

TCPDump Kullanımı

Afşin Taşkıran

Tcpdump, Unix/Linux benzeri sistemler için vazgeçilmez paket yakalama ve analiz aracıdır.

afsin@taskiran.org
Son Güncelleme:
25/08/2010

İçindekiler

GİRİŞ	3
KULLANIM ÖRNEKLERİ.....	3
1. Belirli Bir Ağ Kartından Okuma Yapmak	3
2. Belirli Sayıda Paketi Dinlemek	4
3. Yakalanan Paketleri Ascii Formatta Görüntülenmesi	4
4. Yakalanan Paketleri Kaydetmek ve Kayıttan Okumak	5
5. Paketlerin Hexadecimal ve Ascii Formatta Görüntülenmesi	5
6. Paketlerin Daha Okunabilir Formatta Zaman Damlalarıyla Görüntülenmesi.....	6
7. Protokol Türüne Göre Filtreleme Yapmak.....	7
8. Paket Boyutuna Göre Filtreleme	8
9. Belli Bir Porta Göre Filtreleme Yapmak	8
10. IP ve Port Filtrelemesi.....	8
11. Mantıksal İfadeler.....	9
Sonuç :	9



Tcpdump, Unix/Linux benzeri sistemler için vazgeçilmesi paket yakalama ve analiz aracıdır. Tcpdump ile kaydedilen paketler yine tcpdump ile açılıp analizleri yapılabilir. Aynı zamanda kaydedilen .pcap uzantılı bu dosyalar wireshark ile de açılabilir.

KULLANIM ÖRNEKLERİ

1. Belirli Bir Ağ Kartından Okuma Yapmak

Tcpdump'ı bir parametre vermeden çalıştırırsak tüm interface leri dinlemeye başlayacaktır. Birden fazla ağ arayüzü olan sistemlerde çalışırken sadece istediğimiz arayüzdeki paketleri görmek isteyebiliriz.

```
root@filyos:~# tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
02:37:44.424093 arp who-has 192.168.58.128 tell 192.168.58.1
02:37:44.424128 arp reply 192.168.58.128 is-at 00:0c:29:5e:f4:e5 (oui Unknown)
02:37:44.424844 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 3, length 40
02:37:44.425018 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 3, length 40
02:37:44.426608 IP 192.168.58.128.50227 > 192.168.58.2.domain: 47623+ PTR? 128.58.168.192.in-addr.arpa. (45)
02:37:44.428445 arp who-has 192.168.58.128 tell 192.168.58.2
02:37:44.428485 arp reply 192.168.58.128 is-at 00:0c:29:5e:f4:e5 (oui Unknown)
02:37:44.428775 IP 192.168.58.2.domain > 192.168.58.128.50227: 47623 NXDomain 0/1/0 (130)
02:37:44.429349 IP 192.168.58.128.35318 > 192.168.58.2.domain: 32796+ PTR? 1.58.168.192.in-addr.arpa. (43)
02:37:44.430865 IP 192.168.58.2.domain > 192.168.58.128.35318: 32796 NXDomain 0/1/0 (128)
02:37:44.431558 IP 192.168.58.128.45188 > 192.168.58.2.domain: 56022+ PTR? 2.58.168.192.in-addr.arpa. (43)
02:37:44.433226 IP 192.168.58.2.domain > 192.168.58.128.45188: 56022 NXDomain 0/1/0 (128)
02:37:45.425147 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 4, length 40
02:37:45.425201 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 4, length 40
02:37:49.423220 arp who-has 192.168.58.1 tell 192.168.58.128
02:37:49.423793 arp reply 192.168.58.1 is-at 00:50:56:c0:00:08 (oui Unknown)
02:37:49.428982 arp who-has 192.168.58.2 tell 192.168.58.128
02:37:49.429256 arp reply 192.168.58.2 is-at 00:50:56:ea:d2:88 (oui Unknown)
02:37:54.076419 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 5, length 40
02:37:54.076465 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 5, length 40
02:37:55.078258 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 6, length 40
02:37:55.078287 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 6, length 40
```



Yukarıdaki örnekte de görüldüğü üzere tcpdump -i parametresi ile sadece eth0 interface ini dinler konuma geçmiştir.

2. Belirli Sayıda Paketi Dinlemek

Analiz ihtiyacımıza göre belirli sayıda paketi gözlemlemek isteyebiliriz. Bunun için tcpdump -c parametresini kullanıyoruz.

```
root@filyos:~# tcpdump -i eth0 -c 3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
03:02:35.133884 arp who-has 169.254.107.110 tell 192.168.58.1
03:02:35.138707 arp who-has 192.168.58.2 tell 192.168.58.128
03:02:35.139005 arp reply 192.168.58.2 is-at 00:50:56:ea:d2:88 (oui Unknown)
3 packets captured
11 packets received by filter
0 packets dropped by kernel
root@filyos:~#
```

tcpdump -c 3 parametresi ile 3 adet paket yakalıyoruz.

