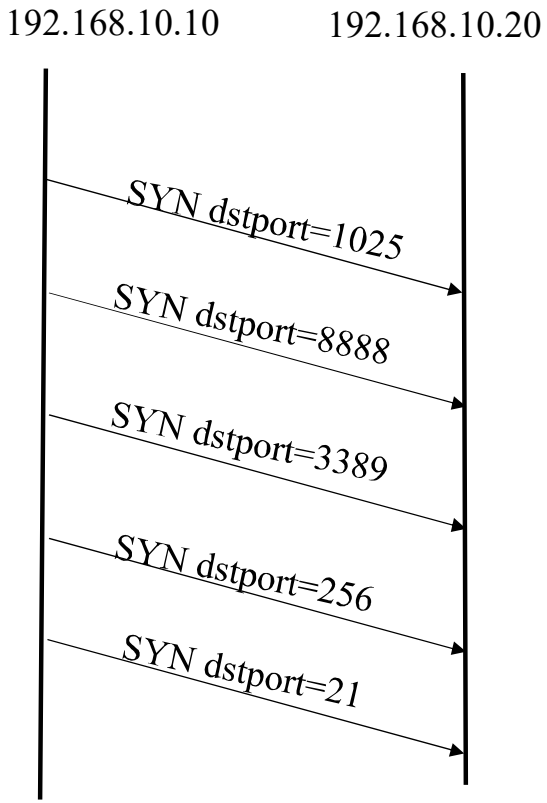


<<차단정책에 의해 차단되어 있는 경우>>

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# nmap -sT 192.168.10.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-12 21:03 EDT
Nmap scan report for 192.168.10.20
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:67:D2:B9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

