Tcpdump Parametreleri

tcpdump	Trafiği analiz eder.
tcpdump -D	Dinlenebilecek bütün arayüzleri listeler.
tcpdump -i "arayüzün adı"	Belirtilen arayüzün dinlenmesini sağlar.
tcpdump -v	Paketin protokol içeriğini de gösteren detaylı bir analiz yapar.
tcpdump -vv	Paketin NFS ve SMB içeriğini de gösteren detaylı bir analiz yapar.
tcpdump -vvv	Paketin Telnet içeriğini de gösteren detaylı bir analiz yapar.
tcpdump -q	Sadece temel bilgilerini içeren bir analiz yapar.
tcpdump –c "sayı"	Belirtilen sayıda paket içeriğini listeler.
tcpdump -n	Analizi yaparken transfer yapılan adresin IP adresi ve port numarasını yazdırır.
tcpdump -n dst "IP adresi"	Belirtilen IP adresine giden paketleri listeler.
tcpdump -n src "IP adresi"	Belirtilen IP adresinden gelen paketleri listeler.
tcpdump -n "IP adresi"	Belirtilen IP adresinden gelen ya da giden bütün paketleri listeler.
tcpdump -n dst net "ağ adresi"	Belirtilen ağ adresine giden paketleri listeler.
tcpdump -n src net "ağ adresi"	Belirtilen ağ adresinden gelen paketleri listeler.
tcpdump -n net "ağ adresi"	Belirtilen ağ adresinden gelen ya da giden paketleri listeler.
tcpdump –n port "port numarası"	Hedef veya kaynak portu belirtilen port olan paketleri listeler.
tcpdump –n dst port "port numarası"	Hedef portu belirtilen port olan paketleri listeler.
tcpdump –n src port "port numarası"	Kaynak portu belirtilen port olan paketleri listeler.
tcpdump –v icmp	ICMP paketlerini listeler.
tcpdump –v arp	ARP paketlerini listeler.
tcpdump –p	Tcpdump ile yalnızca dinleme yapılan arabirime gelen paketleri yakalamak için seçici olmayan moddan çıkılması için kullanılır.
tcpdump –e	Yakalanan paketlerin ikinci katman bilgilerini yani mac adreslerini elde etmek için kullanılır.
tcpdump –w “dosya ismi”	Listelenen paketleri bir dosya halinde kaydeder. Bu kaydettiğimiz dosyayı ‘Wireshark’ gibi programlarla da açarak inceleyebiliriz.
tcpdump –r “dosya ismi”	Dosya halinde olan bir paket listesini açar.

Tcpdump Kullanımı

Öncelikle `-i` parametresi ile konumuza giriş yapalım. Eğer tcpdump kullanıyorsanız, ya kayıtlı bir dosyayı okuyacaksınızdır ya da, bilgisayarınızdaki herhangi bir interfaceyi dinleyeceksinizdir. İnterface diyerek o anda kullanmakta olduğumuz network kartından bahsediyorum. Bilgisayarınızdaki interfaceleri görüntülemek için linux'ta `ifconfig` komutunu kullanabilirsiniz. Bu komuttan sonra karşınıza **eth0**, **eth1** veya **enp0s8**, **enp0s3** gibi farklı farklı interface isimleri çıkacaktır. Bu şekilde dinlemek istediğiniz interface ismini öğrenebilirsiniz. Benim tcpdump ile dinlemek istediğim interface ismi `enp0s3` olduğu için bu ve bundan sonraki örneklerde bunu kullanacağım. Evet bu bilgiden sonra isterseniz, ilk örneğimizi yazalım.

Tcpdump uygulamasını kullanabilmek için root yetkileri ile çalıştırmanız gerekmektedir.

```
sudo tcpdump -i enp0s3
```

Yukarıdaki komutta `i` parametresi ile dinleyeceğimiz interfaceyi belirtmiş olduk. Bu komutu çalıştırdıktan sonra internete bağlandığınız vakit, terminal ekranınızda bağlantınız ile ilgili bilgilerin hızlı bir şekilde akacağını göreceksiniz.

Eğer çıktılarınızdaki **hedef ip ve port** numaralarını `fra07s32-in-f99.1e100.net.https` şeklinde değilde `205.3.12.32.443` şeklinde yani, **çözümlenmeden** görmek istiyorsanız `-n` parametresini kullanmalısınız. Yani komutumuz aşağıdaki gibi olacaktır.

```
sudo tcpdump -n -i enp0s3
```

Yukarıdaki komuttan sonra çıktılarımız aşağıdaki formatta olacaktır. Dikkat ederseniz hedef ip ve port numaraları çözümlenmemiş bir şekilde, direkt rakam olarak yazılmıştır.

```
21:03:50.105109 IP 192.168.2.4.60868 > 172.217.21.106.443: Flags [.], ack 680942, win 65535, length 0
```

