

TCPDUMP

#01

TCPDUMP

TCPDUMP ?

가 ()
TCP/IP .

Wireshark

가 가 .

(Basic / Expression / Header Flag)

Basic ()

-i : 가
-c : .
-v : -vv
-n : IP . -nn Port
-w : .pcap . -r TXT

(-i) 100 (-c) .pcap
(-w) txt 가 Binary -r wireshark

tcpdump -i ens33 -vv -c 100 -w ttt.pcap
tcpdump: listening on ens33, link-type EN10MB (Ethernet),
capture size 262144 bytes
100 packets captured
100 packets received by filter

0 packets dropped by kernel

```
#          (-i)          5      (-c) DNS/PORT          IP
          (-nn) .
tcpdump -i br0 -n -c 5
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on br0, link-type EN10MB (Ethernet), capture size
262144 bytes
14:08:14.531606 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
14:08:15.533556 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
14:08:16.535615 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
14:08:18.531679 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
14:08:19.533632 ARP, Request who-has 8.8.8.8 tell
10.10.10.200, length 28
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

```
#          ( -v , -vv ) .
tcpdump -i br0 -n -vv -c 5
tcpdump: listening on br0, link-type EN10MB (Ethernet),
capture size 262144 bytes
14:10:46.548613 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
14:10:47.549640 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
14:10:48.551557 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
14:10:50.548614 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
14:10:51.549621 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 8.8.8.8 tell 10.10.10.200, length 28
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

(-i) IP 가 (-nn, grep)

tcpdump -i ens33 -nn | grep "1.2.3.4"

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes

5 packets captured

6 packets received by filter

0 packets dropped by kernel

14:28:31.524052 IP 1.2.3.4.22 > 5.6.7.8.53707: Flags [P.], seq 4138122029:4138122237, ack 1068364849, win 1432, length 208

14:28:31.525940 IP 5.6.7.8.53707 > 1.2.3.4.22: Flags [.], ack 208, win 509, length 0

Expression ()

. 가 .

1) Type ()

- host , net , port

2) Dir ()

- src, dst , src or dst, src and dst

3) Proto ()

- ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp, udp

4)

- ('and(&&)', 'or(||)', 'not(!)')

- gateway, broadcast, less, greater

(-i) tcp Destination Port 가 22

IP (-nn)

tcpdump -i ens33 tcp dst port 22 -nn

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes

16:50:25.964928 IP 211.115.223.215.53707 > 211.239.150.48.22: Flags [.], ack 4194846013, win 511, length 0

```
16:50:26.016014 IP 211.115.223.215.53707 > 211.239.150.48.22:
Flags [.], ack 161, win 511, length 0
16:50:26.060903 IP 211.115.223.215.53707 > 211.239.150.48.22:
Flags [.], ack 321, win 510, length 0
```

```
#          (-i)      tcp      "      " Destination Port 가 80 "
" 443          IP      (-nn)
tcpdump -i ens33 -nn tcp and dst port 80 or dst port 443
16:59:12.840778 IP 211.239.150.48.49514 > 8.8.8.8.443: Flags
[F.], seq 5, ack 9, win 229, options [nop,nop,TS val
3924566459 ecr 3515313672], length 0
16:59:14.863982 IP 211.239.150.48.47286 > 8.8.8.8.80: Flags
[S], seq 873533324, win 29200, options [mss 1460,sackOK,TS val
3924568482 ecr 0,nop,wscale 7], length 0
16:59:15.865581 IP 211.239.150.48.47286 > 8.8.8.8.80: Flags
[S], seq 873533324, win 29200, options [mss 1460,sackOK,TS val
3924569484 ecr 0,nop,wscale 7], length 0
```

Header Flag

```
#
[ ] SYN : Client 가          Server          (    )          가
          IN/OUT Port          .
```

TCP Header

Interesting Parts	TCP header
tcp[0:2]	source port
tcp[2:2]	destination port
tcp[4:4]	sequence number
tcp[8:4]	acknowledgement number
tcp[12]	header length
tcp[13]	tcp flags
tcp[14:2]	window size
tcp[16:2]	checksum
tcp[18:2]	urgent pointer
tcp[20..60]	options or data

UDP Header

Interesting Parts	UDP Header
udp[0:2]	source port
udp[2:2]	destination port
udp[4:2]	datagram length
udp[6:2]	UDP checksum

Flags

Flags	Numerically	Meaning
---- --S- 0000 0010	0x02	normal syn
---A --S- 0001 0010	0x12	normal syn-ack
---A ---- 0001 0000	0x10	normal ack
--UA P--- 0011 1000	0x38	psh-urg-ack.
---A -R-- 0001 0100	0x14	rst-ack
---- --SF 0000 0011	0x03	syn-fin scan
--U- P--F 0010 1001	0x29	urg-psh-fin
-Y-- ---- 0100 0000	0x40	anything >= 0x40
XY-- ---- 1100 0000	0xC0	both reserved bits set
XYUA PRSF 1111 1111	0xFF	FULL_XMAS scan

SYN

```
= TCP Flag( tcp[13] )      SYN ( 0x02 )      IP ( -nn )      10
(-c) txt      result.log      ( > )
```

```
tcpdump -i ens33 -c 10 "tcp[13] == 0x02" -n -nn > result.log
```

```
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
```

```
listening on ens33, link-type EN10MB (Ethernet), capture size
262144 bytes
```

```
10 packets captured
```

```
10 packets received by filter
```

```
0 packets dropped by kernel
```

cat resule.log

```
16:16:15.308872 IP 211.239.150.48.43192 > 61.100.13.230.10051:
Flags [S], seq 3596242163, win 29200, options [mss
1460,sackOK,TS val 3921988927 ecr 0,nop,wscale 7], length 0
```

```
16:16:17.048128 IP 121.40.192.14.41265 > 211.239.150.48.4244:
Flags [S], seq 3887030721, win 1024, length 0
```

[S] = SYN Flag

json , .

Unskilled Attackers Pester Real Security Folks

=====

TCPDUMP FLAGS

Unskilled = URG = (Not Displayed in Flag Field, Displayed elsewhere)

Attackers = ACK = (Not Displayed in Flag Field, Displayed elsewhere)

Pester = PSH = [P] (Push Data)

Real = RST = [R] (Reset Connection)

Security = SYN = [S] (Start Connection)

Folks = FIN = [F] (Finish Connection)

SYN-ACK = [S.] (SynAck Packet)

[.] (No Flag Set)

JSON

```
result.log
```

```
IP: 211.239.150.48
```

JSON:

```
[ { ipaddr1: '221.239.150.48',  
  ipaddr2: '61.100.13.230',  
  type: 'Outbound',  
  port: '10051' },  
  { ipaddr1: '121.40.192.14',  
    ipaddr2: '221.239.150.48',  
    type: 'Inbound',  
    port: '4244' } ]
```

Table:

ipaddr1	ipaddr2	type	port
221.239.150.48	61.100.13.230	Outbound	10051
121.40.192.14	211.239.150.48	Inbound	4244

TCP 3 way handshark : <https://websecurity.tistory.com/93>