┌──(root㉿kali)-[/home/kali/Downloads]
└─#
```



❶ Packet List

41 0.097772605	192.168.10.10	192.168.10.20	TCP	54 42298 → 111 [RST] Seq=1 Win=0 Len=0
42 0.097809593	192.168.10.10	192.168.10.20	TCP	58 42298 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
43 0.097812620	192.168.10.10	192.168.10.20	TCP	58 42298 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
44 0.097813590	192.168.10.10	192.168.10.20	TCP	58 42298 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45 0.097842748	192.168.10.10	192.168.10.20	TCP	58 42298 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46 0.097845456	192.168.10.10	192.168.10.20	TCP	58 42298 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
47 0.097846796	192.168.10.10	192.168.10.20	TCP	58 42298 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
48 0.097848448	192.168.10.10	192.168.10.20	TCP	58 42298 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
49 0.097906852	192.168.10.10	192.168.10.20	TCP	58 42298 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
50 0.097944151	192.168.10.10	192.168.10.20	TCP	58 42298 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
51 0.097945166	192.168.10.10	192.168.10.20	TCP	58 42298 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52 0.097946098	192.168.10.10	192.168.10.20	TCP	58 42298 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
53 0.097947010	192.168.10.10	192.168.10.20	TCP	58 42298 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
54 0.097947894	192.168.10.10	192.168.10.20	TCP	58 42298 → 3878 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55 0.097948778	192.168.10.10	192.168.10.20	TCP	58 42298 → 720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
56 0.098006524	192.168.10.20	192.168.10.10	TCP	60 25 → 42298 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