Şimdi ise çıktılarımızın başında yer alan `zaman` kısmı ile ilgili bir değişikliğe gidelim. Eğer tcpdump'tan daha detaylı bir zaman bilgisi elde etmek istiyorsak, ekleyeceğimiz parametre `-tttt` parametresi olacak. Bu parametre ile çıktılarımızın zaman kısmı biraz değişecek. Bu değişimi komutumuzu kullanarak hemen görelim.

```
sudo tcpdump -tttt -n -i enp0s3
```

Yukarıdaki komut uygulandıktan sonra çıktılarımız aşağıdaki gibi olacaktır. Lütfen tarih kımsına dikkat edelim ve bir önceki çıktı ile karşılaştıralım.

```
2018-05-04 21:09:03.436202 IP 192.168.2.4.59270 > 172.217.20.142.443: Flags [.], ack 114372, win 65535, length 0
```

Bir önceki çıktı ile karşılaştırdığımız vakit, bu yeni çıktımızda başa tarih bilgisinin de eklendiği açık bir şekilde görülmektedir. Şimdiye kadarki örnekler, tcpdump adlı uygulamamız ile network trafiğinin nasıl izlendiğine dair ufak bir giriş yapmamıza olanak sağladı. Lakin tcpdump uygulaması sadece network trafiğinin izlenmesi için değil, aynı zamanda `network trafiğinin analiz edilmesinde de` kullanılır.

Hatta bu ikinci özellik, bu uygulamanın asli özelliğidir. Konumuza devam etmeden önce isterseniz şu çıktı formatını bir inceleyelim. Eğer çıktıyı düzgün bir şekilde okuyamazsak, ne anlattığını anlayamayız. Çıktıların formatı aşağıda belirtilmiştir.

`TCP Trafiği İçin;`

timestamp / layer 3 protocol / source IP address.source port > destination IP address.destination port: layer 4 protocol / TCP flags, TCP sequence numbers, TCP acknowledgement numbers, TCP window size, data length

`UDP Trafiği İçin;`

timestamp / layer 3 protocol / source IP address.source port > destination IP address.destination port: layer 4 protocol / data length

Bu yukarıda verilen format ile trafik çıktılarını incelediğiniz zaman, tcpdump'ın trafikleri nasıl ekrana yansıttığını daha iyi anlayacağınız umuyorum. Bu bilgiyi de verdikten sonra konumuza, işinize en çok yarayacak parametreler üzerinden devam edelim.

Eğer çıktılarınızda OSI referans modelinin 2. katmanına karşılık gelen `Link layer` katmanı protokolünü de görüntülemek istiyorsanız, kullanacağınız parametre **`-e`** parametresi olacaktır. Bu paramatre ile eğer Ethernet kullanıyorsanız, kaynak ve hedef mac adreslerini de çıktılarınızda görebilirsiniz. Komutumuzun son hali aşağıdaki gibidir.

```
sudo tcpdump -tttt -n -e -i enp0s3
```

Bu komutu çalıştırdıktan sonra aşağıdaki gibi bir çıktı göreceksiniz.

```
2018-05-04 21:40:05.772011 08:00:27:9d:f0:86 > 52:54:00:12:35:00, ethertype IPv4 (0x0
800), length 477: 192.168.2.4.60576 > 151.101.113.140.443: Flags [P.], seq 2384:2807,
ack 26147, win 65535, length 423
```

Eğer dinlemekte olduğumuz interfaceden geçen trafiği, terminal ekranı yerine bir pcap dosyası olarak diske kaydetmek istiyorsak, kullanacağımız parametre **`-w <dosya_adi.pcap>`** parametresi olacaktır. Hemen aşağıdaki komutumuzu inceleyelim.

```
sudo tcpdump -tttt -n -e -i enp0s3 -w deneme.pcap
```

Eğer yukarıdaki komutu çalıştırdıysanız, siz programı `CTRL-C` komutu ile sonlandırmadığınız sürece ekrana hiçbir çıktı vermeyecktir. Çünkü interface üzerinden geçen tüm trafik `deneme.pcap` adlı dosyaya kaydedilmektedir. Eğer kaç adet paket yakalandığını anlık olarak ekrana basmak istiyorsanız `-v`komutunu kullanabilirsiniz. Tüm trafiğin kayıtlı olduğu `deneme.pcap` dosyasını okumak için ise **`-r`**parametresini kullanmalısınız. Yani trafiği diskten okumak için kullnacağımız komut aşağıdaki gibi olacaktır.

```
sudo tcpdump -tttt -n -e -i enp0s3 -r deneme.pcap
```

Tabi burada -tttt, -n, -e parametrelerine gerek yoktur. Bunları kaldırdığınız vakit, tcpdump'ın default sağlamış olduğu özellikler ile trafiğiniz ekrana yansıtılır. Burada istediğiniz dosyayı istediğiniz parametre veya parametreler vasıtası ile inceleyebilirsiniz. Zaten bu parametreler, network trafiklerinin okunmasında kolaylık ve esneklik sağlaması amacıyla kullanılmaktadır.