3. Yakalanan Paketleri Ascii Formatta Görüntülenmesi

tcpdump -A parametresi ile yakalanan paketleri Ascii formatta görüntüleyebiliriz.

```
root@filyos:~# tcpdump -i eth0 -A
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
03:18:52.472904 arp who-has 192.168.58.128 tell 192.168.58.1
.....PV.....:.....:.....
03:18:52.472969 arp reply 192.168.58.128 is-at 00:0c:29:5e:f4:e5 (oui Unknown)
.....)^.....:PV.....:
03:18:52.474378 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 13, length 40
abcdefghijklmnopqrstuvwabcdefghi
03:18:52.474449 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 13, length 40
abcdefghijklmnopqrstuvwabcdefghi
03:18:52.475235 arp who-has 192.168.58.2 tell 192.168.58.128
.....)^.....:
03:18:52.475333 arp reply 192.168.58.2 is-at 00:50:56:ea:d2:88 (oui Unknown)
.....PV.....:.....)^.....:
03:18:52.475339 IP 192.168.58.128.35131 > 192.168.58.2.domain: 64462+ PTR? 128.58.168.192.in-
addr.arpa. (45)
E..l{.@.@.$.:.....:;5.5.H.....128.58.168.192.in-addr.arpa.....
03:18:52.478125 IP 192.168.58.2.domain > 192.168.58.128.35131: 64462 NXDomain 0/1/0 (130)
E.....E.....:.....:5.;.....128.58.168.192.in-addr.arpa.....16
```



```

03:18:52.478652 IP 192.168.58.128.39481 > 192.168.58.2.domain: 33220+ PTR? 1.58.168.192.in-
addr.arpa. (43)
E..G{.@.@.$.:...:9.5.3.....1.58.168.192.in-addr.arpa.....
03:18:52.479843 IP 192.168.58.2.domain > 192.168.58.128.39481: 33220 NXDomain 0/1/0 (128)
E.....E.....:5.9.<b.....1.58.168.192.in-addr.arpa.....168.
03:18:52.480130 IP 192.168.58.128.41673 > 192.168.58.2.domain: 25122+ PTR? 2.58.168.192.in-
addr.arpa. (43)
E..G{.@.@.$.:...:5.3..b".....2.58.168.192.in-addr.arpa.....
03:18:52.481264 IP 192.168.58.2.domain > 192.168.58.128.41673: 25122 NXDomain 0/1/0 (128)
E.....E.....:5....Ssb".....2.58.168.192.in-addr.arpa.....168.
03:18:57.472466 arp who-has 192.168.58.1 tell 192.168.58.128
.....)^.....:
03:18:57.473068 arp reply 192.168.58.1 is-at 00:50:56:c0:00:08 (oui Unknown)
.....PV.....)^.....:

```

4. Yakalanan Paketleri Kaydetmek ve Kayıttan Okumak

Gerçek hayatta tcpdump ile görüntülenen paketleri daha sonra da analiz edebilmek için bir dosyaya yazdırırız. Daha sonra gerektiğinde bu dosyaları açarak gerekli çalışmamızı yaparız.

Tcpdump ile yakalanan paketleri dosyaya yazdırmak için `-w` , dosyadan okumak için ise `-r` parametresini kullanıyoruz.

```

root@filyos:~# tcpdump -i eth0 -w analizdosyasi.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
^C12 packets captured
12 packets received by filter
0 packets dropped by kernel
root@filyos:~# tcpdump -i eth0 -r analizdosyasi.pcap
reading from file analizdosyasi.pcap, link-type EN10MB (Ethernet)
03:34:51.477351 arp who-has 192.168.58.128 tell 192.168.58.1
03:34:51.477471 arp reply 192.168.58.128 is-at 00:0c:29:5e:f4:e5 (oui Unknown)
03:34:51.477978 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 17, length 40
03:34:51.478032 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 17, length 40
03:34:52.478739 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 18, length 40
03:34:52.478783 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 18, length 40
03:34:53.480683 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 19, length 40
03:34:53.480708 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 19, length 40
03:34:54.482846 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 20, length 40
03:34:54.482883 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 20, length 40
03:34:56.475525 arp who-has 192.168.58.1 tell 192.168.58.128
03:34:56.476052 arp reply 192.168.58.1 is-at 00:50:56:c0:00:08 (oui Unknown)
root@filyos:~#