57 0.098006609	192.168.10.20	192.168.10.10	TCP	60 143 → 42298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58 0.098036006	192.168.10.10	192.168.10.20	TCP	54 42298 → 25 [RST] Seq=1 Win=0 Len=0
59 0.098084810	192.168.10.20	192.168.10.10	TCP	60 1025 → 42298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60 0.098084868	192.168.10.20	192.168.10.10	TCP	60 8888 → 42298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61 0.098233239	192.168.10.20	192.168.10.10	TCP	60 3389 → 42298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62 0.098233397	192.168.10.20	192.168.10.10	TCP	60 256 → 42298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63 0.098233436	192.168.10.20	192.168.10.10	TCP	60 21 → 42298 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
64 0.098233478	192.168.10.20	192.168.10.10	TCP	60 587 → 42298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65 0.098272993	192.168.10.10	192.168.10.20	TCP	54 42298 → 21 [RST] Seq=1 Win=0 Len=0
66 0.098342848	192.168.10.20	192.168.10.10	TCP	60 22 → 42298 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
67 0.098342892	192.168.10.20	192.168.10.10	TCP	60 23 → 42298 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
68 0.098342947	192.168.10.20	192.168.10.10	TCP	60 554 → 42298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
69 0.098342988	192.168.10.20	192.168.10.10	TCP	60 1723 → 42298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70 0.098356802	192.168.10.10	192.168.10.20	TCP	54 42298 → 22 [RST] Seq=1 Win=0 Len=0
71 0.098391880	192.168.10.10	192.168.10.20	TCP	54 42298 → 23 [RST] Seq=1 Win=0 Len=0
72 0.098435526	192.168.10.20	192.168.10.10	TCP	60 995 → 42298 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

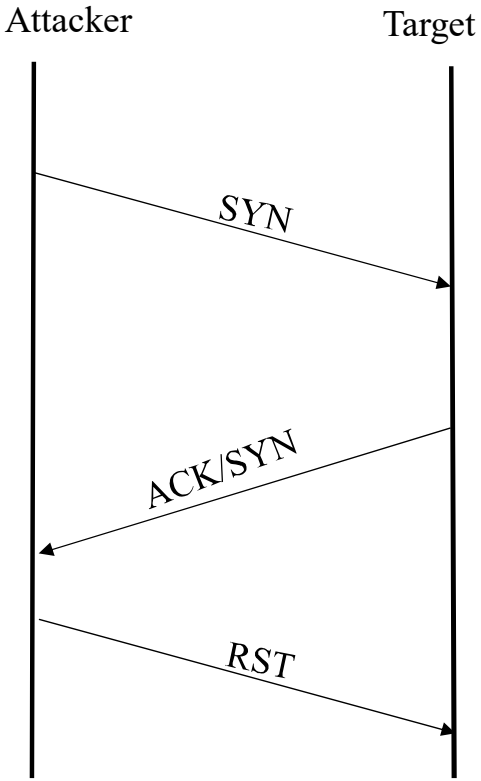
❷ Statistic > Conversations > TCP > ***Port Number***

➔ 어떤 포트를 대상으로 스캔이 시도되었는지 쉽게 확인 가능

Stealth Scan (스텔스 스캔)

- 3Way Handshaking 연결 기법을 이용한 것이 아님
