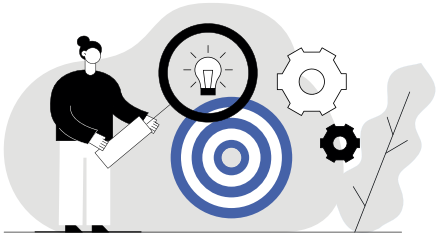
Basque CyberSecurity Centre



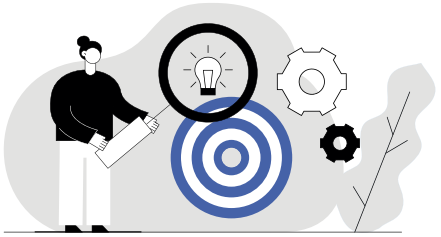
TCPDUMP cheat sheet

Komando-lerrotik exekutatzen den **pakete-analizatzailea** da. Sare bateko trafikoa aztertzeko erabil daiteke, paketeak intertzeptatuz eta erakutsiz.

1. Paketeak atzitzeko aukerak

Sintaxia	Adibidea	Azalpena
-i any	tcpdump –i any	Interfaze guztietatik atzitzen du
-i eth0	tcpdump –i eth0	Interfaze espezifikoetatik atzitzen du (adibidez, Eth0 interfazetik)
-C	tcpdump –i eth0 –c 10	Lehen 10 paketeak atzitzen ditu
-D	tcpdump –D	Eskura dauden interfazeak erakusten ditu
-A	tcpdump –i eth0 -A	ASCIIn inprimatzen du
-w	tcpdump –i eth0 –w tcpdump.txt	Atzipena emandako fitxategi batean gordetzen du
-r	tcpdump –r tcpdump.txt	Fitxategiaren atzipena irakurri eta aztertzen du
-n	tcpdump –n -I eth0	Ez ditu ostalarien izenak ebazten
-nn	tcpdump –n -i eth0	Ostalari eta ataken izenak itzuli eta bilatzen ditu
tcp	tcpdump –i -i eth0 –c 10 –w tcpdump.pcap tcp	TCP paketeak soilik atzitzen ditu
port	tcpdump -i eth0 port 80	Ataka jakin bateko trafikoa atzitzen du
host	tcpdump host 192.168.1.55	Ostalari jakin bateko paketeak atzitzen ditu
net	tcpdump net 10.1.1.0/16	Azpisare bateko paketeak atzitzen ditu
src	tcpdump src 10.1.20.50	Emandako iturburu-helbide bateko paketeak atzitzen ditu
dst	tcpdump dst 10.1.20.50	Xede-helbide espezifiko bat atzitzen ditu
<service>	tcpdump http	Ataka-zenbakian oinarritutako trafikoa iragazten du zerbitzu baterako
<port>	tcpdump port 80	Zerbitzu batean oinarritutako trafikoa iragazten du
port range	tcpdump portrange 21-125	Ataka-barruti batean oinarrituta iragazten du
-S	tcpdump –S http	Pakete osoa zabaltzen du
ipv6	tcpdump IPV6	IPV6 paketeak soilik erakusten ditu
-d	tcpdump –d tcpdump.pcap	Fitxategi irakurgarri bat zabaltzen du irteera estandar batetik
-F	tcpdump –F tcpdump.pcap	Iragazteko sarrera gisa erabiltzen ditu jasotako fitxategiak
-I	tcpdump –I eth0	Interfazea monitore-moduan finkatzen du
-L	tcpdump –L	Datu-moten esteka zabaltzen du interfazerako
-N	tcpdump –N tcpdump.pcap	Ez ditu domeinu-izenak inprimatzen
-K	tcpdump –K tcpdump.pcap	Ez du checksuma egiaztatzen
-p	tcpdump –p –i eth0	Ez du modu nahasian atzitzen

Basque CyberSecurity Centre



2. Monitorea – Irteera-aukerak

Sintaxia	Azalpena
-q	Zehaztasun txikiko hedapen-modua
-t	Ez ditu inprimatzen time stamp-aren xehetasunak dump-en
-v	Zehaztasun txikiko irteera
-vv	Zehaztasun handiagoko irteera
-vvv	Zehaztasun handieneko irteera
-x	Datuak eta goiburuak HEX formatuan inprimatzen ditu
-xx	Datuak eta goiburudun estekak HEX formatuan inprimatzen ditu
-X	Irteera HEX eta ASCII formatuetan inprimatzen du, goiburudun estekak izan ezik
-XX	Irteera HEX eta ASCII formatuetan inprimatzen du, goiburudun estekak barne hartuta
-e	Goiburudun estekak inprimatzen ditu (ethernet)
-S	Zenbaki-segida formatu zehatzean inprimatzen du

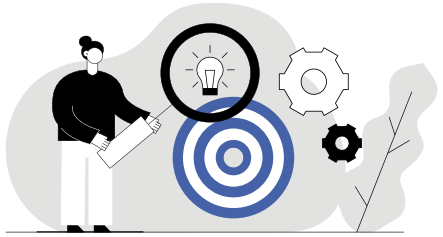
3. Instalazio-komandoa

CENT OS eta REDHAT	$ sudo yum install tcpdump
Fedora	$ dnf install tcpdump
Ubuntu, Debian, Linux Mint	#apt-get install tcpdump

4. Protokoloak

Ether, ffdi, icmp, ip, ip6, ppp, radio, rarp, slip, tcp, udp, wlan

Basque CyberSecurity Centre



5. Atzipenak iragazteko protokoloak dituzten komando komunak	
src/ dst host (ostalariaren izena edo IPa)	IP helbidearen iturburuaren/xedearen edo emandako ostalariaren izenaren arabera iragazten du
ether src/ dst host (etherneta, ostalariaren izena edo IPa)	Iturburua/xedea etherneteko ostalariaren arabera iragazten du
src/ dst net (azpisare-maskara CIDRn)	Azpisare bidez iragazten du
tcp/udp src/ dst port (ataka-zenbakia)	TCP edo UDP paketeak iragazten ditu emandako iturburuaren edo atakaren arabera
tcp/udp src/ dst portrange (ataka-barrutia)	TCP edo UDP paketeak iragazten ditu ataka-barruti baten arabera
ether/ ip broadcast	Broadcast ethernet edo IP bidez iragazten du
ether/ ip multicast	Multicast ethernet edo IP bidez iragazten du

6. Eragile logikoak			
Eragilea	**Sintaxia**	**Adibidea**	**Azalpena**
AND	and, &&	tcpdump –n src 192.168.1.55 and dst puerto 21	Iragazketa-aukerak konbinatzen ditu
OR	or, ||	tcpdump dst 10.10.20.1 && ! icmp	Iragazteko baldintzetako edozein
EXCEPT	not, !	tcpdump dst 10.20.10.1 and not icmp	Baldintza ukatzen du
LESS	<	tcpdump <20	20ko tamainatik beherako paketeak erakusten ditu
GREATER	>	Tcpdump >=20	20ko tamaina edo handiagoa duten paketeak erakusten ditu