```

5. Paketlerin Hexadecimal ve Ascii Formatta Görüntülenmesi



Analiz gereksinimlerine göre paketlerin hex ve ascii formatta görüntülenmeleri gerekebilmektedir. Bunun için tcpdump -XX parametresini kullanabiliriz.

```
root@filyos:~# tcpdump -i eth0 -XX
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
03:23:49.055462 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 16, length 40
 0x0000: 000c 295e f4e5 0050 56c0 0008 0800 4500  ..)^...PV.....E.
 0x0010: 003c 0270 0000 8001 427f c0a8 3a01 c0a8  .<.p....B.....
 0x0020: 3a80 0800 4d4b 0001 0010 6162 6364 6566  ....MK....abcdef
 0x0030: 6768 696a 6b6c 6d6e 6f70 7172 7374 7576  ghijklmnopqrstuv
 0x0040: 7761 6263 6465 6667 6869                wabcdefghijklmnopghi
03:23:49.055599 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 16, length 40
 0x0000: 0050 56c0 0008 000c 295e f4e5 0800 4500  .PV.....)^....E.
 0x0010: 003c b8ba 0000 4001 cc34 c0a8 3a80 c0a8  .<....@..4.....
 0x0020: 3a01 0000 554b 0001 0010 6162 6364 6566  ....UK....abcdef
 0x0030: 6768 696a 6b6c 6d6e 6f70 7172 7374 7576  ghijklmnopqrstuv
 0x0040: 7761 6263 6465 6667 6869                wabcdefghijklmnopghi
```

6. Paketlerin Daha Okunabilir Formatta Zaman Damlalarıyla Görüntülenmesi

Tcpdump ile yakalanan paketler öntanımlı olarak kolayca analiz edilebilecek formatta değildir. Tcpdump çıktılarımızı daha okunabilir formatta görüntülemek için -tttt parametresini kullanabiliriz.

```
root@filyos:~# tcpdump -i eth0 -tttt
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
2010-08-25 03:45:21.872947 arp who-has 192.168.58.128 tell 192.168.58.1
2010-08-25 03:45:21.873062 arp reply 192.168.58.128 is-at 00:0c:29:5e:f4:e5 (oui Unknown)
2010-08-25 03:45:21.875526 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 21,
length 40
2010-08-25 03:45:21.875630 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 21, length
40
2010-08-25 03:45:21.879291 arp who-has 192.168.58.2 tell 192.168.58.128
2010-08-25 03:45:21.879603 arp reply 192.168.58.2 is-at 00:50:56:ea:d2:88 (oui Unknown)
2010-08-25 03:45:21.879614 IP 192.168.58.128.56451 > 192.168.58.2.domain: 43060+ PTR?
128.58.168.192.in-addr.arpa. (45)
2010-08-25 03:45:21.881897 IP 192.168.58.2.domain > 192.168.58.128.56451: 43060 NXDomain
0/1/0 (130)
2010-08-25 03:45:21.882827 IP 192.168.58.128.36688 > 192.168.58.2.domain: 21986+ PTR?
1.58.168.192.in-addr.arpa. (43)
```



```
2010-08-25 03:45:21.884683 IP 192.168.58.2.domain > 192.168.58.128.36688: 21986 NXDomain
0/1/0 (128)
2010-08-25 03:45:21.885796 IP 192.168.58.128.44435 > 192.168.58.2.domain: 59575+ PTR?
2.58.168.192.in-addr.arpa. (43)
2010-08-25 03:45:21.887281 IP 192.168.58.2.domain > 192.168.58.128.44435: 59575 NXDomain
0/1/0 (128)
2010-08-25 03:45:22.875805 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 22,
length 40
2010-08-25 03:45:22.875851 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 22, length
40
2010-08-25 03:45:23.877822 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 23,
length 40
2010-08-25 03:45:23.877866 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 23, length
40
2010-08-25 03:45:24.880917 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 24,
length 40
2010-08-25 03:45:24.880965 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 24, length
40
root@filyos:~#
```

7. Protokol Türüne Göre Filtreleme Yapmak

Tcpdump da hayatı kolaylaştıran bir diğer özellik de protokol türüne göre filtreleme yapmaktır. Tcp, udp, icmp, arp, rarp, fddi, tr, wlan, ip, ip6, decnet gibi protokol türleriyle klayca filtreleme yapabiliriz.

```
root@filyos:~# tcpdump -i eth0 arp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
04:30:38.332169 arp who-has 192.168.58.128 tell 192.168.58.1
04:30:38.332301 arp reply 192.168.58.128 is-at 00:0c:29:5e:f4:e5 (oui Unknown)
04:30:38.334770 arp who-has 192.168.58.2 tell 192.168.58.128
04:30:38.334924 arp reply 192.168.58.2 is-at 00:50:56:ea:d2:88 (oui Unknown)
04:30:43.331610 arp who-has 192.168.58.1 tell 192.168.58.128
04:30:43.332097 arp reply 192.168.58.1 is-at 00:50:56:c0:00:08 (oui Unknown)
root@filyos:~# tcpdump -i eth0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
04:31:00.619664 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 31, length 40
04:31:00.619720 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 31, length 40
04:31:01.622342 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 32, length 40
04:31:01.622384 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 32, length 40
04:31:02.624446 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 33, length 40
04:31:02.624490 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 33, length 40
```



