

**

* Copyright (c) 2004 Huzeyfe
Ä-NAL

*

* Bu belgenin telif haklarÄ±
'GNU Free Documentation License'

* lisansÄ± ÄYartlarÄ± altÄ±nda
Huzeyfe Ä-NALi ½a aittir.

*

* Belgenin en gÄ¼ncel sÄ¼rÄ¼mÄ¼ne
<http://www.enderunix.org/docs/tcpdump.htm>

* adresinden eriÅYebilirsiniz

* Ä°lk baskÄ±: 2004-12-12

* Son gÄ¼ncelleme: 2004-12-12

*

**

Â

Tcpdump kullanarak AÄY
trafiÄYi izlemek i¸ ½ BÄ¶IÄ¼m 1

Trafik Nedir? TrafiÄYi izleyerek ne elde edebiliriz, ya
da hangi sorunlarÄ±mÄ±za Ä¶zÄ¼m bulabiliriz?

Â

Sniffer olarak adlandÄ±rÄ±lan ve aÄY trafiÄYini izlemek
amacÄ±ylaÂ yazÄ±lan [birÄ¶ok](#)
[program vardÄ±r](#), bunlardan UNIX/Linux dÄ¼nyasÄ± iÄ¶in en bilineni ve sÄ±k
kullanÄ±lanÄ± tcpdumpi¸ ½tÄ±r, tcpdump ilk olarak UNIX sistemler iÄ¶in yazÄ±lmÄ±ÄY
sonrasÄ±nda NRG (Network
Research Group) tarafÄ±ndan Windowsi¸ ½a da port edilmiÄYtir ve
windump olarak adlandÄ±rÄ±lmÄ±ÄYtÄ±r. Ben bu yazÄ±yÄ± hazÄ±rladÄ±ÄYÄ±m sÄ±rada
tcpdumpi¸ ½Ä±nÄ± son versiyonu 3.8 idi, programÄ±n son sÄ¼rÄ¼mÄ¼ne ve Ä¶eÄYitli ek
bilgilere ulaÄYmak iÄ¶in ana sayfasÄ±nÄ± ziyaret edebilirsiniz(<http://www.tcpdump.org>).
Windows Ä¼zerinde kullanmak istiyorsanÄ±z <http://netgroup-serv.polito.it/winpcap>
adresinden indireceÄYiniz ek yazÄ±lÄ±mÄ± kurup yine <http://netgroup-serv.polito.it/windump>
adresinden edinebileceÄYiniz ana yazÄ±lÄ±mÄ± kurmanÄ±z gerekmektedir.

Â

Promiscious Mode Nedir?

Ä Kaba sakal bulunduklarÄ± ortamÄ±n hub olduÄYunu bildiÄYi iÄŒin Ethernet kartÄ±nÄ± promisc moda geÄŒiriyor ve Temel Reis ile Safinaz arasÄ±ndaki trafiÄYi dinliyor ve internette yaptÄ±ÄYÄ± kÄ±sa bir araÄYtÄ±rma neticesinde Temel Reis ile Safinaz i¸ ½Ä±n iletiÄYiminde araya girerek Temel Reisi i¸ ½in Safinaz i¸ ½a yolladÄ±ÄYÄ± paketleri istediÄYi gibi deÄYiÄYtirebiliyor. Temel Reis SafinazÄ± kaba sakala kaptÄ±rdÄ±ktan sonra kendini AÄY gÄ¼venliÄYine adÄ±yor ve yaptÄ±ÄYÄ± araÄYtÄ±rmalar sonucu saÄYlam bir switch Ä¼zerinde ÄŒeÄYitli kurallar yazarak trafiÄYini dinlenemeyecek hale getiriyor;)

Ä

Ä

Ä

Ethernet kartlarÄ± sÄ±fÄ±r yapÄ±landÄ±rma ile i¸ ½promisc i¸ ½ Ä¶zelliÄYine sahip deÄYildirler, ethernet arabirimimizi normal moddan Ä¼promisc i¸ ½ moda geÄŒirmek iÄŒin ifconfig komutuna promisc parametresini vermemiz yeterlidir.