- TCP 헤더를 조작하여 특수한 패킷을 만들어 스캔 대상의 시스템에 보내어 그 응답으로 포트 활성화 여부를 알아내는 기법
- **세션을 성립하지 않고 공격 대상 시스템 포트 활성화 여부를 알아내기 때문에 공격 대상 시스템에 로그를 남기지 않음**
- 공격 대상의 시스템 관리자는 어떤 IP를 가진 공격자가 시스템을 스캔 했는지 확인 할 수 없음

❶ TCP half open scan

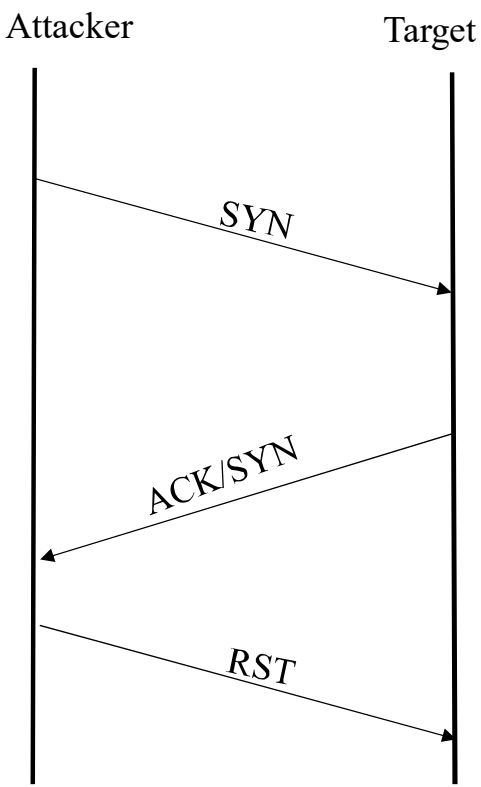


<<열린 포트인 경우 >>

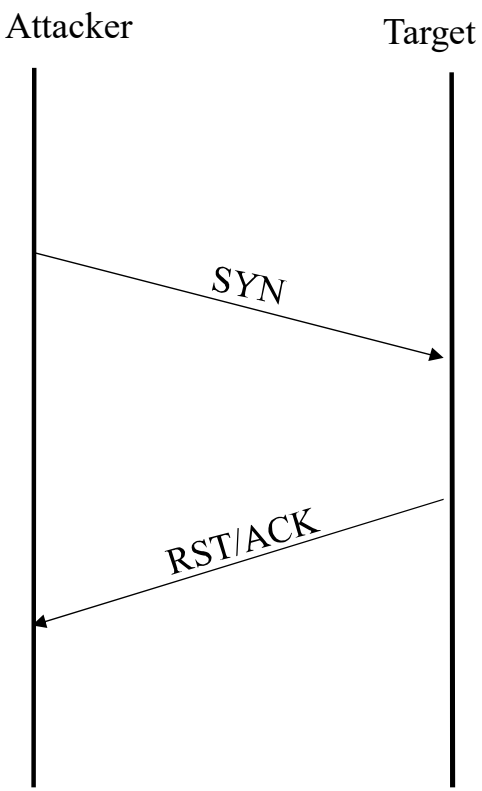
$nmap –sS [대상IP]

- 세션에 대한 로그가 남는 TCP Full Openscan을 보안하기 위한 기법
- 공격대상으로부터 SYN/ACK 패킷을 받으면 공격자는 RST 패킷을 보내 연결을 끊음
- 세션을 완전히 연결하지 않음
- 로그를 남기지 않아 추적이 불가능하도록 하는 기법

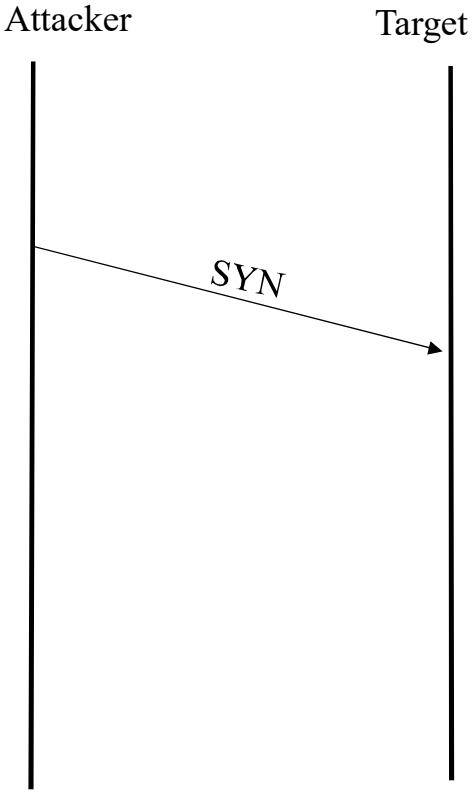
❶ TCP half open scan



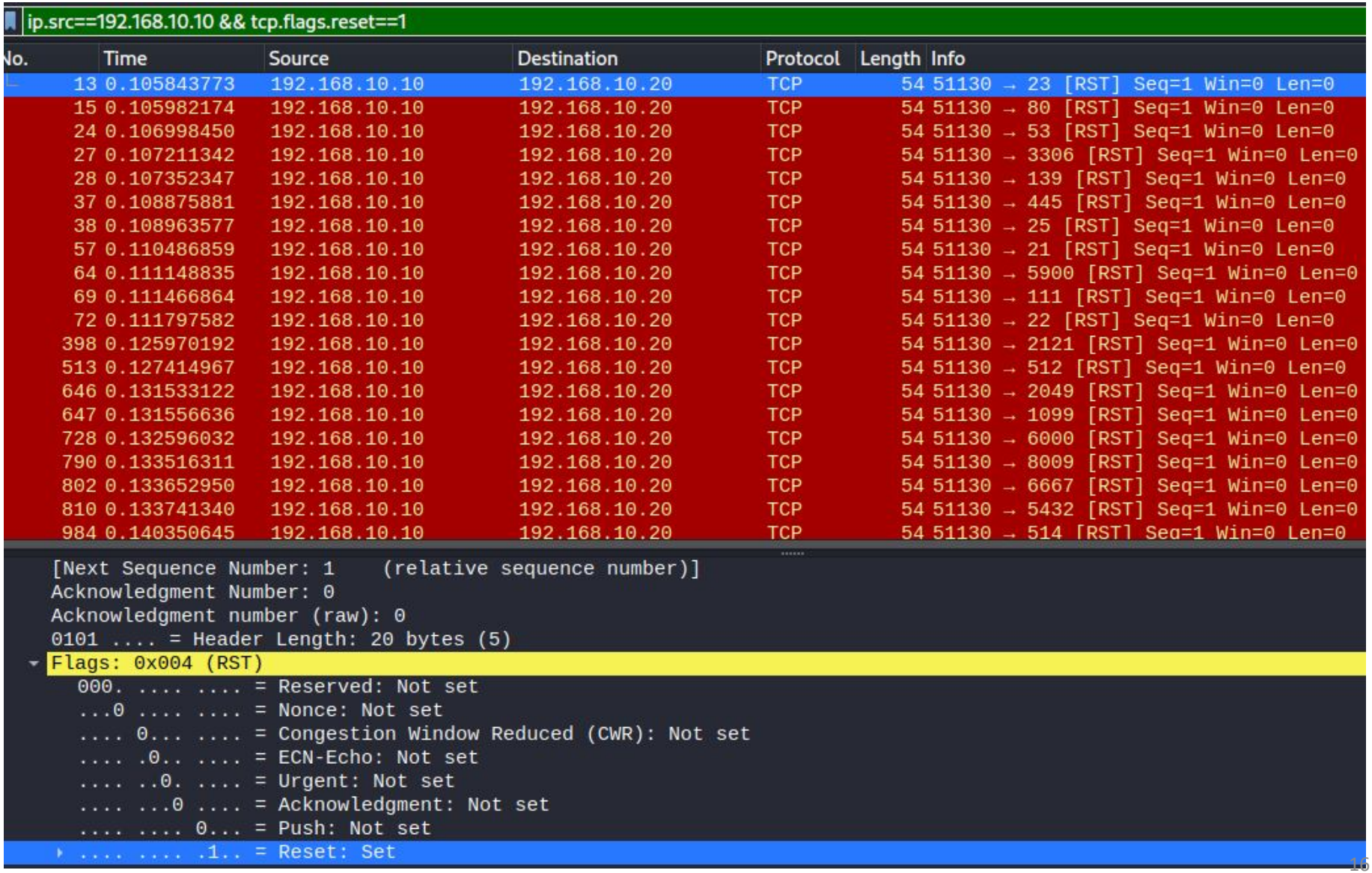
<<열린 포트인 경우 >>



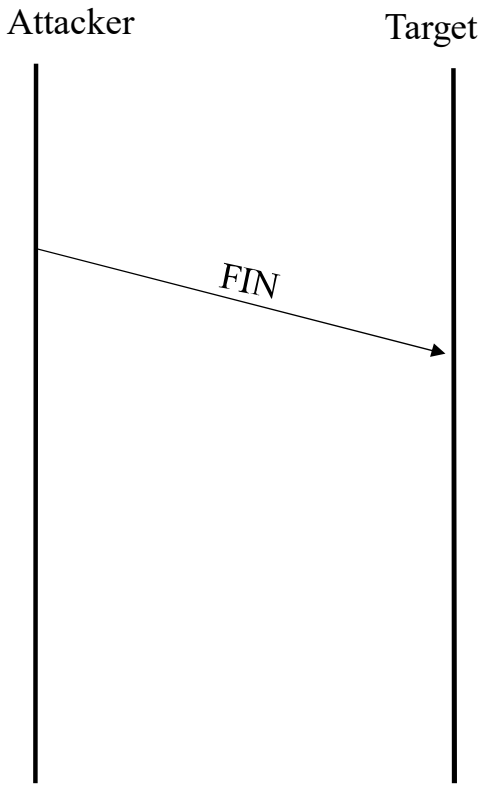
<<닫힌 포트인 경우 >>



<<차단정책에 의해 차단되어 있는 경우>>


ip.src==192.168.10.10 && tcp.flags.reset==1
No. Time Source Destination Protocol Length Info
13 0.105843773 192.168.10.10 192.168.10.20 TCP 54 51130 → 23 [RST] Seq=1 Win=0 Len=0
15 0.105982174 192.168.10.10 192.168.10.20 TCP 54 51130 → 80 [RST] Seq=1 Win=0 Len=0
24 0.106998450 192.168.10.10 192.168.10.20 TCP 54 51130 → 53 [RST] Seq=1 Win=0 Len=0
27 0.107211342 192.168.10.10 192.168.10.20 TCP 54 51130 → 3306 [RST] Seq=1 Win=0 Len=0
28 0.107352347 192.168.10.10 192.168.10.20 TCP 54 51130 → 139 [RST] Seq=1 Win=0 Len=0
37 0.108875881 192.168.10.10 192.168.10.20 TCP 54 51130 → 445 [RST] Seq=1 Win=0 Len=0
38 0.108963577 192.168.10.10 192.168.10.20 TCP 54 51130 → 25 [RST] Seq=1 Win=0 Len=0
57 0.110486859 192.168.10.10 192.168.10.20 TCP 54 51130 → 21 [RST] Seq=1 Win=0 Len=0
64 0.111148835 192.168.10.10 192.168.10.20 TCP 54 51130 → 5900 [RST] Seq=1 Win=0 Len=0
69 0.111466864 192.168.10.10 192.168.10.20 TCP 54 51130 → 111 [RST] Seq=1 Win=0 Len=0
72 0.111797582 192.168.10.10 192.168.10.20 TCP 54 51130 → 22 [RST] Seq=1 Win=0 Len=0
398 0.125970192 192.168.10.10 192.168.10.20 TCP 54 51130 → 2121 [RST] Seq=1 Win=0 Len=0