8. Paket Boyutuna Göre Filtreleme

Tcpdump da istediğimiz boyuttan büyük ya da küçük paketleri yakalayabiliriz. Bunun için greater ve less parametrelerini kullanabiliriz.

```
root@filyos:~# tcpdump -i eth0 greater 512
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
04:44:23.152249 IP 192.168.58.128.1246 > 10.1.1.2.0: S 1677317564:1677318564(1000) win 512
04:44:24.149044 IP 192.168.58.128.1247 > 10.1.1.2.0: S 1407859487:1407860487(1000) win 512
04:44:25.151118 IP 192.168.58.128.1248 > 10.1.1.2.0: S 1165250754:1165251754(1000) win 512
04:44:26.152060 IP 192.168.58.128.1249 > 10.1.1.2.0: S 890457140:890458140(1000) win 512
04:44:27.153133 IP 192.168.58.128.1250 > 10.1.1.2.0: S 1907146083:1907147083(1000) win 512
root@filyos:~# tcpdump -i eth0 less 1000
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
04:45:11.429317 IP 192.168.58.128.2675 > 10.1.1.2.0: S 113087061:113087111(50) win 512
04:45:12.430908 IP 192.168.58.128.2676 > 10.1.1.2.0: S 871831544:871831594(50) win 512
04:45:13.432320 IP 192.168.58.128.2677 > 10.1.1.2.0: S 1838942293:1838942343(50) win 512
root@filyos:~#
```

9. Belli Bir Porta Göre Filtreleme Yapmak

Tcpdump a port parametresi vererek istediğimiz port filtrelemesini yapabiliriz.

```
root@filyos:~# tcpdump -i eth0 port 6767
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
04:59:34.258804 IP 192.168.58.128.2535 > 10.1.1.2.6767: S 1675618050:1675618100(50) win 512
04:59:35.259806 IP 192.168.58.128.2536 > 10.1.1.2.6767: S 237854318:237854368(50) win 512
04:59:36.260889 IP 192.168.58.128.2537 > 10.1.1.2.6767: S 469372295:469372345(50) win 512
root@filyos:~#
```

10. IP ve Port Filtrelemesi

Tcpdump ın birçok mantıksal ifadesi bulunmakla birlikte paketin hedef adresi ve portunu filtrelemek için aşağıdaki komutu kullanabiliriz.

```
root@filyos:~# tcpdump -i eth0 dst 1.1.1.1 and port 6767
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
05:16:00.577696 IP 192.168.58.128.skkserv > 1.1.1.1.6767: S 250705392:250705442(50) win 512
05:16:01.580649 IP 192.168.58.128.1179 > 1.1.1.1.6767: S 1644577269:1644577319(50) win 512
05:16:02.581710 IP 192.168.58.128.1180 > 1.1.1.1.6767: S 1892348747:1892348797(50) win 512
05:16:03.582659 IP 192.168.58.128.1181 > 1.1.1.1.6767: S 1828562185:1828562235(50) win 512
```



```
05:16:04.583700 IP 192.168.58.128.1182 > 1.1.1.1.6767: S 867049958:867050008(50) win 512
root@filyos:~#
```

11. Mantıksal İfadeler

Tcpdump ile aradığımız paketi bulabilmek için or, not, and gibi mantıksal bağlaçlar kullanılabilir.

```
root@filyos:~# tcpdump -i eth0 not arp and icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
05:23:34.221460 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 34, length 40
05:23:34.221510 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 34, length 40
05:23:35.223268 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 35, length 40
05:23:35.223318 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 35, length 40
05:23:36.225208 IP 192.168.58.1 > 192.168.58.128: ICMP echo request, id 1, seq 36, length 40
05:23:36.225251 IP 192.168.58.128 > 192.168.58.1: ICMP echo reply, id 1, seq 36, length 40
root@filyos:~#
```

Sonuç :

Tcpdump, görüldüğü üzere analiz tekniklerinde oldukça kullanışlı bir araçtır. Bu belge tcpdump resmi sayfasından ve yazarın deneyimlerden derlemeler içermektedir.

Tcpdump ve diğer analiz teknikleri hakkındaki eğitimler için

<http://www.enderunix.org/afsin/index.php/verdigim-egitimler/> adresini ziyaret edebilirsiniz.