Ä

ifconfig

```
eth0Ä Ä Ä Ä Ä Link encap:EthernetÄ HWaddr  
00:D0:B7:B6:D1:0C
```

```
Ä Ä Ä Ä Ä Ä Ä Ä Ä inet  
addr:194.27.72.88Ä Bcast:194.27.127.255Ä Mask:255.255.192.0
```

Genel: Tcpdump kullanarak AÄY trafiÄYi izlemek i; ½ BÄ¶/Ä¼m 1

Ä Ä Ä Ä Ä Ä Ä Ä Ä UP BROADCAST
RUNNING MULTICASTÄ MTU:1500Ä Metric:1

Ä Ä Ä Ä Ä Ä Ä Ä Ä RX
packets:5228531 errors:0 dropped:0 overruns:0 frame:0

Ä Ä Ä Ä Ä Ä Ä Ä Ä TX
packets:4528739 errors:0 dropped:0 overruns:0 carrier:0

Ä Ä Ä Ä Ä Ä Ä Ä Ä collisions:0
txqueuelen:1000

Ä Ä Ä Ä Ä Ä Ä Ä Ä RX
bytes:1796789472 (1713.5 Mb)Ä TX bytes:3725692 (3.5 Mb)

Ä Ä Ä Ä Ä Ä Ä Ä Ä Interrupt:18 Base
address:0x5400 Memory:f6101000-f6101038

Ä

Ä

ifconfig eth0 promisc

Ä

ifconfig

Genel: Tcpdump kullanarak AÄY trafiÄYi izlemek i; ½ BÄ¶/Ä¼m 1

eth0Ä Ä Ä Ä Ä Link encap:EthernetÄ HWaddr
00:D0:B7:B6:D1:0C

Ä Ä Ä Ä Ä Ä Ä Ä Ä inet
addr:194.27.72.88Ä Bcast:194.27.127.255Ä Mask:255.255.192.0

Ä Ä Ä Ä Ä Ä Ä Ä Ä UP BROADCAST
RUNNING **PROMISC** MULTICASTÄ MTU:1500Ä Metric:1

Ä Ä Ä Ä Ä Ä Ä Ä Ä RX
packets:5228715 errors:0 dropped:0 overruns:0 frame:0

Ä Ä Ä Ä Ä Ä Ä Ä Ä TX
packets:4528864 errors:0 dropped:0 overruns:0 carrier:0

Ä Ä Ä Ä Ä Ä Ä Ä Ä collisions:0
txqueuelen:1000

Ä Ä Ä Ä Ä Ä Ä Ä Ä RX
bytes:1796807077 (1713.5 Mb)Ä TX bytes:3737015 (3.5 Mb)

Ä Ä Ä Ä Ä Ä Ä Ä Ä Interrupt:18 Base
address:0x5400 Memory:f6101000-f6101038

Ä

Ä

YukarÄ±daki farklÄ±lÄ±ktan(**PROMISC**)da gÄ¶rebileceÄYimiz gibi ifconfig komutuna promisc parametresini ekleyince Ä¶zellikler satÄ±rÄ±nda arabirimin i½PROMISCi½ moda geÄŖtiÄYi hamen belirdi.

Ä

Promisc moddan cÄ±karmak istediÄYimizde ise

Ä

ifconfig eth0 i½promisc

Ä

komutunu vermemiz yeterlidir.

Ä

NOTE:! Tcpdump komutu ÄŖalÄ±ÄYtÄ±rdÄ±ldÄ±ÄYÄ±nda aÄY arabirimini otomatik olarak promisc moda geÄŖsirir ve tcpdumpi½Ä± sonlandÄ±rdÄ±ÄYÄ±nÄ±zda yine aÄY arabirimini promisc moddan ÄŖÄ±karÄ±r.

Ä

Ä KarÄ±ÄYÄ±k bir aÄYda Ä tcpdump ile sadece kendi makinenizi ilgilendiren paketleri yakalamanÄ±z icap ederse tcpdump'a sadece

Genel: Tcpdump kullanarak AÄY trafiÄYi izlemek i¸ ½ BÄ¶/Ä¼m 1

kendi makinemizle ilgilenmesini sÄ¶yleyebiliriz. Yani kÄ±saca hedef adresi ben olmayan paketlere karÄ±ÄYma demiÄY oluruz, bu bize amacÄ±mÄ±za daha kolay ulaÄYmamÄ±zÄ± saÄYlar .Tcpdump'i ½in baÄYlatÄ±ldÄ±ÄYÄ±nda promisc moda geÄŞmemesini saÄYlamak iÄŞin gerekli parametre yazÄ±nÄ±n ilerleyen bÄ¶/Ä¼mlerinde detaylÄ±ca verilmiÄYtir.