Parametrelerin kullanımı ile ilgili örnekleri burada bitiriyorum. Aşağıdaki listede tcpdump tarafından kullanılabilecek bir çok parametre ve anlamları var. Ayrıca tcpdump'ın manuel sayfasını da inceleyebilirisiniz. Artık ihtiyacınıza göre kullanmak istediğiniz parametreyi seçip, trafiklerinizi analiz edebilirsiniz.

- x: Çıktıları HEX formatında basar.
- xx: Çıktıların HEX formatına 2. katman protokol bilgisini de ekler ve ekrana öyle basar.
- X: Çıktıları hem HEX hemde ASCII olarak basar.
- XX: Çıktılar hem HEX hemde ASCII olarak lakin 2. katman bilgisi eklenmiş olarak basar.
- c: Kaç adet paket yakalanacağını belirler.
- A: Çıktıları sadece ASCII olarak basar.
- s: Her bir paketten kaç byte yakalanacağının üst limitini belirler.(-s 65 = her bir paket için maksimum 65 byte yakala)

Tcpdump ve Filtreleme

Bu zamana kadar gördükleriniz, tcpdump'ı kullanırken işinize yarayacak olan parametreler ve bu parametrelerin kullanımını kapsamaktaydı. Şimdi inceleyeceğimiz konu ise tcpdump adlı uygulamamıza müthiş bir esneklik katan `filtreleme kavramı` olacak. Peki nedir bu filtreleme? Bu soruya örnekler ile cevap verelim. Mesela tcpdump ile analiz yaparken, ona `sadece tcp trafiğini göster`, `tcp trafiğini ve hedef portu 80 olan trafiği göster`, `sadece dns protokolü kullanılan trafiği göster`, `hedef ip adresi X olan trafiği ve hedef portu 25 olan trafiği göster` gibi **network trafiğini anlamlandırmamıza** olanak sağlayan, müthiş bir fonksiyondur filtreleme. Bu filtreleme sayesinde okuduğumuz veya yazdığımız trafikleri anlamlandırabilmekteyiz. Bu filtreleme işlemini yaparken Berkeley Packet Filter (BPF) syntax yapısını kullanacağız. Konunun daha iyi anlaşılması için hemen örneklere geçelim.

Sadece tcp trafiğini kaydeden komut

```
sudo tcpdump -i enp0s3 -w deneme.pcap tcp
```

Yukarıdaki komut çalıştırdıktan sonra bilgisayarınızdan bir web sitesine girin. Url'den ip adresi çözümlenmesi yapılabilmesi için ilk olarak `dns protokolü` kullanılacaktır. Daha sonra ip adresi öğrenilen bu site ile tcp protokolü üzerinden http paketleri gelip gidecek ve bağlantı sağlanmış olacaktır. Lakin biz komutumuzun sonuna `tcp` yazarak, tcpdump'a bir nevi `sadece tcp trafiğini kaydet` emri vermiş olduk. Sağlamasını yapmak için, kaydettiğimiz deneme.pcap dosyasını aşağıdaki filtreleme ile beraber okuduğumuzda içinde `udp` protokolüne ait hiç bir trafik olmadığını görebiliriz.

```
sudo tcpdump -tttt -n -e -r deneme.pcap udp
```

DNS protokolü, taşıma katmanında UDP protokolünü kullanmaktadır.

Sadece tcp trafiğini ve hedef portu 80 olan trafiği kaydeden komut

```
sudo tcpdump -i enp0s3 -w deneme.pcap tcp and dst port 80
```

Kaynak ip adresi sadece X olan trafiği gösteren komut

```
sudo tcpdump -n -tttt -r deneme.pcap src host 192.168.2.4
```

Hedef network adresi X olan tüm paketleri gösteren komut

```
sudo tcpdump -tttt -n -XX -e -r icmp.pcap dst net 192.168.2.0
```

Yukarıdaki komutta `icmp.pcap` dosyası içinde hedef ip adresi 192.168.2.0/24 networküne dahil olan tüm paketler gösterilecek, bu network dışındaki paketler gösterilmeyecektir.

Sadece icmp reply paketlerini gösteren komut

```
sudo tcpdump -tttt -n -XX -e -r icmp.pcap 'icmp[icmptype] = icmp-echoreply'
```

Evet yeteri kadar örnek verdiğimi düşünüyorum. Filtreleme konusu çok geniş bir konu, yukarıda vermiş olduğum linkten detayına inebilirsiniz. Lakin mantığını anladığınızı umuyorum.