513 0.127414967 192.168.10.10 192.168.10.20 TCP 54 51130 → 512 [RST] Seq=1 Win=0 Len=0
646 0.131533122 192.168.10.10 192.168.10.20 TCP 54 51130 → 2049 [RST] Seq=1 Win=0 Len=0
647 0.131556636 192.168.10.10 192.168.10.20 TCP 54 51130 → 1099 [RST] Seq=1 Win=0 Len=0
728 0.132596032 192.168.10.10 192.168.10.20 TCP 54 51130 → 6000 [RST] Seq=1 Win=0 Len=0
790 0.133516311 192.168.10.10 192.168.10.20 TCP 54 51130 → 8009 [RST] Seq=1 Win=0 Len=0
802 0.133652950 192.168.10.10 192.168.10.20 TCP 54 51130 → 6667 [RST] Seq=1 Win=0 Len=0
810 0.133741340 192.168.10.10 192.168.10.20 TCP 54 51130 → 5432 [RST] Seq=1 Win=0 Len=0
984 0.140350645 192.168.10.10 192.168.10.20 TCP 54 51130 → 514 [RST] Seq=1 Win=0 Len=0
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0101 .... = Header Length: 20 bytes (5)
Flags: 0x004 (RST)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .1.. = Reset: Set

❷ FIN scan

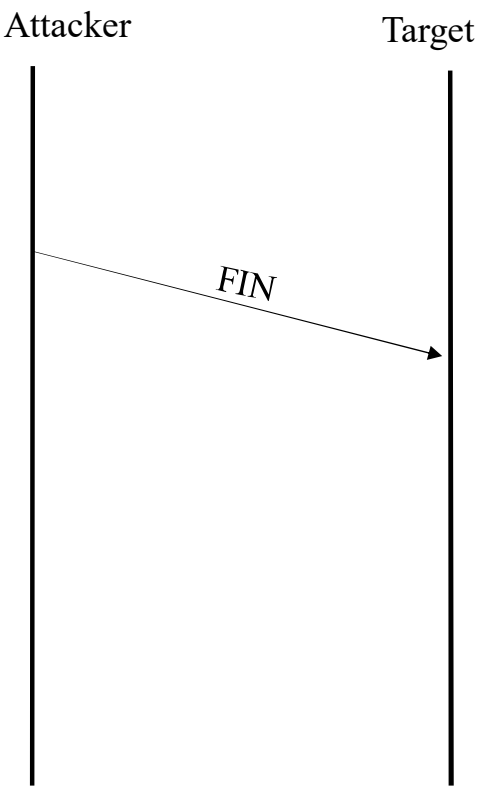


<< 열린 포트의 경우 >>

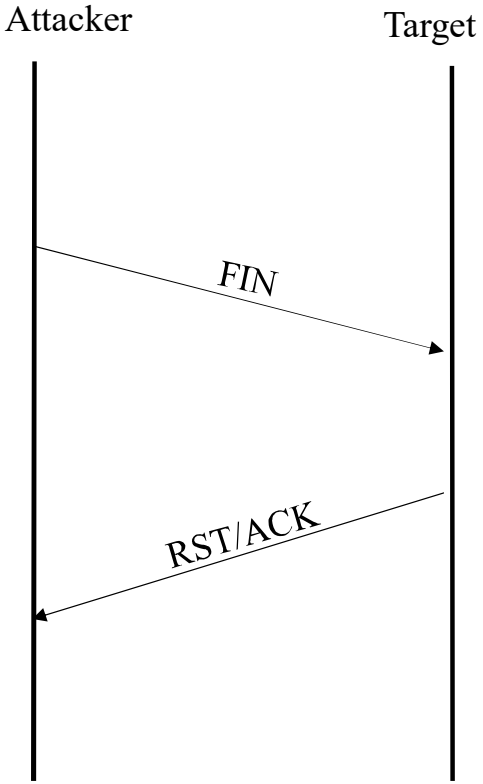
$nmap –sF [대상IP]

- TCP 헤더 내에서 FIN 플래그를 설정하여 공격 대상으로 메시지를 전송
- 포트가 열려 있는 경우 응답이 없음

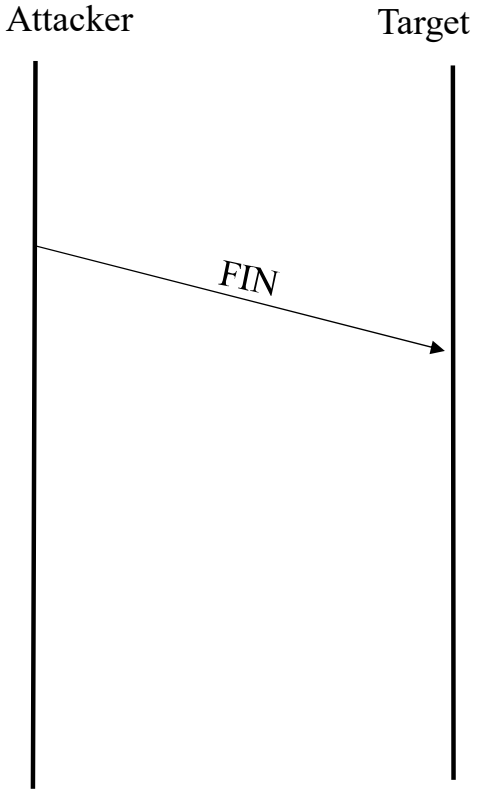
❷ FIN scan



<< 열린 포트의 경우 >>

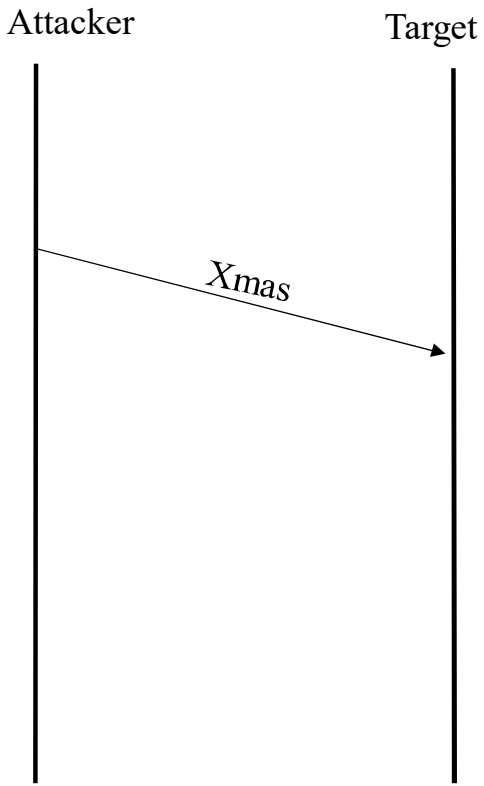


<< 닫힌 포트의 경우 >>



<<차단정책에 의해 차단되어 있는 경우>>

❸ Xmas scan

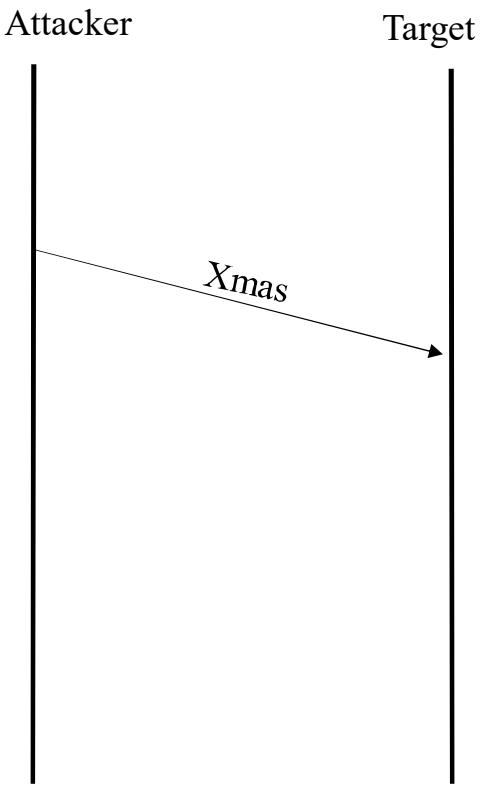


<< 열린 포트의 경우 >>

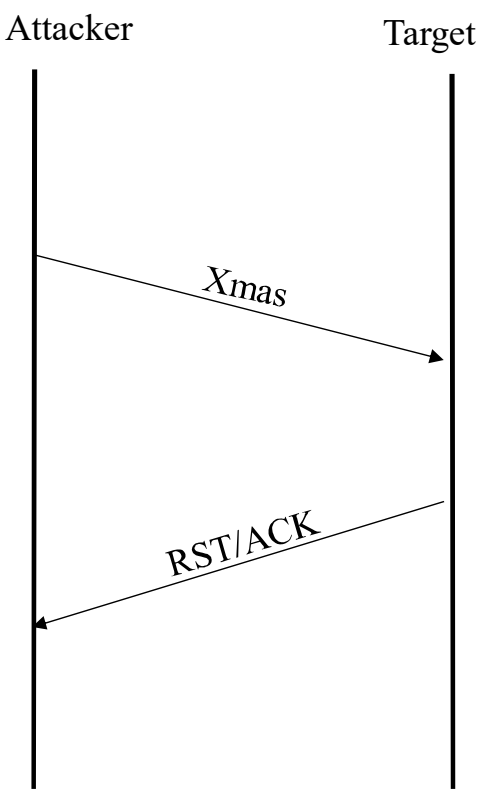
$nmap –sX [대상IP]

- TCP 헤더 내에서 ACK, FIN, RST, SYN, URG 플래그를 모두 설정하여 전송
- 포트가 열려 있는 경우 응답이 없음

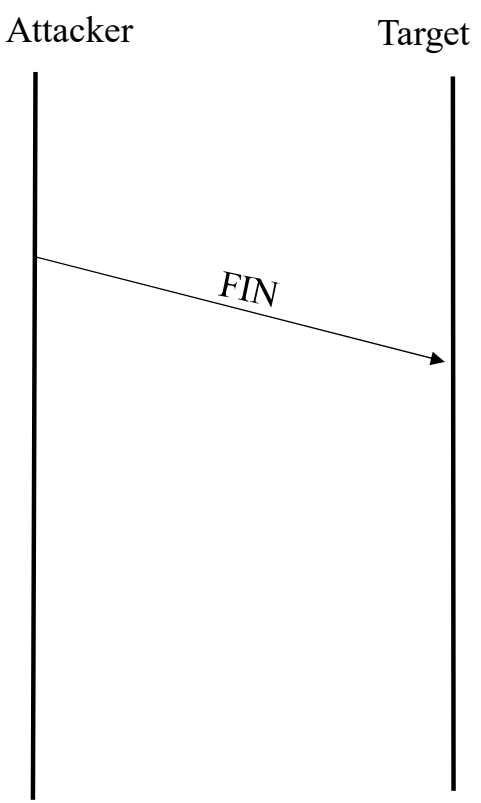
❸ Xmas scan



<< 열린 포트의 경우 >>



<< 닫힌 포트의 경우 >>



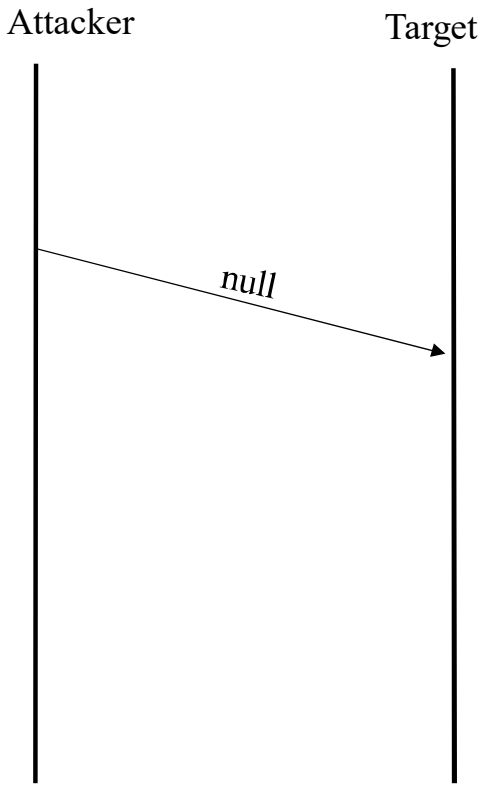
<<차단정책에 의해 차단되어 있는 경우>>

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# nmap  -sX 192.168.10.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-12 21:38 EDT
Nmap scan report for 192.168.10.20
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ss
445/tcp  open|filtered microsoft-
```