Ä

Ä

KullanÄ±mÄ±

Ä

NOT! Linux/UNIX altÄ±nda tcpdump programÄ±nÄ± kullanabilmek iÄŞin ya root haklarÄ±na sahip olmak lazÄ±m ya da tcpdump programÄ±nÄ±n suid olarak ÄŞalÄ±ÄYmasÄ± lazÄ±m

Ä

NOT! Tcpdump,Ä paketleri kernel'i ½a giriÄY-ÄŞÄ±kÄ±ÄY yapmadan yakalar bu sebeple iptables(Linux iÄŞin) ile yazdÄ±ÄYÄ±nÄ±z kurallar tcpdump'i ½Ä± etkilemez.

Ä

Ä

Ä Tcpdump'Ä±n en basit kullanÄ±mÄ± parametresiz

kullanÄ±mdÄ±r

tcpdump

Gibi.

Ä

**Tcpdump ile
kullanabileceÄYimiz Temel Parametreler**

Ä

Ä

-i / Arabirim SeÄŞimi

Ä

SistemimizdeÄ± birden fazla arabirim varsa ve biz hangi arabirimini dinlemesini belirtmezsek Ä± tcpdump aktif olan aÄY arabirimleri arasÄ±nda numarasÄ± en dÄ¼ÄYÄ¼k olanÄ±nÄ± dinlemeye alÄ±r, mesela 3 adet aktif Ethernet aÄY arabirimimiz var; eth0, eth1, eth2[Linux iÄŞin geÄŞerlidir,diÄYer unix ÄŞeÄYitlerinde farklıÄ±dÄ±r,Ekler kÄ±smÄ±nda diÄYer unixler iÄŞin neler olabileceÄYi listelenmiÄYtir.] ÄYeklindeÄ± biz bu makinede tcpdump komutunu yalÄ±n olarak kullanÄ±rsak tcpdump eth0 arabirimini dinlemeye alacaktır.

Ä

Genel: Tcpdump kullanarak AÄY trafiÄYi izlemek i½ BÄ¶/Ä¼m 1

EÄYer ilk arabirimi deÄYilde istediÄYimiz bir arabirimi dinlemek istiyorsak i½'i parametresi ile bunu belirtebiliriz

Ä

tcpdump -i eth2

Ä

komutu ile sistemimizdeki 3.Ethernet kartÄ±nÄ± dinlemeye alÄ±yoruz.

Ä

-n Ä /Ä°sim Ä±Ä¶zÄ¼mleme

Ä

EÄYer tcpdump ile yakalanan paketlerin dns isimlerinin Ä¶Ä¶zÄ¼lmesini istemiyorsak

-n parametresini kullanabiliriz,

Ä

Genel: Tcpcdump kullanarak AÄY trafiÄYi izlemek i; ½ BÄ¶/Ä¼m 1

normal kullanÄ±m;

Ä Ä Ä Ä Ä

tcpcdump

Ä

17:18:21.531930

IP **huzeyfe.32829** › **erhan.telnet**: S 3115955894:3115955894(0)
win 5840 ‹mss 1460,sackOK,timestamp 826880 0,nop,wscale 0›

Ä

17:18:21.531980

IP **erhan.telnet** › **huzeyfe.32829**: R 0:0(0) ack 3115955895 win 0

Ä

-n parametresi ile kullanÄ±m;

Ä

tcpcdump -n

Ä

Genel: Tcpcdump kullanarak AÄY trafiÄYi izlemek i ½ BÄ¶/Ä¼m 1

17:18:53.802776

IP 192.168.0.100.32835 › 192.168.0.1.telnet: S 3148097396:3148097396(0) win 5840 ‹mss 1460,sackOK,timestamp 859156 0,nop,wscale 0›

Ä

17:18:53.802870

IP 192.168.0.1.telnet › 192.168.0.100.32835: R 0:0(0) ack 3148097397 win 0

Ä

burada **huzeyfe** makinesi 192.168.0.100, **erhan** makinesi 192.168.0.1 IP adresine sahiptir. Ä°simlerin yanÄ±nda **protocol ve port** numaralarÄ±nÄ±nda isimlere Ä°şevrimini istemiyorsak i ½nn parametresini kullanabiliriz

Ä

tcpcdump i ½nn

Ä

yukarÄ±da (-n iÄ°sin)verdiÄYimiz Ä¶rnekte i ½ yerine -nn koyarsanÄ±z hem isim hemde port Ä°şÄ¶zÄ¼mlemesi yapÄ±lmayacaktÄ±r,yani telnet yerine 23 yazacaktÄ±r.

Ä

Ä

-t /Zaman DamgasÄ± GÄ¶sterimi

Ä

EÄYer tcpdump'Ä±n daha sade bir Ä¶Ä±ktÄ± vermesini istiyorsak ekrana yazdÄ±ÄYÄ± satÄ±rlarÄ±n baÄYÄ±ndaki timestamp(zaman damgasÄ±, hangi paketin hangi zaman aralÄ±ÄYÄ±nda yakalandÄ±ÄYÄ±nÄ± belirtir) kÄ±smÄ±nÄ± istemediÄYimizi belirtebiliriz.

Ä

Timestamp[zaman damgasÄ±]leri istemediÄYim durumlarda i; ½ t parametresi ile bunu belirleyebiliriz.

Ä

Timestamp li Ä¶Ä±ktÄ±

tcpdump

```
15:32:13.479577cc.kou.edu.tr.200
> 212.174.108.162.29157: . 68:1528(1460)
ackÄ Ä Ä Ä Ä Ä Ä Ä Ä Ä Ä Ä
53 win 20440 (DF) [tos 0x10]
```

```
15:32:13.479582
cc.kou.edu.tr.200 > 212.174.108.162.29157: P 1528:2456(928) ack 53 win 20440
```

Genel: Tcpcdump kullanarak AÄY trafiÄYi izlemek i; ½ BÄ¶/Ä¼m 1

(DF) [tos 0x10]

Ä

Timestamp(Zaman damgasÄ±)siz Ä§Ä±ktÄ±

Ä

Ä # tcpcdump i;½t

2.174.108.162.29157

› cc.huzeife.net.2000: P 3329:3381(52) ack 11236 win 17520 (DF) [tos 0x20]

cc.huzeife.net.2000

› 2.174.108.162.29157: . ack 2289 win 8576 ‹nop,nop,sack sack 2
{2965:3381}{2393:2861} › (DF) [tos 0x10]

Ä

Ä

-wÄ /Yakalanan paketleri kaydetme

Ä

Tcpcdumpi;½Ä±n yakaladÄ±ÄYÄ± paketleri ekrandan deÄYilde
sonradan incelemek Ä¼zere bir uygun bir ÄYekilde Ä dosyaya yazmasÄ±nÄ± istersek

Genel: Tcpdump kullanarak AÄY trafiÄYi izlemek i; ½ BÄ¶/Ä¼m 1

-w parametresini kullanabiliriz. kaydettiÄYimiz dosya libpcap uyumlu olduÄYü iÄŞin sadece tcpdump ile deÄYil birÄŞok network snifferi tarafÄ±ndan okunup analiz edilebilir.

Ä

Ä

tcpdump -w dosya_ismi

Ä

Ä

-r /KaydedilmiÄY Paketleri Okuma

Ä

-w ile kaydettiÄYimiz paketleri okumak iÄŞinde -r parametresini kullanabiliriz.

Ä Ä

tcpdump -r dosya_ismi

Ä

not!! -w

ile herhangi bir dosyaya kaydederken filtreleme yapabiliriz,yani sadece su tip paketleri kaydet ya da timestampleri kaydetme gibi,aynÄ± ÄYekilde -r ile paketlerle okurken filtre belirtebiliriz.Bu filtrenin -w ile belirlediÄYimiz filtre ile aynÄ± olma zorunluluÄYu yoktur.