No.	Time	Source	Destination	Protocol	Length	Info
40	0.116144157	192.168.10.10	192.168.10.20	TCP	54	36515 → 993 [FIN, PSH, URG] Seq=1 W
41	0.116318743	192.168.10.10	192.168.10.20	TCP	54	36515 → 554 [FIN, PSH, URG] Seq=1 W
42	0.116414998	192.168.10.10	192.168.10.20	TCP	54	36515 → 23 [FIN, PSH, URG] Seq=1 Wi
43	0.116504219	192.168.10.10	192.168.10.20	TCP	54	36515 → 8080 [FIN, PSH, URG] Seq=1
44	0.116724691	192.168.10.10	192.168.10.20	TCP	54	36515 → 256 [FIN, PSH, URG] Seq=1 W
45	0.116947632	192.168.10.10	192.168.10.20	TCP	54	36515 → 5900 [FIN, PSH, URG] Seq=1

```
[Conversation completeness: Incomplete (36)]
[TCP Segment Len: 0]
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 1670894971
[Next Sequence Number: 2    (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0101 .... = Header Length: 20 bytes (5)
Flags: 0x029 (FIN, PSH, URG)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Nonce: Not set
  .... 0... .... = Congestion Window Reduced (CWR): Not set
  .... .0.. .... = ECN-Echo: Not set
  .... ..1. .... = Urgent: Set
  .... ...0 .... = Acknowledgment: Not set
  .... .... 1... = Push: Set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...1 = Fin: Set
```