Ä

cd /tmp/

tcpdump -w log icmp

tcpdump: listening on eth0, link-type
EN10MB (Ethernet), capture size 96 bytes

ctrl c

Ä

tcpdump -r log -nn

reading
from file log, link-type EN10MB (Ethernet)

17:31:01.225007
IP 192.168.0.100 > 192.168.0.1: icmp 64: echo request seq 0

Genel: Tcpcdump kullanarak AÄY trafiÄYi izlemek i; ½ BÄ¶/Ä¼m 1

17:31:01.225119

IP 192.168.0.1 › 192.168.0.100: icmp 64: echo reply seq 0

17:31:02.224988

IP 192.168.0.100 › 192.168.0.1: icmp 64: echo request seq 1

17:31:02.225111

IP 192.168.0.1 › 192.168.0.100: icmp 64: echo reply seq 1

Ä

-c / Yakalanacak paket miktarÄ±nÄ± belirleme

Ä

tcpcdump'aÄ -c parametresini vererek ne kadar paket yakalayÄ±p duracaÄYÄ±nÄ± sÄ¶yleriz.

Ä

tcpcdump -i eth0 -c 5

Ä

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

Genel: Tcpcdump kullanarak AÄŸ trafiÄŸi izlemek için ½ BÄŸ¼m 1

listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes

*00:59:01.638353 IP maviyan.net.ssh › 10.0.0.2.1040: P
1010550647:1010550763(116) ack 774164151 win 8576*

*00:59:01.638783 IP 10.0.0.2.1040 › maviyan.net.ssh: P 1:53(52) ack
116 win 16520*

*00:59:01.638813 IP maviyan.net.ssh › 10.0.0.2.1040: P 116:232(116)
ack 53 win 8576*

*00:59:01.639662 IP 10.0.0.2.1040 › maviyan.net.ssh: P 53:105(52) ack
232 win 16404*

*00:59:01.640377 IP maviyan.net.ssh › 10.0.0.2.1040: P 232:380(148)
ack 105 win 8576*

5 packets captured

5 packets received by filter

0 packets dropped by kernel

Ä

tcpcdump -c sayi ile belirlediÄŸimiz sayÄ±da
paketi yakaladÄ±ktan sonra ÄŸalÄ±ÄŸmasÄ±nÄ± durduracaktÄ±r.

Ä

Ä

**-s /Yakalanacak paket boyutunu
byte cinsinden belirleme**

Ä

-s parametresi ile yakalanacak paketlerin
boyutunu byte olarak belirleyebiliriz.

Ä

Ä -vÄ /DetaylÄ± Loglama

Ä

-v parametresi ile tcpcdumpi; ½dan biraz daha
detaylÄ± loglama yapmasÄ±nÄ± isteyebiliriz. Mesela bu parametre ileÄ tcpcdump
ÄÄ±ktÄ±larÄ±nÄ± TTL ve ID deÄYerleri ile birlikte edinebiliriz.

Ä

**Ä #
tcpcdump -v**

Genel: Tcpcdump kullanarak AÄY trafiÄYi izlemek i; ½ BÄ¶/Ä¼m 1

tcpcdump:

listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes

17:36:55.161861

IP (tos 0x10, ttlÄ 64, id 17228, offset 0, flags [DF], proto 6, length: 60) huzeyfe.32981 › erhan.ssh: S [tcp sum ok]

4229750775:4229750775(0) win 5840 ‹mss 1460,sackOK,timestamp 1940667 0,nop,wscale 0›

17:36:55.161940

IP (tos 0x0, ttlÄ 64, id 0, offset 0, flags [DF], proto 6, length: 60)

erhan.ssh › huzeyfe.32981: S [tcp sum ok] 3303151192:3303151192(0) ack

4229750776 win 5792 ‹mss 1460,sackOK,timestamp 2233545 1940667,nop,wscale 0›

Ä

-pÄ /Promisc Moddan KaÄ¶Ä±ÄY

Ä

Ä parametresi ile de sniff yaptÄ±ÄYÄ±mÄ±z

arabirimizin promisc moddan Ä¶Ä±kmasÄ±nÄ± saÄYlarÄ±z,promisc moddan Ä¶Ä±kma bize ne saÄYlar? Promisc moddan Ä¶Ä±kma sadece o arabirimimize gelen ve o arabirimimize ilgilendiren paketler iÄYlenir ki bu paketlerde ya broadcast ya da direct o arabirimimizin adresi olmasÄ± lazÄ±m. Daha Ä¶ok tcpcdumpi; ½Ä±n Ä¶alÄ±ÄYtÄ±ÄYÄ± Ä makineye ait bir paket analizi Ä yapmak istediÄYimiz zaman kullanÄ±labilecek tÄ¼rden bir parametredir.

Ä

Mesela yerel aÄYÄ±nÄ±zda baÄYIÄ± bulunduÄYunuz

makinede sorun gidermeye Ä¶alÄ±ÄYtÄ±ÄYÄ± yorsunuz ve bu sebeple tcpcdump Ä¶alÄ±ÄYtÄ±ÄYÄ±p

Genel: Tcpdump kullanarak AÄY trafiÄYi izlemek i; ½ BÄ¶/Ä¼m 1

makinenizi dinlemeye aldÄ±nÄ±z fakat o da ne? tÄ¼m yerel aÄYda geÅŸen paketler ekranÄ±nÄ±zda akÄ±p gidiyor(baÄYIÄ± bulunduÄYunuz aygÄ±tÄ±n HUB olduÄYunu gÄ±z Ä¶nÄ¼ne aldÄ±m)iÄYte bu karmaÄYadan kurtulmak istiyorsak sadece bizim arabirimiz hedefli gelen paketleri almalÄ±yÄ±z

Ä

```
# tcpdumpÄ -p i;½i eth0
```

Ä Ä

host Parametresi

Ä

Sadece belli bir host a ait paketlerin izlenmesini istiyorsak host parametresi ile belirtim yapabiliriz.

Ä

```
bash-2.05b# tcpdumpÄ host  
10.0.0.21
```

Ä

bu komutla kaynak ya da hedef ip adresi 10.0.0.21 olan paketlerin alÄ±nmasÄ±nÄ± istiyoruz.

Ä

dst hostÄ
(Hedef Host Belirtimi)

Ä

dsh host ;hedef host olarak belirtilen
adrese ait paketleri yakalar,

Ä

**# tcpdump -i eth0 dst host
10.0.0.1**

Ä

yukarÄ±daki komutla makinemizin eth0 arabirimine gelen ve hedefi 10.0.0.1 olan tÄ¼m paketler yakalanacaktır, burada dikkat etmemiz gereken bir nokta var o da ÄYu:yerel aÄYÄ±mÄ±zda 10.0.0.21 makinesinden 10.0.0.1 makinesine bir trafik oluÄYtuÄYu zaman, dinlemede olan makinemizde(10.0.0.101)hedef adresi 10.0.0.1 olan paketler oluÄYtuÄYunu gÄ¶receksiniz.

Ä

**# tcpdump -i eth0 dst host
10.0.0.1**

tcpdump: listening on eth0

10:47:20.526325 10.0.0.21 › 10.0.0.1:
icmp: echo request

Ä

ile de hedef ip si 10.0.0.1 olan ip
adreslerini izlemiÄY oluyoruz.

Ä

Ä

**src hostÄ Ä (Kaynak Host
Belirtimi)**

Ä

src host tanÄ±mÄ± ilede kaynak hostu
belirterek dinleme yapabiliriz, mesela kaynak hostu 10.0.0.21 olan paketleri
(10.0.0.21 makinesinde)dinlemeye alalim.

Ä

**# tcpdump -i eth0 src host
10.0.0.21**

Â

tcpdump: listening on eth0

10:52:00.620897 10.0.0.21.3409 ›
baym-cs253.msgr.hotmail.com.1863: P 1541540362:1541540367(5) ack 3598940393 win
17484 (DF)

10:52:01.025286 10.0.0.21.3409 ›
baym-cs253.msgr.hotmail.com.1863: . ack 9 win 17476 (DF)

10:52:14.758635 10.0.0.21.4013 ›
10.0.0.1.telnet: S 3499731684:3499731684(0) win 16384 ‹mss
1460,nop,nop,sackOK› (DF)

Â

sadece ip adresi deÄYil host ismide
belirtebiliriz.

bash-2.05b# tcpdump host hotmail.com

dst ve src i aynÄ± komuttada kullanabiliriz.

ÄrneÄ±,

Genel: Tcpdump kullanarak AÄY trafiÄYi izlemek i ½ BÄ¶IÄ¼m 1

kaynak ip si 10.1.0.59 hedef hostu 10.1.0.1 olan paketleri izlemek istersek

```
# tcpdump src host 10.1.0.59 and dst host 10.1.0.1
```

komutunu verebiliriz.