❹ Null scan

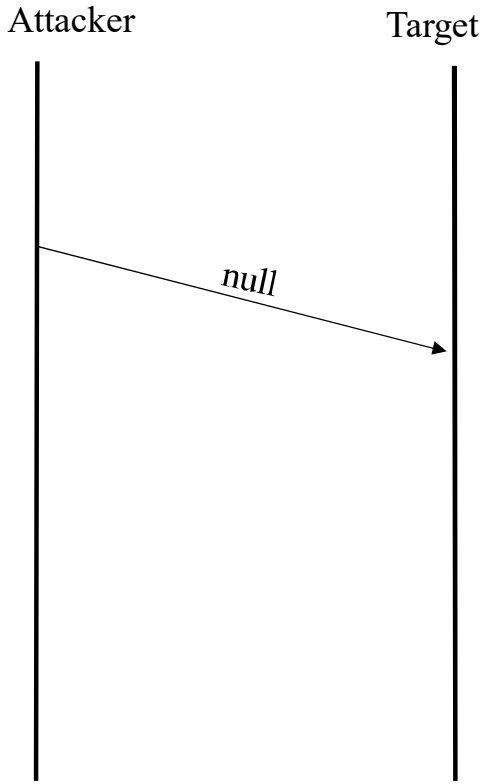


<< 열린 포트의 경우 >>

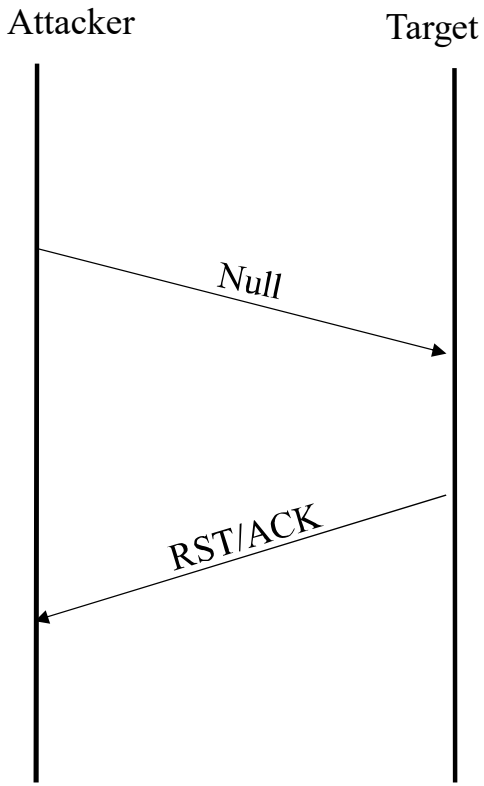
$nmap –sN [대상IP]

- TCP 헤더 내에 플래그 값을 설정하지 않고 패킷을 전송

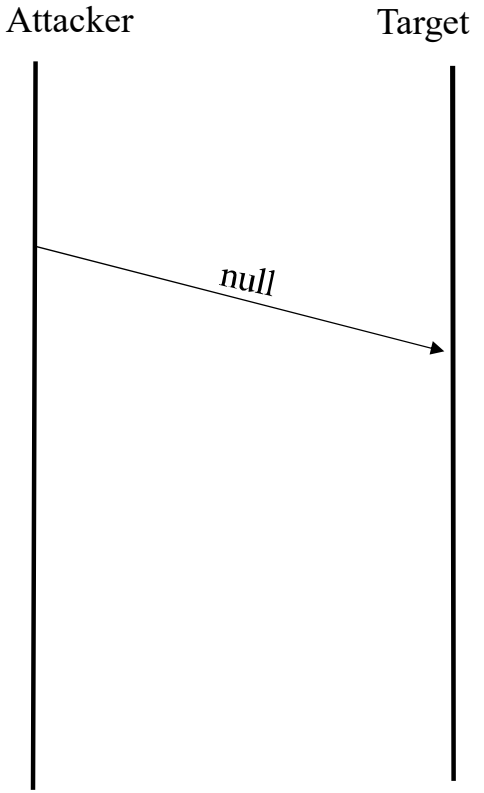
❹ Null scan



<< 열린 포트의 경우 >>



<< 닫힌 포트의 경우 >>



<<차단정책에 의해 차단되어 있는 경우>>

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# nmap  -sN 192.168.10.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-12 21:41 EDT
Nmap scan report for 192.168.10.20
Host is up (0.00016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
```