Ä

burada dikkatimizi ÄŒeken ufak bir deÄYiÄYiklik oldu,src host ve dst host arasÄ±na i ½ and i ½ geldi,evet tcpdump ile kompleks Ä kurallar yazarken sÄ±kÄŒa kullanacaÄYÄ±mÄ±z kelimelerden biri de i ½ and i ½ dir,ilerleyen bÄ¶IÄ¼mlerde i ½ and i ½ in yerine hangi dizimler gelebilir onlarÄ±da gÄ¶receÄYiz. Host parametresi ile de aynÄ± ÄYekilde bir sonuca ulaÄYabiliriz host parametresi ile kaynak ya da hedef hosttan herhangi biri uygunsu paket yakalanÄ±r.

Ä

Ä

port Parametresi (Port Belirtimi)

Ä

belirli bir portu dinlemek istediÄYimizde kullanacaÄYÄ±mÄ±z parametredir. Host gibi src ve dst oneklerini alabilir.

Ä

src ile kaynak portu dst ile hedef portu belirtebiliriz
. dst ya da src Ä¶nekinini kullanmazsak hem kaynak hemde hedefÄ portu alÄ±r.

Ä

tcpdump port 23

Ä

tcpdump dst portÄ 23

ile hedef portu 23 olanlar

Ä

tcpdump src portÄ 23

ile de kaynak portu 23 olan paketler Ä izlemeye
alÄ±nÄ±r.

Ä

Ä

Genel: Tcpdump kullanarak AÄY trafiÄYi izlemek için ½ BÄY¼m 1

AÄYaÄYÄ±daki ÄYrnekte belirli ip ve belirli port numaralarÄ±nÄ± iÄŞeren paketleri port ve isim ÄŞÄY¼mleme yapmamasÄ±nÄ±(-nn)sÄY¼yoruz.

Ä

tcpdump -nn host 192.168.2.165 and port 23

tcpdump: listening on eth0

19:20:00.804501 192.168.2.10.1221 ›
192.168.2.165.23:

S2565655403:2565655403(0) win 16384
‹mss 1460,nop,nop,sackOK› (DF)

Ä

-e / (Layer 2 paket loglama)

Ä

Bu komuta ek olarak için ½e parametresini de verirsek bu sefer tcpdump 2.katmana göre paket yakalama iÄYlemi baÄYlatÄ±r yani bu durumda ip adresleri deÄYilde MAC adresleri ile iÄYlem yapÄ±mÄ±ÄY olur.

Ä

Genel: Tcpcdump kullanarak AÄY trafiÄYi izlemek i¸ ½ BÄ¶/Ä¼m 1

tcpcdump i¸ ½t i¸ ½nn -e

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

*listening on eth0,
link-type EN10MB (Ethernet), capture size 96 bytes*

Ä

*00:0b:db:1c:4b:61
¸ 00:02:44:27:73:79, ethertype IPv4 (0x0800), length 52: IP
192.168.0.100.32768 ¸ 192.168.0.1.33435: UDP, length 10*

*00:0b:db:1c:4b:61 ¸
00:02:44:27:73:79, ethertype IPv4 (0x0800), length 52: IP 192.168.0.100.32768
¸ 192.168.0.1.33436: UDP, length 10*

*00:02:44:27:73:79 ¸
00:0b:db:1c:4b:61, ethertype IPv4 (0x0800), length 80: IP 192.168.0.1 ¸
192.168.0.100: icmp 46: 192.168.0.1 udp port 33436 unreachable*

*00:0b:db:1c:4b:61 ¸
00:02:44:27:73:79, ethertype IPv4 (0x0800), length 52: IP 192.168.0.100.32768
¸ 192.168.0.1.33437: UDP, length 10*

Ä

Ä

Ä

Sumele ve hitit veya kapadokya hostlarÄ± arasÄ±nda geÄŒen trafiÄYi izlemek iÄŒin

Ä

tcpcdump host sumele and \ (hitit or kapadokya \)

Ä

Ä

Kaynaklar;

Ä

<http://www.firewall.cx>

<http://www.olympus.org>

<http://www.tcpcdump.org>

<http://www.huzeyfe.net>