```
    19 0.099773438   192.168.10.10   192.168.10.20   TCP   54 34902 → 1025 [<None>]
    20 0.099915964   192.168.10.10   192.168.10.20   TCP   54 34902 → 110 [<None>] S
    21 0.099995867   192.168.10.10   192.168.10.20   TCP   54 34902 → 993 [<None>] S
    22 0.100069133   192.168.10.10   192.168.10.20   TCP   54 34902 → 995 [<None>] S
    23 0.100171487   192.168.10.10   192.168.10.20   TCP   54 34902 → 3389 [<None>]
    24 0.100407173   192.168.10.10   192.168.10.20   TCP   54 34902 → 3306 [<None>]
    25 0.100559211   192.168.10.10   192.168.10.20   TCP   54 34902 → 113 [<None>] S
```

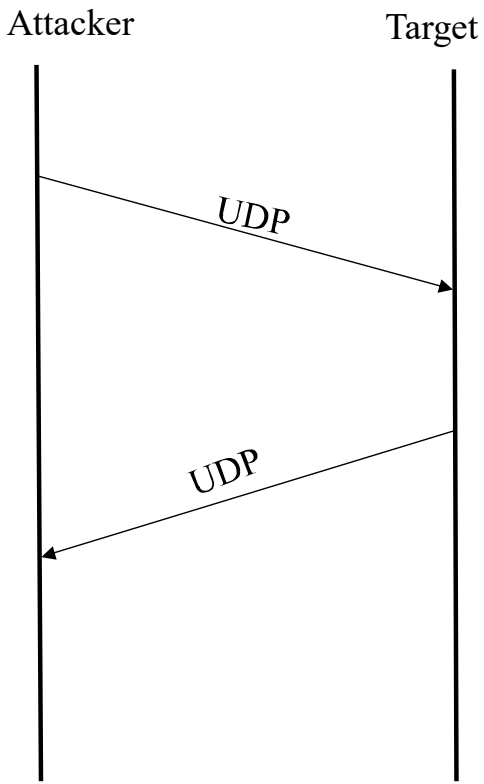
```
[TCP Segment Len: 0]
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 4272708618
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0101 .... = Header Length: 20 bytes (5)
▾ Flags: 0x000 (<None>)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Nonce: Not set
  .... 0... .... = Congestion Window Reduced (CWR): Not set
  .... .0.. .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...0 .... = Acknowledgment: Not set
  .... .... 0... = Push: Not set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...0 = Fin: Not set
```

UDP Scan

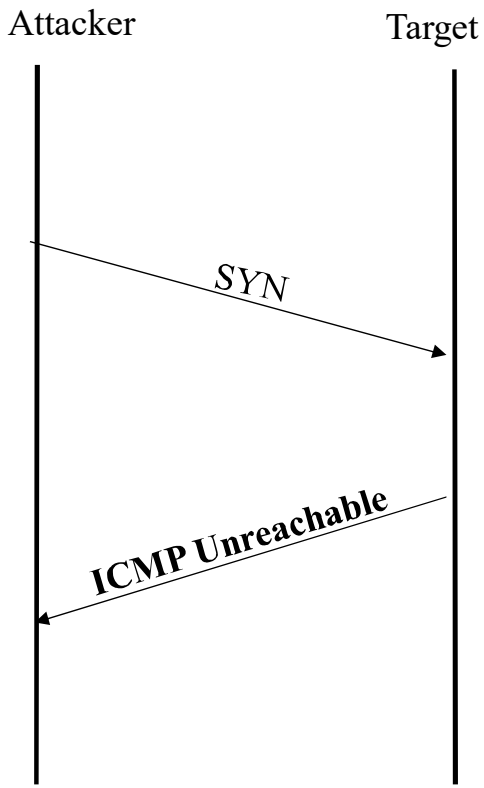
- UDP는 3-way handshake 와 같은 절차가 없음
- UDP 패킷을 전송 시 열려 있는 포트로부터 특정 UDP 응답값으로 수신
- 수신측의 포트가 닫혀 있는 경우 ICMP Port Unreachable 에러 메시지를 통해 포트 활성화 유무 확인

$nmap –sU [대상서버IP]

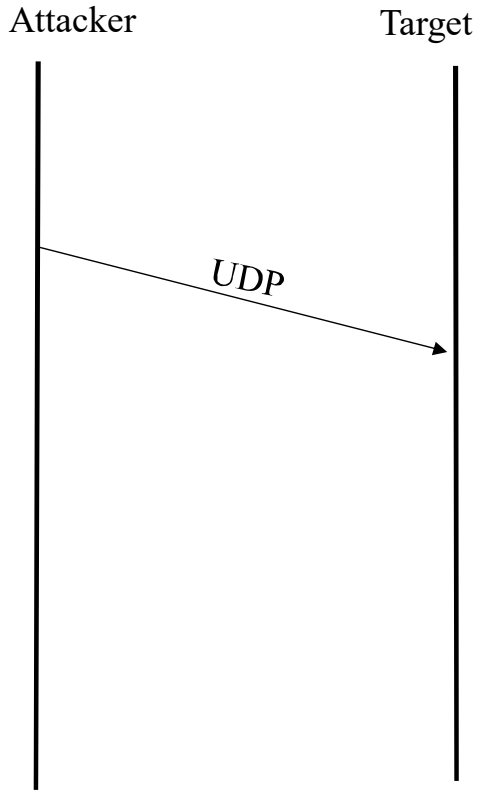
UDP Port Scan



<<열린 포트인 경우 >>



<<닫힌 포트인 경우 >>



<<차단정책에 의해 차단되어 있는 경우>>